UNIVERSIDAD DE GRANADA

UNIVERSIDAD DE GRANADA

PROGRAMA DE DOCTORADO EN CIENCIAS ECONÓMICAS Y EMPRESARIALES

TESIS DOCTORAL

# LA DIVULGACIÓN DE INFORMACIÓN SOBRE CIBERSEGURIDAD EN EMPRESAS COTIZADAS DE AMÉRICA LATINA


Presentado por:
**Maricela Ramírez**

Dirigida por:
**María Elena Gómez Miranda**


Granada – España, 2024

UNIVERSIDAD DE GRANADA

PROGRAMA DE DOCTORADO EN CIENCIAS ECONÓMICAS Y EMPRESARIALES

TESIS DOCTORAL

# LA DIVULGACIÓN DE INFORMACIÓN SOBRE CIBERSEGURIDAD EN EMPRESAS COTIZADAS DE AMÉRICA LATINA


Presentado por:
**Maricela Ramírez**

Dirigida por:
**María Elena Gómez Miranda**


Granada – España, 2024

Editor: Universidad de Granada. Tesis Doctorales
Autor: Maricela Ramírez
ISBN: 978-84-1195-683-3
URI: https://hdl.handle.net/10481/102484

## ÍNDICE DE CONTENIDO

**INTRODUCCIÓN** ..... **13**
**CAPÍTULO 1. LA CIBERSEGURIDAD** ..... **25**
**1.1. La Ciberseguridad** ..... **29**
1.1.1. Concepto de Ciberseguridad ..... 29
1.1.2. Origen y evolución de los tipos de ciberataques ..... 44
**1.2. Marco normativo y regulatorio de Ciberseguridad en el ámbito internacional** ..... **50**
**1.3. La Ciberseguridad en las organizaciones** ..... **55**
1.3.1. Gobernanza del riesgo de Ciberseguridad ..... 58
1.3.2. Estrategia de Ciberseguridad ..... 63
1.3.3. Gestión de riesgos de Ciberseguridad ..... 64
1.3.4. Implicaciones financieras ..... 69
**1.4. Conclusiones** ..... **69**
**1.5. Referencias** ..... **72**
**CAPÍTULO 2. LA DIVULGACIÓN DE INFORMACIÓN SOBRE RIESGOS CIBERNÉTICOS** ..... **85**
**2.1. El Riesgo Corporativo** ..... **89**
**2.2. Divulgación de información corporativa sobre riesgos** ..... **93**
2.2.1. Estados Unidos ..... 95
2.2.2. Unión Europea ..... 96
2.2.3. Acuerdo de Basilea III ..... 97
2.2.4. América Latina ..... 98
**2.3. La divulgación de información corporativa sobre riesgos de Ciberseguridad** ..... **98**
**2.4. Tipos de divulgación de información sobre Ciberseguridad** ..... **103**
2.4.1. Divulgación voluntaria de información de Ciberseguridad ..... 105
2.4.2. Divulgación de información obligatoria en Ciberseguridad ..... 109
**2.5. Informes y comunicaciones utilizados para la divulgación de información sobre Ciberseguridad** ..... **118**

2.5.1. Las directrices del Estándar Global Reporting Iniciative (GRI) .....119
2.5.2. Los estándares emitidos por el American Sustainability Accounting Standard Board (SASB) .....120
2.5.3. El marco del International Integrated Reporting Council (IIRC).....121
2.5.4. Presentaciones 10-K en EDGAR.....121
2.5.5. Presentaciones 20-F en EDGAR .....122
**2.6. Conclusiones..... 123**
**2.7. Referencias .....125**
**CAPÍTULO 3. ALCANCE DE LA DIVULGACIÓN DE INFORMACIÓN SOBRE CIBERSEGURIDAD EN AMÉRICA LATINA.....133**
**3.1. La Ciberseguridad en el Contexto Latinoamericano ..... 137**
**3.2. Propuesta de un Índice de Divulgación de Información sobre Ciberseguridad.. ..... 145**
3.2.1. Población y muestra **..... 146**
3.2.2. Índice de Divulgación de Información sobre Ciberseguridad propuesto**..... 150**
**3.3. Análisis de la Divulgación de Información sobre Ciberseguridad en Empresas Latinoamericanas ..... 162**
3.3.1. Alcance de las Revelaciones sobre Ciberseguridad por Dimensiones del Índice 166
3.3.2. Alcance de las Revelaciones de Ciberseguridad en América Latina por Países..182
3.3.3. Alcance de las Revelaciones de Ciberseguridad por Sectores .....189
**3.4. Conclusiones..... 196**
**3.5. Referencias ..... 199**
**CAPÍTULO 4. INCIDENCIA DEL GOBIERNO CORPORATIVO SOBRE LA DIVULGACIÓN DE INFORMACIÓN SOBRE RIESGOS DE CIBERSEGURIDAD EN AMÉRICA LATINA.....249**
**4.1. El Gobierno Corporativo..... 255**
4.1.1. Evolución Histórica del Concepto de Gobierno Corporativo .....255
4.1.2. Teorías de Gobierno Corporativo.....273
4.1.3. Mecanismos de Gobierno Corporativo .....282
**4.2. Gobierno Corporativo en América Latina..... 289**
4.2.1. Marco Normativo .....289

4.2.2. Prácticas de Gobierno Corporativo en América Latina .....293
**4.3. Investigación sobre Gobierno Corporativo como Factor de Divulgación de Ciberseguridad ..... 296**
4.3.1. Marco teórico .....297
4.3.2. Literatura Previa.....299
4.3.3. Hipótesis de Estudio.....310
**4.4. Metodología..... 315**
4.4.1. Población y Muestra.....315
4.4.2. Variables .....316
4.4.3. Modelo .....318
**4.5. Resultados y Discusión..... 319**
**4.6. Conclusiones.....325**
**4.7. Referencias ..... 327**
**CAPÍTULO 5. INCIDENCIA DE LAS CARACTERÍSTICAS PAÍS EN LA DIVULGACIÓN DE INFORMACIÓN SOBRE RIESGOS DE CIBERSEGURIDAD EN AMÉRICA LATINA.....365**
**5.1. Panorama de la Ciberseguridad Nacional ..... 369**
5.1.1. Índice Global de Ciberseguridad.....370
5.1.2. Índice Global de Ciberseguridad en la esfera internacional.....377
5.1.3. Índice Global de Ciberseguridad en América Latina.....384
**5.2. Panorama de la Gobernanza Nacional: Índice de Gobernanza Mundial ..... 402**
5.2.1. Índice de Gobernanza Mundial en América Latina .....404
**5.3. Panorama de la Globalización: Índice de la Globalización..... 410**
5.3.1. Índice de la Globalización de América Latina.....411
**5.4. Panorama Económico y Social: Índice de Desarrollo Humano ..... 413**
5.4.1. Índice de Desarrollo Humano en América Latina.....414
**5.5. Investigación sobre variables país como factor de divulgación de riesgos..... 415**
5.5.1. Marco teórico .....415
5.5.2. Literatura Previa.....418
5.5.3. Hipótesis del Estudio .....422
**5.6. Metodología..... 426**

5.6.1. Población y Muestra.....426
5.6.2. Variables .....427
5.6.3. Modelo .....429
**5.7. Resultados y Discusión ..... 430**
**5.8. Conclusiones..... 436**
**5.9. Referencias ..... 437**
**CAPÍTULO 6. CONCLUSIONES, IMPLICACIONES, LIMITACIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN .....484**
**6.1. Conclusiones..... 486**
**6.2. Implicaciones ..... 494**
**6.3. Limitaciones y futuras líneas de investigación……...491**
**6.4. Referencias ……...492**

# ÍNDICE DE TABLAS

Tabla 1. Definiciones de Ciberseguridad en la literatura previa ..... 34
Tabla 2. Definiciones de Ciberseguridad planteadas por organismos internacionales... 40
Tabla 3. Estudios sobre efectos de la regulación en la Divulgación de Ciberseguridad ..... 104
Tabla 4. Estudios previos relacionados con la divulgación de información voluntaria 108
Tabla 5. Estudios previos relacionados con la divulgación de información obligatoria ..... 116
Tabla 6. Muestra de empresas por país, índice bursátil y sector de actividad..... 147
Tabla 7. Empresas que componen la muestra por país..... 147
Tabla 8. Investigación previa bajo la técnica del análisis de contenido ..... 150
Tabla 9. Instrumentos de divulgación en estudios previos de Ciberseguridad..... 153
Tabla 10. Índice de Divulgación de Ciberseguridad ..... 154
Tabla 11. Alfa de Cronbach..... 161
Tabla 12. Normativa relacionada con Ciberseguridad en los países objeto de estudio 164
Tabla 13. Alcance de la divulgación de información en las dimensiones de la Ciberseguridad en Latinoamérica en el período 2016-2020..... 166
Tabla 14. Prueba de diferencia de medias índice de divulgación entre 2016 y 2020... 182
Tabla 15. Medidas descriptivas de Índice de Divulgación de Ciberseguridad a nivel país (2016-2020) ..... 183
Tabla 16. Índice de Divulgación de Ciberseguridad a nivel país ..... 184
Tabla 17. Prueba no paramétrica para igualdad del índice de divulgación entre países ..... 189
Tabla 18. Alcance de la Divulgación de Ciberseguridad en Latinoamérica por sectores ..... 190
Tabla 19. Prueba no paramétrica para igualdad del índice de divulgación entre sectores ..... 196
Tabla 20. Conceptos de Gobierno Corporativo de aceptación internacional ..... 269
Tabla 21. Códigos y normativas de Gobierno Corporativo vigentes en América Latina ..... 292

Tabla 22. Prácticas de Gobierno Corporativo en países objeto de estudio..... 294
Tabla 23. Estudios previos sobre la incidencia del Gobierno Corporativo en la divulgación de riesgos ..... 302
Tabla 24. Estudios previos sobre la Divulgación de Riesgos de Ciberseguridad y las características de la Junta ..... 309
Tabla 25. Resumen de las medidas utilizadas para las variables..... 318
Tabla 26. Estadísticas descriptivas ..... 320
Tabla 27. Matriz de Correlaciones ..... 321
Tabla 28. Factor de Inflación de la Varianza VIF ..... 322
Tabla 29. Resultados del análisis de regresión ..... 323
Tabla 30. Voz y Responsabilidad ..... 407
Tabla 31. Estabilidad Política y Ausencia de Violencia/Terrorismo..... 407
Tabla 32. La Eficacia del Gobierno..... 408
Tabla 33. Calidad Regulatoria ..... 408
Tabla 34. Estado de Derecho ..... 409
Tabla 35. Puntajes percepción sobre corrupción ..... 409
Tabla 36. Estudio previo sobre los efectos de las características institucionales a nivel país y la divulgación de información de Ciberseguridad ..... 419
Tabla 37. Estudios previos sobre los efectos de las variables de gobernanza nacional en la divulgación de información corporativa ..... 421
Tabla 38. Resumen de las medidas utilizadas para las variables..... 429
Tabla 39. Estadísticas descriptivas de variables ..... 431
Tabla 40. Matriz de correlación..... 432
Tabla 41. Factor de inflación de la varianza VIF ..... 433
Tabla 42. Resultados del análisis de regresión ..... 435

## ÍNDICE DE FIGURAS

Figura 1. Artículos de investigación período 2002-2022 ..... 30
Figura 2. Áreas de conocimiento de Ciberseguridad en el alcance CyBOK..... 31
Figura 3. Dominios del término Ciberseguridad ..... 32
Figura 4. Seguridad de la información y Ciberseguridad..... 37
Figura 5. Componentes en la definición de Ciberseguridad..... 39
Figura 6. Índice de Ciberseguridad por dimensiones en países de América Latina (2020) ..... 143
Figura 7. Índice de Ciberseguridad en países en América Latina (2014, 2017 y 2018)144
Figura 8. Evolución del Índice de divulgación de Ciberseguridad a nivel de dimensión ..... 169
Figura 9. Alcance de la divulgación de información sobre Gobernanza de la Ciberseguridad en Latinoamérica en el período 2016-2020..... 170
Figura 10. Alcance de la divulgación de información sobre Estrategia de la Ciberseguridad en Latinoamérica en el período 2016-2020..... 173
Figura 11. Alcance de la divulgación de información en Gestión de Riesgos de Ciberseguridad en Latinoamérica en el periodo 2016-2020..... 175
Figura 12. Alcance de las Revelaciones sobre Implicaciones Financieras de la Ciberseguridad en Latinoamérica en el período 2016-2020..... 177
Figura 13. Alcance de las Revelaciones sobre Ciberseguridad de los diez ítems de mayor relevancia..... 178
Figura 14. Alcance de la divulgación de información de Ciberseguridad (Índice) 2016 y 2020 ..... 181
Figura 15. Índice de divulgación de Ciberseguridad a nivel país por año..... 185
Figura 16. Dispersión de la divulgación por países..... 187
Figura 17. Distribución de frecuencias del índice entre países ..... 188
Figura 18. Índice de divulgación de Ciberseguridad a nivel de sector por año..... 193
Figura 19. Dispersión del índice de divulgación por sectores..... 194
Figura 20. Distribución de frecuencias del índice por sectores..... 195
Figura 21. Puntajes promedio de los pilares por región 2015 ..... 379

Figura 22. Puntajes promedio de los pilares por región 2017 ..... 380
Figura 23. Puntajes promedio de los pilares por región 2018 ..... 381
Figura 24. Puntajes promedio de los pilares por región 2020 ..... 382
Figura 25. Índice Global de Ciberseguridad por país ..... 385
Figura 26. Puntajes promedio de los pilares por país 2017 ..... 387
Figura 27. Puntajes promedio de los pilares por país 2018 ..... 388
Figura 28. Puntajes promedio de los pilares por país 2020 ..... 389
Figura 29. Medidas legales en los países objeto de estudio Informe (ITU, 2020) ..... 391
Figura 30. Medidas técnicas en los países objeto de estudio Informe (ITU, 2020) ..... 392
Figura 31. Medidas organizacionales en los países objeto de estudio Informe (ITU, 2020) ..... 395
Figura 32. Medidas de creación de capacidad en los países objeto de estudio Informe (ITU, 2020) ..... 397
Figura 33. Medidas de cooperación en los países objeto de estudio ITU (2020) ..... 400
Figura 34. Gobernanza en América Latina 2016- 2020 ..... 406
Figura 35. Índice de Globalización países de América Latina ..... 413
Figura 36. Índice de Desarrollo Humano Mundial 2016-2020 ..... 414
Figura 37. Índice de Desarrollo Humano en América Latina 2016-2020 ..... 415

# INTRODUCCIÓN

La dinámica mundial de las tecnologías y las comunicaciones en la sociedad digitalizada y conectada de hoy define el desempeño de los gobiernos, el quehacer de las organizaciones y la vida de las personas. Según WEF (2023), entre los mayores riesgos globales clasificados por gravedad a corto y largo plazo se encuentra el riesgo de la ciberdelincuencia generalizada y la Ciberseguridad. En particular, existe la necesidad de abordar los riesgos de Ciberseguridad desde una perspectiva de sistemas de múltiples escalas, reconociendo las diversas interacciones entre los sistemas cibernéticos, físicos y humanos (Collier et al., 2013). Así, la cobertura del concepto de Ciberseguridad corrobora su naturaleza multidisciplinaria y la omnipresencia de las preocupaciones de seguridad cibernética en toda la sociedad (Cains et al., 2021). Bajo este marco, la vulnerabilidad de los sistemas informáticos obliga a implementar procesos cada vez más resilientes que anticipen los ataques cibernéticos y aumenten la capacidad de respuesta ante la materialización de incidentes informáticos a través de estrategias de inteligencia de amenazas, resiliencia tecnológica, recuperación ante desastres y coberturas de ciber riesgo.

Es a partir de esta problemática que el riesgo de Ciberseguridad se incorpora dentro de los riesgos corporativos como un tema material y, desde la responsabilidad social empresarial, en un tópico objeto de divulgación de información en los reportes anuales corporativos preparados bajo diferentes estándares de aceptación nacional e internacional. En efecto, los inversionistas reclaman más información sobre estos riesgos y las violaciones de datos, y cómo las empresas están abordando estos temas (Amir et al., 2018). De esta forma, la divulgación sobre gestión de riesgos de Ciberseguridad permite evaluar mejor si las empresas están gestionando los riesgos de Ciberseguridad y cómo lo están haciendo (SEC, 2022).

Una cantidad limitada de estudios han analizado la divulgación de la seguridad cibernética (Héroux & Fortin, 2020). La literatura previa sobre divulgación de riesgos de Ciberseguridad es reciente y la mayoría se ha desarrollado en el contexto estadounidense (Amir et al., 2018; Berkman et al., 2018; Ettredge et al., 2018; Gao et al., 2020; Gordon et al., 2010; Hilary et al., 2016; Wang et al., 2013) y en Canadá (Héroux & Fortin, 2020;

Radu & Smaili, 2021), países que cuentan con guías que incorporan el tema de las revelaciones de Ciberseguridad [Guías Division of Corporation Finance & SEC (2011); SEC (2018; 2022) y CSA ACVM (2013; 2017), respectivamente]. Por su parte, Barry et al. (2021) estudian la incidencia de las diferencias institucionales entre Estados Unidos y China en relación con las revelaciones de Ciberseguridad. En el contexto europeo, únicamente Eijkelenboom & Nieuwesteeg (2021) han realizado aportes desde el análisis de la divulgación de Ciberseguridad en los Países Bajos. Mientras que Masud & Hossain, (2022), examinan la importancia de la Junta en la Divulgación de Ciberseguridad en la industria bancaria de Bangladesh.

Respecto a la literatura de la divulgación de información de Ciberseguridad en América Latina podemos afirmar que, según nuestra búsqueda, es inexistente. De esta manera, el presente estudio busca cerrar esta brecha y aportar nuevo conocimiento a la escasa investigación relacionada con la divulgación de información sobre Ciberseguridad en general, y en el ámbito latinoamericano en particular.

Según OAS (2019), Internet ha revolucionado el mundo que nos rodea y la forma en que interactuamos con los demás, siendo particularmente cierto en el caso de América Latina, donde casi el 70% de la población está en línea y la tasa de crecimiento de usuarios de Internet es la tercera más alta del mundo –2,4% entre 2000 -2019. En consecuencia, el riesgo cibernético es una realidad latente en la región y la fragilidad del comportamiento económico del mercado bursátil latinoamericano requiere de estrategias corporativas que, como la divulgación de información, permitan mejorar la confianza del inversionista y demás partes interesadas. De esta manera, esta investigación permitirá conocer la situación actual de la región latinoamericana frente al alcance de las revelaciones sobre seguridad cibernética en el ámbito corporativo.

Es importante señalar que las empresas cotizantes de América Latina que participan en el mercado bursátil estadounidense reportarán en el informe anual 20 F ítem 3D los factores de riesgo relacionados con el riesgo cibernético de acuerdo con SEC (2018) y, recientemente, SEC (2022). Sin embargo, el resto de las empresas latinoamericanas

incorporan las revelaciones de Ciberseguridad en sus informes anuales de manera voluntaria, debido a que no existe una normativa que refiera la divulgación del riesgo cibernético en particular. En este sentido, los entes de vigilancia y control, especialmente en el sector financiero y desde las directrices de Gobierno Corporativo, gestión de riesgos y privacidad de los datos, entre otros, motivan la posibilidad de que las organizaciones realicen revelaciones sobre Ciberseguridad. Es de resaltar que, en el análisis de contenido, el riesgo de Ciberseguridad en las empresas latinoamericanas, en un alto porcentaje, es concebido por parte de las organizaciones como un riesgo operativo en el sistema de gestión de riesgos empresarial.

En el ámbito internacional, la última década ha sido testigo de un sinnúmero de incidentes de Ciberseguridad de gran magnitud, entre los que podemos destacar el ataque de WannaCry (2017), el robo de datos de Equifax (2017), el ataque de NotPetya (2017), las fugas de datos Facebook y Cambridge Analytica (2018) y el ataque SolarWinds (2020). Estos ciberataques han tenido importantes repercusiones en el panorama corporativo. Entre ellos, han desencadenado que en los últimos años las empresas reciban presiones para divulgar información relacionada con el riesgo cibernético. Pero, en general, existe un desconocimiento sobre qué aspectos informar y cómo hacerlo. Por ello, sería interesante diseñar una herramienta que permita conocer el alcance de las divulgaciones de Ciberseguridad desde las dimensiones que se manejan en el ámbito organizacional y, a la vez, estudiar qué factores inciden en el nivel de divulgación de información sobre Ciberseguridad, desde las características del Gobierno Corporativo y desde algunos determinantes propios del país de origen de las empresas.

Bajo este contexto, el principal propósito de este trabajo es llevar a cabo un estudio sobre la divulgación de información de Ciberseguridad en empresas cotizadas de América Latina. Hemos seleccionado América Latina por ser una región con literatura inexistente en el tema de divulgación sobre Ciberseguridad que, además, representa el comportamiento de los países emergentes. Para ello, se han establecido una serie de objetivos específicos a alcanzar a lo largo de este trabajo.

En primer lugar, presentar y analizar de forma sistemática el estado del arte del concepto de Ciberseguridad, el marco normativo internacional que la regula y sus componentes temáticos.

Seguidamente, describir y relacionar los principales antecedentes de la divulgación de riesgos, en general, y de la divulgación de riesgos de Ciberseguridad, en particular, desde una revisión exhaustiva de la literatura previa.

A continuación, elaborar un índice de divulgación de información como instrumento de medición del alcance de la divulgación sobre Ciberseguridad, a partir de su aplicación en la muestra del estudio, mostrando si existen diferencias entre países y sectores de actividad.

Finalmente, analizar qué factores pueden afectar al nivel de divulgación de información sobre Ciberseguridad en las empresas latinoamericanas. Y ello desde dos perspectivas. En primer lugar, a nivel de empresa, estudiando la relación entre las características del Gobierno Corporativo y el alcance de la divulgación de Ciberseguridad en la región. En segundo lugar, a nivel de país, analizando la influencia de los determinantes propios de la nación de origen de las empresas sobre el alcance de la divulgación de información sobre Ciberseguridad.

Para la realización de este estudio contamos con la información correspondiente a 85 empresas listadas en los principales índices bursátiles de los países latinoamericanos de mayor capitalización de la región: Argentina, Brasil, Chile, Colombia, México y Perú. Estas empresas desarrollan su actividad en cuatro sectores económicos distintos: energía, financiero, consumo discrecional y materiales. La muestra final arrojó un total de 425 observaciones en el período 2016-2020. La recopilación de los datos se realiza a partir del análisis de contenido de los informes anuales publicados en los sitios web de las empresas y del informe 20 F en el caso de las empresas emisoras en Estados Unidos reguladas por SEC.

Además de la introducción, este trabajo consta de seis capítulos. En el primer capítulo, desde un enfoque cualitativo y de forma sistemática, a partir de un análisis documental y una revisión exhaustiva de la literatura, elaboramos un estado del arte que nos permita identificar los diversos conceptos de Ciberseguridad y los principales avances del tema en el campo investigativo. En este sentido, podemos indagar si existe un único concepto de aceptación mundial del término ¨Ciberseguridad¨, y si su desarrollo denota la incorporación de algunos componentes o elementos básicos en su significado. Seguidamente, describimos el origen y la evolución de los tipos de ciberataques, sucesos que nos permiten confirmar el avance de la seguridad cibernética, y su actual cobertura global a medida que la tecnología avanza y el aumento de las amenazas cibernéticas crece y se diversifica. En esta misma línea, en el siguiente epígrafe buscamos relacionar el marco normativo y regulatorio de la Ciberseguridad en el ámbito internacional con el objetivo de definir las principales iniciativas de aplicación mundial que repercutirán, de forma directa, en las regulaciones nacionales objeto de estudio. Por último, en este capítulo, proponemos una estructura que agrupa en cuatro los componentes temáticos de la Ciberseguridad en las organizaciones: gobernanza, estrategia, gestión del riesgo e implicaciones financieras. A partir de estas dimensiones creemos que se abarca la totalidad de la organización y se estipulan las diferentes áreas a nivel empresa entorno a la divulgación de Ciberseguridad.

En el capítulo dos, desde un análisis documental, se presenta una recopilación cronológica de los principales acontecimientos que dibujan la historia del riesgo corporativo a nivel mundial, con el fin de comprender los principales antecedentes relacionados con la actual gestión de riesgos. A continuación, se presentan las características de la divulgación de información sobre riesgos en general, a partir de algunos referentes internacionales: Estados Unidos, Unión Europea, Acuerdo de Basilea y América Latina. Desde estos diversos contextos se busca interpretar el avance de la divulgación de información sobre riesgo corporativo y sus diferentes connotaciones. En el siguiente epígrafe concentramos nuestra atención en la divulgación de información corporativa sobre riesgos de Ciberseguridad, definiendo la literatura previa y las regulaciones que enmarcan las características propias de la rendición de cuentas de este tipo de riesgo en particular.

Posteriormente, recopilamos las características y condicionantes de las revelaciones de Ciberseguridad, diferenciando la información voluntaria de la obligatoria. Por último, en este capítulo se exponen los informes y comunicaciones utilizados para la divulgación de información en el ámbito internacional: las directrices del Estándar Global Reporting Iniciative (GRI), los estándares emitidos por el American Sustainability Accounting Standard Board (SASB) y las presentaciones EDGAR 10-K y 20-F, describiendo de forma puntual en qué aparte de cada informe se presume se realizará el reporte de información de Ciberseguridad en particular.

En el capítulo tres, a partir de un análisis de la situación de la Ciberseguridad en el contexto latinoamericano, identificamos los avances de los países de la región entorno a los principales requerimientos internacionales, así como, las limitaciones más marcadas para enfrentar los ataques que se producen en el ciberespacio. Bajo este panorama particular de los compromisos de América Latina frente a la seguridad cibernética, y dada la inexistencia de un instrumento de medición del alcance de la divulgación de la Ciberseguridad para las empresas de la región, planteamos un índice autoconstruido. Este instrumento de medición ha sido validado, estableciendo su consistencia a partir del cálculo del coeficiente de Cronbach utilizando la matriz de correlación para comprobar la fiabilidad y consistencia con los ítems seleccionados de la muestra. El índice propuesto, que se estructura en cuatro ejes temáticos que representan el núcleo de cómo operan las organizaciones (gobernanza, estrategia, gestión de riesgos e implicaciones financieras), podrá ser utilizado en cualquier contexto específico, debido a que se construye a partir de estándares nacionales e internacionales de amplia aceptación mundial. La aplicación de este índice en las empresas cotizadas de Argentina, Brasil, Chile, Colombia, México y Perú, nos permite evaluar el estado de las revelaciones de Ciberseguridad y, además, establecer comparaciones a nivel de dimensiones, países y sectores de actividad en Latinoamérica.

Una vez se conoce el nivel de la divulgación de Ciberseguridad en América Latina, en el capítulo cuatro buscamos evaluar si existe una relación condicionante en el contexto corporativo que enmarque el alcance de estas revelaciones. Para lograr este objetivo, en

un primer momento realizamos una búsqueda documental que nos permita definir la evolución histórica del Gobierno Corporativo y delimitar los antecedentes que enmarcan su estado actual. Seguidamente, presentamos las teorías y los mecanismos más utilizados en la investigación de Gobierno Corporativo, elementos que nos permiten la formulación de las hipótesis de nuestro estudio. La descripción del contexto del Gobierno Corporativo en América Latina, nos mostrará las circunstancias propias de las empresas cotizantes de la región entorno a su marco normativo, y un análisis de la aplicación de las principales prácticas de Gobierno Corporativo en los países objeto de estudio. Desde las condiciones expuestas, se realiza un estudio empírico a partir de la investigación del Gobierno Corporativo como factor de la divulgación de riesgos de Ciberseguridad. Para ello, a partir del contexto de empresa, y desde la teoría de la agencia y la teoría de la partes relacionadas, evaluamos la incidencia de las características del Gobierno Corporativo: tamaño de la Junta, porcentaje de mujeres y porcentaje de miembros independientes dentro del consejo, la delegación del control de los riesgos de Ciberseguridad al Comité de Auditoría o la designación de estos riesgos cibernéticos a un comité exclusivo en Ciberseguridad dentro de la Junta Directiva. Para el desarrollo del estudio empírico estimamos un modelo Data Panel por efectos fijos en concordancia con los únicos estudios que persiguen evaluar la influencia de algunos factores de Gobierno Corporativo en la divulgación de información sobre Ciberseguridad (Masud & Hossain, 2022; Radu & Smaili, 2021).

En el capítulo cinco, al igual que en el capítulo anterior, evaluamos la existencia de una relación condicionante que enmarque el alcance de las revelaciones de Ciberseguridad en América Latina, esta vez a partir de determinantes a nivel país. Para lograr este objetivo, en primer lugar, se describe la situación de la Ciberseguridad en la esfera internacional y, en segundo lugar, se analiza la situación de la Ciberseguridad en América Latina, exponiendo la realidad de la Ciberseguridad desde las dimensiones contempladas a nivel global: medidas legales, organizacionales, técnicas, de creación de capacidades y de cooperación en el Índice Global de Ciberseguridad. En esta misma línea, a partir de los resultados de la aplicación del Índice de Gobernanza se evalúan los seis pilares: voz y responsabilidad, estabilidad política y ausencia de violencia/terrorismo, efectividad del

gobierno, calidad regulatoria, imperio de la ley y control de la corrupción. De la aplicación del Índice de Globalización se mide la conectividad, la integración e interdependencia global de los países en las esferas culturales, ecológicas, económicas, políticas, sociales y tecnológicas en Latinoamérica. Por último, la medición del desarrollo humano en la región nos describe el panorama social y económico de América Latina, durante el período objeto de estudio 2016-2020.

Con base en este diagnóstico, resultado de la aplicación de cada índice multidimensional, a partir de la teoría institucional y a partir de la literatura previa, se plantean como hipótesis de estudio la relación de las variables país (Índice Global de Ciberseguridad, Índice de Gobernanza, Índice de Globalización e Índice de Desarrollo Humano) como factor de la divulgación de riesgos de Ciberseguridad. Para el desarrollo del estudio empírico estimamos un modelo Data Panel por efectos fijos tomando como referente el único estudio que busca evaluar la incidencia de los determinantes definidos a nivel país en la divulgación de información (Barry et al., 2021) .

Finalmente, en el capítulo seis se presentan las conclusiones del trabajo y sus principales implicaciones, las limitaciones del estudio y las líneas de investigación que se podrían abordar en el futuro.

## Referencias


Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Barry, T., Jona, J., & Soderstrom, N. S. (2021). The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3916525

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. https://doi.org/10.1111/RISA.13687

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems and Decisions 2013 33:4*, *33*(4), 469–470. https://doi.org/10.1007/S10669-013-9484-Z

CSA ACVM. (2013). *CSA Staff Notice 11-326 - Cyber Security*.

https://www.osc.ca/en/securities-law/instruments-rules-policies/1/11-326/csa-staff-notice-11-326-cyber-security

CSA . (2017). *CSA Multilateral Staff Notice 51-347-Disclosure of cyber security risks and incidents*. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

Division of Corporation Finance, & SEC. (2011). *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law and Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly: Management Information Systems*,

*34*(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692

Héroux, S., & Fortin, A. (2020). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2852519

Masud, M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*. https://doi.org/10.1108/JAEE-07-2021-0237

OAS. (2019). Challenges of cyber risk in the financial sector for Colombia and Latin America. *Asobancaria*, 170. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Rel ated Disclosure. *Journal of Business Ethics*, *1*, 3. https://doi.org/10.1007/s10551-020-04717-9

SEC. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

SEC. (2022). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. *13*(34), 1–204.

Wang, T., Ulmer, J. R., & Kannan, K. (2013). The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities. *Journal of Organizational Computing and Electronic Commerce*, *23*(3), 200–223. https://doi.org/10.1080/10919392.2013.807712

WEF. (2023). *The Global Risks Report 2023 18th Edition*.

# CAPÍTULO 1. LA CIBERSEGURIDAD

A medida que las amenazas a la Ciberseguridad se multiplican, aumentan y se fusionan, es imperativo que la comunidad mundial trate el riesgo de Ciberseguridad como un desafío sistémico que requiere una toma de decisiones colectivas y una acción coordinada entre los gobiernos, el sector privado y la sociedad civil (WEF, 2022). La transformación digital y las nuevas tecnologías, como *big data*, inteligencia artificial, movilidad como servicio, Internet de las cosas, computación cuántica o *blockchain*, entre otras, en algunos casos democratizan la sociedad digital, en otros aumentan el poder de algunos países u organizaciones, generando ventajas competitivas: apertura de nuevos mercados, innovadoras estrategias de defensa, ataque y control en un mundo no físico e ilimitado denominado ciberespacio. Desde la geopolítica internacional es imprescindible citar el duopolio por la superioridad tecnológica que representan Estados Unidos y China, y la permanente competencia entre estas dos naciones por el liderazgo mundial, aspecto que marca el devenir de la Ciberseguridad.

Desde la esfera internacional se observa cada vez más la participación de un variado número de actores: ciberdelincuentes, ciberactivistas, estados nación que generan un escenario sin fronteras para este tipo de delitos; situación que, aunada a la falta de colaboración o confianza entre estados y organizaciones, y a la ausencia de líderes internacionales que permitan su persecución, hacen que cada país intente defenderse de una manera determinada. Bajo este contexto, es fundamental una colaboración público-privada que permita perseguir el delito que se da en forma *on line* y global. Además, es necesario actuar en tiempo real, porque los incidentes cibernéticos ocurren en un país, independientemente del origen del ataque. De ahí que la búsqueda de acuerdos internacionales para perseguir al cibercrimen sea fundamental para mitigar su impacto.

En el ámbito corporativo los retos consisten en afrontar los desafíos ante la violación de la privacidad, las amenazas a la seguridad de la información y la pérdida de la salvaguarda de algunos activos físicos, aspectos atractivos para la ciberdelincuencia organizada a la cual nos enfrentamos hoy, y cada vez con un mayor número de ataques y mayor sofisticación. Esta vulnerabilidad de los sistemas informáticos obliga a implementar procesos cada vez más resilientes que anticipen los ataques cibernéticos y aumenten la

capacidad de respuesta ante la materialización de incidentes informáticos a través de estrategias de inteligencia de amenazas, resiliencia tecnológica, recuperación ante desastres y coberturas de ciberriesgo. En particular, existe la necesidad de abordar los riesgos de seguridad cibernética desde una perspectiva de sistemas de múltiples escalas, reconociendo las diversas interacciones entre los sistemas cibernéticos, físicos y humanos (Lambert et al. 2013 ). En este sentido, la Ciberseguridad protege los datos e información de individuos, la propiedad intelectual de las corporaciones y las administraciones públicas de diferentes ataques intencionados como: ransomware, ingeniería social, phishing, denegación del servicio e inteligencia artificial, entre otros.

Bajo este panorama, la justificación sobre revelaciones de información relacionadas con Ciberseguridad está dada por la presencia latente de estos riesgos en el mundo corporativo y las connotaciones económicas que representan. La Ciberseguridad se encuentra en la intersección de las preocupaciones de seguridad pública sobre la protección de la infraestructura crítica y la seguridad privada en torno a la protección de los derechos de propiedad y las libertades civiles (McCarthy, 2018). Estos son motivos suficientes para considerar que la seguridad cibernética es un tema candente para los *stakeholders,* especialmente actores del Gobierno Corporativo, reguladores financieros y emisores de estándares contables profesionales, en general.

Desde una perspectiva corporativa, esta investigación busca evaluar el alcance de las divulgaciones relacionadas con la Ciberseguridad en América Latina, para lo cual en el presente capítulo centraremos la atención en mostrar la evolución del concepto desde diferentes ópticas, a partir del cual podemos concluir que una definición de Ciberseguridad requiere contemplar aspectos mínimos, como la protección de las cualidades de la seguridad de la información, la protección de las personas y los activos físicos e infraestructuras que se encuentran en el ciberespacio. Este capítulo también presenta el origen y la evolución de los diferentes tipos de ciberataques, así como su marco normativo y regulatorio en el ámbito internacional. Por último, en este aparte, se hace referencia a la Ciberseguridad en las organizaciones.

## 1.1. La Ciberseguridad

En la actualidad no existe un concepto único de aceptación mundial del término "Ciberseguridad"; sin embargo, desde diferentes miradas se pretende observar la multidimensionalidad e interdisciplinariedad de su significado, el cual, en tan solo tres décadas, ha obtenido una cobertura global sin precedentes. Como muestra de ello, la iniciativa inglesa Cuerpo de Conocimiento de Ciberseguridad CyBOK (2021), a partir de una investigación mundial, vinculó veintiuna áreas del conocimiento al término "Ciberseguridad". Hoy en día, y acorde con la literatura previa, la evolución del significado del término abarca la seguridad de la información, la protección de las personas y los activos físicos dentro del denominado "ciberespacio".

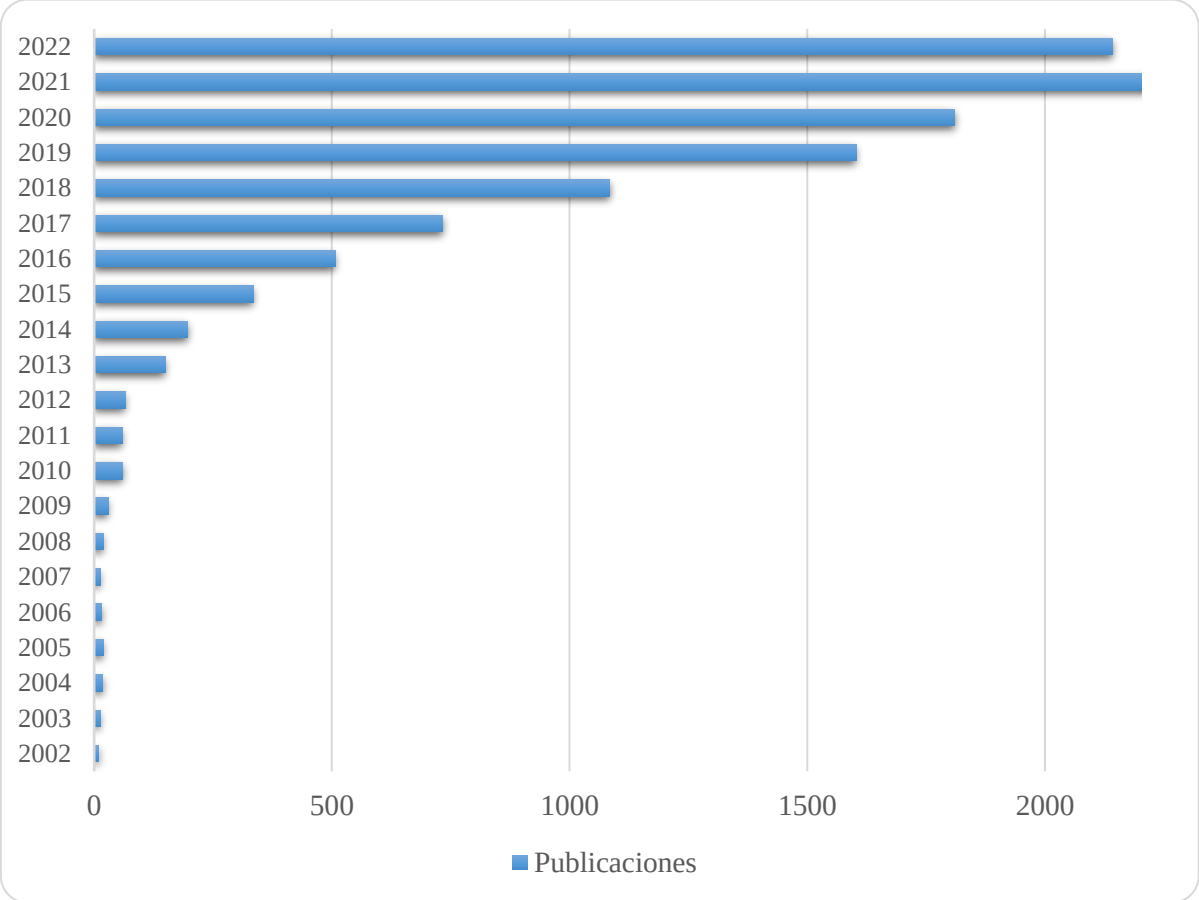
### 1.1.1. Concepto de Ciberseguridad

Se puede afirmar que la Ciberseguridad es una palabra relativamente nueva para un conjunto de prácticas antiguas en torno a la protección de las redes informáticas (Von Solms y Van Niekerk, 2013). El término ´Ciberseguridad´ probablemente se utilizó por primera vez en 1989 (Williams, 2020). Esta es la fecha dada por el diccionario (Merriam -Webster, 2021). No obstante, este concepto surge a partir del término ´cibernética´, utilizado originalmente por el matemático Norbert Wiener en 1941, en el libro *Cybernetics.* Según el diccionario de la lengua española, la palabra cibernética viene del griego *κυβερνητική kybernētikḗ,* ´arte de gobernar una nave´, y su definición hace referencia a una ciencia que estudia las analogías entre los sistemas de control y comunicaciones de los seres vivos y los de las máquinas (RAE; ASALE, 2020). Es a partir de estas bases que la actual definición de Ciberseguridad obtiene algunos de sus principales matices.

La revisión de la literatura previa a través de la búsqueda de la palabra clave *´cybersecurity´* en la colección principal de la base de datos *Web of Science,* reporta 11.173 resultados en el período 2002 – 2022, y confirma cómo su presente uso es relativamente reciente (Stevens, 2018). En esta búsqueda se identifican 6.473 artículos,

de los cuales el 27% tienen su origen en Estados Unidos, seguido de un 8% en la República Popular de China, 7% en Inglaterra, 6% Australia y 5% Arabia Saudita . Por América Latina, Brasil tiene una participación del 1%, con 71 artículos sobre el tema durante este período. La participación, liderada por Estados Unidos y China en el número de publicaciones, confirma la pugna histórica por el liderazgo mundial en transformación tecnológica de estas dos naciones.

**Figura 1. Artículos de investigación período 2002-2022**

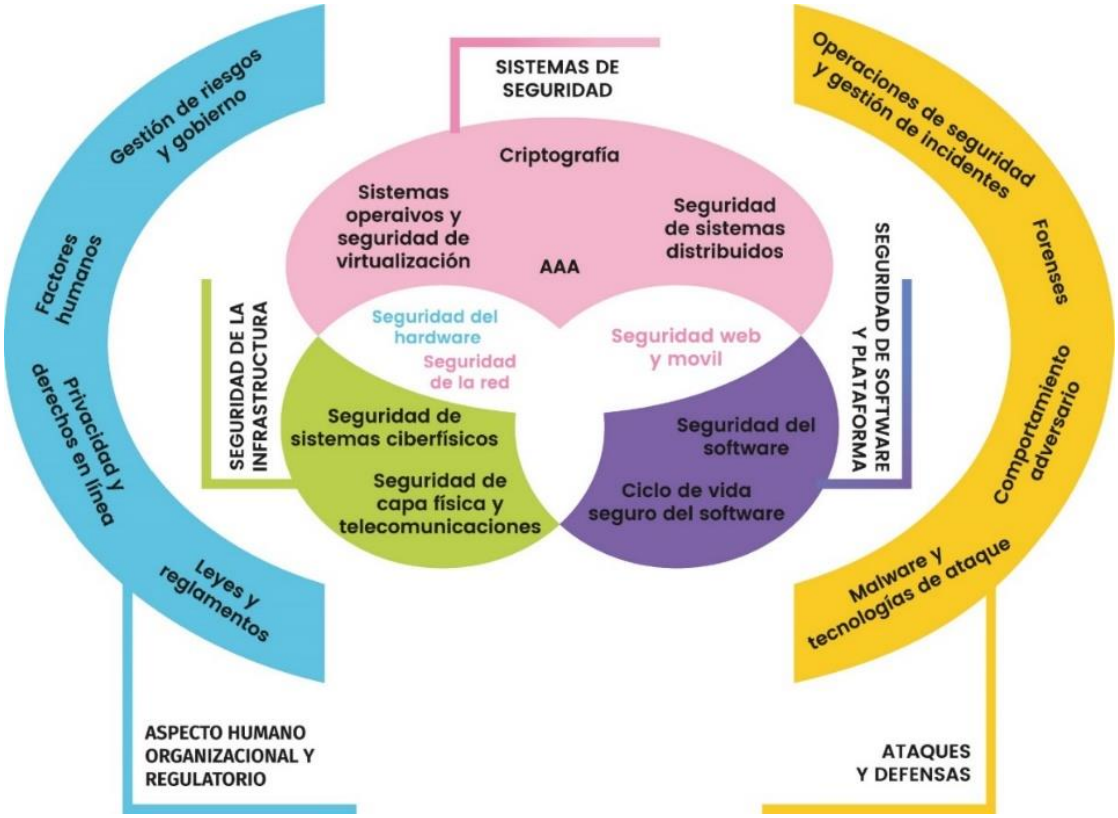



Nota. Elaborado con base en *Web of Science*, diciembre de 2022

Como se observa en la Figura 1, los artículos de investigación en temas de Ciberseguridad muestran un aumento exponencial en la última década. Es probable que el incremento de

publicaciones entre 2018 y 2019 se relacione con los ciberataques de *Wannacry* y *NotPetya* en junio de 2017, los cuales dominaron las noticias mundiales con un impacto colosal (Eijkelenboom & Nieuwesteeg, 2021). Por su parte, el aumento de la producción en los años 2020 - 2021 seguramente esté conexo con la aparición de COVID – 19 como agente catalizador de la transformación digital y el aumento de forma exponencial de los ataques cibernéticos(Fidler, 2020).

**Figura 2. Áreas de conocimiento de Ciberseguridad en el alcance CyBOK**



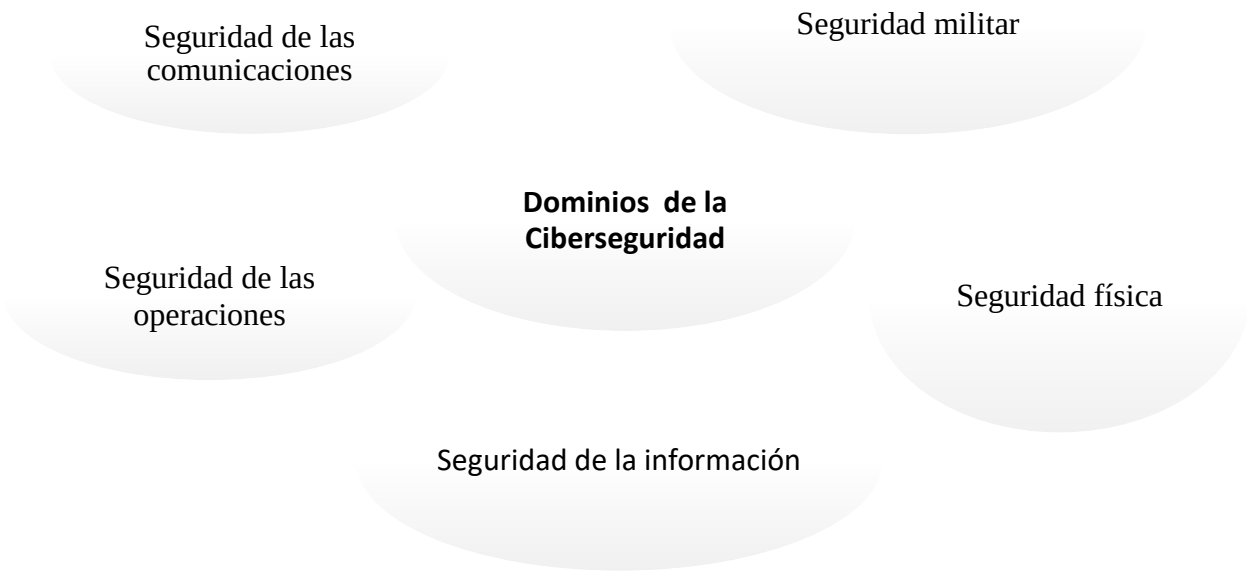

Nota. Elaborado con base en Martin et al. (2021)

Cabe señalar que en la actualidad existe una iniciativa conocida como CyBOK cuyo objetivo es codificar el conocimiento fundamental y generalmente reconocido sobre Ciberseguridad (CyBOK, 2021). El equipo del proyecto CyBOK llevó a cabo un extenso ejercicio que involucró un mapeo y análisis de textos relevantes, así como una variedad de consultas comunitarias tanto en el Reino Unido como a nivel internacional, a través de talleres, una encuesta en línea y entrevistas. Como resultado, los temas sobre

Ciberseguridad se agruparon en veintiuna áreas de conocimiento asociadas en cinco dimensiones: (1) aspectos humano, organizacional y regulatorio; (2) ataques y defensas; (3) sistemas de seguridad; (4) seguridad de la infraestructura, y (5) seguridad de software y plataforma. Así, la cobertura del concepto de Ciberseguridad corrobora su naturaleza multidisciplinaria y la omnipresencia de las preocupaciones de seguridad cibernética en toda la sociedad (Cains et al., 2021). Ver Figura 2.

En la misma línea, la Agencia Europea de Seguridad de las Redes y de la Información ENISA (2015), resume en cinco los aspectos que abarca la Ciberseguridad en cuanto a la seguridad de las naciones se refiere: seguridad de las comunicaciones, seguridad de las operaciones, seguridad de la información, seguridad militar y seguridad física. Estos dominios igualmente representan la amplitud del alcance global del término. Ver Figura 3.

**Figura 3. Dominios del término Ciberseguridad**




Nota. Elaborado con base en ENISA (2015)

Desde estas dos iniciativas CyBOK - Martin et al. (2021) y ENISA (2015), podemos ratificar la importancia de la Ciberseguridad en la esfera global como un renglón con repercusiones sociales, políticas y económicas, tanto en el ámbito nacional como internacional.

Una vez visto el alcance del tema de la Ciberseguridad, nos concentraremos en revisar su concepto desde el punto de vista de la literatura previa, resultado de investigaciones. Respecto al avance conceptual de la Ciberseguridad, según CyBOK - Rashid et al. (2019) no existe un consenso sobre lo que la diversa comunidad de investigadores, educadores y profesionales ve como conocimiento fundamental en Ciberseguridad. De acuerdo con Stevens (2018), hasta la fecha, la lucha por regular y gobernar este complejo paisaje se refleja en la falta de multiplicidad en la teoría y los métodos utilizados para comprender este entorno novedoso y para interpretar las respuestas políticas a sus problemas, esta temática espera una oferta de ideas para revestir este desequilibrio.

La Ciberseguridad en el ámbito mundial ha evolucionado y atravesado varias fases a lo largo de los años, resultando en un legado teórico granular que actualmente necesita unificarse para fomentar más teorías beneficiosas y aplicabilidad (Althonayan & Andronache, 2018). La ausencia de una definición concisa y universalmente aceptable que capture la multidimensionalidad de la Ciberseguridad impide los avances tecnológicos y científicos al reforzar la visión predominantemente técnica de la misma, al tiempo que separa las disciplinas que deberían actuar en conjunto para resolver sus complejos desafíos (Craigen et al., 2014).

En esta línea, Henshel et al. (2015) afirman que la Ciberseguridad trasciende los niveles de análisis, requiere un conocimiento interdisciplinario considerable y será moldeada por la disponibilidad de nuevos datos y métodos. La Ciberseguridad ha construido progresivamente su posición actual sobre sus raíces tempranas en los principios de la informática, la seguridad de la información, la garantía de la información y la gestión de riesgos. Fruto de algunos estudios (Alshaikh et al., 2014; Althonayan & Andronache, 2018; Chang, 2016; Craigen et al., 2014; Da Veiga & Eloff, 2007; Kotulic & Clark, 2004;

Ramirez & Choucri, 2016; Schatz et al., 2017; Von Solms & Van Niekerk, 2013; Von Solms & Von Solms, 2018) se ha enriquecido la semántica y la etimología entorno a la palabra Ciberseguridad.

Según nuestra búsqueda, en los estudios relacionados con Ciberseguridad es común encontrar que las investigaciones no plantean una definición del término; en la mayoría de los casos se omite y en otros se toman definiciones ya existentes emanadas desde diferentes organismos nacionales o internacionales. Según nuestra búsqueda, tan solo un número reducido de autores se dan a la tarea de proponer una definición de Ciberseguridad: Craigen et al. (2014); Gordon et al. (2006); Haapamäki & Sihvonen (2019); Le & Hoang, (2017); Reid & Van Niekerk, 2014; Schatz et al. (2017); Tissir et al. (2020); Von Solms & Von Solms (2018). Ver Tabla 1.

**Tabla 1. Definiciones de Ciberseguridad en la literatura previa**

| Autor | Definición |
|---|---|
| Gordon et al. (2006) | Los objetivos de la Ciberseguridad se pueden dividir en tres grandes categorías. Primero, la Ciberseguridad protege la confidencialidad de la información privada; segundo, asegura que los usuarios autorizados puedan acceder a la información de manera oportuna; y tercero, la Ciberseguridad protege la precisión, confiabilidad y validez de la información. |
| Craigen et al. (2014) | La Ciberseguridad es la organización y el conjunto de recursos, procesos y estructuras que se utilizan para proteger el ciberespacio y los sistemas habilitados para éste, de sucesos que desalinean de jure los derechos de propiedad de facto. |
| Reid & Van Niekerk (2014) | La seguridad cibernética es la protección de los intereses de una persona, sociedad o nación, incluidos sus activos de información y no información que necesitan protección contra los riesgos relativos a su interacción con el ciberespacio. |
| Schatz et al. (2017) | El enfoque y las acciones asociadas con procesos de gestión de seguridad seguido por organizaciones y estados para proteger la confidencialidad, integridad y disponibilidad de datos y activos utilizados en el espacio cibernético. El concepto incluye lineamientos, políticas y colecciones de salvaguardas, tecnologías, herramientas y capacitación para brindar la protección para el estado del entorno cibernético y sus usuarios. |
| Le & Hoang (2017) | La Ciberseguridad puede considerarse sistemas, herramientas, procesos, prácticas, conceptos y estrategias para prevenir y |

| | |
|---|---|
| | proteger el espacio cibernético de la interacción no autorizada por parte de agentes con elementos del espacio para mantener y preservar la confidencialidad, integridad, disponibilidad y otras propiedades del espacio y sus recursos protegidos. |
| Von Solms & Von Solms (2018) | La Ciberseguridad es esa parte de la seguridad de la información que se enfoca específicamente en proteger la confidencialidad, integridad y disponibilidad (CIA) de los activos de información digital contra cualquier amenaza que pueda surgir de dichos activos que se ven comprometidos. a través de (usando) Internet. |
| | |
| Haapamäki & Sihvonen, (2019) | La Ciberseguridad comprende tecnologías, procesos y controles que están diseñados para proteger sistemas, redes y datos de ataques cibernéticos. La Ciberseguridad eficaz reduce el riesgo de ciberataques y protege a las sociedades, organizaciones e individuos de la explotación no autorizada de sistemas, redes y tecnologías. |
| | |
| Tissir et al. (2020) | El término "Ciberseguridad" puede describirse como un término que refleja las relaciones e interconexiones entre el ciberespacio y el mundo físico; y la información es el elemento clave en esta relación. |
| | |

Los antecedentes relacionan términos como: seguridad informática (Madnick, 1978); seguridad de la información (Blakley et al., 2002; Von Solms & Von Solms, 2018); riesgo cibernético (Cebula & Young, 2010; McShane et al., 2021; Strupczewski, 2021) y Ciberseguridad (Althonayan & Andronache, 2018; Chang, 2016; Von Solms & Van Niekerk, 2013). Estos términos están relacionados con la definición de Ciberseguridad, más no son necesariamente sinónimos (Sattarova Feruza & Kim, 2007).

Respecto a la seguridad informática, ésta se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, y cuyos efectos puedan conllevar daños sobre la información, equipo o software (Gómez, 2006). Por su parte, autores como CyBOK - Rashid et al. (2019) refieren la seguridad de la información como una gran contribución a la noción de Ciberseguridad, a partir de los tres elementos principales que la componen: preservación de la confidencialidad, integridad y disponibilidad de la información. Frente al riesgo cibernético, según Cebula & Young (2010), éste se define como el riesgo operativo a los activos de información y tecnología que tienen consecuencias que afectan los sistemas de información.

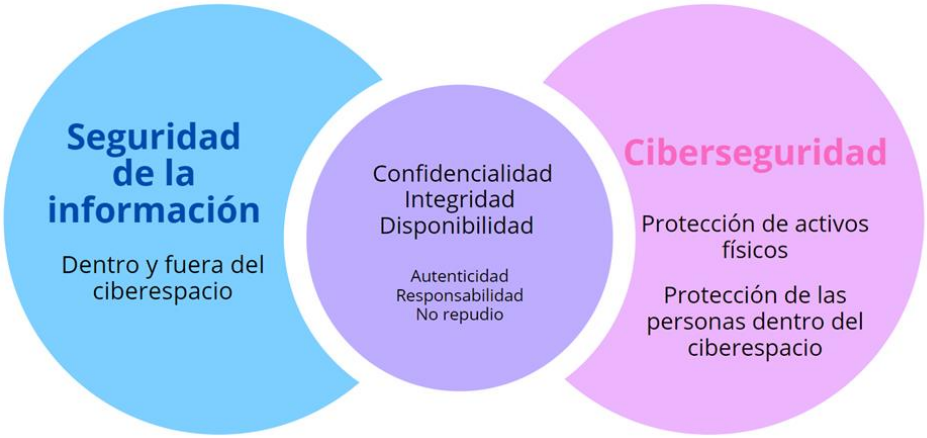
Bajo este panorama sobre la complejidad del significado de Ciberseguridad, es importante distinguir muy bien este concepto del de "seguridad de la información". En este sentido, Rowe et al. (2012), expresan que la seguridad de la información ha sido diseñada para proteger la información y lo hace muy bien, pero sus limitaciones no le permiten hacer frente a la protección de los activos, recursos claves, entrelazados con la vida cotidiana, la infraestructura crítica y los sistemas globales; esta distinción es lo que separa la seguridad de la información de la Ciberseguridad.

Por su parte, según Von & Van Niekerk (2013), la Ciberseguridad debe consistir en proteger algo más que la información o los recursos de los sistemas de información de una persona u organización; ésta también se refiere a la protección de la(s) persona(s) que utilizan los recursos en un ciberentorno y a la salvaguarda de cualquier otro activo, incluidos los pertenecientes a la sociedad en general, que hayan estado expuestos a riesgos como resultado de vulnerabilidades derivadas del uso de las TIC. Según Le & Hoang (2017), actualmente una parte integral de la definición de Ciberseguridad la constituye su función de prevención, no solo la protección. Tiene sentido mirar la seguridad en un contexto más amplio donde la prevención y la protección van de la mano. Prevenir que alguna vulnerabilidad sea explotada y dañe un ciberespacio puede considerarse proteger el espacio y, por otro lado, saber cómo proteger el ciberespacio implica en cierta medida el conocimiento de las brechas de seguridad que ocurren y cómo se pueden prevenir.

Como ilustra la Figura 4, la seguridad de la información aporta a la Ciberseguridad los elementos que componen los activos conexos con la información: confidencialidad, integridad y disponibilidad. No obstante, la seguridad de la información tiene un campo de aplicación que no se limita al ciberespacio. También se ocupa de la información, independientemente de su formato: abarca documentos en papel, propiedad digital e intelectual en la mente de las personas y comunicaciones verbales o visuales (Von Solms & Von Solms, 2018). La Ciberseguridad protege los activos digitales, desde las redes hasta el hardware y la información que se procesa, almacena o transporta mediante sistemas de información interconectados. Además, conceptos como los ataques patrocinados por el estado-nación y las amenazas persistentes avanzadas (APT)

pertenecen casi exclusivamente a la Ciberseguridad (Von Solms & Von Solms, 2018). En general, todos los activos relacionados con la información, todos los que se encuentren en el ciberespacio, como son los activos físicos, infraestructuras y las personas que actúan en él.

**Figura 4. Seguridad de la información y Ciberseguridad**




Nota. Elaboración propia

Como también ilustra la Figura 4, de la relación entre el concepto de seguridad de la información y Ciberseguridad podemos colegir que se tratan de términos con significados diferentes cuyo tema común lo constituye la defensa y la protección de las cualidades de la información en el ámbito organizacional contempladas en ISO 27002 (2013): preservación de la confidencialidad, integridad y disponibilidad de la información. Pueden estar involucradas otras propiedades, como la autenticidad, la responsabilidad y el no repudio. Whitman & Mattord (2011) agregan: precisión, autenticidad, utilidad y posesión a la lista de características de la información que deben protegerse.

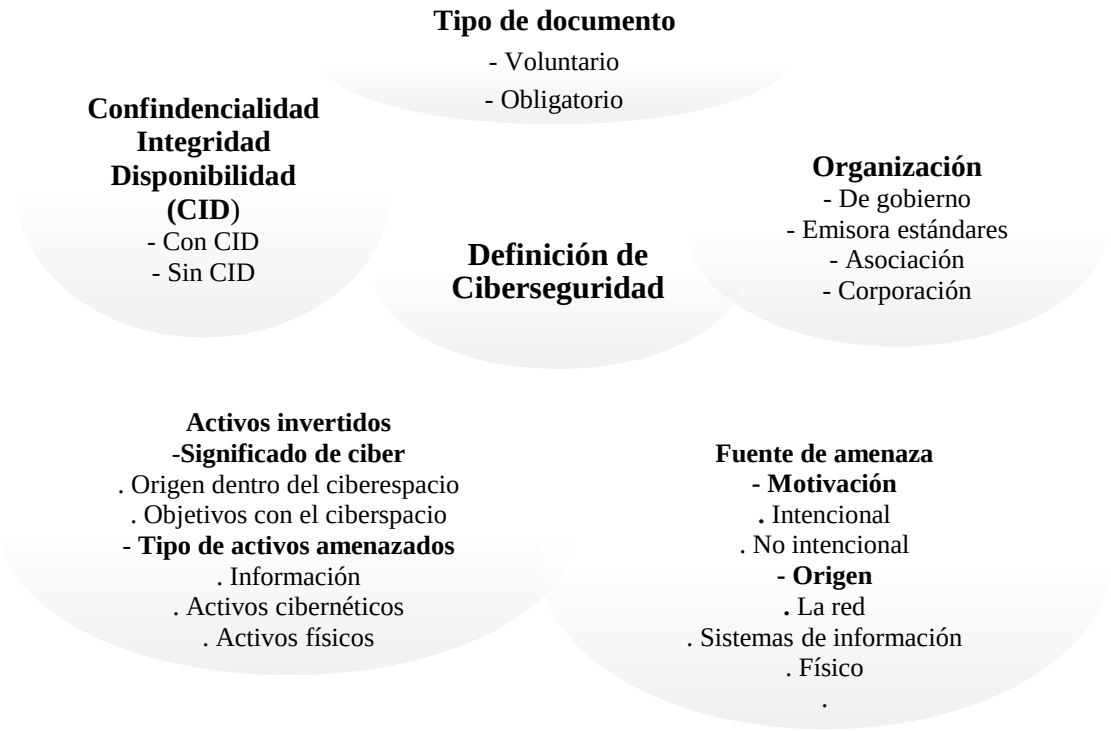
Respecto a la digitalización aplicada a la Ciberseguridad, si bien se aplica en una organización, al final lo que hay son personas, el *core* son las personas. Así, el componente "factor humano" es un elemento decisivo de tal definición (Adams & Sasse, 1999; Cains et al., 2021; Henshel et al., 2015; Rashid et al., 2019; Von Solms & Van Niekerk, 2013 y Whitten & Tygar, 1999). Henshel et al. (2015) aseveran cómo el ser humano juega un papel en la creación, propagación y mitigación del riesgo de

Ciberseguridad como usuario, defensor y atacante. Esta dimensión adicional tiene implicaciones éticas para la sociedad en su conjunto, ya que significa la protección de ciertos grupos vulnerables, por ejemplo, los niños (Von Solms & Van Niekerk, 2013).
Otro componente conceptual importante lo constituye la diferenciación de los activos específicos del ciberespacio. Los activos que la Ciberseguridad pretende proteger incluyen una dimensión adicional que se extiende más allá de los límites formales de la seguridad de la información (Von Solms & Van Niekerk, 2013). En este marco, Collier et al. (2013) argumentan que la Ciberseguridad debe pasar de un enfoque en ´problemas técnicos a nivel de componentes´ hacia un análisis de sistemas que integre los dominios físicos, de información, cognitivo y social, a partir de estas visiones y de la definición de ciberespacio entendido como el "ambiente en donde interactúan los seres humanos, el software y los servicios que en Internet se ofrecen" (ISO 27032, 2012). El ciberespacio no es estático; es un ecosistema dinámico, en evolución y de múltiples niveles de infraestructura física, software, regulaciones, ideas e innovaciones (Craigen et al., 2014). Así recientemente, el ciberespacio ha crecido para incluir redes sociales, nubes, ciudades inteligentes de Internet de las cosas (IOT), redes inteligentes y otros sistemas definidos por software (Le & Hoang, 2017).

La Figura 5 presenta los diversos componentes que pueden hacer parte de la definición de Ciberseguridad, tomando como referencia a ENISA (2015). Ésta asegura que para analizar las definiciones existentes sobre Ciberseguridad es importante evaluar como primer componente el tipo de documento, considerando lo vinculante o no de su aplicación, por lo que puede ser voluntario u obligatorio, dependiendo del contexto y del ente emisor. Como segundo componente se estudia el tipo de organización emisora, que puede ser de gobierno, emisora de estándares, una asociación o una corporación. El tercer componente hace referencia a la fuente de la amenaza cibernética; se analiza si el concepto contempla si la amenaza surge de forma intencional o no intencional; y, además, se tiene en cuenta si se expresa el origen de la fuente de amenaza, si ha sido la red, los sistemas de información o un activo físico. El cuarto componente, denominado activos invertidos, evalúa si el significado de Ciberseguridad tiene su origen dentro del ciberespacio o se relaciona como objetivos con el ciberespacio; también en este

componente se revisan los activos amenazados, a los cuáles hace referencia el concepto, ya sea la información, los activos cibernéticos o los activos físicos. El quinto componente coincide con Rashid et al. (2019), al referirse a los tres elementos que componen la seguridad de la información: confidencialidad, integridad y disponibilidad (CID); en este aparte se evalúa si la definición analizada, los contempla o no.

**Figura 5. Componentes en la definición de Ciberseguridad**




Nota. Elaborado con base en (ENISA, 2015)

A continuación, en la Tabla 2 se analizan algunas definiciones de Ciberseguridad planteadas por organismos internacionales, tomando como referencia los componentes que pueden constituir la definición de Ciberseguridad con base en ENISA (2015).

## Tabla 2. Definiciones de Ciberseguridad planteadas por organismos internacionales

| Definición del término Ciberseguridad ITU, (2008) | Detalles |
|---|---|
| El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicación, las comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La Ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad.<br><br>ITU, (2008) Unión Internacional de Telecomunicaciones. Organización internacional. Documento UIT-T X.1205- (04/2008)<br>https://www.itu.int/rec/T-REC-X.1205-200804-I | **Tipo de documento:** de aplicación voluntaria.<br>**Organización:** emisora de estándares internacionales de telecomunicaciones<br>**Motivación fuente de amenaza**: no se menciona.<br>**Origen de amenazas**: los sistemas de información, la red.<br>**El significado de ciber:** contempla su origen en el ciberespacio<br>**Tipo de activos amenazados:** información<br>**CID:** si refiere. La definición describe la seguridad de la información como una gran contribución a la noción de Ciberseguridad, a partir de los tres elementos principales que la componen: preservación de la confidencialidad, integridad y disponibilidad de la información.<br><br>La Recomendación UIT-T X.1205 proporciona una taxonomía de las amenazas a la seguridad desde el punto de vista de la organización. Es un documento de cobertura internacional. Contempla la protección de las personas y la protección de los activos dentro del ciberespacio. Esta definición describe de forma amplia las actividades que involucra la Ciberseguridad desde las organizaciones. |

| Definición del término Ciberseguridad (ISO 27032, 2012) | Detalles |
|---|---|
| Condición de estar protegido contra las consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, ocupacionales, psicológicas, educativas o de otro tipo de fallas, daños, errores, accidentes, daños o cualquier otro evento en el Ciberespacio que pueda ser considerado no deseable. Nota 1: Esto puede tomar la forma de estar protegido del evento o de la exposición a algo que cause pérdidas económicas o de salud. Puede incluir la protección de las personas o de los bienes. Nota 2: La seguridad en general también se define como el estado de certeza de que algún agente no causará efectos adversos en condiciones definidas.<br>La Ciberseguridad seguridad del ciberespacio: preservación de la confidencialidad, integridad y disponibilidad de la información en el Ciberespacio. Nota 1: Además, también pueden estar involucradas otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad. | **Tipo de documento:** de aplicación voluntaria.<br>**Organización:** emisora de estándares internacionales de Seguridad de la Información<br>**Motivación fuente de amenaza:** no se menciona.<br>**Origen de amenazas:** los sistemas de información<br>**El significado de ciber:** contempla su origen en el ciberespacio<br>**Tipo de activos amenazados**: información<br>**CID:** si refiere. La definición describe la seguridad de la información como una contribución a la noción de Ciberseguridad, a partir de los tres elementos principales que la componen: preservación de la confidencialidad, integridad y disponibilidad de la información.<br><br>Este estándar propone directrices para la Ciberseguridad. En definición contempla la protección de las personas y la protección de los activos dentro del ciberespacio. Esta definición describe de forma amplia las actividades que involucra la Ciberseguridad |

Nota 2: Adaptado de la definición de seguridad de la información en ISO/IEC 27000:2009.

**(ISO 27032, 2012) Organización internacional de Normalización. Documento ISO/IEC 27032:2012**
https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27032:ed-1:v1:en

desde las organizaciones. Es un documento de cobertura internacional. Incluye la protección de las personas o de los bienes. Inicia expresando las consecuencias de los eventos no deseables en el ciberespacio.

| Definición del término Ciberseguridad (NIST, 2015) | Detalles |
|---|---|
| Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas comunicaciones por cable y comunicaciones y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. https://csrc.nist.gov/glossary/term/cybersecurity | **Tipo de documento:** de aplicación voluntaria.<br>**Organización:** de gobierno.<br>**Motivación fuente de amenaza**: no se menciona.<br>**Origen de amenazas**: los sistemas de información y la red.<br>**El significado de ciber:** contempla su origen en el ciberespacio<br>**Tipo de activos amenazados:** información<br>**CID:** Si refiere.<br><br>Este documento hace referencia al glosario del Instituto Nacional de Estándares y Tecnología de Estados Unidos NIST es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos |

| Definición del término Ciberseguridad (NICCS, 2017) | Detalles |
|---|---|
| La actividad o proceso, habilidad o capacidad, o estado mediante el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación o explotación, no autorizados.<br><br>Definición ampliada: estrategia, política y estándares relacionados con la seguridad y las operaciones en el ciberespacio, y que abarcan toda la gama de políticas y actividades de reducción de amenazas, reducción de vulnerabilidades, disuasión, compromiso internacional, respuesta a incidentes, resiliencia y recuperación, incluidas operaciones de redes informáticas, seguridad de la información, aplicación de la ley, diplomacia, misiones militares y de inteligencia en lo que respecta a la seguridad y estabilidad de la infraestructura mundial de información y comunicaciones.<br>Adaptado de: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, Meta Nacional de Preparación del DHS; Revisión de la política del ciberespacio de la Casa Blanca, mayo de 2009. | **Tipo de documento:** de aplicación voluntaria.<br>**Organización:** de gobierno.<br>**Motivación fuente de amenaza**: no se menciona.<br>**Origen de amenazas**: los sistemas de información y la red.<br>**El significado de ciber:** contempla su origen en el ciberespacio<br>**Tipo de activos amenazados:** información<br>**CID:** no refiere.<br>NICCS como Iniciativa Nacional de Carreras y Estudios de Ciberseguridad, propone una definición.<br>Este es un documento de cobertura nacional, de aplicación voluntaria. La definición incluye la protección de la información y las comunicaciones en el ámbito nacional. Abarca la protección de los activos dentro del ciberespacio. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad´. Describe el origen de algunas amenazas. Es una definición planteada desde el contexto país. |

(NICCS, 2017) Iniciativa nacional de carreras y estudi Ciberseguridad.
Definición adaptada de: CNSSI 4009, NIST SP 800-53 Rev 4, Meta
Nacional de Preparación del DHS; Revisión de la polític ciberespacio
de la Casa Blanca, Estados Unidos mayo de 2009.
https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C

| Definición del término Ciberseguridad | Detalles |
|---|---|
| **EU, (2019).**<br><br>Todas las actividades necesarias para la protección de las redes y sistemas de información de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas.<br>EU, (2019). Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la Ciberseguridad de las tecnologías de la información y la comunicación.<br>https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN | .<br>**Tipo de documento**: de aplicación obligatoria<br>**Organización:** de gobierno<br>**Motivación fuente de amenaza:** no se menciona.<br>**Origen de amenazas:** no menciona.<br>**El significado de ciber:** contempla su origen en el ciberespacio<br>**Tipo de activos amenazados**: información, redes.<br>**CID**: no refiere.<br>El documento constituye el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2009.<br>La definición de Ciberseguridad incluye la protección de las redes, sistemas de información y usuarios. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad. No señala la protección a determinados activos, ni contempla la frontera del ciberespacio. Describe el origen de algunas amenazas. |

| Definición del término Ciberseguridad | Detalles |
|---|---|
| **(IOSCO, 2016)**<br><br>La seguridad cibernética se refiere en términos generales a la capacidad de protegerse contra los ataques cibernéticos y recuperarse de ellos. A los efectos de este informe, la seguridad cibernética se entiende como un concepto muy amplio, que abarca todas las actividades importantes asociadas con la mitigación del riesgo cibernético, es decir, identificar, proteger, detectar, responder y recuperarse de los ataques cibernéticos.<br><br>**(IOSCO, 2016) Organización Internacional de Comisiones de Valores.**<br>https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf | **Tipo de documento:** de aplicación voluntaria para sector financiero.<br>**Organización:** organización internacional<br>**Motivación fuente de amenaza:** no se menciona.<br>**Origen de amenazas:** no refiere.<br>**El significado de ciber:** no menciona el ciberespacio<br>**Tipo de activos amenazados:** información<br>**CID**: no refiere.<br><br>Este marco denominado "Seguridad cibernética en los mercados de valores: una perspectiva internacional" es un informe sobre los esfuerzos de coordinación de riesgos cibernéticos de IOSCO. La definición relaciona la Ciberseguridad con el riesgo cibernético. No precisa los términos 'Confidencialidad', 'Integridad' y 'Disponibilidad. No especifica la protección de las personas, ni activos dentro del ciberespacio. No describe los activos, no especifica el origen de las amenazas. |

| Definición del término Ciberseguridad (IDB; OAS, 2020) | Detalles |
|---|---|
| Más allá de la protección operativa de los sistemas y redes, la Ciberseguridad es, y seguirá siendo, fundamental para garantizar la integridad y la capacidad de recuperación de los procesos socieconómicos interconectados, de gobierno y de negocios que operan en el marco del siempre complejo ecosistema tecnológico, por lo que aborda el riesgo cibernético en todos los ámbitos requiere continuos esfuerzos y adaptación.<br>**(IDB; OAS, 2020)**<br>https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf | **Tipo de documento:** de aplicación voluntaria.<br>**Organización:** organización internacional<br>**Motivación fuente de amenaza:** no se menciona.<br>**Origen de amenazas:** no refiere.<br>**El significado de ciber:** no menciona el ciberespacio<br>**Tipo de activos amenazados:** información<br>**CID:** no refiere.<br><br>Este informe "Riesgos, avances y el camino a seguir en América Latina y el Caribe 2020 expone la situación de esta región. La definición que presenta es de aplicación voluntaria y hace referencia al papel en aspectos sociales, económicos y de gobierno. No precisa los términos "Confidencialidad", "Integridad" y "Disponibilidad"No especifica la protección de las personas, ni la protección de los activos dentro del ciberespacio. No describe los activos, no especifica el origen de las amenazas. |

A partir de las definiciones analizadas en la Tabla 2, se puede observar la falta de uniformidad en torno al concepto de Ciberseguridad, y como dos de éstas, ITU (2008) e ISO (2012), relacionan el mayor número de componentes. Las demás presentan un alcance reducido, al no abordarlos en su mayoría y no incluir los elementos de la seguridad de la información, la protección de las personas y omitir la salvaguarda de los activos físicos.

En general, el número de opciones por cada componente y las diferencias marcadas en el concepto desde la mirada transnacional, dificultan su estudio y por ende su aplicación. De acuerdo con Martin et al. (2021), gran parte de estas definiciones depositan una confianza excesiva en los controles técnicos y se centran, casi exclusivamente, en la información; extenderlos para relacionarlos con los sistemas físicos cibernéticos conectados a la red es un desafío apremiante para evitar que los dispositivos físicos presenten comportamientos no deseados. Bajo este panorama, coincidimos con ENISA (2015) en que se debe considerar una definición contextual de Ciberseguridad, basada en una que sea relevante, se ajuste y se use por parte de una organización emisora de estándares internacionales o en una organización en particular. No es necesario que exista una definición de Ciberseguridad, en el sentido convencional que tendemos a aplicar

definiciones a las cosas simples. El problema es que ´la Ciberseguridad´ es un término envolvente, y no es posible hacer una definición para cubrir el alcance de las cosas que abarca.

En esta misma línea, según Cavelty (2010), el discurso y la investigación en Ciberseguridad necesariamente cambia a contextos y condiciones que determinan el proceso por el cual los actores clave llegan subjetivamente a una comprensión compartida de cómo conceptualizar y, en última instancia, responder a una amenaza a la seguridad.

Respecto a la afirmación de ENISA (2015), probablemente resume la incertidumbre entre los muchos actores en este campo sobre lo que implica exactamente la Ciberseguridad. Esta interpretación de la Ciberseguridad como un ´término envolvente´, junto con las muchas definiciones e interpretaciones diversas, hacen que no sea fácil explicar ya en el terreno de las organizaciones exactamente cuál es su responsabilidad y el alcance de la rendición de cuentas hacia la Ciberseguridad (Von Solms & Von Solms, 2018). En general, podemos concluir que una definición de Ciberseguridad requiere contemplar aspectos mínimos, como la protección de las cualidades de la seguridad de la información, la protección de las personas y los activos físicos e infraestructuras que se encuentran en el ciberespacio.

### 1.1.2. Origen y evolución de los tipos de ciberataques

Una de las formas de comprender mejor el concepto de Ciberseguridad y su campo de aplicación consiste en recrear el comienzo de las redes informáticas, las comunicaciones y los avances que dibujan el ciberespacio de hoy, con sus vulnerabilidades, amenazas y riesgos inherentes. La historia muestra cómo las técnicas de jaqueo se originan inicialmente en ataques entre los estados nación, enseguida los hackers atacan las empresas y, posteriormente, a los individuos. Los tipos de ciberataques que se exponen a continuación hacen referencia a los originados en el ámbito organizacional.

Se suele afirmar que la era cibernética comenzó a finales de la década de 1960 y principios de 1970, con el advenimiento de la Red de la Agencia de Proyectos de Investigación Avanzada, ARPANET (Hatfield, 2018). ARPANET fue un complejo de computadores interactivos construidos por ARPA durante la Guerra Fría en universidades estadounidenses específicas (Packard, 2020). Esta red predecesora de Internet, financiada en 1969 por el Departamento de Defensa de Estados Unidos (Roberts, 1988), mejoró la actividad de espionaje con su capacidad de transmisión de alta velocidad y procesamiento de datos de supercomputadora (Packard, 2020).

En 1975, el Pentágono relevó a ARPA de sus responsabilidades de administrar ARPANET y la entregó a la Agencia de Comunicaciones de Defensa (Abbate, 2011), iniciando un proceso de evolución que, en 1983, da lugar al Internet que usamos hoy (Packard, 2020). Sin embargo, ya desde 1982 la preocupación por la seguridad de la red llevó a la decisión de dividirla en dominios civiles y militares. El dominio ARPANET continuaría como empresa de investigación; y MILNET estaría de ahora en adelante enteramente dedicado a las comunicaciones militares. Durante las dos primeras décadas de su existencia, ARPANET fue exclusiva de una élite tecnológica, académica y de investigación.

Esta exclusividad explica la razón por la cual sólo hasta principios de la década de 1990 comienza a filtrarse al público el dominio de la red, convirtiéndose en una tecnología de propósito general sin la cual la sociedad moderna no podría funcionar (Naughton, 2016). Así surge la revolución de Internet, marcando un antes y un después en la historia de la humanidad. En el mundo corporativo, la conectividad a Internet y la seguridad en la www desde ese momento representan la amenaza más importante para muchas organizaciones (Arnum, 1995).

A la par con el desarrollo de las comunicaciones, también surgen interrupciones provocadas. La primera registrada se presenta a principios de la década de 1970, creada por Bob Thomas y conocida como *The creeper,* primer gusano informático en el mundo, que se auto replicaba en ARPANET y mostraba un mensaje en otras computadoras (Chen

& Robert, 2004). En respuesta a estas interrupciones, en 1972 aparece el primer antivirus, llamado *Reaper*, básicamente un virus que se propagaba a través de la red en busca de computadores infectados para eliminarlo (Sofistic, 2017).

Una labor principal en la seguridad informática temprana involucró esfuerzos técnicos en el desarrollo de tecnologías de encriptación para salvaguardar información importante (Shankar, 1977). Es así como la Ciberseguridad empieza a dar respuesta para controlar las amenazas que van surgiendo y, al considerarse un tema de interés, también surgen organizaciones que investigan los delitos informáticos en red como *Stanford Research Institute* (SRI), la cual elaboró el primer informe sobre el tema, publicado en 1973 (Parker, 2007).

Posteriormente, en 1988, el ´gusano Morris´ fue el primer incidente de seguridad en red que involucró la propagación automatizada de un gusano por la red que causó efectos secundarios no deseados (Orman, 2003). El gusano informático, técnicamente un troyano de malware, fue creado por un estudiante de la Universidad de Cornell, Robert Tappan Morris, y lanzado el 2 de noviembre de 1988 (Woollacott, 2007). Éste fue un momento de transición para Internet y, si bien el gusano podría no haber sido un evento decisivo, marcó un límite desigual entre la Internet en gran parte confiada de la época y la Internet mundial heterogénea y peligrosa de hoy (Orman, 2003). Éste es considerado por muchos como el primer malware de denegación del servicio (DoS) y, sin duda, el primero en ganar la atención de los medios de comunicación. En 1989, con la financiación inicial del gobierno de Estados Unidos, la comunidad de seguridad informática desarrolló productos llamados cortafuegos que ayudaban a proteger los sistemas de los usuarios de daños cuando se conectaban a Internet y otras redes fuera de su control (Anderson, Brand, Gong, 2004).

Históricamente se han identificado muchos tipos de amenazas a la seguridad cibernética (Dobran, 2021). Los ciberataques son las amenazas de más rápido crecimiento, y quizás los más peligrosos, que enfrentan las organizaciones actuales (OAS; ISA, 2020). Según Nwosu et al. (2020), los ciberataques hacen uso de un código malicioso para cambiar la

lógica o los datos de la computadora, lo que genera consecuencias disruptivas que pueden exponer los datos y dar lugar a delitos cibernéticos, como el robo de información y de identidad. Se puede afirmar que gran parte del quehacer de la Ciberseguridad ha estado dedicado a la prevención y manejo de los incidentes o ataques cibernéticos. En este sentido, a continuación se presentan algunos de los principales tipos de ciberataques.

**Malware**, también conocido como código malicioso. Se refiere a un programa que se inserta de manera encubierta en otro con la intención de destruir datos, ejecutar programas destructivos o intrusivos o comprometer la confidencialidad, integridad o disponibilidad de los datos y aplicaciones del sistema operativo de la víctima (Souppaya & Scarfone, 2013). Como firman Ngo et al. (2020) y WEF (2017), existen muchos tipos de malware, según cómo se propaguen y la naturaleza del daño que pretenden; algunos ejemplos incluyen virus, gusanos, troyanos, spyware, keyloggers, botnets, rootkits, ransomware, scareware y descargas no autorizadas. Las amenazas de malware autónomo auto replicable presentan diversas características de ofuscación, que no solo se limitan a afectar el software, sino que también infectan componentes de hardware con ataques dirigidos altamente sofisticados (Menges & Pernul, 2018). Algunos virus de malware notables en la historia de los ciberataques incluyen el gusano Morris en 1988, el virus Melissa en 1999, el virus *ILOVEYOU* en 2000, el virus Anna Kournikova en 2001, el gusano Code Red en 2001, el virus Slammer en 2003, el gusano Mydoom en 2004, los gusanos Sasser y Netsky en 2004, el gusano Storm en 2007, el malware Mirai en 2016 y el ransomware WannaCry en 2017 (Ngo et al., 2020). Hasta la fecha, se han detectado más de un millón de virus diferentes y otros malware (Ngo et al., 2020).

**Ransomware** es otra forma muy conocida de malware, ampliamente utilizada. Consiste en tomar como rehenes los archivos o las computadoras de los usuarios mediante el cifrado de registros, dificultando el acceso al sistema u otros métodos, y luego exigir un rescate para devolverlos (Scaife et al., 2016). A finales de la década de 1980, los delincuentes ya tenían computadoras o archivos como rehenes a cambio de dinero en efectivo enviado a través del servicio postal. Uno de los primeros virus ransomware documentados fue el troyano AIDS (PC Cyborg Virus) que se lanzó a través de un

disquete en 1989; las víctimas necesitaban enviar $189 USD a un apartado de correos en Panamá para restaurar el acceso (Crowdstrike, 2021). Ransomware se diferencia de otros tipos de malware en que sus efectos son reversibles solo a través de las claves criptográficas que posee un adversario remoto (Scaife et al., 2016). De acuerdo con Crowdstrike (2021), las monedas virtuales crearon la oportunidad para que el ransomware se convirtiera en un negocio lucrativo con la aparición de las criptomonedas, como Bitcoin en 2010, operación difícil de rastrear cuando se trata de encontrar el destino del pago de las víctimas.

**Ingeniería social** es el arte de lograr que los usuarios comprometan los sistemas de información. En lugar de ataques técnicos a los sistemas, los ingenieros sociales se dirigen a los humanos con acceso a la información, manipulándolos para que divulguen información confidencial o incluso para que lleven a cabo sus ataques maliciosos a través de la influencia y la persuasión (Krombholz et al., 2015). La ingeniería social es una táctica que se desarrolla de manera diferente según la forma específica que adopte el ataque (Hatfield, 2018). Kevin Mitnick, desde 1976, usó la ingeniería social como técnica principal para obtener información, incluidos nombres de usuario, contraseñas y números de teléfono de módem (Middleton, 2017).

**Phishing** es un tipo de ataque informático que comunica mensajes de ingeniería social a humanos a través de canales de comunicación electrónicos para persuadirlos de realizar ciertas acciones en beneficio del atacante (Khonji et al., 2013). Utilizado por primera vez en Internet en 1996 por un grupo de piratas informáticos, que robaron cuentas de América Online (AOL), engañando a los usuarios para que revelaran sus contraseñas. Las estafas de phishing siguen siendo enormemente rentables para los profesionales que las ejecutan y las empresas continúan luchando por proteger los datos personales de sus clientes (Gunter, 2004).

**La denegación del servicio (**DDoS) se caracteriza por un ataque explícito e intento de impedir el uso legítimo de un servicio. Una forma frecuente de realizarlo es que el atacante envíe un flujo de paquetes a una víctima; este flujo consume algún recurso

clave, por lo que no está disponible para los clientes legítimos de la víctima. Otro enfoque común es que el atacante envíe unos paquetes con formato incorrecto que confunden una aplicación o un protocolo en la máquina víctima y la obligan a congelarse o reiniciarse (Mirkovic et al., 2004).

**La inteligencia artificial ofensiva** permitirá a los ciberdelincuentes efectuar ataques dirigidos a una velocidad y escala sin precedentes mientras vuelan bajo el radar de las herramientas de detección tradicionales basadas en reglas (Security Boulevard, 2021). La inteligencia artificial ofensiva tiene un gran número de aplicaciones que pueden actualizar y hacer más peligrosos los tipos de ciberataques que ha ido surgiendo hasta este momento, como malware inteligente o nuevas formas de ingeniería social capaces de suplantar perfectamente la voz de un empleado de alto rango en la empresa, o un *deepfake* en un vídeo capaz de copiar incluso las expresiones faciales de la persona suplantada (Sofistic, 2017).

Este panorama actual del riesgo de Ciberseguridad es descrito en el Foro Económico Mundial 2020: las tecnologías de la "Cuarta Revolución Industrial (4IR)", como la inteligencia artificial (IA), la computación cuántica, los dispositivos de Internet de las cosas (IoT), las redes 5G, las tecnologías en la nube y la cadena de bloques tienen el potencial de aumentar drásticamente la eficiencia e impulsar el crecimiento económico, pero también el potencial para aumentar el riesgo cibernético, resultando en pérdidas de hasta US$6 billones en 2021 (WEF, 2020). Así, es más que visible el aumento y la transformación de las diferentes formas de ataque a la seguridad cibernética, y la realidad es que hoy se manifiestan más amenazas de las que jamás se hayan visto (Ernst & Young, 2021).

En este sentido, según Deloitte (2019), el futuro es la salud digital, automatización industrial y robótica, e-commerce mejorado, chat bots de servicio al cliente, entretenimiento basado en realidad virtual, restaurantes virtuales, Fintech, entre otros, actividades que contribuyen a la expansión de la economía digital. ATOS (2020) señala que, para 2022, el escenario de la Ciberseguridad estará condicionado en gran medida por

el desafío de proteger eficientemente estos innumerables dispositivos con los que nos enfrentaremos en la vida diaria. Este ecosistema hiperconectado ofrecerá un blanco sumamente tentador para ciberdelincuentes buscando aprovecharse de superficies de ataque más extendidas y de vulnerabilidades con gran alcance y con impactos críticos.

En este recorrido de poco más de 50 años, vemos cómo ciertos hechos se han convertido en catalizadores de un panorama digital globalizado, sin fronteras e hiperconectado. Según Collier et al. (2013), si bien se han logrado avances significativos en el campo de la Ciberseguridad, las soluciones se han centrado más en los problemas técnicos a nivel de componentes, como la detección de amenazas, el cifrado y otros procedimientos y tecnologías de mitigación, y menos en cómo abordar el riesgo cibernético general y apoyar decisiones a nivel de sistemas a gran escala.

### 1.2. Marco normativo y regulatorio de Ciberseguridad en el ámbito internacional

El marco normativo internacional sobre Ciberseguridad es el resultado de las medidas tomadas desde la geopolítica y la cooperación internacional en torno a las amenazas y a la gestión del riesgo cibernético. Los lineamientos tomados desde el ámbito global direccionan la operatividad de la seguridad cibernética, tanto en el ámbito nacional como en el organizacional. Por esta razón, en este apartado se presentarán las principales iniciativas emanadas desde los organismos internacionales.

A medida que los avances tecnológicos y la interconectividad global se aceleran exponencialmente en la cuarta revolución industrial, los riesgos y amenazas de seguridad sistémica sin precedentes están socavando la confianza y el crecimiento (WEF, 2021a). Así, la Ciberseguridad está emergiendo como un enfoque de abajo hacia arriba, un hecho natural cuando existen disparidades entre estados nacionales, sectores público y privado e industrias. Sin embargo, una cultura global de Ciberseguridad puede tener más éxito de arriba hacia abajo (ITU, 2018). De esta forma, el marco normativo en materia de Ciberseguridad tiene como origen la respuesta a los acelerados y crecientes cambios

tecnológicos (Yang et al., 2020), y la preferencia por el cumplimiento de una normativa antes de invertir en mayores costos de seguridad informática (Berkman et al., 2018).

Se considera que el Convenio de Budapest, celebrado en el año 2001, marca el inicio de la legislación en materia de Ciberseguridad, al ser el primer tratado internacional sobre violaciones cometidas en el ciberespacio. En él se buscaba tipificar como delito actos que pusieran en peligro la confidencialidad, integridad y disponibilidad de sistemas de redes y datos informáticos (Convenio de Budapest, 2001). Inicia su redacción con la definición y clasificación de los delitos, disposiciones en materia de derecho procesal y finaliza con unas normas en cooperación internacional, en el caso que se presenten actos delictivos.
La cooperación internacional se materializa con la celebración de la primera Cumbre Mundial sobre Sociedad de la Información, aprobada por parte de la Organización Internacional de Comunicaciones, organismo especializado en TI y comunicación de la ONU, mediante Resolución 56/183 del 21 de diciembre de 2002 de la Asamblea General de las Naciones Unidas. Este evento reviste de gran importancia en la medida que plantea la elaboración de un documento guía, en el que radica el objetivo de redactar y propiciar una clara declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la sociedad de la información (Asamblea General de las Naciones Unidas, 2001).

La Cumbre se desarrolló en dos etapas. La primera de ellas, en Ginebra en diciembre de 2003, siendo su principal meta la reducción de las brechas digitales, un tema altamente diferencial y discriminatorio entre naciones, cuyo resultado final fue la declaración de principios y plan de acción para todo el marco del evento. La segunda etapa, desarrollada en Túnez en noviembre del 2005, tuvo un enfoque más inclusivo al involucrar entidades gubernamentales y organismos competentes del grupo de tareas sobre la tecnología de la información y las comunicaciones, organizaciones del sector privado, sociedad civil e instituciones regionales; su propósito, como evaluador de los avances logrados en la fase anterior, trajo como resultado final la expedición de la Resolución 1334 por parte del Consejo de la Unión Internacional de Telecomunicaciones (UIT), mediante la cual comienza una nueva gestión para el desarrollo de la Cumbre Mundial sobre sociedad de

la información, CMSI+10, con el objetivo de evaluar los logros de los últimos 10 años y plantear nuevas propuestas y objetivos para los años venideros.

Uno de los avances de la UIT fue la Agenda sobre Ciberseguridad Global, surgida en el año 2007 como un marco internacional que busca el mejoramiento de la confianza y seguridad en la sociedad de la información (Unión Internacional de Telecomunicaciones, 2007). De ella se desprenden algunos hechos de gran relevancia en la actualidad como: (i) el Índice Mundial de Ciberseguridad (IMC), entre cuyos fines está sensibilizar el papel que juegan los gobiernos en la promoción de la cultura de la Ciberseguridad; (ii) la recopilación de información relacionada con los reglamentos CERT (Equipo de Respuesta de Emergencias Informáticas) y CIRT (Equipos de respuesta a incidentes de seguridad) ; (iii) estrategias nacionales, políticas, de certificación y de sensibilización; y (iv) la alianza UIT-IMPACT que, en general, se enfoca en programar ciber simulacros en diferentes regiones del mundo para evaluar y mejorar la capacidad de respuesta en caso de eventos cibernéticos (UIT, 2012).

En el año 2008, la UIT emite la recomendación UIT-T X.1205 sobre aspectos generales de la Ciberseguridad: una clara definición de la Ciberseguridad, se revela la importancia de una gestión de riesgos, los requisitos de seguridad para las organizaciones en función de sus necesidades, una serie de posibles estrategias para la protección de la red (política de seguridad), la autenticación como punto clave para la gestión de red, técnicas para garantizar la fiabilidad ante posibles ataques, una descripción de tipos de ataque, tecnologías para luchar contra las amenazas, y ejemplos de seguridad de red (Unión Internacional de Telecomunicaciones, 2008).

Mediante la Resolución 64/25 del 02-12-2009, denominada ´Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional´, la ONU ratifica la invitación a sus estados miembros, por un lado al examen multilateral de las amenazas en seguridad de la información con nuevas estrategias de aplicación en el ámbito mundial, y a la evaluación de los inconvenientes en seguridad de la información;

y, por otro, a la mitigación y salvaguarda de la circulación de la información (United Nations General Assembly, 2009).

En el año 2015, la Organización para la Cooperación y el Desarrollo Económico (OCDE), como resultado de una creciente apertura digital, emite una recomendación enfocada en la gestión de riesgos de seguridad digital para la prosperidad económica y social. En ella se plantea algunos puntos como: la adopción de una estrategia nacional de seguridad digital para gestionar el riesgo, la adopción de medidas para gestión de riesgos en seguridad por parte de organizaciones públicas y privadas, y al mismo tiempo, la colaboración de éstas con el empoderamiento de los individuos y pequeñas unidades de negocios en materia de gestión de este riesgo, todo lo anterior enmarcado con el objetivo de la generación de confianza y seguridad en los entornos digitales (OCDE, 2015).

A nivel europeo, la UE emite la Directiva 2016/1148, más conocida como NIS, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información. Surge ante el incremento en número y gravedad de los incidentes en Ciberseguridad en la Unión Europea, con el objetivo de crear niveles apropiados de seguridad en las redes y sistemas de información. Entre las medidas tomadas se encuentran el deber de adoptar, entre los estados miembros, una estrategia nacional de Ciberseguridad; crear un Equipo de Respuesta ante Emergencias Informáticas o CSIRT; identificar autoridades nacionales competentes que se encarguen de la supervisión en la aplicación de esta directiva; y enfatizar la importancia de que los estados miembros velen porque las organizaciones, objeto de esta Directiva en caso de incidentes, notifiquen a las autoridades competentes e implanten medidas para su mitigación (Unión Europea, 2016).

Otra de las contribuciones normativas expedidas por la Unión Europea, en el año 2016, fue el Reglamento 679, por medio del cual se adopta el Reglamento General para la Protección de Datos. En él se establecen las normas relativas a la protección y circulación de los datos para personas físicas, organizaciones públicas y privadas sin distinción de su residencia, siempre que los datos personales tratados sean de personas residentes en la

Unión. También se legisló sobre aspectos como las condiciones que se deben cumplir para un tratamiento de datos lícitos, las obligaciones del encargado de tratar los datos, y algunas especificaciones para notificar violaciones de seguridad, tanto al interesado como a entes de control; en caso de incumplimiento, se reglamentaron las posibles sanciones y la necesidad de una unificación normativa en todos los países miembros de la UE (Unión Europea, 2016b).

Domenech (2017) afirma que las organizaciones ya no se encontrarán con veintiocho normativas distintas en la materia, sino con un único derecho o reglamento "paneuropeo". Por su parte, Mayor (2016) enuncia que entre los derechos rectores del reglamento se encuentran la transparencia, el acceso, la rectificación, la limitación del tratamiento, la oposición, la supresión o derecho al olvido, y la portabilidad de datos; estos dos últimos incorporados como nuevos derechos. Bajo el mismo Reglamento expedido por la Unión Europea, se plantea una estrategia de Ciberseguridad en la cual se establecen cinco prioridades, la más importante, resiliencia cibernética, es decir, aun cuando suceda un incidente cibernético la entidad debe contar con un plan estratégico que le genere capacidad para afrontar y responder rápidamente a fallos; las otras prioridades se enmarcan en la capacidad de reducir el ciberdelito acorde con la formulación de políticas a nivel institucional e internacional y la asignación de recursos en Ciberseguridad.

Continuando con la Unión Europea, en el año 2018 surgen otras iniciativas que incluyen lo que se pudiera llamar en el contexto actual como hacking ético. Una de éstas es el marco de pruebas de Ciberseguridad para el sector financiero TIBER-EU, el cual indica ciertas técnicas que se pueden utilizar para la detección de puntos quebrantables en una entidad o vulnerabilidades susceptibles de ataques como su tecnología, su capital humano o sus procesos. Autores como Berkman et al. (2018) señalan, como la primera normativa sobre Ciberseguridad a nivel empresarial, el Real Decreto-Ley 12/2018, especialmente por su obligatoriedad para brindar información bajo un informe anual sobre los incidentes que se perciban.

En el año 2019 entra en vigor el Reglamento Europeo 2019/881, conocido como Ley de Ciberseguridad para la UE. A través de esta legislación se establecen algunos objetivos y tareas orientadas a la Agencia de la Unión Europea para la Ciberseguridad (ENISA), reconociéndola como centro de conocimiento técnico en Ciberseguridad. Su papel es fundamental en tanto que se encarga de elaborar y aplicar las políticas relativas al tema objeto de estudio, y la certificación, investigación e innovación bajo el concepto de ciber resiliencia (Unión Europea, 2019), concepto ampliamente desarrollado en la Guía de 2016 CPMI-IOSCO.

### 1.3. La Ciberseguridad en las organizaciones

Las fallas de Ciberseguridad en las organizaciones se han convertido en uno de los riesgos de mayor probabilidad e impacto. Bajo este panorama, la Ciberseguridad desde las organizaciones es una práctica que sensibiliza y prepara a sus partes para enfrentar el riesgo cibernético propio de este ecosistema digital en donde se desarrolla, y establece un conjunto de estrategias y políticas para la protección, defensa, control y resiliencia. En este apartado se busca advertir del desenvolvimiento del riesgo cibernético en el mundo corporativo y los aspectos que las organizaciones requieren para mitigar y hacer frente a este tipo de amenazas.

La Confederación Europea de Asociaciones de Directores (ecoDa) ha descrito la Ciberseguridad como la ´amenaza de más rápido crecimiento y quizás la más peligrosa´ a la que se enfrentan las organizaciones en la actualidad (Clinton & Higgins, 2020). Según EY (2020), seis de cada diez organizaciones han sufrido un incidente cibernético material o significativo en los últimos doce meses. Los riesgos no podrían ser mayores. Los atacantes, cada vez más sofisticados, están sondeando los rincones oscuros de los sistemas y redes, buscando y encontrando vulnerabilidades (PwC, 2022), apuntando a un área de superficie cada vez mayor y utilizando tácticas más impredecibles. Cano (2021) plantea que los ciber-riesgos son riesgos líquidos porque adquieren la característica de líquidos, pues se configuran y mutan de acuerdo con el nivel de acoplamiento e interacción que tienen los objetos físicos digitalmente modificados, creando zonas ciegas de control que

terminan motivando escenarios inciertos, con objetos no conocidos y consecuencias inesperadas.

De acuerdo con Ernst & Young (2021), la disrupción económica y operativa desatada por COVID-19 ha aumentado notablemente tanto la motivación como la oportunidad para atacantes cibernéticos: un grupo grande y diverso que va, desde actores patrocinados por el estado y grupos del crimen organizado, hasta individuos motivados financieramente y activistas políticos y sociales tecnológicamente habilitados. Cabe aclarar la importancia de diferenciar la Ciberseguridad empresarial: no se puede ni se debe confundir con el ejercicio que se hace a escala nacional para proteger y defender las infraestructuras críticas de la nación (Cano, 2021).

Según PwC (2022), las organizaciones primero deben establecer esa buena base que llamamos confianza en los datos: asegurarse de que sus datos sean precisos, verificados y seguros, para que puedan confiar en ellos y tomar decisiones. Según Kaplan et al. (2015), el primer ejercicio para movilizar esfuerzos hacia la Ciberseguridad empresarial es reconocer y construir el mapa de actores y relaciones en su ecosistema digital; sabiendo que no puede eliminar de su análisis la materialización de un ciberataque, debe fundamentar sus acciones para lograr la resiliencia digital.

Una vez recreado el mapa de actores y relaciones propios del ecosistema digital, la empresa debe fundamentar sus acciones para alcanzar la resiliencia digital (Kaplan et al., 2015):

- La empresa comprende los riesgos de los ciberataques y puede tomar decisiones en que los retornos de las iniciativas tecnológicas planteadas justifican el incremento del riesgo.

- La compañía confía en que los riesgos de los ciberataques son manejables, más que los estratégicos, los cuales no ponen en riesgo la posición competitiva de la empresa o su existencia.

- Los clientes y los negocios tienen confianza en la economía en línea, en la que los riesgos sobre los activos de información y los fraudes en línea no son un freno para el crecimiento del comercio digital.

- El riesgo de ciberataques no limita a las empresas a la hora de continuar tomando ventaja de las innovaciones tecnológicas.

El ejercicio de resiliencia debe procurar la continuidad de los negocios, fundada en la capacidad de la empresa para gestionar los incidentes de seguridad y asegurar la disponibilidad de los sistemas, con base no solamente en sus posibilidades técnicas y operacionales, sino con el apoyo de sus socios estratégicos en el ecosistema digital en el que participa (Cano, 2021).

Como afirma PwC (2022), en este proceso la seguridad cibernética es una preocupación para todo el negocio, en cada función y para cada empleado, y se aconseja que la responsabilidad designada se de a un miembro específico de la Junta, idealmente alguien con experiencia relacionada. De hecho, dada la exposición al alto riesgo de las amenazas digitales, es fundamental evaluar periódicamente la eficacia de la función de Ciberseguridad y proporcionar al director de seguridad de la información el presupuesto y los recursos adecuados para abordar las debilidades identificadas (EY, 2021). A la vez, se espera que la Junta (EY, 2021):

- Solicite y revise un conjunto de indicadores clave de rendimiento perspicaces en relación con la seguridad cibernética y reciba informes periódicos de la gerencia.

- Tenga acceso a la información sobre las cadenas de suministro: qué proveedores tienen acceso a los sistemas de la organización y qué controles y protocolos de seguridad tienen implementados.

- Considere si la organización tiene un seguro adecuado para cubrir una brecha de seguridad cibernética importante.

- Programe demostraciones de piratería en vivo que le brinden información sobre la efectividad de la Ciberseguridad de la organización.

Teniendo en cuenta que la organización para su funcionamiento se estructura en dimensiones temáticas que representan los elementos de cómo operan, se describe a continuación cómo la Ciberseguridad se involucra en la gobernanza, gestión de riesgos, estrategia corporativa y evaluación de las implicaciones financieras.

### 1.3.1. Gobernanza del riesgo de Ciberseguridad

La gobernanza se presenta en este estudio como uno de los elementos que direccionan la operación de las organizaciones. Desde la óptica del riesgo de Ciberseguridad se busca definir el papel de la Junta Directiva o la alta dirección en el manejo de este riesgo emergente. De acuerdo con Burnap (2021), la gobernanza de riesgos se define como un conjunto general de procesos y principios en curso que tiene como objetivo garantizar la conciencia y la educación de los riesgos que se enfrentan cuando ocurren ciertas acciones, y para inculcar un sentido de responsabilidad y rendición de cuentas a todos los involucrados en su gestión. Según Renn (2008), es la base de la toma de decisiones colectivas y abarca tanto la evaluación como la gestión de riesgos, incluida la consideración de los contextos legal, social, organizativo y económico en los que se evalúa el riesgo.

La Blue Ribbon Commission de la NACD sobre Gobernanza del Riesgo recomendó que la supervisión del riesgo debería ser una función de toda la Junta (NACD, 2009). En relación con el riesgo de Ciberseguridad, OEA Internet Security Allience (2020) señala que las juntas directivas deben asumir un papel de liderazgo en la supervisión de la seguridad de los sistemas cibernéticos de su empresa. Antes de considerar cómo la Junta debe supervisar las actividades de la organización para administrar el riesgo, es útil

considerar las metas y objetivos de este esfuerzo de supervisión. ¿Qué debe tratar de lograr la Junta en su función de supervisión? Es importante señalar que ´supervisión´ incorpora tanto la función de vigilancia de los directores como la toma de decisiones que involucra el juicio desde el negocio. Si bien los objetivos de supervisión de riesgos pueden variar de una compañía a otra, cada directorio debe estar seguro que (NACD, 2009):

- El apetito de riesgo implícito en el modelo de negocio, estrategia y ejecución de la compañía es adecuado.
- Los riesgos esperados son proporcionales a los beneficios esperados.
- La dirección ha implantado un sistema de gestión, seguimiento y mitigación de riesgos adecuado al modelo de negocio y estrategia de la empresa.
- El sistema de gestión de riesgos informa al directorio de los principales riesgos que enfrenta la compañía.
- Existe una adecuada cultura de concienciación del riesgo en toda la organización.
- Se reconoce que la gestión del riesgo es fundamental para la ejecución exitosa de la estrategia de la empresa.

Por su parte, el estándar COSO (2017) contempla cinco componentes para el manejo del riesgo; el primero de ellos, la gobernanza. Desde este marco, la gobernanza: (1) ejerce la supervisión de riesgos del directorio, (2) establece la estructura de las operaciones, (3) define la cultura deseada, y (4) demuestra compromiso con los valores fundamentales.

ISO IEC 27014:2020 establece que la gobernanza de Ciberseguridad es un sistema mediante el cual se dirigen y controlan las actividades de seguridad de la información de una organización (ISO, 2020) para la protección de los activos de información digital frente a los riesgos relacionados con el uso de Internet (Von Solms & Von Solms, 2018).

Las pautas de la Asociación Nacional de Directores Corporativos (NACD) aconsejan que las juntas evalúen los riesgos cibernéticos considerando toda la empresa y comprendan los posibles impactos legales. Deben analizar, conjuntamente con la gerencia, los riesgos

de Ciberseguridad y la preparación y tener en cuenta las amenazas cibernéticas en el contexto de la tolerancia general al riesgo de la organización (NACD, 2009).

El papel principal de la Junta en la organización puede ser la supervisión, pero los miembros de la Junta están siendo cada vez más atraídos hacia el meollo de los problemas de seguridad cibernética (Deloitte, 2019b). Los líderes organizacionales reconocen ahora la importancia de verificar y salvaguardar la información de su negocio; el hecho de que en muchas ocasiones este tipo de eventos sean el primer eslabón de una serie de acciones consecutivas que, mal gestionadas, pueden tener un gran impacto en la reputación de la compañía, han convertido a los ciberataques en una de las principales preocupaciones de los directivos (PwC, 2022). Es probable que la evaluación de riesgos y el desarrollo de principios de mitigación para gestionarlos sean efectivos siempre que exista una política de gobernanza coordinada y bien comunicada dentro del sistema que se gestiona (CyBOK, 2019).

OEA; ISA (2020) proponen cinco principios para la supervisión efectiva del riesgo cibernético, y advierte que los directores adaptarán estas recomendaciones en función de las características únicas de su organización, incluyendo el tamaño, la etapa del ciclo de vida, la estrategia, los planes de negocios, el sector industrial, la huella geográfica, la cultura, los vínculos con las empresas familiares y las inquietudes de las partes interesadas mayoritarias. Los cinco principios se reproducen a continuación.

- Principio 1. Los directores deben comprender y abordar la Ciberseguridad como un problema de gestión de riesgos en toda la empresa, no solo como un problema de TI.
- Principio 2. Los directores deben entender las implicaciones legales de los riesgos cibernéticos según se relacionan con las circunstancias específicas de su empresa.
- Principio 3. Las juntas deben tener un acceso adecuado a la experiencia en Ciberseguridad, y se le debe proporcionar un tiempo regular y adecuado a

las discusiones sobre la gestión de riesgos cibernéticos en las agendas de las reuniones de la Junta.

- Principio 4. Los directores de la Junta deben establecer la expectativa de que la gerencia establecerá un marco de gestión de riesgo cibernético para toda la empresa con personal y presupuesto adecuados.
- Principio 5. La discusión de la Junta Directiva sobre el riesgo cibernético debe incluir la identificación de qué riesgos evitar, cuáles aceptar y cuáles mitigar o transferir a través de un seguro, así como planes específicos asociados con cada abordaje.

De acuerdo con Rashid et al. (2019), la seguridad cibernética debe pensarse como un conjunto claro de procesos que reducen el riesgo de daños a las personas y la empresa. Todos los involucrados en el diario funcionamiento del sistema en cuestión deben comprender que la seguridad es eficaz y hace parte de la cultura operativa diaria (PwC, 2022; Rashid et al., 2019). Vale la pena señalar que, según EY (2021), los propios miembros de la Junta pueden ser objetivos de interés para los piratas informáticos. Esto se debe a que:

- Tienen acceso a datos comerciales confidenciales.
- Es posible que hayan recibido una capacitación limitada en seguridad cibernética y no necesariamente estarán en el radar del equipo de TI de la organización debido a su antigüedad.
- Pueden estar intercambiando información confidencial por correo electrónico, exponiendo inadvertidamente a la organización al riesgo de ataques cibernéticos y filtraciones de datos.

A partir de estos imaginarios, se puede decir que es desde la gobernanza donde se lidera y supervisa el proceso contra el riesgo de Ciberseguridad, y la actitud del Gobierno Corporativo es decisiva en este proceso porque de su conocimiento, compromiso y sus actuaciones puede depender el futuro de la organización. Los comités con responsabilidad destinada a la supervisión del riesgo (y para la supervisión de los riesgos relacionados

con la cibernética en particular) deben recibir información general sobre Ciberseguridad por lo menos trimestralmente y cuando surjan incidentes o situaciones específicas (OAS; ISA, 2020). El riesgo de Ciberseguridad en las organizaciones puede ser designado bien sea al Comité de Auditoría  o al comité de riesgos de Ciberseguridad (Deloitte, 2016).

El Comité de Auditoría es una pieza angular en la gestión de áreas tan críticas como la supervisión del riesgo, la interacción con los auditores externos, la salvaguarda de los controles internos y la vigilancia de la información financiera (Deloitte, 2012). Frente al riesgo de Ciberseguridad, al igual que con otros temas de auditoría y riesgo, dicha supervisión lógicamente podría ser asignada por la Junta a su Comité de Auditoría (Fontaine & Reed 2018). El grado de participación del Comité de Auditoría en los problemas de Ciberseguridad varían significativamente según la empresa e industria (Deloitte, 2016). Es habitual que este comité sea generalmente responsable de la estrategia de Ciberseguridad (Héroux & Fortin, 2020). Poco más de la mitad de las juntas le asignan la mayoría de las responsabilidades de supervisión de riesgos relacionados con la Ciberseguridad al Comité de Auditoría, que ya suele estar sobrecargado y que también asume una responsabilidad importante en la supervisión de la información financiera y los riesgos de cumplimiento (OAS; ISA, 2020).

En el segundo caso, el Comité de Riesgos de Ciberseguridad se ocupará exclusivamente de los problemas de seguridad cibernética. Éste nuevo comité de la Junta puede supervisar la amplia gama de problemas relacionados con la cibernética que enfrentan las empresas, entre los que se incluyen: seguros cibernéticos, planes de respuesta a incidentes,; planes de continuidad del negocio, amenazas internas y los llamados malos abandonos (aquellos que dejan una empresa y presentan una amenaza, por ejemplo, causando estragos en los sistemas tecnológicos), debida diligencia de Ciberseguridad de terceros, prevención y respuesta al ransomware, contratación de personal de TI, formación en Ciberseguridad y presupuesto de seguridad de datos. En el desarrollo de estas funciones, y a partir de la experticia y conocimientos específicos del Comité de Ciberseguridad, se espera que éste aborde mejor estos riesgos y amenazas y, en consecuencia, aumente el alcance de las

revelaciones y la información que se comparte por parte de estas empresas a los diferentes grupos.

### 1.3.2. Estrategia de Ciberseguridad

La estrategia de Ciberseguridad se presenta en este estudio como el segundo elemento que direcciona la operación de las organizaciones. Acorde con el marco internacional COSO (2017), la estrategia se considera el segundo componente en el marco de la gestión de riesgos y le corresponde: (1) analizar el contexto de los negocios (2) definir el apetito del riesgo corporativo, (3) evaluar la estrategia alternativa y (4) formular los objetivos de los negocios. Las empresas entienden que las prácticas básicas de seguridad de la información, sustentadas en los estándares ISO 27002, NIST SP800-53, determinan los elementos que articulan las estrategias que se desarrollen para asegurar la nueva función de Ciberseguridad de la organización (Cano, 2021).

Una estrategia de Ciberseguridad se compone de planes de alto nivel sobre cómo una organización va a asegurar sus activos y minimizar el riesgo cibernético. Por lo general, se desarrollan con una visión de tres a cinco años, y son objeto de actualización y revisión con la mayor frecuencia posible (AT&T Cybersecurity, 2021). Hoy en día, es crucial tener una estrategia bien articulada de cumplimiento y control legal, y una gobernanza sólida para reducir los errores técnicos (Calderón et al., 2018). Uno de los objetivos más críticos para cualquier estrategia de Ciberseguridad es lograr la ciber-resiliencia; para ello, los líderes empresariales deben tener en cuenta que cada organización es única y requiere un enfoque de estrategia personalizado (AT&T Cybersecurity, 2021). Si bien es responsabilidad de todos cooperar para garantizar una mayor resiliencia cibernética, los líderes que establecen la estrategia para una organización son los responsables en última instancia, y se les ha hecho cada vez más responsables de incluir la resiliencia cibernética en la estrategia organizacional (WEF, 2017).

Desde esta perspectiva, podemos observar que la estrategia es el eje articulador de la gestión de riesgos corporativos. En el ámbito de la Ciberseguridad, de acuerdo con Kent

Baker et al. (2020), la Junta Directiva es de vital importancia para la empresa porque proporciona el enfoque estratégico y protege los intereses de los accionistas. Dentro del Gobierno Corporativo, el Comité de Auditoría es generalmente el responsable de la estrategia de Ciberseguridad (Héroux & Fortin, 2020). En la elaboración de esta estrategia las organizaciones enfrentan una batalla cuesta arriba al intentar definir procedimientos administrativos para cada posible situación de riesgo de seguridad. Por lo tanto, es necesario considerar la mentalidad de los empleados con respecto a la seguridad de la información (Karlsson et al., 2015). Las empresas deben considerar todo el ecosistema de Ciberseguridad que consiste en el riesgo cibernético, los impactos en la sociedad, la capacitación y educación, la ética, las técnicas, etc. (Radu & Smaili, 2021). Cuando se trata de gestionar el riesgo, un enfoque proactivo siempre es superior a uno reactivo. Pero para ser proactivo, especialmente cuando se descubren y detectan nuevas amenazas a un ritmo tan alarmante (AT&T Cybersecurity, 2021), se requiere de una estrategia organizacional dinámica y pensada al largo plazo.

### 1.3.3. Gestión de riesgos de Ciberseguridad

El riesgo está en el corazón de la vida cotidiana (Martín et al., 2021). Respecto a los indicios del riesgo, Slovic (1987) comenta que ha surgido como uno de los principales temas políticos de los años ochenta. El descubrimiento frecuente de nuevos peligros y la amplia publicidad que recibe está causando que más y más individuos se vean a sí mismos como las víctimas, más que beneficiarios, de la tecnología. Estos miedos y la oposición a la tecnología que producen han desconcertado a industriales y reguladores frustrados y han llevado a numerosos observadores para argumentar que la aparente búsqueda de un ´riesgo cero´ amenaza la estabilidad política y económica de la nación.

Esta reseña, consignada en 1987, coincide con la definición de riesgos de Renn (1998), que postula que ´los riesgos son siempre representaciones mentales de amenazas que son capaces de reclamar pérdidas reales´. El autor precisa que el riesgo es una construcción social y a la vez el resultado de una estimación técnica. Las personas han tenido que lidiar con peligros a lo largo de la historia, pero es solo recientemente que han podido hacerlo

de una manera anticipada y sistemática para controlar el riesgo (NCSC, 2022). La investigación sobre los temas de riesgo cibernético ha sido muy limitada hasta el año 2010, pero desde entonces ha crecido exponencialmente. Esto enfatiza la creciente relevancia del tema, tanto desde una perspectiva práctica como académica (Eling & Schnell, 2016a). La administración del riesgo relacionada con los sistemas de información y la comunicación han sido objeto de estudio durante décadas (Alavi & Weiss, 1985; Eloff et al., 1993; Rainer et al., 1991). Según Blakley et al. (2002), la seguridad de la información descuida la gestión de riesgos, está fallando debido a un enfoque en los tratamientos técnicos de mitigación de riesgos para reducir solo la probabilidad, pero no el impacto, de los eventos de seguridad ( Collier et al., 2013). Siponen & Oinas-Kukkonen (2007) revelan que la mayoría de las investigaciones hasta el año 2000 sobre seguridad de la información se centraron en el contexto técnico y en cuestiones de acceso a la seguridad de la información y comunicación segura. Argumentan que la seguridad cibernética debe pasar de un enfoque de ´problemas técnicos a nivel de componentes´ hacia un análisis de sistemas que integre los dominios físicos, de información, cognitivo y social.

De acuerdo con Eling & Schnell (2016), la investigación sobre el riesgo cibernético es limitada. Se pueden encontrar muchos artículos en el dominio de TI, pero se ha realizado relativamente poca investigación en la literatura empresarial y económica. La literatura muestra aportes desde el punto de vista semántico a medida que el riesgo de Ciberseguridad ha venido incorporándose en el panorama del riesgo organizacional (Biener et al., 2015; Cebula & Young, 2010; Eling & Schnell, 2016; Gordon et al., 2003; Mukhopadhyay et al., 2013; Öğüt et al., 2011).

Una de las definiciones más recientes es la de Strupczewski (2021), quien indica que: el riesgo cibernético es un riesgo operativo asociado con la realización de actividades en el ciberespacio, amenazando los activos de información, los recursos TIC y los activos tecnológicos, que pueden causar daños materiales a los activos tangibles e intangibles de una organización, interrupción del negocio o daño a la reputación.

Considerando el riesgo operativo como la posibilidad de ocurrencia de pérdidas derivadas de la materialización de una amplia variedad de eventos que incluyen fraude, robo, piratería informática, pérdida de personal clave, juicios, pérdida de información, terrorismo, vandalismo y desastres naturales (Moosa, 2007), vemos cómo el riesgo cibernético corresponde con esta definición. Se espera que este tipo de riesgo opere a partir de un sistema de gestión de riesgo empresarial (ERM, por sus siglas en inglés) relevante, debidamente desarrollado y en operación, en el que se recopilan, evalúan, priorizan, mitigan e informan adecuadamente los principales riesgos estratégicos de la empresa y otros riesgos (OAS; ISA, 2020).

Un proceso de gestión de riesgos cibernéticos aplica técnicas de mitigación y transferencia de riesgos para reducir el riesgo residual a niveles aceptables (Gordon, Loeb, & Sohail, 2003; Marotta & McShane, 2018; Siegel et al., 2002). Algunos autores proponen la compra de seguros como una estrategia para mitigar y transferir el riesgo (Bolot & Lelarge, 2008; Gordon, Loeb, & Lucyshyn, 2003; Siegel et al., 2002; Zeller & Scherer, 2020). Durante el proceso de gestión de riesgos, existe una interacción entre la mitigación de riesgos y la compra de seguros, es decir, los compradores de seguros suelen pagar primas más bajas al invertir más en la mitigación de riesgos (McShane et al., 2021).

La naturaleza correlacionada de los riesgos de vulneración de la seguridad, la capacidad imperfecta de demostrar la pérdida de una filtración a una aseguradora y la incapacidad de las aseguradoras y los agentes externos para observar los esfuerzos de autoprotección de las empresas, han planteado desafíos importantes para la gestión de riesgos de seguridad cibernética (Öğüt et al., 2011). Después de décadas tratando de superar las medidas técnicas (Madnick, 1978), este aspecto técnico aun domina el aspecto de gestión y carece de una visión económica de la seguridad de la información (Alshaikh et al., 2014).

La evaluación holística de los riesgos de Ciberseguridad es un problema complejo de múltiples componentes y niveles que involucra hardware, software, factores ambientales y humanos (Henshel et al., 2015). De acuerdo con McShane & Nguyen (2020), este riesgo

es difícil de incluir en el proceso general de gestión de riesgos empresariales, siendo necesario avanzar hacia la resiliencia cibernética para hacer frente a un riesgo tan complejo. El ciberriesgo, como una propiedad emergente de las relaciones digitalmente modificadas de la realidad, establece un reto cognitivo y social que demanda romper con los paradigmas disciplinares para encontrar respuestas o mejores preguntas en escenarios cada vez más inestables e inciertos, fruto de una mayor densidad digital en la dinámica de los elementos sociales (Cano, 2021). De acuerdo con Eling & Schnell (2016) los riesgos cibernéticos se pueden clasificar según la actividad (por ejemplo, delictiva y no delictiva), el tipo de ataque (por ejemplo, malware, ataque interno, spam o denegación de servicio distribuida) y la fuente (por ejemplo, terroristas, delincuentes y gobierno). Los ataques dependen principalmente de la actividad delictiva y se ven reforzados por efectos de red (por ejemplo, gusanos).

Von Solms & Van Niekerk (2013) definen como gestión del riesgo cibernético la protección de los activos de información y no información que se encuentran dentro del ciberespacio o que pueden verse afectados a través del ciberespacio. Para implementar un marco de Ciberseguridad efectivo, el proceso de gestión de riesgos de una organización comienza con una comprensión clara del entorno de amenazas y vulnerabilidades, su particular apetito de riesgo y la disponibilidad de recursos necesarios para mitigar los riesgos cibernéticos potenciales, los cuales deben abordarse desde una perspectiva estratégica, económica, interdepartamental e inter divisional (Internet Security Alliance and American National Standards, 2010).

En tal sentido, el ciberriesgo se configura como una apuesta relacional entretejida en la conectividad de los objetos físicos y las realidades sociales, que cambia la manera como se percibe el mundo y crea escenarios inéditos que retan las prácticas de gestión de riesgos actuales (Cano, 2021). La evaluación del riesgo, tanto cuantitativa como cualitativa, son procesos imprescindibles para lograr modelos de gestión de riesgos maduros y confiables (Escuela Europea, 2022). Sin embargo, según PwC (2022), actualmente solo el 26% cuantifica los riesgos cibernéticos. Para COSO ERM (2017) la evaluación de riesgos involucra un proceso dinámico e interactivo para identificar y analizar riesgos que

afectan el logro de objetivos de la entidad, dando las bases para determinar cómo los riesgos deben ser administrados. La evaluación de riesgos es, por lo tanto, un proceso de recopilación de observaciones y percepciones del mundo que pueden justificarse mediante razonamiento lógico o comparaciones con resultados reales (Renn, 2008).

Las características distinguen fundamentalmente al riesgo cibernético de otro tipo de riesgos. En primer lugar, la realidad virtual enfatiza el carácter intangible y, por tanto, las dificultades para evaluar las pérdidas. En segundo lugar, las redes están estrechamente relacionadas con el término ciberespacio que, con frecuencia, se utiliza como sinónimo de Internet (Biener & Eling, 2012).

Un aspecto importante para una buena gestión del riesgo cibernético es que el riesgo cibernético no es responsabilidad del departamento de TI, y requiere un diálogo global entre los diferentes departamentos (por ejemplo, sensibilización, formación) (Eling & Schnell, 2016a). Además, el compromiso institucional, demostrado al tener un responsable de seguridad de la información, es muy importante. Consecuentemente, las empresas deben contar con un director de seguridad de la información o un puesto similar (Eling & Schnell, 2016a)

El ciber-riesgo, como una propiedad emergente de las relaciones digitalmente modificadas de la realidad, establece un reto cognitivo y social que demanda romper con los paradigmas disciplinares, para encontrar respuestas o mejores preguntas en escenarios cada vez más inestables e inciertos, fruto de una mayor densidad digital en la dinámica de los elementos sociales (Cano, 2021). El riesgo cibernético puede mitigarse y minimizarse significativamente si se aborda como un problema de gestión de riesgos en toda la empresa. Sin embargo, al igual que con los riesgos tradicionales, los cibernéticos nunca podrán eliminarse por completo.

### 1.3.4. Implicaciones financieras

Según WEF (2021), en menos de una década la Ciberseguridad se ha convertido en uno de los problemas sistémicos más importantes para la economía mundial. El gasto global colectivo ha alcanzado los 145.000 millones de dólares al año y los incidentes y ataques siguen aumentando. Las empresas afectadas por ciberataques tienden a sufrir pérdidas económicas y de reputación duraderas (Agrafiotis et al., 2018; Kamiya et al., 2020). Los riesgos e incidentes de Ciberseguridad pueden afectar el desempeño financiero o la posición de una empresa (SEC, 2022).

Estas consecuencias financieras negativas, se materializan en costos de investigación forense, honorarios de abogados, gastos de litigio, costos de mejora de la seguridad cibernética y aumentos de las primas del seguro de riesgo cibernético (Deloitte, 2019; Meisner, 2018).

Bajo este panorama, la inversión en seguridad debe analizarse utilizando un enfoque holístico que combine diferentes factores (Bose & Luo, 2014) y que permitan, entre otros, proteger a las empresas contra eventos negativos (Gordon & Loeb, 2002). Sin embargo, las consecuencias de los diferentes incidentes cibernéticos y las violaciones de seguridad no solo repercuten al interior de las organizaciones sino que generan impactos globales asociados con una reacción negativa en los mercados (Berkman et al., 2018; Gordon et al., 2010).

## 1.4. Conclusiones

La multidimensionalidad e interdisciplinariedad de su significado nos permite afirmar hoy que no existe un único concepto de aceptación mundial del término Ciberseguridad. Para ratificar la amplia cobertura de su significado podemos citar la iniciativa inglesa CyBOK (2021). Ésta vincula veintiuna áreas de conocimiento desde el campo de acción de la Ciberseguridad, clasificadas en cinco dimensiones: (1) aspectos humano, organizacional y regulatorio; (2) ataques y defensas; (3) sistemas de seguridad; (4) seguridad de la infraestructura, y (5) seguridad de software y plataforma.

En la misma línea, la Agencia Europea de Seguridad de las Redes y de la Información ENISA (2015), respecto a la seguridad de las naciones, vincula cinco dominios relacionados con la Ciberseguridad: seguridad de las comunicaciones, seguridad de las operaciones, seguridad de la información, seguridad militar y seguridad física. Estos dominios, enmarcados desde el ámbito país, representan la amplitud del alcance global del término. Es de anotar que Estados Unidos y China, desde la geopolítica internacional, obtienen el liderazgo mundial en el manejo de la Ciberseguridad por la superioridad tecnológica que presentan.

Los antecedentes de la evolución del concepto de Ciberseguridad presentan términos relacionados que aportan en la construcción de su definición. Se trata de expresiones que cuentan con significados diferentes: seguridad informática, seguridad de la información y riesgo cibernético. Al respecto, es de resaltar que la definición de la seguridad de la información aporta las cualidades de la información en el ámbito organizacional: preservación de la confidencialidad, integridad y disponibilidad. En general, el concepto de Ciberseguridad requiere contemplar la protección de tres aspectos que necesariamente se adhieren a su definición: la protección de las personas, la protección de las cualidades de la seguridad de la información, y la protección de los activos físicos e infraestructuras que se encuentran en el ciberespacio.

Según nuestra búsqueda, un número reducido de autores se dan a la tarea de proponer una definición de Ciberseguridad: Craigen et al. (2014); Gordon et al. (2006); Haapamäki & Sihvonen (2019); Le & Hoang, (2017); Reid & Van Niekerk, 2014; Schatz et al. (2017); Tissir et al. (2020); Von Solms & Von Solms (2018). De igual manera, y respecto a las definiciones de Ciberseguridad planteadas por organismos internacionales, se puede observar la falta de uniformidad en torno al concepto, y el reducido alcance que presentan frente a los elementos que deben constituir hoy su definición: la seguridad de la información, la protección de las personas y la salvaguarda de los activos físicos.

Respecto al marco normativo internacional sobre Ciberseguridad, se puede afirmar que éste es el resultado de las medidas tomadas desde la geopolítica y la cooperación

internacional en torno a las amenazas y a la gestión del riesgo cibernético. Se considera que el Convenio de Budapest, la Recomendación de la Unión Internacional de Telecomunicaciones en 2008, la Recomendación OCDE, la Directiva 2016/1148, el Reglamento General para la Protección de Datos y la Ley de Ciberseguridad para la UE, son iniciativas legislativas que constituyen las regulaciones más importantes por su impacto en el ámbito internacional. Es de anotar que la búsqueda de acuerdos internacionales para perseguir al cibercrimen es fundamental para mitigar su impacto a nivel mundial, escenario sin fronteras para este tipo de delitos.

Desde el ámbito corporativo, las fallas de Ciberseguridad son uno de los riesgos de mayor probabilidad e impacto. Bajo este panorama, la Ciberseguridad desde las organizaciones es una práctica que sensibiliza y prepara a sus partes para enfrentar el riesgo cibernético propio de este ecosistema digital en donde se desarrolla, y establece un conjunto de estrategias y políticas para la protección, defensa, control y resiliencia. Estos retos se deben traducir en planes de acción y estrategias concretas que permitan asegurar la incorporación de la nueva normalidad, para así cambiar no solamente la estrategia de participación de la empresa en su entorno digital, sino activar un nuevo conjunto de habilidades y recursos que constituyan un nivel de resiliencia mayor.

Es importante señalar que el proceso de seguridad cibernética se lleva a cabo por parte de toda la organización, y para su funcionamiento se estructura en dimensiones temáticas que representan los elementos de cómo operan las organizaciones: (i) gobernanza (base para la toma de decisiones por parte de la Junta Directiva o la alta gerencia sobre las estrategias de las organizaciones con el objetivo de lograr la supervisión y liderazgo para el manejo del riesgo cibernético), (ii) estrategia corporativa (una estrategia de Ciberseguridad se compone de planes de alto nivel sobre cómo una organización va a asegurar sus activos y minimizar el riesgo cibernético), (iii) gestión de riesgos (sistema de gestión de riesgo empresarial en el que se priorizan, mitigan e informan los principales riesgos de la organización), y (iv) evaluación de las implicaciones financieras (la afectación económica que traen consigo las pérdidas económicas y de reputación por

posibles ciberataques o incidentes cibernéticos requieren ser evaluadas y valoradas dentro de la información financiera de la organización).

## 1.5. Referencias


Abbate, J. (2011). Inventing the internet. En *Networks of Innovation*. https://doi.org/10.1093/acprof:oso/9780199269051.003.0003

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/CYBSEC/TYY006

Alavi, M., & Weiss, I. R. (1985). Managing the Risks Associated with End-User Computing. *Journal of Management Information Systems*, *2*(3), 5–20. https://doi.org/10.1080/07421222.1985.11517734

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). *Towards a Taxonomy of Information Security Management Practices in Organisations*. https://openrepository.aut.ac.nz/handle/10292/8174

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *ACM International Conference Proceeding Series*, *September 2018*, 68–79. https://doi.org/10.1145/3285957.3285971

Arnum, E. (1995). Doing business on the Internet-A question of balance. *Business Communications Review*.

Asamblea General de las Naciones Unidas. (2001). *Resolución 56/183. Cumbre Mundial sobre la Sociedad de la Información*. 3.

AT&T Cybersecurity. (2021). *What is a Cybersecurity Strategy and How to Develop One*. https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

ATOS. (2020). *Universal Registration Document Board of Directors 2020*.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and

market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Biener, C., & Eling, M. (2012). *Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions*. *37*, 77–107. https://doi.org/10.1057/gpp.2011.29

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance: Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Blakley, B., Mcdermott, E., Morganchase, J. P., & Geer, D. (2002). Information Security is Information Risk Management. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*. https://doi.org/10.1145/508171

Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, *22*(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Burnap, P. (2021). Risk Management & Governance Knowledge Area. *The Cyber Security Body Of Knowledge*, 19–48.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. https://doi.org/10.1111/RISA.13687

Calderón, R., Piñero, R., & Redín, D. M. (2018). Can compliance restart integrity? Toward a harmonized approach. The example of the audit committee. *Business Ethics: A European Review*, *27*(2), 195–206. https://doi.org/10.1111/BEER.12182

Cano, J. (2021). *Ciberseguridad empresarial Reflexiones y retos para los ejecutivos del siglo XXI*.

Cavelty, M. D. (2010). *Cyber-Security* (Routledge (ed.)). The Routledge Handbook of New Security Studies: 154-162.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images*. *December*. http://www.sei.cmu.edu

Chang, H. C. (2016). The Synergy of Scientometric Analysis and Knowledge Mapping with Topic Models: Modelling the Development Trajectories of Information Security and Cyber-Security Research.

*http://dx.doi.org/10.1142/S0219649216500441*, *15*(4). https://doi.org/10.1142/S0219649216500441

Chen, T. ; R. J. (2004). *The Evolution of Viruses and Worms*. 289–310. https://doi.org/10.1201/9781420030884-19

Clarkson, P. M., Li, Y., Richardson, G. D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis. Accounting, Organizations and Society, 33(4–5), 303–327. https://doi.org/10.1016/j.aos.2007.05.003

Clinton, L., & Higgins, J. (2020). Cyber-Risk Oversight Cyber-Risk Oversight.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. Environment Systems and Decisions 2013 33:4, 33(4), 469–470. https://doi.org/10.1007/S10669-013-9484-Z

Convenio de Budapest, | (2001).

COSO. (2017). COSO II ERM.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Crowdstrike. (2021). The evolution of ransomware: how to protect against new adversary trends and methods. 1–9.

CyBOK. (2019). The Cyber Security Body of Knowledge (CyBoK) 1.0. CyBoK, 299. https://www.cybok.org/

CyBOK. (2021). Introduction to CyBOK Knowledge Areas. The Cyber Security Body of Knowledge, 22. www.cybok.org

Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. https://doi.org/10.1080/10580530701586136, 24(4), 361–372. https://doi.org/10.1080/10580530701586136

Deloitte. (2012). Guía Práctica Consejeros del Comité de Auditoría.

Deloitte. (2016). Cyber security: The changing role of the Board and the Audit Committee. June, 5. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

Deloitte. (2019a). Índice Global de Ciberseguridad - 2018. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html

Deloitte. (2019b). Managing Cyber Risk in a Digital Age. Coso, 28. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Dobran, B. (2021). 17 Types of Cyber Security Attacks To Protect Against in 2021. https://phoenixnap.com/blog/cyber-security-attack-types/

Domenech, J. J. G. (2017). La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE. REVISTA LEX MERCATORIA Doctrina, Praxis, Jurisprudencia y Legislación, 37–42. https://doi.org/10.21134/LEX.VI.534

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law and Security Review, 40, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Eling, M., & Schnell, W. (2016a). What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance, 17(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122/FULL/PDF

Eling, M., & Schnell, W. (2016b). What do we know about cyber risk and cyber risk insurance? En Journal of Risk Finance (Vol. 17, Número 5, pp. 474–491). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-09-2016-0122

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. Computers & Security, 12(6), 597–603. https://doi.org/10.1016/0167-4048(93)90056-B

ENISA. (2015). Definition of Cybersecurity | Gaps and overlaps in standardisation. En European Union Agency For Network And Information Security: Vol. v1.0 (Número December).

Ernst & Young. (2021). EY Global Information Security Survey 2021: Cybersecurity: how do you rise above the waves of a perfect storm?

EU. (2019). Regulation (EU) 2019/881. Regulation (EU) 2019/881 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

Europea, U. (2015). Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document. https://doi.org/10.1787/9789264245471-en

Excelencia, E. E. de. (2022). Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál escoger? https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-riesgo-cuantitativa-vs-cualitativa-cual-escoger/

EY. (2020). EY Global Information Security Survey 2020. How does security evolve from bolted on to built-in? https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf

EY. (2021). Board Agenda 2021. 1(1), 21.

Fidler, D. P. (2020). Cybersecurity in the Time of COVID-19. Council on Foreign Relations, 2020, 7–9. https://www.cfr.org/blog/cybersecurity-time-covid-19

Fontaine, David; Reed, J. (2018). Cybersecurity: The SEC's Wake-up Call to Corporate Directors. Harvard Law School. https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/

Gómez Vieites, A. (2006). Enciclopedia de la seguridad informática.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. En Computer Security Journal (Vol. 19, Número 2, pp. 1–7). Computer Security Institute.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. Journal of Accounting and Public Policy, 25(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81–85. https://doi.org/10.1145/636772.636774

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. MIS Quarterly: Management Information Systems, 34(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692

Gunter, O. (2004). The Phishing Guide. History.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. En Managerial Auditing Journal (Vol. 34, Número 7, pp. 808–834). Emerald Group Publishing Ltd. https://doi.org/10.1108/MAJ-09-2018-2004

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers and Security, 73, 102–113. https://doi.org/10.1016/J.COSE.2017.10.008

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. Procedia Manufacturing, 3, 1117–1124. https://doi.org/10.1016/J.PROMFG.2015.07.186

Héroux, S., & Fortin, A. (2020a). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. Accounting Perspectives, 19(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S., & Fortin, A. (2020b). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. Accounting Perspectives, 19(2), 73–100. https://doi.org/10.1111/1911-3838.12220

IDB; OAS. (2020). Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

International Telecommunication Union. (2008). Overview Cybersecurity. ITU-T X.1205 Recommendation, 1205(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I

Internet Security Alliance and American National Standards. (2010). The Financial Management of Cyber Risk: An Implementation Framework for CFOs. Order A Journal On The Theory Of Ordered Sets And Its Applications.

IOSCO. (2016). Cyber Security in Securities Markets – An International Perspective Report on IOSCO ’ s cyber risk coordination efforts.

ISO. (2012). ISO/IEC 27032: Information technology — Security techniques — Guidelines for cybersecurity. ISO 27032. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO. (2013). ISO 27002.

ISO. (2020). ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security. https://www.iso.org/standard/74046.html

ITU. (2018). Global Cybersecurity Index (GCI) 2018 ITUPublications Studies & research.

James P. Anderson, Sheila Brand, Li Gong, T. H. (2004). Firewalls: an Expert Roundtable. En Book Security, Statistical Methods in Computer (Edition, E, pp. 333–350). CRC Press. https://doi.org/10.1201/9781420030884-21

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics. https://doi.org/10.1016/j.jfineco.2019.05.019

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). Beyond Cybersecurity: Protecting Your Digital Business. Exhibit 1, 1–9. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1119026849,descCd-buy.html

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. Information & Computer Security, 23(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020). A bibliometric analysis of board diversity: Current status, development, and future research directions. Journal of Business Research, 108, 232–246. https://doi.org/10.1016/j.jbusres.2019.11.025

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. IEEE Communications Surveys and Tutorials, 15(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597–607. https://doi.org/10.1016/J.IM.2003.08.001

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122. https://doi.org/10.1016/J.JISA.2014.09.005

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? 2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016. https://doi.org/10.1109/PCCC.2016.7820663

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. Sloan management review, 20(1), 61–74.

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. Risk Management and Insurance Review, 21(3), 435–452. https://doi.org/10.1111/RMIR.12109

Mayor Gómez, R. (2016). Contenido y novedades del reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). Gabilex. Revista del gabinete jurídico de Castilla la Mancha.

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93–125. https://doi.org/10.1111/RMIR.12169

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. Geneva Papers on Risk and Insurance: Issues and Practice, 45(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63. https://doi.org/10.12775/cjfa.2017.017

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. Computers & Security, 73, 87–101. https://doi.org/10.1016/J.COSE.2017.10.009

Merriam -Webster. (2021). Cybersecurity | Definition of Cybersecurity. Merriam-Webster.com Dictionary, Merriam-Webster. https://www.merriam-webster.com/dictionary/cybersecurity

Middleton, B. (2017). A History of Cyber Security Attacks 1980 to present (T. & Francis (ed.)).

Mirkovic, J., Reiher, P., & Hall, B. (2004). A Taxonomy of DDoS Attack and DDoS

Defense Mechanisms *.

Moosa, I. A. (2007). Operational Risk: A Survey. Financial Markets, Institutions & Instruments, 16(4), 167–200. https://doi.org/10.1111/J.1468-0416.2007.00123.X

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? Decision Support Systems, 56(1), 11–26. https://doi.org/10.1016/J.DSS.2013.04.004

NACD. (2009). Report of the NACD blue ribbon commission. Risk governance: balancing risk and reward. https://www.wlrk.com/docs/1605831_1.pdf

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. https://doi.org/10.1080/23738871.2016.1157619, 1(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

NCSC. (2022). Essential Topics - NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious Software Threats. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 793–813. https://doi.org/10.1007/978-3-319-78440-3_35

NICCS. (2017). Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies. Explore terms: a glossary of common cybersecurity terminology. https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C ( 2017 )

Nwosu, A. U., Goyal, S. B., & Bedi, P. (2020). Blockchain Transforming Cyber-Attacks: Healthcare Industry. Advances in Intelligent Systems and Computing, 1372 AISC, 258–266. https://doi.org/10.1007/978-3-030-73603-3_24

OAS; ISA. (2020). Manual de supervisión de riesgos cibernéticos para juntas corporativas. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. Risk Analysis, 31(3), 497–512. https://doi.org/10.1111/J.1539-6924.2010.01478.X

Orman, H. (2003). The Morris worm: a fifteen-year perspective. IEEE Security & Privacy, 1(5), 35–43. https://doi.org/10.1109 / MSECP.2003.1236233

Packard, N. (2020). Three kinds of demand pull for the ARPANET into the Internet. http://www.editorialmanager.com/cogentsocsci, 6(1). https://doi.org/10.1080/23311886.2020.1720565

Parker, D. B. (2007). The dark side of computing: SRI International and the study of computer crime. IEEE Annals of the History of Computing, 29(1), 3–15. https://doi.org/10.1109/MAHC.2007.15

PwC. (2022). 2022 Global Digital Trust Insights.

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Rel ated Disclosure. Journal of Business Ethics, 1, 3. https://doi.org/10.1007/s10551-020-04717-9

RAE ASALE. (2020). Diccionario de la lengua española. Edición 2020. https://dle.rae.es/cibernético?m=form

Rainer, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. Journal of Management Information Systems, 8(1), 129–147. https://doi.org/10.1080/07421222.1991.11517914

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. IEEE Access, 4, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Reid, R., & Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies. Information Security South Africa (ISSA), 1–7. https://doi.org/978-1-4799-3383-9

Renn, B. O. (2008). Risk Governance new & Forthcoming Titles. En Sustainable Development. https://www.routledge.com/Risk-Governance-Coping-with-Uncertainty-in-a-Complex-World/Renn/p/book/9781844072927

Renn, O. (1998). The role of risk perception for risk management. Reliability Engineering and System Safety, 59(1), 49–62. https://doi.org/10.1016/S0951-8320(97)00119-1

Roberts, L. G. (1988). The ARPANET & Computer Networks. Proceedings of the ACM Conference on The history of personal workstations. https://doi.org/10.1145/12178

Rowe, D. C., Ekstrom, J. J., & Lunt, B. M. (2012). Cyber-Security, IAS and the Cyber Warrior. The Colloquium for Information Systems Security Education.

Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access

control, assurance and system security. International Journal of Multimedia and Ubiquitous Engineering, 2(2), 17–32.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. Proceedings - International Conference on Distributed Computing Systems, 2016-August, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law, 12(2), 8. https://doi.org/https://doi.org/10.15394/jdfsl.2017.1476

SEC. (2022). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. 13(34), 1–204.

Security Boulevard. (2021). How Offensive AI Can Disarm Cybersecurity. https://securityboulevard.com/2021/06/how-offensive-ai-can-disarm-cybersecurity/

Shankar, K. S. (1977). The Total Computer Security Problem: An overview.

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Information Security Management Handbook, Sixth Edition, 357–380. https://doi.org/10.1201/9781420072419-28

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions.

Slovic, P. (1987). Perception of Risk. Science, 236(4799), 280–285. https://doi.org/10.1126/SCIENCE.3563507

Sofistic, C. (2017). Breve historia de la Ciberseguridad. https://www.sofistic.com/blog-Ciberseguridad/la-breve-historia-de-la-Ciberseguridad/

Souppaya, M., & Scarfone, K. (2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. https://doi.org/10.6028/NIST.SP.800-83R1

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. En Politics and Governance (Vol. 6, Número 2, pp. 1–4). Cogitatio Press. https://doi.org/10.17645/pag.v6i2.1569

Strupczewski, G. (2021). Defining cyber risk. Safety Science, 135, 105143. https://doi.org/10.1016/J.SSCI.2020.105143

Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. Journal of Reliable Intelligent Environments 2020 7:2, 7(2), 69–84. https://doi.org/10.1007/S40860-020-00115-0

UIT. (2012). UIT-IMPACT organizan un cibersimulacro transfronterizo para la región de los Estados Árabes.

Unión Europea. (2016a). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo. Unión Europea.

Unión Europea. (2016b). Reglamento (UE) 2016/ 679. Diario Oficial de la Unión Europea.

Unión Europea. (2019). REGLAMENTO (UE) 2019/881. Diario Oficial de la Unión Europea.

Unión Internacional de Telecomunicaciones. (s. f.). La agenda sobre ciberseguridad global – actualizacion.

Unión Internacional de Telecomunicaciones. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. Unión Internacional de Telecomunicaciones, 1205, 66.

United Nations General Assembly. (2009). Resolución 64/25.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? Information & Computer Security, 26(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

WEF. (2017). Advancing Cyber Resilience - Principles and Tools for Boards. World Economic Forum, January, 40.

WEF. (2021a). Centre for Cybersecurity > Platforms | World Economic Forum. https://www.weforum.org/platforms/the-centre-for-cybersecurity

WEF. (2021b). Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico | foro Economico Mundial. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

WEF. (2022). The Global Risks Report 2022. https://www.weforum.org/reports/global-

risks-report-2022

WEF, W. E. F. (2020). The Global Risks Report 2020. https://es.weforum.org/reports/the-global-risks-report-2020

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. En Cengage Learning.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt. USENIX Security Symposium, 679–702. http://www.doug-tygar.com/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf

Williams, T. D. (2020). Epistemological Questions for Cybersecurity. International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020, 1–4. https://doi.org/10.1109/CyberSecurity49315.2020.9138884

Woollacott, P. (2007). Cybercrime comes of age. ITNOW, 49(2), 6–7. https://doi.org/10.1093/COMBUL/BWL110

Yang, A., Kwon, Y. J., & Lee, S. Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. Industrial Management & Data Systems, 120(9), 1777–1794. https://doi.org/10.1108/IMDS-10-2019-0536

Zeller, G., & Scherer, M. (2020). A comprehensive model for cyber risk based on marked point processes and its application to insurance. European Actuarial Journal. https://doi.org/10.1007/s13385-021-00290-1

# CAPÍTULO 2. LA DIVULGACIÓN DE INFORMACIÓN SOBRE RIESGOS CIBERNÉTICOS

Según SEC (2022), los inversionistas se benefician de una mayor divulgación sobre gestión de riesgos de Ciberseguridad, estrategia y prácticas de gobierno para evaluar mejor si las empresas están gestionando los riesgos de Ciberseguridad y cómo lo están haciendo. En general, se acepta que en el ámbito empresarial hubo una subestimación del riesgo ampliamente compartida antes de la crisis financiera de 2008. No obstante, la crisis también condujo a llamados para una mejor información de riesgos por parte de las organizaciones en todos los sectores (ICAWE, 2011). Actualmente, el mundo corporativo cuenta con diferentes modelos opcionales de riesgo, como los propuestos por COSO ERM y por la norma ISO 31.000, entre otros, que tratan sobre gestión de riesgos con relación a los sistemas de información, gobierno de Tecnologías de la Información, continuidad de negocios y resiliencia organizacional.

Las complejidades y la controversia de regular las prácticas de información de riesgos, así como las propias normas, han jugado un papel importante en el surgimiento de una gran y creciente literatura sobre información de riesgos (Elshandidy et al., 2018). A la vez, se ha trazado un cuerpo sustancial de regulaciones sobre informes de riesgos. En Estados Unidos la primera modificación se presenta en 1980 por parte de la SEC, frente al informe MD&A; en 1990 aumentan los requisitos en el informe de instrumentos financieros SFAS 119 y SFAS 133 (FASB, 1998) y FRR 48 (SEC, 1997); y a partir de 2002, las revelaciones sobre factores de riesgo según el artículo 503 (c) de la Regulación S-K se realizan a partir de la Sección 404 de la Ley Sarbanes Oxley de 2002. Desde la Unión Europea (UE) se establece la Directiva 2014/95 de la UE que, entre otros temas, relaciona el alcance de la divulgación de riesgos corporativos. El Código de Gobierno Corporativo del Reino Unido de 2018 determina la naturaleza y el alcance de los principales riesgos. En el sector financiero, el Acuerdo de Basilea solicita la divulgación de los riesgos materiales y promueve la comparabilidad de los diferentes perfiles de riesgo de los bancos. En América Latina, los principios generales de Gobierno Corporativo de OCDE y G20 (2016) son el referente para el tratamiento de riesgos organizacionales. En la actualidad es de resaltar el papel preponderante de la divulgación de riesgos relacionados con la sostenibilidad, en especial las revelaciones establecidas por el Grupo

de Trabajo sobre Divulgaciones Financieras relacionadas con el riesgo de Cambio Climático (TCFD).

La Ciberseguridad se ha convertido en un problema importante que enfrentan la mayoría de las organizaciones (Calderon & Gao, 2021), y en un mundo conectado digitalmente, se presentan riesgos y amenazas constantes para los mercados de capitales y las empresas que operan en todas las industrias (SEC, 2018). Respecto a la divulgación de riesgos de Ciberseguridad, ésta se traduce en una responsabilidad social ineludible por parte de las organizaciones. Los riesgos de Ciberseguridad, en su mayoría, son categorizados como riesgos operacionales que se incorporan en la gestión de riesgos corporativos. En este marco, la divulgación sobre la gestión del riesgo cibernético es una práctica que aumenta significativamente en los informes anuales corporativos, en los informes voluntarios y obligatorios, así como en los sitios web de las empresas.

En la actualidad, los informes anuales se pueden presentar tomando como base diferentes estándares de aceptación internacional. Entre ellos: Estándar GRI 2016, Reporte Integrado, estándares emitidos por el American Sustainability Accounting Standard Board (SASB), Formulario 10 K EDGAR y Formulario 20 F EDGAR, todos con apartes especiales para la divulgación de riesgos de Ciberseguridad. La literatura reciente presenta avances entorno a la divulgación de información relacionada con Ciberseguridad (Amir et al., 2018; Berkman et al., 2018; Eijkelenboom & Nieuwesteeg, 2021; Ettredge et al., 2018; Gao et al., 2020; Héroux & Fortin, 2020a; Mazumder & Hossain, 2022; Radu & Smaili, 2021). Según Gordon et al. (2006), las empresas han aumentado sus divulgaciones voluntarias sobre seguridad de la información.

En este contexto, el presente capítulo tiene como objetivo describir los avances sobre la divulgación de información sobre riesgos cibernéticos. Para ello, en primer lugar, se presenta un breve resumen cronológico de los principales acontecimientos que perfilan la historia del riesgo corporativo en el ámbito mundial. Seguidamente, se presentan las características de la divulgación de información corporativa sobre riesgos, tanto obligatoria como voluntaria, a partir de los estudios previos en el ámbito internacional.

Finalmente, nos referimos a la divulgación de información sobre Ciberseguridad, tanto obligatoria como voluntaria, así como a los tipos de informes y comunicaciones utilizados para reportar las revelaciones relacionadas con Ciberseguridad.

## 2.1. El Riesgo Corporativo

Según el estándar internacional COSO ERM (2017), el riesgo comprende barreras que se imponen a la organización en su crecimiento o inclusive para su supervivencia. Eliminar completamente el riesgo es una situación hipotética, porque los factores a considerar son demasiados en un entorno donde el dinamismo es una constante. A su vez, el estándar internacional sobre gestión de riesgos en su última versión ISO 31000 (2018), define el riesgo, como: …el efecto de la incertidumbre sobre los objetivos. Este efecto, como una desviación respecto a lo previsto, puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Con frecuencia, el riesgo se expresa en términos de fuentes de riesgos, sus consecuencias de eventos potenciales y sus probabilidades. Las partes interesadas en este proceso pueden ser una persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

Estas definiciones son el resultado de algunos acontecimientos que marcaron el devenir del riesgo corporativo, tal como lo conocemos actualmente. Varias discusiones sobre riesgo surgieron en la década de 1950, pero se relacionaban con la matemática; a menudo, consistían en aplicar la probabilidad, buscando predecir los resultados en los mercados volátiles de las organizaciones. El uso del término ´gestión de riesgos´ comenzó en 1956 con la publicación de ´Gestión de riesgos: una nueva fase de control de costos´, escrito por Russell Gallagher, quien planteó un “programa viable para la 'gestión de riesgos', dejando éste bajo la dirección de un ejecutivo, denominado ‘gestor de riesgos” (Fraser, 2010). El surgimiento de la gestión de riesgos fue una revolución que marcó un cambio en la filosofía y ocurrió cuando la actitud hacia los seguros cambió, al perder su estatus tradicional como enfoque estándar para tratar los riesgos (Brazilian Institute of Corporate Governance, 2020). De este modo, se acepta que la gestión de riesgos evolucionó a partir de la compra de seguros corporativos (Sinha & Vaughan, 1994).

No fue hasta principios de la década de 1970 que la gestión de riesgos comenzó a tener una participación más amplia en los negocios, particularmente en los Estados Unidos. En París, en 1971, un grupo de ejecutivos de compañías de seguros se reunieron para crear la Asociación Internacional para el Estudio de la Economía de los Seguros; dos años más tarde, la Asociación de Ginebra, su nombre más familiar, celebra su primera asamblea constituyente y comienza a vincular la gestión de riesgos, seguros y economía (Fraser, 2010). Según Ting (1988), en 1973, cuando los precios del petróleo se dispararon, la crisis trajo consigo una mayor volatilidad en el entorno económico y, en consecuencia, los gerentes comenzaron a ver más de cerca la evaluación de riesgos. En 1974, Gustav Hamilton, el administrador de riesgos de Statsforetag, de Suecia, crea un ´círculo de gestión de riesgos´, que describe gráficamente la interacción de todos los elementos del proceso, desde la evaluación y el control, hasta la financiación y comunicación (Fraser, 2010). En 1975, en Estados Unidos, la Sociedad Americana de Gestión de Seguros cambia su nombre a Sociedad de Gestión de Riesgos y Seguros (Vaughan, 1997).

Por lo que respecta al sector financiero, el incentivo para implementar la gestión de riesgos surgió en la década de 1980, con la creciente preocupación del Banco de Inglaterra y de la Reserva Federal de EEUU por la exposición de los bancos a operaciones desmedidas, combinadas con problemas de préstamos (Brazilian Institute of Corporate Governance, 2020). En 1985 surge COSO, organización de carácter voluntario, constituida por representantes de cinco organizaciones del sector privado en Estados Unidos. Esta organización nace con la misión de crear y proporcionar conocimiento frente a tres grandes temas relacionados, concretamente, la gestión del riesgo empresarial (ERM), el control interno y la lucha contra el fraude. Un año después se crea el Instituto para la Gestión de Riesgos en Londres. En 1987, el ´Lunes Negro´ trae al mercado de valores de Estados Unidos un choque global de olas, recordando a todos los inversores el riesgo inherente del mercado y su volatilidad (Fraser, 2010). Con el nombre de Basilea I se conoce al acuerdo publicado en 1988, en Suiza, por el Comité de Basilea, compuesto por los dirigentes de los bancos centrales de Alemania, Bélgica, Canadá, España, Estados Unidos, Francia, Italia, Japón, Luxemburgo, Holanda, Reino Unido, Suecia y Suiza. Se

trataba de un conjunto de recomendaciones para establecer un capital mínimo que debía tener una entidad bancaria en función de los riesgos que afrontaba.

En algún momento a mediados de 1990, las empresas comenzaron a poner en marcha una amplia gama de iniciativas bajo el estandarte de la gestión de riesgos. A finales de la década, las organizaciones habían elaborado marcos institucionalizados al respecto, bajo el título de 'gestión de riesgos´ en toda la empresa (Hunt, 2003). La nueva ola de gestión de riesgo puede ser considerada como una reacción defensiva a un entorno cada vez más exigente (Power, 2004). En 1992, el Comité COSO publicó el primer informe, denominado COSO I, que tenía el objetivo de ayudar a las entidades a evaluar y mejorar sus sistemas de control interno.

En este mismo año, el Comité Cadbury emite su informe en el Reino Unido, sugiriendo que los consejos de administración son los encargados de establecer la gestión de la política de riesgos, asegurando que la organización comprende todos sus riesgos y aceptando la supervisión de todo el proceso. En esta línea, Canadá, Estados Unidos, Sudáfrica, Alemania y Francia establecen un mandato nuevo y más amplio para las organizaciones. En ese mismo año, el Banco de Pagos Internacionales emite su Acuerdo Basilea I para ayudar a instituciones financieras a medir sus riesgos crediticios y de mercado, y fijan el capital respectivo. A partir de 1993 se introdujeron reglas para el riesgo de mercado, que tienen como referencia principal la publicación por JP Morgan, ´Métricas del riesgo´, en octubre de 1994; el documento surgió en respuesta a los grandes desastres financieros de inicios de los años 1990 (casos conocidos como los de Procter & Gamble, Orange County, Barings, entre otros) e introdujo el concepto de ´valor en riesgo´ (VaR). El VaR mide la pérdida potencial máxima del valor de una cartera con determinado nivel de confianza en un intervalo de tiempo dado y en condiciones normales de funcionamiento del mercado (Brazilian Institute of Corporate Governance, 2020; Jorion, 2002).

En 1995, un grupo de trabajo multidisciplinario de Standards Australia y Standards Nueva Zelanda publica el primer Estándar de Gestión de Riesgos, AS/NZS 4360:1995 (revisado

desde 1999 y 2004), reuniendo por primera vez diferentes subdisciplinas. Este estándar es seguido por esfuerzos similares en Canadá, Japón y el Reino Unido. Mientras algunos observadores piensan que el esfuerzo es prematuro, debido a la constante evolución de la naturaleza de la gestión de riesgos, la mayoría lo saluda como un importante primer paso hacia un marco común global de referencia. En la última década, éste y otros problemas de riesgo operacional han provocado que los reguladores de la banca de todo el mundo se centren más en el riesgo operativo en bancos.

Pero el Siglo XXI se iniciaría con una nueva onda de escándalos corporativos (Enron, WorldCom, Adelphia, entre otros), que demandarían aún mayor regulación. Como respuesta, fue creada en 2002 en los Estados Unidos la Ley Sarbanes-Oxley (SOX), norma que enfatizó el papel fundamental de los controles internos, la identificación y evaluación de riesgos y transformó en exigencia legal, las buenas prácticas de Gobierno Corporativo. La Ley SOX afectó a todas las empresas americanas y extranjeras con títulos y acciones negociados en bolsas americanas, además de sus subsidiarias. En 2004, el Comité de Supervisión Bancaria de Basilea publicó el Acuerdo de Basilea II, extendiendo sus lineamientos de capital global al riesgo operacional (Basilea I riesgos de crédito y de mercados cubiertos). En 2005, es aprobado y publicado por ISO y por la Comisión Electrotécnica Internacional como estándar internacional ISO/IEC 27001, norma para la seguridad de la información. En este mismo año, ISO también crea un grupo de trabajo para redactar una nueva "guía" global para la definición, aplicación y práctica de la gestión de riesgos, aprobada en 2009 como ISO /IEC 31000. En el año 2010 el Comité de Supervisión Bancaria de Basilea volvió a proponer un nuevo acuerdo, Basilea III, que pasó a promover el aumento de reserva de capital por parte de los bancos en busca de protección a eventuales crisis y sus consecuencias, ´estampida bancaria por incertidumbre´. Como resultado de la crisis financiera de 2007-2008, se revelaron graves deficiencias en términos de regulación en el sistema financiero mundial. El riesgo sistémico y la importancia sistémica de las instituciones financieras fueron impulsados al frente de la investigación y el debate por la crisis financiera mundial de 2007–2008 y, más tarde, por la crisis de la deuda soberana de la Eurozona (Dungey et al., 2022).

En la actualidad, como resultado de los antecedentes descritos, existen varias estructuras y modelos de gestión de riesgo corporativo, como los propuestos por COSO - ERM 2017 y por la norma ISO 31.000 (pudiendo integrarse aquí también, de forma auxiliar, las normas ISO 22.301, familia ISO 27.000 y NIST, ISO 38.500, COBIT 5, la norma BS 65.000 del British Standard Institute -BSI-, que tratan sobre gestión de riesgos con relación a los sistemas de información, gobierno de TI, continuidad de negocios y de la resiliencia organizacional). A la fecha, el tema de riesgos se ha desarrollado como una metodología estructurada a partir de varias vertientes, entre las que destacan las de finanzas, auditoría, estrategia y tecnología de la información (Brazilian Institute of Corporate Governance, 2020).

## 2.2. Divulgación de información corporativa sobre riesgos

Una rama de la literatura sobre divulgación de información corporativa se refiere, particularmente, a la información sobre riesgos (Abraham & Cox, 2007). Se espera que las revelaciones sobre riesgos se realicen con una visión prospectiva. Según Oliveira et al. (2011), una mayor divulgación de información sustantiva y relevante relacionada con el riesgo en los informes anuales de la empresa apuntan a una mejor rendición de cuentas. Ha habido muchos llamamientos para reducir las asimetrías de acceso a la información corporativa y mejorar la medición y divulgación de los asuntos relacionados con el riesgo (Beretta & Bozzolan, 2004; Konishi & Ali, 2007; Szegö, 2002), los cuales han sido motivados por la inadecuación de las prácticas de reporte de riesgos (Solomon et al., 2000).

En general, se acepta que hubo una subestimación del riesgo ampliamente compartida antes de la crisis financiera de 2008. Esto ha reforzado los llamamientos a mejorar los informes de riesgo (ICAWE, 2011). Como consecuencia, algunos métodos de gestión de riesgos han evolucionado con el tiempo, las empresas han aprendido a utilizar técnicas sofisticadas para cuantificar y monitorear el riesgo de manera efectiva, reduciendo así, la brecha de calidad en los sistemas internos de gestión de riesgos. Sin embargo, se percibía que la información externa de las empresas a principios de siglo carecía de una

divulgación adecuada sobre el riesgo y las incertidumbres (Cabedo & Tirado, 2004). Solomon et al., (2000) señalaron que los inversores exigían más información para ayudarlos a evaluar el perfil de riesgo de una empresa y tomar decisiones informadas. Del camino recorrido en este tema de riesgos, se puede decir que la transformación de las características y alcance del ´control´ es un proyecto de dar vuelta a las organizaciones ´de adentro hacia afuera´ y de hacer públicos sus sistemas de control interno basados en riesgos, materia divulgable como nunca antes (Power, 2004).

Un referente internacional en la divulgación de riesgos lo constituyen los Principios de Gobierno Corporativo del G20 y de la OCDE. Desde su primera publicación en 1999, los Principios se han convertido en un referente internacional para legisladores, inversores y otros actores interesados en todo el mundo (OCDE, 2016). Asimismo, se encuentran entre las Normas Fundamentales de los Sistemas Financieros Sólidos del Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés) y constituyen la base de los informes relativos a la observancia de códigos y normas (IOCN) del Banco Mundial en el área de Gobierno Corporativo.

Respecto a la divulgación de riesgos relacionados con la sostenibilidad en el ámbito internacional, goza de un reconocimiento muy marcado las divulgaciones financieras establecidas por el Grupo de Trabajo sobre Divulgaciones Financieras relacionadas con el Cambio Climático (TCFD), cuya aceptación mundial se realiza por múltiples jurisdicciones que han propuesto leyes y reglamentos para exigir la divulgación alineada con las recomendaciones del TCFD, algunas de las cuales entrarán en vigor a partir de 2022 (TCFD, 2021). Los partidarios de TCFD ahora abarcan 89 países y jurisdicciones y casi todos los sectores de la economía, con una capitalización de mercado combinada de más de $25 billones, y un aumento del 99 % desde el año 2020 (TCFD, 2021).

A continuación se presentan las características generales de la divulgación de riesgos en diferentes áreas geográficas y sectorial. Concretamente, en Estados Unidos, en la Unión Europea, en el contexto del Acuerdo de Basilea (para el sector financiero) y en América Latina.

### 2.2.1. Estados Unidos

El primer intento importante para satisfacer la demanda de mayores divulgaciones de riesgo en EE.UU. fue la modificación, en 1980, de las reglas de SEC, al incluir revelaciones relacionadas con una discusión y análisis de gestión (MD&A) en el informe anual. Las reglas de MD&A incluyen un requisito para describir tendencias conocidas o incertidumbres que la compañía espera razonablemente que tendrán un impacto material favorable o desfavorable en las ventas netas o los ingresos de las operaciones continuas, y requisitos similares en relación con el capital y la liquidez. Se trata, en cierta medida, de los riesgos a los que se enfrenta la empresa (ICAWE, 2011).

Posteriormente, en 1990, la demanda de información sobre el comportamiento de instrumentos financieros, especialmente derivados, propició la exigencia de requisitos de divulgación, SFAS 119 Divulgaciones sobre instrumentos financieros derivados y valor razonable de instrumentos financieros (FASB, 1994); SFAS 133 Contabilidad de instrumentos derivados y actividades de cobertura (FASB, 1998) y FRR 48 Divulgación de políticas contables para instrumentos financieros derivados (SEC, 1997).

Por su parte, la regulación SK para empresas cotizadas establece los requisitos de informes para algunas presentaciones a SEC, generalmente descripciones cualitativas utilizadas por las empresas públicas. A partir de 2005, la Comisión de Bolsa y Valores (SEC) ordenó a las empresas que incluyeran una sección de ´factor de riesgo´ en su Formulario 10-K para discutir los factores más importantes que hacen que la empresa sea especulativa o riesgosa (Campbell et al., 2014). El artículo 503(c) de la Regulación S-K solicita a un emisor en el ítem 105 (SEC, 2017): proveer bajo el título 'factores de riesgo' una presentación de los factores materiales que hacen que una inversión del emisor sea especulativa o riesgosa. Esta discusión debe organizarse lógicamente con encabezados relevantes y cada factor de riesgo debe establecerse bajo un subtítulo que describa adecuadamente el riesgo. Se solicita explicación concisa sobre cómo cada riesgo afecta al emisor o los valores que se ofrecen. El solicitante de registro debe proporcionar esta información en un lenguaje sencillo.

Además de ser obligatorio por la Comisión de Bolsa y Valores (SEC), los factores de riesgo son importantes en Estados Unidos por razones de protección de responsabilidad (Gelfond et al., 2017). ´Si un inversor pierde dinero en una inversión, pero se le advierte adecuadamente sobre los riesgos potenciales, un tribunal puede, en ciertas circunstancias, fallar a favor de la empresa demandada, incluso si el precio de las acciones cae drásticamente. Las leyes de valores en EE.UU. brindan un puerto seguro para declaraciones si la empresa ha establecido la divulgación adecuada con respecto a los riesgos e incertidumbres´.

A la vez que las empresas reguladas por SEC divulgan temas materiales que afecten la información financiera (MD&A) y las revelaciones sobre factores de riesgo, según el artículo 503(c) de la Regulación S-K, a partir de la sección 404 de la Ley Sarbanes Oxley de 2002, les corresponde incluir en sus informes anuales "una evaluación... de la eficacia de [su] estructura y procedimientos de control interno... para la información financiera". Dado que los controles y procedimientos que subyacen al sistema de información financiera de una empresa son componentes importantes de sus controles generales, estas revelaciones son potencialmente útiles para evaluar los riesgos de una empresa y/o sus procedimientos de mitigación.

### 2.2.2. Unión Europea

A partir de la Directiva 2014/95 de la Unión Europea del Parlamento Europeo y del Consejo de la Unión Europea, se establecen determinados requisitos legales mínimos acerca del alcance de la información que las empresas deben poner a disposición del público y de las autoridades en la Unión. Las empresas sujetas a esta Directiva deben ofrecer una imagen fiel y completa de sus políticas, resultados y riesgos (EU, 2014). Según el artículo 19 numeral 1 literal d) sobre el contenido del informe no financiero, a éste le corresponde incluir "d) los principales riesgos relacionados a las actividades de la empresa, entre ellas, cuando sea pertinente y proporcionado, sus relaciones comerciales, productos o servicios que puedan tener efectos negativos en esos ámbitos y cómo la empresa gestiona dichos riesgos (EU, 2014).

Por su parte, el Código de Gobierno Corporativo del Reino Unido de 2018, emitido por el *Financial Reporting Council (FRC),* establece explícitamente que los directores y las empresas necesitan construir y mantener relaciones exitosas con una amplia gama de grupos de interés en un lenguaje que refleje el del Marco del Consejo Internacional de Informes Integrados (IIRC). El nuevo Código también hace un llamado a los directores para que describan en su informe anual cómo se han considerado los intereses de una amplia comunidad de partes interesadas como se establece en la sección 172 de la Ley de Sociedades en las discusiones de la Junta y en la toma de decisiones. Respecto a la rendición de cuentas sobre gestión de riesgos y control interno, el Consejo de administración será responsable de determinar la naturaleza y alcance de los principales riesgos que desee asumir para lograr sus objetivos estratégicos. Deberá mantener sólidos sistemas de control interno y de gestión de riesgos.

### 2.2.3. Acuerdo de Basilea III

El Acuerdo de Basilea se ha desarrollado en respuesta a la crisis financiera de 2008. El objetivo de dichas medidas es reforzar la regulación, la supervisión y la gestión del riesgo de los bancos. Respecto a la divulgación, el Comité de Normas de Supervisión Bancaria de Basilea (Committee Basel, 2015) expone cómo proporcionar a los mercados información significativa sobre medidas comunes de los principales riesgos es fundamental para la solidez del sistema bancario, ya que reduce la asimetría de la información y promueve la comparabilidad de los perfiles de riesgo de los bancos, dentro de una misma jurisdicción y entre jurisdicciones. Los bancos deben identificar, divulgar y gestionar sistemáticamente los riesgos Ambientales, Sociales y de Gobernanza en el marco de su gestión de riesgos, por ejemplo, con pruebas de resistencia al cambio climático periódicas, tanto por parte de los supervisores como de los bancos.

### 2.2.4. América Latina

En América Latina, en la mayoría de los casos de forma voluntaria, las empresas cotizadas, tomando como referencia los principios generales de Gobierno Corporativo de OCDE y G20 (2016), revelarán, como mínimo: "… la información relevante sobre los factores de riesgo previsibles. Los usuarios de información financiera y los agentes del mercado precisan de datos sobre riesgos materiales que resulten razonables de prever, entre los que se encuentran los siguientes: los riesgos específicos del sector o de las zonas geográficas en las que la empresa desarrolla su actividad; la dependencia de productos básicos; los riesgos de los mercados financieros, incluidos los vinculados a los tipos de interés o las divisas; el asociado a los instrumentos derivados y las operaciones fuera de balance; los que se desprenden de las prácticas empresariales; y los relacionados con el medio ambiente.

En estos Principios se propone difundir información suficiente y lo bastante exhaustiva como para informar completamente a los inversores sobre los riesgos materiales y previsibles que afectan a la empresa.

La divulgación sobre los riesgos adquiere su mayor eficacia cuando se ajusta a la empresa concreta y al sector en cuestión. La divulgación de información sobre el sistema de seguimiento y gestión del riesgo está ganando aceptación como buena práctica".

## 2.3. La divulgación de información corporativa sobre riesgos de Ciberseguridad

Una vez examinadas las generalidades del riesgo de Ciberseguridad, y presentadas las características de la divulgación de información corporativa sobre riesgos en general, nos centramos en este epígrafe en el proceso de divulgación de información corporativa sobre riesgos de Ciberseguridad por parte de las empresas en el ámbito internacional.

El primer paso en la evolución de las prácticas de presentación de informes ha sido la generación de reportes financieros, seguido de iniciativas voluntarias para informar sobre el desempeño no financiero (Rivera et al., 2017), de ahí que ésta sea necesaria para

permitir que las condiciones de la rendición de cuentas sea democrática en un entorno incierto (Bebbington & Larrinaga-González, 2008). Con la difusión casi instantánea de datos en la era moderna, las políticas relativas a la divulgación de información sensible se han convertido en el foco de importantes debates en varios contextos (Mitra & Ransbotham, 2015).

La evidencia muestra sólidos argumentos sobre cómo los inversores también consideran útil la información no financiera en sus decisiones (Amir & Lev, 1996). No obstante, la divulgación se ha ampliado para satisfacer las necesidades, no solo de los accionistas y acreedores, sino también de las partes interesadas, incluidos los clientes, proveedores, gobierno y público en general (Kiliç et al., 2015) para rendir cuentas ante ellos (Solomon, 2019). A partir de estas necesidades, la literatura reciente presenta avances en torno a la divulgación de información relacionada con Ciberseguridad como una parte importante de la información no financiera (Amir et al., 2018; Berkman et al., 2018; Ettredge et al., 2018; Gao et al., 2020; Gordon et al., 2006; Gordon et al., 2010; Héroux & Fortin, 2020a; Radu & Smaili, 2021a; Wang, et al., 2013). A su vez, Gordon et al. (2006) también afirman que las empresas han aumentado sus divulgaciones voluntarias sobre seguridad de la información, a partir de requerimientos y exigencias cada vez mayores de aquellas partes interesadas.

La justificación sobre revelaciones relacionadas con Ciberseguridad está dada en parte por la presencia latente de estos riesgos en el mundo corporativo y las connotaciones económicas que representan. En efecto, los inversionistas reclaman más información sobre los riesgos de Ciberseguridad y las violaciones de datos, y cómo las empresas están abordando esos riesgos (Amir et al., 2018). La Ciberseguridad se encuentra en la intersección de las preocupaciones de seguridad pública sobre la protección de la infraestructura crítica y la seguridad privada en torno a la protección de los derechos de propiedad y las libertades civiles (McCarthy, 2018). Estos son motivos suficientes para considerar que la seguridad cibernética es un tema candente para los stakeholders, especialmente actores del Gobierno Corporativo, reguladores financieros y emisores de estándares contables profesionales en general.

Frente a la presión de múltiples partes interesadas, las empresas están implementando medidas para combatir las crecientes amenazas a la Ciberseguridad (Berkman et al., 2018). Según el Informe de Riesgos Globales 2021, los ciberataques están en aumento y son riesgos de alta probabilidad e impacto (WEF, 2021c). Dada la frecuencia, magnitud y costo de los problemas de seguridad cibernética, es fundamental que las empresas cotizantes tomen todas las medidas necesarias para informar a los inversores sobre riesgos e incidentes de seguridad cibernética de manera oportuna (SEC, 2018a).

Con los ciberataques a la orden del día y en constante evolución, es solo cuestión de tiempo que los esfuerzos para la gestión de riesgos de Ciberseguridad de una empresa y los controles relacionados, así como el Gobierno Corporativo, estén expuestos al escrutinio regulatorio (Holland & Knight, 2021). Por ello, es la SEC quien anuncia sanciones por controles y procedimientos de divulgación deficientes relacionados a los riesgos de Ciberseguridad por parte de las empresas públicas (Holland & Knight, 2021).

Estudios anteriores atribuyen el avance de la divulgación sobre Ciberseguridad a reguladores financieros (CSA ACVM, 2019; Division of Corporation Finance & SEC, 2011; SEC 2018), grandes firmas de contabilidad y auditoría (PWC, 2018b; EY, 2018), organismos profesionales (AICPA, 2017a) y las reglas del mercado (Amir et al., 2018; Berkman et al., 2018). Aun así, a pesar de los incentivos dados por reguladores financieros y las sugerencias de las partes interesadas contables, la divulgación sobre seguridad cibernética muestra que la información reportada parece ser insuficiente (Héroux & Fortin, 2020b).

Según Eijkelenboom & Nieuwesteeg (2021), estas revelaciones en informes anuales presentan beneficios sociales para los actores que tienen una relación directa con la empresa (inversionistas, acreedores) e indirecta con el desarrollo de conocimiento sobre la naturaleza del riesgo de Ciberseguridad y el retorno de la inversión. Las empresas varían ampliamente en la cantidad de detalles que brindan y, a menudo, la información no es específica de la empresa, y las variaciones entre los sectores industriales involucran

las categorías relacionadas con el riesgo de Ciberseguridad, la mitigación del riesgo cibernético y otros elementos (Héroux & Fortin, 2020a).

Bajo el contexto descrito, se observa la importancia de divulgar información en Ciberseguridad, dadas las repercusiones reales y potenciales del riesgo cibernético en todo tipo de organizaciones, impacto que ha sido objeto de estudio en las dos últimas décadas. La investigación empírica previa sugiere que el nivel de divulgación sobre riesgo cibernético en los mercados estadounidenses es el más alto del mundo (Hilary et al., 2016). No obstante, según Héroux & Fortin, (2020) solo un número limitado de investigaciones han analizado la divulgación de Ciberseguridad y, en general, los niveles de revelación sobre el tema son bajos. Esto indica que las prácticas de divulgación de seguridad cibernética aún están en desarrollo.

Dado que el riesgo cibernético es una de las principales preocupaciones de las organizaciones, la gobernanza y los líderes empresariales, la divulgación de la seguridad cibernética es un tema corporativo importante (Radu & Smaili, 2021). A este tipo de revelaciones corporativas se les atribuyen algunas ventajas y desventajas que relacionamos a continuación.

**Ventajas de la divulgación de información sobre Ciberseguridad:**

- Según Gao et al. (2020), la divulgación de los riesgos de seguridad cibernética que enfrentan las empresas, y cómo se gestionan, se vuelve cada vez más importante y favorece a los inversores, gobiernos, consumidores, proveedores y otras partes interesadas, para hacer juicios informados sobre las implicaciones financieras, reputacionales y legales de los ataques cibernéticos de alto perfil.

- El mercado valora positivamente la conciencia de seguridad cibernética (Berkman et al., 2018), los organismos del mercado financiero se esfuerzan por mejorar la responsabilidad empresarial y la rendición de cuentas en relación con los ataques cibernéticos y, en última instancia, proteger a los inversores y al mercado

financiero (Radu & Smaili, 2021). Las empresas que divulgan voluntariamente elementos relacionados con la seguridad de la información tienen valoraciones de mercado más altas por parte de los inversores (Gordon et al., 2010).

- Las empresas divulgan a las partes interesadas sobre las siguientes áreas, al evaluar los riesgos de Ciberseguridad y los incidentes de Ciberseguridad (SEC, 2018): 1) la ocurrencia de incidentes cibernéticos; 2) la probabilidad de posibles incidentes cibernéticos; 3) las acciones preventivas para reducir los riesgos de Ciberseguridad; 4) los riesgos de Ciberseguridad de la naturaleza de los negocios u operaciones de las empresas; 5) los costos de mantener los riesgos de seguridad cibernética, como la cobertura de seguros; 6) el daño reputacional; 7) los costos relacionados con la nueva regulación existente o potencial; y 8) los riesgos de litigio.

- La divulgación sobre Ciberseguridad debe revelar información sobre el rol del consejo de administración en la supervisión de los riesgos de Ciberseguridad (SEC, 2018 ). Se espera que la Junta divulgue información importante que sea relevante para los accionistas, incluida información sobre el riesgo cibernético y cómo lo aborda la empresa (Radu & Smaili, 2021).

- Los ataques cibernéticos a menudo no son observables por el público cuando ocurren y, por lo tanto, los gerentes pueden ocultar información sobre los ataques a los inversores sin ser descubiertos. Sin divulgación, los inversores reducirán los precios de las acciones solo por el valor esperado de las malas noticias retenidas, que en el caso de los ataques cibernéticos es igual a la probabilidad de que ocurra un ataque (y el gerente está reteniendo la información) multiplicada por el daño promedio.

**Desventajas de la divulgación de información sobre Ciberseguridad:**

- La revelación completa de incidentes puede acelerar la difusión de los ataques, aumentar la penetración de éstos dentro de la población objetivo e incrementar el riesgo de un primer ataque después de que se informa la vulnerabilidad (Mitra & Ransbotham, 2015).

- Para los ataques cibernéticos que eventualmente se revelan, los datos indican cuándo la empresa se enteró del ataque y, por lo tanto, si se ocultó información. En muchas ocasiones las revelaciones sobre los ataques se realizan después de que los inversores los descubren (Amir et al., 2018).

- No se puede observar el alcance de la retención de información y solo tenemos conocimiento de las violaciones de datos que finalmente revelan las empresas atacadas o fuentes externas a la empresa (Amir et al., 2018).

## 2.4. Tipos de divulgación de información sobre Ciberseguridad

Mencionar la Ciberseguridad tiene claros beneficios y solo un pequeño costo para la organización que la publica en el informe anual (Eijkelenboom & Nieuwesteeg, 2021). Estudios precedentes muestran cómo la divulgación de información se puede dividir en dos categorías: voluntaria y obligatoria (Cheung et al., 2010).

La revelación voluntaria permite la discreción de la gerencia al decidir el contenido a publicar (Cheung et al., 2010). Puede ser información financiera y no financiera la que las empresas no están obligadas a divulgar (Scaltrito, 2016); es decir, revelaciones más allá de lo requerido por la regulación (Gordon et al., 2010).

Entre tanto, la divulgación obligatoria está establecida por estatutos, reglamentos profesionales y requerimientos de cotización de las bolsas de valores (Marston & Shrives,

1991b). Los requisitos legales relacionados tienen como objetivo proteger a los acreedores, inversores y accionistas (Eijkelenboom & Nieuwesteeg, 2021).

**Tabla 3. Estudios sobre efectos de la regulación en la Divulgación de Ciberseguridad**

| Autores | País | Período de Análisis | Variables | Muestra de estudio/ Metodología utilizada |
|---|---|---|---|---|
| (Berkman et al., 2018) | EE.UU. | 2012-2016 | Dependiente<br>El precio de las acciones<br><br>Independiente<br>Medida de seguridad de la información. | Muestra<br>3,084 firmas Russell 3000.<br><br>Metodología<br>Metodología de mapeo de dominios y enfoque general para identificar, categorizar y clasificar las divulgaciones de Ciberseguridad |
| (Li et al., 2018) | EE.UU. | 2007-2015 | Dependiente<br>Incumplimientos<br>Independiente<br>Tamaño, LN segmentos, edad perdidas, LN analistas, extranjero, fusión, crecimiento, ICW, Consumidor, guía, puntaje, unicidad.<br>Control<br>Divulgación anterior | Muestra<br>26.626 observaciones<br><br>Metodología<br>Modelo logístico y panel<br><br>Divulgación voluntaria 2007- 2011; Divulgación obligatoria 2012-2015 Guía SEC 2011. |
| (Morse et al., 2018) | EE.UU | 12 meses antes y después de 13 octubre 2011 | No presenta | Muestra<br>167 observaciones 10K, 37 empresas que cotizan en la bolsa.<br>Metodología<br>Estudio de eventos<br><br>SEC 2011 obligatorio / voluntario |

Estudios relacionados han buscado evidenciar los efectos de la promulgación de la Guía SEC 2011, es decir, analizan los cambios de la divulgación cuando pasa de ser voluntaria a obligatoria (Berkman et al., 2018; Li et al., 2018a; Morse et al., 2018). Berkman et al. (2018) comprueban cómo el aumento de la divulgación se debe en gran medida a la Guía SEC 2011, la cual proporciona orientación para la divulgación de cuestiones relacionadas

con el ciberespacio en las presentaciones 10-K. Con base en esta divulgación posterior a la orientación, el autor desarrolla una nueva medida que captura el alcance y la relevancia de las divulgaciones cibernéticas, y muestra que el mercado valora positivamente la conciencia de la seguridad cibernética. Li et al. (2018) encuentran que, en el período previo a la orientación de la Guía SEC 2011, la divulgación de riesgos de Ciberseguridad se asocia positivamente con incidentes cibernéticos posteriores y, después de la Guía, esta percepción cambia porque la divulgación se amplía para las empresas que no tienen riesgos materiales de Ciberseguridad. Por su parte, Morse et al. (2018) analizan un año antes y uno después de la emisión de la Guía SEC 2011, y encuentran que la mayoría de las empresas eligen no revelar ningún riesgo de Ciberseguridad y que tan solo una proporción relativamente pequeña eligió modificar sus divulgaciones de factores de riesgo.

### 2.4.1. Divulgación voluntaria de información de Ciberseguridad

Las divulgaciones voluntarias en el informe anual sobre seguridad de la información permiten que una corporación participe activamente en la prevención, detección y corrección de las brechas de seguridad (Gordon et al., 2010; Verrecchia, 1983). Se podría suponer que los gerentes deben tomar una decisión estratégica en cuanto a la presentación de divulgaciones voluntarias de seguridad de la información y su relación con los beneficios netos en términos del valor de mercado de sus empresas (Gordon et al., 2010). Las revelaciones voluntarias relativas a la seguridad de la información también podrían servir para mitigar los costos potenciales del litigio debido a la reducción de la responsabilidad derivada de la mayor transparencia asociada con la revelación (Kasznik & Lev, 1995; Skinner, 1997). Sin embargo, debe tenerse en cuenta que puede existir un sesgo en los informes voluntarios para que las empresas informen solo de los éxitos, o para "disfrazar la ventana" o encubrir la mala conducta corporativa (Wang & Tuttle, 2014).

En el contexto estadounidense, en un primer momento la divulgación sobre información de Ciberseguridad se realizó de forma voluntaria. Gordon et al. (2010) desarrollaron un

instrumento que capturaba la existencia de revelaciones voluntarias en el formulario 10 K relacionadas con la "seguridad de la información", y expusieron una asociación positiva, al igual que entre la valoración del mercado y su instrumento de medida. Su período de muestra es anterior tanto a los requisitos de la SEC para la presentación de informes obligatorios de riesgos (que ocurrió en 2005), como a la guía complementaria de 2011 de la SEC sobre divulgaciones de seguridad cibernética (Berkman et al., 2018).

Respecto a la Ley Sarbanes Oxley, se puede expresar que no aborda explícitamente el tema de la seguridad de la información. No obstante, Gordon et al. (2006) proporcionan evidencia empírica de que SOX está teniendo un impacto significativo en la divulgación voluntaria de las actividades de seguridad de la información de las empresas.

En relación con la divulgación voluntaria sobre ciberataques, la fuente de información sobre estas vulnerabilidades, en la mayoría de los estudios, es la propia empresa. Amir et al. (2018), utilizando datos sobre ataques cibernéticos revelados voluntariamente y aquellos que fueron retenidos y luego descubiertos por fuentes externas, estiman hasta qué punto las compañías retienen información sobre ciberataques y su asociación con una disminución en los valores de las acciones en el mes en que se descubre el ataque. Los hallazgos de Baginski et al. (2018) respaldan la evidencia teórica previa de que los gerentes retrasan la divulgación de malas noticias debido a preocupaciones profesionales, y sugieren un mecanismo a través del cual las empresas pueden mitigar el retraso. Finalmente, la divulgación voluntaria sobre la seguridad de la información puede reducir el costo de la empresa al disminuir la asimetría de la información entre la dirección y sus inversores (Verrecchia, 1983).

Recientemente, en el ámbito mundial, otro factor que ha generado un aumento importante en la divulgación voluntaria sobre información de Ciberseguridad en las empresas cotizantes ha sido la entrada en vigencia del Reglamento General de Protección de Datos de la Unión Europea (Gao et al., 2020). El Reglamento General de Protección de Datos de la Unión Europea establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales, y se aplica tanto a las

organizaciones europeas que tratan datos personales de ciudadanos en la UE como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE (EU, 2016). Es de anotar que las empresas tienen la opción de divulgar parte de esta información en el ítem GRI 418-1, “Privacidad del cliente”.

Los gobiernos de Canadá y Estados Unidos han alentado la divulgación relacionada con el riesgo, razón por la cual se presenta una tendencia ascendente a incluir riesgos de tipo cibernético en los informes anuales (Radu & Smaili, 2021). Sin embargo, a pesar de la ventaja de esta información, que señala información nueva y valiosa para los inversores, hay un aspecto negativo: revelar información interna crítica que los piratas informáticos y los ciberdelincuentes podrían utilizar para atacar la empresa (Li et al., 2018; Wang & Hsu, 2013).

Atendiendo a la literatura previa, en la Tabla 4 se resumen las investigaciones relacionadas con la divulgación de información sobre Ciberseguridad. En un primer renglón, Gordon et al. (2006) demuestran que la divulgación aumenta de forma voluntaria debido a los lineamientos de la Ley Sarbanes Oxley 2002. Seguidamente, Gordon et al. (2010) verifican la relación positiva existente entre el precio de las acciones y la medida o índice de divulgación que han construido. Por su parte, Ettredge et al (2018) estudian la asociación entre las divulgaciones de las empresas en el Formulario 10-K sobre la existencia de información de propiedad corporativa, a saber, secretos comerciales y robo cibernético, y concluyen que las empresas que mencionan la existencia de secretos comerciales tienen una probabilidad posterior significativamente mayor de ser violadas en relación con las empresas que no lo hacen. Finalmente, Eijkelenboom & Nieuwesteeg, (2021) estudian 75 informes anuales de empresas cotizadas en Países Bajos buscando establecer la relación de la revelación de información sobre Ciberseguridad con la regulación financiera vigente, y concluyen que no hay ningún requisito en derecho financiero que induzca a las empresas que cotizan en bolsa a revelar cualquier información sobre Ciberseguridad; por lo tanto, la información revelada se ha presentado de forma voluntaria en los reportes anuales.

**Tabla 4. Estudios previos relacionados con la divulgación de información voluntaria**

| Autores | País | Período de análisis | Variables estadísticas | Muestra de estudio/ Metodología utilizada |
|---|---|---|---|---|
| (Gordon et al., 2006) | Estados Unidos | 2000-2004 | Dependiente<br>- Divulgación de información.<br>Independiente<br>- SOX. | **Muestra:**<br>27.253 informes.<br>**Metodología:**<br>Análisis de contenido (palabras clave).<br>Prueba de contingencia<br>Proporciones de dos muestras. |
| (Gordon et al., 2010) | Estados Unidos | 2000-2004 | Dependiente<br>- El precio de las acciones de la empresa;<br>Independiente<br>- Medida de seguridad de la información; divulgación voluntaria, | **Muestra**<br>1.641 informes<br>**Metodología**<br>Modelo de relevancia de valor de mercado, así como en un análisis de diferenciales de oferta y demanda. |
| (Ettredge et al., 2018) | Estados Unidos | 2007-2015 | Dependiente<br>Incumplimiento, secreto comercial, índice de secretos comerciales.<br><br>Independiente<br>Defensa Cibernética, vulnerabilidad cibernética, tamaño, complejidad, riesgo de la empresa en la investigación de auditoria.<br>Control<br>Defensa cibernética, vulnerabilidad cibernética, tamaño, complejidad, riesgo de la empresa en la investigación de auditoria, edad de la empresa, ROA, perdida, BIG4, LN N. total de palabras 10K, legibilidad del texto 10K, industria minorista, industria financiera, gasto I+D, LN tarifa de auditoria, activos a largo plazo, SEC Letters on Cyber Defense y SEC Letters on Cyber Vulnerability, número de analistas. | **Muestra:**<br>Violación de datos: 591 incidentes cibernéticos; que representan 511 observaciones de años firma atacadas de 318 firmas atacadas; cumplimiento 39992 observaciones de años firmes (7462 firmas únicas)<br>**Metodología:**<br>Regresión logística multivariante.<br>**Teoría:**<br>No describe teoría |

| | | | | |
|---|---|---|---|---|
| (Eijkelenboom & Nieuwesteeg, 2021) | Países Bajos | 2018 | Dependiente<br>El precio de las acciones de la empresa.<br>Independiente<br>Medida de seguridad de la información. | **Muestra**<br>75 empresas Bolsas de los países bajo - índices AEX, AMX, AScX<br>**Metodología**<br>Investigación empírico-exploratoria.<br>Violación de datos: 591 incidentes cibernéticos; que representan 511 observaciones de años firma atacadas de 318 firmas atacadas; cumplimiento 39992 observaciones de años firmes (7462 firmas únicas). |

### 2.4.2. Divulgación de información obligatoria en Ciberseguridad

Normalmente, la divulgación de información relacionada con Ciberseguridad en el ámbito mundial se realiza de manera voluntaria. No obstante, en el contexto estadounidense, y desde el panorama bursátil internacional que éste enmarca, las divulgaciones de la Sección 1A ante la SEC se ordenaron en 2005 a través del Artículo 503 (c) del Reglamento SK (SEC, 2005) por el que las empresas deben divulgar y describir sus factores de riesgo específicos. Esto sugiere que los reguladores creen que los inversores se benefician de las divulgaciones sobre riesgos e incertidumbres de la empresa (Campbell et al., 2014). Según la Division of Corporation Finance & SEC (2011), si bien las empresas están obligadas a divulgar todos los riesgos materiales, esta guía no abordó explícitamente la divulgación de los riesgos e incidentes cibernéticos. Aun así, de acuerdo con Li et al. (2018), la divulgación de riesgos de Ciberseguridad ha recibido gran atención en los últimos años, especialmente después de la aprobación de la Guía de Divulgación de Ciberseguridad de la Securities and Exchange Commission (SEC) publicada el 13 de octubre de 2011.

Estudios previos informan el debate en torno a los niveles de divulgación de riesgos cibernéticos. Por ejemplo, la divulgación deficiente del riesgo cibernético tiene un efecto limitado en los precios de las acciones (Hilary et al., 2016), pero la divulgación excesiva

puede ser contraproducente (Héroux & Fortin, 2020a). Según Campbell et al. (2014), Hope et al. (2016) y Li et al. (2018), la divulgación de riesgos de Ciberseguridad es más informativa que la repetición, ya que es útil para los participantes del mercado al evaluar la probabilidad de futuros incidentes cibernéticos.

Dado que los incidentes cibernéticos pueden tener impactos negativos en las organizaciones, mejorar la divulgación de sucesos de seguridad cibernética podría ser útil para varias partes interesadas (Héroux & Fortin, 2020a). Sin embargo, la divulgación completa acelera la difusión de los ataques, aumenta la penetración de los mismos dentro de la población objetivo e incrementa el riesgo de un primer ataque después de que se informa la vulnerabilidad (Mitra & Ransbotham, 2015).

Según IOSCO (2016), la divulgación de los riesgos materiales debe adaptarse a las circunstancias del emisor individual y proporcionar suficientes detalles para describir la naturaleza y consecuencias de un riesgo particular, o de un ciberataque previo, logrando el equilibrio adecuado sin revelar información que pudiera comprometer la seguridad cibernética. Como principio general, la divulgación debe centrarse en la información material y específica de la entidad, y evitar el lenguaje repetitivo (CSA, 2017).

En el período 2011-2015, la SEC pasó de fomentar la divulgación de Ciberseguridad a enviar cartas de comentarios solicitando información sobre incidentes cibernéticos y seguridad de la información. A raíz de las orientaciones de la SEC y estas cartas de comentarios, las empresas incluyen cada vez más discusiones generales sobre riesgos de Ciberseguridad en sus divulgaciones de riesgos corporativos (Schubert, 2015). Así, esta primera guía proporciona los lineamientos para la revelación de cuestiones relacionadas con el ciberespacio en el Formulario 10-K (Berkman et al., 2018; Gordon et al., 2015). Sin embargo, según Amir et al. (2018), si los reguladores desean garantizar que la información sobre los ataques cibernéticos llegue a los inversores, deberían considerar la imposición de reglas de divulgación obligatoria más estrictas con respecto a los ataques cibernéticos y umbrales de materialidad más claros.

En 2014, siguiendo la guía de divulgación de 2011, la SEC organizó una mesa redonda para discutir cuestiones prácticas relacionadas con Ciberseguridad, incluida la eficacia de la divulgación. PCAOB (2014) discute cuestiones de Ciberseguridad y las posibles implicaciones para la presentación de informes financieros y revisión de cuentas. Algunos participantes anotaron que muchas de las divulgaciones actuales en los archivos de la SEC son de naturaleza 'repetitiva' y repiten casi literalmente las palabras de la guía del personal de la SEC, mientras que otros expresaron cautela de que proporcionar información específicamente adaptada podría aumentar la vulnerabilidad de una empresa porque dicha información podría incluir detalles que ayudarían a los atacantes a infiltrarse en la empresa (Héroux & Fortin, 2020b).

En febrero de 2018, la SEC aprueba la segunda guía interpretativa sobre divulgación de riesgos de Ciberseguridad y enfatiza la importancia de controles y procedimientos de divulgación suficientes y de la prohibición del uso de la información privilegiada no pública de incidentes cibernéticos (Gao et al., 2020). Según la División de Finanzas Corporativas de SEC (2011) y SEC (2018), al igual que con otros riesgos operativos y financieros, los solicitantes de registro deben revisar, de manera continua, la idoneidad de su divulgación en relación con los riesgos de Ciberseguridad y los incidentes cibernéticos.

La guía actualizada agrega dos consideraciones específicas (PWC, 2018c): (1) políticas y controles establecidos para detectar y divulgar riesgos e incidentes de seguridad cibernética importantes y, (2) políticas para evitar que los empleados negocien con información no pública sobre riesgos e incidentes de seguridad cibernética. Según Gao et al. (2020), aunque la Guía de 2018 fue aprobada por unanimidad de los comisionados de la SEC, algunos sintieron que la nueva guía no fue lo suficientemente lejos. Además de revelar los riesgos de posibles ataques cibernéticos, las empresas deben divulgar los incidentes cibernéticos materiales conocidos que ya ocurrieron y discutir los costos y consecuencias potenciales (Gao et al., 2020). Según Bakker (2015), informar sobre las consecuencias de un incidente de Ciberseguridad y la gestión de los riesgos de

Ciberseguridad (incluida la identificación y evaluación de dichos riesgos y la responsabilidad relacionada) es de interés para las partes interesadas.

La nueva guía SEC (2018) recomienda que en este aparte del informe se incluyan las divulgaciones sobre riesgos e incidentes de Ciberseguridad en el artículo 3. D del Formulario 20-F. Esta medida va dirigida para todos los ´emisores privados extranjeros´ con acciones de capital inscritas en las bolsas de Estados Unidos, por lo que podemos decir que ésta es una exigencia con repercusiones en el contexto internacional. Pasados tres años de la emisión de la Guía (SEC, 2018b), la Comisión de Bolsa y Valores de Estados Unidos ha pasado de la orientación a la aplicación, aumentando los riesgos en los casos en que las empresas públicas no implementan sistemas sólidos de gestión de riesgos de Ciberseguridad y procedimientos de divulgación relacionados (Holland & Knight, 2021).

Ahora bien, en el contexto canadiense, siguiendo los pasos de la SEC, el Administrador de Valores Canadiense (CSA), en 2013, enfatizó la importancia de los riesgos cibernéticos y de implementar medidas de seguridad cibernética para proteger a los emisores y sus partes interesadas (CSA, 2013a ). La CSA proporcionó a los emisores referencias relacionadas con los estándares y publicaciones existentes (CSA, 2016 ), junto con conocimientos sobre el desarrollo de guías sobre prácticas de Ciberseguridad y redes sociales (CSA, 2017a;.Héroux & Fortin, 2020a).

Algunos estudios analizan la divulgación de información reportada ante la SEC, a partir de requisitos establecidos. Concretamente, Berkman et al. (2018) y Wang, et al. (2013) demuestran que existen diferentes percepciones entre los inversores con respecto al impacto de los incidentes de seguridad dependiendo de la naturaleza de la divulgación, y presentan esbozos de cómo los participantes del mercado pueden interpretar mejor los factores de riesgo de seguridad revelados. Por su parte, Li et al. (2018) examinan la utilidad de los factores de riesgo relacionados con la Ciberseguridad divulgados en las presentaciones 10 K, y documentan que la presencia de estos factores en el período previo a la orientación SEC están relacionados con futuros incidentes informados de

Ciberseguridad; sus hallazgos, en general, respaldan la decisión de la SEC de enfatizar la divulgación de riesgos de Ciberseguridad.

Según IRRC (2016), la divulgación sobre los factores de riesgo representan el 7% de la extensión promedio de una presentación 10-K por recuento de páginas. De acuerdo con Gao et al. (2020), los dos riesgos de Ciberseguridad que se revelan con mayor frecuencia por parte de las empresas cotizantes son los relacionados con la interrupción del servicio y la pérdida de datos confidenciales. Asimismo, el artículo 1A del Informe 10 K es el lugar más utilizado para la divulgación; sin embargo, algunas empresas también emplean los artículos 1 y 7 para revelar los riesgos de regulación y los incidentes cibernéticos, respectivamente.

Otras investigaciones sobre divulgaciones de Ciberseguridad evalúan las condiciones bajo las cuales los incentivos/regulaciones del gobierno federal de EEUU, como la Ley Sarbanes-Oxley de 2002 y la Ley de 2011, la Guía de divulgación de la SEC sobre riesgos e incidentes de Ciberseguridad, conducen a un aumento en las inversiones en seguridad cibernética y, a su vez, a una mayor divulgación de dicha información (Gordon et al., 2015b). Hilary et al. (2016), a partir de un análisis cualitativo de cinco casos corporativos de violaciones de datos en EE.UU. y de un examen sistemático posterior a la divulgación del riesgo cibernético, determinan una reacción muy limitada en los precios de las acciones asociadas con una divulgación repetitiva y no específica del riesgo cibernético.

Recientemente, Héroux & Fortin (2020) examinan si el contenido de las divulgaciones de seguridad cibernética de las empresas canadienses inscritas en el índice S&P/TSX 60 está alineado con las mejores prácticas, a partir de un índice autoconstruido con 40 elementos. Concluyen que los niveles de Divulgación de Ciberseguridad son bajos, y sugieren que los reguladores financieros podrían emitir requisitos más estrictos. Gao et al. (2020) concluyen que, si bien los riesgos de Ciberseguridad son importantes y podrían afectar materialmente las operaciones comerciales y la integridad de los informes financieros, existe una investigación empírica limitada sobre las tendencias y prácticas de divulgación de riesgos de Ciberseguridad de las empresas públicas. En consecuencia, los reguladores

financieros han publicado pautas de divulgación de seguridad cibernética para informar a las partes interesadas sobre la naturaleza y la gestión de los riesgos cibernéticos, el impacto de los ataques cibernéticos y la forma de informar sobre estos problemas (Héroux & Fortin, 2020a).

La naturaleza cualitativa de las divulgaciones de riesgos facilita que los gerentes sean estratégicos en sus divulgaciones. Dados los riesgos sustanciales asociados con la divulgación de vulnerabilidades, consideramos que las divulgaciones relacionadas con la Ciberseguridad están relacionadas con la conciencia de seguridad cibernética de la empresa (Berkman et al., 2018). Considerando que las empresas solo están obligadas a proporcionar descripciones cualitativas y no necesitan cuantificar la probabilidad o el impacto de los riesgos revelados, tienen un gran grado de discreción sobre qué revelar y cómo hacerlo (Li et al., 2018).

Puesto que los incidentes cibernéticos pueden tener impactos negativos en las organizaciones, mejorar la divulgación de incidentes de seguridad cibernética podría ser útil para varias partes interesadas (Héroux & Fortin, 2020a). En términos generales, la literatura relacionada con la divulgación de información de Ciberseguridad se enmarca en su mayoría en el contexto norteamericano (Amir et al., 2018; Hilary et al., 2016; Gordon, et al., 2010; Gao et al., 2020; Berkman et al., 2018; Ettredge et al., 2018; Wang, et al., 2013) y Canadá (Héroux & Fortin, 2020), países que disponen de medidas regulatorias específicas sobre divulgación de Ciberseguridad: SEC (2011; 2018) y CSA ACVM (2013; 2017), respectivamente.

Por otro lado, en el contexto europeo los requisitos de información sobre Ciberseguridad están ausentes en la legislación específica europea (Eijkelenboom & Nieuwesteeg, 2021). Sin embargo, las empresas sujetas a la Directiva (EU, 2014) deberán ofrecer una imagen fiel y completa de sus políticas, resultados y riegos, y facilitar información adecuada sobre aquellos aspectos sobre los que existen más probabilidades de que se materialicen los principales riesgos de efectos graves, junto con los tópicos respecto de los que dichos riesgos ya se han materializado (EU, 2014). En este sentido, podemos afirmar que en

algunas circunstancias, por las connotaciones que involucra el riesgo cibernético, esta información relacionada se debe estar divulgando, así como los incidentes cibernéticos ya materializados.

Del panorama europeo también se puede afirmar que, aunque existe la divulgación obligatoria de incidentes de Ciberseguridad de acuerdo con la Ley de Ciberseguridad y Privacidad, el Reglamento General de Protección de Datos y la Directiva sobre Seguridad de Redes y Sistemas de Información, estas directrices no exigen específicamente una incorporación de incidentes en el informe financiero anual. Las obligaciones de divulgación de incidentes de datos desde la perspectiva de la Ley de Ciberseguridad podrían proporcionar incentivos para que la Junta también revele información de Ciberseguridad en el informe anual (Eijkelenboom & Nieuwesteeg, 2021). Un incidente de violación de datos debe notificarse al interesado (a menudo, el consumidor) de acuerdo con el artículo 34 del Reglamento General de Protección de Datos.

Por su parte, las empresas de los países de América Latina tampoco refieren una normativa exclusiva para la divulgación de información de Ciberseguridad en el informe anual. No obstante, las diferentes regulaciones expedidas por los entes de vigilancia y control en torno al papel del Gobierno Corporativo se convierten, desde la gestión de riesgos y la privacidad de los datos, en temas objeto de revelación por parte de las organizaciones. En este sentido, las empresas cotizantes de Latinoamérica que participan en el mercado bursátil estadounidense reportarán en el informe anual 20 F ítem 3D los factores de riesgo relacionados con el riesgo cibernético de acuerdo con SEC (2018b).

Atendiendo a la literatura previa, en la Tabla 5 se presentan algunas investigaciones que se han centrado en la divulgación obligatoria de información sobre Ciberseguridad.

Gao et al. (2020), a partir de un análisis longitudinal del contenido y las características lingüísticas de las prácticas de divulgación obligatoria de riesgos de Ciberseguridad de las empresas públicas, encuentran que entre otras razones el aumento de las revelaciones está asociada con la emisión de la Guía de la SEC (2011 y 2018) y que el elemento 1A del Informe 10-K es el lugar de divulgación más utilizado. Héroux & Fortin (2020), examinan el contenido de las divulgaciones de Ciberseguridad obligatorias respecto a las pautas de los reguladores financieros en la materia. Los resultados muestran que los niveles de divulgación de Ciberseguridad son bajos. Las empresas varían mucho en cuanto a la cantidad de detalles que proporcionan y, a menudo, la información no es específica de la empresa. La mayoría de las empresas proporcionaron divulgaciones de seguridad cibernética en el MD&A anual, y varias reiteraron algunos elementos de divulgación en el Informe anual AIF. Leo, (2020) analiza por primera vez las divulgaciones relacionadas con la resiliencia operativa en los informes anuales. Además, para los formuladores de políticas, destaca la disparidad en las divulgaciones en torno a esta área de riesgo relativamente nueva, lo que exige una guía regulatoria adicional. Radu & Smaili (2021) examinan cómo la composición de género de la Junta puede influir en el alcance de la divulgación de Ciberseguridad y muestran evidencia de una asociación positiva entre la presencia y el nivel de divulgación de Ciberseguridad y la diversidad de género en la Junta.

**Tabla 5. Estudios previos relacionados con la divulgación de información obligatoria**

| Autores | País | Período de análisis | Variables | Muestra de estudio/ Metodología utilizada |
|---|---|---|---|---|
| (Gao et al., 2020) | EE.UU | 2007-2018 | Dependiente Cantidad total de palabras utilizadas para revelar riesgos de Ciberseguridad, legibilidad de las divulgaciones de riesgos de Ciberseguridad, lenguaje litigioso utilizado.<br><br>Independiente.Tamaño, rentabilidad, riesgos especifico de Ciberseguridad, cambio de auditor, cambio ejecutivo y ratio de activos | Muestra:<br>112 empresas un total de 1344 observaciones<br>Metodología:<br>Análisis de regresión línea y múltiple<br>Teoría:<br>Teoría de la agencia<br>Toma como variable independiente una dimensión de regulación: SEC: 2011;2018) |

| | | | | |
|---|---|---|---|---|
| | | | intangibles, industria, índice de riesgo; SEC 2011, SEC 2018. | |
| (Héroux & Fortin, 2020a) | Canadá | | No presenta | Muestra: 60 empresas cotizan en el índice S & P / TSX<br>Metodología:<br>Análisis de contenido<br>Teoría:<br>No describe teoría.<br>Obligatorio |
| (Leo, 2020) | Global | 2019 | No presenta | Muestra<br>30 bancos G-SIB<br>Metodología<br>Análisis de frecuencia de términos, evaluación para comprender existencia de relaciones entre estos términos<br>Teoría<br>No describe teoría.<br>Obligatorio |
| (Radu & Smaili, 2021) | Canadá | 2014-2018 | Dependiente<br>Índice de seguridad de la información,<br>Independiente<br>Diversidad de género en Junta Directiva, porcentaje de mujeres, índice Blau de heterogeneidad, masa crítica de mujeres (1 mujer, 2 mujeres, 3 mujeres)<br>Control<br>Tamaño de la empresa, rentabilidad, oportunidades de inversión, apalancamiento, tamaño de la Junta, independencia de la Junta, afiliación de la empresa a la Junta, total de páginas informe anual. | Muestra:<br>300 observaciones<br>Metodología:<br>Modelo de relevancia de valor de mercado, así como en un análisis de diferenciales de oferta y demanda.<br>"modelo de regresión lineal múltiple"<br>Teoría<br>Señalización<br>Obligatoria<br>Canadá comenzó a utilizar canales regulatorios para promover la divulgación de información relacionada con la Ciberseguridad en 2013 |

## 2.5. Informes y comunicaciones utilizados para la divulgación de información sobre Ciberseguridad

El informe anual es un método bien establecido para transferir información (Eijkelenboom & Nieuwesteeg, 2021) y una fuente importante y confiable relacionada con el riesgo para los inversores y otras partes interesadas (Allini et al. 2016). Además, este tipo de reporte contribuye al buen Gobierno Corporativo, porque permite a los inversores hacer uso de los derechos que les corresponden (Chang et al., 1983; Hijink, 2010).

Los grupos de interés exigen transparencia, responsabilidad e información estratégica que conecte el pasado con los riesgos y oportunidades futuras, información generalmente no proporcionada por los informes financieros tradicionales (Rupley et al., 2017). La divulgación sobre las prácticas de RSE cada día gana más espacio en los informes anuales de las empresas, junto a la información de carácter económico-financiero, ya que además de conocer la salud financiera y el desempeño de las empresas, los inversores y las partes interesadas necesitan saber cómo se gestionan (Wuerges & Borba, 2014) y cómo se manejan los riesgos (Allini et al., 2015).

Entre las investigaciones que han centrado sus estudios en la divulgación de información sobre Ciberseguridad en el informe anual, podemos citar a Eijkelenboom & Nieuwesteeg (2021) y Radu & Smaili (2021a). La mención de la Ciberseguridad por parte del consejo de administración o de la Junta Directiva y del consejo de supervisión en el informe anual tiene beneficios en cuanto a su relación con (Eijkelenboom & Nieuwesteeg, 2021): (i) actores del mercado, como información, inversores potenciales, accionistas y acreedores; (ii) actores reguladores, como la autoridad de protección de datos o los centros de Ciberseguridad; y (iii) la organización interna de la empresa.

En la actualidad la preparación de los informes anuales reportados por las organizaciones se efectúa, a partir de algunos estándares de aceptación internacional. A continuación nos referimos brevemente a ellos.

### 2.5.1. Las directrices del Estándar Global Reporting Iniciative (GRI)

Son estándares emitidos por la Junta de Estándares de Sostenibilidad Global (GSSB) promueven las prácticas de informes ambientales y de sostenibilidad. Las organizaciones convergen internacionalmente en torno a sus directrices, a pesar de que Global Reporting Iniciative (GRI) carece de un mandato gubernamental vinculante (Bebbington et al., 2012). Si bien se han propuesto varios estándares al respecto, la mayoría de las empresas utilizan las directrices de (GRI) para redactar sus declaraciones de responsabilidad social empresarial (García-Sánchez et al., 2019). Los aspectos a revelar en el informe de sostenibilidad preparados bajo Estándares GRI 2016 se pueden relacionar en especial con el ítem GRI 418 Privacidad de cliente GRI 418 – 1 "Reclamaciones fundamentadas relativas a violaciones de la privacidad del cliente y pérdida de datos del cliente" (GRI, 2016):

La organización informante debe presentar la siguiente información, respecto a GRI 418-1:

> (a) El número total de reclamaciones fundamentadas relativas a violaciones de la privacidad del cliente, clasificadas por: i. reclamaciones recibidas por terceras partes y corroboradas por la organización; ii. reclamaciones de autoridades regulatorias.
>
> (b) El número total de casos identificados de filtraciones, robos o pérdidas de datos de clientes.
>
> (c) Si la organización no ha identificado ninguna reclamación fundamentada, basta con señalar este hecho en una declaración breve.

Al recopilar la información específica en el Contenido 418-1, la organización informante debe indicar si una cifra significativa de dichas violaciones está relacionada con eventos acontecidos en años anteriores.

### 2.5.2. Los estándares emitidos por el American Sustainability Accounting Standard Board (SASB)

Están diseñados para ayudar a las organizaciones a divulgar información a los inversores sobre la materialidad financiera de aspectos relacionados con sostenibilidad entre las empresas registradas ante la Securities Exchange Commission (SEC) (Rupley et al., 2017). SASB identifican el subconjunto de problemas ambientales, sociales y de gobierno más relevantes para el desempeño financiero en 77 industrias (SASB, 2021a).

Se espera que la información relacionada con Ciberseguridad desde la matriz de materialidad se incorpore en la dimensión de capital social y liderazgo y gobernanza en las siguientes categorías (SASB, 2021b):

En la dimensión de capital social (SASB, 2021b):

> (i) privacidad del cliente, la cual aborda la gestión de riesgos relacionados con el uso de información de identificación personal y otros datos de clientes o usuarios para fines secundarios que incluyen, entre otros, el marketing a través de afiliados y no afiliados.
>
> (ii) seguridad de los datos, categoría que aborda la gestión de riesgos relacionados con la recopilación, retención y uso de datos sensibles, confidenciales y/o patentados de clientes o usuarios.

En la dimensión de liderazgo y gobernanza se encuentra la categoría (SASB, 2021b):

> (i) gestión de riesgos de incidentes críticos, la cual aborda el uso por parte de la empresa de sistemas de gestión y planificación de escenarios. Se relaciona con la cultura de seguridad en una empresa, sus sistemas de gestión de seguridad y controles tecnológicos relevantes, las posibles implicaciones

humanas, ambientales y sociales de tales eventos que ocurren, y los efectos a largo plazo para una organización.

### 2.5.3. El marco del International Integrated Reporting Council (IIRC)

A partir del ´pensamiento integrado´, el Reporte RI combina la contabilidad financiera tradicional con cuestiones relacionadas con la sostenibilidad y el Gobierno Corporativo para mejorar la toma de decisiones de los informes modernos (Velte & Stawinoga, 2016). Un reporte integrado debe ser un relato conciso de la historia futura de creación de valor de una organización, incluida la información sobre capitales financieros y no financieros, y haciendo referencia a la estrategia y al modelo comercial de la organización (De Villiers et al., 2020).

En general, un informe integrado es una comunicación resumen sobre cómo la estrategia, gobernanza, rendimiento y perspectivas de una organización desde el contexto de su medio ambiente, conducen a la creación, preservación o deterioro del valor sobre el corto, mediano y largo plazo (International Integrated Reporting Council, 2021).

Los aspectos a divulgar relacionados con Ciberseguridad se presentan en el capital denominado ´el capital intelectual´ el cual se define como espacios y herramientas de investigación y desarrollo, procesos y sistemas de gestión para implementar nuevas tecnologías e ideas innovadoras al servicio de la gestión del negocio (International Integrated Reporting Council, 2021).

### 2.5.4. Presentaciones 10-K en EDGAR

La presentación 10–K es el formulario oficial del informe anual requerido por la Comisión de Bolsa y Valores de EE.UU., que presenta un resumen completo del desempeño financiero de una compañía. Las empresas estadounidenses informan sobre los riesgos relacionados con la Ciberseguridad especialmente en el Ítem 1A. “Factores de riesgo” (SEC, 2020). De acuerdo con la Regla 421 (d) de la Ley de Valores 1933 (§230.421) literal (d) cualquier discusión sobre los factores de riesgo debe presentarse en

un lenguaje sencillo. La Guía de 2011 (Division of Corporation Finance & SEC, 2011) y la Guía actualizada de 2018 (SEC, 2018b) proporcionan varias ubicaciones que las empresas públicas pueden utilizar para divulgar sus riesgos de seguridad cibernética. Por ejemplo, el Ítem 1A (factores de riesgo), el Ítem 7 (MD&A) y el Ítem 8 (estados financieros y datos complementarios).

Según Gao et al. (2020), el Ítem 1A (factores de riesgo) es la ubicación más utilizada para las divulgaciones de Ciberseguridad, y en el Ítem 7 (MD&A) se revelan riesgos de Ciberseguridad y los incidentes de ciberdelincuencia. Las divulgaciones relacionadas con el ciberespacio en el Formulario 10-K son en gran medida cualitativas, lo que brinda a los gerentes la oportunidad de ser estratégicamente optimistas/pesimistas en la forma en que discuten los problemas cibernéticos (Berkman et al., 2018). En vista de que las empresas solo están obligadas a proporcionar descripciones cualitativas y no necesitan cuantificar la probabilidad o el impacto de los riesgos revelados, tienen un gran grado de discreción sobre qué revelar y cómo hacerlo (Li et al., 2018). Algunos autores afirman que las presentaciones del Formulario 10-K son documentos largos y complejos (Bloomfield, 2002; Grossman & Stiglitz, 1980; Rennekamp, 2012). Una buena parte de la investigación previa sobre divulgación de Ciberseguridad en el contexto estadounidense, evalúa el contenido del Informe 10 K (Berkman et al., 2018; Campbell et al., 2014; Gao et al., 2020; Gordon et al., 2010; Gordon et al., 2015; Li et al., 2018).

### 2.5.5. Presentaciones 20-F en EDGAR

Finalmente, la presentación 20-F es el formulario anual que deben presentar los titulares privados extranjeros que emiten acciones de acuerdo con la Ley de la Bolsa de Valores en los Estados Unidos 1934. Se espera, según SEC (2018b), que la información sobre Ciberseguridad se revele en el Ítem 3 D. Factores de riesgo del Formulario 20 F. No obstante, Brooks et al. (2021) afirman que el número de informes anuales presentados por empresas extranjeras, Formulario 20-F, está disminuyendo con el tiempo. Concretamente, un total de 2.513 empresas presentaron 20-F en 2005, mientras que solo 959 presentaron 20-F en 2018.

## 2.6. Conclusiones

En la actualidad la definición de riesgo consignada en la última versión ISO 31000 (2018) presenta una serie de elementos que dejan ver el avance de este concepto. El repaso histórico del riesgo corporativo muestra cómo las crisis económicas han sido las impulsoras de su avance. Es de anotar que el primer Estándar de Gestión de Riesgos, AS/NZS 4360:1995 de Australia (revisado desde 1999 y 2004), reúne por primera vez diferentes subdisciplinas. Este estándar es seguido de esfuerzos similares en Canadá, Japón y el Reino Unido.

Respecto a la divulgación de riesgos se espera que se realicen desde una óptica prospectiva que mejore la rendición de cuentas y las asimetrías de acceso a la información corporativa, al mejorar la medición y divulgación de los asuntos relacionados con el riesgo. Un referente internacional en la divulgación de riesgos lo constituyen los Principios de Gobierno Corporativo del G20 y de la OCDE. Respecto a la divulgación de riesgos relacionados con la sostenibilidad, en el ámbito internacional gozan de un reconocimiento muy marcado las divulgaciones financieras establecidas por el Grupo de Trabajo sobre Divulgaciones Financieras relacionadas con el Cambio Climático (TCFD).

Estados Unidos presenta avances importantes en la divulgación de información de riesgos de Ciberseguridad. La emisión de las guías SEC (2011) y SEC (2018) recomiendan que en el informe se incluyan las divulgaciones sobre riesgos e incidentes de Ciberseguridad para el caso de empresas extranjeras reguladas por la SEC en el artículo 3. D del Formulario 20-F. Esta medida va dirigida para todos los “emisores privados extranjeros” con acciones de capital inscritas en las bolsas de Estados Unidos, por lo que podemos decir que ésta es una exigencia con repercusiones en el contexto internacional.

La divulgación de información sobre los riesgos de Ciberseguridad se presenta especialmente en el informe anual, el cual se ha convertido en el medio de comunicación de las corporaciones con sus diferentes partes interesadas. Desde la responsabilidad social que se atribuye a las organizaciones, la sociedad interpela cada vez con mayor frecuencia

el comportamiento organizacional, por lo que se exige transparencia, responsabilidad e información estratégica que conecte el pasado con los riesgos y oportunidades futuras. Las revelaciones sobre Ciberseguridad expuestas en el informe anual mejoran las relaciones con los actores del mercado, reguladores y autoridad de protección de datos y la organización interna de la empresa. En la actualidad, la preparación de los informes anuales reportados por las organizaciones se efectúa a partir de algunos estándares de aceptación internacional. Concretamente, podemos destacar los siguientes:

- Las directrices GRI 2016 emitidos por la Junta de Estándares de Sostenibilidad Global (GSSB). Los aspectos de Ciberseguridad a revelar en el informe de sostenibilidad se pueden relacionar en especial con el ítem GRI 418 Privacidad de cliente GRI 418 – 1 "Reclamaciones fundamentadas relativas a violaciones de la privacidad del cliente y pérdida de datos del cliente".

- Los estándares emitidos por el American Sustainability Accounting Standard Board (SASB), que divulgan información a los inversores sobre la materialidad financiera de aspectos relacionados con sostenibilidad entre las empresas registradas ante la Securities Exchange Commission (SEC). La información sobre Ciberseguridad se divulga en la dimensión de capital social (SASB, 2021b).
- En el marco del International Integrated Reporting Council (IIRC), el informe integrado es una comunicación resumen sobre cómo la estrategia, gobernanza, rendimiento y perspectivas de una organización desde el contexto de su medio ambiente, conducen a la creación, preservación o deterioro del valor sobre el corto, mediano y largo plazo.

- Presentaciones 10-K en EDGAR, que es el formulario oficial del informe anual requerido por la Comisión de Bolsa y Valores de EE.UU, en el que se presenta un resumen completo del desempeño financiero de una compañía.

- Presentaciones 20-F en EDGAR, formulario anual que deben presentar los titulares privados extranjeros que emiten acciones de acuerdo con la Ley de la Bolsa de Valores en los Estados Unidos 1934.

## 2.7. Referencias


Abraham, S. The determinants of narrative risk information in U. F. 100 annual reports, & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/J.BAR.2007.06.002

AICPA. (2017). *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*. 29. https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/Description-Criteria.pdf%0Ahttps://web.archive.org/web/20170706132715/https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocum

Allini, A., Rossi, F. M., & Hussainey, K. (2015). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *http://dx.doi.org/10.1080/09540962.2016.1118935*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Amir, E., & Lev, B. (1996). Value-relevance of nonfinancial information: The wireless communications industry. *Journal of Accounting and Economics*, *22*(1–3), 3–30. https://doi.org/10.1016/S0165-4101(96)00430-2

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Baginski, S. P., Campbell, J. L., Hinson, L. A., & Koo, D. S. (2018). Do Career Concerns Affect the Delay of Bad News Disclosure? *The Accounting Review*, *93*(2), 61–95. https://doi.org/10.2308/ACCR-51848

Bakker, T. G. (2015). *Beadle Scholar Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks*. https://scholar.dsu.edu/theses/294

Bebbington, J., Kirk, E. A., & Larrinaga, C. (2012). The production of normativity: A comparison of reporting regimes in Spain and the UK. *Accounting, Organizations and Society*, *37*(2), 78–94. https://doi.org/10.1016/j.aos.2012.01.001

Bebbington, J., & Larrinaga-González, C. (2008). Carbon Trading: Accounting and Reporting Issues. *European Accounting Review*, *17*(4), 697–717. https://doi.org/10.1080/09638180802489162

Beretta, S., & Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *International Journal of Accounting*, *39*(3), 265–288. https://doi.org/10.1016/j.intacc.2004.06.006

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Bloomfield, R. J. (2002). The "Incomplete Revelation Hypothesis" and Financial Reporting. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.312671

Brazilian Institute of Corporate Governance. (2020). *Gestión de Riesgos Corporativos* (Brazilian Institute of Corporate Governance (ed.)). https://idbinvest.org/sites/default/files/2021-04/Cuaderno 19 - Gestión de Riesgos Corporativos.pdf

Brooks, L. (Lily) Z., Cheng, Y., Liu, L., & Yu, M. D. (2021). The timeliness of 10-K filings, early filers, and effects of filing deadline changes. *Journal of Corporate Accounting & Finance*, *32*(2), 169–186. https://doi.org/10.1002/JCAF.22492

Cabedo, J. D., & Tirado, J. M. (2004). The disclosure of risk in financial statements. *Accounting Forum*, *28*(2), 181–200. https://doi.org/10.1016/j.accfor.2003.10.002

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, *25*(1), 24–39. https://doi.org/10.1111/ijau.12209

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. min, & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396–455. https://doi.org/10.1007/s11142-013-9258-3

Chang, L. S., Most, K. S., & Brain, C. W. (1983). The Utility of Annual Reports: An International Study. *Journal of International Business Studies 1983 14:1*, *14*(1), 63–84. https://doi.org/10.1057/PALGRAVE.JIBS.8490507

Cheung, Y. L., Jiang, P., & Tan, W. (2010). A transparency Disclosure Index measuring disclosures: Chinese listed companies. *Journal of Accounting and Public Policy*, *29*(3), 259–280. https://doi.org/10.1016/j.jaccpubpol.2010.02.001

Committee Basel. (2015). Standards: Revised Pillar 3 Disclosure Requirements. En *Bank for International Settlements* (Número January). http://www.bis.org/bcbs/publ/d309.pdf

COSO. (2017). *COSO II ERM*.

CSA. (2017). *CSA Multilateral Staff Notice 51-347-Disclosure of cyber security risks and incidents*. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

CSA ACVM. (2013). *CSA Staff Notice 11-326 - Cyber Security*.

CSA ACVM. (2017). *CSA Staff Notice 33-321: Cyber Security and Social Media*. https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2017/2017oct19-33-321-avis-acvm-en.pdf

CSA ACVM. (2019). *Disclosure of cyber security risks and incidents*. *2017*, 605–608.

De Villiers, C., Hsiao, P.-C. K., & Maroun, W. (2020). Introduction to the Routledge Handbook of Integrated Reporting : An overview of integrated reporting and this book, which entails different perspectives on a maturing field and a framework for future research. *The Routledge Handbook of Integrated Reporting*, 1–14. https://doi.org/10.4324/9780429279621-1

Division of Corporation Finance, & SEC. (2011). *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Dungey, M., Flavin, T., O'Connor, T., & Wosser, M. (2022). Non-financial corporations and systemic risk. *Journal of Corporate Finance*, *72*, 102129. https://doi.org/10.1016/J.JCORPFIN.2021.102129

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law and Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Elshandidy, T., Shrives, P. J., Bamber, M., & Abraham, S. (2018). Risk reporting: A review of the literature and implications for future research. *Journal of Accounting Literature*, *40*, 54–82. https://doi.org/10.1016/j.acclit.2017.12.001

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

EU. (2014). *Directive 2014/95 / EU of the European Parliament and of the Council - of October 22, 2014*.

EU. (2016). *EU general data protection regulation* (Vol. 2014, Número April).

EY. (2018). *SEC guidance on cybersecurity: board considerations* (Número March). https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cybersecurity/ey-sec-guidance-on-cybersecurity-board-considerations.pdf

FASB. (1994). Statement of Financial Accounting Standards No. 119, Disclosure about Derivative Financial Instruments and Fair Value of Financial Instruments. *Financial Accounting Standards Board: Norwalk, Connecticut*, *119*.

FASB. (1998). Statement of Financial Accounting Standards No. 133, Accounting for Derivative Instruments and Hedging Activities. *Financial Accounting Standards Board: Norwalk, Connecticut.*, *133*.

Fraser, J. S. B. J. (2010). *Enterprise risk management*.

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

García-Sánchez, I. M., Gómez-Miranda, M. E., David, F., & Rodríguez-Ariza, L. (2019). Board independence and GRI-IFC performance standards: The mediating effect of the CSR committee. *Journal of Cleaner Production*, *225*, 554–562. https://doi.org/10.1016/J.JCLEPRO.2019.03.337

Gelfond, S., Wechsler, J., Cohen, H., & Llp, J. (2017). *Top 10 Practice tips by experts: risk factors*.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692

GRI. (2016). GRI 418: Customer privacy 2016 418. *GRI Standards*. www.globalreporting.org

Grossman, B. S. J., & Stiglitz, J. E. (1980). *On the Impossibility of Informationally Efficient Markets Author ( s ): Sanford J . Grossman and Joseph E . Stiglitz Source : The American Economic Review , Jun ., 1980 , Vol . 70 , No . 3 ( Jun ., 1980 ), pp . 393- Published by : American Economic Associ*. *70*(3), 393–408.

Héroux, S., & Fortin, A. (2020a). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S., & Fortin, A. (2020b). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Hijink, J. B. S. (2010). *Publicatieverplichtingen voor beursvennootschappen*.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2852519

Holland & Knight. (2021). *SEC Issues First-Ever Penalties for Deficient Cybersecurity Risk Controls*. https://www.hklaw.com/en/insights/publications/2021/06/sec-issues-first-ever-penalties-for-deficient-cybersecurity-risk

Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies*, *21*(4), 1005–1045. https://doi.org/10.1007/s11142-016-9371-1

Hunt, B. (2003). *The Timid Corporation: Why Business is Terrified of Taking Risk*.

ICAWE. (2011). *Reporting Business Risks: Meeting Expectations*.

International Integrated Reporting Council. (2021). < IR > Framework about the IIRC. *Jo*, *January*, 58. https://integratedreporting.org/wp-content/uploads/2021/01/InternationalIntegratedReportingFramework.pdf

IOSCO. (2016). *Cyber Security in Securities Markets – An International Perspective Report on IOSCO ' s cyber risk coordination efforts*.

IRRC. (2016). *The Corporate Risk Factor Disclosure Landscape*. *January*, 27. https://www.weinberg.udel.edu/irrci/research/887

ISO. (2018). *ISO 31000 Risk management*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Jorion, P. (2002). *The Accounting Review* (Vol. 77).

Kasznik, R., & Lev, B. (1995). To warn or not to warn: Management disclosures in the face of an earnings surprise. *Accounting review: A quarterly journal of the American Accounting Association*, *70*(1), 113–134.

Kiliç, M., Kuzey, C., & Uyar, A. (2015). The impact of ownership and board structure on corporate social responsibility (CSR) reporting in the Turkish banking industry. *Corporate Governance (Bingley)*, *15*(3), 357–374. https://doi.org/10.1108/CG-02-2014-0022

Konishi, N., & Ali, M. M. (2007). Risk reporting of Japanese companies and its association with corporate characteristics. *undefined*, *4*(3), 263–285. https://doi.org/10.1504/IJAAPE.2007.016281

Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, *8*(4), 1–15. https://doi.org/10.3390/risks8040128

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/J.ACCINF.2018.06.003

Marston, C. L., & Shrives, P. J. (1991). The use of disclosure indices in accounting research: A review article. En *The British Accounting Review* (Vol. 23, Número 3, pp. 195–210). Academic Press. https://doi.org/10.1016/0890-8389(91)90080-L

Masud, M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*. https://doi.org/10.1108/JAEE-07-2021-0237

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

Mitra, S., & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *https://doi.org/10.1287/isre.2015.0587*, *26*(3), 565–584. https://doi.org/10.1287/ISRE.2015.0587

Morse, E. A., Raval, V., & Wingender, J. R. (2018). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. En *Business Lawyer* (Vol. 73, Número 1, pp. 1–34). American Bar Association. https://doi.org/10.2139/ssrn.2711439

OCDE. (2016). *Principios de Gobierno Corporativo de la OCDE y del G20*. https://doi.org/10.1787/9789264259171-es

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011). Risk-related disclosures by non-finance companies: Portuguese practices and disclosure characteristics. *Managerial Auditing Journal*, *26*(9), 817–839. https://doi.org/10.1108/02686901111171466

PCAOB. (2014). *Standing Advisory Group meeting cybersecurity*.

Power, M. (2004). The risk management of everything. *Journal of Risk Finance*, *5*(3), 58–65. https://doi.org/10.1108/eb023001

PWC. (2018a). *Rethinking cybersecurity disclosures to investors - What executives and boards need to know about the SEC's guidance: June 2018*. www.pwc.com/cybersecurity

PWC. (2018b). *US2018-07: SEC issues interpretive guidance on cybersecurity disclosures*. https://viewpoint.pwc.com/dt/us/en/pwc/in_briefs/2018/2018__7_US/us201807_sec_issues__US.html

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Rel ated Disclosure. *Journal of Business Ethics*, *1*, 3. https://doi.org/10.1007/s10551-020-04717-9

Rennekamp, K. (2012). Processing Fluency and Investors' Reactions to Disclosure Readability. *Journal of Accounting Research*, *50*(5), 1319–1354. https://doi.org/10.1111/J.1475-679X.2012.00460.X

Rivera-Arrubla, Y. A., Zorio-Grima, A., & García-Benau, M. A. (2017). Integrated reports: Disclosure level and explanatory factors. *Social Responsibility Journal*, *13*(1), 155–176. https://doi.org/10.1108/SRJ-02-2016-0033

Rupley, K. H., Brown, D., & Marshall, S. (2017). Evolution of corporate reporting: From stand-alone corporate social responsibility reporting to integrated reporting. *Research in Accounting Regulation*, *29*(2), 172–176. https://doi.org/10.1016/J.RACREG.2017.09.010

SASB. (2021a). *Estándares SASB*. https://www.sasb.org/standards/download/

SASB. (2021b). *SASB Materiality Map*. https://materiality.sasb.org/

Scaltrito, D. (2016). Voluntary disclosure in Italy: Firm-specific determinants an empirical analysis of Italian listed companies. *EuroMed Journal of Business*, *11*(2), 272–303. https://doi.org/10.1108/EMJB-07-2015-0032

Schubert, D; Cedarbaum, J and Schloss, W. (2015). The SEC's Two Primary Theories in Cybersecurity Enforcement Actions. *The Cybersecurity Law Report*, *1*(1), 39–70.

SEC. (1997). Disclosure of Accounting Policies for Derivative Financial Instruments, and Derivative Commodity Instruments and Disclosure of Quantitative and Qualitative Information about Market Risk Inherent in Derivative Financial Instruments, Other Financial Instrum. *Federal Register*, *62*(27), 6044–6079. https://www.federalregister.gov/documents/1997/02/10/97-2991/disclosure-of-accounting-policies-for-derivative-financial-instruments-and-derivative-commodity

SEC. (2005). *Staff Statement on Management's Report on Internal Control Over Financial Reporting*. https://www.sec.gov/info/accountants/stafficreporting.htm

SEC. (2017). *Prospectus summary, risk factors § 229.503 (Item 503)*. 473–475. https://doi.org/10.4135/9781608712380.n519

SEC. (2018a). *Federal Register Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures

SEC. (2018b). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

SEC. (2020). *17 CFR § 229.105 - (Item 105) Risk factors*. https://www.law.cornell.edu/cfr/text/17/229.105

SEC. (2022). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. *13*(34), 1–204.

Sinha, T., & Vaughan, E. J. (1994). Fundamentals of Risk and Insurance. En *The Journal of Risk and Insurance* (Vol. 61, Número 2). https://doi.org/10.2307/253725

Skinner, D. J. (1997). Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics*, *23*(3), 249–282. https://doi.org/10.1016/S0165-4101(97)00010-4

Solomon, J. (2019). *Corporate Governance and Accountability* (5TH ed.). John Wiley.

Solomon, J. F., Solomon, A., Norton, Si. D., & Joseph, N. L. (2000). A conceptual

framework for corporate risk disclosure emerging from the agenda for corporate goverance reform. *The British Accounting Review*, *32*(4), 447–478. https://doi.org/10.1006/bare.2000.0145

Szegö, G. (2002). Measures of risk. *Journal of Banking & Finance*, *26*, 1253–1272. https://doi.org/10.1016/S1548-5315(11)70388-6

TCFD. (2021). *TCFD Status Report*. *October*.

Vaughan, E. (1997). *Risk Management*. Wileyl.

Velte, P., & Stawinoga, M. (2016). Integrated reporting: The current state of empirical research, limitations and future research implications. *Journal of Management Control 2016 28:3*, *28*(3), 275–320. https://doi.org/10.1007/S00187-016-0235-4

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*(C), 179–194. https://doi.org/10.1016/0165-4101(83)90011-3

Wang, L., & Tuttle, B. (2014). Using corporate social responsibility performance to evaluate financial disclosure credibility. *https://doi.org/10.1080/00014788.2014.922408*, *44*(5), 523–544. https://doi.org/10.1080/00014788.2014.922408

Wang, T., & Hsu, C. (2013). Board composition and operational risk events of financial institutions. *Journal of Banking and Finance*, *37*(6), 2042–2051. https://doi.org/10.1016/j.jbankfin.2013.01.027

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Wang, T., Ulmer, J. R., & Kannan, K. (2013). The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities. *Journal of Organizational Computing and Electronic Commerce*, *23*(3), 200–223. https://doi.org/10.1080/10919392.2013.807712

WEF. (2021). *The Global Risks Report 2021: 16th Edition*.

Wuerges, A. F. E., & Borba, J. A. (2014). Fraudes contábeis: Uma estimativa da probabilidade de detecção. *Revista Brasileira de Gestao de Negocios*, *16*(52), 466–483. https://doi.org/10.7819/rbgn.v16i52.1555

# CAPÍTULO 3. ALCANCE DE LA DIVULGACIÓN DE INFORMACIÓN SOBRE CIBERSEGURIDAD EN AMÉRICA LATINA

El Foro Económico Mundial WEF (2021) presenta, entre los riesgos emergentes de alta probabilidad, las fallas de Ciberseguridad generadas por el rápido aumento de la digitalización. Profesionales de la industria aseguradora de seis regiones del planeta, incluida América Latina, señalaron en la encuesta de Axa (2020) que el segundo riesgo emergente más importante, después del cambio climático, proviene de las fallas de Ciberseguridad, una percepción que casi ha duplicado su importancia desde 2019, con una tasa del 54%. Según King (2016), la tecnología es ahora la fuente de muchas oportunidades futuras para una organización, así como de posibles interrupciones, y es un excelente ejemplo de cómo el riesgo y la oportunidad se están convirtiendo cada vez más en dos caras de la misma moneda.

Desde el ámbito empresarial, la responsabilidad social según ISO 26.000 (2011) se relaciona con el impacto organizacional, entendido como aquel cambio positivo o negativo que se genera en la sociedad, la economía o el entorno, producido en su totalidad o en parte, por las decisiones y actividades pasadas y presentes de una compañía. Según Rashid et al. (2019), la Ciberseguridad debe pensarse como un conjunto claro de procesos que reducen el riesgo de daño a las personas y a la empresa. Así, la rendición de cuentas se convierte en una forma de comunicar, con base en información financiera y no financiera, los efectos de las acciones de la organización con la sociedad. En este sentido, las empresas deben fortalecer sus divulgaciones de información sobre seguridad cibernética para demostrar responsabilidad y compromiso frente a este riesgo, y generar confianza en las partes interesadas sobre cómo se prioriza, gestiona y monitorea como una amenaza comercial crítica y una oportunidad estratégica (E&Y, 2020).

En este contexto, las empresas latinoamericanas han ido incorporando paulatinamente revelaciones sobre Ciberseguridad en sus informes anuales corporativos de manera voluntaria con base en la gestión de riesgos, entre los cuales es cada vez más común encontrar el riesgo de Ciberseguridad y/o seguridad de la información. En algunos casos, éste se revela inicialmente como un riesgo emergente y, en períodos posteriores, como un riesgo operacional. Si bien no existe una regulación exclusiva en la región para la divulgación de información de Ciberseguridad en el reporte anual, algunas normas

emitidas por los entes de vigilancia y control en materia de Gobierno Corporativo, gestión de riesgos y privacidad de datos han generado una mayor divulgación sobre Ciberseguridad, especialmente en el sector financiero. Al mismo tiempo, las empresas latinoamericanas que participan como emisoras en el mercado de valores de Estados Unidos también reportan los factores de riesgo relacionados con el riesgo cibernético de manera obligatoria en el informe anual 20 F ítem 3D (SEC, 2018).

En el panorama del mercado de capitales internacional, el aumento en las divulgaciones de seguridad cibernética ha sido motivado por diferentes lineamientos o sucesos. En orden cronológico, cabe mencionar que, en 2011, la Guía de la Comisión de Bolsa y Valores SEC (Division of Corporation Finance & SEC, 2011) proporcionó pautas para la divulgación de temas relacionados con el ciberespacio en las presentaciones 10-K (Berkman et al., 2018; Ettredge et al., 2018). En 2018, la SEC emitió la segunda guía sobre divulgación de riesgos de Ciberseguridad y, tres años depués, la Comisión de Valores de Estados Unidos impuso las primeras sanciones por controles y procedimientos de divulgación deficientes relacionados con riesgos de Ciberseguridad por parte de empresas emisoras en junio y agosto de 2021, respectivamente (SEC, 2021b; SEC, 2021a). Finalmente, en 2022 la SEC propone reglas para la divulgación sobre gestión de riesgos de Ciberseguridad, estrategia, gobernanza y divulgación de incidentes por parte de empresas públicas (SEC, 2022).

Respecto al mercado de capitales europeo, se puede decir que existe un requerimiento de divulgación obligatoria de incidentes cibernéticos en el Reglamento General de Protección de Datos y la directiva sobre seguridad de redes y sistemas de información (NIS). Según Eijkelenboom & Nieuwesteeg (2021), si bien este tipo de divulgación no requiere específicamente una incorporación en el informe financiero anual, la obligación de divulgar incidentes de datos desde la perspectiva de la Ley de Seguridad Cibernética podría proporcionar incentivos para que la Junta también publique información sobre este tema en el informe. Así, en el ámbito empresarial, la Ciberseguridad se convierte en una responsabilidad empresarial ineludible, y la rendición de cuentas en una forma de generar

confianza y asegurar resiliencia frente a los ciberriesgos y las ciberamenazas de alto impacto.

En este contexto, el propósito de este capítulo es proponer un índice de divulgación como instrumento novedoso que permita medir el alcance de la divulgación de información de Ciberseguridad voluntaria y obligatoria, a partir de veintisiete elementos asociados en cuatro dimensiones: gobernanza, estrategia, gestión de riesgos e implicaciones financieras. Este instrumento de medición ha sido elaborado con base en la literatura previa y estándares internacionales relacionados con el riesgo de Ciberseguridad corporativo. Dado que los estudios sobre la evaluación de la divulgación de la Ciberseguridad en América Latina son inexistentes, esta investigación intenta cerrar esta brecha, tomando como objeto de estudio a las empresas emisoras de los principales índices bursátiles de algunos países de la región. La técnica de análisis de contenido utilizada se centra en el examen e identificación de la información de Ciberseguridad revelada en los informes anuales y los formularios 20 F anuales de las empresas con las cotizaciones bursátiles más altas de Argentina, Brasil, Chile, Colombia, México y Perú durante el período de 2016-2020.

Este capítulo se organiza en base a la siguiente estructura. En primer lugar, se presentan los avances en Ciberseguridad en América Latina. Seguidamente, se expone la metodología del estudio, que incluye la presentación del índice de divulgación propuesto. Finalmente, se muestran las hipótesis del estudio y los resultados de la aplicación del índice por dimensión, país y sector de actividad.

## 3.1. La Ciberseguridad en el Contexto Latinoamericano

La Ciberseguridad en el contexto de América Latina no es ajena al desarrollo experimentado en el ámbito internacional. En este sentido cabe indicar que los grandes retos de la Ciberseguridad tienen un carácter global (Porrúa & Contreras, 2020), y la intrusión del ámbito digital en todas las áreas de la actividad humana, junto con niveles sin precedentes de innovación tecnológica e interdependencia, han hecho imposible que

la Ciberseguridad se trate de forma aislada como un problema técnico o un área de política separada (Barmpaliou, 2020). Los esfuerzos de Ciberseguridad deben ser de naturaleza multidimensional, debido a que se necesita una variedad de factores para construir una cíber sociedad resiliente (Urrutia, 2020), y colaborativa, debido a que requieren que las naciones trabajen mano a mano con otros países (Creese, 2020).

A nivel mundial se han tomado diferentes medidas de Ciberseguridad que, en cierto modo, han marcado la agenda latinoamericana. Entre ellas cabe destacar la firma del Convenio de Budapest en 2001 que, siendo el primer tratado internacional sobre violaciones cometidas en el ciberespacio, marca el inicio de la legislación en materia de Ciberseguridad. Posteriormente, eventos como las Cumbres Mundiales sobre la Sociedad de la Información desde 2003 han consolidado procesos de cooperación internacional.

En 2007, como marco internacional, la Agenda Mundial de la ITU (ITU, 2007) propuso: (i) el Índice Mundial de Ciberseguridad (IMC), entre cuyos propósitos se encuentra la sensibilización sobre el papel que juegan los gobiernos en la promoción de la cultura de la Ciberseguridad; (ii) la recopilación de información relacionada con las normas CERT y CIRT; (iii) estrategias, políticas, certificación y concienciación nacionales; y (iv) la alianza ITU-IMPACT, que generalmente se enfoca en programar simulacros cibernéticos en diferentes regiones del mundo para evaluar y mejorar la capacidad de respuesta en caso de eventos cibernéticos.

En 2008, la UIT emitió la Recomendación UIT-T X.1205 como marco internacional sobre aspectos generales de la Ciberseguridad. Con base en la Resolución 64/25 de 2009, titulada Avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, la ONU ratifica la invitación a sus Estados Miembros, por un lado, al examen multilateral de amenazas en seguridad de la información con nuevas estrategias de aplicación en el mundo, sumado a la evaluación de los inconvenientes en seguridad de la información; y, por otro lado, a la mitigación y salvaguarda de la circulación de información (Asamblea General de Naciones Unidas, 2009).

Posteriormente, en 2015, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) emitió una recomendación centrada en la gestión de los riesgos de seguridad digital para la prosperidad económica y social (OECD, 2015). Al mismo tiempo, para dar cumplimiento a las disposiciones internacionales, en Estados Unidos y Europa se emitieron diferentes lineamientos y regulaciones, en la mayoría de los casos vinculantes a nivel de país, medidas que han sido objeto de convergencia y adaptación a nivel mundial.

En este escenario internacional cabe destacar que, si bien los gobiernos de América Latina son conscientes de la necesidad de proteger el espacio digital del que tanto depende el funcionamiento de la sociedad, la Ciberseguridad no ha ganado presencia en la agenda política de la región con la urgencia que se esperaría (Creese, 2020). Por tanto, los países de América Latina deben continuar fomentando una mayor cooperación entre ellos, involucrando a todos los actores relevantes, así como estableciendo mecanismos de monitoreo, análisis y evaluaciones de impacto relacionado con la seguridad cibernética, tanto a nivel nacional como regional (Porrúa & Contreras, 2020). De acuerdo con Day (2018), los formuladores de políticas, los líderes de la industria y los profesionales legales de América Latina están prestando una atención significativa a las regulaciones centradas con la privacidad de acuerdo a los requisitos de la Unión Europea, las exigencias para notificar a las autoridades reguladoras de violaciones de datos, y otros asuntos de Ciberseguridad, como la tecnología financiera y la actividad criminal.

La creación de conciencia sobre las amenazas cibernéticas a nivel político es sólo el primer paso para desarrollar capacidades de seguridad cibernética más armonizadas en la región. Los actores de América Latina y el Caribe, como la Organización de los Estados Americanos (OEA), ya han contribuido a este proceso (Porrúa & Contreras, 2020). Es así como, en el año 2004, los estados miembros de la OEA aprueban la Estrategia Interamericana Integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética y cooperación internacional para la región. Posteriormente, a través, del Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo

de la OEA, se fortalece la capacidad técnica y el desarrollo de políticas de Ciberseguridad en las Américas.

Respecto a la política internacional, el Convenio de Budapest se ha transformado en el modelo preferido para muchos países, en términos de la promoción de su propia legislación nacional, en la construcción de la cooperación internacional y en cuanto al intercambio de pruebas electrónicas (Porrúa & Contreras B, 2020). La región está utilizando el Convenio de Budapest sobre la ciberdelincuencia como modelo (Argentina, Chile, Costa Rica, República Dominicana, Panamá y Paraguay, fueron partes del Convenio de Budapest, y Colombia, México y Perú, fueron observadores) y la aplicación las directivas de la UE de Ciberseguridad ya están en vigor (OAS; ISA, 2020).

Con el impulso de la Organización de Estados Americanos (OEA) se ha logrado la adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, a partir de la Resolución AG/RES.2004 (Comisión Interamericana de Telecomunicaciones, 2004), así como la adhesión a la legislación de la Unión Europea en materia procesal sobre el delito cibernético en Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay y República Dominicana (Porrúa & Contreras, 2020). Aguilar (2019) resalta la importancia de que las estrategias nacionales de Ciberseguridad de la región estén relacionadas y no sean distantes con la comprensión actual de las ciberamenazas y el potencial del ciberespacio para vulnerar la seguridad pública y nacional.

Según OEA (ISA, 2020) están surgiendo nuevos requisitos para el sector financiero por cuenta de las políticas de Ciberseguridad y los requisitos para el procesamiento y almacenamiento de datos. Estas regulaciones aún están en desarrollo, pero se espera que le brinden más certeza a la industria sobre las medidas de Ciberseguridad de los dispositivos y servicios de tecnología financiera (Fintech). Debido a la implementación de las normas de la UE, muchos países latinoamericanos están comenzando a crear autoridades nacionales de protección de datos y a adoptar normas de ´notificación a la

autoridad´ similares a las incluidas en el Reglamento General de Protección de Datos, estableciendo requisitos no solo para notificar a los consumidores afectados sino también a las autoridades reguladoras pertinentes (OAS; ISA, 2020).

A principios de 2020, doce países han aprobado estrategias nacionales de Ciberseguridad, incluidos Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Paraguay (2017), Chile (2017), Costa Rica (2017), México (2017), Guatemala (2018), República Dominicana (2018), Argentina (2019) y Brasil (2020), entre otros en progreso (Porrúa & Contreras, 2020). Según OEA (2019), en este aspecto se puede resaltar que Colombia fue el primer país de la región en desarrollar una estrategia nacional de Ciberseguridad en 2011, así como el primer país en revisarla en 2016, con un enfoque integral y colaborativo, fomentando la gestión del riesgo y la participación de las múltiples partes interesadas. El BID & OEA (2020), confirman que siete países, de los treinta y dos analizados, cuentan con un plan de protección de su infraestructura crítica, y veinte han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT, por sus siglas en inglés. También se considera que en veintidós de los treinta y dos países hay pocas capacidades para investigar los delitos que se cometen en el ciberespacio. Más aún, que dichos delitos resulten en juicio es todavía un reto mayor, por lo cual se puede concluir que la región aún no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio (Creese, 2020).

Además de los compromisos con el desarrollo de capacidades de seguridad cibernética a nivel nacional, América Latina y el Caribe ha sido más que el fundamento de una serie de iniciativas regionales muy dinámicas (Barmpaliou, 2020). Por ejemplo, en 2016 se realizó el lanzamiento de CSIRT Américas, una plataforma que permite la cooperación regional y el intercambio de información entre los equipos de respuesta a incidentes gubernamentales y nacionales de los Estados Miembros de la OEA (Barmpaliou, 2020).

Según ITU & ABI Research (2014), el Índice Global de Ciberseguridad tiene como objetivo proporcionar una instantánea de dónde se encuentran los países en sus compromisos de Ciberseguridad. ITU (2021) mide la responsabilidad de los estados

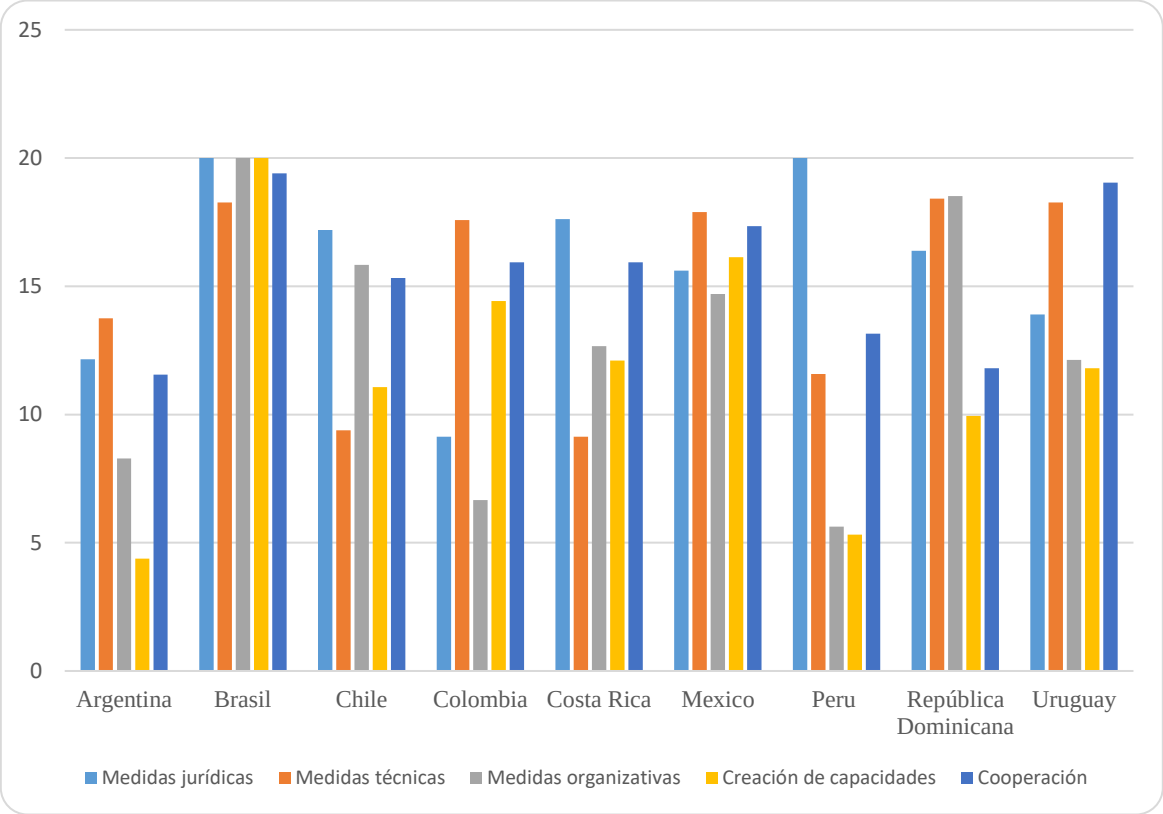
miembros con la Ciberseguridad, y para su cálculo mapea 82 preguntas sobre los compromisos de Ciberseguridad de los Estados miembros en cinco dimensiones: (i) medidas legales, (ii) medidas técnicas, (iii) organizativas, (iv) medidas de desarrollo de la capacidad y (v) medidas de cooperación.

Revisando cada una de las dimensiones del Índice (Figura 6) se destaca el pilar legal correspondiente a la parte legislativa y regulatoria emitida en materia de Ciberseguridad, protección de datos e infraestructuras críticas. En esta dimensión los mayores índices se dan en Brasil y Perú con la máxima puntuación (20) y Chile con un alto grado de cumplimiento (17,2).

Otro pilar de gran importancia es la cooperación, relativo a la evaluación de si los países cuentan con acuerdos (bilaterales y multilaterales) o alianzas que contribuyan al intercambio de información, a la aplicación de buenas prácticas y a la uniformidad en las medidas de seguridad. En este caso, cabe resaltar las puntuaciones de Brasil (19,41) y Uruguay (19,04).

En la dimensión de medidas técnicas nuevamente toma una participación importante Brasil (18,27), junto con República Dominicana (18,42) y Uruguay (18,27), destacándose por la implementación y el estado activo de los equipos de respuesta a incidentes de Ciberseguridad (CIRT). Por lo que respecta al grado de cumplimento del pilar de creación de capacidades enfocado a las iniciativas de capacitación, concienciación y desarrollo de las capacidades en Ciberseguridad, el mayor grado de cumplimiento lo presenta Brasil (20) seguido de México (16,13). Finalmente, en el pilar de medidas organizativas focalizado en las agencias y estrategias nacionales de Ciberseguridad repuntan República Dominicana (18,52) y Chile (15,84).

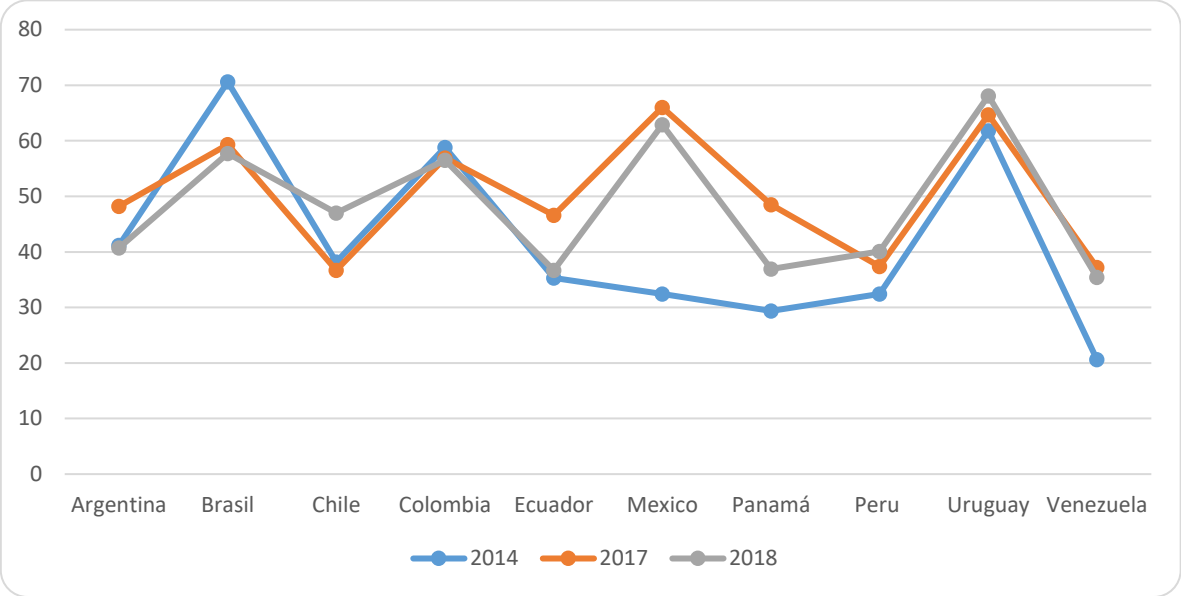
**Figura 6. Índice de Ciberseguridad por dimensiones en países de América Latina (2020)**




Nota: elaborado con base en (ITU, 2021)

Por lo que respecta a la evolución del Índice de Ciberseguridad en América Latina durante los años 2014, 2017 y 2018 (Figura 7), se puede observar que, en general, el compromiso de la Ciberseguridad en Latinoamérica está por debajo de 0,70. Los países que obtienen las mayores puntuaciones son Brasil y Uruguay, destacando Colombia por cuanto se mantiene constante en los tres años objeto de análisis. Mientras México mejora en alto grado en 2017 y se mantiene en 2018, Paraguay presenta una mejora importante en el año 2018.

**Figura 7. Índice de Ciberseguridad en países en América Latina (2014, 2017 y 2018)**




Nota: elaborado con base en (ITU & ABI Research, 2014; ITU, 2017; ITU, 2018)

En términos generales se puede afirmar que, desde la iniciativa de la OEA en 2004, América Latina ha venido presentando marcos regulatorios regionales y nacionales que apoyan de manera importante los aspectos jurídicos relacionados con Ciberseguridad. No obstante, el proceso de digitalización acelera a un ritmo vertiginoso, y la región aún no cuenta con la infraestructura tecnológica, ni con las capacidades institucionales para combatir el riesgo cibernético latente.

## 3.2. Propuesta de un Índice de Divulgación de Información sobre Ciberseguridad

Un índice de divulgación es una de las principales formas de evaluar la transparencia informativa de las instituciones públicas y privadas (Bonsón & Escobar, 2004). Así, Marston & Shrives (1991) consideran que el índice de divulgación es una herramienta de investigación que persiste en el tiempo y representa listas extensas de elementos seleccionados que pueden revelarse en los informes de las empresas. En este sentido, Ortiz & Clavel (2006) indican que la construcción de índices de divulgación es una práctica muy extendida, su elaboración forma parte de una vertiente de la metodología de análisis de contenido y es una de las principales técnicas utilizadas para estudiar la información que brindan las organizaciones. Los estudios de índice de divulgación son una forma parcial de análisis de contenido donde los ítems a estudiar se especifican ex ante (Beattie et al., 2004). Este procedimiento mide el alcance de la divulgación (Allegrini & Greco, 2013). Estudios anteriores, relacionados con temas de revelación de información de sostenibilidad, confirman su amplia aceptación en la investigación (Andrikopoulos et al., 2014; Clarkson et al., 2008; Clarkson et al., 2013; Chithambo & Tauringana, 2014; Choi et al., 2010; Chu et al., 2013; Datt et al., 2019; Darus et al., 2019; Haque & Deegan, 2010; Hardiyansah & Agustini, 2020; Liesen et al., 2015; Luo et al., 2013; Marshall & Weetman, 2007; Pitrakkos & Maroun, 2019; Plumlee et al., 2015; Prado-Lorenzo et al., 2009; Rankin et al., 2011). A la vez estudios previos relacionados con la divulgación de riesgos proponen algunos índices de divulgación (Elzahar & Hussainey, 2012; Lim et al., 2007; Ntim et al., 2013; Patelli & Prencipe, 2007).

Por nuestra parte, el índice de divulgación propuesto corresponde a un instrumento de medición novedoso que tiene como objetivo evaluar las revelaciones de información sobre Ciberseguridad, y puede constituir un punto de referencia para la valoración del alcance de la divulgación en las organizaciones por parte de los diferentes grupos de interés.

Se estructura en cuatro dimensiones que representan el núcleo de cómo operan las organizaciones a partir de los siguientes referentes: (i) Gobernanza (TCFD, 2021; CSA,

2017; E&Y, 2020), (ii) Estrategia (Héroux & Fortin, 2020a;TCFD, 2021), (iii) Gestión de riesgos (E&Y, 2020) e, (iv) Implicaciones financieras (SEC, 2018). La medida de divulgación de Ciberseguridad se basa en 27 elementos individuales, cada uno de los cuales se refiere a un tema particular asociado a una de las cuatro dimensiones. Concretamente, gobernanza (5 elementos), estrategia (6), gestión de riesgo (13) e implicaciones financieras (3).

### 3.2.1. Población y muestra

Como población objeto de estudio se seleccionaron las empresas listadas en los principales índices bursátiles de los países latinoamericanos de mayor capitalización de la región: Argentina, Brasil, Chile, Colombia, México y Perú, que captan más del 70% del mercado en la región (S&P, 2020). Las empresas que no reportaron sobre Ciberseguridad no han sido tenidas en cuenta en el estudio, situación que ha disminuido de forma importante la muestra. Se estudiaron cuatro sectores económicos: energía, financiero, consumo discrecional y materiales, bajo dos criterios: (i) su alta vulnerabilidad al riesgo cibernético, y (ii) la presencia de empresas de cada sector en la mayoría de los países de la muestra. Para fines de agrupación, las empresas fueron analizadas por país y sector de actividad económica de acuerdo con la clasificación propuesta por los Global Industry Classifications Standards (GICS). La muestra final arrojó un total de 425 observaciones en el período 2016-2020 (Tabla 6). El período de tiempo objeto de estudio se inicia en 2016 porque es el año en que de forma incipiente se abordan las revelaciones sobre Ciberseguridad (en los años anteriores la divulgación sobre Ciberseguridad fue escasa o inexistente en la mayoría de las empresas de nuestra muestra), y finaliza con el año 2020 porque nos hemos propuesto evaluar el impacto de la Pandemia COVID -19 en las variables de nuestro estudio, además hemos decidido evaluar tan solo un período de cinco años.

**Tabla 6. Muestra de empresas por país, índice bursátil y sector de actividad**

| País | Índice bursátil | N ° empresas | Sectores | | | |
|---|---|---|---|---|---|---|
| | | | Consumidor discrecional | Energía | Financiero | Materiales |
| **Argentina** | S&P Merval | 7 | 0 | 2 | 4 | 1 |
| **Brasil** | Ibovespa | 25 | 5 | 7 | 9 | 4 |
| **Chile** | IPSA | 18 | 7 | 5 | 6 | 0 |
| **Colombia** | Colcap | 16 | 2 | 7 | 5 | 2 |
| **México** | S&P/BMV IPC | 11 | 1 | 1 | 3 | 6 |
| **Perú** | S&P/BVL Perú | 8 | 1 | 3 | 4 | 0 |

La Tabla 7 presenta el listado de las empresas que conforman la muestra por país.

**Tabla 7. Empresas que componen la muestra por país**

| País | Empresa/Año |
|---|---|
| **Argentina** | BBVA Banco Francés S.A. |
| | Banco Macro S.A. |
| | Grupo Financiero Galicia S.A. |
| | Transportadora de Gas del Norte |
| | YPF S.A. |
| | Grupo Supervielle S.A. |
| | Ternium Argentina S.A. |
| **Brasil** | B3 S.A. |
| | Banco do Brasil S.A. |
| | Bradesco S.A. |
| | Cielo S.A. |
| | Cemig S.A. |
| | Cosan S.A. |
| | Sid Nacional S.A. |
| | Engie Brasil |
| | Eletrobras |
| | Energias do Brasil |

| | |
|---|---|
| | Gerdau S.A. |
| | Irbbrasil |
| | Itausa S.A. |
| | Itauunibanco |
| | Lojas Renner S.A. |
| | Magaz Luiza |
| | Grupo Natura |
| | P. Acucar-CBD |
| | Petrobras |
| | Petrorio |
| | Localiza |
| | Banco Santander S.A. |
| | Sul America |
| | Ultrapar |
| | Vale |
| **Chile** | Aesgener |
| | Banco de Chile (SN) |
| | Banco de Crédito e Inversiones |
| | Cencosud |
| | Cervecerías |
| | Colbún |
| | Embotelladora Andina |
| | Empresas Copec |
| | ENEL Américas |
| | Engie Energía Chile |
| | Falabella |
| | Grupo Security |
| | Inv La Constru |
| | Itaú CorpBanca |
| | Plaza |
| | Ripley Corp. |
| | Santander Chile |
| | SMU |
| **Colombia** | Almacenes Éxito |
| | Banco Davivienda |
| | Bancolombia |
| | Bolsa de Valores de Colombia |
| | Canacol Energy |
| | Celsia |
| | Cementos Argos |
| | Cemex Latam |

| | |
|---|---|
| | Ecopetrol |
| | Grupo Energía Bogotá |
| | Grupo Aval |
| | Interconexión Eléctrica |
| | Nutresa |
| | Grupo Sura |
| | Promigas |
| | Terpel |
| **México** | Fomento Económico Mexicano |
| | Grupo México, S.A.B. de C.V. |
| | Grupo Financiero Banorte |
| | Grupo Cementos de Chihuahua. |
| | Infraestructura Energética Nova |
| | Kimberly-Clark de México |
| | Bolsa Mexicana de Valores |
| | Cemex, S.A.B. de C.V. |
| | Gentera, S.A.B. de C.V. |
| | Mexchem. Mx |
| | Peñoles |
| **Perú** | Alicorp SA |
| | BBVA Continental |
| | Bolsa de Valores de Lima SA |
| | Credicorp Limited |
| | Enel Generación Perú SA |
| | Enel Distribución Perú |
| | Graña y Montero |
| | Rimac Seguros y Reaseguros |

---

La recopilación de los datos se realizó a partir del análisis de contenido de los informes anuales publicados en los sitios web de las empresas y del informe 20 F en el caso de las empresas emisoras en Estados Unidos reguladas por SEC. La medición sobre el alcance de las revelaciones se realizó tomando como referencia el índice de divulgación propuesto.

### 3.2.2. Índice de Divulgación de Información sobre Ciberseguridad propuesto

Si bien los estudios previos relacionados con la divulgación sobre Ciberseguridad en su mayoría han utilizado el conteo de palabras y el análisis textual, en esta investigación hemos optado por la construcción de un índice de divulgación. Coincidimos con Marston & Shrives (1991) respecto a que medir la revelación de información contando elementos de datos no es una solución satisfactoria al problema de investigación, porque hay repeticiones de ciertos datos, números y palabras en los informes anuales y demás medios de revelación de información organizacional. La revisión de la literatura corrobora cómo el análisis de contenido es la metodología que prevalece sin importar la técnica utilizada para la recopilación de la información. Según Berelson (1952), ésta pretende ser objetiva, sistemática y cuantitativa en el estudio del contenido manifiesto de las comunicaciones, su uso en la evaluación de las revelaciones de Ciberseguridad se presenta en (Berkman et al., 2018; Eijkelenboom & Nieuwesteeg, 2021; Gao et al., 2020; Gordon et al., 2006; Gordon et al., 2010; Héroux & Fortin, 2020; Lernia et al., 2020; Li et al., 2018; Morse et al., 2017; Radu & Smaili, 2021). Estas investigaciones en su mayoría evalúan la información reportada sobre Ciberseguridad por parte de las empresas cotizadas en los informes presentados a SEC.

**Tabla 8. Investigación previa bajo la técnica del análisis de contenido**

| Autores | País | Palabras clave | Metodología aplicada |
|---|---|---|---|
| (Gordon et al., 2006) | Estados Unidos | Efecto de la Ley Sarbanes Oxley, divulgación de información de riesgos. | Análisis de contenido (palabras clave) |
| (Gordon et al., 2010) | Estados Unidos | Medida de seguridad, autenticación, cifrado, virus informático, violación de seguridad, recuperación ante desastres, seguridad de la información, red o computadora, control de acceso, intrusión, continuidad del negocio, gestión de seguridad, hacker, monitoreo de seguridad, denegación de servicio, seguridad cibernética, violación de la computadora, intrusión informática. | Metodología de relevancia de valor debido a que la divulgación de la seguridad de la información es parte de un paquete que incluye otras divulgaciones presentadas ante la SEC. La medida de divulgación utilizada a través de las palabras clave es original. |
| (Berkman et al., 2018) | Estados Unidos | La medida de divulgación de Ciberseguridad específica de la empresa | Metodología Examinan el efecto de la conciencia de la |

| | | | |
|---|---|---|---|
| | | se basa en una puntuación obtenida del análisis textual de las divulgaciones 10-K. Se complementa con la lista de NICCS incluye leyes relacionadas con la Ciberseguridad. | Ciberseguridad en la valoración del mercado utilizando el Modelo de Ohlson. |
| Li et al., 2018 | Estados Unidos | En este estudio de forma manual ubican primero los factores de riesgo individuales del punto 1A y luego identifican los factores de riesgo relacionados con la seguridad en las presentaciones 10 K. | Examinan la utilidad de los factores de riesgo relacionados con la seguridad cibernética divulgado en presentaciones 10-K. |
| (Gao et al., 2020) | Estados Unidos | Toma como base diccionario de palabras de (Loughran & Mcdonald, 2011). | En este estudio, se realiza un estudio longitudinal del contenido y las características lingüísticas de las prácticas de divulgación de riesgos de Ciberseguridad de las empresas públicas, así como de los factores que pueden impulsar las tendencias de divulgación. |
| (Héroux & Fortin, 2020) | Canadá | El índice se compone de cuarenta elementos, los cuales toman el valor de uno si la información pública está disponible y, cero en caso contrario. | Aplicación y medición de índice autoconstruido. |
| (Leo, 2020) | Internacional Bancos GSIB | Búsqueda de palabras clave: tecnología, operación, BCP, seguridad, resiliencia, subcontratación, nube y pandemia.<br>Analiza hasta qué punto los bancos, a saber, los GSIB, han hecho revelaciones, en sus informes anuales, con respecto a la resiliencia operativa sobre si las empresas hacen revelaciones sobre la resiliencia operativa en sus informes anuales y, de ser así, en qué medida. | Se realizó un análisis de frecuencia de términos relacionados con la resiliencia operativa, seguido de una evaluación para comprender la existencia de relaciones entre estos términos. |
| (Lernia et al., 2020) | Australia | Realiza un análisis de contenido en torno al primer Estándar Prudencial sobre Seguridad de la Información para entidades reguladas, y en vista de un estudio realizado por ASX. | Análisis de contenido. |
| (Calderon & Gao, 2021) | Estados Unidos | Utiliza la medida de divulgación (Gordon et al., 2010) | Metodología de mapeo de dominios y enfoque general para identificar, categorizar y clasificar las divulgaciones de Ciberseguridad. |
| (Eijkelenboom & Nieuwesteeg, 2021) | Países Bajos | Utiliza las siguientes palabras: Ciber (incluidos los términos más específicos Ciberseguridad y riesgo cibernético), Seguridad de información, Protección de Datos.<br>Verifican la información sobre medidas de Ciberseguridad específicas mediante | Análisis de contenido – conteo de palabras |

| | | | |
|---|---|---|---|
| | | la búsqueda de la siguiente selección de palabras clave: autenticación de dos o varios factores, prueba de penetración, monitoreo de red, compartimentación de la red y Seguro cibernético | |
| (Morse et al., 2017) | Estados Unidos | Análisis de contenido a partir de los factores de riesgos divulgados a partir de la Guía SEC 2011. | Examina las pautas y las divulgaciones de seguridad cibernética en el contexto de las leyes existentes que rigen la regulación de valores. |
| (Radu & Smaili, 2021) | Canadá | A partir de un conteo de las palabras clave "ciber" (incluidas en riesgo y divulgación cibernéticos), "Ciberseguridad", "ciberataque" y "seguridad de la información" identifican todos los párrafos de los informes anuales relacionados con la Ciberseguridad, y con una búsqueda manual se comprueban la verificación de la validez de cada párrafo identificado. | Metodología modelo de regresión lineal múltiple para probar la asociación entre la divulgación de Ciberseguridad y la diversidad de género de la Junta. |

En octubre de 2011, la SEC emitió nuevas pautas para la divulgación de riesgos de seguridad cibernética. Algunas empresas respondieron a estas pautas emitiendo nuevas divulgaciones de factores de riesgo. Este artículo examina las pautas y las divulgaciones de seguridad cibernética en el contexto de las leyes existentes que rigen la regulación de valores. Luego examina los resultados empíricos de las divulgaciones de las empresas siguiendo las nuevas pautas. La evidencia muestra que una proporción relativamente pequeña de empresas optó por modificar sus divulgaciones de factores de riesgo, y la mayoría de las empresas optaron por no divulgar ningún riesgo de Ciberseguridad específico. Además, las empresas divulgadoras generalmente experimentaron efectos negativos significativos en el precio del mercado de valores debido a la realización de nuevas divulgaciones. En lugar de ver la divulgación como una señal positiva de la atención de la gerencia, los inversores aparentemente la vieron como una señal de advertencia.

A continuación, la Tabla 9 presenta los dos estudios previos que proponen antecedentes importantes para la construcción del Índice de Divulgación sobre Ciberseguridad. El primero, corresponde al elaborado de forma consecutiva por E&Y (2018; 2019; 2020), esta firma internacional ha analizado las divulgaciones relacionadas con la

Ciberseguridad en las declaraciones y presentaciones del Formulario 10-K de las compañías Fortune 100 para identificar tendencias y desarrollos emergentes. El segundo estudio, de Héroux & Fortin (2020), ha sido elaborado con base en las pautas de los reguladores financieros de empresas que cotizan en el índice S & P / TSX 60 de la Bolsa de Valores de Toronto (TSX).

**Tabla 9. Instrumentos de divulgación en estudios previos de Ciberseguridad**

| Autores | País | Dimensiones | Metodología aplicada |
|---|---|---|---|
| (E&Y, 2018; 2019; 2020) | Estados Unidos Lista Fortune 100 | El instrumento de medición se compone de tres dimensiones: Supervisión de la Junta (Supervisión de riesgos (1), Nivel de directorio (3), Gestión para la elaboración de informes (2), Manejo de la frecuencia de informes (2)). Declaraciones sobre riesgo de Ciberseguridad (divulgación de factores de riesgo). Gestión de riesgos (esfuerzos de gestión riesgos de Ciberseguridad (3). Educación y entrenamiento (1) | Análisis de contenido |
| (Héroux & Fortin, 2020) | Canadá | El índice se compone de cuarenta elementos, distribuidos en siete categorías: (i) factores de riesgo (4 ítems); (ii) impactos potenciales (11 ítems); (iii) responsabilidad de la estrategia de Ciberseguridad (6 ítems); (iv) mitigación de riesgos (11 ítems); (v) posibles incidentes de Ciberseguridad (2 elementos); (vi) incidentes reales de Ciberseguridad (3 elementos); y (vii) otros elementos de Ciberseguridad divulgados (3 elementos). Elaborado con base en (CSA, 2017; SEC, 2018b). | Aplicación y medición de índice autoconstruido elaborado con base en las pautas de los reguladores financieros de empresas que cotizan en el índice S & P / TSX 60 de la Bolsa de Valores de Toronto (TSX). Se evalúo el alcance general y la ubicación de la divulgación sobre Ciberseguridad en los informes anuales y demás comunicaciones de cada empresa emisora. |

Nota: Elaborado con base en consulta de bases de datos Web of Science y Scopus, diciembre de 2021.

En el presente estudio, hemos optado por un índice no ponderado para impedir la arbitrariedad inherente al uso de cualquier índice ponderado referida por Giner (1997), y basándonos en el supuesto de que cada elemento divulgado tiene la misma importancia (Cooke & Wallace, 1989). En cualquier caso, se ha de tener en cuenta que, según Choi (1973) y Chow & Wong-Boren (1987), los estudios que utilizan índices ponderados y no ponderados obtienen resultados similares.

**Tabla 10. Índice de Divulgación de Ciberseguridad**

| **Gobernanza** (CSA, 2017; E&Y, 2020; TCFD, 2021) | |
|---|---|
| G1. Describe la participación de la Junta Directiva en la supervisión de los riesgos y oportunidades relacionados con la Ciberseguridad | (E&Y, 2020; Héroux & Fortin, 2020b;SEC, 2018b). |
| G2. Revela la existencia de un comité a nivel de directorio encargado específicamente de la Ciberseguridad y/o seguridad de la información | (E&Y, 2020) |
| G3. Revela la existencia de un comité encargado de supervisar la Ciberseguridad diferente al Comité de Auditoría, p. tecnología, riesgos | (E&Y, 2020; Héroux & Fortin, 2020a) |
| G4. Revela la supervisión de los asuntos de seguridad cibernética por parte de un Comité de Auditoría | (E&Y, 2020; Héroux & Fortin, 2020a; AICPA, 2018) |
| G5. Informa sobre la contribución de la dirección al diseño y evaluación del sistema de gestión de riesgos de seguridad de la información de la organización | (TCFD, 2021) |

| **Estrategia** (Héroux & Fortin, 2020a;TCFD, 2021) | |
|---|---|
| E1. Difunde la formulación de una(s) política(s) de Ciberseguridad destinadas a gestionar la seguridad de la información | (TCFD, 2021) |
| E2. Revela la existencia de un sistema de gestión de la seguridad en la organización | (AICPA, 2017b) |
| E3. Revela que el sistema de gestión de la seguridad de la información se establece de acuerdo con normas y estándares reconocidos internacionalmente | (La normativa nacional en algunos países exige la aplicación de estos estándares en algunos sectores) |
| E4. Revela la existencia de una política de protección de datos personales y/o garantía de los derechos digitales | (Héroux & Fortin, 2020b) |
| E5. Revela la aplicación de estrategias de concientización y capacitación en Ciberseguridad para los miembros de la organización para mitigar el riesgo de Ciberseguridad | (E&Y, 2020; Héroux & Fortin, 2020b) |
| E6. Revela la existencia de procedimientos de comunicación que brindan información sobre Ciberseguridad a los tomadores de decisiones, clientes, empleados, otros participantes del mercado y reguladores, según corresponda | (OCIE, 2020) |

| **Gestión de riesgos** (E&Y, 2020) | |
|---|---|
| R1. Presenta una descripción de los riesgos de Ciberseguridad y/o seguridad de la información | (Héroux & Fortin, 2020b; AICPA, 2017b) |
| R2. Incluye la protección de datos como tema material | (RobecoSAM, 2018) |
| R3. Incluye la Ciberseguridad y/o seguridad de la información como factor de riesgo | (RobecoSAM, 2018) |
| R4. Incluye la privacidad de datos como factor de riesgo | (SEC, 2018b) (E&Y, 2018) (CPMI-IOSCO, 2016) |
| R5. Incluye la privacidad de datos como factor de riesgo | (SEC, 2018b; E&Y, 2018) |
| R6. Revela el riesgo de Ciberseguridad dentro de otros riesgos organizacionales | (CPMI-IOSCO, 2016) |
| R7. Informes sobre procedimientos de respuesta a incidentes en los sistemas de información (plan de contingencia) | (CSA ACVM, 2017) |
| R8. Revela el desarrollo de pruebas y monitoreo para validar la efectividad de las políticas y procedimientos de Ciberseguridad | (Division of Corporation Finance & SEC, 2011; Berkman et al., 2018; IOSCO, 2016) |
| R9. Presenta información previa sobre incidentes de Ciberseguridad en curso u otros eventos pasados que pueden ser relevantes como factor de riesgo para la organización | (SEC, 2018b) |
| R10. Revela la frecuencia de los informes de gestión a la Junta o comité | (E&Y, 2020) |
| R11. Revela reclamos relacionados con violaciones de privacidad y pérdida de datos de clientes | (OCIE, 2020) (GSSB, 2016) (OECD, 2011) |
| R12. Informes sobre la participación de la auditoría interna en la gestión del riesgo cibernético y/o seguridad de la información | (E&Y, 2020) |
| R13. Informes sobre la participación de un asesor externo independiente en la mitigación de riesgos de Ciberseguridad | (E&Y, 2020) |

| **Implicaciones Financieras** (SEC, 2018b) | |
|---|---|
| I1. Menciona coberturas de seguros relacionadas con Ciberseguridad o pagos a proveedores de servicios. | (SEC, 2018b) |
| I2. Revela información relacionada con la medición de los esfuerzos continuos en Ciberseguridad. | (SEC, 2018b) |
| I3. Informes sobre la medición de los costes, consecuencias riesgos de los incidentes de Ciberseguridad. | (SEC, 2018b) |

El índice propuesto tiene como objetivo evaluar la divulgación de información sobre Ciberseguridad y ha tenido en cuenta la metodología utilizada en las construcción de índices de divulgación en otras temáticas como (Briano, 2012) y (Clarkson, 2008). Se estructura en cuatro dimensiones, a partir de los siguientes referentes: (i) Gobernanza (TCFD, 2021; CSA, 2017; E&Y, 2020), (ii) Estrategia (Héroux & Fortin, 2020a; TCFD, 2021), (iii) Gestión de riesgos (E&Y, 2020) e, (iv) Implicaciones financieras (SEC, 2018).

La medida de divulgación de Ciberseguridad se basa en 27 elementos individuales, cada uno de los cuales se refiere a un tema particular, asociado a una de las cuatro dimensiones, así: gobernanza (5 elementos), estrategia (6), gestión de riesgo (13), e implicaciones financieras (3).

La selección de los ítems que integran el Índice de Divulgación de Ciberseguridad se realiza a partir de E&Y, (2020), Héroux & Fortin (2020), TCFD (2021) y de algunas investigaciones previas (Berkman et al., 2018; Calderon & Gao, 2021; Eijkelenboom & Nieuwesteeg, 2021; Gao et al., 2020; Gordon et al., 2010; Leo, 2020; Radu & Smaili, 2021). También se han tenido en cuenta los estándares internacionales relacionados con el manejo del sistema de información corporativo. Concretamente, la familia de estándares ISO 27000, las guías SEC (2011; 2018), el Reglamento General de Protección de Datos de la Unión Europea y otros documentos propuestos por entidades con amplio reconocimiento internacional, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), el Banco Interamericano de Desarrollo (BID), la Organización de Estados Americanos (OEA) y la Iniciativa de Reporte Global (GRI), entre otros.

En este índice, si la empresa divulga un ítem de información en el informe anual se le asigna el valor de "1", y si no lo divulga se le asigna el valor de "0". La puntuación de divulgación de Ciberseguridad se obtiene del cociente entre la suma de los puntos conseguidos respecto a la totalidad de los puntos que podía haber obtenido la empresa si hubiera difundido el máximo de ítems.

El Índice de Divulgación de Ciberseguridad no ponderado para cada empresa se expresa de la siguiente manera:

$$IDC = \frac{\sum_{i=1}^{t} c_i}{t}$$

Donde $c_i = 0$ o 1 de acuerdo con las siguientes condiciones:
$c_i = 0$ Si no se encontró el elemento de divulgación,
$c_i = 1$ Si se encontró el elemento de divulgación.
$t =$ El número máximo de elementos de divulgación de Ciberseguridad que una empresa podría divulgar.

A continuación, se presenta la composición del Índice de Divulgación de Ciberseguridad, por cada dimensión:

***Dimensión 1. Gobernanza***

En esta primera dimensión se recomienda divulgar el papel del Gobierno Corporativo en torno a los riesgos y oportunidades relacionados con la Ciberseguridad. La gobernanza de la Ciberseguridad, como parte de la gobernanza de la seguridad de la información, es el proceso de dirigir y controlar la protección de los activos de información digital de una empresa frente a los riesgos relacionados con el uso de Internet (Von Solms & Von Solms, 2018). ISO/IEC 27014 (2020) la define como el sistema mediante el cual se dirigen y controlan las actividades de seguridad de la información de una organización. Por lo tanto, cuando se trata de la gobernanza de la seguridad cibernética, lo más importante que puede hacer una Junta es establecer el tono correcto y alinear el apetito de riesgo apropiado relacionado con la seguridad cibernética con la administración. Es probable que la evaluación de riesgos y el desarrollo de principios de mitigación para gestionarlos sean efectivos, siempre que exista una política de gobernanza bien comunicada y coordinada dentro del sistema que se gestiona (CyBOK, 2019). En su enfoque, deben participar la Junta Directiva, la gerencia, los líderes de las unidades de negocios y los grupos de seguridad y TI (PWC, 2018). Todos los involucrados en la operación diaria del sistema en cuestión deben entender que para que la seguridad sea efectiva, debe ser parte de la cultura operativa diaria (CyBOK, 2019). En este contexto, las partes interesadas quieren comprender mejor cómo las empresas se preparan y responden a los incidentes de seguridad cibernética, así como también cómo las juntas directivas supervisan estos esfuerzos críticos de gestión de riesgos (E&Y, 2018).

Al respecto, la Guía de Divulgación de Seguridad Cibernética (SEC, 2018) establece cómo la divulgación sobre la participación de la Junta en la supervisión del proceso de gestión de riesgos debe proporcionar información importante para los inversores sobre cómo una empresa percibe el papel de la Junta, y la relación entre la Junta Directiva y la alta dirección en la gestión de las amenazas materiales a las que se enfrenta. De acuerdo

con E&Y (2018), también es de interés para los inversionistas saber si el directorio en pleno está a cargo de la supervisión, la comparte entre los diferentes comités de auditoría, riesgos y tecnología, o crea un comité que se dedique exclusivamente a la Ciberseguridad. Según Ernst & Young (2019) las funciones de supervisión de la Junta incluyen solicitar a la gerencia que revise las divulgaciones de seguridad cibernética durante los últimos dos o tres años con evaluación comparativa.

***Dimensión 2. Estrategia***

En esta dimensión se revelan los efectos de ls amenazas del riesgo cibernético en las organizaciones. Bajo este marco, una estrategia cibernética personalizada, dirigida por el negocio y basada en amenazas, permite a las organizaciones centrarse en las debilidades de seguridad y reducir la probabilidad de daños financieros o de reputación en el futuro (Deloitte, 2021a). Teniendo en cuenta que dos de las principales responsabilidades de la Junta son la estrategia y la gestión de riesgos de Ciberseguridad (Ernst & Young, 2019), el índice propuesto define ´la estrategia´ y ´la gestión de riesgos´ como dos dimensiones temáticas que representan los elementos de cómo operan las organizaciones (TCFD, 2021). En este aparte, se presenta la dimensión de estrategia de Ciberseguridad orientada al negocio como el paso más importante para los líderes de la seguridad en medio de la digitalización acelerada del negocio (PWC, 2021).

Desde esta perspectiva, la guía de divulgación SEC (2018) destaca la importancia de mantener políticas y procedimientos integrales relacionados con los riesgos e incidentes de Ciberseguridad, y AICPA (2017) ratifica la opción de revelar en los informes corporativos una descripción narrativa que incluya estas políticas clave de seguridad y los procesos implementados y operados para proteger la información y los sistemas contra esos riesgos.

Según AICPA (2017), los esfuerzos de gestión han llevado al desarrollo de numerosos marcos de gestión de riesgos cuyo objetivo es proporcionar orientación a las organizaciones sobre cómo gestionar el riesgo de Ciberseguridad (por ejemplo, ISO / IEC

27001, Marco de Ciberseguridad del NIST). Desde esta perspectiva, las empresas intentan diseñar e implementar programas eficaces, situación que amerita ser comunicada a las partes interesadas. De acuerdo con Ernst & Young (2019), la capacitación y la evaluación se convierten también en controles y procesos que también protegen sus operaciones.

***Dimensión 3. Gestión de Riesgos de Ciberseguridad***

En esta dimensión se sugiere divulgar cómo la organización identifica, evalúa y gestiona los riesgos relacionados con la Ciberseguridad. La gestión de riesgos es la práctica de utilizar procesos, métodos y herramientas para gestionar estos riesgos. Para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para lograr sus objetivos organizacionales y pueden expresar esto como su tolerancia al riesgo (NITS, 2018). De hecho, las políticas y procedimientos de divulgación deben garantizar que la información sobre los riesgos e incidentes de Ciberseguridad se procese y divulgue (PWC, 2018). Comprender la información transmitida por las divulgaciones de riesgos de Ciberseguridad es importante, ya que puede ayudar a los inversores a evaluar el riesgo de Ciberseguridad de una empresa y proporcionar a los reguladores información sobre si son necesarias normas legislativas adicionales para alentar a las empresas a divulgar más sobre sus riesgos de Ciberseguridad (Li et al., 2018).

El objetivo de proporcionar información a revelar sobre los factores de riesgo es discutir los elementos más importantes que hacen que la empresa sea riesgosa (SEC, 2005b). De hecho, las políticas y procedimientos de revelación deben garantizar que la información sobre los riesgos e incidentes de Ciberseguridad se procese y divulgue (PWC, 2018). El monitoreo regular de los controles de seguridad de la información puede mejorar la efectividad general del programa de seguridad de la información de una organización (Ransbotham & Mitra, 2009). Las empresas deben divulgar los incidentes cibernéticos materiales conocidos que ya ocurrieron, y discutir los costos y consecuencias potenciales (Gao et al., 2020). NIST (2020), define un incidente de Ciberseguridad como

un suceso que pone en peligro real o inminente, sin autoridad legal, la integridad, confidencialidad o disponibilidad de información de un sistema de información, o bien, constituye una violación o amenaza inminente de violación de la ley, las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.

Respecto a la protección de la privacidad del cliente, es un objetivo reconocido generalmente en la legislación nacional y políticas de las organizaciones (GRI 418-1, 2016). Como se estipula en las Líneas Directrices de la OCDE para Empresas Multinacionales de la Organización para la Cooperación y el Desarrollo Económico, se espera que las organizaciones respeten la privacidad de los consumidores y adopten medidas razonables para garantizar la seguridad de los datos de carácter personal que recaban, almacenan, procesan o difunden. La función de auditoría interna puede desempeñar un papel importante, tanto para proporcionar garantía con respecto a la seguridad de la información como para generar conocimientos sobre cómo mejorar la seguridad de la información de la organización (Steinbart et al., 2018).

También puede ser útil buscar las aportaciones de especialistas externos en la evaluación de la Ciberseguridad. Las empresas pueden realizar revisiones externas anuales de programas de seguridad y privacidad, incluida la respuesta a incidentes, notificación de incumplimiento, recuperación ante desastres y planes de comunicación de crisis; además, las evaluaciones de seguridad de terceros también pueden proporcionar evaluación comparativa en relación con otras empresas de tamaño similar o en la misma industria (Deloitte, 2015). Los auditores externos funcionan como intermediarios o representan algunos de los grupos con los que el administrador realiza transacciones y, por lo tanto, la seguridad cibernética se ha convertido cada vez más en parte de la conversación con estos actores (Kiesow Cortez & Dekker, 2022).

***Dimensión 4. Implicaciones Financieras***

En esta última dimensión se propone revelar el real y el potencial impacto financiero de los riesgos relacionados con la Ciberseguridad en los negocios de la organización. En este

sentido, es fundamental que las juntas directivas comprendan desde la gerencia de riesgo, la probabilidad de que ocurra el riesgo y la estimación del costo financiero de los daños que resultarían (Ernst & Young, 2019). La Ciberseguridad, así como las amenazas físicas a la infraestructura de la red, pueden tener importantes repercusiones económicas. Invertir en seguridad de datos y actualizar la infraestructura de la red es, por lo tanto, crucial (RobecoSAM, 2018; SEC, 2018). Se espera que las empresas revelen los riesgos e incidentes de Ciberseguridad que son importantes para los inversores, incluidas las consecuencias financieras, legales o de reputación concomitantes. El seguro de Ciberseguridad ayuda a las empresas a transferir una parte del riesgo potencial y la exposición asociados con los incidentes de Ciberseguridad (Radu & Smaili, 2021).

## Validación del Índice de Divulgación de Ciberseguridad

Para validar la consistencia de este índice se ha calculado el coeficiente Alfa de Cronbach, utilizando la matriz de correlación para comprobar la fiabilidad de los ítems del instrumento. De acuerdo con los valores incluidos en la Tabla 11, este coeficiente arroja un resultado de 0.8168, lo que confirma que el Indice de Divulgación de Ciberseguridad es confiable y consistente con los ítems seleccionados de la muestra.

**Tabla 11. Alfa de Cronbach**

| Dimensión | Obs. | Señal | Correlación ítem-prueba | Correlación artículo-resto | Correlación promedio entre ítems | Alfa |
|---|---|---|---|---|---|---|
| Gobernanza | 425 | + | 0.8104 | 0.6485 | 0.5197 | 0.7645 |
| Estrategia | 425 | + | 0.8182 | 0.6614 | 0.5113 | 0.7584 |
| Riesgo | 425 | + | 0.862 | 0.7358 | 0.4644 | 0.7223 |
| Financiero | 425 | + | 0.7229 | 0.5119 | 0.6133 | 0.8263 |
| Escala de prueba | | | | | 0.5272 | 0.8168 |

## 3.3. Análisis de la Divulgación de Información sobre Ciberseguridad en Empresas Latinoamericanas

Con base en el Índice de Divulgación de Ciberseguridad propuesto , realizamos un estudio sobre el nivel de divulgación de información sobre Ciberseguridad en las empresas de América Latina. A partir de su aplicación y análisis, resulta interesante conocer el grado de divulgación de información sobre Ciberseguridad y cómo ha evolucionado, en función de la dimensión del índice, en empresas de distintos países y sectores de Latinoamérica.

Si bien en el ámbito organizacional las empresas de América Latina no refieren una normativa exclusiva para la divulgación de información de Ciberseguridad en el informe corporativo anual, las diferentes regulaciones expedidas por los entes de vigilancia y control sobre Gobierno Corporativo, gestión de riesgos y aplicación vinculante de estándares internacionales sobre seguridad de la información (como ISO 27001), se han convertido en temas objeto de divulgación corporativa en la región. Las empresas cotizantes de Latinoamérica que participan en el mercado bursátil estadounidense, también reportan en el informe anual 20 F ítem 3D los factores de riesgo relacionados con el riesgo cibernético de acuerdo con SEC (2018).

Otro referente para América Latina que puede haber generado un aumento en la divulgación de Ciberseguridad, lo constituye la adaptación del modelo europeo de las normas relacionadas con la protección de la privacidad de datos por parte de las empresas emisoras. En este sentido, también podemos mencionar cómo desde los estándares GRI se promueve la divulgación sobre Ciberseguridad, específicamente con el estándar GRI 418 Privacidad del cliente.

Bajo este contexto, proponemos la siguiente hipótesis de estudio que será contrastada mediante análisis empírico:

***H1:*** *Existe una tendencia creciente en el nivel de divulgación de información sobre Ciberseguridad en empresas latinoamericanas.*

Según Barry et al. (2021), el entorno institucional de la Ciberseguridad difiere enormemente de un país a otro. En este sentido, los avances relacionados con seguridad cibernética en América Latina varían entre países, como lo ilustraban las Figuras 6 y 7. Estas diferencias institucionales reflejan una transferencia del riesgo de Ciberseguridad entre gobiernos y empresas (Falco et al., 2019). En este sentido, y desde la teoría institucional podemos señalar que existen diversos factores que determinan el comportamiento respecto al manejo del riesgo cibernético en el ámbito nacional, efecto que se traslada a las empresas. Scott (2008) aduce que el marco institucional conduce a diferentes acciones y estrategias organizacionales para obtener legitimidad. En esta línea, la divulgación de información de las empresas de diferentes países se ve afectada por factores institucionales, como lo corroboran Barry et al. (2021), Clarkson et al., (2008), García-Sanchez et al., (2016), Haniffa & Cooke, (2005) y Holland & Foo, (2003).

Respecto a la divulgación de Ciberseguridad en América Latina, la normativa no precisa la revelación de información en el reporte anual. No obstante, diferentes regulaciones de orden nacional obligan el informe de incidentes de Ciberseguridad ante las autoridades establecidas y otras normas sobre Gobierno Corporativo y gestión del riesgo cibernético. Especialmente en el sector financiero, puntualizan el manejo de riesgos operativos y de Ciberseguridad. En algunos países, para las empresas de ciertos sectores se hace obligatorio adoptar los estándares de la Organización Internacional de Normalización ISO 27000 o normas como del Instituto Nacional de Estándares y Tecnología NITS de Estados Unidos, entre otras. Además, con base en el modelo europeo, también se han adoptado normas relacionadas para la protección de la privacidad de datos. Cabe pensar, por tanto, que este entorno normativo pueda tener un efecto en el aumento de la divulgación en los informes anuales corporativos.

A continuación, se presenta un resumen de la normatividad vigente relacionada con Ciberseguridad en cada uno de los países objeto de este estudio (Tabla 12).

**Tabla 12. Normativa relacionada con Ciberseguridad en los países objeto de estudio**

| País | Normativa |
|---|---|
| Argentina | Estrategia Nacional de Ciberseguridad 2019<br>Código de mejores prácticas de las organizaciones para la República de Argentina<br>(divulgación de riesgos no financieros).<br>Comunicación A7266 (2021) Respuesta y recuperación ante ciber incidente para sector financiero (manejo de riesgo de Ciberseguridad).<br>Ley 25326 de 2000 Habeas Data y Provisión 60 E/2016 que regula la transferencia de datos personales entre fronteras. |
| Brasil | Estrategia Nacional de Ciberseguridad. Decreto 222 de 2020<br>ABNTNBR ISO/IEC 27001 de 2006 Metodología de gestión de seguridad de la información y comunicación para la Administración Pública Federal directa e indirecta.<br>Ley 13.709 de 2018 Ley General de Protección de Datos |
| Colombia | Estrategia Nacional de Ciberseguridad 2011 – 2016<br>Nuevo Código País<br>Circular Externa 29 de 2014. Modificada por la Circular Externa 7 de 2018.<br>Modelo Nacional de Gestión de Riesgo Digital<br>Ley de Protección de Datos Personales Ley 1581 de 2012 |
| Chile | Estrategia Nacional de Ciberseguridad 2017<br>RAN Bancos CMF Recopilación actualizada de normas de bancos – Capítulo 20<br>NSG 454 de 2021 Instrucciones en manejo de riesgo operacional y Ciberseguridad<br>Manejo de riesgo.<br>Ley sobre Protección de la vida privada 19.628 de 1999 |
| México | Estrategia Nacional de Ciberseguridad 2017<br>Circular Única de Bancos<br>Código de Principios y Mejores Prácticas de Gobierno Corporativo<br>Ley Federal de Protección de Datos Personales en posesión de los particulares<br>Ley General de Protección de Datos personales en posesión de sujetos obligados |
| Perú | Código de buen Gobierno Corporativo para las sociedades peruanas (principio 25 y 28)<br>Resolución ministerial PCM. Uso obligatorio de la Norma Técnica Peruana ISO NTP 27001: 2014 todas las entidades del sistema nacional de informática.<br>Ley 29733 de Protección de Datos Personales |

Con base en esta información se puede afirmar que, en relación con los países objeto de estudio, excepto Perú, todos cuentan ya con una estrategia nacional de Ciberseguridad. En general, todos han avanzado de forma significativa en la normativa relacionada con Gobierno Corporativo y en la promulgación de una Ley de protección de datos de nivel nacional. De forma particular, en el caso de Argentina se presenta el Código de Mejores Prácticas de las Organizaciones, en el que se contempla la divulgación de riesgos no financieros. Y, por lo que respecta a Brasil y Perú, en ambos se asigna la obligatoriedad del estándar internacional ISO 27001 para la gestión de la seguridad de la información, aunque en Brasil este estándar se aplica para la administración pública, y en Perú para todas las entidades del sistema nacional de informática.

Teniendo en cuenta este contexto, planteamos la siguiente hipótesis:

***H2:*** *Existen diferencias significativas en el nivel de divulgación de información sobre Ciberseguridad entre empresas latinoamericanas de distintos países.*

A partir de la definición de infraestructura crítica dada por *United States Department of Justice (2001),* como el sistema y activos, ya sean físicos o virtuales, tan vitales para cada país que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad económica nacional, la salud y seguridad pública, o cualquier combinación de estos mismos, se entiende que algunos sectores se encuentran más vulnerables al riesgo cibernético que otros. Entre ellos, el sector de comunicaciones, tecnología, energético, financiero y alimentos, entre otros, presentan una amenaza latente. De acuerdo con OEA; ISA (2020) los requisitos de divulgación y presentación de informes de una empresa dependen del tipo de negocio que realiza y del sector en el que opera.

Para el caso de Latinoamérica, de acuerdo al informe IDB OAS (2020), el sector financiero es objetivo frecuente. Es así como la digitalización de esta industria debe tener en cuenta la gestión de ciberdelitos, dado que establecer ambientes digitales implica también analizar riesgos cibernéticos que se deben evitar y manejar adecuadamente (OAS, 2019). Así lo corroboran Porrúa & Contreras (2020), cuando indican que los

ciberataques en la región han ido en aumento, apuntando principalmente a las instituciones financieras de América Latina. Estudios previos (Freedman & Jaggi, 2005; Prado-Lorenzo et al., 2009) evidencian que las empresas de diversos sectores presentan diferencias importantes en el alcance de la divulgación de información no financiera. Bajo este panorama, y con base en el objetivo de nuestro estudio, se plantea la conveniencia de verificar el cumplimiento de la siguiente hipótesis:

***H3:*** *Existen diferencias significativas en el nivel de divulgación de información sobre Ciberseguridad entre empresas latinoamericanas de distintos sectores.*

### 3.3.1. Alcance de las Revelaciones sobre Ciberseguridad por Dimensiones del Índice

La Tabla 13 presenta la puntuación obtenida en cada uno de los 27 ítems que conforman el Índice de Divulgación de Información sobre Ciberseguridad y su evolución durante los cinco años de estudio.

**Tabla 13. Alcance de la divulgación de información en las dimensiones de la Ciberseguridad en Latinoamérica en el período 2016-2020**

| Ítems | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| **Gobernanza** | | | | | |
| G1. Describe la participación de la Junta Directiva en la supervisión de los riesgos y oportunidades relacionadas con Ciberseguridad. | 0,18 | 0,24 | 0,35 | 0,42 | 0,53 |
| G2. Revela la existencia de un comité a nivel de directorio encargado específicamente de la Ciberseguridad y/o seguridad de la información. | 0,11 | 0,16 | 0,16 | 0,19 | 0,24 |
| G3. Revela la existencia de un comité encargado de supervisar la Ciberseguridad diferente al Comité de Auditoría Ej. Tecnología, riesgos. | 0,18 | 0,24 | 0,26 | 0,32 | 0,38 |
| G4. Revela la supervisión de los asuntos de Ciberseguridad por parte de un Comité de Auditoría. | 0,02 | 0,06 | 0,09 | 0,13 | 0,20 |
| G5. Informa sobre la contribución de la dirección en el diseño y evaluación del sistema de gestión de riesgos de seguridad de la información de la organización. | 0,19 | 0,25 | 0,34 | 0,41 | 0,45 |
| | | | | | |

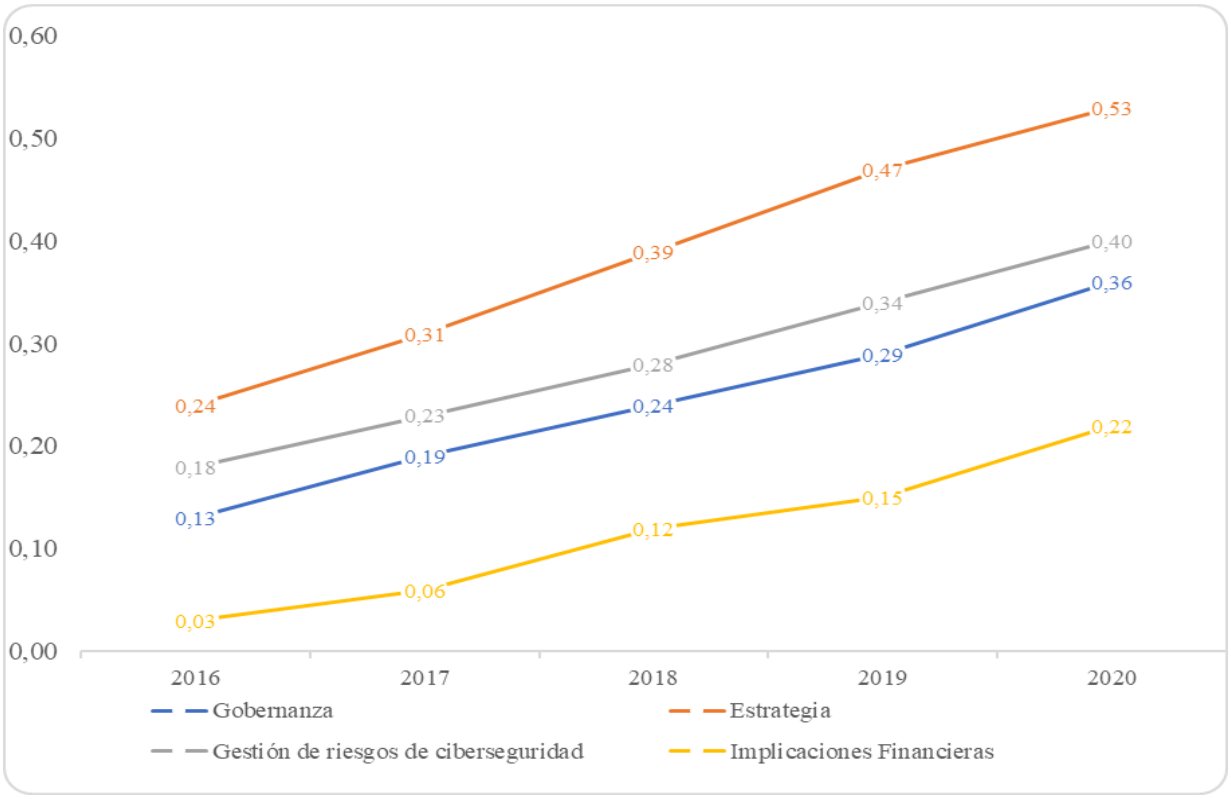
| | | | | | |
|---|---|---|---|---|---|
| **Estrategia** | | | | | |
| E1. Divulga sobre la formulación de una(s) política(s) de Ciberseguridad orientada(s) a gestionar la seguridad de la información. | 0,24 | 0,36 | 0,44 | 0,52 | 0,58 |
| E2. Revela la existencia de un sistema de gestión de la seguridad de la información en la organización. | 0,46 | 0,53 | 0,64 | 0,68 | 0,68 |
| E3. Revela que el sistema de gestión de seguridad de la información se establece de acuerdo con normas y estándares reconocidos en el ámbito internacional. | 0,13 | 0,20 | 0,26 | 0,33 | 0,39 |
| E4. Revela la existencia de una política de protección de datos personales y/o garantía de derechos digitales | 0,19 | 0,24 | 0,34 | 0,42 | 0,48 |
| E5. Divulga sobre la aplicación de estrategias de concienciación y capacitación en Ciberseguridad para los miembros de la organización para mitigar el riesgo de Ciberseguridad. | 0,29 | 0,38 | 0,46 | 0,58 | 0,72 |
| E6. Revela sobre la existencia de procedimientos de comunicación que brindan información sobre Ciberseguridad a los tomadores de decisiones, clientes, empleados, otros participantes del mercado y reguladores, según corresponda. | 0,11 | 0,13 | 0,21 | 0,27 | 0,33 |
| **Gestión de riesgos** | | | | | |
| R1. Presenta una descripción de los riesgos de Ciberseguridad y /o seguridad de la información. | 0,32 | 0,40 | 0,46 | 0,52 | 0,59 |
| R2. Incluye la protección de datos como tema material. | 0,14 | 0,19 | 0,25 | 0,34 | 0,44 |
| R3. Incluye la Ciberseguridad y/o seguridad de la información como tema material. | 0,09 | 0,16 | 0,26 | 0,33 | 0,48 |
| R4. Incluye la Ciberseguridad y/o seguridad de la información como factor de riesgo. | 0,40 | 0,44 | 0,49 | 0,56 | 0,58 |
| R5. Incluye la privacidad de los datos como factor de riesgo. | 0,25 | 0,31 | 0,33 | 0,41 | 0,44 |
| R6. Revela el riesgo de Ciberseguridad dentro de otros riesgos organizacionales. | 0,18 | 0,25 | 0,33 | 0,39 | 0,44 |
| R7. Informa sobre procedimientos de respuesta ante incidencias en los sistemas de información (Plan de contingencias). | 0,15 | 0,18 | 0,19 | 0,24 | 0,36 |
| R8. Revela el desarrollo de pruebas y monitoreo para validar la efectividad de las políticas y procedimientos de Ciberseguridad. | 0,22 | 0,32 | 0,35 | 0,41 | 0,47 |
| R9. Presenta información previa de incidentes de seguridad cibernética en curso u otros eventos pasados que puedan ser relevantes como factor de riesgo de la organización. | 0,06 | 0,15 | 0,19 | 0,18 | 0,24 |
| R10. Se divulga sobre la frecuencia de los informes de gestión a la Junta o comité (s). | 0,02 | 0,06 | 0,07 | 0,11 | 0,14 |
| R11. Revela reclamaciones relativas a violaciones de la privacidad y pérdida de datos del cliente. | 0,31 | 0,35 | 0,38 | 0,42 | 0,45 |
| R12. Informa sobre la participación de la auditoría interna en el manejo del riesgo cibernético y/o de seguridad de la información. | 0,12 | 0,14 | 0,21 | 0,29 | 0,34 |

| | | | | | |
|---|---|---|---|---|---|
| R13. Informa sobre la participación de un asesor externo independiente en la mitigación de riesgos de Ciberseguridad. | 0,04 | 0,09 | 0,14 | 0,16 | 0,26 |
| **Implicaciones Financieras** | | | | | |
| I1. Menciona coberturas de seguros relacionada con Ciberseguridad cibernética o pagos a proveedores de servicio. | 0,06 | 0,12 | 0,18 | 0,20 | 0,28 |
| I2. Revela información relacionada con la medición de los esfuerzos continuos en Ciberseguridad. | 0,02 | 0,04 | 0,12 | 0,19 | 0,21 |
| I3. Se informa sobre la medición de los costos, consecuencias y riesgos de los incidentes de seguridad cibernética. | 0,01 | 0,04 | 0,06 | 0,05 | 0,15 |

En lo que refiere a las dimensiones del Índice de Divulgación de Información de Ciberseguridad, es de mencionar que se observa una importante evolución para las empresas objeto de análisis. En general, en todos los ítems y para todos los años, se observa un aumento en la cantidad de información divulgada, la cual es especialmente significativa en 2019 y 2020.

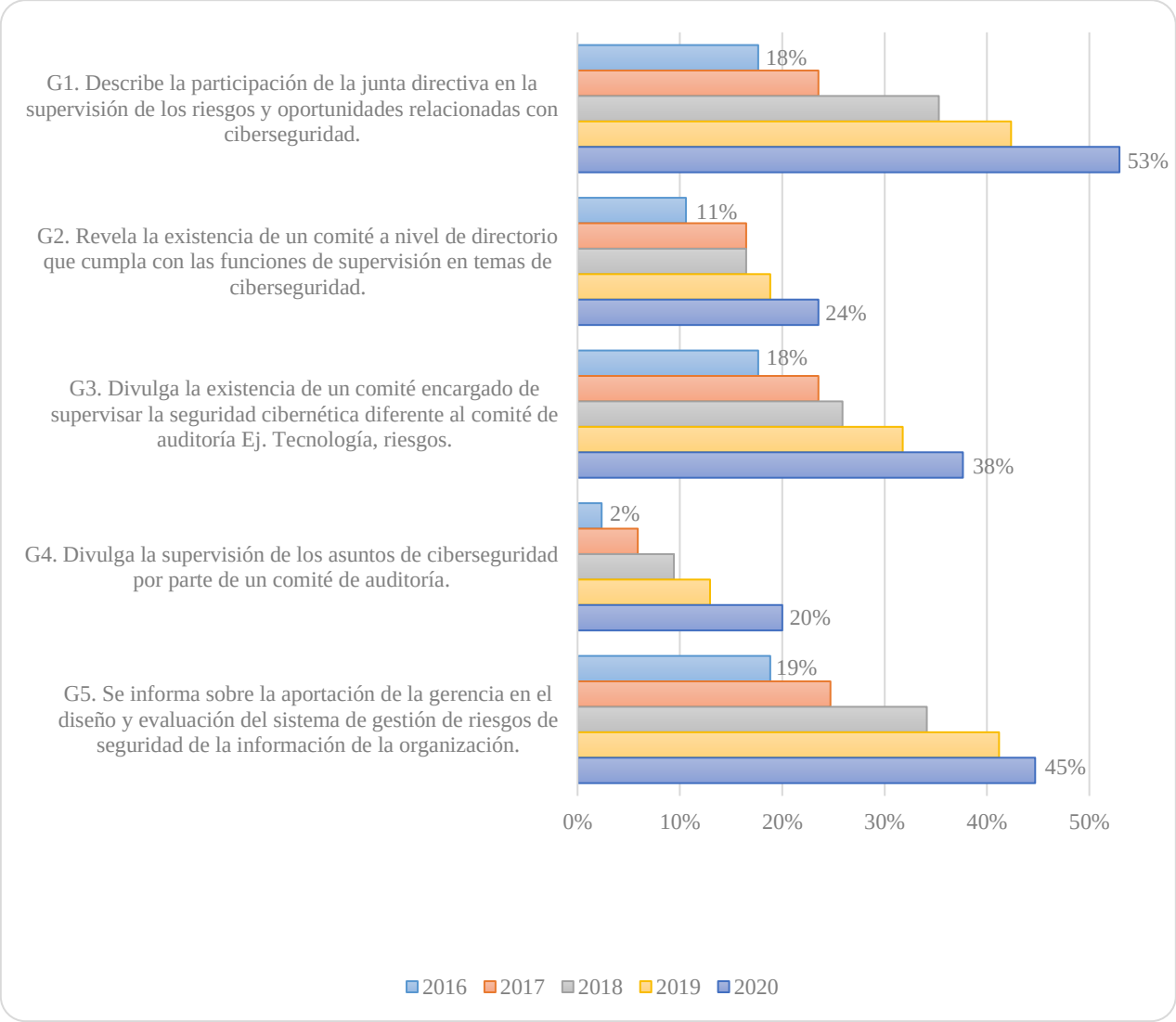
La representación gráfica de la evolución del Índice de Divulgación de Ciberseguridad a nivel de dimensión (Figura 8) permite observar cómo la dimensión del índice que muestra una mayor divulgación en el tema de estudio es la estrategia (53% en 2020), seguida de todas aquellas actividades que sirven y aportan a la gestión de riesgos de Ciberseguridad (40% en 2020). En tercer lugar, se encuentra la gobernanza (36% en 2020) y finalmente, lo que de forma muy limitada se divulga son las implicaciones financieras (22% en 2020).

**Figura 8. Evolución del Índice de Divulgación de Ciberseguridad a nivel de dimensión**




A continuación, la Figura 9 ilustra el alcance de la divulgación de información en los cinco ítems de la dimensión de gobernanza de la Ciberseguridad en Latinoamérica en el período 2016-2020.

**Figura 9. Alcance de la divulgación de información sobre Gobernanza de la Ciberseguridad en Latinoamérica en el período 2016-2020**




En cuanto al alcance de la divulgación de la participación de la Junta Directiva en la supervisión de riesgos relacionados con la Ciberseguridad (G1), el puntaje aumenta de (18%) para 2016 a (53%) para 2020. Estos puntajes reflejan la importante participación que está asumiendo la Junta Directiva en materia de la revelación relacionada con la seguridad y gestión de riesgos de Ciberseguridad.

En cuanto a la divulgación de la existencia de un comité de directorio específicamente encargado de la Ciberseguridad y/o seguridad de la información (G2), se puede observar que su calificación fue de (11%) en 2016 y (24%) en 2020, lo que significa que han llevado a cabo acciones dirigidas en trabajar la Ciberseguridad desde el Gobierno Corporativo mediante la creación de los comités que gestionarán exclusivamente el ciberriesgo.

Sobre la divulgación de la existencia de un comité encargado de supervisar la Ciberseguridad, distinto del Comité de Auditoría, G3 arrojó valores de (18%) en 2016 y (38%) en 2020.

El siguiente ítem, G4, reveló la supervisión de asuntos de Ciberseguridad por parte de un Comité de Auditoría: (2%) en 2016 y (20%) en 2020. Estos resultados muestran que el Comité de Auditoría, en algunos casos, lidera el tema de la Ciberseguridad.

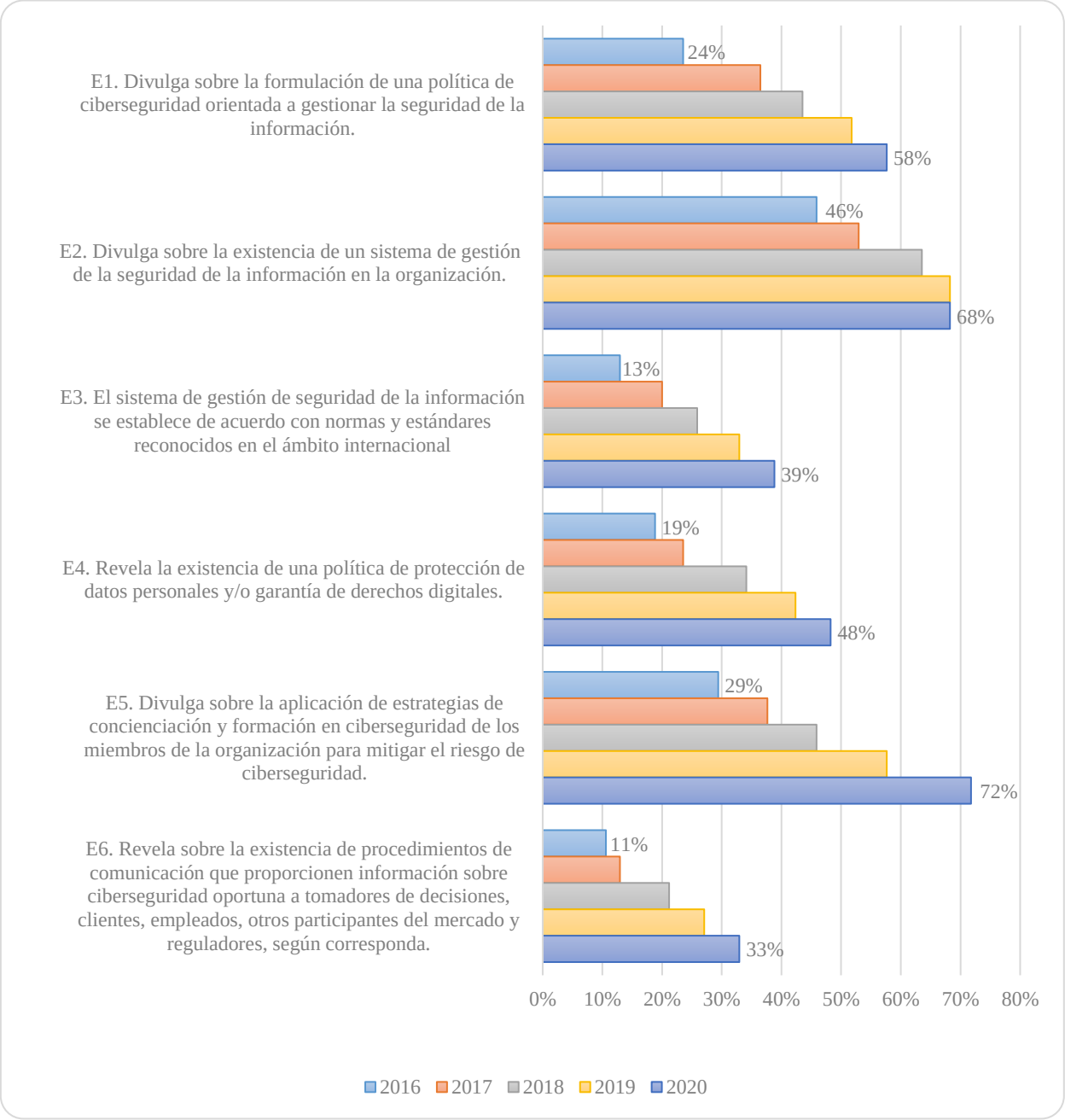
El último ítem de la dimensión de gobernanza informa sobre la contribución de la dirección en el diseño y evaluación del sistema de gestión de riesgos de Ciberseguridad de la organización (G5), presentó un puntaje de (19%) en 2016 y (45%) en 2020, esto demuestra cómo la participación de la gerencia ha sido objeto de mayor divulgación en los últimos años.

Por su parte, en la Figura 10 se evalúan los seis ítems relacionados con la divulgación de información en la dimensión de estrategia. Respecto al alcance de la divulgación de la dimensión de estrategia se puede decir que la estrategia más revelada en 2020 con un porcentaje de (72%) es la concienciación y capacitación sobre Ciberseguridad a los miembros de la organización. Seguida de la existencia de un sistema de gestión de riesgos (68%). En tercer lugar, se revela la información sobre la formulación de una(s) política(s) de Ciberseguridad (58%). Los demás ítems de la dimensión no alcanzan la media. En cuanto a la difusión de la formulación de una(s) política(s) de Ciberseguridad orientada(s) a gestionar la seguridad cibernética (E1) en América Latina, el año 2016 presentó un puntaje de (24%), y 2020 de (58%), pudiendo evidenciar la importancia de las políticas

corporativas de Ciberseguridad. La evaluación del alcance de las revelaciones del siguiente ítem se concentra en la existencia de un sistema de gestión de la seguridad de (SGS) en la organización (E2), y presenta un puntaje de (46%) en 2016 y (68%) en 2020, lo que puede significar que las organizaciones están interesadas en comunicar la implementación y gestión de SMS como estrategia para mitigar el riesgo cibernético. Al mismo tiempo, también buscamos evaluar la divulgación sobre si el sistema de gestión ha sido desarrollado bajo normas y estándares reconocidos internacionalmente (E3). Este ítem reportó una puntuación de (13%) en 2016 y (39%) en 2020 esto significa que las empresas han tomado la iniciativa de acercarse a las prácticas de reconocido valor técnico en el ámbito internacional.

Frente a la divulgación de la existencia de una política de protección de datos personales y/o garantía de los derechos digitales (E4), se observa que este ítem obtuvo una puntuación de (19%) en 2016 y de (48%) en 2020. Como ya se dijo respecto de algunos países en el período de 2016-2020, se han creado leyes relacionadas con la protección de datos, factor que puede promover divulgaciones sobre el tema. Frente a la divulgación sobre la aplicación de estrategias de concientización y capacitación en Ciberseguridad de los integrantes de la organización para mitigar el riesgo de Ciberseguridad (E5) en el 2016 se obtuvo un puntaje de (29%), así como un puntaje de divulgación de (72%) en el 2020. El Ítem E6 también revela la existencia de procedimientos de comunicación que brindan información sobre Ciberseguridad a los tomadores de decisiones, clientes, empleados, otros participantes del mercado y reguladores, según corresponda, y obtuvo una puntuación de 0.

**Figura 10. Alcance de la divulgación de información sobre Estrategia de la Ciberseguridad en Latinoamérica en el período 2016-2020**



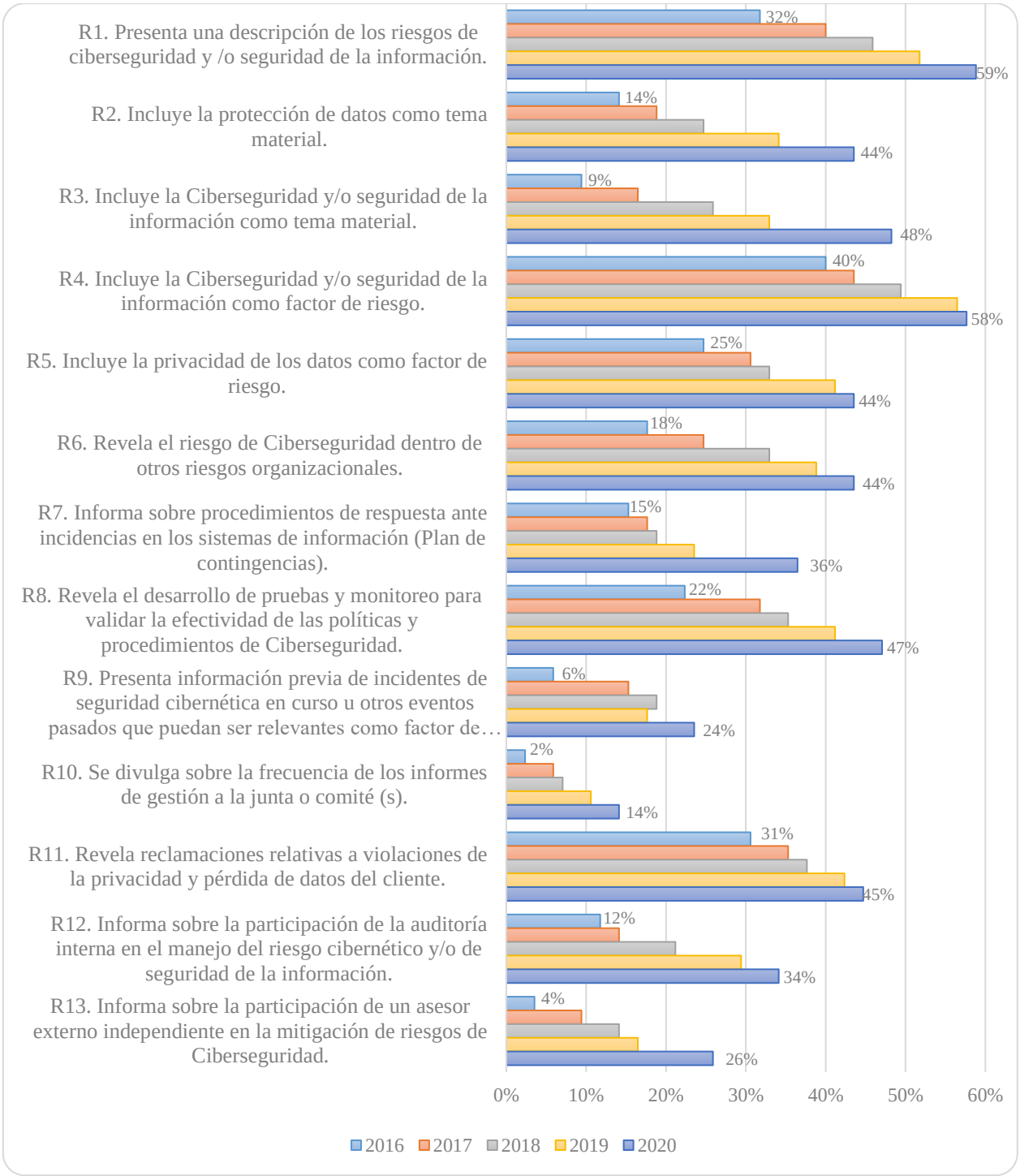

En cuanto a la dimensión de gestión de riesgos de Ciberseguridad (Figura 11), se evaluaron 13 ítems. Se observa que el ítem más revelado corresponde a (R1) la divulgación de la descripción de los riesgos de Ciberseguridad en 2020 con un porcentaje

de 59%. Con un 58% se presenta la revelación que incluye la Ciberseguridad y/o seguridad de la información como factor de riesgo. Los demás numerales en esta dimensión no obtienen un valor superior a la media.

Los resultados por ítem evidencian algunas cuestiones interesantes. Así, el primero de ellos (R1) ofrece una clara provisión creciente para describir los riesgos de Ciberseguridad y/o seguridad de la información, pasando de 32% en 2016 a 59% en 2020. Si bien hubo un aumento en la mayoría de las observaciones, la inclusión de la protección de datos como tema (R2) no alcanzó el promedio en 2020 (44%), de igual forma que la Ciberseguridad y/o seguridad de la información como materia temática (R3) presentó una tendencia creciente, de 9% en 2016 a 48% en 2020, y el factor de riesgo (R4), obtuvo un porcentaje de divulgación en 2020 de 58%. Por su parte, la privacidad de datos como factor de riesgo en las organizaciones (R5) también mostró un incremento que llegó a 44% en 2020.

En esta misma orientación, la divulgación de información de la muestra estudiada reveló un crecimiento del foco en Ciberseguridad en el apartado de supervisión de riesgos (R6) de 18% en 2016 a 44% en 2020. En la divulgación de información sobre procedimientos de respuesta a incidentes en sistemas de información —es decir, la existencia de un plan de contingencia (R7)— hubo un aumento de 21puntos porcentuales, bajo una tendencia creciente de 15% en 2016 a 36% en 2020. Por otro lado, en cuanto a los métodos para evitar vulnerabilidades, hubo un desarrollo creciente, de 22% en 2016 a 47% en 2020, en la ejecución de pruebas y seguimientos para validar la eficacia de las políticas y procedimientos de Ciberseguridad (R8) que implantan las organizaciones.

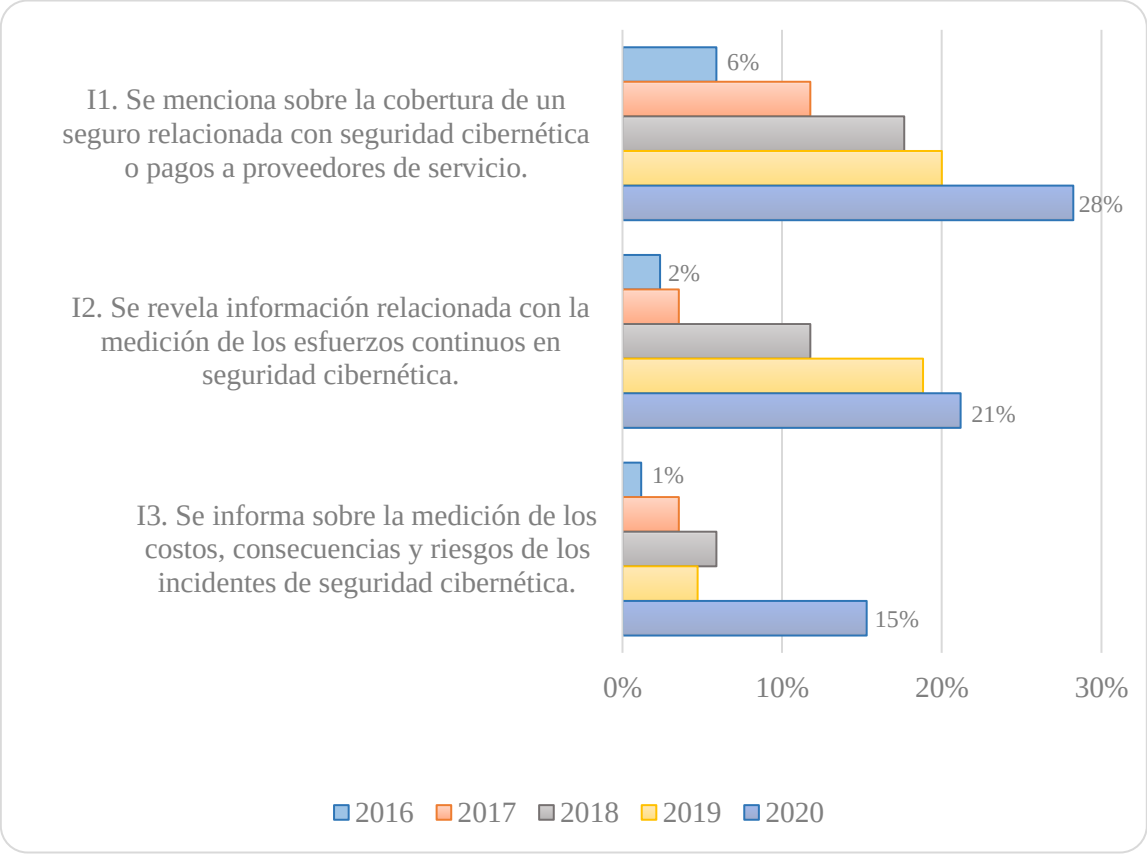
**Figura 11. Alcance de la divulgación de información en Gestión de Riesgos de Ciberseguridad en Latinoamérica en el periodo 2016-2020**



En términos generales, el ítem revelación de información previa sobre incidentes de Ciberseguridad en curso u otros eventos pasados que puedan ser relevantes como factor de riesgo para la organización (R9), en 2016 obtuvo 6%, y su máxima revelación solo alcanzó el 24% en 2020. Respecto a la revelación del ítem que examina la frecuencia de los informes de gestión al directorio o comité (R10), la variación osciló entre 2% para 2016 y 14% para 2020. Reclamos relacionados con violaciones a la privacidad y pérdida de datos de clientes (R11) han pasado de 31% en 2016 a 45% en 2020, con un importante grado de divulgación. En cuanto a la participación de auditoría interna en la gestión del riesgo cibernético y/o seguridad de la información (R12), se divulgó 12% en 2016 y 34% en 2020. Finalmente, se inició la participación de un asesor externo independiente en mitigación de riesgos de Ciberseguridad (R13), comenzando con una puntuación de 4% en 2016 y finalizando con una puntuación de 26% en 2020.

En cuanto a la dimensión de implicaciones financieras (Figura 12), cabe destacar que es la dimensión que presenta un menor alcance de divulgación durante el período de estudio. En cuanto al primer ítem, que tiene que ver con la cobertura de seguros relacionados con la Ciberseguridad o pagos a proveedores de servicios, en 2016 se reportó en 6% y para 2020 en 28%, siendo éste el componente más significativo de los tres analizados. En cuanto al segundo ítem - información relacionada con la medición de esfuerzos continuos en Ciberseguridad - el incremento durante los cinco años ha sido de 19 puntos porcentuales, pasando de 2% en 2016 a 21% en 2020. Finalmente, el ítem con menor divulgación fue la medición de los costos, consecuencias y riesgos de los incidentes de Ciberseguridad, obteniendo únicamente una puntuación de 1% en 2016 y de 15% en 2020. En resumen, se puede decir que la divulgación de las implicaciones financieras de los riesgos de Ciberseguridad en Latinoamérica aumenta en el período de estudio. Sin embargo, dado el efecto material en las cifras de los estados financieros de los esfuerzos continuos en Ciberseguridad, se hace imperante que las organizaciones informen sobre la medición de los costos, consecuencias y riesgos de los incidentes de seguridad cibernética.

**Figura 12. Alcance de las Revelaciones sobre Implicaciones Financieras de la Ciberseguridad en Latinoamérica en el período 2016-2020**




Tomando como referencia el aumento del alcance de las revelaciones de los diez ítems de mayor relevancia del índice de divulgación de información sobre Ciberseguridad (Figura 13), se observa una tendencia creciente generalizada que, en cierto modo, evidencia el esfuerzo de las empresas latinoamericanas por reforzar su seguridad de información y Ciberseguridad durante el período objeto de análisis.

**Figura 13. Alcance de las Revelaciones sobre Ciberseguridad de los diez ítems de mayor relevancia**

En orden de importancia, el ítem más divulgado alcanza el 72% en el año 2020, y se relaciona con la aplicación de estrategias de concienciación de los miembros de la organización en temas de Ciberseguridad (E5). El segundo ítem con mayor reporte de revelaciones corresponde a la existencia de un sistema de gestión de la seguridad de la información (E2) alcanzando 68% en el año 2020. Le siguen el ítem relacionado con la divulgación de la descripción de los riesgos de Ciberseguridad (R1) ocupando el 59%, y la revelación de una política de Ciberseguridad (E1) que, en efecto, logra articularse para gestionar la seguridad de la información alcanzando el 58% en el año 2020. El quinto ítem, relacionado con la inclusión de una política de Ciberseguridad o seguridad de la información como factor de riesgo (R4), también se revela en un alto porcentaje, circunstancia que puede atribuirse a las exigencias de la SEC.

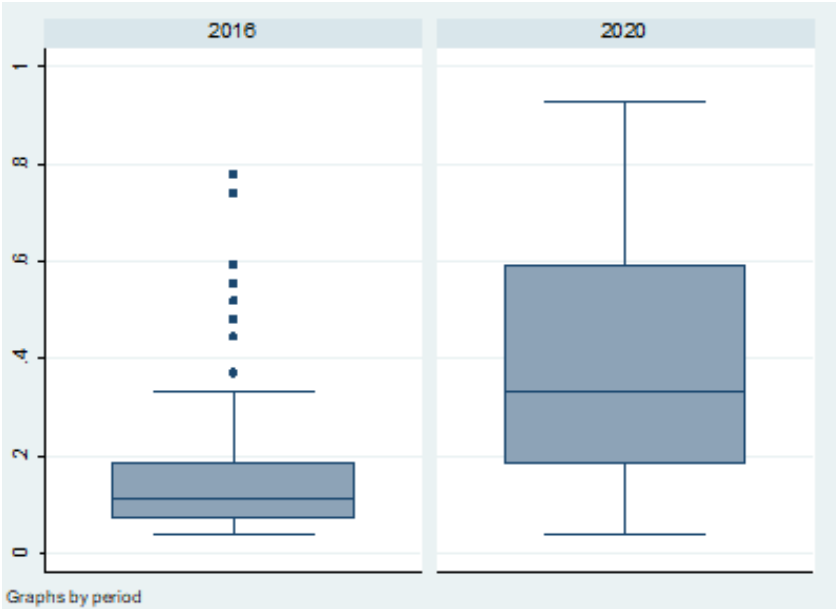
El sexto ítem, correspondiente a la divulgación de la existencia de una política de protección de datos personales y garantía de derechos digitales (E4), muestra también un porcentaje significativo (48% en 2020). En séptimo lugar, se puede observar que las organizaciones de los países estudiados le dan gran importancia (47%) al desarrollo de pruebas y monitoreo de Ciberseguridad (R8), en pro de evaluar las políticas y procedimientos existentes al respeto y reforzarlos en los puntos clave necesarios. En este mismo orden de ideas, la información que se brinda a la gerencia sobre el diseño y evaluación del sistema de gestión de riesgos de seguridad de la información (G5) ocupa el octavo puesto, con un 45% de preponderancia en los países latinoamericanos en el año 2020. Este mismo porcentaje lo presenta el ítem sobre reclamaciones relativas a violaciones de privacidad y pérdida de datos del cliente (R11), este como factor clave para la toma de decisiones relativas a seguridad de la información. Finalmente, en décimo lugar, se encuentra la privacidad de datos como factor de riesgo (R5), que es preocupación de las empresas de Latinoamérica y representa un 44% en el año 2020.

Cabe destacar que la mayoría de los ítems que han experimentado un mayor incremento en su puntuación, y que obtuvieron un mayor porcentaje en 2020, pertenecen a las dimensiones de estrategia y gestión de riesgos, mostrando que las empresas otorgan mayor relevancia a las divulgaciones que participan en acciones de Ciberseguridad

diseñadas a largo plazo cuyo objetivo corresponde a la mitigación del ciberriesgo. En cuanto a la divulgación del año 2020, se observan dos valores importantes, uno de ellos del ítem (E5), que da a conocer la aplicación de estrategias de concientización y capacitación en Ciberseguridad a los miembros de la organización para mitigar el riesgo de Ciberseguridad, y el ítem (E2) que da a conocer la existencia de un sistema de gestión de la seguridad en la organización, con puntuaciones de 0,72 y 0,68, respectivamente.

El análisis descriptivo realizado permite observar que el índice de divulgación de información sobre Ciberseguridad difiere entre los años del periodo analizado, aumentando de forma generalizada y sostenida entre 2016 y 2020. No obstante, para inferir si el índice crece de forma estadísticamente significativa a través del tiempo, es necesario una prueba de diferencia de medianas entre el primer y último año de estudio. Para ello, en principio se grafica sobre el alcance de divulgación de Ciberseguridad entre el primer y el último año del período objeto de estudio, es decir, 2016 y 2020, respectivamente. El rango de los gráficos (Figura 14) parece ratificar la hipótesis del aumento del alcance de divulgación de Ciberseguridad entre el primer y el último año.

**Figura 14. Alcance de la divulgación de información de Ciberseguridad (Índice) 2016 y 2020**




Seguidamente, para confirmar el crecimiento se contrastó una prueba $T$ con las siguientes hipótesis:

$$H_0: \mu_{2016} - \mu_{2020} \leq 0$$

$$H_A: \mu_{2016} - \mu_{2020} > 0$$

**Tabla 14. Prueba de diferencia de medias índice de divulgación entre 2016 y 2020**

Ttest Índice de Ciberseguridad

Two- sample t test with equal variances

| Group | Obs | Mean | Std. Err. | Std. Dev | 95% Conf. Interval | |
|---|---|---|---|---|---|---|
| 2016 | 85 | .1655773 | .0172408 | .1589522 | .1312921 | .1998625 |
| 2020 | 85 | .3973856 | .0274036 | .2526487 | .3428906 | .4518807 |
| Combined | 170 | .2814815 | .0184388 | .2404126 | .2450814 | .3178815 |
| diff | | -.2318083 | .0323759 | | -.2957244 | -.1678922 |

Diff = mean (2016) – mean (2020) t= -7.1599

H0: diff = 0 degrees of freedom= 168

Ha: diff < 0 Ha: diff != 0 Ha: diff ! > 0

Pr (T < t) = 0. 0000 Pr (|T| > |t|) = 0. 0000 Pr (|T| > |t|) = 1. 0000

El valor-p obtenido no rechaza la hipótesis nula. En consecuencia, se concluye que el índice de divulgación crece durante el período de estudio con 95% de confianza. Los resultados obtenidos permiten confirmar la hipótesis H1, constatándose, por tanto, que existe una tendencia creciente en el nivel de divulgación de información sobre Ciberseguridad en las empresas latinoamericanas.

### 3.3.2. Alcance de las Revelaciones de Ciberseguridad en América Latina por Países

La Tabla 15 representa los estadísticos descriptivos de los puntajes obtenidos en la aplicación del índice de Ciberseguridad (media, mediana, desviación estándar, máximo y mínimo) a las empresas objeto de la muestra en los distintos países analizados. Vemos como, en el caso de la media, Argentina presenta el promedio más alto (0,41), seguido de Colombia (0,29), Brasil (0,28) y Chile (0,27). En general en la muestra todos los países cuentan con un mínimo de 4% y un máximo que oscila entre el 93% en Colombia y el 74% obtenido en México, resultados que expresan una gran variabilidad a nivel de gestión de riesgos de Ciberseguridad entre los diferentes países objeto de análisis.

**Tabla 15. Medidas descriptivas de Índice de Divulgación de Ciberseguridad a nivel país (2016-2020)**

| | Argentina | Brasil | Chile | Colombia | México | Perú |
|---|---|---|---|---|---|---|
| Media | 0,41 | 0,28 | 0,27 | 0,29 | 0,24 | 0,22 |
| Mediana | 0,48 | 0,26 | 0,19 | 0,17 | 0,19 | 0,15 |
| Desviación Estándar | 0,24 | 0,22 | 0,20 | 0,27 | 0,17 | 0,23 |
| Máximo | 0,78 | 0,81 | 0,81 | 0,93 | 0,74 | 0,78 |
| Mínimo | 0,04 | 0,04 | 0,04 | 0,04 | 0,04 | 0,04 |

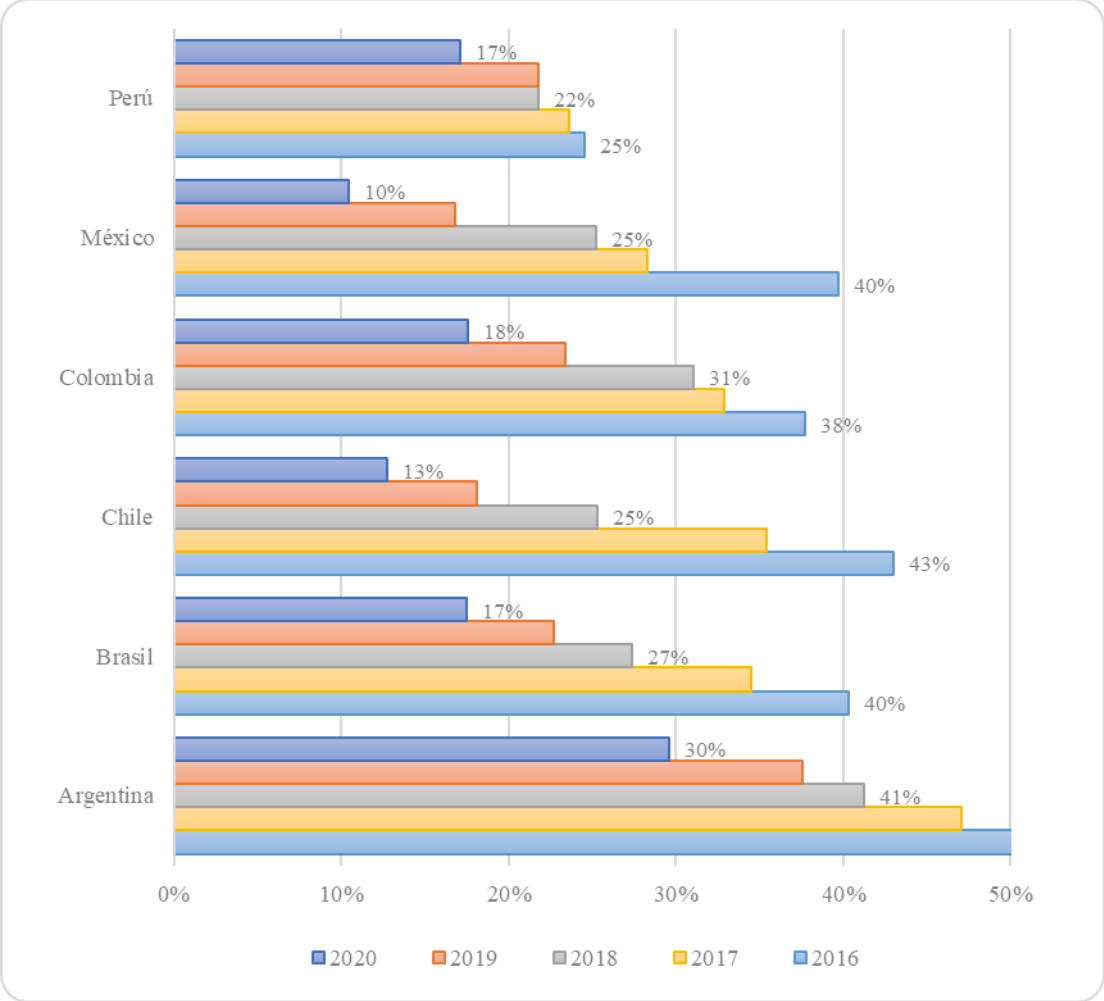
En la Tabla 16 se pueden evidenciar los resultados obtenidos con la aplicación del procedimiento de cuantificación de la información obtenida a nivel de país. A partir de este primer análisis exploratorio se pueden observar los resultados de las medidas estadísticas calculadas, concretamente, media, mediana, desviación estándar, máximo y mínimo. En este sentido, la aplicación del Índice de Divulgación de Ciberseguridad y su agrupación en las cuatro dimensiones generales, permite observar que, en Argentina, la dimensión de estrategia obtiene el primer lugar (54%), seguida de la dimensión de gestión de riesgos (44%). En ese mismo sentido, en términos medios, en Brasil la dimensión de estrategia obtiene una mayor puntuación (41%). En Chile, por su parte, la media con más relevancia se ubica en gobernanza (36%). En Colombia, México y Perú lidera también la dimensión de estrategia, con medias de 32%, 43% y 27%, respectivamente.

**Tabla 16. Índice de Divulgación de Ciberseguridad a nivel país**

| Estadística | Dimensión | Argentina | Brasil | Chile | Colombia | México | Perú |
|---|---|---|---|---|---|---|---|
| Media | Gobernanza | 0,31 | 0,24 | 0,36 | 0,00 | 0,25 | 0,13 |
| | Estrategia | 0,54 | 0,41 | 0,00 | 0,32 | 0,43 | 0,27 |
| | Gestión de riesgos | 0,44 | 0,30 | 0,24 | 0,28 | 0,30 | 0,00 |
| | Implicaciones Financieras | 0,20 | 0,05 | 0,24 | 0,28 | 0,30 | 0,05 |
| Mediana | Gobernanza | 0,40 | 0,20 | 0,40 | 0,00 | 0,00 | 0,00 |
| | Estrategia | 0,33 | 0,33 | 0,00 | 0,33 | 0,33 | 0,17 |
| | Gestión de riesgos | 0,54 | 0,23 | 0,23 | 0,23 | 0,23 | 0,08 |
| | Implicaciones Financieras | 0,00 | 0,00 | 0,23 | 0,23 | 0,23 | 0,00 |
| Desviación estándar | Gobernanza | 0,27 | 0,27 | 0,28 | 0,00 | 0,36 | 0,22 |
| | Estrategia | 0,35 | 0,34 | 0,00 | 0,26 | 0,34 | 0,26 |
| | Gestión de riesgos | 0,26 | 0,26 | 0,24 | 0,28 | 0,18 | 0,21 |
| | Implicaciones Financieras | 0,25 | 0,13 | 0,24 | 0,28 | 0,18 | 0,16 |
| Máximo | Gobernanza | 0,80 | 0,80 | 0,80 | 0,00 | 1,00 | 1,00 |
| | Estrategia | 1,00 | 1,00 | 0,00 | 0,83 | 1,00 | 1,00 |
| | Gestión de riesgos | 0,92 | 0,85 | 1,00 | 0,85 | 0,69 | 0,77 |
| | Implicaciones Financieras | 0,67 | 0,67 | 1,00 | 0,85 | 0,69 | 0,67 |
| Mínimo | Gobernanza | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| | Estrategia | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 | 0,00 |
| | Gestión de riesgos | 0,00 | 0,00 | 0,00 | 0,00 | 0,08 | 0,00 |
| | Implicaciones Financieras | 0,00 | 0,00 | 0,00 | 0,00 | 0,08 | 0,00 |

En todos los países estudiados se observa un incremento progresivo en el valor del Índice de Divulgación de Ciberseguridad y, por lo tanto, un aumento en el alcance de la divulgación de información durante el período objeto de análisis (Figura 15). Si analizamos en detalle los índices por país, observamos que Argentina se presenta como la nación que reporta el mayor índice de divulgación durante los cinco años de estudio. La puntuación que se obtiene puede deberse a diferentes factores. Uno de ellos es que el 57% de las empresas de la muestra pertenecen al sector financiero y, al comparar el puntaje obtenido por las empresas de este sector con el de los demás sectores, se obtiene una diferencia significativa en este país. También podemos observar que el 86% de las organizaciones en Argentina reportan información a la SEC en el Formulario 20 F. Adicionalmente cabe señalar que, en el ámbito nacional, Argentina cuenta con una estrategia de Ciberseguridad y política de protección de datos.

**Figura 15. Índice de Divulgación de Ciberseguridad a nivel país por año**




Haciendo un estudio pormenorizado durante el período objeto de estudio, en general se puede apreciar que los países latinoamericanos presentan importantes avances en el tema de Ciberseguridad nacional. Sin embargo, el mayor aumento de revelaciones en el período de análisis lo presentan Chile y México, alcanzando un aumento del 20% entre 2016 y 2020.

En el caso de Argentina, pasó de 30% en el año 2016 a 51% en 2020, correspondiente a un aumento de 21 puntos porcentuales. Para Brasil, el rango del Índice de Divulgación de Ciberseguridad pasó de 17% en 2016 a 40% en 2020, alcanzando un aumento de 23 puntos porcentuales. Asimismo, Colombia pasó de 18% en 2016 a 38% en 2020.

Finalmente, hubo un menor aumento en Perú, con 8 puntos porcentuales, ya que su Índice de Divulgación de Ciberseguridad se registró en 17% en 2016 y 25% en 2020.

La interpretación de estos resultados requiere considerar dos eventos que han marcado el futuro de la Ciberseguridad en los países de estudio en el período 2016-2020. Primero, la aprobación de la Estrategia Nacional de Ciberseguridad: en Colombia (2016), Chile (2017), México (2017), Argentina (2019) y Brasil (2020). Perú aún no cuenta con una estrategia nacional. En segundo lugar, la expedición de leyes de protección de datos: en Argentina (2016), Brasil (2018), Colombia (2018), Chile (1999), México (2017) y Perú (2011). Otro evento que generó cambios importantes en la Ciberseguridad regional fue el ciberataque del ransomware WannaCry en 2017, del cual, según Creese (2020) CSIRT Americas facilitó la identificación temprana y el aislamiento de puntos críticos de infección en América Latina para detener la propagación de WannaCry dentro de la región. Por lo tanto, la plataforma ha creado un repositorio central de herramientas para sus componentes regionales para prevenir y combatir infecciones de ransomware mitigando futuros brotes. Finalmente, la crisis provocada por la pandemia del COVID-19 durante 2020, además de exponer las carencias estructurales que nuestra sociedad ha venido cargando en múltiples sistemas, también ha puesto de relieve el papel catalizador de la tecnología en la forma en que hemos enfrentado colectivamente la pandemia (Barmpaliou, 2020). De esta forma, todas y cada una de las medidas que se han adoptado para mitigar el ciberriesgo durante esta crisis se han convertido en actuaciones a favor de la Ciberseguridad presente y futura.

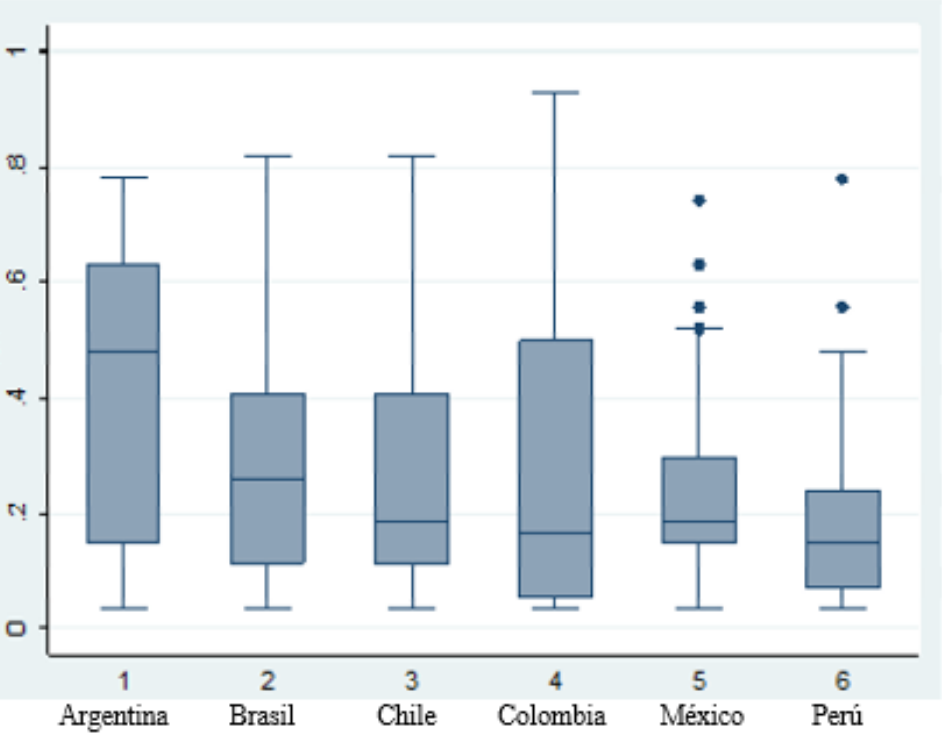
Para realizar el contraste de hipótesis para el Índice de Divulgación de Ciberseguridad entre períodos a partir de los resultados del índice por países, hay que determinar si se cumplen dos supuestos fundamentales para la comparación paramétrica de promedios. En primer lugar, si la distribución de frecuencias del índice tiene una distribución normal entre las diferentes agrupaciones países y, en segundo lugar, si los valores del índice son homocedásticos.

El objetivo de diagnosticar estos supuestos es decidir si es válido realizar un contraste paramétrico tipo ANOVA. En caso de que los supuestos no se cumplan el contraste ANOVA queda invalidado y se hace necesario realizar un contraste análogo no paramétrico.

**Dispersión entre períodos**

El diagrama de dispersión de los valores del índice, agrupado por países (Figura 16), evidencia que Argentina repunta. Por su parte México y Perú presentan valores atípicos, lo que significa que existen observaciones que numéricamente están distantes del resto de los datos.

**Figura 16. Dispersión de la divulgación por países**



**Contraste de normalidad**

**Prueba de Bartlett para igualdad de varianzas del índice de divulgación entre países**

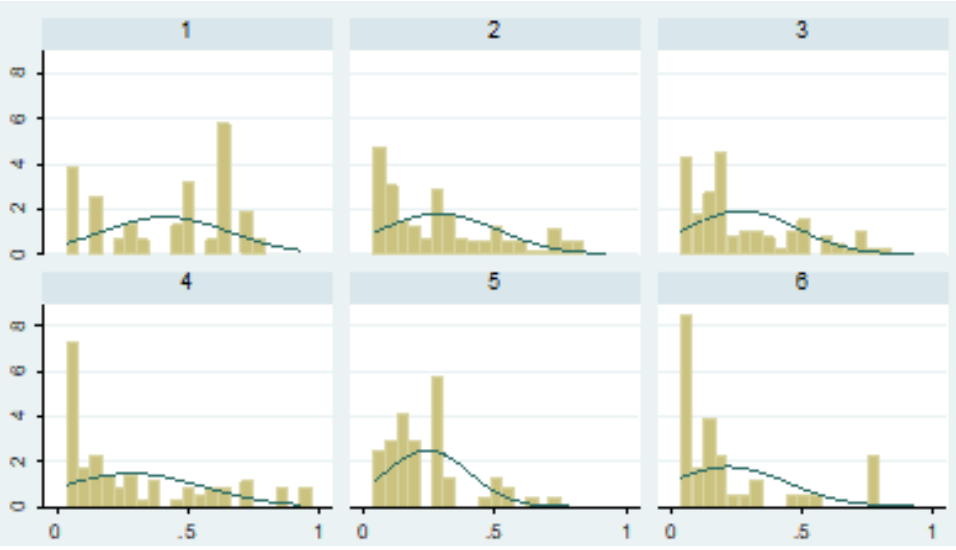
La Prueba de Bartlett sirve para contrastar la normalidad de los datos y permite la contrastación de la homocedasticidad (igualdad de varianzas). Mientras mayor sea la diferencia en los promedios, es más probable que las varianzas de las muestran no sean iguales.

*Prueba de Bartlett para igualdad de varianzas: chi2(5) = 18.6620 Prob>chi2=0.002*

Como el p- valor es 0,002, y este es un valor menor que 0,05, esto indica que la muestra no presenta varianzas iguales. Por lo tanto, podemos afirmar que la muestra no es normal.

El otro supuesto fundamental del ANOVA es que la variable tenga una distribución aproximadamente normal entre los grupos de interés. Trazando histogramas de frecuencia del índice de divulgación, agrupado por países, y ajustando a ellos la curva normal respectiva se evidencia que no tienen forma aproximadamente normal (Figura 17). De esta forma se invalida el análisis paramétrico y no aplica un contraste ANOVA.

**Figura 17. Distribución de frecuencias del índice entre países**



**Análisis no paramétrico**

Como alternativa para contrastar medias de variables no normales y no homocedásticas, se puede aplicar la prueba no paramétrica de Kruskal-Wallis, la cual compara si las medianas de una variable cuantitativa provienen de poblaciones iguales. De esta forma, disponemos de una buena alternativa para el caso del índice de divulgación distribuido entre países.

**Tabla 17. Prueba no paramétrica para igualdad del índice de divulgación entre países**

| País | Obs. | Rank.Sum |
|---|---|---|
| 1 Argentina | 35 | 9689.50 |
| 2 Brasil | 125 | 27163.50 |
| 3 Chile | 90 | 19346.50 |
| 4 Colombia | 80 | 15982.50 |
| 5 México | 55 | 11512.00 |
| 6 Perú | 40 | 683100 |

Chi-squared = 15.335 with 5 d.f.
Probability = 0.0090

Chi-squared with ties= 15.443 with 5 d.f.
Probability = 0.0086

Al ejecutar el contraste no paramétrico se encontra que, para el caso de los países, el Índice de Divulgación de Ciberseguridad difiere. Por tanto, se concluye que existen diferencias significativas del índice de divulgación según el período temporal con 95% de confianza. Así según estos resultados podemos confirmar la hipótesis H2, constatando que existen diferencias significativas en el nivel de divulgación de información sobre Ciberseguridad entre empresas latinoamericanas de distintos países.

### 3.3.3. Alcance de las Revelaciones de Ciberseguridad por Sectores

Dedicamos este apartado a analizar el alcance de las revelaciones de información sobre Ciberseguridad atendiendiendo a la actividad empresarial. La Tabla 18 presenta la puntuación obtenida en cada uno de los sectores objeto de estudio, concretamente, sector

financiero, energía, materiales y consumo discrecional, a partir de los 27 ítems que conforman el índice de divulgación.

**Tabla 18. Alcance de la Divulgación de Ciberseguridad en Latinoamérica por sectores**

| Ítems | Financiero | Energía | Materiales | Consumo Discrecional |
|---|---|---|---|---|
| **Gobernanza** | | | | |
| G1. Describe la participación de la Junta Directiva en la supervisión de los riesgos y oportunidades relacionadas con Ciberseguridad. | 67% | 20% | 7% | 7% |
| G2. Revela la existencia de un comité a nivel de directorio encargado específicamente de la Ciberseguridad y/o seguridad de la información. | 100% | 0% | 0% | 0% |
| G3. Revela la existencia de un comité encargado de supervisar la Ciberseguridad diferente al Comité de Auditoría Ej. Tecnología, riesgos. | 60% | 20% | 7% | 13% |
| G4. Revela la supervisión de los asuntos de Ciberseguridad por parte de un Comité de Auditoría. | 50% | 50% | 0% | 0% |
| G5. Informa sobre la contribución de la dirección en el diseño y evaluación del sistema de gestión de riesgos de seguridad de la información de la organización. | 75% | 13% | 6% | 6% |
| **Estrategia** | | | | |
| E1. Divulga sobre la formulación de una(s) política(s) de Ciberseguridad orientada(s) a gestionar la seguridad de la información. | 50% | 25% | 5% | 20% |
| E2. Revela la existencia de un sistema de gestión de la seguridad de la información en la organización. | 46% | 31% | 13% | 10% |
| E3. Revela que el sistema de gestión de seguridad de la información se establece de acuerdo con normas y estándares reconocidos en el ámbito internacional. | 64% | 27% | 0% | 9% |
| E4. Revela la existencia de una política de protección de datos personales y/o garantía de derechos digitales | 69% | 13% | 13% | 6% |
| E5. Divulga sobre la aplicación de estrategias de concienciación y capacitación en Ciberseguridad para | 50% | 17% | 17% | 17% |

| | | | | |
|---|---|---|---|---|
| los miembros de la organización para mitigar el riesgo de Ciberseguridad. | | | | |
| E6. Revela sobre la existencia de procedimientos de comunicación que brindan información sobre Ciberseguridad a los tomadores de decisiones, clientes, empleados, otros participantes del mercado y reguladores, según corresponda. | 78% | 22% | 0% | 0% |
| **Gestión de Riesgos** | | | | |
| R1. Presenta una descripción de los riesgos de Ciberseguridad y /o seguridad de la información. | 42% | 19% | 15% | 23% |
| R2. Incluye la protección de datos como tema material. | 75% | 17% | 8% | 0% |
| R3. Incluye la Ciberseguridad y/o seguridad de la información como tema material. | 75% | 13% | 0% | 13% |
| R4. Incluye la Ciberseguridad y/o seguridad de la información como factor de riesgo. | 47% | 24% | 15% | 15% |
| R5. Incluye la privacidad de los datos como factor de riesgo. | 67% | 29% | 0% | 5% |
| R6. Revela el riesgo de Ciberseguridad dentro de otros riesgos organizacionales. | 57% | 36% | 7% | 0% |
| R7. Informa sobre procedimientos de respuesta ante incidencias en los sistemas de información (Plan de contingencias). | 58% | 25% | 8% | 8% |
| R8. Revela el desarrollo de pruebas y monitoreo para validar la efectividad de las políticas y procedimientos de Ciberseguridad. | 63% | 26% | 0% | 11% |
| R9. Presenta información previa de incidentes de seguridad cibernética en curso u otros eventos pasados que puedan ser relevantes como factor de riesgo de la organización. | 40% | 60% | 0% | 0% |
| R10. Se divulga sobre la frecuencia de los informes de gestión a la Junta o comité (s). | 0% | 0% | 50% | 50% |
| R11. Revela reclamaciones relativas a violaciones de la privacidad y pérdida de datos del cliente. | 48% | 28% | 20% | 4% |
| R12. Informa sobre la participación de la auditoría interna en el manejo del riesgo cibernético y/o de seguridad de la información. | 50% | 30% | 10% | 10% |
| R13. Informa sobre la participación de un asesor externo independiente en la mitigación de riesgos de Ciberseguridad. | 100% | 0% | 0% | 0% |

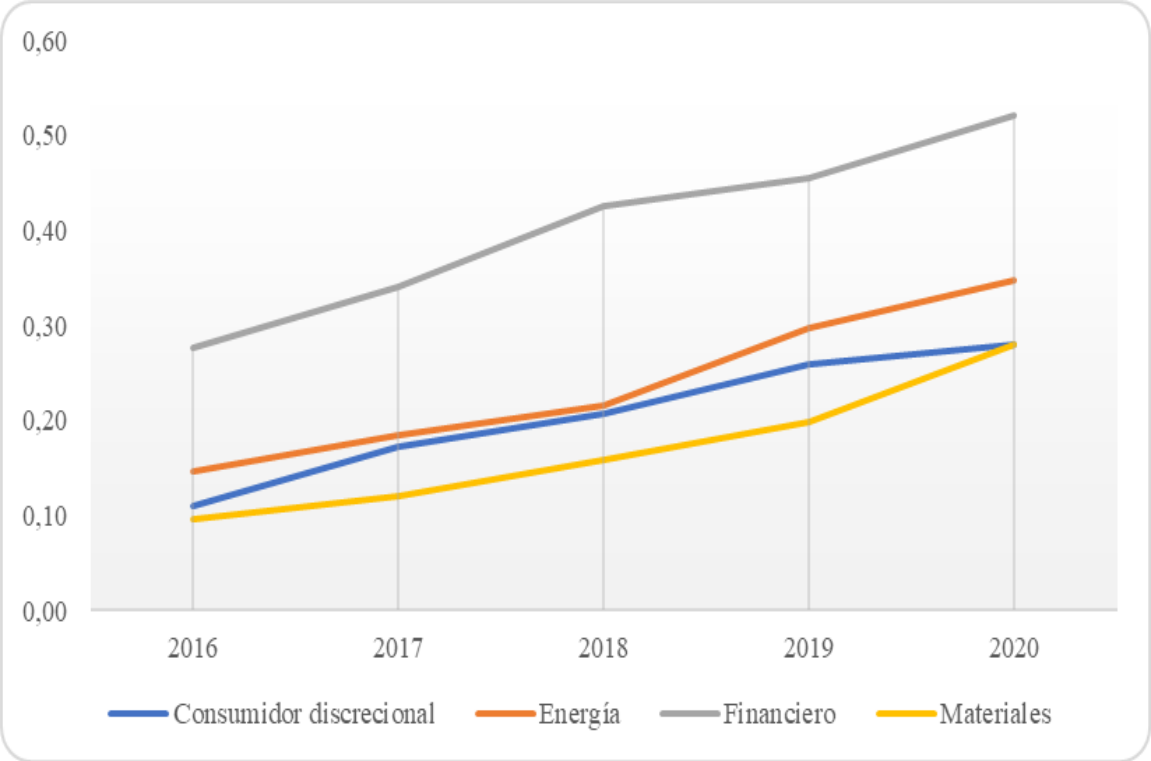
| | | | | |
|---|---|---|---|---|
| **Implicaciones Financieras** | | | | |
| I1. Menciona coberturas de seguros relacionada con Ciberseguridad cibernética o pagos a proveedores de servicio. | 80% | 20% | 0% | 0% |
| I2. Revela información relacionada con la medición de los esfuerzos continuos en Ciberseguridad. | 50% | 0% | 50% | 0% |
| I3. Se informa sobre la medición de los costos, consecuencias y riesgos de los incidentes de seguridad cibernética. | 0% | 100% | 0% | 0% |

Constatamos que el mayor porcentaje de divulgación por ítem se concentra en el sector financiero, e ítems como ´Revela la existencia de un comité a nivel de directorio encargado específicamente de la Ciberseguridad y/o seguridad de la información´ e ´Informa sobre la participación de un asesor externo independiente en la mitigación de riesgos de Ciberseguridad´ se divulgan únicamente en este sector. Mientras tanto, ítems como ´Se divulga sobre la frecuencia de los informes de gestión a la Junta o comité (s)´ y ´Se informa sobre la medición de los costos, consecuencias y riesgos de los incidentes de seguridad cibernética´ no son reportados en la información divulgada por empresas del sector financiero. Ahora bien, respecto al sector energético podemos observar porcentajes que denotan un menor alcance en las revelaciones corporativas, tan solo, repuntan con un 60% en el ítem ´Presenta información previa de incidentes de seguridad cibernética en curso u otros eventos pasados que puedan ser relevantes como factor de riesgo de la organización´. En los demás no alcanzan más del 50% de divulgación frente a los demás sectores. En el sector materiales y consumo discrecional presentan un alcance muy reducido en las revelaciones, estos dos sectores son los únicos que divulgan el ítem ´Se divulga sobre la frecuencia de los informes de gestión a la Junta o comité (s)´.

Por su parte, la Figura 18 ilustra la divulgación de Ciberseguridad revelada durante el período objeto de análisis, corroborándose que son las empresas ubicadas en el sector financiero las que presentan un mayor alcance en la divulgación sobre Ciberseguridad, y se encuentran en el extremo opuesto las empresas ubicadas en el sector de materiales y consumo discrecional. Los resultados de la divulgación de información de Ciberseguridad

a través de los años han experimentado diferentes cambios aunque, en general, se observa un crecimiento sostenido y generalizado en todos los sectores de actividad. Se destaca el elevado crecimiento en la información cibernética divulgada por el sector financiero desde el 2016 (26%) hasta el 2020, cuando se postula por encima de la media con un 53%.

**Figura 18. Índice de Divulgación de Ciberseguridad a nivel de sector por año**



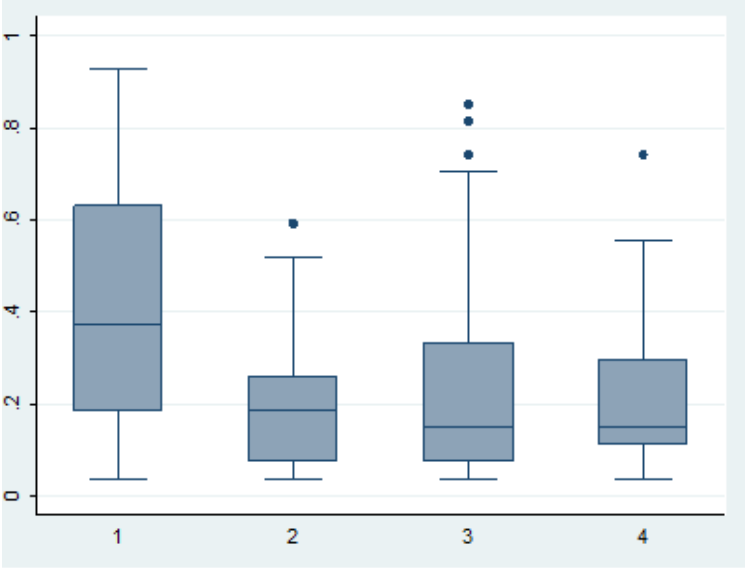

Una vez realizado el estudio descriptivo, a simple vista se observa un aumento en el nivel de divulgación de información por sectores y diferencias entre ellos. No obstante, aunque parece haber diferencias, es necesario comprobar si son estadísticamente significativas.

**Dispersión entre períodos**

El diagrama de dispersión de los valores del índice, agrupado por sectores (Figura 19), muestra que el sector Financiero presenta un alcance en su divulgación significativo frente a los otros sectores estudiados. Por su parte el sector de consumo discrecional,

energía y materiales presentan valores atípicos, lo que significa que existen observaciones que numéricamente están distantes del resto de los datos.

**Figura 19. Dispersión del índice de divulgación por sectores**




Sector financiero (1) Energía (2) Consumo discrecional (3) Materiales (4)

**Contraste de normalidad**

Prueba de Bartlett para igualdad de varianzas del índice de divulgación entre sectores. La evidencia gráfica sugiere que el índice de divulgación entre sectores varía con el tiempo. El contraste estadístico ANOVA exige varianzas homogéneas entre grupos (sectores). Por ello, se ejecutó la prueba de Bartlett para igualdad de varianzas, la cual rechaza la hipótesis de que el índice de divulgación sea homocedástico entre diferentes y sectores (0.000).

*Prueba de Bartlett para igualdad de varianzas: chi2(3) = 53.3250*
*Prob>chi2=0.000*

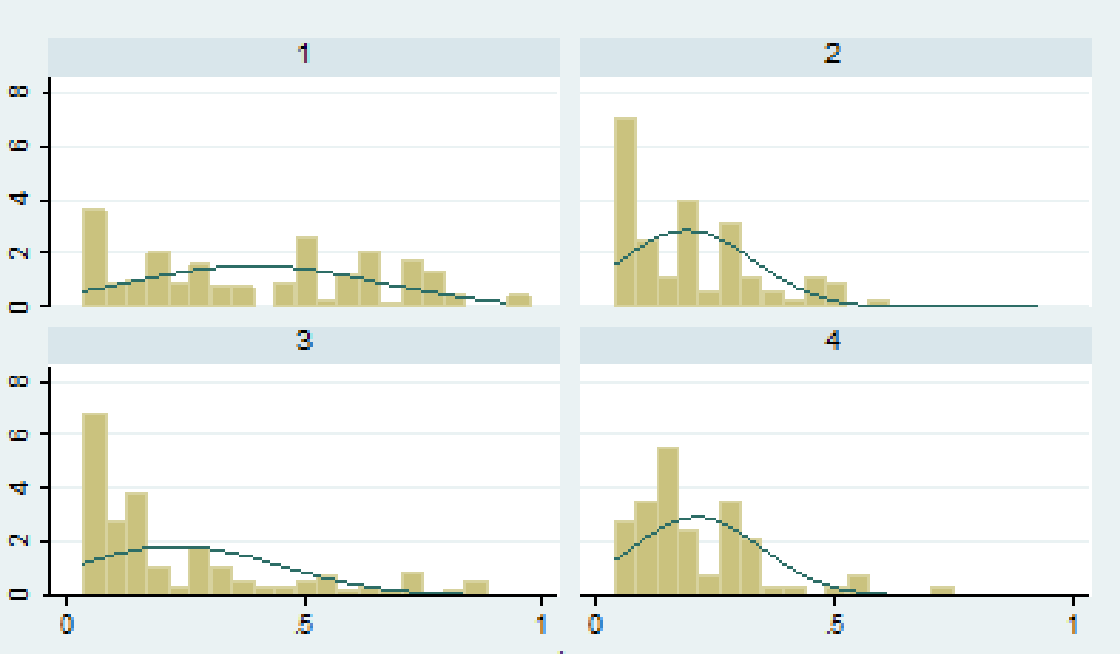
Para confirmar el crecimiento, se contrastó una prueba $T$ con las siguientes hipótesis:

$$H_0: \mu_{2016} - \mu_{2020} \leq 0$$

$$H_A: \mu_{2016} - \mu_{2020} > 0$$

El otro supuesto fundamental del ANOVA es que la variable tenga una distribución aproximadamente normal entre los grupos de interés (Figura 20). Trazando histogramas de frecuencia del índice de divulgación, agrupado por sectores, y ajustando a ellos la curva normal respectiva se evidencia que no tienen forma aproximadamente normal. De esta forma, se invalida el análisis paramétrico y no se aplica un contraste ANOVA.

**Figura 20. Distribución de frecuencias del índice por sectores**




Sector financiero (1) Energía (2) Consumo discrecional (3) Materiales (4)

**Análisis no paramétrico**

Como alternativa para contrastar medias de variables no normales y no homocedásticas, aplicamos nuevamente la prueba no paramétrica de Kruskal-Wallis que, como indicamos anteriormente, compara si las medianas de una variable cuantitativa provienen de

poblaciones iguales. Así, se tiene una buena alternativa para el caso del índice de divulgación distribuidos entre sectores. Al ejecutar el contraste no paramétrico, se encontró que para el caso de los sectores, el Índice de Divulgación de Ciberseguridad también difiere. Por tanto, se concluye que existen diferencias estadísticamente significativas en el valor del índice de divulgación según el período temporal con 95% de confianza (Tabla 19).

**Tabla 19. Prueba no paramétrica para igualdad del índice de divulgación entre sectores**

| Sector | Observaciones | Rank. Sum |
|---|---|---|
| 1 | 35 | 9689.50 |
| 2 | 125 | 27163.50 |
| 3 | 90 | 19346.50 |
| 4 | 80 | 15982.50 |

Chi-squared = 49.771 with 3 d.f.
Probability = 0.0001

Chi-squared with ties = 50.120 with 3 d.f.
Probability = 0.0001

Con base en estos resultados podemos confirmar la hipótesis H3, constatando la existencia de diferencias significativas en el alcance de divulgación de información sobre Ciberseguridad entre empresas latinoamericanas de distintos sectores de actividad.

### 3.4. Conclusiones

En América Latina las acciones en materia de Ciberseguridad son impulsadas por la OEA con diferentes iniciativas que promueven la Ciberseguridad y la cooperación internacional para la región. A nivel nacional, los países se han adherido gradualmente a las medidas de política internacional. Algunas han tenido avances importantes, como la ratificación del Convenio de Budapest, la aprobación de la estrategia nacional y la

creación de leyes de protección de datos, entre otras. Es por ello que la medición del compromiso nacional en Ciberseguridad en 2020 muestra un mejor puntaje, en comparación con años anteriores, en las diferentes dimensiones que componen el Índice Global de Ciberseguridad: medidas legales, técnicas, organizacionales, de desarrollo de capacidades y de cooperación.

El mayor nivel de desarrollo se encontró en Brasil (97,68), seguido de México (81,68), Uruguay (75,15), República Dominicana (75,07), Chile (68,83), Costa Rica (67,46), Colombia (63,74), Perú (55,68) y Argentina (50,12). Pero, a pesar de los logros alcanzados hasta la fecha, el rezago de la región en algunos frentes obliga a tomar medidas para mejorar su capacidad de respuesta ante riesgos y amenazas cibernéticas.

El Índice de Divulgación de Información sobre Ciberseguridad propuesto en este trabajo tiene como objetivo obtener una herramienta que, tomando como base para su elaboración los principales estándares de aceptación global, permita evaluar el alcance de la divulgación de la información sobre Ciberseguridad por parte de las empresas. Está compuesto por 27 elementos individuales, asociados con una de las cuatro dimensiones siguientes: gobernanza (5), estrategia (6), gestión de riesgos (13) e implicaciones financieras (3). La selección de los ítems que componen el Índice de Ciberseguridad se hizo a partir de literatura previa, estudios de firmas internacionales de contabilidad y auditoría, estándares internacionales, como ISO y GRI, guías SEC (2011; 2018), la Norma General de Protección de Datos Reglamento de la Unión Europea, y otros documentos propuestos por entidades con amplio reconocimiento internacional, como la OCDE, el BID, la OEA y el Global Reporting Iniciative (GRI), entre otros.

Los resultados obtenidos a través de su aplicación a una muestra de empresas cotizadas en América Latina muestran que, si bien ha habido un aumento sostenido en el nivel de divulgación de información sobre Ciberseguridad en las empresas latinoamericanas, tendencia que se evidencia en otros estudios (Gao et al., 2020; Radu & Smaili, 2021; Gordon et al., 2006), la nota media anual no supera el 40% de la nota total. Por ello, podemos concluir que, en línea con resultados obtenidos en trabajos precedentes (Héroux

& Fortin, 2020a), el nivel de divulgación de información sobre Ciberseguridad en las empresas latinoamericanas es bajo.

En cuanto al análisis longitudinal por países, la aplicación del instrumento permite verificar que las empresas que constantemente divulgaron más información sobre Ciberseguridad durante el período 2016-2020 fueron las argentinas. Según nuestros resultados, el 86% de las empresas de la muestra de este país reportaron a la SEC. En su mayoría estas empresas pertenecen al sector financiero, situación que puede generar un aumento en la divulgación de Ciberseguridad. La medición de la divulgación por sector muestra cómo el sector financiero obtuvo liderazgo durante los cinco años del estudio. En este sentido, podemos señalar que en los países objeto de estudio, y a nivel internacional, la normativa para este sector se ha incrementado y es más exigente, debido a que estas organizaciones presentan una mayor vulnerabilidad a los ciberataques. Estamos de acuerdo con Barry et al. (2021) en que las prácticas de divulgación de información sobre Ciberseguridad han evolucionado a la luz de las expectativas de los reguladores financieros.

Además, el estudio comparativo por dimensión indica cómo la dimensión estrategia obtuvo el puntaje más alto durante el período 2016-2020. En concreto, a partir de los resultados obtenidos, podemos concluir que, en términos generales, las empresas analizadas revelaron información sobre las acciones diseñadas a largo plazo, como las estrategias de Ciberseguridad, y se han interesado en comunicar las medidas relacionadas con los ciberriesgos de gestión, concretando cómo este riesgo emergente se va vinculando, poco a poco, con otros riesgos corporativos. Las revelaciones también permiten visualizar cómo la Junta Directiva y la gerencia se vinculan gradualmente en la supervisión de los asuntos de Ciberseguridad.

El índice de divulgación propuesto constituye un instrumento novedoso que permite evaluar el alcance de la divulgación de información sobre Ciberseguridad. Teniendo en cuenta que la Ciberseguridad se ha convertido en una responsabilidad empresarial y parte importante de la información no financiera, la información que revela este índice puede

constituir un punto de referencia para la valoración de las organizaciones en este sentido por parte de los diferentes grupos de interés.

Los resultados de la aplicación del índice dejan ver que se cumplen las tres hipótesis planteadas, pudiendo concluir que existe una tendencia creciente en el nivel de divulgación de información sobre Ciberseguridad en empresas latinoamericanas, existen diferencias estadísticamente significativas en el nivel de divulgación de información sobre Ciberseguridad entre empresas latinoamericanas de distintos países, y también existen diferencias estadísticamente significativas en el nivel de divulgación de información sobre Ciberseguridad entre empresas latinoamericanas de distintos sectores de actividad.

Dado que el índice propuesto ha sido elaborado con base en estándares internacionales relacionados con el riesgo cibernético empresarial, puede ser aplicable en futuras investigaciones a empresas que desarrollan su actividad en otras áreas geográficas. De esta forma, se espera que este índice se convierta en un punto de partida para el análisis comparativo en otros países en diferentes períodos de tiempo, lo que permitirá conocer las tendencias en la divulgación de información de Ciberseguridad desde diferentes perspectivas.

### 3.5. Referencias


Abbate, J. (2011). Inventing the internet. En *Networks of Innovation*. https://doi.org/10.1093/acprof:oso/9780199269051.003.0003

Abraham, S., & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/J.BAR.2007.06.002

Abraham, S., & Shrives, P. J. (2014). Improving the relevance of risk factor disclosure in corporate annual reports. *British Accounting Review*, *46*(1), 91–107. https://doi.org/10.1016/j.bar.2013.10.002

Abraham, S. the determinants of narrative risk information in U. F. 100 annual reports, &

Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/J.BAR.2007.06.002

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Adams, R. B., & Ferreira, D. (2007). A Theory of Friendly Boards. *The Journal of Finance*, *62*(1), 217–250. https://doi.org/10.1111/J.1540-6261.2007.01206.X

Adams, R. B., & Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. *Journal of Financial Economics*, *94*(2), 291–309. https://doi.org/10.1016/j.jfineco.2008.10.007

Adams, R. B., & Funk, P. (2012). Beyond the glass ceiling: Does gender matter? *Management Science*, *58*(2), 219–235. https://doi.org/10.1287/mnsc.1110.1452

Afep Medef. (2015). *Code de gouvernement entreprise revise*.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/CYBSEC/TYY006

Agrawal, A., & Chadha, S. (2005). Corporate governance and accounting scandals. *Journal of Law and Economics*, *48*(2), 371–406. https://doi.org/10.1086/430808/ASSET/IMAGES/LARGE/FG1.JPEG

Agrawal, A., & Knoeber, C. R. (2001). Do some outside directors play a political role? *Journal of Law and Economics*, *44*(1), 179–198. https://doi.org/10.1086/320271

Agrawal, A., & Knoeber, C. R. (2015). Do Some Outside Directors Play a Political Role?*. *https://doi.org/10.1086/320271*, *44*(1), 179–198. https://doi.org/10.1086/320271

Aguilar Antonio, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, *25*.

Agyei-Mensah, B. K. (2017). The relationship between corporate governance mechanisms and IFRS 7 compliance: evidence from an emerging market. *Corporate Governance (Bingley)*, *17*(3), 446–465. https://doi.org/10.1108/CG-06-2016-

0129/FULL/PDF

Ahmed, K., Hossain, M., & Adams, M. B. (2006). The Effects of Board Composition and Board Size on the Informativeness of Annual Accounting Earnings. *Corporate Governance: An International Review*, *14*(5), 418–431. https://doi.org/10.1111/J.1467-8683.2006.00515.X

AICPA. (2017a). *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*. 29. https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/Description-Criteria.pdf%0Ahttps://web.archive.org/web/20170706132715/https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocum

AICPA. (2017b). *Guide Reporting on an Entity´s Cybersecurity Risk Management Program and Controls*.

AICPA. (2018). *Cybersecurity risk management reporting*. 1–4.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Al-Hadi, A., Hasan, M. M., & Habib, A. (2016). Risk Committee, Firm Life Cycle, and Market Risk Disclosures. *Corporate Governance: An International Review*, *24*(2), 145–170. https://doi.org/10.1111/corg.12115

Al-Sartawi, A. M. A. M., Wadi, R. M. A., & Hannoon, A. (2018). Information Technology Governance and Electronic Financial Disclosure. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11195 LNCS*, 449–458. https://doi.org/10.1007/978-3-030-02131-3_40

Alavi, M., & Weiss, I. R. (1985). Managing the Risks Associated with End-User Computing. *Journal of Management Information Systems*, *2*(3), 5–20. https://doi.org/10.1080/07421222.1985.11517734

Albitar, K., Hussainey, K., Kolade, N., & Gerged, A. M. (2020). ESG disclosure and firm performance before and after IR: The moderating role of governance mechanisms. *International Journal of Accounting & Information Management*, *28*(3), 429–

444. https://doi.org/10.1108/IJAIM-09-2019-0108

Alchian, A., & Demsetz, H. (1972). Linked references are available on JSTOR for this article : Production , Information Costs , and Economic Organization. *The American Economic Review*, *62*(5), 777–795. https://knowledgehub.unsse.org/es/knowledge-hub/relaciones-entre-los-ods-el-plan-para-una-decada-cooperativa-y-el-balance-social-en-cooperativas-2/

Allegrini, M., & Greco, G. (2013). Corporate boards, audit committees and voluntary disclosure: Evidence from Italian Listed Companies. *Journal of Management and Governance*, *17*(1), 187–216. https://doi.org/10.1007/S10997-011-9168-3/TABLES/6

Allini, A., Manes Rossi, F., & Hussainey, K. (2016). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *Public Money & Management*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Allini, A., Manes Rossi, F., & Macchioni, R. (2014). Do Corporate Governance Characteristics Affect Non-Financial Risk Disclosure in Government-owned Companies? The Italian Experience. *FINANCIAL REPORTING*, *1*, 5–31. https://doi.org/10.3280/FR2014-001001

Allini, A., Rossi, F. M., & Hussainey, K. (2015). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *http://dx.doi.org/10.1080/09540962.2016.1118935*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Almazan, A., & Suarez, J. (2003). Entrenchment and Severance Pay in Optimal Governance Structures. *The Journal of Finance*, *58*(2), 519–547. https://doi.org/10.1111/1540-6261.00536

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). *Towards a Taxonomy of Information Security Management Practices in Organisations*. https://openrepository.aut.ac.nz/handle/10292/8174

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *ACM International Conference Proceeding Series, September 2018*, 68–79. https://doi.org/10.1145/3285957.3285971

Amir, E., & Lev, B. (1996). Value-relevance of nonfinancial information: The wireless

communications industry. *Journal of Accounting and Economics*, *22*(1–3), 3–30. https://doi.org/10.1016/S0165-4101(96)00430-2

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Anderson, R. C., Mansi, S. A., & Reeb, D. M. (2004). Board characteristics, accounting report integrity, and the cost of debt. *Journal of Accounting and Economics*, *37*(3), 315–342. https://doi.org/10.1016/j.jacceco.2004.01.004

Andrikopoulos, A., Samitas, A., & Bekiaris, M. (2014). Corporate social responsibility reporting in financial institutions: Evidence from Euronext. *Research in International Business and Finance*, *32*, 27–35. https://doi.org/10.1016/j.ribaf.2014.02.001

Aoki, M., Kim, H.-K., & World Bank. (1995). *Corporate governance in transitional economies : insider control and the role of banks*. 467.

Armstrong, Philip; Segal, Nick; Davis, B. (2006). Corporate Governance in South Africa. En *Handbook on International Corporate Governance*.

Arnum, E. (1995). Doing business on the Internet-A question of balance. *Business Communications Review*.

Asamblea General de las Naciones Unidas. (2001). *Resolución 56/183. Cumbre Mundial sobre la Sociedad de la Información*. 3.

AT&T Cybersecurity. (2021). *What is a Cybersecurity Strategy and How to Develop One*. https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

ATOS. (2020). *Universal Registration Document Board of Directors 2020*.

Axa. (2020). *AXA Future Risks Report*.

Baginski, S. P., Campbell, J. L., Hinson, L. A., & Koo, D. S. (2018). Do Career Concerns Affect the Delay of Bad News Disclosure? *The Accounting Review*, *93*(2), 61–95. https://doi.org/10.2308/ACCR-51848

Bakker, T. G. (2015). *Beadle Scholar Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks*. https://scholar.dsu.edu/theses/294

Baldini, M., Maso, L. D., Liberatore, G., Mazzi, F., & Terzani, S. (2018). Role of

Country- and Firm-Level Determinants in Environmental, Social, and Governance Disclosure. *Journal of Business Ethics*, *150*(1), 79–98. https://doi.org/10.1007/s10551-016-3139-1

Barakat, AhmedBank; Hussainey, K. (2013). Bank governance, regulation, supervision, and risk reporting: Evidence from operational risk disclosures in European banks. *International Review of Financial Analysis*, *30*, 254–273. https://doi.org/10.1016/J.IRFA.2013.07.002

Barakat, A., & Hussainey, K. (2013). 0. *International Review of Financial Analysis*, *30*, 254–273. https://doi.org/10.1016/j.irfa.2013.07.002

Barakat, F. S. Q., López Pérez, M. V., & Rodríguez Ariza, L. (2015). Corporate social responsibility disclosure (CSRD) determinants of listed companies in Palestine (PXE) and Jordan (ASE). *Review of Managerial Science*, *9*(4), 681–702. https://doi.org/10.1007/s11846-014-0133-9

Barclay, M. J., & Holderness, C. G. (1991). Negotiated Block Trades and Corporate Control. *The Journal of Finance*, *46*(3), 861–878. https://doi.org/10.1111/J.1540-6261.1991.TB03769.X

Barmpaliou, N. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*.

Barney, J. (2014). Gaining and sustaining a competitive advantage. En P. E. Limited (Ed.), *Introduction to e-Business*. https://doi.org/10.4324/9780080492780-16

Barry, T., Jona, J., & Soderstrom, N. S. (2021). The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3916525

Bartha, Peter; Gillies, J. (2006). Corporate governance in Russia: is it really necessary? En *Corporate governance handbook on international country analysis*.

Bear, S., Rahman, N., & Post, C. (2010). The Impact of Board Diversity and Gender Composition on Corporate Social Responsibility and Firm Reputation. *Journal of Business Ethics 2010 97:2*, *97*(2), 207–221. https://doi.org/10.1007/S10551-010-0505-2

Beattie, V., McInnes, B., & Fearnley, S. (2004). A methodology for analysing and evaluating narratives in annual reports: A comprehensive descriptive profile and

metrics for disclosure quality attributes. *Accounting Forum*, *28*(3), 205–236. https://doi.org/10.1016/j.accfor.2004.07.001

Bebbington, J., Kirk, E. A., & Larrinaga, C. (2012). The production of normativity: A comparison of reporting regimes in Spain and the UK. *Accounting, Organizations and Society*, *37*(2), 78–94. https://doi.org/10.1016/j.aos.2012.01.001

Bebbington, J., & Larrinaga-González, C. (2008). Carbon Trading: Accounting and Reporting Issues. *European Accounting Review*, *17*(4), 697–717. https://doi.org/10.1080/09638180802489162

Berelson, B. (1952). *Content Analysis, Lindzey: Handbook of social psychology*.

Beretta, S., & Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *International Journal of Accounting*, *39*(3), 265–288. https://doi.org/10.1016/j.intacc.2004.06.006

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Berle, A. a, & Means, G. C. (1932). Property in Transaction, The Appearance of the Corporate System, The Concetration of Economic Power. *The Modern Corporation and Private Property*, 24. http://books.google.com/books?id=mLdLHhqxUb4C&pgis=1

Bhatia, A., & Makkar, B. (2020). Stage of development of a country and CSR disclosure – the latent driving forces. *International Journal of Law and Management*, *62*(5), 467–493. https://doi.org/10.1108/IJLMA-03-2020-0068

Biener, C., & Eling, M. (2012). *Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions*. *37*, 77–107. https://doi.org/10.1057/gpp.2011.29

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance: Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Blakley, B., Mcdermott, E., Morganchase, J. P., & Geer, D. (2002). Information Security is Information Risk Management. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*. https://doi.org/10.1145/508171

Bloomfield, R. J. (2002). The "Incomplete Revelation Hypothesis" and Financial

Reporting. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.312671

Bogle, J. C. (2005). *The Battle for the Soul of Capitalism*.

Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, *22*(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Botosan, C. A. (1997). Disclosure level and the cost of equity capital. *Accounting Review*, *72*(3), 323–349.

Branco, M. C., & Rodrigues, L. L. (2008). Social responsibility disclosure: A study of proxies for the public visibility of Portuguese banks. *The British Accounting Review*, *40*(2), 161–181. https://doi.org/10.1016/j.bar.2008.02.004

Brandeis, L. D. (1914). *Other people's money and how the bankers use it*. https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-by-louis-d.-brandeis

Bratton, W. W. (1989). *Penn Law : Legal Scholarship Repository The New Economic Theory of the Firm : Critical Perspectives from History The New Economic Theory of the Firm : Critical Perspectives from History*.

Bratton, W. W. (2007). *Hedge Funds and Governance Targets*. https://scholarship.law.upenn.edu/faculty_scholarship://scholarship.law.upenn.edu/faculty_scholarship/862

Brazilian Institute of Corporate Governance. (2020). *Gestión de Riesgos Corporativos* (Brazilian Institute of Corporate Governance (ed.)). https://idbinvest.org/sites/default/files/2021-04/Cuaderno 19 - Gestión de Riesgos Corporativos.pdf

Brennan, N. (2006). Boards of directors and firm performance: Is there an expectations gap? *Corporate Governance: An International Review*, *14*, 577–594.

Brennan, N. M., & Solomon, J. (2008). Corporate governance, accountability and mechanisms of accountability: An overview. *Accounting, Auditing & Accountability Journal*, *21*(7), 885–906. https://doi.org/10.1108/09513570810907401/FULL/PDF

Briano-Turrent, G. D. C., & Poletti-Hughes, J. (2017). Corporate governance compliance of family and non-family listed firms in emerging markets: Evidence from Latin America. *Journal of Family Business Strategy*, *8*(4), 237–247.

https://doi.org/10.1016/J.JFBS.2017.10.001

Briano, G. del C. (2012). *Tesis doctoral: Factores institucionales que inciden en la transparencia del Gobierno Corporativo: un estudio en empresas cotizadas*. Universidad de Cantabria.

Brooks, L. (Lily) Z., Cheng, Y., Liu, L., & Yu, M. D. (2021). The timeliness of 10-K filings, early filers, and effects of filing deadline changes. *Journal of Corporate Accounting & Finance*, *32*(2), 169–186. https://doi.org/10.1002/JCAF.22492

Burnap, P. (2021). Risk Management & Governance Knowledge Area. *The Cyber Security Body Of Knowledge*, 19–48.

Bushee, B. J., Carter, M. E., & Gerakos, J. (2014). Institutional investor preferences for corporate governance mechanisms. *Journal of Management Accounting Research*, *26*(2), 123–149. https://doi.org/10.2308/jmar-50550

Bushman, R. M., & Smith, A. J. (2001). Financial accounting information and corporate governance. *Journal of Accounting and Economics*, *32*(1–3), 237–333. https://doi.org/10.1016/S0165-4101(01)00027-1

Business Roundtable. (2018). *Principles of Corporate Governance 2016*. *153*(153), 84–97.

Cabedo, J. D., & Tirado, J. M. (2004). The disclosure of risk in financial statements. *Accounting Forum*, *28*(2), 181–200. https://doi.org/10.1016/j.accfor.2003.10.002

Cadbury. (1992). The Report of the Cadbury Committee on The Financial Aspects of Corporate Governance: The Code of Best Practice. *Corporate Governance: An International Review*, *1*(3), 124–124. https://doi.org/10.1111/j.1467-8683.1993.tb00025.x

CAF. (2013). *Lineamientos para un Código latinoamericano de Gobierno Corporativo* .

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. https://doi.org/10.1111/RISA.13687

Calder, A. (2008). *Corporate governance : a practical guide to the legal frameworks and international codes of practice* (London).

Calderón, R., Piñero, R., & Redín, D. M. (2018). Can compliance restart integrity? Toward a harmonized approach. The example of the audit committee. *Business*

*Ethics: A European Review*, *27*(2), 195–206. https://doi.org/10.1111/BEER.12182

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, *25*(1), 24–39. https://doi.org/10.1111/ijau.12209

Campbell, J. L. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. En *Academy of Management Review* (Vol. 32, Número 3, pp. 946–967). Academy of Management. https://doi.org/10.5465/AMR.2007.25275684

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. min, & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396–455. https://doi.org/10.1007/s11142-013-9258-3

Campbell, K., & Mínguez-Vera, A. (2008). Gender Diversity in the Boardroom and Firm Financial Performance. *Journal of Business Ethics 2007 83:3*, *83*(3), 435–451. https://doi.org/10.1007/S10551-007-9630-Y

Cano, J. (2021). *Ciberseguridad empresarial Reflexiones y retos para los ejecutivos del siglo XXI*.

Carter, D. A., D'Souza, F., Simkins, B. J., & Simpson, W. G. (2010). The Gender and Ethnic Diversity of US Boards and Board Committees and Firm Financial Performance. *Corporate Governance: An International Review*, *18*(5), 396–414. https://doi.org/10.1111/J.1467-8683.2010.00809.X

Carter, D. A., Simkins, B. J., & Simpson, W. G. (2003). Corporate Governance, Board Diversity, and Firm Value. *Financial Review*, *38*(1), 33–53. https://doi.org/10.1111/1540-6288.00034

Castro, S. (2009). Practicas de Gobierno Corporativo en America Latina. *Revista Latinoamericana de Administración*, *43*, 26–40.

Cavelty, M. D. (2010). *Cyber-Security* (Routledge (ed.)). The Routledge Handbook of New Security Studies: 154-162.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

CCB, & OCDE. (2004). *"White paper" sobre Gobierno Corporativo en Latinoamerica*. *7*, 92.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images*. *December*. http://www.sei.cmu.edu

CEUPE. (2019). Modelos de Gobierno Corporativo. *Centro europeo de postgrado*, 1. https://www.ceupe.com/blog/modelos-de-gobierno-corporativo.html

Chang, H. C. (2016). The Synergy of Scientometric Analysis and Knowledge Mapping with Topic Models: Modelling the Development Trajectories of Information Security and Cyber-Security Research. *http://dx.doi.org/10.1142/S0219649216500441*, *15*(4). https://doi.org/10.1142/S0219649216500441

Chang, L. S., Most, K. S., & Brain, C. W. (1983). The Utility of Annual Reports: An International Study. *Journal of International Business Studies 1983 14:1*, *14*(1), 63–84. https://doi.org/10.1057/PALGRAVE.JIBS.8490507

Chapple, W., & Moon, J. (2005). Corporate social responsibility (CSR) in Asia a seven-country study of CSR Web site reporting. *Business and Society*, *44*(4), 415–441. https://doi.org/10.1177/0007650305281658

Charkham, J. P. (1995). *Keeping good company : a study of corporate governance in five countries*. 389.

Cheffins, B. R. (2012). The History of Corporate Governance. *SSRN Electronic Journal*, *January*. https://doi.org/10.2139/ssrn.1975404

Chen, T. ; R. J. (2004). *The Evolution of Viruses and Worms*. 289–310. https://doi.org/10.1201/9781420030884-19

Cheung, Y. L., Jiang, P., & Tan, W. (2010). A transparency Disclosure Index measuring disclosures: Chinese listed companies. *Journal of Accounting and Public Policy*, *29*(3), 259–280. https://doi.org/10.1016/j.jaccpubpol.2010.02.001

Chithambo, L., & Tauringana, V. (2014). Company specific determinants of greenhouse gases disclosures. *Journal of Applied Accounting Research*, *15*(3), 323–338. https://doi.org/10.1108/JAAR-11-2013-0087

Choe, H., Kho, B. C., & Stulz, R. M. (2005). Do domestic investors have an edge? The

trading experience of foreign investors in Korea. *Review of Financial Studies*, *18*(3), 795–829. https://doi.org/10.1093/rfs/hhi028

Choi, B.B., Lee, D. and Psaros, J. (2010). An analysis and explanation of Australian company carbon emission disclosures. *Paper presented at 2010 AFAANZ Conference, Christchurch, July 3-5.*

Choi, F. D. S. (1973). Financial Disclosure and Entry to the European Capital Market. *Journal of Accounting Research*, *11*(2), 159. https://doi.org/10.2307/2490187

Chong, Alberto; López de Silanes, F. (2007). Investor Protection and Corporate Governance. En S. U. P. (2007) (Ed.), *Investor Protection and Corporate Governance*. The World Bank. https://doi.org/10.1596/978-0-8213-6913-5

Chong, A., & Lopez-de-Silanes, F. (2007). *Investor protection and corporate governance : firm-level evidence across Latin America*. 557.

Chow, C. W., & Wong-Boren, A. (1987). Voluntary Financial Disclosure by Mexican Corporations. *Accounting Review*, *62*(3), 533. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=4496048&S=R&D=bth&EbscoContent=dGJyMNLe80SeqLE4y9f3OLCmr0uep7ZSsKi4TLSWxWXS&ContentCustomer=dGJyMPGqtkqxra5Rue3sfefwuY3x2%2FAA%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=449604

Chu, C. I., Chatterjee, B., & Brown, A. (2013). The current status of greenhouse gas reporting by Chinese companies: A test of legitimacy theory. *Managerial Auditing Journal*, *28*(2), 114–139. https://doi.org/10.1108/02686901311284531

Clarkson, P. M., Fang, X., Li, Y., & Richardson, G. (2013). The relevance of environmental disclosures: Are such disclosures incrementally informative? *Journal of Accounting and Public Policy*, *32*(5), 410–431. https://doi.org/10.1016/J.JACCPUBPOL.2013.06.008

Clarkson, P. M., Li, Y., Richardson, G. D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis. *Accounting, Organizations and Society*, *33*(4–5), 303–327. https://doi.org/10.1016/j.aos.2007.05.003

Clinton, L., & Higgins, J. (2020). *Cyber-Risk Oversight Cyber-Risk Oversight*.

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405.

https://doi.org/10.1111/J.1468-0335.1937.TB00002.X

Coles, J. L., Daniel, N. D., & Naveen, L. (2008). Boards: Does one size fit all? *Journal of Financial Economics*, *87*(2), 329–356. https://doi.org/10.1016/J.JFINECO.2006.08.008

Collier, P., & Institute of Chartered Accountants in England and Wales. Research Board. (1992). *Audit committees in large UK companies.* 203.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems and Decisions 2013 33:4*, *33*(4), 469–470. https://doi.org/10.1007/S10669-013-9484-Z

Comisión Europea. (2022). *Economía justa y sostenible : la Comisión establece normas para que las empresas respeten los derechos humanos y el medio ambiente en las cadenas de suministro mundiales*. https://ec.europa.eu/commission/presscorner/detail/es/ip_22_1145

Comisión Interamericana de Telecomunicaciones. (2004). *Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética*.

Comisión Nacional de Valores. (2019). *Codigo de Gobierno Societario - Resolucion General 797 2019*. https://www.erreius.com/Legislacion/documento/20190619075647772/resolucion-general-797-2019-comision-nacional-de-valores-codigo-de-gobierno-societario-memoria-informacion-modificacion-normas-nt-2013

Committee Basel. (2015). Standards: Revised Pillar 3 Disclosure Requirements. En *Bank for International Settlements* (Número January). http://www.bis.org/bcbs/publ/d309.pdf

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Consejo coordinador empresarial. (2018). *Código de principios y mejores prácticas de Gobierno Corporativo*.

Convenio de Budapest, | (2001).

Cooke, T. E., & Wallace, R. S. O. (1989). Global Surveys of Corporate Disclosure Practices and Audit Firms: A Review Essay. *Accounting and Business Research*, *20*(77), 47–57. https://doi.org/10.1080/00014788.1989.9729394

COSO. (2017). *COSO II ERM*.

CPMI-IOSCO. (2016). *Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures*. www.bis.org

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Creese, S. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Crowdstrike. (2021). *The evolution of ransomware: how to protect against new adversary trends and methods*. 1–9.

CSA. (2017). *CSA Multilateral Staff Notice 51-347-Disclosure of cyber security risks and incidents*. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

CSA ACVM. (2013). *CSA Staff Notice 11-326 - Cyber Security*.

CSA ACVM. (2017). *CSA Staff Notice 33-321: Cyber Security and Social Media*. https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2017/2017oct19-33-321-avis-acvm-en.pdf

CSA ACVM. (2019). *Disclosure of cyber security risks and incidents*. *2017*, 605–608.

CyBOK. (2019). The Cyber Security Body of Knowledge (CyBoK) 1.0. *CyBoK*, 299. https://www.cybok.org/

CyBOK. (2021). Introduction to CyBOK Knowledge Areas. *The Cyber Security Body of Knowledge*, 22. www.cybok.org

Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *https://doi.org/10.1080/10580530701586136*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Dalton, D. R., Hitt, M. A., Certo, S. T., & Dalton, C. M. (2007). The Fundamental Agency Problem and Its Mitigation. *The Academy of Management Annals*, *1*(1), 1–64. https://doi.org/10.1080/078559806

Darus, F., Mohd Zuki, H. I., & Yusoff, H. (2019). The path to sustainability: Understanding organisations' environmental initiatives and climate change in an emerging economy. *European Journal of Management and Business Economics*, *29*(1), 84–96. https://doi.org/10.1108/EJMBE-06-2019-0099

Datt, R. R., Luo, L., & Tang, Q. (2019). Corporate voluntary carbon disclosure strategy and carbon performance in the USA. *Accounting Research Journal*, *32*(3), 417–435. https://doi.org/10.1108/ARJ-02-2017-0031

Day, J. (2018). *Privacy and Cybersecurity Developments in Latin America*. https://www.lexology.com/library/detail.aspx?g=c0701531-2665-4e4b-a87b-00434e25d55f

De Villiers, C., Hsiao, P.-C. K., & Maroun, W. (2020). Introduction to the Routledge Handbook of Integrated Reporting : An overview of integrated reporting and this book, which entails different perspectives on a maturing field and a framework for future research. *The Routledge Handbook of Integrated Reporting*, 1–14. https://doi.org/10.4324/9780429279621-1

Deegan, C. (2002). Introduction: The legitimising effect of social and environmental disclosures – a theoretical foundation. En *Accounting, Auditing & Accountability Journal* (Vol. 15, Número 3, pp. 282–311). MCB UP Ltd. https://doi.org/10.1108/09513570210435852

Deloitte. (2012). *Guía Práctica Consejeros del Comité de Auditoría*.

Deloitte. (2015). *Cybersecurity: The changing role of audit committee and internal audit Contents*. 16. http://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

Deloitte. (2016). *Cyber security: The changing role of the Board and the Audit Committee*. *June*, 5. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

Deloitte. (2019a). *Índice Global de Ciberseguridad - 2018*. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html

Deloitte. (2019b). Managing Cyber Risk in a Digital Age. *Coso*, 28. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Deloitte. (2021a). *Business-aligned cyber strategy | Deloitte | Cyber Risk*. https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/business-aligned-cyber-strategy.html

Deloitte. (2021b). *Practicas nacionales versus practicas internacionales Gobierno Corporativo*.

Deloitte. (2021c). *Progress at a snail's pace*. file:///C:/Users/HP/Desktop/gx-women-in-the-boardroom-seventh-edition (1).pdf

Denis, D. K. (2001). Twenty-five years of corporate governance research … and counting. *Review of Financial Economics*, *10*(3), 191–212. https://doi.org/10.1016/S1058-3300(01)00037-4

DeZoort, F. T., Hermanson, D., Archambeault, D., & Reed, S. (2002). Audit Committee Effectiveness: A Synthesis of the Empirical Audit Committee Literature. *Audit Committee Effectiveness: A Synthesis of the Empirical Audit Committee Literature*, *21*. https://digitalcommons.kennesaw.edu/facpubs/1495

Dezsö, C. L., & Ross, D. G. (2012). Does female representation in top management improve firm performance? A panel data investigation. *Strategic Management Journal*, *33*(9), 1072–1089. https://doi.org/10.1002/SMJ.1955

Dimaggio, P. (1982). Cultural Capital and School Success : The Impact of Status Culture Participation on the Grades. *American Sociological Review*, *47*(2), 189–201.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147. https://doi.org/10.2307/2095101

Division of Corporation Finance, & SEC. (2011). *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Dobran, B. (2021). *17 Types of Cyber Security Attacks To Protect Against in 2021*. https://phoenixnap.com/blog/cyber-security-attack-types/

Domenech, J. J. G. (2017). La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE. *REVISTA LEX MERCATORIA Doctrina, Praxis, Jurisprudencia y Legislación*, 37–42. https://doi.org/10.21134/LEX.VI.534

Donnelly, R., & Mulcahy, M. (2008). Board Structure, Ownership, and Voluntary Disclosure in Ireland. *Corporate Governance: An International Review*, *16*(5), 416–429. https://doi.org/10.1111/j.1467-8683.2008.00692.x

Dungey, M., Flavin, T., O'Connor, T., & Wosser, M. (2022). Non-financial corporations and systemic risk. *Journal of Corporate Finance*, *72*, 102129. https://doi.org/10.1016/J.JCORPFIN.2021.102129

E&Y. (2018). *Cybersecurity disclosure benchmarking*.

E&Y. (2019). *What Companies are Disclosing About Cybersecurity Risk and Oversight*. 1–7.

E&Y. (2020). *What companies are disclosing about cybersecurity risk and oversight in 2020*. *August*.

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law and Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Eisenberg, M. A. (1976). *The structure of the corporation : a legal analysis*. https://books.google.com/books/about/The_Structure_of_the_Corporation.html?hl=es&id=pxY-AQAAIAAJ

Eisenberg, T., Sundgren, S., & Wells, M. T. (1998). Larger board size and decreasing firm value in small firms. *Journal of Financial Economics*, *48*(1), 35–54. https://doi.org/10.1016/s0304-405x(98)00003-8

Eisenhardt, K. M. (1985). Control: Organizational and Economic Approaches. *http://dx.doi.org/10.1287/mnsc.31.2.134*, *31*(2), 134–149. https://doi.org/10.1287/MNSC.31.2.134

Elamer, A. A., AlHares, A., Ntim, C. G., & Benyazid, I. (2018). The corporate governance–risk-taking nexus: evidence from insurance companies. *International Journal of Ethics and Systems*, *34*(4), 493–509. https://doi.org/10.1108/IJOES-07-

2018-0103

Elamer, A. A., Ntim, C. G., Abdou, H. A., & Pyke, C. (2020). Sharia supervisory boards, governance structures and operational risk disclosures: Evidence from Islamic banks in MENA countries. *Global Finance Journal*, *46*, 100488. https://doi.org/10.1016/J.GFJ.2019.100488

Elgadi, E., & Ghardallou, W. (2022). Gender diversity, board of director's size and Islamic banks performance. *International Journal of Islamic and Middle Eastern Finance and Management*, *15*(3), 664–680. https://doi.org/10.1108/IMEFM-09-2019-0397/FULL/PDF

Eling, M., & Schnell, W. (2016a). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122/FULL/PDF

Eling, M., & Schnell, W. (2016b). What do we know about cyber risk and cyber risk insurance? En *Journal of Risk Finance* (Vol. 17, Número 5, pp. 474–491). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-09-2016-0122

Ellimäki, P., Gómez-Bolaños, E., Hurtado-Torres, N., & Aragón-Correa, J. A. (2021). Do global firms increase their environmental disclosure and performance? Symbolic versus effective operations and the moderating role of liability of origin. Legitimation implications. *Industrial Marketing Management*, *92*, 354–363. https://doi.org/10.1016/J.INDMARMAN.2019.10.015

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*(6), 597–603. https://doi.org/10.1016/0167-4048(93)90056-B

Elsayed, M., Elshandidy, T., & Ahmed, Y. (2022). Corporate failure in the UK: An examination of corporate governance reforms. *International Review of Financial Analysis*, *82*, 102165. https://doi.org/10.1016/J.IRFA.2022.102165

Elshandidy, T., & Neri, L. (2015). Corporate Governance, Risk Disclosure Practices, and Market Liquidity: Comparative Evidence from the UK and Italy. *Corporate Governance: An International Review*, *23*(4), 331–356. https://doi.org/10.1111/corg.12095

Elshandidy, T., Shrives, P. J., Bamber, M., & Abraham, S. (2018). Risk reporting: A

review of the literature and implications for future research. *Journal of Accounting Literature*, *40*, 54–82. https://doi.org/10.1016/j.acclit.2017.12.001

Elzahar, H., & Hussainey, K. (2012). Determinants of narrative risk disclosures in UK interim reports. *Journal of Risk Finance*, *13*(2), 133–147. https://doi.org/10.1108/15265941211203189/FULL/PDF

ENISA. (2015). Definition of Cybersecurity | Gaps and overlaps in standardisation. En *European Union Agency For Network And Information Security: Vol. v1.0* (Número December).

Enrique, & Bonsón, E. T. (2004). *La difusión voluntaria de información financiera en Internet. Un análisis comparativo entre Estados Unidos, Europa del Este y la Unión Europea*.

Ernst & Young. (2019). *What Boards Are Doing Today to Better Oversee Cyber Risk*. *July*, 1–6.

Ernst & Young. (2021). *EY Global Information Security Survey 2021: Cybersecurity: how do you rise above the waves of a perfect storm?*

Ernstberger, J., & Grüning, M. (2013). How do firm- and country-level governance mechanisms affect firms' disclosure? *Journal of Accounting and Public Policy*, *32*(3), 50–67. https://doi.org/10.1016/J.JACCPUBPOL.2013.02.003

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

EU. (2014). *Directive 2014/95 / EU of the European Parliament and of the Council - of October 22, 2014*.

EU. (2016). *EU general data protection regulation* (Vol. 2014, Número April).

EU. (2019). *Regulation (EU) 2019/881*. Regulation (EU) 2019/881 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

Europea, U. (2015). *Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document*. https://doi.org/10.1787/9789264245471-en

Excelencia, E. E. de. (2022). *Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál*

*escoger?* https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-riesgo-cuantitativa-vs-cualitativa-cual-escoger/

EY. (2018). *SEC guidance on cybersecurity: board considerations* (Número March). https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cybersecurity/ey-sec-guidance-on-cybersecurity-board-considerations.pdf

EY. (2020). *EY Global Information Security Survey 2020. How does security evolve from bolted on to built-in?* https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf

EY. (2021). *Board Agenda 2021*. *1*(1), 21.

Fakhfakh, I., & Jarboui, A. (2022). Board of director's effectiveness, audit quality and ownership structure: impact on audit risk-Tunisian evidence. *Journal of Accounting in Emerging Economies*, *12*(3), 468–485. https://doi.org/10.1108/JAEE-07-2020-0158/FULL/PDF

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustment of Stock Prices to New Information. *International Economic Review*, *10*(1), 1. https://doi.org/10.2307/2525569

Fama, E. F., & Jensen, M. C. (1983). Separation of Ownership and Control. *Journal of Law & Economics*, *26*. https://heinonline.org/HOL/Page?handle=hein.journals/jlecono26&id=313&div=&collection=

Farrell, K. A., & Hersch, P. L. (2005). Additions to corporate boards: the effect of gender. *Journal of Corporate Finance*, *11*(1–2), 85–106. https://doi.org/10.1016/J.JCORPFIN.2003.12.001

FASB. (1994). Statement of Financial Accounting Standards No. 119, Disclosure about Derivative Financial Instruments and Fair Value of Financial Instruments. *Financial*

*Accounting Standards Board: Norwalk, Connecticut*, *119*.

FASB. (1998). Statement of Financial Accounting Standards No. 133, Accounting for Derivative Instruments and Hedging Activities. *Financial Accounting Standards Board: Norwalk, Connecticut.*, *133*.

Fidler, D. P. (2020). Cybersecurity in the Time of COVID-19. *Council on Foreign Relations, 2020*, 7–9. https://www.cfr.org/blog/cybersecurity-time-covid-19

Fifka, M. S., & Pobizhan, M. (2014). An institutional approach to corporate social responsibility in Russia. *Journal of Cleaner Production*, *82*, 192–201. https://doi.org/10.1016/j.jclepro.2014.06.091

Financial Standards Foundation. (2011). Achieving Effective Boards. *Global Corporate Governance Forum, June*.

Fontaine, David; Reed, J. (2018). *Cybersecurity: The SEC's Wake-up Call to Corporate Directors*. Harvard Law School. https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/

Fortinet. (2022). *Fortinet registró 137 mil millones de intentos de ciberataques en América Latina en la primera mitad del año.* https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

Francoeur, C., Labelle, R., & Sinclair-Desgagné, B. (2008). Gender Diversity in Corporate Governance and Top Management. *Journal of Business Ethics 2007 81:1*, *81*(1), 83–95. https://doi.org/10.1007/S10551-007-9482-5

Fraser, J. S. B. J. (2010). *Enterprise risk management*.

Freedman, M., & Jaggi, B. (2005). Global warming, commitment to the Kyoto protocol, and accounting disclosures by the largest global public firms from polluting industries. *The International Journal of Accounting*, *40*(3), 215–232. https://doi.org/10.1016/J.INTACC.2005.06.004

Freeman, E. (1984). *Edward Freeman*.

Freeman, R. E., & Mcvea, J. (2001). *A Stakeholder Approach to Strategic Management*.

Freeman, R. E., & Reed, D. L. (1983). Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review*, *25*(3), 88–106.

https://doi.org/10.2307/41165018

Frias-Aceituno, J. V., Rodríguez-Ariza, L., & Garcia-Sánchez, I. M. (2014). Explanatory Factors of Integrated Sustainability and Financial Reporting. *Business Strategy and the Environment*, *23*(1), 56–72. https://doi.org/10.1002/bse.1765

Friedman, M. A. (1970). *The social responsibility of business is to increase its profits*. https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html

G20/OECD. (2016). Principles of Corporate Governance. En *G20/OECD Principles of Corporate Governance*. https://doi.org/10.1787/9789264257443-tr

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

García-Sánchez, I. M., Gómez-Miranda, M. E., David, F., & Rodríguez-Ariza, L. (2019). Board independence and GRI-IFC performance standards: The mediating effect of the CSR committee. *Journal of Cleaner Production*, *225*, 554–562. https://doi.org/10.1016/J.JCLEPRO.2019.03.337

Garcia-Sanchez, I. M. of the I. M. C. on the V. D. of C. I., Cuadrado-Ballesteros, B., & Frias-Aceituno, J. V. (2016). Impact of the Institutional Macro Context on the Voluntary Disclosure of CSR Information. *Long Range Planning*, *49*(1), 15–35. https://doi.org/10.1016/J.LRP.2015.02.004

Gelfond, S., Wechsler, J., Cohen, H., & Llp, J. (2017). *Top 10 Practice tips by experts: risk factors*.

Gendron, Y., & Bédard, J. (2006). On the constitution of audit committee effectiveness. *Accounting, Organizations and Society*, *31*(3), 211–239. https://doi.org/10.1016/J.AOS.2005.03.002

German Government Commission. (2022). *Deutscher Corporate Governance Kodex*. https://doi.org/10.1515/zinso-2018-0608

Giner, B. (1997). The influence of company characteristics and accounting regulation on information disclosed by Spanish firms. *https://doi.org/10.1080/096381897336863*, *6*(1), 45–68. https://doi.org/10.1080/096381897336863

Gómez Vieites, A. (2006). *Enciclopedia de la seguridad informática*.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. En *Computer Security Journal* (Vol. 19, Número 2, pp. 1–7). Computer Security Institute.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692

Gray, R., Kouhy, R., & Lavers, S. (1995). Corporate social and environmental reporting A review of the literature and a longitudinal study of UK disclosure. *Accounting, Auditing & Accountability Journal*, *8*(2), 47–77. https://doi.org/10.1108/09513579510146996

GRI. (2016). GRI 418: Customer privacy 2016 418. *GRI Standards*. www.globalreporting.org

Grossman, B. S. J., & Stiglitz, J. E. (1980). *On the Impossibility of Informationally Efficient Markets Author ( s ): Sanford J . Grossman and Joseph E . Stiglitz Source :*

*The American Economic Review , Jun ., 1980 , Vol . 70 , No . 3 ( Jun ., 1980 ), pp . 393- Published by : American Economic Associ*. *70*(3), 393–408.

GSSB. (2016). GRI 418: Privacidad Del Cliente 2016. *GRI Standards*.

Gul, F. A., Srinidhi, B., & Ng, A. C. (2011). Does board gender diversity improve the informativeness of stock prices? *Journal of Accounting and Economics*, *51*(3), 314–338. https://doi.org/10.1016/J.JACCECO.2011.01.005

Gunter, O. (2004). The Phishing Guide. *History*.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. En *Managerial Auditing Journal* (Vol. 34, Número 7, pp. 808–834). Emerald Group Publishing Ltd. https://doi.org/10.1108/MAJ-09-2018-2004

Hacienda, M. D. E., & Hacienda, S. D. E. (2022). *Ley 20382*. 1–34.

Haniffa, R. M., & Cooke, T. E. (2002). Culture, Corporate Governance and Disclosure in Malaysian Corporations. *Abacus*, *38*(3), 317–349. https://doi.org/10.1111/1467-6281.00112

Haniffa, R. M., & Cooke, T. E. (2005). The impact of culture and governance on corporate social reporting. *Journal of Accounting and Public Policy*, *24*(5), 391–430. https://doi.org/10.1016/j.jaccpubpol.2005.06.001

Haque, S., & Deegan, C. (2010). Corporate Climate Change-Related Governance Practices and Related Disclosures: Evidence from Australia. *Australian Accounting Review*, *20*(4), 317–333. https://doi.org/10.1111/J.1835-2561.2010.00107.X

Hardiyansah, M., & Agustini, A. T. (2020). Analysis of carbon emissions disclosure and firm value: Type of industry as a moderating model. *International Journal of Scientific and Technology Research*, *9*(2), 1125–1132.

Harrigan, K. R. (2017). Numbers and Positions Of Women Elected to Corporate Boards. *https://doi.org/10.5465/255580*, *24*(3), 619–625. https://doi.org/10.5465/255580

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*, *73*, 102–113. https://doi.org/10.1016/J.COSE.2017.10.008

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, *3*, 1117–1124. https://doi.org/10.1016/J.PROMFG.2015.07.186

Hermalin, B. E., & Weisbach, M. S. (2003). *Boards of Directors as an Endogenously*

*Determined Institution: A Survey of the Economic Literature*. https://doi.org/10.3386/W8161

Héroux, S., & Fortin, A. (2020a). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S., & Fortin, A. (2020b). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Hijink, J. B. S. (2010). *Publicatieverplichtingen voor beursvennootschappen*.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2852519

Hillman, A. J., Cannella, A. A., & Paetzold, R. L. (2000). The Resource Dependence Role of Corporate Directors: Strategic Adaptation of Board Composition in Response to Environmental Change. *Journal of Management Studies*, *37*(2), 235–256. https://doi.org/10.1111/1467-6486.00179

Holland & Knight. (2021). *SEC Issues First-Ever Penalties for Deficient Cybersecurity Risk Controls*. https://www.hklaw.com/en/insights/publications/2021/06/sec-issues-first-ever-penalties-for-deficient-cybersecurity-risk

Holland, L., & Foo, Y. B. (2003). Differences in environmental reporting practices in the UK and the US: The legal and regulatory context. *British Accounting Review*, *35*(1), 1–18. https://doi.org/10.1016/S0890-8389(02)00127-0

Hope, O.-K. (2003). *Disclosure Practices, Enforcement of Accounting Standards, and Analysts' Forecast Accuracy: An International Study - Hope - 2003 - Journal of Accounting Research - Wiley Online Library*. https://onlinelibrary.wiley.com/doi/10.1111/1475-679X.00102

Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies*, *21*(4), 1005–1045. https://doi.org/10.1007/s11142-016-9371-1

Hunt, B. (2003). *The Timid Corporation: Why Business is Terrified of Taking Risk*.

IBGC. (2015). Código das Melhores Práticas de Governança Corporativa. En *Instituto Brasileiro de Governança Corporativa*.

http://www.ibgc.org.br/userfiles/2014/files/CMPGPT.pdf

ICAWE. (2011). *Reporting Business Risks: Meeting Expectations*.

IDB; OAS. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

International Integrated Reporting Council. (2021). < IR > Framework about the IIRC. *Jo*, *January*, 58. https://integratedreporting.org/wp-content/uploads/2021/01/InternationalIntegratedReportingFramework.pdf

International Telecommunication Union. (2008). Overview Cybersecurity. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I

Internet Security Alliance and American National Standards. (2010). The Financial Management of Cyber Risk: An Implementation Framework for CFOs. *Order A Journal On The Theory Of Ordered Sets And Its Applications*.

Investor Stewardship Group. (2017). Corporate Governance Principles For US Listed Companies. *Isg*, 1–5. https://isgframework.org/corporate-governance-principles/

IOSCO. (2016). *Cyber Security in Securities Markets – An International Perspective Report on IOSCO ' s cyber risk coordination efforts*.

IRRC. (2016). *The Corporate Risk Factor Disclosure Landscape*. *January*, 27. https://www.weinberg.udel.edu/irrci/research/887

ISO. (2011). ISO 26000. *The Corporate Responsibility code book*, 83–129. https://doi.org/10.4324/9781351278881-5

ISO. (2012). *ISO/IEC 27032: Information technology — Security techniques — Guidelines for cybersecurity*. ISO 27032. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO. (2013). *ISO 27002*.

ISO. (2018). *ISO 31000 Risk management*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO. (2020). *ISO/IEC 27014:2020 - Information security, cybersecurity and privacy*

*protection — Governance of information security*. https://www.iso.org/standard/74046.html

*ISO 37000*. (2021).

ITU. (2007). *ITU Global Cybersecurity Agenda - A Framework for International Cooperation in Cybersecurity*. https://www.itu.int/osg/spuold/cybersecurity/gca/

ITU. (2017). Global Cybersecurity Index (GCI) 2017. En *ITU-D Global*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU. (2018). *Global Cybersecurity Index (GCI) 2018 ITUPublications Studies & research*.

ITU. (2020). *ITU Publications*. Índice Global de Ciberseguridad 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

ITU. (2021a). *About the International Telecommunication Union (ITU)*. https://www.itu.int/es/about/Pages/default.aspx

ITU. (2021b). Global Cybersecurity Index (GCI). En *ITU Publications*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU & ABI Research. (2014). *Global Cybersecurity I N D E X*. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

Jaggi, B., & Low, P. Y. (2000). Impact of Culture, Market Forces, and Legal System on Financial Disclosures. *The International Journal of Accounting*, *35*(4), 495–519. https://doi.org/10.1016/S0020-7063(00)00076-5

Jamali, D., Safieddine, A. M., & Rabbath, M. (2008). Corporate Governance and Corporate Social Responsibility Synergies and Interrelationships. *Corporate Governance: An International Review*, *16*(5), 443–459. https://doi.org/10.1111/J.1467-8683.2008.00702.X

Jamaludin, N. D., Sanusi, Z. M., & Kamaluddin, A. (2015). Board Structure and Earnings Management in Malaysian Government Linked Companies. *Procedia Economics and Finance*, *28*, 235–242. https://doi.org/10.1016/S2212-5671(15)01105-3

James P. Anderson, Sheila Brand, Li Gong, T. H. (2004). Firewalls: an Expert Roundtable. En *Book Security, Statistical Methods in Computer* (Edition, E, pp. 333–350). CRC Press. https://doi.org/10.1201/9781420030884-21

Jensen, M. C. (1993). The Modern Industrial Revolution, Exit, and the Failure of Internal

Control Systems. *The Journal of Finance*, *48*(3), 831–880. https://doi.org/10.1111/j.1540-6261.1993.tb04022.x

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: managerial behavior, agency costs and ownership structure. *Journal Of Financial Economics*, *3*, 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Jizi, M. I., Salama, A., Dixon, R., & Stratling, R. (2014). Corporate Governance and Corporate Social Responsibility Disclosure: Evidence from the US Banking Sector. *Journal of Business Ethics*, *125*(4), 601–615. https://doi.org/10.1007/s10551-013-1929-2

Jorion, P. (2002). *The Accounting Review* (Vol. 77).

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019

Kang, H., Cheng, M., & Gray, S. J. (2007). Corporate Governance and Board Composition: diversity and independence of Australian boards. *Corporate Governance: An International Review*, *15*(2), 194–207. https://doi.org/10.1111/J.1467-8683.2007.00554.X

Kanter, R. M. (1977). *Men and women of the corporation*. 348. https://books.google.com/books/about/Men_And_Women_Of_The_Corporation.html?hl=es&id=7L63AAAAIAAJ

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond Cybersecurity: Protecting Your Digital Business*. *Exhibit 1*, 1–9. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1119026849,descCd-buy.html

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Kasznik, R., & Lev, B. (1995). To warn or not to warn: Management disclosures in the face of an earnings surprise. *Accounting review: A quarterly journal of the American Accounting Association*, *70*(1), 113–134.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2010). The Worldwide Governance

Indicators: A Summary of Methodology, Data and Analytical Issues. *The World Bank*, *5430*(September), 1–29.

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020a). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/j.jbusres.2019.11.025

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020b). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/J.JBUSRES.2019.11.025

Khatib, S. F. A., Abdullah, D. F., Elamer, A. A., & Abueid, R. (2021). Nudging toward diversity in the boardroom: A systematic literature review of board diversity of financial institutions. *Business Strategy and the Environment*, *30*(2), 985–1002. https://doi.org/10.1002/BSE.2665

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys and Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Kiesow Cortez, E., & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation*, *January*, 1–23. https://doi.org/10.1017/err.2022.10

Kiliç, M., Kuzey, C., & Uyar, A. (2015). The impact of ownership and board structure on corporate social responsibility (CSR) reporting in the Turkish banking industry. *Corporate Governance (Bingley)*, *15*(3), 357–374. https://doi.org/10.1108/CG-02-2014-0022

King, M. (2016). Report on corporate governance for South Africa 2016. *King IV Report on Corporate Governance for South Africa*, 1–128.

KOF. (2020). *Globalization Report 2020*.

Konishi, N., & Ali, M. M. (2007). Risk reporting of Japanese companies and its association with corporate characteristics. *undefined*, *4*(3), 263–285. https://doi.org/10.1504/IJAAPE.2007.016281

Kor, Y. Y. (2006). Direct and interaction effects of top management team and board compositions on R&D investment strategy. *Strategic Management Journal*, *27*(11),

1081–1099. https://doi.org/10.1002/SMJ.554

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597–607. https://doi.org/10.1016/J.IM.2003.08.001

Kravet, T., & Muslu, V. (2013). Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies*, *18*(4), 1088–1122. https://doi.org/10.1007/s11142-013-9228-9

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/J.JISA.2014.09.005

Kühn, A. L., Stiglbauer, M., & Fifka, M. S. (2018). Contents and Determinants of Corporate Social Responsibility Website Reporting in Sub-Saharan Africa: A Seven-Country Study. En *Business and Society* (Vol. 57, Número 3). https://doi.org/10.1177/0007650315614234

La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (1999). Corporate Ownership Around the World. *The Journal of Finance*, *54*(2), 471–517. https://doi.org/10.1111/0022-1082.00115

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., & Vishny, R. (2000). Investor protection and corporate governance. *Journal of Financial Economics*, *58*(1–2), 3–27. https://doi.org/10.1016/s0304-405x(00)00065-9

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. *Journal of Political Economy*, *106*(6), 1113–1155. https://doi.org/10.1086/250042

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., & Vishny, R. W. (1997). Legal Determinants of External Finance. *The Journal of Finance*, *52*(3), 1131–1150. https://doi.org/10.1111/J.1540-6261.1997.TB02727.X

Lajili, K., & Zéghal, D. (2005). A content analysis of risk management disclosures in canadian annual reports. *Canadian Journal of Administrative Sciences*, *22*(2), 125–142. https://doi.org/10.1111/j.1936-4490.2005.tb00714.x

Larmou, S., & Vafeas, N. (2009). *The relation between board size and firm performance in firms with a history of poor operating performance*.

https://doi.org/10.1007/s10997-009-9091-z

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*. https://doi.org/10.1109/PCCC.2016.7820663

Lee, R. P., Chen, Q., & Hartmann, N. N. (2016). Enhancing Stock Market Return with New Product Preannouncements: The Role of Information Quality and Innovativeness. *Journal of Product Innovation Management*, *33*(4), 455–471. https://doi.org/10.1111/JPIM.12284

Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, *8*(4), 1–15. https://doi.org/10.3390/risks8040128

Lernia, C. Di, Hardy, C., & Dori, A. (2020). *Cyber-related Risk Disclosure in Australia: Evidence from the ASX200 Journal Title: Company and Securities*. *5*, 23–29.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/J.ACCINF.2018.06.003

Li, W., & Zhang, R. (2010). Corporate Social Responsibility, Ownership Structure, and Political Interference: Evidence from China. *Journal of Business Ethics*, *96*(4), 631–645. https://doi.org/10.1007/s10551-010-0488-z

Liesen, A., Hoepner, A. G., Patten, D. M., & Figge, F. (2015). Does stakeholder pressure influence corporate GHG emissions reporting? Empirical evidence from Europe. *Accounting, Auditing and Accountability Journal*, *28*(7), 1047–1074. https://doi.org/10.1108/AAAJ-12-2013-1547

Lim, S., Matolcsy, Z., & Chow, D. (2007). The Association between Board Composition and Different Types of Voluntary Disclosure. *European Accounting Review*, *16*(3), 555–583. https://doi.org/10.1080/09638180701507155

Linck, J. S., Netter, J. M., & Yang, T. (2008). The determinants of board structure. *Journal of Financial Economics*, *87*(2), 308–328. https://doi.org/10.1016/J.JFINECO.2007.03.004

Linsley, P. M., & Shrives, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK companies. *The British Accounting Review*, *38*(4), 387–404. https://doi.org/10.1016/J.BAR.2006.05.002

Lippmann, W. (1914). *Drift and mastery : an attempt to diagnose the current unrest*. Prentice-Hall.

Lipton, M., & Lorsch, J. W. (1992). A modest proposal for improved corporate governance: Business source. *Business Lawyer*, *42*(1), 59–78. http://web.a.ebscohost.com.eserv.uum.edu.my/bsi/detail?vid=19&sid=e3a1315c-d940-4744-b224-1ce498b43ead@sessionmgr4005&hid=4114&bdata=JnNpdGU9YnNpLWxpdmU=#db=bth&AN=5963897

Lopes, P. T., & Rodrigues, L. L. (2007). Accounting for financial instruments: An analysis of the determinants of disclosure in the Portuguese stock exchange. *The International Journal of Accounting*, *42*(1), 25–56. https://doi.org/10.1016/J.INTACC.2006.12.002

Loughran, T., & Mcdonald, B. (2011). When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. *Journal of Finance*, *66*(1), 35–65. https://doi.org/10.1111/j.1540-6261.2010.01625.x

Luo, L., Tang, Q., & Lan, Y. C. (2013). Comparison of propensity for carbon disclosure between developing and developed countries: A resource constraint perspective. *Accounting Research Journal*, *26*(1), 6–34. https://doi.org/10.1108/ARJ-04-2012-0024

Luo, Y. (2005). Corporate governance and accountability in multinational enterprises: Concepts and agenda. En *Journal of International Management* (Vol. 11, Número 1 SPEC. ISS., pp. 1–18). Elsevier Inc. https://doi.org/10.1016/j.intman.2004.11.001

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan management review*, *20*(1), 61–74.

Mahmood, M., & Orazalin, N. (2017). Green governance and sustainability reporting in Kazakhstan's oil, gas, and mining sector: Evidence from a former USSR emerging economy. *Journal of Cleaner Production*, *164*, 389–397. https://doi.org/10.1016/J.JCLEPRO.2017.06.203

Mallin, C. (2006). *Handbook on International Corporate Governance*.

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*(3),

435–452. https://doi.org/10.1111/RMIR.12109

Marshall, A., & Weetman, P. (2007). Modelling Transparency in Disclosure: The Case of Foreign Exchange Risk Management. *Journal of Business Finance & Accounting*, *34*(5–6), 705–739. https://doi.org/10.1111/j.1468-5957.2007.02007.x

Marston, C. L., & Shrives, P. J. (1991). The use of disclosure indices in accounting research: A review article. En *The British Accounting Review* (Vol. 23, Número 3, pp. 195–210). Academic Press. https://doi.org/10.1016/0890-8389(91)90080-L

Masud, M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*. https://doi.org/10.1108/JAEE-07-2021-0237

Mayor Gómez, R. (2016). *Contenido y novedades del reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)*. Gabilex. Revista del gabinete jurídico de Castilla la Mancha.

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/RMIR.12169

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *Geneva Papers on Risk and Insurance: Issues and Practice*, *45*(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Meftah Gerged, A., Beddewela, E. S., Christopher, |, & Cowton, J. (2021). *Does the quality of country-level governance have an impact on corporate environmental disclosure? Evidence from Gulf Cooperation Council countries*. https://doi.org/10.1002/ijfe.2469

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Melis, A. (2006). Corporate Governance in Italy. En *Handbook on international Corporate Governance*.

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security*, *73*, 87–101. https://doi.org/10.1016/J.COSE.2017.10.009

Merriam -Webster. (2021). *Cybersecurity | Definition of Cybersecurity*. Merriam-Webster.com Dictionary, Merriam-Webster. https://www.merriam-webster.com/dictionary/cybersecurity

Meyer, J. W., & Rowan, B. (1977). Slett denne Institutionalized Organizations : Formal Structure as Myth and Ceremony. *American Journal of Sociology*, *83*(2), 340–363.

Middleton, B. (2017). *A History of Cyber Security Attacks 1980 to present* (T. & Francis (Ed.)).

Mintzberg, H. (1984). Who Should Control the Corporation?: *http://dx.doi.org/10.2307/41165115*, *27*(1), 90–115. https://doi.org/10.2307/41165115

Mirkovic, J., Reiher, P., & Hall, B. (2004). *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms* *.

Mitra, S., & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *https://doi.org/10.1287/isre.2015.0587*, *26*(3), 565–584. https://doi.org/10.1287/ISRE.2015.0587

Mokhtar, E. S., & Mellett, H. (2013). Competition, corporate governance, ownership structure and risk reporting. *Managerial Auditing Journal*, *28*(9), 838–865. https://doi.org/10.1108/MAJ-11-2012-0776/FULL/PDF

Moosa, I. A. (2007). Operational Risk: A Survey. *Financial Markets, Institutions & Instruments*, *16*(4), 167–200. https://doi.org/10.1111/J.1468-0416.2007.00123.X

Morse, E. A., Raval, V., & Wingender, J. R. (2018). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. En *Business Lawyer* (Vol. 73, Número 1, pp. 1–34). American Bar Association. https://doi.org/10.2139/ssrn.2711439

Moumen, N., Ben Othman, H., & Hussainey, K. (2016). Board structure and the informativeness of risk disclosure: Evidence from MENA emerging markets. *Advances in Accounting*, *35*, 82–97. https://doi.org/10.1016/J.ADIAC.2016.09.001

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*(1),

11–26. https://doi.org/10.1016/J.DSS.2013.04.004

Muñoz-Izquierdo, N., Segovia-Vargas, M. J., Camacho-Miñano, M. del M., & Pascual-Ezama, D. (2019). Explaining the causes of business failure using audit report disclosures. *Journal of Business Research*, *98*, 403–414. https://doi.org/10.1016/J.JBUSRES.2018.07.024

NACD. (2009). *Report of the NACD blue ribbon commission. Risk governance: balancing risk and reward*. https://www.wlrk.com/docs/1605831_1.pdf

Nader, R., Green, M. J., & Seligman, J. (1976). *Taming the giant corporation*. 312.

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *https://doi.org/10.1080/23738871.2016.1157619*, *1*(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

NCSC. (2022). *Essential Topics - NCSC.GOV.UK*. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious Software Threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 793–813. https://doi.org/10.1007/978-3-319-78440-3_35

NICCS. (2017). *Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies*. Explore terms: a glossary of common cybersecurity terminology. https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C ( 2017 )

Nielsen, S., & Huse, M. (2010). The Contribution of Women on Boards of Directors: Going beyond the Surface. *Corporate Governance: An International Review*, *18*(2), 136–148. https://doi.org/10.1111/J.1467-8683.2010.00784.X

NIST. (2020). NIST Privacy Framework. En *January 16, 2020*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

NITS. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

Ntim, C. G., Lindop, S., & Thomas, D. A. (2013). Corporate governance and risk reporting in South Africa: A study of corporate risk disclosures in the pre- and post-2007/2008 global financial crisis periods. *International Review of Financial Analysis*, *30*, 363–383. https://doi.org/10.1016/j.irfa.2013.07.001

Nwosu, A. U., Goyal, S. B., & Bedi, P. (2020). Blockchain Transforming Cyber-Attacks:

Healthcare Industry. *Advances in Intelligent Systems and Computing*, *1372 AISC*, 258–266. https://doi.org/10.1007/978-3-030-73603-3_24

O'Reilly, C. A., Caldwell, D. F., & Barnett, W. P. (1989). Work Group Demography, Social Integration, and Turnover. *Administrative Science Quarterly*, *34*(1), 21. https://doi.org/10.2307/2392984

OAS; ISA. (2020). *Manual de supervisión de riesgos cibernéticos para juntas corporativas*. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

OAS. (2019). Challenges of cyber risk in the financial sector for Colombia and Latin America. *Asobancaria*, 170. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Ocasio, W., & Joseph, J. (2005). Cultural adaptation and institutional change: The evolution of vocabularies of corporate governance, 1972–2003. *Poetics*, *33*(3–4), 163–178. https://doi.org/10.1016/J.POETIC.2005.10.001

OCDE. (2004). Directrices de la OCDE para la seguridad de sistemas y redes de información. En *Directrices de la OCDE para la seguridad de sistemas y redes de información*. https://doi.org/10.1787/9789264065819-es

OCDE. (2016). *Principios de Gobierno Corporativo de la OCDE y del G20*. https://doi.org/10.1787/9789264259171-es

OCIE. (2020). *OCIE Cybersecurity and Resiliency Obervations 2020*. www.sec.gov/spotlight/cybersecurity.

OECD. (1999). *OECD Principles of Corporate Governance Principles of*.

OECD. (2011). *OECD Guidelines for Multinational Enterprises 2011 Edition*. https://doi.org/10.1787/9789264115415-en

OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity. En *Digital Security Risk Management for Economic and Social Prosperity*. https://doi.org/10.1787/9789264245471-en

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/J.1539-6924.2010.01478.X

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011). Risk-related disclosures by non-finance companies: Portuguese practices and disclosure characteristics. *Managerial Auditing Journal*, *26*(9), 817–839. https://doi.org/10.1108/02686901111171466

Oliveira, J., Serrasqueiro, R., & Mota, S. N. (2018). Determinants of risk reporting by Portuguese and Spanish non-finance companies. *European Business Review*, *30*(3), 311–339. https://doi.org/10.1108/EBR-04-2017-0076/FULL/PDF

Oliver, C. (1991). *Strategic Responses to Institutional Processes*. *16*(1), 145–179.

ONU. (2011). *Developing countries most vulnerable to cyberattacks – UN*. https://news.un.org/en/story/2011/12/397922

Orman, H. (2003). The Morris worm: a fifteen-year perspective. *IEEE Security & Privacy*, *1*(5), 35–43. https://doi.org/10.1109 / MSECP.2003.1236233

Ortiz, E., & Clavel, J. G. (2006). Disclosures indexes: a propose to improve the metodology applied to the case of Human Resources disclosure included in Form 20-F. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, *35*(128), 87–113. https://doi.org/10.1080/02102412.2006.10779574

Packard, N. (2020). Three kinds of demand pull for the ARPANET into the Internet. *http://www.editorialmanager.com/cogentsocsci*, *6*(1). https://doi.org/10.1080/23311886.2020.1720565

Parker, D. B. (2007). The dark side of computing: SRI International and the study of computer crime. *IEEE Annals of the History of Computing*, *29*(1), 3–15. https://doi.org/10.1109/MAHC.2007.15

Patelli, L., & Prencipe, A. (2007). The relationship between voluntary disclosure and independent directors in the presence of a dominant shareholder. *European Accounting Review*, *16*(1), 5–33. https://doi.org/10.1080/09638180701265820

PCAOB. (2014). *Standing Advisory Group meeting cybersecurity*.

Perez-Batres, L. A., Miller, V. V, & Pisani, M. J. (2010). CSR, Sustainability and the Meaning of Global Reporting for Latin American Corporations. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-010-0614-y

Pfeffer, Jeffrey; Salancik, G. (1978). *The External Control of Organizations: A Resource Dependence Perspective by :: SSRN*.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496213

Pitrakkos, P., & Maroun, W. (2019). Evaluating the quality of carbon disclosures. *Sustainability Accounting, Management and Policy Journal*, *11*(3), 553–589. https://doi.org/10.1108/SAMPJ-03-2018-0081

Plumlee, M., Brown, D., Hayes, R. M., & Marshall, R. S. (2015). Voluntary environmental disclosure quality and firm value: Further evidence. *Journal of Accounting and Public Policy*, *34*(4), 336–361. https://doi.org/10.1016/J.JACCPUBPOL.2015.04.004

Porrúa, M., & Contreras B. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*.

Power, M. (2004). The risk management of everything. *Journal of Risk Finance*, *5*(3), 58–65. https://doi.org/10.1108/eb023001

Prado-Lorenzo, J. M., Rodríguez-Domínguez, L., Gallego-Álvarez, I., & García-Sánchez, I. M. (2009). Factors influencing the disclosure of greenhouse gas emissions in companies world-wide. *Management Decision*, *47*(7), 1133–1157. https://doi.org/10.1108/00251740910978340

Pucheta-Martínez, M. C., & Gallego-Álvarez, I. (2019). An international approach of the relationship between board attributes and the disclosure of corporate social responsibility issues. *Corporate Social Responsibility and Environmental Management*, *26*(3), 612–627. https://doi.org/10.1002/CSR.1707

PwC. (2022). *2022 Global Digital Trust Insights*.

PWC. (2018a). *2018 Global Investor Survey 2018: Anxious Optimism in a Complex World*.

PWC. (2018b). *Better Oversee Cyber Risk. November*.

PWC. (2018c). *Rethinking cybersecurity disclosures to investors - What executives and boards need to know about the SEC's guidance: June 2018*. www.pwc.com/cybersecurity

PWC. (2018d). *US2018-07: SEC issues interpretive guidance on cybersecurity disclosures*. https://viewpoint.pwc.com/dt/us/en/pwc/in_briefs/2018/2018__7_US/us201807_sec_issues__US.html

PWC. (2021). *Encuesta Global Digital Trust Insights 2021 Contenido*.

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Rel ated Disclosure. *Journal of Business Ethics*, *1*, 3. https://doi.org/10.1007/s10551-020-04717-9

RAE ASALE. (2020). *Diccionario de la lengua española*. Edición 2020. https://dle.rae.es/cibernético?m=form

Rainer, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, *8*(1), 129–147. https://doi.org/10.1080/07421222.1991.11517914

Rajgopal, S. (1999). Early evidence on the informativeness of the SEC's market risk disclosures: The case of commodity price risk exposure of oil and gas producers. *Accounting Review*, *74*(3), 251–280. https://doi.org/10.2308/accr.1999.74.3.251

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rankin, M., Windsor, C., & Wahyuni, D. (2011). An investigation of voluntary corporate greenhouse gas emissions reporting in a market governance system: Australian evidence. *Accounting, Auditing and Accountability Journal*, *24*(8), 1037–1070. https://doi.org/10.1108/09513571111184751

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121–139. https://doi.org/10.1287/ISRE.1080.0174

Reid, R., & Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies. *Information Security South Africa (ISSA)*, 1–7. https://doi.org/978-1-4799-3383-9

Renn, B. O. (2008). Risk Governance new & Forthcoming Titles. En *Sustainable Development*. https://www.routledge.com/Risk-Governance-Coping-with-Uncertainty-in-a-Complex-World/Renn/p/book/9781844072927

Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering and System Safety*, *59*(1), 49–62. https://doi.org/10.1016/S0951-8320(97)00119-1

Rennekamp, K. (2012). Processing Fluency and Investors' Reactions to Disclosure

Readability. *Journal of Accounting Research*, *50*(5), 1319–1354. https://doi.org/10.1111/J.1475-679X.2012.00460.X

Reverte, C. (2009). Determinants of corporate social responsibility disclosure ratings by Spanish listed firms. *Journal of Business Ethics*, *88*(2), 351–366. https://doi.org/10.1007/s10551-008-9968-9

Rhodes, M. J. (2010). Information Asymmetry and Socially Responsible Investment. *Journal of Business Ethics*, *95*(1), 145–150. https://doi.org/10.1007/s10551-009-0343-2

Ripley, W. Z. (1927). *Main Street and Wall Street*. https://www.amazon.es/Main-Street-Wall-William-Ripley/dp/0914348078

Rivera-Arrubla, Y. A., Zorio-Grima, A., & García-Benau, M. A. (2017). Integrated reports: Disclosure level and explanatory factors. *Social Responsibility Journal*, *13*(1), 155–176. https://doi.org/10.1108/SRJ-02-2016-0033

RobecoSAM. (2018). *The sustainability yearbook 2018*. https://www.comunicarseweb.com/sites/default/files/the_sustainability_yearbook_2018_spanish.pdf

Roberts, L. G. (1988). The ARPANET & Computer Networks. *Proceedings of the ACM Conference on The history of personal workstations*. https://doi.org/10.1145/12178

Rodríguez-Ariza, L., Frías Aceituno, J. V., & García Rubio, R. (2014). The board of directors and the sustainability report. *Revista de Contabilidad-Spanish Accounting Review*, *17*(1), 5–16. https://doi.org/10.1016/j.rcsar.2013.02.002

Rogers, E. (2003). Review Diffusion of Innovations, by Everett Rogers (1995). *Stanford University*, *1995*, 5. http://web.stanford.edu/class/symbsys205/Diffusion of Innovations.htm

Rose, C. (2007). Does female board representation influence firm performance? The Danish evidence. *Corporate Governance: An International Review*, *15*(2), 404–413. https://doi.org/10.1111/J.1467-8683.2007.00570.X

Ross, S. A. (1977). Determination of financial structure: the incentive- signalling approach. *Bell J Econ*, *8*(1), 23–40. https://doi.org/10.2307/3003485

Roundtable, B. (1978). The Role and Composition of the Board of Directors of the Large Publicly Owned Corporation — Statement of the bussiness Roundtable. *The*

*Roundtable*, *33*(4), pp . 2083-2113. https://www.jstor.org/stable/40685901?seq=1

Rowe, D. C., Ekstrom, J. J., & Lunt, B. M. (2012). Cyber-Security, IAS and the Cyber Warrior. *The Colloquium for Information Systems Security Education*.

Rupley, K. H., Brown, D., & Marshall, S. (2017). Evolution of corporate reporting: From stand-alone corporate social responsibility reporting to integrated reporting. *Research in Accounting Regulation*, *29*(2), 172–176. https://doi.org/10.1016/J.RACREG.2017.09.010

S&P. (2020). *América Latina*.

Salet, H. A. (2004). *Delaware ' s Good Faith*. *89*(2).

Sánchez, I. M. G., Domínguez, L. R., & Álvarez, I. G. (2011). Corporate governance and strategic information on the internet: A study of Spanish listed companies. *Accounting, Auditing and Accountability Journal*, *24*(4), 471–501. https://doi.org/10.1108/09513571111133063

Santiago Castro, M., Brown, C. J., & Baéz, A. (2009). Prácticas de Gobierno Corporativo en América Latina. *Revista Latinoamericana de Administración*, *43*, 26–40. http://revistaacademia.cladea.org

Sargent, John & Ghaddar, S. (2001). *International Success of Business Groups as an Indicator of National Competitiveness The Mexican Example*. https://www.tandfonline.com/doi/abs/10.1300/J140v02n03_05

SASB. (2021a). *Estándares SASB*. https://www.sasb.org/standards/download/

SASB. (2021b). *SASB Materiality Map*. https://materiality.sasb.org/

Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *Proceedings - International Conference on Distributed Computing Systems*, *2016-August*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Scaltrito, D. (2016). Voluntary disclosure in Italy: Firm-specific determinants an empirical analysis of Italian listed companies. *EuroMed Journal of Business*, *11*(2), 272–303. https://doi.org/10.1108/EMJB-07-2015-0032

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/https://doi.org/10.15394/jdfsl.2017.1476

Schubert, D; Cedarbaum, J and Schloss, W. (2015). The SEC's Two Primary Theories in Cybersecurity Enforcement Actions. *The Cybersecurity Law Report*, *1*(1), 39–70.

Scott, W. R. (2008). Approaching adulthood: The maturing of institutional theory. *Theory and Society*, *37*(5), 427–442. https://doi.org/10.1007/s11186-008-9067-z

SEC. (1997). Disclosure of Accounting Policies for Derivative Financial Instruments, and Derivative Commodity Instruments and Disclosure of Quantitative and Qualitative Information about Market Risk Inherent in Derivative Financial Instruments, Other Financial Instrum. *Federal Register*, *62*(27), 6044–6079. https://www.federalregister.gov/documents/1997/02/10/97-2991/disclosure-of-accounting-policies-for-derivative-financial-instruments-and-derivative-commodity

SEC. (2005a). *Release #33-8591: Securities Offering Reform (Section VII: Additional Exchange act Disclosure Provisions)* (Número 1294).

SEC. (2005b). *Staff Statement on Management's Report on Internal Control Over Financial Reporting*. https://www.sec.gov/info/accountants/stafficreporting.htm

SEC. (2017). *Prospectus summary, risk factors § 229.503 (Item 503)*. 473–475. https://doi.org/10.4135/9781608712380.n519

SEC. (2018a). *Federal Register Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures

SEC. (2018b). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

SEC. (2020). *17 CFR § 229.105 - (Item 105) Risk factors*. https://www.law.cornell.edu/cfr/text/17/229.105

SEC. (2021a). *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures*. https://www.sec.gov/news/press-release/2021-169

SEC. (2021b). *SEC Charges Issuer With Cybersecurity Disclosure Controls Failures*. https://www.sec.gov/news/press-release/2021-102

SEC. (2022). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. *13*(34), 1–204.

Security Boulevard. (2021). *How Offensive AI Can Disarm Cybersecurity*. https://securityboulevard.com/2021/06/how-offensive-ai-can-disarm-cybersecurity/

Shankar, K. S. (1977). *The Total Computer Security Problem: An overview*.

Shleifer, A., Vishny, R. W., Diamond, D., Easterbrook, F., Harris, M., Hellwig, M., Hines, J., Jonsson, T., Kaplan, S., Porta, R. La, Lopez-De-Silanes, F., Rajan, R., Scharfstein, D., Stulz, R., & Zingales, L. (1997). A Survey of Corporate Governance. *The Journal of Finance*, *52*(2), 737–783. https://doi.org/10.1111/J.1540-6261.1997.TB04820.X

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Security Management Handbook, Sixth Edition*, 357–380. https://doi.org/10.1201/9781420072419-28

Sinha, T., & Vaughan, E. J. (1994). Fundamentals of Risk and Insurance. En *The Journal of Risk and Insurance* (Vol. 61, Número 2). https://doi.org/10.2307/253725

Siponen, M. T., & Oinas-Kukkonen, H. (2007). *A Review of Information Security Issues and Respective Research Contributions*.

Skinner, D. J. (1997). Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics*, *23*(3), 249–282. https://doi.org/10.1016/S0165-4101(97)00010-4

Slovic, P. (1987). Perception of Risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/SCIENCE.3563507

Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations. Oxford: UK: Clarendon Press.*

Sofistic, C. (2017). *Breve historia de la Ciberseguridad*. https://www.sofistic.com/blog-Ciberseguridad/la-breve-historia-de-la-Ciberseguridad/

Solomon, J. (2010). *Corporate governance and accountability*. 414.

Solomon, J. F., Solomon, A., Norton, Si. D., & Joseph, N. L. (2000). A conceptual

framework for corporate risk disclosure emerging from the agenda for corporate goverance reform. *The British Accounting Review*, *32*(4), 447–478. https://doi.org/10.1006/bare.2000.0145

Solomon, Jill. (2019). *Corporate Governance and Accountability* (5TH ed.). John Wiley.

Souppaya, M., & Scarfone, K. (2013). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. https://doi.org/10.6028/NIST.SP.800-83R1

Spence, M. (1973). Job Market Signaling. En *The Quarterly Journal of Economics* (Vol. 87, Número 3). https://www.sciencedirect.com/science/article/pii/B9780122148507500255

Spence, M. (2002). La señalización y la estructura informativa de los mercados. *RAE: Revista Asturiana de Economía*, *25*, 49–94.

Srinidhi, B., Gul, F. A., & Tsui, J. (2011). Female Directors and Earnings Quality*. *Contemporary Accounting Research*, *28*(5), 1610–1644. https://doi.org/10.1111/J.1911-3846.2011.01071.X

Stapledon, G. (2006). The development of corporate governance in Australia. En *Handbook on International Corporate Governance*.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. En *Politics and Governance* (Vol. 6, Número 2, pp. 1–4). Cogitatio Press. https://doi.org/10.17645/pag.v6i2.1569

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/J.SSCI.2020.105143

Subcommittee of Capital Markets; Capital Markets Committee, Capital Financial and, & Federation Japan Business. (2022). *Improve the effectiveness of the revised Corporate Governance Code*. https://www.keidanren.or.jp/policy/2022/047.pdf

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review*, *20*(3), 571. https://doi.org/10.2307/258788

Superintendencia del Mercado de Valores. (2013). *Código De Buen Gobierno*

*Corporativo Para Las Sociedades Peruanas 2013*.

SuperSociedades, Confecámaras, & CCB. (2020). *Guía de Buenas Prácticas de Gobierno Corporativo para Empresas Competitivas, Productivas y Perdurables*.

Szegö, G. (2002). Measures of risk. *Journal of Banking & Finance*, *26*, 1253–1272. https://doi.org/10.1016/S1548-5315(11)70388-6

Szulc, T., & American Assembly. (1970). *The United States and the Caribbean*. 212.

Tabassum, N., & Singh, S. (2020). Corporate governance and organisational performance: The impact of board structure. En *Corporate Governance and Organisational Performance: The Impact of Board Structure*. https://doi.org/10.1007/978-3-030-48527-6

Taiwo, O. J., Owowlabi, B. A., Adedokun, Y., & Ogundajo, G. (2021). Sustainability reporting and market value growth of quoted companies in Nigeria. *Journal of Financial Reporting and Accounting*, *20*(3/4), 542–557. https://doi.org/10.1108/JFRA-05-2020-0143/FULL/PDF

Taylor, G., Tower, G., & Neilson, J. (2010). Corporate communication of financial risk. *Accounting & Finance*, *50*(2), 417–446. https://doi.org/10.1111/j.1467-629X.2009.00326.x

TCFD. (2021). *TCFD Status Report*. *October*.

Terjesen, S., Sealy, R., & Singh, V. (2009). Women directors on corporate boards: A review and research agenda. *Corporate Governance: An International Review*, *17*(3), 320–337. https://doi.org/10.1111/j.1467-8683.2009.00742.x

Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments 2020 7:2*, *7*(2), 69–84. https://doi.org/10.1007/S40860-020-00115-0

Toronto Stock Exchange. (2014). Corporate Governance in Canada. *The International Corporate Governance System*, *December*, 90–100. https://doi.org/10.1057/9781137360014_7

Trend Micro; OEA. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. 60. https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend Micro Reporte Seguridad Cibernetica y Porteccion de la Inf Critica.pdf

Tricker, R. (1978). *The independent director : a study of the non-executive director and of the audit committee*. 104. https://books.google.com/books/about/The_Independent_Director.html?hl=es&id=8aAjAQAAMAAJ

Tricker, R. (2020). The evolution of corporate governance. En *The SAGE Handbook of Corporate Governance* (Vol. 7175). https://doi.org/10.4135/9781446200995.n1

UIT. (2012). *UIT-IMPACT organizan un cibersimulacro transfronterizo para la región de los Estados Árabes*.

Unión Europea. (2016a). *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo*. Unión Europea.

Unión Europea. (2016b). Reglamento (UE) 2016/ 679. *Diario Oficial de la Unión Europea*.

Unión Europea. (2019). *REGLAMENTO (UE) 2019/881*. Diario Oficial de la Unión Europea.

Unión Internacional de Telecomunicaciones. (s. f.). L*a agenda sobre ciberseguridad global – actualizacion*.

Unión Internacional de Telecomunicaciones. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. *Unión Internacional de Telecomunicaciones*, *1205*, 66.

United Nations General Assembly. (2009). *Resolución 64/25*.

United States Department of Justice. (2001). The USA PATRIOT Act : Preserving Life and Liberty. *USA Department of Justice*. http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

Urrutia, F. D. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Van der Walt, N., & Ingley, C. (2003). Board Dynamics and the Influence of Professional Background, Gender and Ethnic Diversity of Directors. *Corporate Governance: An International Review*, *11*(3), 218–234. https://doi.org/10.1111/1467-8683.00320

Vaughan, E. (1997). *Risk Management*. Wileyl.

Veblen, T. (1904). *The Theory of Business Enterprise*.

Velte, P., & Stawinoga, M. (2016). Integrated reporting: The current state of empirical research, limitations and future research implications. *Journal of Management Control 2016 28:3*, *28*(3), 275–320. https://doi.org/10.1007/S00187-016-0235-4

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*(C), 179–194. https://doi.org/10.1016/0165-4101(83)90011-3

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, L., & Tuttle, B. (2014). Using corporate social responsibility performance to evaluate financial disclosure credibility. *https://doi.org/10.1080/00014788.2014.922408*, *44*(5), 523–544. https://doi.org/10.1080/00014788.2014.922408

Wang, M. C. (2017). The relationship between firm characteristics and the disclosure of sustainability reporting. *Sustainability (Switzerland)*, *9*(4). https://doi.org/10.3390/SU9040624

Wang, T., & Hsu, C. (2013). Board composition and operational risk events of financial institutions. *Journal of Banking and Finance*, *37*(6), 2042–2051. https://doi.org/10.1016/j.jbankfin.2013.01.027

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Wang, T., Ulmer, J. R., & Kannan, K. (2013). The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities. *Journal of Organizational Computing and Electronic Commerce*, *23*(3), 200–223. https://doi.org/10.1080/10919392.2013.807712

WEF. (2017). Advancing Cyber Resilience - Principles and Tools for Boards. *World Economic Forum*, *January*, 40.

WEF. (2020a). A New Paradigm for Business of Data: Briefing paper. *World Economic Forum*, 15. http://www3.weforum.org/docs/WEF_New_Paradigm_for_Business_of_Data_Report_2020.pdf

WEF. (2021a). *Centre for Cybersecurity > Platforms | World Economic Forum*. https://www.weforum.org/platforms/the-centre-for-cybersecurity

WEF. (2021b). *Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico | foro Economico Mundial*. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

WEF. (2021c). *The Global Risks Report 2021: 16th Edition*.

WEF. (2022). *The Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022

WEF. (2023). *The Global Risks Report 2023 18th Edition*.

WEF, W. E. F. (2020b). *The Global Risks Report 2020*. https://es.weforum.org/reports/the-global-risks-report-2020

Wells, H. (2010). The Birth of Corporate Governance The traditional view dates them to 1932 with the publication of Adolf A . *Seattle University Law Review*, *33*(4), 1247–1292.

Werder, Axel ; Talaulicar, T. (2006). Corporate governance developments in Germany. En *Handbook on International Corporate Governance*.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. En *Cengage Learning*.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt. *USENIX Security Symposium*, 679–702. http://www.doug-tygar.com/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf

Williams, T. D. (2020). Epistemological Questions for Cybersecurity. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*, 1–4. https://doi.org/10.1109/CyberSecurity49315.2020.9138884

Woollacott, P. (2007). Cybercrime comes of age. *ITNOW*, *49*(2), 6–7. https://doi.org/10.1093/COMBUL/BWL110

Wuerges, A. F. E., & Borba, J. A. (2014). Fraudes contábeis: Uma estimativa da

probabilidade de detecção. *Revista Brasileira de Gestao de Negocios*, *16*(52), 466–483. https://doi.org/10.7819/rbgn.v16i52.1555

Yang, A., Kwon, Y. J., & Lee, S. Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, *120*(9), 1777–1794. https://doi.org/10.1108/IMDS-10-2019-0536

Yermack, D. (1996). Higher market valuation of companies with a small board of directors. *Journal of Financial Economics*, *40*(2), 185–211. https://doi.org/10.1016/0304-405X(95)00844-5

Yeung, W. H., & Lento, C. (2018). Ownership structure, audit quality, board structure, and stock price crash risk: Evidence from China. *Global Finance Journal*, *37*, 1–24. https://doi.org/10.1016/J.GFJ.2018.04.002

Zeller, G., & Scherer, M. (2020). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*. https://doi.org/10.1007/s13385-021-00290-1

# CAPÍTULO 4. INCIDENCIA DEL GOBIERNO CORPORATIVO SOBRE LA DIVULGACIÓN DE INFORMACIÓN SOBRE RIESGOS DE CIBERSEGURIDAD EN AMÉRICA LATINA

La creciente dependencia de los sistemas digitales, intensificada por el COVID-19, ha afectado a la sociedad (WEF, 2021; 2022). Estos desarrollos han llevado a una transformación de la superficie de ciberataque y han agregado complejidad e interdependencia a lo largo de la cadena de suministro digital (Kiesow Cortez y Dekker, 2022). Según WEF (2022), las cifras de incidentes están creciendo (en 2020, los ataques de malware y ransomware aumentaron un 358% y un 435%, respectivamente) y están superando la capacidad de la sociedad para prevenirlos o responder a ellos de manera eficaz. Estos incidentes de riesgo cibernético perjudican a las empresas que se han visto comprometidas y provocan que incurran en costos de remediación, multas y pérdida de reputación (Gordon et al., 2015). Como señala WEF (2022), a medida que la sociedad continúa migrando al mundo digital, la amenaza del delito cibernético se cierne sobre las organizaciones y les cuesta decenas, incluso cientos, de millones de dólares.

América Latina, la región objeto de este estudio, tiene una de las poblaciones de Internet de más rápido crecimiento en el mundo, lo que también crea una serie de importantes desafíos de Ciberseguridad, tanto ahora como en el futuro (Trend Micro; OEA, 2015). Algunos informes han demostrado que la revolución digital está emergiendo en América Latina más que quizás en cualquier región del mundo (OEA; ISA, 2020). La ONU (2011) afirma que los países en desarrollo, con una capacidad de vigilancia relativamente débil, son los más vulnerables a este tipo de ciberataques. Según Fortinet (2022), América Latina sufrió 137 mil millones de intentos de ciberataques desde enero de 2022 hasta junio de 2022, un aumento del 50% en comparación con el mismo período del año pasado. Durante los primeros seis meses de 2022, se detectaron aproximadamente 384.000 intentos de distribución de ransomware en todo el mundo. De estos, 52.000 tenían como destino América Latina.

En el ámbito corporativo internacional, PWC (2018) corrobora las formas en que los directores e inversores se preocupan por las ciberamenazas. En este sentido, el Gobierno Corporativo enfatiza los principios de transparencia, rendición de cuentas, independencia y equidad (Fakhfakh & Jarboui, 2022). En este contexto, las partes interesadas quieren comprender mejor cómo las empresas se preparan y responden a los incidentes de

Ciberseguridad, así como también cómo las juntas directivas supervisan estos esfuerzos críticos de gestión de riesgos (EY, 2018).

Según Li et al. (2018), la divulgación de información sobre el riesgo cibernético puede ser vista como una decisión ética por parte de las organizaciones porque esta divulgación es útil para las partes interesadas al evaluar la probabilidad de futuros incidentes. Un régimen de divulgación exigente que promueva la transparencia real es una característica crucial de la vigilancia del mercado empresarial y es esencial para que los accionistas puedan ejercer sus derechos de manera informada (G20/OCDE, 2016). Una Junta Directiva vigilante debe considerar los beneficios y las desventajas de la divulgación de Ciberseguridad, y considerar un equilibrio entre la divulgación de información relevante de Ciberseguridad y el mantenimiento de la seguridad de los sistemas de la empresa (Radu & Smaili, 2021). Las empresas que divulgan voluntariamente información relacionada con valores tienen valoraciones de mercado más altas por parte de los inversores (Berkman et al., 2018).

Según Eijkelenboom & Nieuwesteeg (2021) y Radu & Smaili (2021), la divulgación de los riesgos de Ciberseguridad que enfrentan las empresas y las formas en que se gestionan es cada vez más importante, lo que permite a los inversores, gobiernos, consumidores, proveedores y otras partes interesadas hacer juicios informados sobre las implicaciones financieras y reputacionales de los ataques cibernéticos de alto perfil. La divulgación de Ciberseguridad brinda a los usuarios información valiosa y conocimientos significativos sobre la susceptibilidad de una empresa al riesgo cibernético y su gestión (Masud & Hossain, 2022).

La composición de la Junta suele ser un factor determinante en la divulgación de información relacionada con los riesgos de Ciberseguridad. Si los inversores quieren aumentar la divulgación de información de Ciberseguridad, deben solicitar directorios más diversificados (Radu & Smaili, 2021). De acuerdo con EY (2018), también es de interés para los inversionistas saber si el directorio completo se encarga de la supervisión,

comparte la responsabilidad con los diferentes comités de auditoría, riesgos y tecnología, o crea un comité dedicado exclusivamente a la Ciberseguridad.

En el panorama internacional, el aumento de las revelaciones de Ciberseguridad en el mercado de capitales ha sido motivado por diferentes eventos. Cabe señalar que en 2011, la Guía de la SEC de la Comisión de Bolsa y Valores (Division of Corporation Finance & SEC, 2011) proporcionó pautas para la divulgación de temas relacionados con la cibernética en las presentaciones 10-K (Berkman et al., 2018 ; Ettredge et al., 2018); en 2018, la SEC emitió la segunda guía sobre divulgación de riesgos de Ciberseguridad; en 2021 aplicó las primeras sanciones por controles y procedimientos de divulgación deficientes relacionados con riesgos de Ciberseguridad por parte de las empresas emisoras (SEC, 2021b ; SEC, 2021a); y, en 2022, la SEC propone reglas para la divulgación sobre la gestión de riesgos de Ciberseguridad en las dimensiones de estrategia, gobernanza y divulgación de incidentes por parte de las empresas públicas (SEC, 2022). En el mercado de capitales europeo, según Eijkelenboom & Nieuwesteeg (2021), la obligación de revelar incidentes de datos desde la perspectiva de la ley de Ciberseguridad podría motivar la publicación de información sobre este tema en el informe anual a nivel corporativo. En cuanto a la divulgación de Ciberseguridad en América Latina, la normativa no especifica la divulgación de información en el informe anual. Sin embargo, diferentes normativas nacionales exigen el reporte de incidentes de Ciberseguridad a las autoridades establecidas y algunas normas sobre Gobierno Corporativo y gestión de riesgos emitidas por los diferentes entes de vigilancia y control promueven la divulgación de Ciberseguridad.

En este contexto, la literatura previa sobre divulgación de información de Ciberseguridad presenta los siguientes estudios (Amir et al., 2018; Barry et al., 2021; Berkman et al., 2018; Calderon & Gao, 2021; Ettredge et al., 2018; Eijkelenboom & Nieuwesteeg, 2021 Gao et al., 2020; Gordon et al., 2010; Héroux & Fortin, 2020; Hilary et al., 2016; Radu y Smaili, 2021; Wang & Hsu, 2013). Una reducida literatura previa ha relacionado la divulgación de riesgos con la composición de la Junta (Allini et al., 2016; Elzahar & Hussainey, 2012; Elshandidy & Neri, 2015; Mokhtar & Mellett, 2013; Ntim et al., 2013;

Oliveira et al., 2011; Taylor et al., 2010). Según nuestra búsqueda, solo dos estudios han vinculado la divulgación de información sobre riesgos de Ciberseguridad y la composición de la Junta (Masud & Hossain, 2022; Radu & Smaili, 2021).

Por lo tanto, para contribuir a la investigación en este campo, y dada la falta de estudios previos sobre el tema en América Latina, basados en la teoría de la agencia y la teoría de las partes interesadas y a partir de la aplicación del Índice de Divulgación sobre Ciberseguridad propuesto en el capítulo anterior, se evalúa el alcance de la información de Ciberseguridad divulgada en los informes anuales y se evalúan los factores de riesgo relacionados con el riesgo cibernético del informe 20F SEC (2018) de las empresas con mayores cotizaciones bursátiles de Argentina, Brasil, Chile, Colombia, México y Perú durante el período 2016-2020. Para lograr este objetivo, la primera sección de este capítulo presenta las características del Gobierno Corporativo desde un punto de vista histórico, se delinea la evolución de su concepto, se describen las principales teorías que enmarcan su estudio y los mecanismos que se proponen para su implementación en el ámbito corporativo. Seguidamente, se describe el contexto propio de América Latina, a partir de su marco normativo y las prácticas de Gobierno Corporativo que se desarrollan en la región. Posteriormente, desde las teorías de la agencia y de las partes interesadas, y tomando como referencia la literatura previa sobre el Gobierno Corporativo como factor de divulgación de riesgo, se analiza la incidencia del Gobierno Corporativo sobre la divulgación de información sobre riesgos de Ciberseguridad en las empresas cotizadas de América Latina. Para ello, se formulan las hipótesis del estudio, se relaciona la metodología, la población y la muestra, se presenta el modelo empírico y se analizan y discuten los resultados obtenidos. Finalmente, se exponen las principales conclusiones del estudio.

## 4.1. El Gobierno Corporativo

### 4.1.1. Evolución Histórica del Concepto de Gobierno Corporativo

De acuerdo con Cheffins (2012), no existe un marco histórico definitivo del Gobierno Corporativo y puede que nunca haya uno, dada la amplitud del tema. El Gobierno Corporativo nos acompaña desde que el uso de la forma corporativa creó la posibilidad de conflicto entre los inversores (Wells, 2010). La historia del Gobierno Corporativo se remonta al año 1600 con la conformación de la Compañía de las Indias Orientales como sociedad anónima, monopolio de todo el comercio entre Inglaterra y Asia, en virtud de una carta real otorgada por la reina Isabel I. La compañía contó con más de 1000 accionistas y una Junta Directiva de veinticuatro directores por año (Tricker, 2020). La estructura jurídica de dicha tipología societaria guarda similitud con la estructura actual (CEUPE, 2019). En el siglo XVII, otras grandes compañías fueron autorizadas bajo la carta de un monarca o del estado, por citar algunas: las Indias Orientales Holandesas (carta otorgada por la República de los Países Bajos en 1602), la Compañía Holandesa de las Indias Occidentales (1621), la Bahía de Hudson Company (recibe carta en 1670), la *South Sea Company* (incorporada bajo la autorización de la Cámara británica de los Lores en 1711). Pese a que en 1720 las acciones de esta última compañía se revalorizaron por una burbuja económica creada, su desplome arruinó a miles de inversores, los miembros de la aristocracia británica perdieron sus fortunas, los bancos quebraron, mientras que los directores de las compañías fueron encarcelados y sus riquezas confiscadas, se descubrió que el Ministerio de Hacienda había aceptado sobornos para promover la empresa. Desde este incidente, la evolución del Gobierno Corporativo se ha visto afectada por dudosos modelos de negocio y la asunción de riesgos poco realistas (Tricker, 2020).

Adam Smith (1776), refiriendose a los directores corporativos, escribió que, “siendo los gerentes del dinero de otros en lugar del suyo propio", nunca velaran por este dinero con la “misma vigilancia ansiosa con que los socios en una copartícipe privada con frecuencia vela por los suyos”. Por lo tanto, argumentó Smith, “negligencia y profusión. . . siempre prevalecerá. . . en la administración de la compañía”. En este sentido, de una forma u otra,

el Gobierno Corporativo siempre ha estado presente, al menos mientras la forma corporativa ha permitido conflictos entre inversores y gestores (Wells, 2010).

La propuesta de Berle & Means (1932), en *The Modern Corporation and Private Property,* posterior a la Gran Depresión de 1929, se considera la predecesora más significativa en los debates sobre el Gobierno Corporativo (Bratton, 2007). Estos autores llegaron a sugerir que este problema convertía a la corporación en una forma de organización insostenible (Denis, 2001). El impacto de Berle y Means en la erudición jurídica es catalogado "como un paradigma que dominó el campo" y su libro, como "un evento singular en el último siglo de la historia académica de derecho societario" (Bratton, 1989). Las raíces intelectuales de estas ideas se remontan al menos a la década de 1890, y autores como Louis Brandeis (1914), Walter Lippmann (1914) y Thorsten Veblen (1904) lucharon con este mismo paradigma antes de la Primera Guerra Mundial (Wells, 2010).

Otro referente previo, fue el trabajo del economista de Harvard William Z. Ripley, con la publicación de algunos artículos en el *Atlantic Monthly* y su libro *Main Street and Wall Street* (1927), famoso por sus críticas a la economía ferroviaria y las prácticas comerciales estadounidenses en los años 1920 y 1930. El trabajo de Ripley no solo influyó esta decada, sino que es el más recordado de una serie de estudios de reformas en la ley y el Gobierno Corporativo destinados a proporcionar nuevas protecciones para los accionistas (Wells, 2010). Posteriormente, Coase (1937) se refiere al problema entre inversores y gestores definiendo la firma como un conjunto de contratos. Hasta este momento el término Gobierno Corporativo no estaba en uso y solo hasta los años setenta vuelve a tener revelancia con el crecimiento económico mundial, el cual aumenta el problema corporativo de la separación entre la propiedad y el control.

### Década 1970: Primeros Conceptos de Gobierno Corporativo.

El hallazgo a mediados de la década de 1970 de pagos ilícitos generalizados por parte de las corporaciones estadounidenses para los funcionarios extranjeros llevó a la SEC más allá del ámbito del Gobierno Corporativo (Cheffins, 2012). Es así como, el término

Gobierno Corporativo surge en la década de 1970 como marco para explicar los escándalos corporativos contemporáneos (Ocasio & Joseph, 2005): “la Asamblea Estadounidense teorizó una versión de Gobierno Corporativo que era particularmente accesible, señalándolo como ‘... un término elegante para las diversas influencias que determinan lo que una corporación hace y no hace o debe y no debe hacer... encuentra reconocimiento y entendimiento en prácticamente todas las oficinas ejecutivas y salas de juntas de la nación’ (Szulc & American Assembly., 1970). Así, colectivamente, la Asamblea instó a las corporaciones a recuperar el control sobre los ejecutivos por parte de la Junta Directiva.

En este contexto, el primer uso de las palabras "gobierno" y "corporativo" en forma simultánea se presenta en diciembre de 1972, el término compuesto apareció en New York Times, por un aparente aumento en las demandas de los accionistas que enfatizan las responsabilidades legales de los directores. El enfoque del artículo fue la necesidad de mejorar el "gobierno y la disciplina corporativos" a través de comités de auditoría integrados por directores externos encargados de monitorear los sistemas de control interno de la empresa (Ocasio & Joseph, 2005). Estos comités de auditoría debían proporcionar un puente entre el auditor externo y la Junta principal, asegurando que los directores estuvieran al tanto de cualquier problema que hubiera surgido entre el auditor y el departamento financiero de la empresa (Tricker, 2020).

Por su parte, la Comunidad Económica Europea (CEE), tratando de armonizar la ley de sociedades en todos los estados miembros, emitió una serie de proyectos de directivas. El borrador de la quinta directiva de la CEE (1972) propuso que las juntas unitarias, con directores externos tanto ejecutivos como no ejecutivos, utilizadas en el Reino Unido y en otros lugares de la CEE, fueran reemplazadas por juntas de dos niveles, como se aplicaba en Alemania y Holanda (Tricker, 2020). No obstante, esta propuesta no se materializó por lo que “en la actualidad dentro de Europa existe tanto el sistema de Junta unitaria de gobierno como el sistema de Junta dual” (Mallin, 2006).

En 1971 Ralph Nader, un defensor de los derechos del consumidor en EE. UU, propuso un modelo de gobernabilidad desde una perspectiva de los stakeholders. Nader, promovió la ampliación de la base democrática de las juntas directivas de las grandes corporaciones, haciendo un llamado a elecciones de "directores públicos" (Mintzberg, 1984). En el libro *The Taming of the Giant Corporation,* Nader et al. (1976) conceptualizan el dominio del Gobierno Corporativo sobre la irresponsabilidad gubernamental y empresarial argumentando la necesidad de repensar y rediseñar el derecho corporativo. Solo hasta 1976, aparece por primera vez el término Gobierno Corporativo en el Registro Federal de EE.UU (Ocasio & Joseph, 2005), momento en el cual, la SEC comienza a tratar cuestiones de responsabilidad gerencial como parte de sus regulaciones e instar a la Bolsa de Valores de Nueva York cambios en la composición de las juntas de las compañías cotizadas, con el fin de incluir un Comité de Auditoría compuesto por directores independientes (Cheffins, 2012).

Al respecto, Nader et al. (1976) sustentan que la gobernanza de la empresa debe reformarse mediante la promulgación de leyes federales que devuelvan a la Junta su rol histórico como auditor interno de la corporación responsable de constreñir la administración de violaciones de la ley y los abusos de confianza. Su propuesta de cambio acorde con Eisenberg (1976), abogó sin invocar específicamente la causa de Gobierno Corporativo reemplazando el modelo legal recibido de la Junta por un modelo de "supervisión" en el que la mayoría de los directores serían independientes de la administración y la tarea principal de las juntas sería fomentar la responsabilidad gerencial. En esta línea, Jensen & Meckling (1976) hacen un aporte al Gobierno Corporativo con su escrito sobre "Theory of the firm: mangerial behavior , agency costs and ownership structure" en el que abordan el problema de la agencia y su relación con la separación de la propiedad y el control de las empresas modernas.

Otros aportes de la época al concepto de Gobierno Corporativo, lo constituyen: Fama et al. (1969), con la propuesta de una nueva medida de eficiencia de los mercados; Akerlof (1970), demostrando que el fenómeno de selección adversa es debido al problema de información asimétrica entre los administradores de las firmas y los accionistas,

acreedores, inversores, clientes y proveedores; Friedman (1970), al afirmar que la responsabilidad social de las empresas es incrementar sus utilidades, respaldando la teoría de la agencia; Spence (1973), proponiendo la señalización como mecanismo para contratar a los mejores trabajadores; y (Ross, 1977), desarrollando un modelo de señalización a través de la emisión de deuda y acciones de monitoreo o detección.

En 1978, Business Roundtable, un grupo establecido en 1974, emitió un comunicado sobre "The Role and Compositión of the Directors of the Large Public Limited Company" que discutió el lugar de la Junta en "la tríada de Gobierno Corporativo de accionistas, directores, administración operativa" y reconoció que, las juntas de las empresas deben estar compuestas por una mayoría de directores no administrativos y debe establecer comités de auditoría, compensación y nominación fuera de los directores dominados (Roundtable, 1978). Otro concepto importante de la época fue el expuesto por Robert Tricker (1978) en el libro "*The Independence of the director*" quien considera el Gobierno Corporativo como el interés por la forma en que las empresas son gobernadas, a diferencia de la forma en que estos negocios son administrados.

En general, los primeros conceptos de Gobierno Corporativo en esta época fueron propuestos por Nader et al. (1976), por los participantes en la Asamblea Americana SEC (1978) y la Business Roundtable. Las organizaciones públicas y privadas prominentes como Business Roundtable y la Securities and Exchange Commission establecieron teorizaciones oficiales y semioficiales que dieron estabilidad y reproducibilidad a los significados y referentes de los vocabularios de Gobierno Corporativo (Ocasio & Joseph, 2005). Estas concepciones se centran en la separación de poderes en la alta dirección y abordan el Gobierno Corporativo en el contexto de las preocupaciones más amplias de política pública y con el papel de la corporación en la sociedad (Ocasio & Joseph, 2005) en el contexto estadounidense. De otro lado, desde el contexto inglés, Calder (2008) señala que el concepto de aparece en Reino Unido en 1979 en las publicaciones del Instituto de secretarios y administradores colegiados sobre las responsabilidades de la Junta Directiva.

**Década 1980: Participación de Inversionistas Institucionales.**

En los primeros años del siglo XX a medida que muchas empresas cotizadas se hicieron grandes y complejas, también lo era su base de accionistas, que ahora podría ser numerosa y estar geográficamente extendida. Los inversores privados estaban siendo eclipsados por los inversores institucionales: fondos de pensiones, instituciones financieras, fondos de cobertura y empresas de capital privado (Tricker, 2020). La propiedad institucional de acciones creció considerablemente en la década de 1980 y, como resultado, se volvió cada vez más activa como defensora de los derechos de los accionistas (Ocasio & Joseph , 2005). Los objetivos de estos inversores diferían tanto en sus horizontes temporales estratégicos como en sus expectativas sobre los dividendos y el crecimiento del capital. Los accionistas de las principales empresas se habían distanciado de las salas de juntas de las empresas de las que eran propietarios (Tricker, 2020).

Durante la década de 1980, las políticas de privatización y globalización, especialmente en Estados Unidos y Reino Unido, trajeron cambios importantes al Gobierno Corporativo. En todo el mundo económicamente desarrollado, los consejos de administración de las empresas públicas se enfrentaron a posibles ofertas hostiles por el control de sus empresas por parte de depredadores, a veces financiados por bonos "basura" de alto rendimiento y alto riesgo recientemente disponibles (Tricker, 2020). Es así como de la década de 1980 en adelante, hubo un aumento continuo en el número y tamaño de las sociedades anónimas que abrieron su patrimonio al público. Si hay que extraer un mensaje de la proliferación de literatura internacional sobre Gobierno Corporativo desde finales de la década de 1980 es que la forma en que se gobiernan las empresas tiene un profundo impacto en la competitividad internacional (Charkham, 1995; La Porta et al., 1998, 2000; Shleifer et al., 1997). Hasta ahora el análisis es necesariamente americano en la orientación, dado que el Gobierno Corporativo sólo adquirió una fuerte dimensión internacional en la década de 1990.

**Década 1990: Códigos de Buenas Prácticas.**

A comienzos de 1990, los avances en Gobierno Corporativo se centran en la definición de las buenas prácticas corporativas. De esta manera, se prepara el Informe Cadbury (1992) , Informe Dey de Canada (1993), King Report de Sudáfrica (1994), Informe Viénot de Francia (1995), Informe Peters de Holanda (1997). Estas iniciativas ilustran el interés por mejorar la gobernabilidad en diferentes países. Una definición de Gobierno Corporativo de amplia aceptación es la contemplada en el Informe Cadbury "el Gobierno Corporativo es el sistema por el cual las empresas son dirigidas y controladas" (Cadbury, 1992). El Reporte Cadbury, por ejemplo, fue pionero en la materia al recopilar recomendaciones, principalmente sobre (Deloitte, 2021b): i) la disposición de los Consejos de Administración y los sistemas de contabilidad para mitigar riesgos y fracasos; ii) la división de responsabilidades en el puesto de presidente del Consejo y el Director General de la empresa; iii) la independencia del consejo; iv) la composición del consejo por consejeros independientes; así como, v) el establecimiento de un Comité de Auditoría con al menos tres consejeros independientes. Ese mismo año se publicó el informe COSO dirigido a la implantación y gestión del sistema de control interno en los Estados Unidos (Deloitte, 2021b).

Se identificó un comité de nominaciones como una forma posible de garantizar un proceso de designación transparente. El Código de Cadbury (1992) establece que los directores no ejecutivos deben ejercer un juicio independiente sobre cuestiones de estrategia, desempeño, recursos, incluidos los nombramientos clave y estándares de conducta. Posteriormente, al Reporte Cadbury (1992) en Reino Unido se han elaborado informes complementarios Greenbury (1995), Hampel (1998), el Código combinado (1998) y Turnbull (1999).

Otro acontecimiento que marca esta década es la participación de los inversionistas institucionales quienes reflejan la creciente importancia de la propiedad institucional, particularmente en los Estados Unidos. En este país los inversionistas institucionales son tenedores de acciones que presentan declaraciones 13F SEC e incluyen fideicomisos

bancarios, compañías de seguros, compañías de inversión (fondos mutuos), asesores de inversiones (empresas de corretaje), fondos de pensiones, entre otros. Mientras que inicialmente los inversores institucionales poseían un modesto 3% de las acciones ordinarias de Estados Unidos, estos mismos propietarios en esta década poseen el 66% de las acciones de Estados Unidos (Bogle, 2005). Con estos avances se puede evidenciar la evolución del concepto de Gobierno Corporativo con el surgimiento de los inversores institucionales como actores políticos (Cheffins, 2012). En EE.UU. el Comité Blue Ribbon patrocinado por NYSE y NASDAQ en 1999 hizo recomendaciones sobre la independencia de los comités de auditoría. En respuesta, la NYSE comenzó a exigir que cada empresa tuviera un Comité de Auditoría compuesto únicamente por directores independientes (Agrawal & Chadha, 2005). Durante la década de 1990, el número de mujeres que formaban parte de los directorios corporativos también aumentó sustancialmente (Farrell & Hersch, 2005).

En el ámbito internacional en este período se aprueban los principios para el desarrollo de buenas prácticas de Gobierno Corporativo (OECD, 1999). En esta decada la crisis asiática también aporta nuevos enfoques e instrumentos al Gobierno Corporativo. En general en este período el estudio del problema de asimetría de información va más alla de las finanzas e incluye a toda la organización.

Es de resaltar el caso de Sudáfrica, por cuanto allí el Gobierno Corporativo ha sido un concepto razonablemente bien desarrollado desde el establecimiento del Comité King sobre Gobierno Corporativo en 1992, a instancias del Instituto de Directores de Sudáfrica y la publicación del primer Informe King en noviembre de 1994. Esta iniciativa no fue estimulada por ninguna crisis significativa en el sector empresarial en ese momento; más bien se refería a la competitividad del sector privado sudafricano luego de la readmisión del país a la economía global después de su transición a una democracia de pleno derecho luego del colapso del apartheid (Armstrong, et al., 2006).

Por otra parte en Italia la Ley Draghi de 1998, el Código de conducta de Preda y algunos de los desarrollos de la época relacionados con el Gobierno Corporativo se ven afectados

por el escándalo de Parmalat (Melis, 2006). La Ley Draghi (1998) regula los mercados financieros y el Gobierno Corporativo en las sociedades cotizadas, con el objetivo principal de fortalecer la protección de los inversores y accionistas minoritarios. Esta Ley no ha previsto ninguna regulación sobre el consejo de administración, pero ha modificado el papel y funcionamiento del consejo de auditoría. El Código Preda (1999, 2002) recomienda que el consejo de administración esté compuesto por directores ejecutivos y no ejecutivos. Este Código representa uno de los primeros ejemplos de autorregulación en el sistema empresarial italiano (Melis, 2006). Al igual que el Informe Cadbury, el principio rector en la aplicación del Código Preda es "libertad con responsabilidad". Esto significa que una empresa cotizada es libre de elegir su propia estructura de gobierno dado que garantiza la transparencia de su elección, revelando en qué medida cumple con el código y dando las razones de cualquier área de incumplimiento (Melis, 2006).

### Primera Década 2000: Los Casos de Fraude Corporativo y la Crisis Financiera.

A finales del siglo XIX y principios del XX, el Imperio Británico difundió el concepto de sociedad de responsabilidad limitada en todo el mundo. Las leyes de sociedades de Australia, Canadá, algunas islas del Caribe, Hong Kong, India, Malaya (ahora Malasia), Nueva Zelanda, Singapur, Sudáfrica y algunos otros países africanos aún reflejan esos orígenes; aunque posteriormente su ley de sociedades evolucionó para adaptarse a las circunstancias locales (Tricker, 2020). Los casos de fraude corporativo de comienzos de la década del 2000 de América del Norte y Europa Occidental trajeron consigo la emisión por parte de los reguladores financieros de una serie de medidas tendientes a mejorar el Gobierno Corporativo y controlar el riesgo organizacional (Mallin, 2006). Como resultado, el Gobierno Corporativo recibe gran atención en los medios de comunicación y en el ámbito público en general, especialmente en mercados de capitales desarrollados. Bajo este panorama se inicia un programa de difusión del concepto de Gobierno Corporativo en el mundo liderado por la OCDE, el Banco Mundial a través de la Corporación Financiera Internacional junto con el Foro Global de Gobierno Corporativo. La Organización para la Cooperación y el Desarrollo Económicos (OCDE)

emitió sus principios de Gobierno Corporativo revisados en 2004, y la Red Internacional de Gobierno Corporativo pronunció su Declaración revisada sobre Principios de Gobierno Corporativo Global en julio de 2005.

También como parte de la respuesta a estos eventos, los países de todo el mundo han introducido códigos de Gobierno Corporativo o han fortalecido sus códigos y directrices existentes (Mallin, 2006). Se incorporaron documentos de políticas, voluntarios u obligatorios, tanto a nivel nacional como internacional (Stapledon, 2006). Por citar algunos ejemplos, en Estados Unidos se promulga la Ley Sarbanes Oxley, en Reino Unido se emiten: el Informe Higgs (2003), Smith (2003), el Código Combinado revisado (2003) y la Guía Turnbull revisada (2005). En el caso de Sudáfrica también inicia la aplicación del Informe King II. En Australia se emiten los Principios y recomendaciones de ASX Corporate Governance Council (2003). A la par en Europa, la Directiva 1/2004 establece la obligación de las empresas cotizadas de declarar el cumplimiento de las recomendaciones de los dos códigos de buenas prácticas, Informes Olivencia y Aldama, siguiendo la regla anglosajona del "cumplir o explicar" (Tricker, 2020). Por ejemplo, España siguiendo las conclusiones y recomendaciones del Informe Aldama, reformó la ley de sociedades y estableció la obligación de publicar un Reglamento del Consejo de Administración y un Reglamento de las Juntas Generales, y registrar dichas normas en la Agencia Española de Supervisión. La Ley de Transparencia también estableció la necesidad de publicar, a partir de 2004, un Informe Anual de Gobierno Corporativo de carácter obligatorio y de divulgar la información sobre Gobierno Corporativo en la página web de las sociedades. En Italia se promulga la versión de 2002 del Código Preda. En Estados Unidos, la Bolsa de Valores de Nueva York (NYSE) y NASDAQ en 2003 adoptaron un conjunto adicional de reglas de Gobierno Corporativo que se aplican a la mayoría de las empresas con acciones que cotizan en estos mercados. La Bolsa de Valores de Estados Unidos (AMEX) se unió con reglas similares este mismo año (Agrawal & Chadha, 2005). Debido a que las juntas en ese momento han sido criticadas por ser demasiado amistosas con los gerentes en: los Estados Unidos, Reino Unido y otros lugares, la independencia de los auditores se convirtió en el foco de gran atención después de los grandes colapsos y escándalos corporativos de 2001 (Stapledon, 2006).

A raíz de la crisis financiera mundial de 2008-2009, la confianza de las partes interesadas en la eficacia de la Junta disminuyó (Terjesen et al., 2009). Varios países reconocieron la necesidad de legislación para cambiar la composición de la junta. Con este fin, muchas naciones han implementado una cuota de mujeres en los directorios corporativos. Noruega lideró esta iniciativa al exigir una representación mínima del 40% de cada género en los directorios de sus empresas (Rose, 2007). Le siguieron Bélgica, Dinamarca, Francia, Alemania, Islandia, Italia, Malasia, los Países Bajos y España, cuyas cuotas obligatorias oscilan entre el 30 % y el 40 %, mientras que Finlandia, India, Israel y los Emiratos Árabes Unidos han exigido la presencia de al menos una mujer en las juntas (Baker et al., 2020). El Informe Higgs, encargado por el Departamento Británico de Comercio e Industria, sugiere que la diversidad demográfica aumenta la eficacia de los directorios y recomienda que se incluyan más mujeres en los directorios (R. B. Adams & Ferreira, 2009).

También la crisis financiera de 2008 revive el debate sobre la necesidad de un Gobierno Corporativo efectivo a través de prácticas sólidas de gestión de riesgos, transparencia y rendición de cuentas corporativa" (Ntim et al., 2013). Ahora solo los directores independientes podían formar parte de los comités de auditoría y remuneración, los accionistas tenían que aprobar planes para las opciones sobre acciones de los directores y se prohibieron los préstamos subsidiados a los directores (Tricker, 2020). En este momento el término "Gobierno Corporativo" es ampliamente utilizado para referirse al equilibrio de poder entre funcionarios, directores y accionistas (Salet, 2004). Esta crisis también plantea algunos problemas fundamentales de Gobierno Corporativo, incluida la exposición al riesgo (Tricker, 2020). En 2009 se presenta una nueva versión del Código King de Principios de Gobierno Corporativo conocida como King III este código presenta un capítulo sobre la Gobernanza de las TI.

**Segunda Década 2000 - Actual: Responsabilidad Social Corporativa, Sostenibilidad.**

Según King (2016), en esta década nuevas realidades globales están poniendo a prueba el liderazgo de las organizaciones en temas tan diversos como la desigualdad, el comercio globalizado, las tensiones sociales, el cambio climático, el crecimiento demográfico, el exceso ecológico, las tensiones geopolíticas, la transparencia radical y el rápido avance tecnológico y científico. En 2010, el Reino Unido establece un objetivo de 33 por ciento de mujeres en sus directorios para 2020. En 2014, se emite la Directiva 2014/95/UE del Parlamento Europeo y del Consejo por la que se modifica la Directiva 2013/34/UE en lo que respecta a la divulgación de información no financiera e información sobre diversidad por parte de determinadas grandes empresas y determinados grupos. En la actualidad corresponde al Gobierno Corporativo liderar y velar por la sostenibilidad de las organizaciones. Es así como, en el ámbito mundial se han generado medidas regulatorias y nuevas directrices de debida diligencia desde la responsabilidad social corporativa y el desarrollo sostenible como respuesta a una sociedad que interpela, cada vez con más fuerza el comportamiento organizacional en las dimensiones económicas, sociales y ambientales.

Según la Comisión Europea (2022): “el análisis de la evaluación de impacto abordó en sentido amplio el problema derivado de la necesidad de reforzar la sostenibilidad en los sistemas de gestión y gobernanza empresarial, con dos dimensiones: 1) los intereses de las partes interesadas y los riesgos (de sostenibilidad); 2) las empresas no mitigan suficientemente sus efectos adversos sobre los derechos humanos y el medio ambiente y no disponen de gobernanza, sistemas de gestión ni medidas adecuados para mitigar sus efectos nocivos”.

En 2015 la OCDE se une al grupo de naciones G20 para promover la revisión de los principios emitidos en su primera versión. En 2016, el Instituto de Directores de Sudáfrica publicó King Reporte de Gobierno Corporativo este informe enfatizó las responsabilidades éticas y sociales de órganos de gobierno, proponiendo un comité de

ética y social en el directorio. King reconoció que todas las entidades corporativas deben ser gobernadas, y su informe es aplicable a: sectores público y privado, organizaciones lucrativas y no lucrativas. El Código de Gobierno Corporativo del Reino Unido, se actualiza en 2018, este nuevo Código ha puesto un enfoque esencial en la red de la Junta Directiva, la diversidad de género, la independencia de los comités de supervisión y la compensación ejecutiva para lograr un gobierno efectivo y eficiente que pueda promover la salud corporativa (Elsayed et al., 2022).

En Estados Unidos las empresas han continuado adaptando y perfeccionando sus prácticas de gobierno en el marco de leyes y normas bursátiles. Durante este período se suscitan publicaciones importantes sobre Gobierno Corporativo: un esfuerzo liderado por inversionistas por parte de Investor Stewardship Group (2017) denominado "Principios de Gobierno Corporativo para empresas estadounidenses que cotizan en bolsa". Otros grupos tienen el Marco para la Administración y Gobernanza de Estados Unidos, un esfuerzo de Busines Roundtable (2018) llamado "Principios de Gobierno Corporativo", y una pieza del Consejo Empresarial Internacional del Foro Económico Mundial WEF (2020) presentan la publicación "El Nuevo Paradigma". Algunas de estas publicaciones pretenden incluir temas de actualidad como la sostenibilidad y ampliar sus objetivos corporativos con una visión enfocada en el largo plazo.

De este recuento de acontecimientos históricos que han delineado el concepto y la aplicación del Gobierno Corporativo podemos observar que, a pesar de que el Gobierno Corporativo se ha convertido en una palabra de moda, su definición precisa permanece borrosa (Gillan, 2006). Una revisión de la literatura reveló una ausencia de consenso en cuanto a lo que constituye Gobierno Corporativo (Solomon, 2010). El concepto de Gobierno Corporativo, y la comprensión de éste, varía de una empresa a otra, de un país a otro. Es así como desde el código de buen gobierno de cada país también se ha generado un concepto sobre Gobierno Corporativo. En especial, la falta de transparencia corporativa en determinados momentos de la historia ha conducido a la adopción de medidas tendientes a mejorar la práctica del Gobierno Corporativo, particularmente con la emisión de principios rectores de Gobierno Corporativo relacionados con los actores

corporativos, la composición y estructura de la Junta y sus comités, el funcionamiento del Directorio, la relación corporativa con los grupos de interés y en los últimos años la vinculación de Gobierno Corporativo con los temas relacionados con comunidades, medio ambiente y sostenibilidad. Aunque no existe una definición universal única de Gobierno Corporativo, los formuladores de políticas en diferentes países persiguen los mismos objetivos cuando buscan hacer crecer en el público la confianza de los inversores, y es claro que el buen Gobierno Corporativo se fundamenta en los principios de protección, rendición de cuentas, transparencia y divulgación.

Como se puede observar en los acontecimientos históricos que marcan el Gobierno Corporativo en el ámbito mundial, así como la participación de la Junta pueden estar sujetas a leyes, reglamentos y opiniones dependiendo del país que se trate. Algunos autores precisan que el Gobierno Corporativo se compone en el entorno empresarial de elementos internos y externos. Entre los componentes internos se encuentran la Junta Directiva. Los antecedentes históricos del Gobierno Corporativo denotan el rol de la Junta Directiva como el componente más importante del mecanismo interno de Gobierno Corporativo, ésta asume la responsabilidad de asesorar y dar seguimiento a la gerencia, la contratación y los equipos de la alta dirección (Jensen, 1993). Entre los componentes externos se enfatiza la división entre proveedores y accionistas en las empresas cotizadas, esta circunstancia amerita estructuras de Gobierno Corporativo idóneas para fomentar la transparencia, la redición de cuentas y la responsabilidad social corporativa. La Junta Directiva, en la cúspide de los sistemas de control interno, se encarga de asesorar y monitorear a la gerencia y tiene la responsabilidad de contratar, despedir y compensar al equipo de alta gerencia (Jensen, 1993). Así el término de Gobierno Corporativo se utiliza como representante de autoridad y control en el contexto de las organizaciones. Como se puede evidenciar en los avances cronológicos del concepto de Gobierno Corporativo, desde la década de 1970 se han realizado un sinnúmero de intentos de definir el término. La Tabla 20 presenta los conceptos de Gobierno Corporativo emitidos desde organismos internacionales, tomados en la actualidad, como referentes para inversores, políticos, organizaciones y otras partes interesadas.

**Tabla 20. Conceptos de Gobierno Corporativo de aceptación internacional**

| Autor | Definición |
|---|---|
| (Cadbury, 1992) | El sistema por el cual las empresas son dirigidas y controladas. |
| (Toronto Stock Exchange, 2014) | Proceso y estructura para gestionar las empresas con el objetivo de crear valor para el accionista, lo que incluye asegurar la viabilidad financiera de la empresa. |
| (OCDE, 2016) | El Gobierno Corporativo de una sociedad implica el establecimiento de un conjunto de relaciones entre la dirección de la empresa, su consejo de administración, sus accionistas y otros actores interesados. El Gobierno Corporativo proporciona también la estructura a través de la cual se fijan los objetivos de la sociedad y se determina la forma de alcanzarlos y supervisar su consecución. |
| (King, 2016) | Según King IV, el Gobierno Corporativo se define como el ejercicio de un liderazgo ético y eficaz por parte del órgano de gobierno hacia el logro de los siguientes resultados de gobierno: cultura ética, buen desempeño, control efectivo y legitimación. El uso de "corporativo" en el término "Gobierno Corporativo" se utiliza para diferenciarlo de otras formas de gobierno, por ejemplo, gobierno nacional o político. |
| (ISO 37000:2021) | Sistema basado en humanos por el cual una organización es dirigida, supervisada y responsable de lograr su propósito definido. El buen gobierno significa que la toma de decisiones dentro de la organización se basa en la ética, la cultura, las reglas, las prácticas, los comportamientos, las estructuras y los procesos organizacionales de la organización. Éste hace posible establecer y sostener una organización con un propósito claro que crea valor a largo plazo en consonancia con las expectativas de sus grupos de interés. La implementación del buen gobierno se basa en el liderazgo, los valores y un conjunto de arreglos, procesos y estructuras organizacionales que sean adecuadas al contexto interno y externo de la organización. |
| (CAF, 2013) | Define el Gobierno Corporativo como el conjunto de prácticas, formales e informales, que gobiernan las relaciones entre los administradores y todos aquellos que invierten recursos en la empresa, principalmente accionistas y acreedores. Es obvio que unas buenas prácticas garantizan un mejor uso de los recursos en las empresas, contribuyen a una mayor transparencia contable y mitigan los problemas de información asimétrica que caracterizan a los mercados financieros. En estas circunstancias, unas buenas prácticas son clave para el acceso de las empresas a los mercados de capital. |

| | |
|---|---|
| (German Government Commission, 2022) | El Gobierno Corporativo se entiende como el marco normativo de hecho y de derecho para la gestión y seguimiento de una empresa. |
| (Subcommittee of Capital Markets; Capital Markets Committee et al., 2022) | El Gobierno Corporativo es un sistema en el que los gerentes externos, como directores externos y auditores corporativos externos, supervisan la gestión para evitar malas conductas en toda la organización y mejorar el valor corporativo a largo plazo para maximizar los intereses de los accionistas y otras partes interesadas (partes interesadas) que son los propietarios de la corporación, directores y funcionarios ejecutivos separados. |

Se evidencia que algunos autores institucionales han definido el término en su sentido estricto, mientras que otros lo explican en relación con sus significados más amplios (Abdullah & Page, 2009). En la definición de Gobierno Corporativo, en sentido estricto, se encuentran las que tienen su origen en el sistema anglosajón (Cadbury, 1992; Toronto Stock Exchange, 2014). Éstas lo definen como un sistema de relaciones entre los actores internos de una empresa, a saber, su directorio, gerencia y accionistas. En este sentido, la definición sugiere que tanto los directores como la gerencia de la empresa sólo rinden cuentas a sus accionistas. La visión estrecha de Gobierno Corporativo tiene que ver con la protección de los intereses de aquellos que han aportado recursos financieros a la empresa (Cadbury, 1992; La Porta et al., 1999; Shleifer et al., 1997). Por otra parte los autores que explican Gobierno Corporativo con un significado más amplio (CAF, 2022; ISO 37000:2021; King, 2016; German Government Commission, 2022; OCDE, 2016; Subcommittee of Capital Markets; Capital Markets Committee et al., 2022) presentan una visión más vasta del Gobierno Corporativo y sugieren ir más allá de los intereses de los inversionistas y las responsabilidades internas de la empresa. En su sentido más amplio, el Gobierno Corporativo crea confianza general a nivel de la economía agregada. Sugiere que las empresas tienen un conjunto de responsabilidades económicas, ambientales y sociales, así como hacia otros grupos de interés de la empresa, incluyendo, por ejemplo, empleados, proveedores y la comunidad.

Es desde estas dos ópticas que se modela el Gobierno Corporativo organizacional, las funciones de la Junta y, por ende, la divulgación de información organizacional. El Gobierno Corporativo con una visión de mayor cobertura también ha sido definido como: “el sistema de frenos y contrapesos, tanto internos como externos a las empresas, que

asegura que estas cumplan con su obligación de rendir cuentas a todos sus grupos de interés y actuar de forma socialmente responsable en todos los ámbitos de su actividad de negocios" (Solomon, 2010). Se trata de un conjunto de reglas y relaciones entre las partes interesadas internas y externas de una empresa, con el objetivo de crear un entorno en el que la empresa puede alcanzar sus objetivos de negocio (Tabassum & Singh, 2020). Se reconoce que los inversores, tanto individuales como institucionales, son más propensos a arriesgar sus recursos financieros invirtiendo en empresas con un buen historial de logros de Gobierno Corporativo (Bushee et al., 2014), menos asimetría de información y explotación de los derechos de las minorías accionistas (Choe et al., 2005).

Las definiciones expuestas en la Tabla 20 también evidencian las diferencias del concepto de Gobierno Corporativo desde los diversos modelos. Así, el modelo angloamericano, como el modelo más antiguo de Gobierno Corporativo, está basado en una estructura de propiedad difusa en la que los inversores individuales e institucionales no están estrechamente relacionados con las empresas (Tabassum & Singh, 2020). Este modelo de gobernanza es apropiado para las economías de mercado, como: Estados Unidos, Reino Unido, Canadá y Australia. En el modelo angloamericano, la dirección de la empresa nombra a los miembros del Consejo de Directores. Estos directores luego son seleccionados por los accionistas de la compañía en su asamblea general anual. También conocido como el modelo de directorio de un solo nivel, se caracteriza por ejecutivos y no ejecutivos directores sirviendo juntos dentro de una sola capa organizacional (Tabassum & Singh, 2020). En este modelo la literatura proporciona evidencia de una confianza excesiva en el uso de la teoría de la agencia (Shleifer et al., 1997). Por lo que el supuesto subyacente del modelo de Gobierno Corporativo es una estructura de propietario débil/ gerente fuerte con un enfoque en mitigar el abuso gerencial en el contexto de propiedad ampliamente dispersa y protecciones legales elaboradas de intereses minoritarios (Mallin, 2006). No obstante, las empresas del Reino Unido se gestionan en un régimen de Gobierno Corporativo que tiene diferencias fundamentales con el que prevalece en los Estados Unidos (Elsayed et al., 2022). Éstas se gestionan bajo una aplicación de la ley menos severa en comparación con la aplicada a las empresas estadounidenses (Muñoz-Izquierdo et al., 2019).

Entretanto, el modelo alemán de Gobierno Corporativo hace hincapié en la cooperación, el consenso y el entendimiento entre las diversas partes interesadas de la empresa. La definición de Gobierno Corporativo es la propuesta por German Government Commission (2022). El modelo alemán se basa en una Junta Directiva de dos niveles: el consejo ejecutivo y el consejo de vigilancia. Éste es un modelo "privilegiado" de gobernanza, donde una gran proporción de los directores de la Junta son nominados y elegidos por los accionistas, los bancos y los empleados para monitorear la gestión de la empresa, quienes, a su vez, son responsables de administrar los asuntos cotidianos de la empresa (Tabassum & Singh, 2020). Los actores clave en el modelo de Gobierno Corporativo alemán son los bancos, los accionistas y los representantes de los sindicatos. El alcance del modelo alemán no es restringido a los principales accionistas. También defiende y protege los intereses de los empleados y otras partes interesadas de la empresa.

Por su parte, en el modelo japonés de Gobierno Corporativo las empresas públicas y privadas en Japón están conectadas a través de participaciones cruzadas, donde los directorios entrelazados son relativamente comunes. El sector empresarial japonés es caracterizado por un alto nivel de propiedad de acciones, en manos de bancos afiliados y empresas del grupo. Esto sirve para hacer que el modelo Gobierno Corporativo japonés sea más eficiente y eficaz. La definición de Gobierno Corporativo Subcommittee of Capital Markets; Capital Markets Committee et al. (2022) muestra la importancia de la supervisión y la cobertura a todas las partes interesadas. Las empresas miembros tienden a comercializar extensamente con unos y otros. Es bastante normal que las instituciones financieras formen parte de las redes entrelazadas—algo que refleja la cohesión social típica de la sociedad japonesa y que enfatiza la unidad en toda la red (Tricker, 2012). El modelo japonés de gobernanza es visto como una alternativa eficiente a los modelos angloamericano y occidental (Weinstein y Yafeh, 1998).

El problema de países de Europa continental, Japón y otras naciones "es diferente del conflicto de intereses inherente entre propietarios y gerentes, como se conceptualiza en el llamado "problema de agencia" de Estados Unidos, Reino Unido, Canadá y Australia. Las economías de la Europa continental y Japón operan de manera diferente a este

modelo (Aoki et al., 1995). Las empresas públicas del tipo de Berle y Means (1932) son una excepción. Especialmente en Alemania, el modelo se basa en una estructura de propietario fuerte/administrador débil donde la administración puede carecer de incentivos de desempeño, pero los bancos, como propietarios que controlan, brindan tanto el capital de inversión requerido como la capacidad de monitoreo necesaria (Bartha, Peter; Gillies, 2006). En general, Estados Unidos, Alemania, Japón y el Reino Unido tienen algunos de los mejores sistemas de Gobierno Corporativo del mundo, y las diferencias entre ellos probablemente sean pequeñas en relación con sus diferencias con otros países (Shleifer et al., 1997). En general, dentro de Europa existe tanto el sistema de Junta unitaria de gobierno como el sistema de Junta dual (Mallin, 2006). Respecto al caso particular de China, el sistema de Gobierno Corporativo desde principios de la década de 1990 es "dominado por el estado", el papel del Estado chino en el desarrollo y la reforma de su sistema de Gobierno Corporativo, en el que, irónicamente, una gran parte de los problemas han sido producidos por el propio Estado. En general son estas diferencias institucionales a nivel país las que impiden la creación de un único código internacional, capaz de contemplar recomendaciones lo bastante generales para englobar las distintas políticas de Gobierno Corporativo en las diferentes culturas.

### 4.1.2. Teorías de Gobierno Corporativo

El desarrollo de Gobierno Corporativo está estrechamente vinculado con el crecimiento económico y diversos mecanismos de gobernanza desarrollados para acomodar diferentes formas de estructuras corporativas diseñadas para lograr metas. Se han desarrollado varias estructuras teóricas únicas en un esfuerzo por explicar y comprender el Gobierno Corporativo, cada uno de los cuales considera Gobierno Corporativo desde diferentes ángulos. La literatura sobre el desarrollo de Gobierno Corporativo, basada en una serie de teorías, tiene sus raíces en diversas disciplinas, incluyendo contabilidad, finanzas, derecho, economía e internacional negocio (Solomon, 2010). Aunque el concepto de Gobierno Corporativo ha llegado recientemente a la prominencia, las teorías que sustentan su desarrollo datan de mucho antes (Mallin, 2006). Actualmente, los estudios existentes sobre Gobierno Corporativo han tendido a basarse en diferentes teorías

económicas (agencia, dependencia de los recursos y de la señalización) y sociopolíticas (institucionales, de legitimidad y de partes interesadas).

Por lo tanto, algunas teorías son reconocidas como más adecuadas, aplicables y relevantes para algunos países que para otros. En este aparte presentamos un resumen de teorías centrales relacionadas con el desarrollo de sistemas y prácticas de Gobierno Corporativo.

## Teorías Económicas

### Teoría de la Agencia

La teoría de la agencia está segura entre el panteón de fundamentos conceptuales/teóricos que informan la investigación en el Gobierno Corporativo (Dalton et al., 2007). Esta teoría involucra los conflictos de intereses resultantes de las diferencias entre los intereses de los accionistas y los de los administradores (Al-Sartawi et al., 2018) y considera a la corporación como un nexo de contratos entre agentes económicos que maximizan la utilidad que operan en mercados eficientes (Jensen & Meckling, 1976). Su objetivo es explicar la relación entre los principales (accionistas y reguladores) y los agentes (los gerentes de una empresa).

La literatura de Gobierno Corporativo, especialmente en economías desarrolladas y en desarrollo, se ha construido en torno al concepto de teoría de la agencia. Introducida por primera vez por Alchian & Demsetz (1972), la definición clásica propuesta por Jensen & Meckling (1976) hace referencia a "aquel contrato explícito o implícito que se establece entre dos partes, por el cual se comprometen a cooperar en la realización de una actividad". La teoría se basa en el concepto de una separación entre accionistas (principales) y dirección ejecutiva (agentes) debido a la estructura de propiedad difusa de las empresas públicas (Berle & Means, 1932; Jensen & Meckling, 1976). En consecuencia, el agente es responsable de cumplir con las tareas asignadas por el principal (Fama & Jensen, 1983) y, bajo este modelo de agente-principal, la separación de la

propiedad y el control entre los gerentes y propietarios de una empresa genera conflictos de interés.

La teoría se ocupa principalmente de dos problemas. El primero surge, cuando las partes en la relación tienen objetivos conflictivos, y es costoso y difícil para el principal monitorear y confirmar tanto las acciones reales del agente como si éste ha seguido correctamente el contrato de agencia. El segundo problema se relaciona a la gestión del riesgo cuando el principal y el agente tienen diferentes puntos de vista y actitudes hacia la gestión de riesgos.

La teoría de la agencia sostiene que el gobierno efectivo mejora la capacidad de la empresa para enfrentar los desafíos emergentes y reducir los conflictos de agencia (Haniffa & Cooke, 2002). De acuerdo con Dalton et al. (2007), estas dos nociones -teoría de la agencia y Gobierno Corporativo - son esencialmente equivalentes. En este sentido, el Gobierno Corporativo enfatiza los principios de transparencia, rendición de cuentas, independencia y equidad (Elgadi & Ghardallou, 2022). La teoría de la agencia propone, al respecto, que la Junta Directiva actúa como representante de los distintos grupos de accionistas para monitorear el desempeño y controlar las actividades de los gerentes (Albitar et al., 2020), y subraya la importancia de un buen Gobierno Corporativo para minimizar las brechas de información que se producen de todas las partes interesadas. Por lo tanto, para reducir esta brecha de información (asimetría) y los costos de agencia relacionados, las empresas deben divulgar información precisa, transparente y oportuna al público (Al-Sartawi et al., 2018).

La literatura previa ha documentado, de acuerdo con sus argumentos teóricos, una relación entre el Gobierno Corporativo y la divulgación de riesgos basada en el papel de ésta última como mecanismo de control de los problemas de agencia (Abraham & Cox, 2007; Allini et al., 2016; Barakat & Hussainey, 2013; Elshandidy & Neri, 2015; Lajili & Zéghal, 2005; Lim et al., 2007; Ntim et al., 2013). Diversas investigaciones precedentes (Campbell et al., 2014; Jorion, 2002; Kravet & Muslu, 2013; Rajgopal, 1999) han revelado que la información precisa sobre riesgos como mecanismo de control externo

reduce los costos de agencia, y es fundamental para accionistas, analistas e inversores, ya que les permite evaluar el perfil de riesgo de una empresa, estimar su valor de mercado y tomar decisiones de inversión acertadas. Los efectos del Gobierno Corporativo en la práctica de informes mitigan la asimetría de la información y mejoran la función de administración.

Respecto a la divulgación de riesgos de Ciberseguridad, las partes contratantes, tanto accionistas como administradores, están sujetas a las revelaciones reportadas por las compañías. Con base en la teoría de la agencia, la regulación débil sobre la divulgación de riesgos de Ciberseguridad brinda a los gerentes la oportunidad de manipular la información divulgada de acuerdo con sus propios intereses. En efecto, la teoría de la agencia establece que los gerentes tienen conocimientos y habilidades de gestión de los que carecen los accionistas, y emplean dichas habilidades para enmarcar la divulgación para su propio beneficio. Como sugiere la teoría de la agencia, una mayor proporción de directores independientes mitiga el conflicto entre los gerentes y los propietarios al aumentar la transparencia, así como la diversidad de ésta.

En esta línea, Masud & Hossain (2022), basándose en la teoría de la agencia, examinan la asociación entre la composición de la Junta y la divulgación de información de Ciberseguridad, argumentando que la Junta Directiva sirve como aparato de monitoreo para minimizar la asimetría de la información. Según Kies Cortez & Dekker (2022) los problemas de agencia pueden ser generalizados y aumentar el desafío de supervisar a los gerentes, especialmente en dominios complejos como la gestión de riesgos de seguridad cibernética. En general, esta teoría es más relevante para los modelos anglosajones de Gobierno Corporativo, ya que las condiciones específicas asumidas bajo estos modelos son la excepción, más bien que la norma, para una gran parte del mundo, incluidos los países de la región del sur de Asia, que tiende a presentar una alta concentración de propiedad en empresas cotizadas (La Porta et al., 1999).

### Teoría de la Dependencia de los Recursos

Esta teoría sugiere que las empresas en gran medida dependen de su entorno externo, en particular de otras organizaciones, para su éxito económico y, en algunos casos, para su supervivencia (Tabassum & Singh, 2020). La teoría proporciona una visión hipotética en la que la Junta Directiva es un recurso crítico para las empresas (Hillman et al., 2000)**.** El núcleo de la teoría sugiere que, en un entorno de negocio altamente competitivo, las empresas buscan controlar la incertidumbre de los factores externos asegurándose de que los recursos internos adecuados estén disponibles y puestos en marcha para hacer frente a la competencia (Barney, 2014).

Pfeffer & Salancik (1978) sugieren cuatro beneficios principales para los vínculos externos: (1) provisión de recursos tales como información y experiencia; (2) creación de canales de comunicación con componentes de importancia para la empresa; (3) provisión de compromisos de apoyo de organizaciones o grupos importantes en el entorno externo; y (4) creación de legitimidad para la empresa en el entorno externo. La extensión de la teoría de la dependencia de los recursos de Hillman et al. (2000) sugiere que diferentes tipos de directores proporcionarán diferentes recursos beneficiosos para la empresa. Como resultado, una Junta más diversa proporcionará recursos más valiosos, lo que debería producir un mejor desempeño de la empresa. Hillman et al. (2000) examinan el papel de dependencia de los recursos de los directores y postulan que las categorizaciones de interno/externo ampliamente utilizadas no capturan adecuadamente este papel de los directores. Se presenta una taxonomía de directores específicamente para estudiar el rol de dependencia de recursos.

Tomando una perspectiva de dependencia de los recursos en las organizaciones, analizan los componentes básicos del control, incluida la concentración y disponibilidad de recursos, el papel de los gerentes, la interdependencia entre organizaciones, el entorno y la estructura organizacional. En otras palabras, la teoría de la dependencia de los recursos adopta una visión estratégica de Gobierno Corporativo, considera que el órgano de gobierno es el eje entre empresa y los recursos que necesita. Los directores son el nodo de la red que conecta a la empresa con sus mundos (Tricker, 2020).

La teoría de la dependencia de los recursos sugiere que las empresas que se comprometen con altos niveles de transparencia en forma de mayor divulgación pueden disfrutar de ventajas competitivas únicas al obtener acceso a recursos críticos, como las finanzas (Branco & Rodrigues, 2008; Pfeffer, Jeffrey; Salancik, 1978). De hecho, dado que es costoso involucrarse en cuestiones de divulgación (en términos financieros, legales, de propiedad, competencia, regulación e impuestos) (Lajili & Zéghal, 2005), los beneficios pueden acumularse para la empresa en forma de mayor gestión de riesgos internos, experiencia en gestión, imagen y reputación corporativa (Branco & Rodrigues, 2008; Linsley & Shrives, 2006), así como un costo de capital más barato (Botosan, 1997). Sin embargo, la teoría de la dependencia de los recursos ha sido criticada por indicar que la divulgación debe llevarse a cabo principalmente por motivos estratégicos corporativos en lugar de exhibir responsabilidad y rendición de cuentas ante una gama más amplia de partes interesadas corporativas (Lopes & Rodrigues, 2007).

### Teoría de la Señalización

Como afirma Spence (2002), la Obra de Akerlof en 1970 "*The Market for Lemons*" expone un análisis claro y plausible de las características correspondientes al funcionamiento de un mercado que contaba con información incompleta y asimétrica. A partir de esta obra, Spence (1973) relaciona las consecuencias de la información incompleta en los mercados de trabajo, y desde el concepto de "señales", describe el proceso de contratación como una inversión y lo compara con jugar a la lotería y así como el número final se elige en una lotería, no sabe hasta que eso suceda si hizo la inversión correcta o no. Es a partir de estos antecedentes que la teoría de la señalización se incorpora en el pensamiento económico.

Ahora bien, respecto al tema de la divulgación de información podemos retomar autores como Connelly et al. (2011) y Lee et al., (2016) quienes afirman que la teoría de la señalización es útil para describir el comportamiento cuando dos partes (individuos u organizaciones) tienen acceso a información diferente. Por lo general, una parte, el remitente, debe elegir si desea comunicar (o señalar) esa información y cómo, y la otra

parte, el receptor, debe elegir cómo interpretar la señal. Es a partir de estos postulados que desde los informes anuales y demás comunicaciones empresariales las organizaciones pretenden enviar señales a sus partes interesadas a través de la divulgación de riesgos (Allini et al., 2014; Elzahar & Hussainey, 2012; Mokhtar & Mellett, 2013).

Respecto a la divulgación en Ciberseguridad se pueden citar las investigaciones de Gordon et al. (2010) y Radu & Smaili (2021). Sus hallazgos apoyan el argumento de la señalización, al establecer que los gerentes divulgan información para revisar creencias de los inversores de una manera coherente con el aumento de valor.

## Teorías Sociopolíticas

### Teoría Institucional

La teoría institucional involucra las diferentes dimensiones o factores que conducen las acciones de los diversos agentes que actúan en la sociedad, a partir del concepto de "institución" en su acepción más amplia. Esto significa que "las instituciones" se conciben como las normas y reglas restrictivas que rigen en la sociedad, condicionando y dirigiendo el marco de relaciones que se producen en ella. El desarrollo de la teoría económica institucional ofrece un acercamiento para entender y tratar las diferentes formas de interacción humana, ya sean formales o informales, en el marco general de unas "reglas de juego" establecidas (North, 1993). Bajo la premisa de la teoría institucional, las organizaciones responden a presiones externas y adoptan estructuras y prácticas que son consideradas legítimas y socialmente aceptables por otras organizaciones en su campo. Esta teoría se ve obstaculizada por la vaguedad con respecto a la identidad de las partes interesadas corporativas, priorizando a las partes interesadas desde el punto de vista financiero y la capacidad limitada para predecir y explicar el comportamiento gerencial (Deegan, 2002; Gray et al., 1995).

Según Dimaggio (1982), el proceso para la definición de la institucionalidad consta de cuatro partes: un aumento en el grado de interacción entre organizaciones; el surgimiento de inter organizaciones claramente definidas estructuras nacionales de dominación y

patrones de coalición; un aumento en la carga de información con las que las organizaciones en un campo deben contender; y el desarrollo de una conciencia mutua entre los participantes en un conjunto de organizaciones que están involucradas en una empresa común. En esta línea, se argumenta que las compañías más propensas a actuar de manera responsable e informar sobre su comportamiento son las que operan en entornos institucionales con una fuerte presión coercitiva y normativa, es decir, con un importante y desarrollado sistema legal orientado a la protección de los stakeholders (Campbell, 2007). Asumir esta relación permite aceptar que las compañías que operan en países con similitudes institucionales adoptan comportamientos homogéneos (Abraham & Shrives, 2014; DiMaggio & Powell, 1983; Garcia-Sanchez et al., 2016; La Porta et al., 1998; Meyer & Rowan, 1977; Ntim et al., 2013 Rogers, 2003). DiMaggio & Powell (1983) denominaron a este proceso "isomorfismo" y argumentaron que mejora la estabilidad y supervivencia de las empresas, facilitando el poder político y la legitimidad institucional. Estas prácticas isomórficas emanan de la decisión de la organización de parecerse a los demás (isomorfismo mimético), de hacer lo profesionalmente correcto (isomorfismo normativo), o de cumplir con reglas aplicadas por fuerzas externas (isomorfismo coercitivo) (Perez-Batres et al., 2010). En este marco, desde la divulgación de riesgos desde una perspectiva teórica múltiple que incluye la teoría institucional, Ntim et al. (2013) y Oliveira et al. (2018) examinan las motivaciones de las divulgaciones relacionadas con el riesgo respecto a la influencia de los mecanismos de Gobierno Corporativo.

### Teoría de la Legitimidad

La teoría de la legitimidad se refiere a un contrato social de nivel macro entre una corporación y la sociedad en general, y por lo tanto, la empresa recibe su legitimidad para existir en la sociedad en general (Ntim et al., 2013). Este contrato es sumamente difícil de establecer, pero comúnmente se asocia este concepto a la representación de una gran variedad de expectativas implícitas y explícitas que la sociedad tiene con relación a la forma en la cual las organizaciones deben de llevar a cabo sus actividades (Deegan, 2000). Por lo tanto, podemos decir que este contrato supera la dimensión económica. La

legitimidad institucional ve la legitimidad como un conjunto de creencias constitutivas (Oliveira et al., 2018). La legitimidad estratégica ve la legitimidad como un recurso operativo que necesita ser ganado, mantenido o restaurado (Suchman, 1995). Para mejorar la reputación corporativa, buscan estabilidad y legitimidad controlando estratégicamente el proceso de legitimación a través de la divulgación para influir en las percepciones de las dependencias externas sobre sí mismas y controlar el flujo de recursos (Oliver, 1991). Según Abraham & Shrives (2014), los gerentes pueden usar las divulgaciones de riesgos para administrar la legitimidad organizacional (estratégica e institucional).

### Teoría de las Partes Interesadas

A mediados de la década de 1980 Freeman (1984) define las partes interesadas como cualquier grupo o individuo que se ve afectado o puede afectar el logro de los objetivos de una organización. El enfoque busca ampliar el concepto de gestión estratégica más allá de sus raíces económicas tradicionales, al definir a las partes interesadas como cualquier grupo o individuo que se ve afectado o puede afectar el logro de los objetivos de una organización. Freeman & Reed, (1983) sustentan la existencia de las empresas a partir de los grupos. Si bien la década de 1980 proporciona un entorno que demostró el poder de un enfoque de las partes interesadas, la idea no era del todo nueva. El uso del término, parte interesada surgió del trabajo pionero en el Instituto de Investigación de Stanford (ahora SRI International) en la década de 1960 (Freeman & Mcvea, 2001). SRI argumentó que los gerentes necesitaban comprender las preocupaciones de los accionistas, empleados, clientes, proveedores, prestamistas y la sociedad, con el fin de desarrollar objetivos que las partes interesadas apoyarían (Freeman & Mcvea, 2001). La teoría de las partes interesadas sostiene que debe existir una relación simbiótica entre la empresa y sus grupos externos e internos, y que el valor de la empresa depende de la capacidad de la empresa para satisfacer las necesidades de sus partes interesadas (Khatib et al., 2021).

Las partes interesadas también incluyen otras personas que podrían verse afectadas por la entidad corporativa, incluida la comunidad local, que se vería afectada económica,

socialmente e incluso políticamente por acción corporativa (Tricker, 2020). Esta teoría explica que la empresa no es una entidad que solo opera por sí misma, sino que también debe beneficiar a sus partes relacionadas, en este caso mostrando un mayor interés en divulgar información (Rodríguez-Ariza et al., 2014). En este sentido, la divulgación de los impactos se soporta en esta teoría de los stakeholders debido a que son los grupos de interés quienes interpelan el comportamiento empresarial. Así, la información presentada en los diferentes informes anuales se convierte en una comunicación de la organización con sus partes interesadas. Puntualmente frente a la seguridad en Internet y en el ciberespacio, se trata de un tema que nos preocupa a todos (partes interesadas). Cada vez hay más presencia en el ciberespacio, sitios web y otras aplicaciones tienden a aprovechar este nuevo mundo virtual (ISO 27032).

En contraste, la teoría de las partes interesadas proporciona una resolución más refinada al identificar y referirse a partes interesadas poderosas específicas dentro de la sociedad en general y, por lo tanto, son las partes interesadas identificadas las que confieren legitimidad a una corporación (Gray et al., 1995; Reverte, 2009).

### 4.1.3. Mecanismos de Gobierno Corporativo

Con un número cada vez mayor de escándalos y fracasos corporativos, el Gobierno Corporativo se ha convertido en un tema común y controvertido en las últimas décadas (Jamaludin et al., 2015). De acuerdo con Donnelly & Mulcahy (2008), el Gobierno Corporativo es un conjunto de mecanismos de control que están especialmente diseñados para monitorear y ratificar las decisiones gerenciales, y para asegurar la operación eficiente de una empresa en nombre de sus grupos de interés. Dichos mecanismos de Gobierno Corporativo pueden frenar la expropiación de personas con información privilegiada, proteger los intereses de los accionistas minoritarios y/o de inversionistas extranjeros y garantizar un desempeño operativo eficiente y decisiones empresariales óptimas (Fama & Jensen, 1983). Los miembros del órgano de gobierno deben asumir la responsabilidad colectiva de dirigir y establecer la dirección de la organización; aprobar la política y la planificación; supervisión y seguimiento de la implementación y ejecución por parte de la gerencia; y garantizar la rendición de cuentas por el desempeño de la

organización (King, 2016). En este sentido, el Gobierno Corporativo enfatiza sobre los principios de transparencia, rendición de cuentas, independencia, y equidad (Fakhfakh & Jarboui, 2022). Estos mecanismos de Gobierno Corporativo, que fueron diseñados principalmente para proteger los intereses de los accionistas minoritarios, también podrían fomentar la administración gerencial en beneficio de todas las partes interesadas (Jizi et al., 2014). En general, la adopción de mecanismos de Gobierno Corporativo se considera positiva tanto para las empresas como para los mercados de capitales y las economías nacionales (La Porta et al., 2000).

El consejo de administración es la máxima autoridad legal con respecto a la toma de decisiones en la empresa (R. B. Adams & Ferreira, 2007). Las variables de Gobierno Corporativo que se prevé que influyan en la transparencia varían desde mecanismos externos en forma de sistemas legales para los estudios a nivel de país, hasta mecanismos de Gobierno Corporativo relacionados con la Junta Directiva, sus comités, su independencia, la propiedad accionaria de los directores y gerentes, la concentración de la propiedad entre los grandes accionistas y la calidad de los auditores (Brennan & Solomon, 2008). Según Eisenhardt (1985), el Gobierno Corporativo a menudo incluye la concentración de la propiedad, la composición de la Junta, el liderazgo de la Junta y la compensación ejecutiva. Entre los mecanismos de Gobierno Corporativo basados en el mercado, según Luo (2005) se encuentran el tamaño y la composición del directorio. A ambos nos referimos a continuación. Además, también haremos referencia a la independencia y la diversidad de género de la Junta. Finalmente, nos referiremos al Comité de Auditoría, como comité especializado de la Junta.

**Tamaño de la Junta Directiva**

Según Ahmed et al. (2006), lo que constituye la composición y el tamaño óptimos de la Junta Directiva sigue siendo en gran medida una cuestión empírica de cierta importancia para académicos, profesionales y otros grupos interesados, como los reguladores de la industria. Según Agrawal & Knoeber (2015), el tamaño del directorio es un factor importante del Gobierno Corporativo basado en el mercado, ya que existen inconvenientes cuando los directorios son demasiado pequeños o grandes.

En las juntas grandes, los beneficios del aumento de la capacidad de supervisión se ven superados por los problemas de coordinación y la lentitud en la adopción de decisiones (Lipton & Lorsch, 1992). Según Coles et al. (2008) las empresas grandes y diversificadas tienden a utilizar un mayor número de directores en sus juntas directivas, tanto para fines de monitoreo como de asesoramiento. Linck et al. (2008) sugieren que la estructura de la Junta Directiva en todas las empresas es consistente con los costos y beneficios de la función de supervisión de la junta, sosteniendo la noción popular de que las juntas más pequeñas e independientes son la estructura de gobierno preferible. Cuando una Junta es demasiado grande, a pesar de tener un grupo de experiencia y recursos más grande y diversificado, también es más probable que tenga facciones que aumenten el conflicto grupal (O'Reilly et al., 1989). Además, puede ser ineficaz para tomar medidas decisivas debido a las frecuentes interrupciones de las dificultades de coordinación (Shleifer et al., 1997). Jensen (1993) y Lipton & Lorsch (1992) sostienen que es menos probable que los directores independientes funcionen de manera efectiva cuando los directorios crecen, ya que les resulta más difícil expresar sus ideas y opiniones y, por lo tanto, influir en la eficacia de la toma de decisiones y el control. Además, las juntas grandes dan como resultado una coordinación menos efectiva, mayores costos de información y una toma de decisiones confusa. Al mismo tiempo, los directorios grandes podrían estar controlados por un Director Ejecutivo (CEO) dominante que sofoca la iniciativa, el debate objetivo y la toma de decisiones efectiva (Jensen, 1993). Sin embargo, otros autores opinan que una Junta más grande puede ofrecer más conocimiento y experiencia, así como más capacidad para monitorear y compartir la carga de trabajo (Larmou & Vafeas, 2009).

La Junta Directiva es el vértice común de los sistemas de control de las decisiones de las organizaciones, grandes y pequeñas, en las que los agentes de decisión no tienen una parte importante de los efectos de la riqueza de sus decisiones (Fama & Jensen, 1983). Según Brennan (2006) la Junta Directiva es el principal y dominante mecanismo de Gobierno Corporativo interno. Se puede decir que es una extensión de los propietarios de una corporación (Yeung & Lento, 2018).

En general, se cree que la Junta Directiva tiene al menos cuatro funciones importantes: monitorear y controlar a los gerentes, proporcionar información y asesoramiento a los gerentes, monitorear el cumplimiento de las leyes y regulaciones aplicables, y vincular a la corporación con el entorno externo (Mallin, 2006). De hecho, el Gobierno Corporativo depende no solo de este marco regulatorio, sino también de los procesos fácticos que se desarrollan en estas reglas y activan las prácticas de gobierno (Werder, Axel ; Talaulicar, 2006). El Gobierno Corporativo debe verse como lo que es, es decir, una condición previa altamente deseable, aunque de ninguna manera primordial o suficiente, para las inversiones de capital y, por lo tanto, para el crecimiento (Bartha, Peter; Gillies, 2006).

La Junta es responsable de cuestiones como la contratación, compensación, el despido del CEO y la supervisión de la estrategia comercial general de la empresa, incluida su actividad en el mercado para el control corporativo (Agrawal & Chadha, 2005). Según Fama & Jensen (1983), tales tableros siempre tienen el poder de ratificar y monitorear decisiones importantes. La función de seguimiento que desempeña el directorio es un mecanismo importante de control del Gobierno Corporativo, especialmente en países donde los mecanismos externos están menos desarrollados (Campbell & Mínguez-Vera, 2008). La literatura presenta resultados ambiguos, algunos estudios argumentan que una gobernanza más sólida aumenta el valor de los accionistas (Hermalin & Weisbach, 2003) y otros trabajos exponen que un control excesivo del directorio disminuye este valor (Adams & Ferreira, 2007;  Almazan & Suarez, 2003).

Es de anotar que, a nivel internacional, existen diferencias marcadas respecto a la conformación de los directorios. Así, en los Estados Unidos el sistema de directorio es único mientras, por ejemplo, en algunos países europeos el sistema de directorio dual está formalmente separado en un directorio de administración y un directorio de supervisión (Adams & Ferreira, 2007). Mientras que el consejo de administración es responsable de dirigir la empresa, el consejo de supervisión nombra, supervisa y asesora a los miembros del consejo de administración. Sin embargo, con el fin de garantizar un equilibrio de poder y la independencia de la dirección para llevar a cabo las actividades cotidianas de

la empresa, un miembro del consejo de administración puede ser destituido únicamente por una buena razón (Werder, Axel; Talaulicar, 2006)

Una Junta Directiva que funcione bien debe tener características que sean únicas para la empresa y su entorno regulatorio. La literatura sobre el monitoreo de la Junta se ha centrado en gran medida en la composición de la Junta (Yeung & Lento, 2018). La preocupación primordial, respecto a la composición del órgano de gobierno es si éste tiene los conocimientos, las habilidades, la experiencia, la diversidad y la independencia necesarios para cumplir plenamente con su función y responsabilidades de gobierno (King, 2016). En la literatura financiera empírica, la composición de la Junta se ha considerado muy importante con respecto a la capacidad de monitorear los intereses de los accionistas de manera efectiva (Ahmed et al., 2006). Junto con el tamaño, la composición de la Junta Directiva ha sido el centro de muchos debates sobre Gobierno Corporativo en los últimos años. Muchos investigadores y reguladores han sugerido que las juntas corporativas deberían ser pequeñas y estar compuestas principalmente por directores independientes (Ahmed et al., 2006).

**Independencia**

Esencialmente, para ser independiente un director no debe tener ningún interés en la empresa más que el cargo de director y, tal vez, una participación accionaria insignificante (Tricker, 2020). El uso de directores independientes no ejecutivos para monitorear el desempeño de la gerencia ejecutiva es una práctica ampliamente recomendada en las pautas de Gobierno Corporativo en todo el mundo (Stapledon, 2006). Se espera que los directores independientes mitiguen los conflictos de agencia entre los grandes accionistas controladores y los accionistas externos minoritarios (Allegrini & Greco, 2013; Anderson et al., 2004; Fama & Jensen, 1983; Patelli & Prencipe, 2007).

Respecto a la independencia, según Tricker (2020), se define con precisión en los códigos de Gobierno Corporativo para garantizar que estos directores no tengan ningún interés en la empresa que podría, o podría verse que, afecta adversamente el juicio independiente y

el objetivo genuino. Por citar dos ejemplos, al respecto el Informe Cadbury (1992) establece que los directores no ejecutivos deben ejercer un juicio independiente sobre cuestiones de estrategia, desempeño, recursos, incluidos los nombramientos clave y los estándares de conducta. En concordancia, el Informe King (2016) señala que tener miembros del órgano de gobierno que parezcan independientes es un elemento esencial en la mayoría de los códigos de gobierno. Desde el punto de vista normativo, también podemos ver cómo las diferentes regulaciones del mercado de valores sobre Gobierno Corporativo, por ejemplo la Ley Sarbanes-Oxley suponen que los directores externos son más eficaces en el seguimiento de la gestión (Agrawal & Chadha, 2005).

**La Diversidad de Género de la Junta**

En relación con la diversidad de género de la Junta, el creciente debate sobre el efecto de la diversidad de género en los resultados y estrategias de la empresa ha dado lugar a llamamientos en varios países para una mayor participación de las mujeres en el Gobierno Corporativo (Radu & Smaili, 2021). La participación femenina en las juntas directivas es un tema de frecuente estudio por parte de los organismos reguladores, los encargados de formular políticas, las corporaciones y los académicos como una forma de mejorar el Gobierno Corporativo. Se argumenta que la representación femenina mejora la calidad de la toma de decisiones, ya que tiene en cuenta las opiniones de los grupos subrepresentados, incluidas varias partes interesadas y mujeres accionistas (Deloitte, 2021c).

Así lo confirma, por ejemplo el Informe de Gobierno Corporativo King (2016), “la necesidad de que el órgano de gobierno establezca y divulgue el progreso hacia los objetivos de diversidad de género se ha incluido específicamente en este código”. Algunos estudios transversales recientes sugieren una relación positiva entre la diversidad de la Junta y el valor de la empresa (Agrawal & Knoeber, 2001; Carter et al., 2003; Harrigan, 2017), y otros destacan su incidencia en el desempeño financiero de la empresa (Campbell & Mínguez-Vera, 2008).

El informe de mujeres en la sala de juntas (Deloitte, 2021c) muestra un lento avance hacia el aumento del número de mujeres en los consejos de administración. El promedio mundial de mujeres en juntas en 2021 se encuentra en 19.7%, un aumento de solo 2.8 puntos porcentuales respecto al último informe, publicado en 2019. Las mujeres siguen excluidas de los principales puestos de liderazgo, hay comparativamente pocas mujeres que presiden directorios, concretamente, 6,7% en 2021, frente al 5,3% del último informe 2019 (Deloitte, 2021c). La literatura previa en lo que se refiere a las mujeres, inicia con el estudio seminal *Men and Women of the Corporation,* en el que Rosabeth Moss Kanter (1977) muestra cómo las mujeres en sus diferentes roles tratando de ir hacia arriba, están marcadas por la distribución del poder y la impotencia dentro de la corporación. Según estudios anteriores, la diversidad de género dentro del Gobierno Corporativo expone como trabajos más citados los siguientes: Adams & Ferreira, 2009; Adams & Funk, 2012; Bear et al., 2010; Campbell & Mínguez-Vera, 2007; Carter et al., 2010; Dezsö & Ross, 2012; Farrell & Hersch, 2005; Francoeur et al., 2008; Gul et al., 2011; Kang et al., 2007; Kor, 2006; Nielsen & Huse, 2010; Rose, 2007; Srinidhi et al., 2011; Van der Walt & Ingley, 2003. Específicamente, Adams & Ferreira (2009) evidencian que las mujeres asisten a más reuniones y es más probable que se las asigne a comités relacionados con el monitoreo que los hombres. Si las mujeres también participan activamente en las reuniones de la Junta y del comité de seguimiento, podrían aumentar la intensidad de la supervisión de la Junta.

**Comité de Auditoría**

A diferencia de la Junta en su conjunto, los comités de la Junta se especializan en tareas definidas de manera específica (Adams & Ferreira, 2009). Los comités de auditoría son mecanismos de la Junta para mejorar la rendición de cuentas en torno a las funciones de información financiera y contabilidad, y han sido ampliamente investigados (Collier & Institute of Chartered Accountants in England and Wale., 1992; DeZoort et al., 2002; Gendron & Bédard, 2006). El propósito principal del Comité de Auditoría de la Junta es supervisar el proceso de información financiera de una empresa (Agrawal & Chadha, 2005). Entre sus muchas disposiciones, la Ley Sarbanes-Oxley y las reglas del mercado

de valores en conjunto requieren que el Comité de Auditoría de la Junta esté compuesto en su totalidad por directores independientes, tenga al menos un miembro con experiencia y restrinja los tipos de servicios no relacionados con la auditoría que el auditor externo puede proporcionar (Agrawal & Chadha, 2005). Para ser efectivo, un Comité de Auditoría debe tener un número adecuado de miembros del comité (DeZoort et al., 2002). Son funciones del comité recomendar el nombramiento de auditores independientes y consultar periódicamente con ellos sobre asuntos relacionados con controles y procedimientos financieros internos (Adams & Ferreira, 2009). Los comités de auditoría de las juntas corporativas generalmente no son muy activos. Por lo general, se reúnen solo unas pocas (dos o tres) veces al año. Del mismo modo, a pesar de que una Junta típica se reúne con más frecuencia (generalmente de seis a ocho veces al año) que el Comité de Auditoría, tiene una variedad de otros temas en su agenda además de supervisar los informes financieros de la empresa (Agrawal & Chadha, 2005).

## 4.2. Gobierno Corporativo en América Latina

### 4.2.1. Marco Normativo

La Mesa Redonda Latinoamericana de Gobierno Corporativo, con el respaldo del Banco Mundial y la OCDE, en el año 2000 se convierte en el primer antecedente para el surgimiento del Gobierno Corporativo en América Latina. Con estas mesas regionales la OCDE ha buscado motivar el diálogo permanente entre los agentes del mercado de los países miembros y los colaboradores de la organización, reguladores y los formuladores de políticas, así como estimular la cooperación entre ellos. En cada una de las reuniones de la Mesa Redonda estuvieron presentes líderes políticos, representantes de los reguladores, líderes empresariales, inversores, organizaciones no gubernamentales de varios países de América Latina y otras organizaciones multilaterales con interés en el tema (CCB & OCDE, 2004).

Después de las reuniones en Brasil (2000), Argentina (2001), México (2002) y Chile (2003), se obtuvo el “Informe Oficial sobre Gobierno Corporativo en América Latina”,

en el cual se examinó la pertinencia del Gobierno Corporativo tomando los Principios de Gobierno Corporativo de la OCDE, como un marco de trabajo conceptual para su análisis y discusión (CCB & OCDE, 2004). Se consideraron las tendencias y características regionales, así como las recomendaciones y prioridades para reformas y prácticas adoptadas sobre la efectividad de las juntas directivas, el cumplimiento de normas, el desarrollo de códigos de Gobierno Corporativo y la implementación de buenas prácticas.

Posterior al informe oficial de 2003, las reuniones de la Mesa Redonda se han llevado a cabo anualmente en distintas urbes de los países cuyos mercados de capitales son considerados los más activos de Latinoamérica, entre los que se encuentran Argentina, Brasil, Chile, Colombia, México y Perú. En este proceso también se crea la Red Latinoamericana de Gobierno Corporativo en el año 2002. Posteriormente, en el año 2009, se crea la Red de Institutos de Gobierno Corporativo de Latinoamérica (Gobierno Corporativo), establecida en Santiago de Chile en la Mesa Redonda de Gobierno Corporativo, organizada por la OCDE y el Grupo Banco Mundial a través de la Corporación Internacional (IFC)".

No obstante, aunque las bolsas de valores de América Latina se encuentran entre los mercados más pequeños y menos activos del mundo en relación con el tamaño de las economías (Chong & Lopez-de-Silanes, 2007), éstas han constituido un aporte importante para los países de la región en el marco de la regulación sobre Gobierno Corporativo latinoamericano, a través de la exigencia de nuevos requerimientos, así como con la incorporación de nuevos índices bursátiles para la evaluación de la gobernanza corporativa.

Los países de derecho civil, y en particular los de derecho civil francés, tienen las protecciones de los inversores más débiles y los mercados de capitales menos desarrollados, especialmente en comparación con los países de derecho consuetudinario (La Porta et al., 1997). En este caso, todos los países latinoamericanos comparten un origen común en el derecho civil y sus mercados de capital pueden ofrecer una protección a los accionistas minoritarios por debajo del promedio en relación con otras naciones de

derecho civil (Chong, Alberto; López de Silanes, 2007). Además de los aportes de las bolsas de valores, el Banco de Desarrollo para América Latina CAF también contribuye, con informes anuales sobre prácticas en Gobierno Corporativo necesarias para afrontar los retos empresariales para las organizaciones en la región. No obstante, de acuerdo con OCDE (2016) en la actualidad los Principios de Gobierno Corporativo de la OCDE y del G20 continúan proporcionando un marco de referencia que contribuye al crecimiento sólido y al desarrollo de sociedades más inclusivas en su versión más reciente publicada en 2016, como resultado de una revisión de los principios de 2004.

Según OCDE (2016), en el ámbito mundial el marco de Gobierno Corporativo suele basarse en leyes, reglamentos, sistemas de autorregulación, compromisos voluntarios y prácticas empresariales que son consecuencia de las circunstancias, la historia y la tradición específicas de los países. Los Principios de Gobierno Corporativo del G20 y de la OCDE ayudan a los legisladores a evaluar y mejorar el marco legislativo, reglamentario e institucional del Gobierno Corporativo, con el objetivo de favorecer la eficiencia económica, la estabilidad financiera y el crecimiento económico sostenible (OCDE, 2016). Es importante tener en cuenta que la ley no puede exigir la efectividad de las prácticas de la Junta, pero a veces los requisitos legales y reglamentarios o las recomendaciones de "cumplir o explicar" de los códigos pueden contribuir a la adopción de buenas prácticas (Financial Standards Foundation, 2011). No obstante, el entorno legal, tal como se describe tanto en las normas legales como en su aplicación, es importante para el tamaño y la extensión de los mercados de capitales de un país (La Porta et al., 1997).

La falta de protección legal de los accionistas en América Latina ha resultado en una alta concentración del control de las empresas en las manos de un grupo élite de familias (Sargent, John & Ghaddar, 2001). De acuerdo con Garay y González (2008), como se citó en Briano (2012), Latinoamérica ha optado por la adopción voluntaria de prácticas y políticas de buen gobierno para cubrir parcialmente la deficiencia legal que opera en el entorno. En la Tabla 21 se incluyen los códigos y regulaciones de Gobierno Corporativo que están en vigor en los países con mayor cotización bursátil en Latinoamérica. Según

Deloitte (2021), los países que se han destacado por la implementación regulatoria del marco de Gobierno Corporativo son México y Argentina.

**Tabla 21. Códigos y normativas de Gobierno Corporativo vigentes en América Latina**

| País | Códigos /Normativas |
|---|---|
| Argentina | Código de Gobierno Societario de Argentina (Comisión Nacional de Valores, 2019)<br>Ley de Mercado de Valores 18045<br>Ley General de Sociedades 19550 |
| Brasil | Código de mejores prácticas de Gobierno Corporativo Brasil (IBGOBIERNO CORPORATIVO, 2015)<br>Resolución N° 65, Acta N° 72 de fecha 04/11/10<br>Circular SB.SG. N° 679/2012 de fecha 09/08/12 |
| Chile | Ley 20382 de 2009 que modifica la Ley 18045: 18046 (Ministerio de Hacienda, 2022). |
| Colombia | Guía de Buenas Prácticas de Gobierno Corporativo para empresas competitivas, productivas y perdurables Colombia (SuperSociedades et al., 2020) |
| México | Código de principios y mejores prácticas de Gobierno Corporativo (Consejo coordinador empresarial, 2018). Ley de Mercado de Valores (LMV) Cámara de Diputados del Congreso de la Unión 2019. |
| Perú | Código de buen Gobierno Corporativo para las sociedades peruanas (Superintendencia del Mercado de Valores, 2013) |

Este panorama normativo, que guía el Gobierno Corporativo en América Latina, busca legitimar el sistema económico con miras a incrementar la atracción de inversión extranjera y los fondos en los mercados de capital. Aunque la región se ha librado sorprendentemente de una ola generalizada de escándalos corporativos, los mercados de capital en América Latina están rezagados con respecto al resto del mundo (Chong & Lopez-de-Silanes, 2007), y se caracterizan aún por un escaso nivel de desarrollo relativo que se refleja en una baja profundización financiera e incipiente capitalización bursátil (CAF, 2013). Si bien los distintos países pueden tener su propio marco regulatorio con prácticas de Gobierno Corporativo distintas, en realidad las prácticas tienen el mismo enfoque y la finalidad es la misma, implementar sólidos sistemas de Gobierno

Corporativo que generen mayor valor a sus accionistas y terceros interesados, promoviendo las competitividad y los mejores resultados (Deloitte, 2021b).

El Gobierno Corporativo en el contexto latinoamericano presenta condiciones propias relacionadas con la protección legal de los inversionistas, la presencia de inversionistas de referencia, la amenaza de toma de control corporativo, las juntas directivas, los directorios entrecruzados y los contratos de incentivos, que difieren sustancialmente de las de otros países examinados en estudios anteriores (Castro, 2009). Además, está condicionado por el hecho de que las empresas familiares representan una parte significativa de las empresas que cotizan en bolsa en América Latina (Briano-Turrent & Poletti-Hughes, 2017). En este contexto, las prácticas de Gobierno Corporativo tienen el potencial de convertirse en una poderosa herramienta de desarrollo para las economías emergentes que buscan lograr objetivos nacionales (Tabassum & Singh, 2020).

### 4.2.2. Prácticas de Gobierno Corporativo en América Latina

El marco conceptual clásico del problema de la agencia y los mecanismos de control no aplica en los países latinoamericanos (Castro, 2009). En este contexto, el problema de la agencia se traslada a que los accionistas mayoritarios son los que toman las decisiones y son quienes se supone se benefician a costa de los accionistas minoritarios. En América Latina, donde el sistema de protección legal es débil, el control tiene un valor incremental para los accionistas mayoritarios (controladores) porque provee grandes beneficios privados (Barclay & Holderness, 1991; Chong & López, 2007). El cumplimiento de Gobierno Corporativo puede constituir una herramienta estratégica para alinear los intereses de los accionistas mayoritarios y minoritarios. Bajo estas condiciones, el oportunismo de los accionistas mayoritarios, y no el de la gerencia, menoscaba los incentivos que tienen los inversionistas minoritarios para invertir en las empresas de los países de la región (Castro et al., 2009).

Las prácticas de Gobierno Corporativo de mayor relevancia internacional son, según Deloitte (2021a), el involucramiento de consejeros independientes, la implementación de

una visión estratégica en el consejo de administración, la evaluación del consejo, la ejecución de sesiones ejecutivas, la creación de un Comité de Auditoría y un comité de prácticas societarias, la figura del auditor externo, la vigilancia de los conflictos de interés, los riesgos y el control interno en las empresas, la implementación de planes de compensación en acciones, las votaciones en los consejos, los temas de sucesión directiva en las empresas, la responsabilidad social y las Tecnologías de la I. A continuación, se revisa en qué medida estas prácticas están incorporadas en los códigos de Gobierno Corporativo de los países objeto de estudio (Tabla 22).

**Tabla 22. Prácticas de Gobierno Corporativo en países objeto de estudio**

| Prácticas de Gobierno Corporativo | Argentina | Brasil | Chile | Colombia | México | Perú |
|---|---|---|---|---|---|---|
| 1. Involucramiento de consejeros independientes | X | X | - | X | X | X |
| 2. La implementación de una visión estratégica en el Consejo de Administración | X | X | X | X | X | X |
| 3. La evaluación del Consejo | X | X | - | X | - | - |
| 4. La ejecución de sesiones ejecutivas (independientes) | - | X | - | - | - | - |
| 5. La creación de un Comité de Auditoría | X | X | X | X | X | X |
| 6. La creación de un comité de prácticas societarias | X | X | - | - | X | X |
| 7. Evaluación del auditor externo | X | X | - | - | X | - |
| 8. La vigilancia de los conflictos de interés | X | X | X | X | - | X |
| 9. Supervisar la gestión de riesgos y los sistemas de control interno | X | X | X | X | X | X |
| 10. La implementación de planes de compensación en acciones | - | - | - | X | X | - |
| 11. Las votaciones en contra deben explicarse si superan determinado porcentaje. | - | - | - | - | - | - |
| 12. Existencia de plan de sucesión | X | X | - | X | X | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| 13. La responsabilidad social | X | X | X | X | - | - |
| 14. Las Tecnologías de la Información | - | - | - | X | X | - |

Respecto al ítem 1 podemos observar cómo la participación de directores independientes es una práctica común de Gobierno Corporativo en Argentina, Brasil, Colombia, México y Perú. En Argentina, según el Código de Gobierno Societario, tan solo se exige tener un número suficiente de consejeros independientes. En Brasil, de acuerdo con el Código de mejores prácticas de Gobierno Corporativo Brasil, se requiere que la mayoría de los consejeros sean independientes. Desde la Guía de buenas prácticas de Gobierno Corporativo para empresas competitivas, productivas y perdurables, en Colombia es aconsejable que una tercera parte del consejo esté conformado por miembros independientes. En México solo es obligatorio el 25% en el consejo de administración, según el Código de principios y mejores prácticas de Gobierno Corporativo. Por su parte, en Perú se promueve que al menos un tercio del directorio esté constituido por directores independientes, según el Código de buen Gobierno Corporativo para las sociedades peruanas.

Frente al cumplimiento del ítem 2, relacionado con la implementación de una visión estratégica en el Consejo de Administración, todos los códigos de los países cumplen con este requerimiento. En el ítem 3, Argentina, Brasil y Colombia deben realizar una evaluación anual del consejo de administración. En el caso de Argentina, el Consejo de Administración debe desarrollar un documento escrito como guía para la evaluación. Respecto al ítem 4, la ejecución de sesiones ejecutivas (independientes), el único país que cumple con esta práctica es Brasil. En cuanto al ítem 5, todos los países cuentan con un código o normativa que relaciona el Comité de Auditoría. En el ítem 6, Argentina, Brasil, México y Perú cuentan con un comité de prácticas societarias. En relación al ítem 7, Argentina, Brasil y México contemplan en su código que el consejo es el encargado de la evaluación del desempeño del auditor externo.

Por lo que respecta al ítem 8, la vigilancia de los conflictos de interés, el único país que no contempla esta práctica es México. En Argentina se deben informar las operaciones

con compañías afiliadas y vinculadas, según su Comisión Nacional de Valores (2019). Frente a supervisar la gestión de riesgos y los sistemas de control interno (ítem 9), en todos los países esta función se atribuye al consejo de administración. En relación con el tema de la implementación de planes de compensación en acciones, tan solo Colombia y México requieren esta información (ítem 10), y en México se requiere la aprobación expresa de los accionistas para la aprobación y modificación de un plan en compensación en acciones. En cuanto al ítem 11, en ninguno de los códigos de los países existen disposiciones respecto a la votación en contra de una resolución del consejo, lo cual hace que nunca se conozcan las razones por las cuales los consejeros votan de una u otra forma.

El plan de sucesión (ítem 12) busca la permanencia, el crecimiento y la continuidad de la empresa a través del tiempo. En Argentina se requiere documentar un plan de sucesión formal para el director general, mientras que en México solo se le considera como mejor práctica. También está contemplado en Brasil, Colombia y Perú. En relación con el tema de responsabilidad social (ítem 13), en Argentina se deberán adoptar políticas adecuadas y razonables respecto a la responsabilidad social, mientras que en México no son obligatorias y no existen. En Colombia tocan el tema al dejar abierta la opción de adoptar la norma ISO 26000 estándar de responsabilidad social. Finalmente, las Tecnologías de la Información (ítem 14) es una exigencia tan solo en Colombia y México.

### 4.3. Investigación sobre Gobierno Corporativo como Factor de Divulgación de Ciberseguridad

La literatura previa ha documentado, de acuerdo con sus argumentos teóricos, una relación entre el Gobierno Corporativo y la divulgación de riesgos, basada en el papel de ésta última como mecanismo de control de los problemas de agencia (Abraham & Cox, 2007; Allini et al., 2016; Barakat & Hussainey, 2013; Elshandidy & Neri, 2015; Lajili & Zéghal, 2005; Lim et al., 2007; Ntim et al., 2013). Los efectos del Gobierno Corporativo en la práctica de informes mitigan la asimetría de la información y mejoran la función de administración.

De acuerdo con la evidencia obtenida en investigaciones precedentes (Campbell et al., 2014; Jorion, 2002; Kravet & Muslu, 2013; Rajgopal, 1999), la información precisa sobre riesgos como mecanismo de control externo reduce los costos de agencia, siendo fundamental para accionistas, analistas e inversores, ya que les permite evaluar el perfil de riesgo de una empresa, estimar su valor de mercado y tomar decisiones de inversión acertadas. Con base en la teoría de la agencia, el rol de monitoreo de la Junta es asegurar que la administración corporativa persiga los intereses de los accionistas.

Por lo que respecta a la presente investigación, dadas las características del contexto latinoamericano, la teoría de la agencia se analiza desde una perspectiva diferente, debido a que el problema en estos países radica en los accionistas mayoritarios y no en la gerencia. Así, la teoría de la agencia tiene como objetivo explicar la relación entre los accionistas minoritarios y mayoritarios, y los conflictos de interés que surgen entre estas dos partes. Sin embargo, estos dos tipos de accionistas están sujetos a las divulgaciones de riesgos de Ciberseguridad reportados por las compañías. Con base en la teoría de la agencia, la regulación débil sobre la divulgación de riesgos de Ciberseguridad brinda a los accionistas mayoritarios la oportunidad de manipular la información divulgada de acuerdo con sus propios intereses. Según esta teoría, se establece que los accionistas mayoritarios tienen conocimientos y habilidades de gestión de los que carecen los accionistas minoritarios, y emplean dichas habilidades para enmarcar la divulgación para su propio beneficio.

### 4.3.1. Marco teórico

Tanto los inversores como las partes interesadas están cada vez más preocupados por la necesidad de integrar la tecnología y la información, en particular la información sobre riesgos de Ciberseguridad (Radu & Smaili, 2021). Coincidimos con Pucheta-Martínez & Gallego-Álvarez (2019) en que la composición del directorio, en particular ciertas características, puede ser un mecanismo de Gobierno Corporativo relevante que aliente a las empresas a interactuar con los accionistas y todas las partes interesadas en términos de mayor transparencia. En este sentido, la presente investigación se desarrolla con base

en la teoría de la agencia y la teoría de las partes interesadas. La literatura de Gobierno Corporativo se ha construido en torno a la teoría de la agencia, e investigaciones precedentes han documentado una relación entre Gobierno Corporativo y la divulgación de riesgos basada en el papel de este último como mecanismo de control de los problemas de agencia (Allini et al., 2016; Barakat; Hussainey, 2013; Elshandidy y Neri, 2015; Ntim et al., 2013) y, en particular, sobre la divulgación de riesgos de Ciberseguridad (Masud & Hossain, 2022).

Respecto a la teoría de las partes interesadas, encaja perfectamente con el concepto de Ciberseguridad de Von Solms & Van Niekerk (2013), quienes indican que la Ciberseguridad debe consistir en proteger algo más que la información o los recursos de los sistemas de información de una persona u organización, refiriéndose esto también a la protección de la(s) persona(s) que utilizan los recursos en un entorno cibernético y a la salvaguarda de cualquier otro activo, incluidos los de la sociedad en general, que hayan estado expuestos a riesgos como consecuencia de vulnerabilidades derivados del uso de las TIC. Según la teoría de los stakeholders, debe existir una relación simbiótica entre la empresa y sus grupos externos e internos, y el valor de la empresa depende de la capacidad de la empresa para satisfacer las necesidades de sus partes interesadas (Khatib et al., 2021). En este contexto, la tecnología crea un riesgo ético, además de sus riesgos técnicos y financieros, ya que la empresa y sus grupos de interés pueden verse afectados cuando la tecnología no es utilizada por principios éticos relacionados con la privacidad (Radu & Smaili, 2021). La literatura previa presenta investigaciones desarrolladas bajo la teoría de las partes interesadas, relacionando la divulgación de riesgos con la composición de la Junta (Ntim et al., 2013) y, específicamente, vinculando los riesgos de Ciberseguridad con el Gobierno Corporativo (Radu & Smaili, 2021).

### 4.3.2. Literatura Previa

**Investigación sobre divulgación de información sobre Ciberseguridad**

Mencionar la Ciberseguridad tiene claros beneficios y solo un pequeño costo para la organización que la publica en el informe anual (Eijkelenboom & Nieuwesteeg, 2021). Entre los primeros estudios relacionados con la divulgación de Ciberseguridad, Gordon et al. (2006) muestran que la divulgación aumenta voluntariamente debido a los lineamientos de la Ley Sarbanes Oxley de 2002. A continuación, Gordon et al.(2010) verifican la relación positiva entre el precio de la acción y la divulgación de Ciberseguridad.

La divulgación global de información relacionada con la Ciberseguridad generalmente se realiza de forma voluntaria. Sin embargo, en el contexto estadounidense, y del panorama bursátil internacional que éste enmarca, las divulgaciones de la Sección 1A ante la SEC fueron ordenadas en 2005 a través del Artículo 503 (c) del Reglamento SK (SEC, 2005) por el cual las empresas deben divulgar y describir sus factores de riesgo específicos. Posteriormente, la Guía propuesta por la División de Finanzas Corporativas & SEC (2011), requiere la divulgación de todos los riesgos materiales. Estudios relacionados han buscado demostrar los efectos de la promulgación de esta Guía SEC 2011 (Amir et al., 2018; Berkman et al., 2018; Gordon et al. (2015a); IRRC (2016); Li et al. (2018); Morse et al. (2018); Wang et al., (2013). En 2018, la SEC aprueba la segunda guía interpretativa sobre divulgación de Ciberseguridad y enfatiza la importancia de suficientes controles y procedimientos de divulgación y la prohibición del uso de información privilegiada no pública de incidentes cibernéticos.

Otros estudios relacionados con la divulgación de Ciberseguridad informan del debate sobre los niveles de divulgación de riesgos cibernéticos. Por ejemplo, la divulgación insuficiente del riesgo cibernético tiene un efecto limitado en los precios de las acciones (Hilary et al., 2016), pero la divulgación excesiva puede ser contraproducente (Héroux & Fortin, 2020). Según Campbell et al. (2014), Hope et al.(2016) y Li et al., (2018), la

Divulgación de Ciberseguridad es útil para los participantes del mercado al momento de evaluar la probabilidad de futuros ciber incidentes. Dado que los incidentes cibernéticos pueden tener impactos negativos en las organizaciones, mejorar la divulgación de Ciberseguridad podría ser útil para varias partes interesadas (Héroux & Fortin, 2020a). Sin embargo, la divulgación completa acelera la propagación de los ataques, aumenta su penetración dentro de la población objetivo y aumenta el riesgo de un primer ataque después de que se informa la vulnerabilidad (Mitra & Ransbotham, 2015). Según Bakker (2015), informar sobre las consecuencias de un incidente de Ciberseguridad y la gestión de los riesgos de Ciberseguridad (incluida la identificación y evaluación de dichos riesgos y la responsabilidad relacionada) es de interés para las partes interesadas. En el contexto canadiense, el Canadian Securities Administrator (CSA), proporcionó a los emisores referencias relacionadas con las normas y publicaciones existentes, junto con información sobre el desarrollo de orientación sobre Ciberseguridad y prácticas de redes sociales (CSA, 2013; CSA, 2017; Héroux & Fortin, 2020).

En términos generales, la literatura relacionada con la divulgación de Ciberseguridad se enmarca mayoritariamente en el contexto norteamericano (Estados Unidos y Canadá), países que cuentan con medidas regulatorias específicas sobre divulgación de Ciberseguridad (SEC, 2011; 2018) y CSA ACVM (2013; 2017), respectivamente. Por su parte, en el contexto europeo los requisitos de información sobre Ciberseguridad están ausentes en la legislación europea específica (Eijkelenboom & Nieuwesteeg, 2021). Sin embargo, las empresas sujetas a la Directiva UE (2014) deben ofrecer una imagen fiel y completa de sus políticas, resultados y riesgos, así como proporcionar información adecuada sobre aquellos aspectos en los que es más probable que se materialicen los principales riesgos de efectos graves, junto con los temas respecto de los cuales ya se han materializado dichos riesgos (UE, 2014). Por su parte, las empresas de los países latinoamericanos no hacen referencia a regulaciones exclusivas para la divulgación de Ciberseguridad en el informe anual. En este sentido, las empresas listadas en América Latina que participen en el mercado de valores de Estados Unidos reportarán en el informe anual 20 F ítem 3D los factores de riesgo relacionados con el riesgo cibernético de acuerdo con SEC (2018b).

**Investigación sobre Divulgación de Riesgos y conformación de la Junta Directiva**

La literatura previa evidencia que la función de supervisión del Gobierno Corporativo incide en la tendencia a una mejor divulgación de información corporativa (Lim et al., 2007 ; Patelli & Prencipe, 2007). Dentro de este marco, algunas investigaciones se centran en la incidencia de la composición de la Junta Directiva en las divulgaciones relacionadas con riesgos (Elzahar & Hussainey, 2012; Mokhtar & Mellett, 2013; Ntim et al., 2013; Oliveira et al., 2011; Taylor et al., 2010). Tan solo dos estudios lo relacionan con riesgos de Ciberseguridad (Masud & Hossain, 2022; Radu & Smaili, 2021).

En este apartado presentamos la literatura previa encargada de relacionar el Gobierno Corporativo como factor de divulgación de riesgos, en general, y de riesgo de Ciberseguridad, en particular. En este sentido, la investigación evidencia que la función de supervisión del Gobierno Corporativo incide en la tendencia a una mejor divulgación de información corporativa (Lim et al., 2007; Patelli & Prencipe, 2007). En nuestra búsqueda hemos revisado, en un primer momento, los artículos publicados desde 1999 que han examinado la relación entre la información sobre riesgos y el Gobierno Corporativo en diferentes áreas geográficas. Concretamente,en Reino Unido (Abraham & Cox, 2007; Elzahar & Hussainey, 2012; Solomon et al., 2000); Reino Unido – Italia (Elshandidy & Neri, 2015); Región Consejo de Cooperación del Golfo (Al-Hadi, et al., 2016), Países Bajos (Barakat & Hussainey, 2013), Sudáfrica (Ntim et al., 2013), Canadá (Lajili & Zéghal, 2005), Australia (Taylor et al., 2010); Portugal (Oliveira et al., 2011), Egipto (Mokhtar & Mellett, 2013), países del Medio Oriente y el Norte de África - MENA (Moumen et al., 2016), Italia (Allini et al., 2016) y, finalmente, España y Portugal (Oliveira et al., 2018).

Dentro de este marco, algunas investigaciones se centran en las divulgaciones relacionadas con Gobierno Corporativo y la composición de la Junta Directiva (Abraham & Cox, 2007; Elzahar & Hussainey, 2012; Mokhtar & Mellett, 2013; Ntim et al., 2013; Oliveira et al., 2011; Taylor et al., 2010). Otros investigadores han ido más allá tratando de evaluar la calidad de estas divulgaciones (Abraham & Cox, 2007; Agyei-Mensah,

2017; Elshandidy & Neri, 2015; Elzahar & Hussainey, 2012b; Mokhtar & Mellett, 2013; Ntim et al., 2013; Oliveira et al., 2011; Taylor et al., 2010).

A continuación (Tabla 23), se presenta una selección de estudios previos sobre la incidencia del Gobierno Corporativo en la divulgación de riesgos, ordenados cronológicamente (2000-2020), resultante de una búsqueda en las bases de datos Scopus y Web of sciences, a partir de los términos ´divulgación sobre riesgos´ y ´Gobierno Corporativo´.

**Tabla 23. Estudios previos sobre la incidencia del Gobierno Corporativo en la divulgación de riesgos**

| Autores | País | Período de análisis | Variables | Muestra/Metodología |
|---|---|---|---|---|
| (Solomon et al., 2000) | Reino Unido | Enero – abril 1998 | No se describen | Muestra<br>552 inversores institucionales.<br>Metodología<br>Encuesta |
| (Lajili & Zéghal, 2005) | Canadá | 2002 | Dependiente: Conteo de oraciones tanto en las notas y en la sección MD&A: Riesgo no financiero total; divulgaciones de riesgo total.<br><br>Independiente: Tamaño del directorio, independencia en la Junta, número de comités, fracción de votos del control (%), compensación de incentivos del CEO, acciones y opciones de CEO.<br><br>Control: Tamaño de la empresa (ventas totales). | Muestra<br>228 empresas canadienses que cotizan en bolsa TSX en 2002.<br>Metodología<br>Análisis de contenido. Conteo de número de palabras y oraciones. Análisis de regresión multivariable<br>Tipo de Informe<br>Anual<br>Teoría<br>Agencia |
| (Abraham & Cox, 2007) | Reino Unido | 2002 | Dependientes: Log N del número de palabras dentro de las oraciones relacionadas con el riesgo, respectivamente, para los informes narrativos de riesgos comerciales, financieros, de control interno y los informes narrativos de riesgos totales.<br>Independientes: Fondos de pensiones de gestión interna, fondos de pensiones de gestión externa y fondos de seguros de vida, directores ejecutivos, consejeros no ejecutivos, directores no ejecutivos. | Muestra<br>Índice FTSE 100: 71 empresas sin sector financiero.<br>Metodología<br>Análisis de contenido manual. Conteo de palabras en oraciones. Cuantitativo. Modelo de regresión múltiple.<br>Tipo de informe<br>Anual, Formulario 20F SEC. |

| | | | | |
|---|---|---|---|---|
| | | | Control: Tamaño (Log N de ventas), industria, apalancamiento, riesgo (varianza de los rendimientos de las acciones a 60 meses). | Teoría<br>Agencia |
| (Lim et al., 2007) | Australia | 2001 | Dependiente: divulgación voluntaria total, cuantitativa prospectiva estratégica, no financiera y divulgación financiera histórica<br><br>Independiente: proporción directores independientes al tamaño total del directorio.<br><br>Control: Tamaño de la empresa, LEV, ROA, tipo de auditor (BIG4), Industria, 20 principales accionistas, precio – valor contable. | Muestra<br>181 empresas que debían haber estado en las 500 principales empresas australianas durante 1999-2001 excluyendo las financieras y mineras.<br>Metodología<br>Análisis de contenido. Índice total de divulgación voluntaria y los subíndices de divulgación voluntaria.<br>Tipo de Informe<br>Informe anual.<br>Teoría<br>Agencia |
| (Patelli & Prencipe, 2007) | Italia | 2002 | Dependiente: adaptamos la puntuación de divulgación propuesto por Botosan en 1997 en categorías: información de antecedentes, resumen de resultados históricos, estadísticas no financieras clave, proyecciones información, discusión y análisis de gestión, presentación de informes por segmentos, puntuación como la suma de las seis puntuaciones de divulgación.<br><br>Independiente: Proporción de consejeros independientes, cargos laborales sobre índice de rotación.<br><br>Control: difusión de propiedad residual, tamaño, apalancamiento, rentabilidad, presión laboral. | Muestra<br>175 empresas cotizadas en la Bolsa de Valores de Milán (no financieras, todas controladas por un accionista dominante).<br>Metodología<br>Adaptación índice de divulgación de Botosan. Análisis de regresión, análisis multivariado.<br>Tipo de Informe<br>Informes anuales de Gobierno Corporativo.<br>Teoría<br>Agencia |
| (Taylor et al., 2010) | Australia | 2002-2006 | Dependiente: alcance de la divulgación de la gestión del riesgo financiero se mide utilizando un índice.<br>Independiente: CGS puntaje de Gobierno Corporativo, captación de capital y cotización en el extranjero<br>Control: tamaño de empresa, apalancamiento, subsector y concentración de accionistas | Muestra<br>111 empresas de recursos extractivos cotizadas en Australia<br>Metodología<br>Regresión<br>Tipo de informe Anual<br>Teoría:<br>Agencia |
| (Oliveira et al., 2011) | Portugal | 2005 | Dependiente: Conteo de oraciones<br>Independiente: Estructura de propiedad, N° ejecutivos independientes directores, independencia Comité de Auditoría (proporción de consejeros no ejecutivos | Muestra<br>42 empresas cotizadas que están obligadas a divulgar un informe de gobernabilidad. |

| | | | | |
|---|---|---|---|---|
| | | | en Comité de Auditoría), auditoría externa calidad (big4), apalancamiento, tamaño (empleados, activos, ventas), sensibilidad ambiental.<br>Control: Estado de cotización de la empresa, normas contables (IAS/IFRS). | Metodología<br>Análisis de contenido. Conteo de oraciones. Modelos de regresión. Análisis bivariado<br>Tipo de informe<br>Anual. |
| (Elzahar & Hussainey, 2012) | Reino Unido | 1 de junio de 2009 y el 31 de mayo de 2010 | Dependiente: número de oraciones relacionadas con el riesgo como una medida de los niveles de divulgación del riesgo.<br>Independiente: Tipo de actividad, tamaño de la empresa, rentabilidad, engranaje, liquidez, cotizar mercado Estados Unidos, propiedad institucional, dualidad, tamaño de la Junta (N°. miembros), directorio no ejecutivo, tamaño del consejo (N°. directores).<br>Control: No se enuncian | Teorías<br>Teoría de la agencia, teoría de la legitimidad y la teoría perspectiva basada en los recursos.<br>Muestra<br>Informes intermedios de 72 empresas no financieras del FTSE 100 del Reino Unido. Informes de riesgos<br>Metodología<br>Análisis de contenido. Índice de calidad de divulgación del riesgo operacional. Conteo de oraciones. Modelo de regresión, Análisis de regresión de mínimos cuadrados ordinario.<br>Tipo de informe<br>Anual. |
| (Mokhtar & Mellett, 2013) | Empresas cotizaban en la Bolsa Egipcia (EGX) Egipto | 2007 | Dependiente: índice no ponderado para medir el nivel de cumplimiento con la divulgación obligatoria de riesgos.<br>Independiente: Tamaño, liquidez, barreras para entrar, tamaño del tablero, industria, dualidad, concentración de propiedad y tipo de auditor. | Teorías<br>Teorías de agencia y señalización<br>Muestra<br>105 empresas no financieras cotizadas.<br>Teoría<br>Agencia, partes interesadas, costo político, señalización, legitimidad.<br>Metodología<br>Análisis de regresión múltiple, análisis de contenido.<br>Tipo de informe Anual |
| (Barakat & Hussainey, 2013) | 20 países miembros de la UE | 2008-2010 | Dependiente:<br>A: Calidad total de divulgación de riesgo operacional<br>B: Riesgo Operacional Voluntario<br>Independiente: Puntuación, volatilidad retorno, PIB per cápita inflación, estabilidad política, costo ingresos, depósitos efectivos. | Muestra<br>85 bancos con al menos 1000 millones de euros de 20 países miembros de la UE<br>243 observaciones de años bancarios.<br>Metodología |

| | | | | |
|---|---|---|---|---|
| | | | A: Restricciones de actividad, requisitos de entrada, supervisor<br>B: BRD fuera (consejeros externos), mayor propio, gobierno propio, ejecutivo propio, ac reunión.<br>Control: lista cruzada de activos totales, anti-director, imperio de la ley, concentración, tipo maniquíes. | Análisis de contenido. Índice de divulgación autoconstruido para medir la calidad ORD. Dos modelos de regresión multivariados, análisis Univariado.<br><br>Tipo de informe<br>Anual.<br>Teorías<br>Teoría de la agencia, teoría del afianzamiento de la gestión, teorías de la organización-sociedad<br>Muestra<br>50 empresas no financieras que cotizan en la Bolsa de Valores de Johannesburgo.<br>Metodología<br>Análisis de contenido manual recuento de oraciones e índice de divulgación.<br>Cuantitativo. Análisis Univariado<br>análisis de regresión bivariados y multivariados<br>Informe<br>Anual<br>Teorías<br>De agencia, legitimidad, institucional, dependencia de recursos y partes interesadas |
| (Ntim et al., 2013) | Sudafrica | 2002-2011 | Dependiente: Divulgaciones totales de riesgo corporativo, divulgaciones de riesgo financiero corporativo, divulgaciones de riesgo operacional corporativo, divulgaciones de riesgo estratégico corporativo.<br><br>Independiente: Propiedad del bloque, propiedad institucional, diversidad de directorios en función de la etnia y el género, tamaño del tablero, liderazgo de doble Junta, consejeros no ejecutivos independientes.<br><br>Control: Big four, Capx (% gasto de capital / activo), comité de Gobierno Corporativo, bolsa de valores extranjera, comité de responsabilidad social corporativa, riesgo (crecimiento de las ventas), industria, año. | |
| (Elshandidy & Neri, 2015) | Reino Unido – Italia | 2005-2010 | Dependiente: Divulgación voluntaria de riesgos, Divulgación obligatoria de riesgos.<br>Independientes: Tamaño del directorio, directores no ejecutivos, consejeros no ejecutivos independientes, rentabilidad por dividendo, precio actual de la acción, dualidad del CEO, estructura de propiedad, calidad de auditoría<br>Control: Tamaño de la empresa, rentabilidad, liquidez, riesgo de la empresa, estructura de capital, valor contable de mercado, volatilidad del precio de las acciones. | Muestra:<br>290 empresas no financieras de Reino Unido. 88 empresas no financieras de Italia.<br>Metodología<br>Análisis textual automatizado. Conteo de oraciones. Análisis de contenido<br>Tipo de Informe<br>Anual<br>Teoría<br>Agencia |

| | | | | |
|---|---|---|---|---|
| (Al-Hadi et al., 2016) | Países del Consejo de Cooperación del Golfo (CCG) | 2007-2011 | Dependiente: índices MRD (MRD1 y MRD2) en función de los tipos de divulgación (cuantitativa o cualitativa) y el régimen de divulgación (obligatorio o voluntario)<br>Independiente: Comité de riesgos, características del comité de riegos independencia del comité de riesgos, calificación del comité de riesgos, tamaño del comité de riegos, análisis factorial del comité de riesgos.<br>Control: Tamaño de empresa, apalancamiento, rentabilidad, tipo de auditor, análisis factorial de cuatro características del consejo, índice que cubre tres elementos: independencia de la Junta Directiva, dualidad y el director de una empresa con puesto de director externo, familia en el gobierno, industria, país. | Muestra<br>677 observaciones de empresas financieras<br>Metodología<br>Panel, regresiones.<br>Tipo de informe Anual<br>Teoría: teoría de la agencia, la legitimidad, partes interesadas y la teoría basada en los recursos. |
| (Allini et al., 2016) | Italia | 2008 - 2011 | Dependiente: Conteo de palabras y oraciones.<br><br>Independiente: Índice de divulgación, tamaño del directorio, N°. reuniones, independencia del consejo, mujeres en el directorio, educación de los miembros de la Junta, edad media del consejo de administración.<br><br>Control: Porcentaje de propiedad gubernamental, reuniones Comité de Auditoría, edad media de cotización de la empresa, visibilidad en Internet, tamaño de empresa (N° empleados), ROE, apalancamiento. | Muestra<br>17 empresas públicas cotizadas (EPE)<br>Metodología<br>Análisis de contenido, regresión de mínimos cuadrados ordinarios (OLS)<br>correlaciones.<br>Tipo de Informe<br>Informes anuales de Gobierno Corporativo.<br>Teoría<br>Agencia<br>Señalización |
| (Moumen et al., 2016) | La región de Medio Oriente y África del Norte (MENA)<br>9 países | 2007-2009 | Dependiente: Rentabilidad actual de las acciones<br><br>Independiente: Dualidad, composición del consejo, tamaño de la Junta, consejeros no ejecutivos.<br><br>Control: Apalancamiento financiero, tamaño de la empresa, rentabilidad, sector industrial. | Muestra<br>320 empresas no financieras que cotizan en bolsa MENA ,789 observaciones.<br><br>Metodología<br>Análisis de contenido. Conteo manual de oraciones. Método de codificación. Modelo de regresión.<br>Tipo de Informe<br>Anual<br>Teoría<br>Agencia |

| | | | | |
|---|---|---|---|---|
| | | | | Dependencia de los recursos |
| (Agyei-Mensah, 2017) | Ghana | 2011-2013 | Dependiente: Alcance de la divulgación de riesgos corporativos, calidad del índice de divulgación de riesgos corporativos.<br>Independiente: Tamaño del tablero, independencia de la Junta, propiedad institucional, concentración de propiedad en bloque, independencia del Comité de Auditoría.<br>Control: tamaño de la empresa, rentabilidad, liquidez, apalancamiento y tipo de auditor. | Muestra<br>30 empresas que cotizan en la GSE: 90 observaciones de año de empresa<br>Teoría<br>No describe<br>Metodología<br>Regresión.<br>Tipo de informe:<br>Anual |
| (Oliveira et al., 2018) | España – Portugal | 2011 | Dependiente: Número de palabras<br>Independiente: Estructura de propiedad, Numero de directores, independencia en la Junta, diversidad en la Junta, reuniones del consejo, liderazgo de doble directorio, compensación de la gerencia, independencia del Comité de Auditoría, entorno legal, tamaño (activos, ventas y capitalización.), sensibilidad ambiental, solidez del Gobierno Corporativo.<br>Control: Rentabilidad, riesgo de la empresa, calidad de auditor externo. | Muestra<br>60 empresas financieras portuguesas y españolas cotizadas en Euronext Lisboa y la Bolsa de Valores de España<br>Metodología<br>Análisis de contenido. Regresiones lineales múltiples.<br>Tipo de Informe<br>Informes anuales de Gobierno Corporativo.<br>Teoría<br>Agencia<br>Legitimidad, Perspectivas basadas en los recursos<br>Teoría institucional. |

La mayor parte de estos estudios relacionan las divulgaciones de riesgo con las características del Gobierno Corporativo, utilizando un marco teórico basado en la teoría de la agencia (Abraham & Cox, 2007; Allini et al., 2016; Barakat & Hussainey, 2013; Elshandidy & Neri, 2015; Lajili & Zéghal, 2005; Lim et al., 2007; Ntim et al., 2013). Sin embargo, otras investigaciones han optado por marcos multiteóricos basados en la teoría de la agencia. Así, Oliveira et al. (2011) soporta su estudio, además, en la teoría de la legitimidad y la teoría perspectiva basada en los recursos; Barakat & Hussainey (2013) en la teoría del afianzamiento de la gestión y teoría de la organización-sociedad; Ntim et al. (2013) en la teoría de la legitimidad, institucional, dependencia de los recursos y partes interesadas; Moumen et al. (2016) en la teoría de la dependencia de los recursos; y Oliveira et al. (2018) en la legitimidad, perspectivas basadas en los recursos y teoría

institucional. Podemos concluir, por tanto, que, en general, sobre la teoría de la agencia reposa la investigación que relaciona la divulgación de riesgos y las características del Gobierno Corporativo. Según Rhodes (2010), en teoría la divulgación mitiga los conflictos de agencia al disminuir la asimetría de la información entre el principal y el agente, lo que a su vez afecta la valoración de mercado de las empresas. También desde la teoría de la agencia el informe anual se concibe como un mecanismo de control orientado a alinear los intereses de directivos y accionistas.

Por su parte, el análisis de la investigación precedente evidencia que la investigación sobre divulgación de riesgos a partir de los factores de Gobierno Corporativo se desarrolla en su totalidad desde la técnica de análisis de contenido. La literatura previa muestra que este análisis se realiza a partir del conteo de palabras (Abraham & Cox, 2007; Allini et al., 2016; Lajili & Zéghal, 2005); del conteo de oraciones (Allini et al., 2016; Elzahar & Hussainey, 2012; Lajili & Zéghal, 2005; Moumen et al., 2016; Oliveira et al., 2011; Elshandidy & Neri, 2015; Oliveira et al., 2018); y de los índices de divulgación (Elzahar & Hussainey, 2012; Lim et al., 2007; Ntim et al., 2013; Patelli & Prencipe, 2007; Agyei-Mensah, 2017; Al-Hadi, Hasan, et al., 2016; Barakat & Hussainey, 2013; Mokhtar & Mellett, 2013; Taylor et al., 2010). Por su parte, Solomon et al. (2000) utilizan la encuesta para analizar las actitudes de los inversores institucionales sobre divulgación de riesgos en relación con sus decisiones de inversión de cartera.

En general, las investigaciones relacionan la divulgación de información sobre riesgos especialmente con la composición de la Junta Directiva, tomando como variables independientes el tamaño de la Junta, la independencia, los miembros ejecutivos y los comités.

Revisada la literatura previa sobre la incidencia del Gobierno Corporativo en la divulgación de riesgos en general, se presentan los dos únicos estudios que, según nuestra búsqueda, relacionan la divulgación de información sobre riesgos de Ciberseguridad y la composición de la Junta como mecanismo interno del Gobierno Corporativo (Masud & Hossain, 2022; Radu & Smaili, 2021) (Tabla 24).

**Tabla 24. Estudios previos sobre la Divulgación de Riesgos de Ciberseguridad y las características de la Junta**

| Autores | País | Periodo de análisis | Variables | Muestra/Metodología |
|---|---|---|---|---|
| (Radu & Smaili, 2021) | Canadá | 2014-2018 | **Dependiente**<br>Mide la divulgación de Ciberseguridad en el informe anual.<br>**Independiente**<br>Índice de seguridad de la información Diversidad de género en Junta Directiva, porcentaje de mujeres, índice Blau de heterogeneidad, masa crítica de mujeres (1 mujer, 2 mujeres, 3 mujeres).<br>**Control**<br>Tamaño de la empresa, rentabilidad, oportunidades de inversión, apalancamiento, tamaño de la Junta, independencia de la Junta, afiliación de la empresa a la Junta, total de páginas informe anual. | **Muestra**<br>300 observaciones<br>**Metodología**<br>Análisis de contenido. Número de párrafos, número de palabras. Modelo de relevancia de valor de mercado, análisis de diferenciales de oferta y demanda. Modelo de regresión lineal múltiple.<br>**Tipo de informe**<br>Informe anual<br>**Teoría**<br>La teoría de las partes interesadas.<br>La teoría de la dependencia de los recursos.<br>La teoría de la masa crítica. |
| (Masud & Hossain, 2022) | Bangladesh | 2014-2020 | **Dependiente:** CSD (divulgación de seguridad cibernética)<br>**Independiente:** tamaño de la junta, la independencia de la Junta y la diversidad de género de la Junta.<br>**Control:** tamaño del banco, el apalancamiento, la oportunidad de crecimiento, la rentabilidad, propiedad accionaria institucional, propiedad accionaria extranjera, ISLAM ( Variable ficticia para denotar sistema islámico-Shariah ó sistema bancario convencional) | **Muestra:** 30 bancos comerciales que cotizan en DSE durante el período de muestra (10 observaciones de años bancarios)<br>**Metodologia:** modelo de regresión lineal múltiple<br>**Tipo de informe:** Informe Anual<br>**Teoria:** Teoría de la agencia y la teoría basada en los recursos |

Mientras que sobre Gobierno Corporativo como factor de divulgación de riesgos hay una literatura previa importante, los estudios que centran su atención en la divulgación de riesgos sobre Ciberseguridad son bastante limitados y, concretamente, solo dos presentan objetivos similares (Masud & Hossain, 2022; Radu & Smaili, 2021). Desde estos antecedentes se justifica el presente estudio empírico, que busca evaluar las prácticas de presentación de reportes de riesgo de Ciberseguridad en empresas cotizadas Latinoamericanas y cómo las características de Gobierno Corporativo, específicamente la composición de la Junta Directiva, incide en la divulgación de información relacionada.

Y ello porque, coincidimos con Pucheta-Martínez & Gallego-Álvarez (2019) en que la composición de la Junta, en particular ciertas características, pueden ser un mecanismo de Gobierno Corporativo relevante que impulse a las empresas a interactuar con los accionistas y todas las partes interesadas en términos de mejorar la transparencia informativa.

### 4.3.3. Hipótesis de Estudio

Con base en la evidencia existente en la literatura sobre divulgación de riesgos y la relación con las características del Gobierno Corporativo, nuestro estudio, desde la perspectiva de la teoría de la agencia (Jensen & Meckling, 1976), evalúa el alcance de la divulgación obligatoria y voluntaria de información sobre Ciberseguridad. Según Masud & Hossain (2022), la Junta Directiva es el aparato de control clave de las acciones gerenciales y la responsabilidad corporativa, y una composición efectiva de la misma minimiza la asimetría de información entre la gerencia y los inversionistas al proporcionar divulgaciones adecuadas y relevantes.

**Tamaño de la Junta.**

Según la teoría de la agencia, la Junta Directiva es un mecanismo de control capaz de reducir la asimetría de la información y alinear los intereses de propiedad y gestión (Jensen & Meckling, 1976). Tanto teórica como empíricamente, existe un amplio debate sobre los efectos del tamaño de la Junta y la divulgación de información como una extensión del proceso de supervisión (Frias-Aceituno et al., 2014). Estudios previos relacionan la divulgación de riesgos con el tamaño de la Junta (Allini et al., 2016 ; Elshandidy & Neri, 2015; Elzahar & Hussainey, 2012; Lajili & Zéghal, 2005; Moumen et al., 2016; Ntim et al., 2013; Oliveira et al., 2018; Patelli & Prencipe, 2007). La literatura anterior permite apreciar resultados mixtos entre el número de consejeros de la Junta y el alcance de la divulgación de información de riesgos. Así, algunos encuentran una relación positiva entre el mayor tamaño de la Junta (Allini et al., 2016; Allegrini & Greco, 2013; Elshandidy & Neri, 2015; Ntim et al., 2013; Oliveira et al., 2011), mientras otros estudios

obtienen como resultado una relación negativa (Allini et al., 2014; Moumen et al., 2016). En el caso de estudios previos relacionados con la divulgación de riesgos de Ciberseguridad (Mazumder & Hossain, 2022; Radu & Smaili, 2021) no se encuentra una relación significativa entre el tamaño de la Junta y la divulgación de información sobre Ciberseguridad. Bajo este panorama, en nuestro estudio esperamos que las juntas directivas de menor tamaño comuniquen de manera efectiva la divulgación de Ciberseguridad. La variable de referencia para expresar el tamaño de la Junta corresponde al número de miembros que la conforman. En concordancia, consideramos la siguiente hipótesis:

*H1. Existe una relación significativa y negativa entre el tamaño de la Junta y el alcance de la divulgación de Ciberseguridad de las empresas cotizantes de América Latina.*

**Diversidad de género de la Junta.**

La diversidad del directorio se puede definir como la variedad en la composición de la Junta Directiva (Adams et al., 2015). La diversidad de género de la Junta es un tema central de los esfuerzos de reforma de la gobernanza en todo el mundo (Adams & Ferreira, 2009). La composición de género en la Junta es una dimensión importante del Gobierno Corporativo, porque las mujeres y los hombres son tradicional, cultural y socialmente diferentes (Liao et al., 2015). Las mujeres en los consejos de administración pueden afectar la Ciberseguridad a través de diferentes canales y de múltiples maneras, entre las que se pueden destacar, el conocimiento específico y general, la supervisión y gobernanza de riesgos, la independencia, la sensibilidad ética, la sensibilidad de las partes interesadas, el estilo de liderazgo o el efecto en la dinámica del grupo (Radu & Smaili, 2021). La evidencia sugiere la contribución de la mujer a un Gobierno Corporativo más efectivo (Adams & Ferreira, 2009; Adams et al., 2015; Arayssi et al., 2016; Brieger et al., 2019; Jizi, 2017; Nielsen & Huse, 2010; Radu & Smaili, 2021b; Terjesen et al., 2016a). Además, estudios recientes evidencian cómo se obtienen divulgaciones de riesgo más completas y un mayor valor de la empresa a partir de una mayor diversidad de género en la Junta (Allini et al., 2016, Adams & Ferreira, 2009; Ntim et al., 2013).

Masud & Hossain (2022) y Radu & Smaili (2021) encuentran una asociación positiva entre la divulgación de seguridad cibernética y la diversidad de género. Las mujeres en la Junta también se perciben en general como más responsables socialmente y es probable que tengan valores éticos más elevados (Jaggi et al., 2020). La participación de las mujeres en temas cibernéticos agrega diferentes perspectivas y estilos de liderazgo, cambia las tareas de la Junta, aporta sensibilidad ética y orientada a las partes interesadas (por qué hacerlo) y conocimiento específico y general (cómo hacerlo), y mejora el rol de supervisión (qué hacer) lo que tiene como resultado impactos positivos en la divulgación relacionada con la Ciberseguridad (Radu & Smaili 2021).

A partir de estos antecedentes, suponemos que un mayor número de mujeres en la Junta aumentará la divulgación sobre Ciberseguridad. La variable de referencia para expresar la diversidad de género de la Junta corresponde al porcentaje de mujeres que conforman la Junta. En concordancia, consideramos la siguiente hipótesis:

*H2. Existe una relación significativa y positiva entre la proporción de mujeres en la Junta y el alcance de la divulgación de Ciberseguridad de las empresas cotizantes de América Latina.*

**Independencia de los miembros de la Junta**.

Fama (1980) afirma que el consejo de administración es el mecanismo central de monitoreo y control para supervisar a los gerentes. Desde la investigación de Berle & Means (1932), se ha marcado la designación de directores independientes en los directorios de empresas con estructuras de propiedad difusa. La independencia del consejo se define como el porcentaje de directores no ejecutivos (totalmente independientes) en la Junta (Cai et al., 2006) desprovistos de vínculos de especial interés (Afep Medef, 2015). En línea con Kiliç et al. (2015), los miembros independientes equilibran los intereses de los de dentro y los de fuera, y también supervisan las actividades de los administradores en nombre de los inversores. Con respecto a la

divulgación de información sobre riesgos, las juntas con más consejeros independientes son un mecanismo interno de Gobierno Corporativo para promover los intereses de los accionistas (Allini et al., 2014). Un alto número de directores no ejecutivos proporciona seguridad a los inversores sobre las narrativas del informe anual, y se cree que son más influyentes en términos de la toma de las decisiones de la Junta y, particularmente, en la mejora de la calidad de la divulgación voluntaria corporativa (Moumen et al., 2016). De acuerdo con Rao et al. (2012), la independencia es uno de los principales factores que inciden positivamente en la rendición de cuentas de las entidades, resultando en un aumento en el nivel de divulgación.

Los hallazgos de estudios previos sobre la presencia de consejeros independientes y la divulgación de información son divergentes. Así, mientras que algunos encuentran una relación positiva (Abraham & Cox, 2007b; Moumen et al., 2016; Ntim et al., 2013; Patelli & Prencipe, 2007), otros la hallan negativa. (Allini et al., 2016). Por lo que respecta a los estudios sobre divulgación de información de Ciberseguridad (Masud & Hossain, 2022; Radu & Smaili, 2021), ambos confirman una relación positiva y significativa entre la independencia de la Junta y la divulgación de información sobre Ciberseguridad. En concordancia con la literatura previa, planteamos la siguiente hipótesis:

*H3. Existe una relación significativa y positiva entre la proporción de consejeros independientes en la Junta y el alcance de la divulgación de Ciberseguridad de las empresas cotizantes de América Latina.*

**Comité de Auditoría u otro comité encargado de la supervisión del riesgo de Ciberseguridad.**

El Comité de Auditoría es una pieza angular en la gestión de áreas tan críticas como la supervisión del riesgo, la interacción con los auditores externos, la salvaguarda de los controles internos y la vigilancia de la información financiera (Deloitte, 2012). Frente al riesgo de Ciberseguridad, al igual que con otros temas de auditoría y riesgo, dicha

supervisión lógicamente podría ser asignada por la Junta a su Comité de Auditoría (Fontaine & Reed 2018).

El grado de participación del Comité de Auditoría en los problemas de Ciberseguridad varía significativamente según la empresa e industria (Deloitte, 2016). Es habitual que este comité sea generalmente responsable de la estrategia de Ciberseguridad (Héroux & Fortin, 2020a). Poco más de la mitad de las juntas le asignan la mayoría de las responsabilidades de supervisión de riesgos relacionados con la Ciberseguridad al Comité de Auditoría, que ya suele estar sobrecargado y que también asume una responsabilidad importante en la supervisión de la información financiera y los riesgos de cumplimiento (OEA; ISA, 2020). Según E&Y (2018, 2019 y 2020) las empresas de Fortune 100 divulgan en un porcentaje de 59%, 62% y 67% respectivamente, que el Comité de Auditoría es quien supervisa los asuntos de seguridad cibernética, lo que significa que el manejo de riesgo cibernético ha sido designado al Comité de Auditoría de forma progresiva. Bajo estas consideraciones, planteamos la siguiente hipótesis:

*H4. La participación del Comité de Auditoría u otro comité en la supervisión del riesgo de Ciberseguridad afectará de forma significativa y negativa el alcance de la divulgación de Ciberseguridad de las empresas cotizantes de América Latina.*

**Comité de Ciberseguridad delegado para la supervisión del riesgo de Ciberseguridad**

Tomando como referente los resultados de la encuesta E&Y (2018, 2019 y 2020) sobre la asignación de la supervisión del riesgo cibernético a un comité diferente en la Junta al Comité de Auditoría, las empresas Fortune 100 divulgan 20%, 28% y 26%, respectivamente. De esta forma podemos observar que la delegación del riesgo cibernético a un comité diferente al de auditoría, plantea la iniciativa de la designación de un comité que de forma exclusiva controle los riesgos de Ciberseguridad. Este comité de riesgos de Ciberseguridad de la Junta, puede supervisar la amplia gama de problemas

relacionados con la cibernética que enfrentan las empresas públicas, que incluyen, entre otros, seguros cibernéticos, planes de respuesta a incidentes, planes de continuidad del negocio, amenazas internas y los llamados malos abandonos (aquellos que dejan una empresa y presentan una amenaza, por ejemplo, causando estragos en los sistemas tecnológicos), debida diligencia de Ciberseguridad de terceros, prevención y respuesta al ransomware, contratación de personal de TI, formación en Ciberseguridad o presupuesto de seguridad de datos.. En el desarrollo de estas funciones, y a partir de la experticia y conocimientos específicos del comité en Ciberseguridad, se espera éste aborde mejor estos riesgos y amenazas y, en consecuencia, aumente el alcance de las revelaciones y la información que se comparte por parte de estas empresas a los diferentes grupos. Bajo estas consideraciones, planteamos la siguiente hipótesis:

*H5. La participación del Comité de Ciberseguridad en la supervisión del riesgo de Ciberseguridad afectará de forma significativa y positiva el alcance de la divulgación de Ciberseguridad de las empresas cotizantes de América Latina.*

## 4.4. Metodología

### 4.4.1. Población y Muestra

La población corresponde a las empresas listadas en los principales índices bursátiles de los países latinoamericanos de mayor capitalización de la región: Argentina, Brasil, Chile, Colombia, México y Perú de cuatro sectores económicos distintos: energía, financiero, consumo discrecional y materiales. La muestra final arrojó un total de 85 empresas y 425 observaciones en el período 2016-2020. La recopilación de la información, se lleva a cabo a partir del análisis de contenido de los informes anuales publicados en los sitios web de las empresas y del informe 20 F en el caso de las empresas emisoras reguladas por SEC.

### 4.4.2. Variables

#### Variable dependiente

Esta variable se obtiene a través de la aplicación del Índice de Divulgación de Información sobre Ciberseguridad que se ha diseñado en el capítulo anterior. Nuestra variable dependiente mide el alcance de la divulgación de Ciberseguridad en los informes anuales y en los reportes presentados en el Formulario 20 F de las empresas latinoamericanas, como emisoras privadas extranjeras con acciones cotizadas en las Bolsas de los Estados Unidos. El informe anual es un método bien establecido para transferir información del directorio a los accionistas y partes interesadas (Eijkelenboom & Nieuwesteeg, 2021a). Además constituye una fuente importante y confiable de información relacionada con el riesgo (Allini et al., 2016).

#### Variables independientes

El tamaño de la Junta se mide por el número total de miembros (Allini et al., 2016; Allegrini & Greco, 2013; Elshandidy & Neri, 2015; Ntim et al., 2013; Oliveira et al., 2011). La diversidad de género se mide por el porcentaje de mujeres en la Junta (Radu & Smaili, 2021b). La independencia de la Junta es medida a través del porcentaje de consejeros independientes determinada por su proporción de externos, es decir, por la proporción de miembros independientes (Abraham & Cox, 2007b; Moumen et al., 2016; Ntim et al., 2013; Patelli & Prencipe, 2007). La participación del Comité de Auditoría en la supervisión del riesgo de Ciberseguridad es una variable binaria, que toma el valor 1 si participa, y 0 en caso contrario. Por lo que respecta a la participación del Comité de Ciberseguridad en la supervisión del riesgo de Ciberseguridad, también es una variable binaria que toma el valor 1 si participa, y 0 en caso contrario.

**Variables de control**

Para la definición de las variables a controlar hemos tenido en cuenta las características de la empresa que, de acuerdo con investigaciones previas, se entiende que se asocian con el alcance de la divulgación corporativa de riesgos. Concretamente, se ha considerado el tamaño de la empresa, su rentabilidad, el apalancamiento financiero, los intangibles y la edad de la empresa.

Tamaño de la Empresa**.** Controlamos el tamaño de la empresa con respecto a la divulgación de riesgos con base en Abraham & Cox, (2007a), Allini et al., (2016), Elshandidy & Neri, (2015), Linsley & Shrives, (2006), Lim et al., (2007), Moumen et al., (2016), Oliveira et al., (2011) y Patelli & Prencipe (2007). Y específicamente riesgos de Ciberseguridad (Masud & Hossain, 2022; Radu & Smaili, 2021). El tamaño de la empresa se mide como el logaritmo del total de los activos.

ROA. Las empresas con mayor rentabilidad tienen más recursos para destinar a la gestión de riesgos y divulgar información sobre Ciberseguridad (Radu & Smaili, 2021). Se controla la rentabilidad respecto a la divulgación de información sobre riesgos en investigaciones previas (Elshandidy & Neri, 2015; Moumen et al., 2016; Oliveira et al., 2018). En particular riesgos de Ciberseguridad (Masud & Hossain, 2022; Radu & Smaili, 2021). Se mide como la relación entre los Beneficios Netos Recibidos y los activos totales.

Apalancamiento. Las organizaciones con mayor deuda reportan más información sobre riesgos (Allini et al., 2016), siendo probable que las empresas con mayor deuda traten de desviar la atención de las partes interesadas hacia el riesgo cibernético (Linsley & Shrives, 2006; Oliveira et al., 2018).

Intangibles**.** Una mayor proporción de activos intangibles puede sugerir una mayor inversión en software para combatir los riesgos cibernéticos, lo que puede disminuir los riesgos de Ciberseguridad. Una mayor proporción de los activos intangibles se asocia

negativamente con la cantidad de palabras utilizadas para revelar los riesgos de Ciberseguridad (Gao et al., 2020).

**Tabla 25. Resumen de las medidas utilizadas para las variables**

| | |
|---|---|
| **Variable dependiente** | |
| Divulgación de Ciberseguridad | Alcance de la divulgación medida obtenida a partir de la aplicación del Índice de Divulgación de Información sobre Ciberseguridad |
| **Variables independientes** | |
| Tamaño de la Junta | Tamaño de la Junta Directiva o consejo de administración |
| Diversidad | Porcentaje de mujeres en la Junta Directiva |
| Independencia | Porcentaje de miembros independientes en la Junta Directiva |
| Comité de auditoría | Variable binaria, 1 si el Comité de Auditoría supervisa riesgo Ciberseguridad<br>0 si lo supervisa otro comité dentro de la Junta. |
| Comité de Ciberseguridad | Variable binaria, 1 si existe un Comité de Ciberseguridad exclusivo para supervisar riesgo Ciberseguridad<br>0 si lo supervisa otro comité dentro de la Junta |
| Tamaño | Medido por el logaritmo natural de los activos totales |
| ROA | Rentabilidad de la empresa (medido por el valor de ingresos totales entre el valor de activos totales). |
| Apalancamiento | Porcentaje de la deuda total sobre el patrimonio total. |
| Intangibles | Medido por el valor total de activos intangibles entre el valor total de activos. |

### 4.4.3. Modelo

Se estimó un modelo Data Panel por efectos fijos en concordancia con (Mazumder & Hossain, 2022; Radu & Smaili, 2021), estudios que persiguen evaluar algunos factores de Gobierno Corporativo en la divulgación de información sobre Ciberseguridad. En nuestro caso, a partir del modelo de regresión lineal controlamos los efectos fijos de cada empresa. El presente estudio, se aplica a partir del análisis de contenido de los informes

anuales y demás comunicaciones reportadas por las compañías cotizadas de Argentina, Brasil, Chile, Colombia, México y Perú para el intervalo de tiempo 2016-2020.

De esta forma, se obtiene la ecuación:

**Ecuación 1**

***Modelo corregido data panel por efectos fijos***

$$CyberDiscl_{it} = \beta_0 + \beta_1 Tamaño_junta_{it} + \beta_2 Diversidad_{it} + \beta_3 Independencia_{it} + \beta_4\, Comité_Auditoria_{it} + \beta_5 Comité_Ciberseguridad + \beta_6 Tamaño_{it} + \beta_7 Intangibles_{it} + \beta_8\, Apalancamiento_{it} + \beta_9 ROA_{it} V_i + \varepsilon_{it}$$

## 4.5. Resultados y Discusión

La Tabla 26 informa las estadísticas descriptivas de todas las variables independientes y de control utilizadas en este estudio, lo que nos permite caracterizar a la muestra objeto de estudio. Respecto al tamaño de la Junta, el número de directores en la organización, por término medio cada directorio consta, aproximadamente, de 10 directores, observándose un mínimo de 5 directores y un máximo de 20 en las distintas empresas objeto de análisis. En promedio, el 42% del total de los miembros del directorio se clasifican como directores independientes. El porcentaje medio de mujeres en el directorio es del 11%, lo que indica que, en promedio, un miembro de cada diez pertenece al género femenino. Esto no es sorprendente, ya que existe una preocupación expresada en estudios anteriores sobre la desigualdad de género en el mundo empresarial en el contexto de los países desarrollados y en desarrollo. El valor medio del tamaño de las empresas de la muestra es 9,18. Por lo que respecta a la rentabilidad por término medio se sitúa en el 4,19%. El valor medio del apalancamiento, que mide el porcentaje de deuda sobre los activos totales, es de 133,36 y el porcentaje promedio de los activos intangibles se cifra en 0.06. Por lo que respecta a los Comités, el 82% de las empresas cuentan con un Comité de Auditoria de los cuales el 70% asumiría la supervisión del riesgo de

ciberseguridad, mientras que solo el 12% de las compañías delegan exclusivamente esta función dentro de la junta al Comité de Ciberseguridad.

**Tabla 26. Estadísticas descriptivas**

| Variable | Obs | Mean | Std.Dev. | Mín | Máx |
|---|---|---|---|---|---|
| Tamaño de la junta | 425 | 9,55 | 2,73 | 5,00 | 20,00 |
| Diversidad (mujeres) | 425 | 0,11 | 0,12 | 0,00 | 0,67 |
| Independencia | 425 | 0,42 | 0,21 | 0,07 | 1,00 |
| Comité Auditoria | 425 | 0,70 | 0,45 | 0,00 | 1,00 |
| Comité Ciberseguridad | 425 | 0,12 | 0,32 | 0,00 | 1,00 |
| Tamaño Compañía | 425 | 9,18 | 1,61 | 4,13 | 12,98 |
| ROA | 425 | 4,19 | 4.49 | -11,49 | 26,7 |
| Intangibles | 425 | 0,06 | 0,09 | 0,00 | 0,50 |
| Apalancamiento | 425 | 133,36 | 315,09 | 0,00 | 6135,80 |

La Tabla 27 presenta los coeficientes de correlación entre las variables del modelo. En general, según la matriz de correlación podemos colegir que no existe una asociación marcada entre las variables sobre la significancia de la asociación entre las variables objeto de estudio.

## Tabla 27. Matriz de Correlaciones

| | Índice | Tamaño de la junta | Diversidad (mujeres) | Independencia | Comité de Auditoría | Comité de Ciberseguridad | Tamaño Compañía | ROA | Intangibles | Apalancamiento |
|---|---|---|---|---|---|---|---|---|---|---|
| Índice | **1,0000** | | | | | | | | | |
| Tamaño de la junta | 0,0941 | **1,0000** | | | | | | | | |
| Diversidad (mujeres) | -0,0250 | -0,1045 | **1,0000** | | | | | | | |
| Independencia | 0,0817 | -0,0623 | 0,0934 | **1,0000** | | | | | | |
| Comité de Auditoría | -0,0499 | 0,0702 | 0,0547 | 0,1926 | **1,0000** | | | | | |
| Comité de Ciberseguridad | 0,2492 | 0,1908 | 0,0200 | 0,1409 | -0,5657 | **1,0000** | | | | |
| Tamaño Compañía | 0,4260 | 0,0634 | 0,0454 | -0,1170 | -0,0811 | 0,1174 | **1,0000** | | | |
| ROA | -0.2069 | 0,0740 | -0,0484 | 0,0871 | 0,0861 | -0,0326 | -0,4132 | **1,0000** | | |
| Intangibles | -0.1279 | 0,0450 | -0,0025 | 0,1209 | 0,0525 | 0,0888 | -0,3290 | 0.2850 | **1,0000** | |
| Apalancamiento | 0,0379 | 0,0741 | -0,0230 | -0,0035 | 0,0286 | -0,0326 | 0,0712 | -0,2021 | -0,0825 | **1,0000** |

La Tabla 28 muestra la Prueba de Factor de Inflación de la Varianza VIF, los resultados no se ven afectados por multicolinealidad ya que los factores de inflación de la varianza (VIF) estan dentro del umbral de 10, hallazgos que coinciden con Baldini et al. (2018).

**Tabla 28. Factor de Inflación de la Varianza VIF**

| Variable | VIF | 1/VIF |
|---|---|---|
| Tamaño de la junta | 1.17 | 0.857468 |
| Diversidad (mujeres) | 1.03 | 0.969095 |
| Independencia | 1.21 | 0.823783 |
| Comité de Auditoría | 1.81 | 0.551057 |
| Comité de Ciberseguridad | 1.89 | 0.529382 |
| Tamaño de la Compañía | 1.33 | 0.749295 |
| Intangibles | 1.20 | 0.836693 |
| Apalancamiento | 1.06 | 0.945297 |
| ROA | 1.31 | 0.763322 |
| **Mean VIF** | **1.33** | |

A continuación, se presentan los resultados del modelo estimado identificando las variables de Gobierno Corporativo que inciden en el Índice de Ciberseguridad:

**Tabla 29. Resultados del análisis de regresión**

| Variable | Coeficiente (Error Estándar) |
|---|---|
| Tamaño de la junta | -0.01801* |
| | (0.00892) |
| Diversidad (mujeres) | 0.18481 |
| | (0.11656) |
| Independencia | 0.35460*** |
| | (0.73489) |
| Comité de Auditoría | -0.03625 |
| | (0.48888) |
| Comité de Ciberseguridad | 0.09861* |
| | (0.05405) |
| Tamaño de la compañía | 0.67003** |
| | (0.02460) |
| Intangibles | 0.04438 |
| | (0.21042) |
| Apalancamiento | 0.00001 |
| | 0.00002 |
| ROA | -0.00132 |
| | (0.00259) |

Nota. Los errores estándar corregidos se presentan entre paréntesis

Niveles de significación *Significancia al 10%, ** Significancia al 5%, *** Significancia al 1%,

El modelo de regresión múltiple es significativo (P>0,000). El coeficiente ajustado de determinación $R^2$ presenta un valor de 75, 72%. Los hallazgos de este estudio muestran cómo la variable tamaño de la Junta Directiva presenta una relación significativa y negativa frente a la divulgación sobre Ciberseguridad, lo cual sugiere que las juntas más pequeñas presentan un mayor alcance en la divulgación de información sobre Ciberseguridad. Esto se interpreta al argumentar que un mayor número de integrantes en la Junta puede generar una mayor dispersión en la toma decisiones frente a temas emergentes como la Ciberseguridad. Estos resultados son consistentes con la relación negativa obtenida por Campbell et al. (2014). En este sentido, cabe destacar que investigaciones precedentes Eisenberg et al. (1998), Jensen (1993), Lipton & Lorsch (1992), Sánchez et al. (2011) y Yermack (1996) evidenciaron que la presencia de un mayor número de miembros de la Junta genera un aumento en los problemas de agencia y procesos de monitoreo menos óptimos, circunstancia que podría conducir a una menor predisposición a revelar información sobre las actividades corporativas, por la falta de un mecanismo de control adecuado (Sánchez et al., 2011).

El reporte de la regresión arroja una fuerte asociación positiva entre el número de miembros independientes en la Junta y la divulgación de información sobre Ciberseguridad, situación que puede tener su explicación en el hecho de que los miembros independientes son los encargados de indagar y gestionar la divulgación sobre Ciberseguridad, al buscar proteger a sus accionistas y demás partes interesadas. Estos resultados están en línea con la literatura previa, que también encontró una relación positiva entre la independencia de la Junta y la divulgación de riesgos en general (Abraham & Cox, 2007b; Moumen et al.2016; Ntim et al. 2013; Patelli & Prencipe, 2007), así como con la divulgación sobre riesgos de Ciberseguridad, en particular (Masud & Hossain, 2022).

Por lo que respecta a la variable de diversidad de género, y contrario a los resultados esperados con base en estudios previos sobre la divulgación de riesgos (Allini et al., 2016; Ntim et al., 2013) y de Ciberseguridad (Masud & Hossain, 2022; Radu & Smaili, 2021), nuestro modelo presenta una asociación no significativa respecto a la incidencia de las mujeres en la divulgación de información sobre Ciberseguridad. Una de las posibles razones de este resultado puede ser la baja representatividad del género femenino en los directorios corporativos, ya que según Deloitte (2017), tan solo el 2,1% de los cargos de la Junta Directiva están ocupados por mujeres en las empresas de América Latina.

La variable Comité de Auditoría muestra que delegar la supervisión de los riesgos de seguridad cibernética a este comité dentro de la Junta no afecta de forma significativa la divulgación de información sobre Ciberseguridad. Esto se explica porque los integrantes del Comité de Auditoría no centran su atención en el riesgo cibernético emergente de forma exclusiva. Según KPMG (2018), puede que el Comité de Auditoría no dedique tiempo suficiente a la seguridad cibernética y, de acuerdo con (OEA; ISA, 2020), el Comité de Auditoría ya suele estar sobrecargado pues también asume una responsabilidad importante en la supervisión de la información financiera y los riesgos de cumplimiento. Además, la falta de experiencia en tecnología puede ser un problema por reconocer en los directorios de hoy (Deloitte, 2016) y, probablemente, sea una circunstancia que se replique en el Comité de Auditoría.

En relación a la variable Comité de Ciberseguridad, hemos hallado una asociación significativa y positiva. Esto significa que el hecho de que la delegación de la supervisión del riesgo cibernético este a cargo de este comité en particular, aumenta la divulgación de información sobre Ciberseguridad. Esta correlación se argumenta porque el Comité de

Ciberseguridad, contará con profesionales expertos en el área, con una dedicación exclusiva en el manejo del riesgo quienes fomentaran las revelaciones relacionadas con la seguridad cibernética. Es de anotar que tan solo el 12% de las empresas cuenta con este comité.

En cuanto a las variables de control, el tamaño de la empresa se considera un factor significativo en las divulgaciones de riesgo según la literatura previa. Si bien no preexisten resultados concluyentes, algunos hallan resultados positivos (Abraham & Cox, 2007; Linsley & Shrives, 2006), otros no encuentran correspondencia (Beretta & Bozzolan, 2004) y Campbell et al.(2014) obtiene una relación inversa. Según Radu & Smaili (2021) se supone que las grandes empresas que cotizan en bolsa tienen más probabilidades de divulgar información relacionada con la Ciberseguridad. Se espera que las compañías más grandes tengan más presión de las partes interesadas para la divulgación y pueden asumir los costos adicionales de estas revelaciones. En línea con este argumento, nuestros resultados muestran que el tamaño de la empresa es un aspecto significativo y positivo frente al alcance de las revelaciones dedicadas a Ciberseguridad. Contrario a los resultados obtenidos por Radu & Smaili (2021), la rentabilidad en nuestro estudio es una variable inversa y sin una asociación significativa con la divulgación de información sobre Ciberseguridad. Según nuestros resultados, el apalancamiento y la proporción de activos intangibles no afecta a las revelaciones sobre Ciberseguridad.

Con base en los resultados obtenidos, podemos indicar que se aceptan las hipótesis H1, H3 y H5, mientras que H2 no se confirma. H4 obtiene el signo negativo propuesto y no logra una asociación significativa.

## 4.6. Conclusiones

El Gobierno Corporativo es un tema muy amplio, por lo que delimitar un único marco histórico se entiende poco viable. El recuento de acontecimientos expuesto en la primera parte del capítulo sobre el origen y desarrollo del concepto enfatiza la relación entre la organización y la sociedad, razón por la cual se han ido incorporando nuevos elementos que han ampliado su perspectiva y cobertura en aras a superar los problemas generados por la crisis de confianza e incorporar conceptos que van más allá de la protección del

accionista individual e institucional, como el manejo y vigilancia de nuevos riesgos corporativos de alta probabilidad e impacto. En consecuencia, independientemente del modelo, desde la gobernanza corporativa se entregan mayores responsabilidades a la Junta Directiva entorno a la supervisión como mecanismo de control.

En este contexto, dada la importancia del Gobierno Corporativo desde las dimensiones económicas, ambientales y sociales, los organismos internacionales y nacionales han participado en la generación de conceptos y estándares emanados desde los diferentes modelos, entre otros, angloamericano, alemán o japonés. En general, son estas diferencias institucionales del ámbito nacional las que impiden la creación de un único código internacional, capaz de contemplar recomendaciones lo bastante generales para englobar las distintas políticas de Gobierno Corporativo en las diferentes culturas.

A la par con el desarrollo del concepto de Gobierno Corporativo se ha generado un marco teórico capaz de dar explicación a los diferentes fenómenos que rodean el tema. Por una parte, desde las teorías económicas más estudiadas se presentan la teoría de la agencia (Jensen & Meckling, 1976) y la teoría de la dependencia de los recursos (Pfeffer, Jeffrey; Salancik, 1978). Desde las teorías sociopolíticas encontramos la teoría institucional (Dimaggio, 1982), la teoría de la señalización (Spence, 1973), la teoría de las partes interesadas (Freeman, 1984) y la teoría de la legitimidad (Deegan, 2000). Dado el objetivo del presente estudio, hemos retomado algunos mecanismos de control relacionados con la estructura de la Junta Directiva como factor determinante de la divulgación de información. Específicamente, hemos considerado el tamaño de la Junta, la independencia de sus miembros, la diversidad de género, el Comité de Auditoría y el Comité de Ciberseguridad.

Por su parte, el Gobierno Corporativo en América Latina se ha implementado a través de las recomendaciones del Banco Mundial y la OCDE. A partir de 2000 se han llevado a cabo reuniones anuales en la denominada Mesa Redonda Latinoamericana, como estrategia de dialogo entre los agentes del mercado de los países miembros. La región toma los Principios de Gobierno Corporativo de la OCDE, como un marco de trabajo de aplicación voluntaria y un referente importante en la emisión de distintos códigos y normativas. Es importante resaltar el papel de las bolsas de valores en la contribución de la adopción de buenas prácticas, a partir del marco regulatorio que han impuesto, así como las recomendaciones de "cumplir o explicar" para las empresas cotizadas.

En Latinoamérica el problema de la agencia se traslada a los inversionistas mayoritarios, quienes se supone se benefician de los minoritarios. El Gobierno Corporativo puede constituir una herramienta para alinear estos intereses. En lo relacionado con las prácticas de Gobierno Corporativo, según la revisión de códigos y la normativa de los países objeto de estudio, los seis países considerados contemplan la implementación de una visión estratégica por parte del consejo de administración, la creación de un Comité de Auditoría y la supervisión de la gestión de riesgos y los sistemas de control interno. Respecto a la inclusión de temas como el involucramiento de consejeros independientes, Chile es el único país que no lo considera. En cuanto a temas como la responsabilidad social, tan solo México y Perú no lo observan. Y, finalmente, respecto a las TI, se trata de un tema que se vincula en los códigos de Colombia y México.

En cuanto a los resultados de nuestro estudio empírico, encontramos cómo la estructura del Gobierno Corporativo es un factor determinante en la divulgación de información relacionada con los riesgos de Ciberseguridad en América Latina. Respecto a la estructura de los consejos de administración, las empresas con juntas directivas más pequeñas o con menos miembros presentan un mayor alcance en sus revelaciones sobre Ciberseguridad. La participación de un mayor número de miembros independientes en los consejos de administración también se relaciona de forma significativa con la divulgación. Contrario a los resultados esperados en estudios previos, la participación de las mujeres en la divulgación sobre Ciberseguridad presenta una asociación no significativa, situación que puede obedecer a la baja participación femenina en las juntas corporativas en América Latina. Sobre la delegación de los riesgos de Ciberseguridad al Comité de Auditoría, afecta de forma importante y negativa en la divulgación de Ciberseguridad. Sin embargo, la delegación de los riesgos cibernéticos de forma exclusiva al Comité de Ciberseguridad presenta una fuerte asociación con el alcance de las revelaciones de seguridad cibernética.

## 4.7. Referencias

Abbate, J. (2011). Inventing the internet. En *Networks of Innovation*. https://doi.org/10.1093/acprof:oso/9780199269051.003.0003

Abraham, S., & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248.

https://doi.org/10.1016/J.BAR.2007.06.002

Abraham, S., & Shrives, P. J. (2014). Improving the relevance of risk factor disclosure in corporate annual reports. *British Accounting Review*, *46*(1), 91–107. https://doi.org/10.1016/j.bar.2013.10.002

Abraham, S. the determinants of narrative risk information in U. F. 100 annual reports, & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/J.BAR.2007.06.002

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Adams, R. B., & Ferreira, D. (2007). A Theory of Friendly Boards. *The Journal of Finance*, *62*(1), 217–250. https://doi.org/10.1111/J.1540-6261.2007.01206.X

Adams, R. B., & Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. *Journal of Financial Economics*, *94*(2), 291–309. https://doi.org/10.1016/j.jfineco.2008.10.007

Adams, R. B., & Funk, P. (2012). Beyond the glass ceiling: Does gender matter? *Management Science*, *58*(2), 219–235. https://doi.org/10.1287/mnsc.1110.1452

Afep Medef. (2015). *Code de gouvernement entreprise revise*.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/CYBSEC/TYY006

Agrawal, A., & Chadha, S. (2005). Corporate governance and accounting scandals. *Journal of Law and Economics*, *48*(2), 371–406. https://doi.org/10.1086/430808/ASSET/IMAGES/LARGE/FG1.JPEG

Agrawal, A., & Knoeber, C. R. (2001). Do some outside directors play a political role? *Journal of Law and Economics*, *44*(1), 179–198. https://doi.org/10.1086/320271

Agrawal, A., & Knoeber, C. R. (2015). Do Some Outside Directors Play a Political Role?*. *https://doi.org/10.1086/320271*, *44*(1), 179–198. https://doi.org/10.1086/320271

Aguilar Antonio, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, *25*.

Agyei-Mensah, B. K. (2017). The relationship between corporate governance mechanisms and IFRS 7 compliance: evidence from an emerging market. *Corporate Governance (Bingley)*, *17*(3), 446–465. https://doi.org/10.1108/CG-06-2016-0129/FULL/PDF

Ahmed, K., Hossain, M., & Adams, M. B. (2006). The Effects of Board Composition and Board Size on the Informativeness of Annual Accounting Earnings. *Corporate Governance: An International Review*, *14*(5), 418–431. https://doi.org/10.1111/J.1467-8683.2006.00515.X

AICPA. (2017a). *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*. 29. https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/Description-Criteria.pdf%0Ahttps://web.archive.org/web/20170706132715/https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocum

AICPA. (2017b). *Guide Reporting on an Entity´s Cybersecurity Risk Management Program and Controls*.

AICPA. (2018). *Cybersecurity risk management reporting*. 1–4.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Al-Hadi, A., Hasan, M. M., & Habib, A. (2016). Risk Committee, Firm Life Cycle, and Market Risk Disclosures. *Corporate Governance: An International Review*, *24*(2), 145–170. https://doi.org/10.1111/corg.12115

Al-Sartawi, A. M. A. M., Wadi, R. M. A., & Hannoon, A. (2018). Information Technology Governance and Electronic Financial Disclosure. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11195 LNCS*, 449–458. https://doi.org/10.1007/978-3-030-02131-3_40

Alavi, M., & Weiss, I. R. (1985). Managing the Risks Associated with End-User Computing. *Journal of Management Information Systems*, *2*(3), 5–20. https://doi.org/10.1080/07421222.1985.11517734

Albitar, K., Hussainey, K., Kolade, N., & Gerged, A. M. (2020). ESG disclosure and firm performance before and after IR: The moderating role of governance mechanisms. *International Journal of Accounting & Information Management*, *28*(3), 429–444. https://doi.org/10.1108/IJAIM-09-2019-0108

Alchian, A., & Demsetz, H. (1972). Linked references are available on JSTOR for this article : Production , Information Costs , and Economic Organization. *The American Economic Review*, *62*(5), 777–795. https://knowledgehub.unsse.org/es/knowledge-hub/relaciones-entre-los-ods-el-plan-para-una-decada-cooperativa-y-el-balance-social-en-cooperativas-2/

Allegrini, M., & Greco, G. (2013). Corporate boards, audit committees and voluntary disclosure: Evidence from Italian Listed Companies. *Journal of Management and Governance*, *17*(1), 187–216. https://doi.org/10.1007/S10997-011-9168-3/TABLES/6

Allini, A., Manes Rossi, F., & Hussainey, K. (2016). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *Public Money & Management*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Allini, A., Manes Rossi, F., & Macchioni, R. (2014). Do Corporate Governance Characteristics Affect Non-Financial Risk Disclosure in Government-owned Companies? The Italian Experience. *FINANCIAL REPORTING*, *1*, 5–31.

https://doi.org/10.3280/FR2014-001001

Allini, A., Rossi, F. M., & Hussainey, K. (2015). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *http://dx.doi.org/10.1080/09540962.2016.1118935*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Almazan, A., & Suarez, J. (2003). Entrenchment and Severance Pay in Optimal Governance Structures. *The Journal of Finance*, *58*(2), 519–547. https://doi.org/10.1111/1540-6261.00536

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). *Towards a Taxonomy of Information Security Management Practices in Organisations*. https://openrepository.aut.ac.nz/handle/10292/8174

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *ACM International Conference Proceeding Series*, *September 2018*, 68–79. https://doi.org/10.1145/3285957.3285971

Amir, E., & Lev, B. (1996). Value-relevance of nonfinancial information: The wireless communications industry. *Journal of Accounting and Economics*, *22*(1–3), 3–30. https://doi.org/10.1016/S0165-4101(96)00430-2

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Anderson, R. C., Mansi, S. A., & Reeb, D. M. (2004). Board characteristics, accounting report integrity, and the cost of debt. *Journal of Accounting and Economics*, *37*(3), 315–342. https://doi.org/10.1016/j.jacceco.2004.01.004

Andrikopoulos, A., Samitas, A., & Bekiaris, M. (2014). Corporate social responsibility reporting in financial institutions: Evidence from Euronext. *Research in International Business and Finance*, *32*, 27–35. https://doi.org/10.1016/j.ribaf.2014.02.001

Aoki, M., Kim, H.-K., & World Bank. (1995). *Corporate governance in transitional economies : insider control and the role of banks*. 467.

Armstrong, Philip; Segal, Nick; Davis, B. (2006). Corporate Governance in South Africa. En *Handbook on International Corporate Governance*.

Arnum, E. (1995). Doing business on the Internet-A question of balance. *Business Communications Review*.

Asamblea General de las Naciones Unidas. (2001). *Resolución 56/183. Cumbre Mundial sobre la Sociedad de la Información*. 3.

AT&T Cybersecurity. (2021). *What is a Cybersecurity Strategy and How to Develop One*. https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

ATOS. (2020). *Universal Registration Document Board of Directors 2020*.

Axa. (2020). *AXA Future Risks Report*.

Baginski, S. P., Campbell, J. L., Hinson, L. A., & Koo, D. S. (2018). Do Career Concerns Affect the Delay of Bad News Disclosure? *The Accounting Review*, *93*(2), 61–95. https://doi.org/10.2308/ACCR-51848

Bakker, T. G. (2015). *Beadle Scholar Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks*. https://scholar.dsu.edu/theses/294

Baldini, M., Maso, L. D., Liberatore, G., Mazzi, F., & Terzani, S. (2018). Role of Country- and Firm-Level Determinants in Environmental, Social, and Governance Disclosure. *Journal of Business Ethics*, *150*(1), 79–98. https://doi.org/10.1007/s10551-016-3139-1

Barakat, AhmedBank; Hussainey, K. (2013). Bank governance, regulation, supervision, and risk reporting: Evidence from operational risk disclosures in European banks. *International Review of Financial Analysis*, *30*, 254–273. https://doi.org/10.1016/J.IRFA.2013.07.002

Barakat, A., & Hussainey, K. (2013). 0. *International Review of Financial Analysis*, *30*, 254–273. https://doi.org/10.1016/j.irfa.2013.07.002

Barakat, F. S. Q., López Pérez, M. V., & Rodríguez Ariza, L. (2015). Corporate social responsibility disclosure (CSRD) determinants of listed companies in Palestine (PXE) and Jordan (ASE). *Review of Managerial Science*, *9*(4), 681–702. https://doi.org/10.1007/s11846-014-0133-9

Barclay, M. J., & Holderness, C. G. (1991). Negotiated Block Trades and Corporate Control. *The Journal of Finance*, *46*(3), 861–878. https://doi.org/10.1111/J.1540-6261.1991.TB03769.X

Barmpaliou, N. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*.

Barney, J. (2014). Gaining and sustaining a competitive advantage. En P. E. Limited (Ed.), *Introduction to e-Business*. https://doi.org/10.4324/9780080492780-16

Barry, T., Jona, J., & Soderstrom, N. S. (2021). The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3916525

Bartha, Peter; Gillies, J. (2006). Corporate governance in Russia: is it really necessary? En *Corporate governance handbook on international country analysis*.

Bear, S., Rahman, N., & Post, C. (2010). The Impact of Board Diversity and Gender Composition on Corporate Social Responsibility and Firm Reputation. *Journal of Business Ethics 2010 97:2*, *97*(2), 207–221. https://doi.org/10.1007/S10551-010-0505-2

Beattie, V., McInnes, B., & Fearnley, S. (2004). A methodology for analysing and evaluating narratives in annual reports: A comprehensive descriptive profile and metrics for disclosure quality attributes. *Accounting Forum*, *28*(3), 205–236. https://doi.org/10.1016/j.accfor.2004.07.001

Bebbington, J., Kirk, E. A., & Larrinaga, C. (2012). The production of normativity: A comparison of reporting regimes in Spain and the UK. *Accounting, Organizations and Society*, *37*(2), 78–94. https://doi.org/10.1016/j.aos.2012.01.001

Bebbington, J., & Larrinaga-González, C. (2008). Carbon Trading: Accounting and Reporting Issues. *European Accounting Review*, *17*(4), 697–717. https://doi.org/10.1080/09638180802489162

Berelson, B. (1952). *Content Analysis, Lindzey: Handbook of social psychology*.

Beretta, S., & Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *International Journal of Accounting*, *39*(3), 265–288. https://doi.org/10.1016/j.intacc.2004.06.006

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Berle, A. a, & Means, G. C. (1932). Property in Transaction, The Appearance of the Corporate System, The Concetration of Economic Power. *The Modern Corporation and Private Property*, 24. http://books.google.com/books?id=mLdLHhqxUb4C&pgis=1

Bhatia, A., & Makkar, B. (2020). Stage of development of a country and CSR disclosure – the latent driving forces. *International Journal of Law and Management*, *62*(5), 467–493. https://doi.org/10.1108/IJLMA-03-2020-0068

Biener, C., & Eling, M. (2012). *Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions*. *37*, 77–107. https://doi.org/10.1057/gpp.2011.29

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance: Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

Blakley, B., Mcdermott, E., Morganchase, J. P., & Geer, D. (2002). Information Security is Information Risk Management. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*. https://doi.org/10.1145/508171

Bloomfield, R. J. (2002). The "Incomplete Revelation Hypothesis" and Financial Reporting. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.312671

Bogle, J. C. (2005). *The Battle for the Soul of Capitalism*.

Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, *22*(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Botosan, C. A. (1997). Disclosure level and the cost of equity capital. *Accounting Review*, *72*(3), 323–349.

Branco, M. C., & Rodrigues, L. L. (2008). Social responsibility disclosure: A study of proxies for the public visibility of Portuguese banks. *The British Accounting Review*, *40*(2), 161–181. https://doi.org/10.1016/j.bar.2008.02.004

Brandeis, L. D. (1914). *Other people's money and how the bankers use it*. https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-by-louis-d.-brandeis

Bratton, W. W. (1989). *Penn Law : Legal Scholarship Repository The New Economic Theory of the Firm : Critical Perspectives from History The New Economic Theory of the Firm : Critical Perspectives from History*.

Bratton, W. W. (2007). *Hedge Funds and Governance Targets*. https://scholarship.law.upenn.edu/faculty_scholarship://scholarship.law.upenn.edu/faculty_scholarship/862

Brazilian Institute of Corporate Governance. (2020). *Gestión de Riesgos Corporativos* (Brazilian Institute of Corporate Governance (ed.)). https://idbinvest.org/sites/default/files/2021-04/Cuaderno 19 - Gestión de Riesgos Corporativos.pdf

Brennan, N. (2006). Boards of directors and firm performance: Is there an expectations gap? *Corporate Governance: An International Review*, *14*, 577–594.

Brennan, N. M., & Solomon, J. (2008). Corporate governance, accountability and mechanisms of accountability: An overview. *Accounting, Auditing & Accountability Journal*, *21*(7), 885–906. https://doi.org/10.1108/09513570810907401/FULL/PDF

Briano-Turrent, G. D. C., & Poletti-Hughes, J. (2017). Corporate governance compliance of family and non-family listed firms in emerging markets: Evidence from Latin America. *Journal of Family Business Strategy*, *8*(4), 237–247. https://doi.org/10.1016/J.JFBS.2017.10.001

Briano, G. del C. (2012). *Tesis doctoral: Factores institucionales que inciden en la transparencia del Gobierno Corporativo: un estudio en empresas cotizadas*. Universidad de Cantabria.

Brooks, L. (Lily) Z., Cheng, Y., Liu, L., & Yu, M. D. (2021). The timeliness of 10-K filings, early filers, and effects of filing deadline changes. *Journal of Corporate Accounting & Finance*, *32*(2), 169–186. https://doi.org/10.1002/JCAF.22492

Burnap, P. (2021). Risk Management & Governance Knowledge Area. *The Cyber Security Body Of Knowledge*, 19–48.

Bushee, B. J., Carter, M. E., & Gerakos, J. (2014). Institutional investor preferences for corporate governance mechanisms. *Journal of Management Accounting Research*, *26*(2), 123–149. https://doi.org/10.2308/jmar-50550

Bushman, R. M., & Smith, A. J. (2001). Financial accounting information and corporate governance. *Journal of Accounting and Economics*, *32*(1–3), 237–333. https://doi.org/10.1016/S0165-4101(01)00027-1

Business Roundtable. (2018). *Principles of Corporate Governance 2016*. *153*(153), 84–97.

Cabedo, J. D., & Tirado, J. M. (2004). The disclosure of risk in financial statements. *Accounting Forum*, *28*(2), 181–200. https://doi.org/10.1016/j.accfor.2003.10.002

Cadbury. (1992). The Report of the Cadbury Committee on The Financial Aspects of Corporate Governance: The Code of Best Practice. *Corporate Governance: An International Review*, *1*(3), 124–124. https://doi.org/10.1111/j.1467-8683.1993.tb00025.x

CAF. (2013). *Lineamientos para un Código latinoamericano de Gobierno Corporativo* .

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. https://doi.org/10.1111/RISA.13687

Calder, A. (2008). *Corporate governance : a practical guide to the legal frameworks and international codes of practice* (London).

Calderón, R., Piñero, R., & Redín, D. M. (2018). Can compliance restart integrity? Toward a harmonized approach. The example of the audit committee. *Business Ethics: A European Review*, *27*(2), 195–206. https://doi.org/10.1111/BEER.12182

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, *25*(1), 24–39. https://doi.org/10.1111/ijau.12209

Campbell, J. L. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. En *Academy of Management Review* (Vol. 32, Número 3, pp. 946–967). Academy of Management. https://doi.org/10.5465/AMR.2007.25275684

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. min, & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, *19*(1), 396–455. https://doi.org/10.1007/s11142-013-9258-3

Campbell, K., & Mínguez-Vera, A. (2008). Gender Diversity in the Boardroom and Firm Financial Performance. *Journal of Business Ethics 2007 83:3*, *83*(3), 435–451. https://doi.org/10.1007/S10551-007-9630-Y

Cano, J. (2021). *Ciberseguridad empresarial Reflexiones y retos para los ejecutivos del siglo XXI*.

Carter, D. A., D'Souza, F., Simkins, B. J., & Simpson, W. G. (2010). The Gender and Ethnic Diversity of US Boards and Board Committees and Firm Financial Performance. *Corporate Governance: An International Review*, *18*(5), 396–414. https://doi.org/10.1111/J.1467-8683.2010.00809.X

Carter, D. A., Simkins, B. J., & Simpson, W. G. (2003). Corporate Governance, Board Diversity, and Firm Value. *Financial Review*, *38*(1), 33–53. https://doi.org/10.1111/1540-6288.00034

Castro, S. (2009). Practicas de Gobierno Corporativo en America Latina. *Revista Latinoamericana de Administración*, *43*, 26–40.

Cavelty, M. D. (2010). *Cyber-Security* (Routledge (ed.)). The Routledge Handbook of New Security Studies: 154-162.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach

announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

CCB, & OCDE. (2004). *"White paper" sobre Gobierno Corporativo en Latinoamerica*. *7*, 92.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images*. *December*. http://www.sei.cmu.edu

CEUPE. (2019). Modelos de Gobierno Corporativo. *Centro europeo de postgrado*, 1. https://www.ceupe.com/blog/modelos-de-gobierno-corporativo.html

Chang, H. C. (2016). The Synergy of Scientometric Analysis and Knowledge Mapping with Topic Models: Modelling the Development Trajectories of Information Security and Cyber-Security Research. *http://dx.doi.org/10.1142/S0219649216500441*, *15*(4). https://doi.org/10.1142/S0219649216500441

Chang, L. S., Most, K. S., & Brain, C. W. (1983). The Utility of Annual Reports: An International Study. *Journal of International Business Studies 1983 14:1*, *14*(1), 63–84. https://doi.org/10.1057/PALGRAVE.JIBS.8490507

Chapple, W., & Moon, J. (2005). Corporate social responsibility (CSR) in Asia a seven-country study of CSR Web site reporting. *Business and Society*, *44*(4), 415–441. https://doi.org/10.1177/0007650305281658

Charkham, J. P. (1995). *Keeping good company : a study of corporate governance in five countries*. 389.

Cheffins, B. R. (2012). The History of Corporate Governance. *SSRN Electronic Journal*, *January*. https://doi.org/10.2139/ssrn.1975404

Chen, T. ; R. J. (2004). *The Evolution of Viruses and Worms*. 289–310. https://doi.org/10.1201/9781420030884-19

Cheung, Y. L., Jiang, P., & Tan, W. (2010). A transparency Disclosure Index measuring disclosures: Chinese listed companies. *Journal of Accounting and Public Policy*, *29*(3), 259–280. https://doi.org/10.1016/j.jaccpubpol.2010.02.001

Chithambo, L., & Tauringana, V. (2014). Company specific determinants of greenhouse gases disclosures. *Journal of Applied Accounting Research*, *15*(3), 323–338. https://doi.org/10.1108/JAAR-11-2013-0087

Choe, H., Kho, B. C., & Stulz, R. M. (2005). Do domestic investors have an edge? The trading experience of foreign investors in Korea. *Review of Financial Studies*, *18*(3), 795–829. https://doi.org/10.1093/rfs/hhi028

Choi, B.B., Lee, D. and Psaros, J. (2010). An analysis and explanation of Australian company carbon emission disclosures. *Paper presented at 2010 AFAANZ Conference, Christchurch, July 3-5.*

Choi, F. D. S. (1973). Financial Disclosure and Entry to the European Capital Market. *Journal of Accounting Research*, *11*(2), 159. https://doi.org/10.2307/2490187

Chong, Alberto; López de Silanes, F. (2007). Investor Protection and Corporate Governance. En S. U. P. (2007) (Ed.), *Investor Protection and Corporate Governance*. The World Bank. https://doi.org/10.1596/978-0-8213-6913-5

Chong, A., & Lopez-de-Silanes, F. (2007). *Investor protection and corporate governance : firm-level evidence across Latin America*. 557.

Chow, C. W., & Wong-Boren, A. (1987). Voluntary Financial Disclosure by Mexican Corporations. *Accounting Review*, *62*(3), 533. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=4496048&S=R&D=bth&EbscoContent=dGJyMNLe80SeqLE4y9f3OLCmr0uep7ZSsKi4TLSWxWXS&ContentCustomer=dGJyMPGqtkqxra5Rue3sfefwuY3x2%2FAA%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=449604

Chu, C. I., Chatterjee, B., & Brown, A. (2013). The current status of greenhouse gas reporting by Chinese companies: A test of legitimacy theory. *Managerial Auditing Journal*, *28*(2), 114–139. https://doi.org/10.1108/02686901311284531

Clarkson, P. M., Fang, X., Li, Y., & Richardson, G. (2013). The relevance of environmental disclosures: Are such disclosures incrementally informative? *Journal of Accounting and Public Policy*, *32*(5), 410–431. https://doi.org/10.1016/J.JACCPUBPOL.2013.06.008

Clarkson, P. M., Li, Y., Richardson, G. D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis. *Accounting, Organizations and Society*, *33*(4–5), 303–327. https://doi.org/10.1016/j.aos.2007.05.003

Clinton, L., & Higgins, J. (2020). *Cyber-Risk Oversight Cyber-Risk Oversight*.

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405. https://doi.org/10.1111/J.1468-0335.1937.TB00002.X

Coles, J. L., Daniel, N. D., & Naveen, L. (2008). Boards: Does one size fit all? *Journal of Financial Economics*, *87*(2), 329–356. https://doi.org/10.1016/J.JFINECO.2006.08.008

Collier, P., & Institute of Chartered Accountants in England and Wales. Research Board. (1992). *Audit committees in large UK companies.* 203.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems and Decisions 2013 33:4*, *33*(4), 469–470. https://doi.org/10.1007/S10669-013-9484-Z

Comisión Europea. (2022). *Economía justa y sostenible : la Comisión establece normas para que las empresas respeten los derechos humanos y el medio ambiente en las cadenas de suministro mundiales*. https://ec.europa.eu/commission/presscorner/detail/es/ip_22_1145

Comisión Interamericana de Telecomunicaciones. (2004). *Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética*.

Comisión Nacional de Valores. (2019). *Codigo de Gobierno Societario - Resolucion General 797 2019*. https://www.erreius.com/Legislacion/documento/20190619075647772/resolucion-general-797-2019-comision-nacional-de-valores-codigo-de-gobierno-societario-memoria-informacion-modificacion-normas-nt-2013

Committee Basel. (2015). Standards: Revised Pillar 3 Disclosure Requirements. En *Bank for International Settlements* (Número January). http://www.bis.org/bcbs/publ/d309.pdf

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Consejo coordinador empresarial. (2018). *Código de principios y mejores prácticas de Gobierno Corporativo*.

Convenio de Budapest, | (2001).

Cooke, T. E., & Wallace, R. S. O. (1989). Global Surveys of Corporate Disclosure Practices and Audit Firms: A Review Essay. *Accounting and Business Research*, *20*(77), 47–57. https://doi.org/10.1080/00014788.1989.9729394

COSO. (2017). *COSO II ERM*.

CPMI-IOSCO. (2016). *Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures*. www.bis.org

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Creese, S. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Crowdstrike. (2021). *The evolution of ransomware: how to protect against new adversary trends and methods*. 1–9.

CSA. (2017). *CSA Multilateral Staff Notice 51-347-Disclosure of cyber security risks and incidents*. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

CSA ACVM. (2013). *CSA Staff Notice 11-326 - Cyber Security*.

CSA ACVM. (2017). *CSA Staff Notice 33-321: Cyber Security and Social Media*. https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2017/2017oct19-33-321-avis-acvm-en.pdf

CSA ACVM. (2019). *Disclosure of cyber security risks and incidents*. *2017*, 605–608.

CyBOK. (2019). The Cyber Security Body of Knowledge (CyBoK) 1.0. *CyBoK*, 299.

https://www.cybok.org/

CyBOK. (2021). Introduction to CyBOK Knowledge Areas. *The Cyber Security Body of Knowledge*, 22. www.cybok.org

Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *https://doi.org/10.1080/10580530701586136*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Dalton, D. R., Hitt, M. A., Certo, S. T., & Dalton, C. M. (2007). The Fundamental Agency Problem and Its Mitigation. *The Academy of Management Annals*, *1*(1), 1–64. https://doi.org/10.1080/078559806

Darus, F., Mohd Zuki, H. I., & Yusoff, H. (2019). The path to sustainability: Understanding organisations' environmental initiatives and climate change in an emerging economy. *European Journal of Management and Business Economics*, *29*(1), 84–96. https://doi.org/10.1108/EJMBE-06-2019-0099

Datt, R. R., Luo, L., & Tang, Q. (2019). Corporate voluntary carbon disclosure strategy and carbon performance in the USA. *Accounting Research Journal*, *32*(3), 417–435. https://doi.org/10.1108/ARJ-02-2017-0031

Day, J. (2018). *Privacy and Cybersecurity Developments in Latin America*. https://www.lexology.com/library/detail.aspx?g=c0701531-2665-4e4b-a87b-00434e25d55f

De Villiers, C., Hsiao, P.-C. K., & Maroun, W. (2020). Introduction to the Routledge Handbook of Integrated Reporting : An overview of integrated reporting and this book, which entails different perspectives on a maturing field and a framework for future research. *The Routledge Handbook of Integrated Reporting*, 1–14. https://doi.org/10.4324/9780429279621-1

Deegan, C. (2002). Introduction: The legitimising effect of social and environmental disclosures – a theoretical foundation. En *Accounting, Auditing & Accountability Journal* (Vol. 15, Número 3, pp. 282–311). MCB UP Ltd. https://doi.org/10.1108/09513570210435852

Deloitte. (2012). *Guía Práctica Consejeros del Comité de Auditoría*.

Deloitte. (2015). *Cybersecurity: The changing role of audit committee and internal audit Contents*. 16. http://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

Deloitte. (2016). *Cyber security: The changing role of the Board and the Audit Committee*. *June*, 5. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

Deloitte. (2019a). *Índice Global de Ciberseguridad - 2018*. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html

Deloitte. (2019b). Managing Cyber Risk in a Digital Age. *Coso*, 28. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-

Digital-Age.pdf

Deloitte. (2021a). *Business-aligned cyber strategy | Deloitte | Cyber Risk*. https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/business-aligned-cyber-strategy.html

Deloitte. (2021b). *Practicas nacionales versus practicas internacionales Gobierno Corporativo*.

Deloitte. (2021c). *Progress at a snail's pace*. file:///C:/Users/HP/Desktop/gx-women-in-the-boardroom-seventh-edition (1).pdf

Denis, D. K. (2001). Twenty-five years of corporate governance research … and counting. *Review of Financial Economics*, *10*(3), 191–212. https://doi.org/10.1016/S1058-3300(01)00037-4

DeZoort, F. T., Hermanson, D., Archambeault, D., & Reed, S. (2002). Audit Committee Effectiveness: A Synthesis of the Empirical Audit Committee Literature. *Audit Committee Effectiveness: A Synthesis of the Empirical Audit Committee Literature*, *21*. https://digitalcommons.kennesaw.edu/facpubs/1495

Dezsö, C. L., & Ross, D. G. (2012). Does female representation in top management improve firm performance? A panel data investigation. *Strategic Management Journal*, *33*(9), 1072–1089. https://doi.org/10.1002/SMJ.1955

Dimaggio, P. (1982). Cultural Capital and School Success : The Impact of Status Culture Participation on the Grades. *American Sociological Review*, *47*(2), 189–201.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147. https://doi.org/10.2307/2095101

Division of Corporation Finance, & SEC. (2011). *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Dobran, B. (2021). *17 Types of Cyber Security Attacks To Protect Against in 2021*. https://phoenixnap.com/blog/cyber-security-attack-types/

Domenech, J. J. G. (2017). La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE. *REVISTA LEX MERCATORIA Doctrina, Praxis, Jurisprudencia y Legislación*, 37–42. https://doi.org/10.21134/LEX.VI.534

Donnelly, R., & Mulcahy, M. (2008). Board Structure, Ownership, and Voluntary Disclosure in Ireland. *Corporate Governance: An International Review*, *16*(5), 416–429. https://doi.org/10.1111/j.1467-8683.2008.00692.x

Dungey, M., Flavin, T., O'Connor, T., & Wosser, M. (2022). Non-financial corporations and systemic risk. *Journal of Corporate Finance*, *72*, 102129. https://doi.org/10.1016/J.JCORPFIN.2021.102129

E&Y. (2018). *Cybersecurity disclosure benchmarking*.

E&Y. (2019). *What Companies are Disclosing About Cybersecurity Risk and Oversight*.

1–7.

E&Y. (2020). *What companies are disclosing about cybersecurity risk and oversight in 2020*. *August*.

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law and Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Eisenberg, M. A. (1976). *The structure of the corporation : a legal analysis*. https://books.google.com/books/about/The_Structure_of_the_Corporation.html?hl=es&id=pxY-AQAAIAAJ

Eisenberg, T., Sundgren, S., & Wells, M. T. (1998). Larger board size and decreasing firm value in small firms. *Journal of Financial Economics*, *48*(1), 35–54. https://doi.org/10.1016/s0304-405x(98)00003-8

Eisenhardt, K. M. (1985). Control: Organizational and Economic Approaches. *http://dx.doi.org/10.1287/mnsc.31.2.134*, *31*(2), 134–149. https://doi.org/10.1287/MNSC.31.2.134

Elamer, A. A., AlHares, A., Ntim, C. G., & Benyazid, I. (2018). The corporate governance–risk-taking nexus: evidence from insurance companies. *International Journal of Ethics and Systems*, *34*(4), 493–509. https://doi.org/10.1108/IJOES-07-2018-0103

Elamer, A. A., Ntim, C. G., Abdou, H. A., & Pyke, C. (2020). Sharia supervisory boards, governance structures and operational risk disclosures: Evidence from Islamic banks in MENA countries. *Global Finance Journal*, *46*, 100488. https://doi.org/10.1016/J.GFJ.2019.100488

Elgadi, E., & Ghardallou, W. (2022). Gender diversity, board of director's size and Islamic banks performance. *International Journal of Islamic and Middle Eastern Finance and Management*, *15*(3), 664–680. https://doi.org/10.1108/IMEFM-09-2019-0397/FULL/PDF

Eling, M., & Schnell, W. (2016a). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122/FULL/PDF

Eling, M., & Schnell, W. (2016b). What do we know about cyber risk and cyber risk insurance? En *Journal of Risk Finance* (Vol. 17, Número 5, pp. 474–491). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-09-2016-0122

Ellimäki, P., Gómez-Bolaños, E., Hurtado-Torres, N., & Aragón-Correa, J. A. (2021). Do global firms increase their environmental disclosure and performance? Symbolic versus effective operations and the moderating role of liability of origin. Legitimation implications. *Industrial Marketing Management*, *92*, 354–363. https://doi.org/10.1016/J.INDMARMAN.2019.10.015

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*(6), 597–603. https://doi.org/10.1016/0167-4048(93)90056-B

Elsayed, M., Elshandidy, T., & Ahmed, Y. (2022). Corporate failure in the UK: An

examination of corporate governance reforms. *International Review of Financial Analysis*, *82*, 102165. https://doi.org/10.1016/J.IRFA.2022.102165

Elshandidy, T., & Neri, L. (2015). Corporate Governance, Risk Disclosure Practices, and Market Liquidity: Comparative Evidence from the UK and Italy. *Corporate Governance: An International Review*, *23*(4), 331–356. https://doi.org/10.1111/corg.12095

Elshandidy, T., Shrives, P. J., Bamber, M., & Abraham, S. (2018). Risk reporting: A review of the literature and implications for future research. *Journal of Accounting Literature*, *40*, 54–82. https://doi.org/10.1016/j.acclit.2017.12.001

Elzahar, H., & Hussainey, K. (2012). Determinants of narrative risk disclosures in UK interim reports. *Journal of Risk Finance*, *13*(2), 133–147. https://doi.org/10.1108/15265941211203189/FULL/PDF

ENISA. (2015). Definition of Cybersecurity | Gaps and overlaps in standardisation. En *European Union Agency For Network And Information Security: Vol. v1.0* (Número December).

Enrique, & Bonsón, E. T. (2004). *La difusión voluntaria de información financiera en Internet. Un análisis comparativo entre Estados Unidos, Europa del Este y la Unión Europea*.

Ernst & Young. (2019). *What Boards Are Doing Today to Better Oversee Cyber Risk*. *July*, 1–6.

Ernst & Young. (2021). *EY Global Information Security Survey 2021: Cybersecurity: how do you rise above the waves of a perfect storm?*

Ernstberger, J., & Grüning, M. (2013). How do firm- and country-level governance mechanisms affect firms' disclosure? *Journal of Accounting and Public Policy*, *32*(3), 50–67. https://doi.org/10.1016/J.JACCPUBPOL.2013.02.003

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

EU. (2014). *Directive 2014/95 / EU of the European Parliament and of the Council - of October 22, 2014*.

EU. (2016). *EU general data protection regulation* (Vol. 2014, Número April).

EU. (2019). *Regulation (EU) 2019/881*. Regulation (EU) 2019/881 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

Europea, U. (2015). *Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document*. https://doi.org/10.1787/9789264245471-en

Excelencia, E. E. de. (2022). *Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál escoger?* https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-riesgo-cuantitativa-vs-cualitativa-cual-escoger/

EY. (2018). *SEC guidance on cybersecurity: board considerations* (Número March). https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cybersecurity/ey-sec-guidance-on-cybersecurity-board-considerations.pdf

EY. (2020). *EY Global Information Security Survey 2020. How does security evolve from bolted on to built-in?* https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf

EY. (2021). *Board Agenda 2021*. *1*(1), 21.

Fakhfakh, I., & Jarboui, A. (2022). Board of director's effectiveness, audit quality and ownership structure: impact on audit risk-Tunisian evidence. *Journal of Accounting in Emerging Economies*, *12*(3), 468–485. https://doi.org/10.1108/JAEE-07-2020-0158/FULL/PDF

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustment of Stock Prices to New Information. *International Economic Review*, *10*(1), 1. https://doi.org/10.2307/2525569

Fama, E. F., & Jensen, M. C. (1983). Separation of Ownership and Control. *Journal of Law & Economics*, *26*. https://heinonline.org/HOL/Page?handle=hein.journals/jlecono26&id=313&div=&collection=

Farrell, K. A., & Hersch, P. L. (2005). Additions to corporate boards: the effect of gender. *Journal of Corporate Finance*, *11*(1–2), 85–106. https://doi.org/10.1016/J.JCORPFIN.2003.12.001

FASB. (1994). Statement of Financial Accounting Standards No. 119, Disclosure about Derivative Financial Instruments and Fair Value of Financial Instruments. *Financial Accounting Standards Board: Norwalk, Connecticut*, *119*.

FASB. (1998). Statement of Financial Accounting Standards No. 133, Accounting for Derivative Instruments and Hedging Activities. *Financial Accounting Standards Board: Norwalk, Connecticut.*, *133*.

Fidler, D. P. (2020). Cybersecurity in the Time of COVID-19. *Council on Foreign Relations*, *2020*, 7–9. https://www.cfr.org/blog/cybersecurity-time-covid-19

Fifka, M. S., & Pobizhan, M. (2014). An institutional approach to corporate social responsibility in Russia. *Journal of Cleaner Production*, *82*, 192–201. https://doi.org/10.1016/j.jclepro.2014.06.091

Financial Standards Foundation. (2011). Achieving Effective Boards. *Global Corporate Governance Forum*, *June*.

Fontaine, David; Reed, J. (2018). *Cybersecurity: The SEC's Wake-up Call to Corporate*

*Directors*. Harvard Law School. https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/

Fortinet. (2022). *Fortinet registró 137 mil millones de intentos de ciberataques en América Latina en la primera mitad del año.* https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

Francoeur, C., Labelle, R., & Sinclair-Desgagné, B. (2008). Gender Diversity in Corporate Governance and Top Management. *Journal of Business Ethics 2007 81:1*, *81*(1), 83–95. https://doi.org/10.1007/S10551-007-9482-5

Fraser, J. S. B. J. (2010). *Enterprise risk management*.

Freedman, M., & Jaggi, B. (2005). Global warming, commitment to the Kyoto protocol, and accounting disclosures by the largest global public firms from polluting industries. *The International Journal of Accounting*, *40*(3), 215–232. https://doi.org/10.1016/J.INTACC.2005.06.004

Freeman, E. (1984). *Edward Freeman*.

Freeman, R. E., & Mcvea, J. (2001). *A Stakeholder Approach to Strategic Management*.

Freeman, R. E., & Reed, D. L. (1983). Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review*, *25*(3), 88–106. https://doi.org/10.2307/41165018

Frias-Aceituno, J. V., Rodríguez-Ariza, L., & Garcia-Sánchez, I. M. (2014). Explanatory Factors of Integrated Sustainability and Financial Reporting. *Business Strategy and the Environment*, *23*(1), 56–72. https://doi.org/10.1002/bse.1765

Friedman, M. A. (1970). *The social responsibility of business is to increase its profits*. https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html

G20/OECD. (2016). Principles of Corporate Governance. En *G20/OECD Principles of Corporate Governance*. https://doi.org/10.1787/9789264257443-tr

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

García-Sánchez, I. M., Gómez-Miranda, M. E., David, F., & Rodríguez-Ariza, L. (2019). Board independence and GRI-IFC performance standards: The mediating effect of the CSR committee. *Journal of Cleaner Production*, *225*, 554–562. https://doi.org/10.1016/J.JCLEPRO.2019.03.337

Garcia-Sanchez, I. M. of the I. M. C. on the V. D. of C. I., Cuadrado-Ballesteros, B., & Frias-Aceituno, J. V. (2016). Impact of the Institutional Macro Context on the Voluntary Disclosure of CSR Information. *Long Range Planning*, *49*(1), 15–35. https://doi.org/10.1016/J.LRP.2015.02.004

Gelfond, S., Wechsler, J., Cohen, H., & Llp, J. (2017). *Top 10 Practice tips by experts: risk*

*factors*.

Gendron, Y., & Bédard, J. (2006). On the constitution of audit committee effectiveness. *Accounting, Organizations and Society*, *31*(3), 211–239. https://doi.org/10.1016/J.AOS.2005.03.002

German Government Commission. (2022). *Deutscher Corporate Governance Kodex*. https://doi.org/10.1515/zinso-2018-0608

Giner, B. (1997). The influence of company characteristics and accounting regulation on information disclosed by Spanish firms. *https://doi.org/10.1080/096381897336863*, *6*(1), 45–68. https://doi.org/10.1080/096381897336863

Gómez Vieites, A. (2006). *Enciclopedia de la seguridad informática*.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. En *Computer Security Journal* (Vol. 19, Número 2, pp. 1–7). Computer Security Institute.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692

Gray, R., Kouhy, R., & Lavers, S. (1995). Corporate social and environmental reporting A review of the literature and a longitudinal study of UK disclosure. *Accounting, Auditing & Accountability Journal*, *8*(2), 47–77. https://doi.org/10.1108/09513579510146996

GRI. (2016). GRI 418: Customer privacy 2016 418. *GRI Standards*. www.globalreporting.org

Grossman, B. S. J., & Stiglitz, J. E. (1980). *On the Impossibility of Informationally Efficient*

*Markets Author ( s ): Sanford J . Grossman and Joseph E . Stiglitz Source : The American Economic Review , Jun ., 1980 , Vol . 70 , No . 3 ( Jun ., 1980 ), pp . 393- Published by : American Economic Associ*. *70*(3), 393–408.

GSSB. (2016). GRI 418: Privacidad Del Cliente 2016. *GRI Standards*.

Gul, F. A., Srinidhi, B., & Ng, A. C. (2011). Does board gender diversity improve the informativeness of stock prices? *Journal of Accounting and Economics*, *51*(3), 314–338. https://doi.org/10.1016/J.JACCECO.2011.01.005

Gunter, O. (2004). The Phishing Guide. *History*.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. En *Managerial Auditing Journal* (Vol. 34, Número 7, pp. 808–834). Emerald Group Publishing Ltd. https://doi.org/10.1108/MAJ-09-2018-2004

Hacienda, M. D. E., & Hacienda, S. D. E. (2022). *Ley 20382*. 1–34.

Haniffa, R. M., & Cooke, T. E. (2002). Culture, Corporate Governance and Disclosure in Malaysian Corporations. *Abacus*, *38*(3), 317–349. https://doi.org/10.1111/1467-6281.00112

Haniffa, R. M., & Cooke, T. E. (2005). The impact of culture and governance on corporate social reporting. *Journal of Accounting and Public Policy*, *24*(5), 391–430. https://doi.org/10.1016/j.jaccpubpol.2005.06.001

Haque, S., & Deegan, C. (2010). Corporate Climate Change-Related Governance Practices and Related Disclosures: Evidence from Australia. *Australian Accounting Review*, *20*(4), 317–333. https://doi.org/10.1111/J.1835-2561.2010.00107.X

Hardiyansah, M., & Agustini, A. T. (2020). Analysis of carbon emissions disclosure and firm value: Type of industry as a moderating model. *International Journal of Scientific and Technology Research*, *9*(2), 1125–1132.

Harrigan, K. R. (2017). Numbers and Positions Of Women Elected to Corporate Boards. *https://doi.org/10.5465/255580*, *24*(3), 619–625. https://doi.org/10.5465/255580

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*, *73*, 102–113. https://doi.org/10.1016/J.COSE.2017.10.008

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, *3*, 1117–1124. https://doi.org/10.1016/J.PROMFG.2015.07.186

Hermalin, B. E., & Weisbach, M. S. (2003). *Boards of Directors as an Endogenously Determined Institution: A Survey of the Economic Literature*. https://doi.org/10.3386/W8161

Héroux, S., & Fortin, A. (2020a). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S., & Fortin, A. (2020b). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100.

https://doi.org/10.1111/1911-3838.12220

Hijink, J. B. S. (2010). *Publicatieverplichtingen voor beursvennootschappen*.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2852519

Hillman, A. J., Cannella, A. A., & Paetzold, R. L. (2000). The Resource Dependence Role of Corporate Directors: Strategic Adaptation of Board Composition in Response to Environmental Change. *Journal of Management Studies*, *37*(2), 235–256. https://doi.org/10.1111/1467-6486.00179

Holland & Knight. (2021). *SEC Issues First-Ever Penalties for Deficient Cybersecurity Risk Controls*. https://www.hklaw.com/en/insights/publications/2021/06/sec-issues-first-ever-penalties-for-deficient-cybersecurity-risk

Holland, L., & Foo, Y. B. (2003). Differences in environmental reporting practices in the UK and the US: The legal and regulatory context. *British Accounting Review*, *35*(1), 1–18. https://doi.org/10.1016/S0890-8389(02)00127-0

Hope, O.-K. (2003). *Disclosure Practices, Enforcement of Accounting Standards, and Analysts' Forecast Accuracy: An International Study - Hope - 2003 - Journal of Accounting Research - Wiley Online Library*. https://onlinelibrary.wiley.com/doi/10.1111/1475-679X.00102

Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies*, *21*(4), 1005–1045. https://doi.org/10.1007/s11142-016-9371-1

Hunt, B. (2003). *The Timid Corporation: Why Business is Terrified of Taking Risk*.

IBGC. (2015). Código das Melhores Práticas de Governança Corporativa. En *Instituto Brasileiro de Governança Corporativa*. http://www.ibgc.org.br/userfiles/2014/files/CMPGPT.pdf

ICAWE. (2011). *Reporting Business Risks: Meeting Expectations*.

IDB; OAS. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

International Integrated Reporting Council. (2021). < IR > Framework about the IIRC. *Jo*, *January*, 58. https://integratedreporting.org/wp-content/uploads/2021/01/InternationalIntegratedReportingFramework.pdf

International Telecommunication Union. (2008). Overview Cybersecurity. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I

Internet Security Alliance and American National Standards. (2010). The Financial Management of Cyber Risk: An Implementation Framework for CFOs. *Order A Journal On The Theory Of Ordered Sets And Its Applications*.

Investor Stewardship Group. (2017). Corporate Governance Principles For US Listed Companies. *Isg*, 1–5. https://isgframework.org/corporate-governance-principles/

IOSCO. (2016). *Cyber Security in Securities Markets – An International Perspective Report on IOSCO ' s cyber risk coordination efforts*.

IRRC. (2016). *The Corporate Risk Factor Disclosure Landscape*. *January*, 27. https://www.weinberg.udel.edu/irrci/research/887

ISO. (2011). ISO 26000. *The Corporate Responsibility code book*, 83–129. https://doi.org/10.4324/9781351278881-5

ISO. (2012). *ISO/IEC 27032: Information technology — Security techniques — Guidelines for cybersecurity*. ISO 27032. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO. (2013). *ISO 27002*.

ISO. (2018). *ISO 31000 Risk management*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO. (2020). *ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security*. https://www.iso.org/standard/74046.html

*ISO 37000*. (2021).

ITU. (2007). *ITU Global Cybersecurity Agenda - A Framework for International Cooperation in Cybersecurity*. https://www.itu.int/osg/spuold/cybersecurity/gca/

ITU. (2017). Global Cybersecurity Index (GCI) 2017. En *ITU-D Global*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU. (2018). *Global Cybersecurity Index (GCI) 2018 ITUPublications Studies & research*.

ITU. (2020). *ITU Publications*. Índice Global de Ciberseguridad 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

ITU. (2021a). *About the International Telecommunication Union (ITU)*. https://www.itu.int/es/about/Pages/default.aspx

ITU. (2021b). Global Cybersecurity Index (GCI). En *ITU Publications*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU & ABI Research. (2014). *Global Cybersecurity I N D E X*. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

Jaggi, B., & Low, P. Y. (2000). Impact of Culture, Market Forces, and Legal System on Financial Disclosures. *The International Journal of Accounting*, *35*(4), 495–519. https://doi.org/10.1016/S0020-7063(00)00076-5

Jamali, D., Safieddine, A. M., & Rabbath, M. (2008). Corporate Governance and Corporate Social Responsibility Synergies and Interrelationships. *Corporate Governance: An International Review*, *16*(5), 443–459. https://doi.org/10.1111/J.1467-8683.2008.00702.X

Jamaludin, N. D., Sanusi, Z. M., & Kamaluddin, A. (2015). Board Structure and Earnings Management in Malaysian Government Linked Companies. *Procedia Economics and Finance*, *28*, 235–242. https://doi.org/10.1016/S2212-5671(15)01105-3

James P. Anderson, Sheila Brand, Li Gong, T. H. (2004). Firewalls: an Expert Roundtable. En *Book Security, Statistical Methods in Computer* (Edition, E, pp. 333–350). CRC Press. https://doi.org/10.1201/9781420030884-21

Jensen, M. C. (1993). The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems. *The Journal of Finance*, *48*(3), 831–880. https://doi.org/10.1111/j.1540-6261.1993.tb04022.x

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: managerial behavior, agency costs and ownership structure. *Journal Of Financial Economics*, *3*, 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Jizi, M. I., Salama, A., Dixon, R., & Stratling, R. (2014). Corporate Governance and Corporate Social Responsibility Disclosure: Evidence from the US Banking Sector. *Journal of Business Ethics*, *125*(4), 601–615. https://doi.org/10.1007/s10551-013-1929-2

Jorion, P. (2002). *The Accounting Review* (Vol. 77).

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019

Kang, H., Cheng, M., & Gray, S. J. (2007). Corporate Governance and Board Composition: diversity and independence of Australian boards. *Corporate Governance: An International Review*, *15*(2), 194–207. https://doi.org/10.1111/J.1467-8683.2007.00554.X

Kanter, R. M. (1977). *Men and women of the corporation*. 348. https://books.google.com/books/about/Men_And_Women_Of_The_Corporation.html?hl=es&id=7L63AAAAIAAJ

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond Cybersecurity: Protecting Your Digital Business*. *Exhibit 1*, 1–9. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1119026849,descCd-buy.html

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Kasznik, R., & Lev, B. (1995). To warn or not to warn: Management disclosures in the face of an earnings surprise. *Accounting review: A quarterly journal of the American Accounting Association*, *70*(1), 113–134.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2010). The Worldwide Governance Indicators: A Summary of Methodology, Data and Analytical Issues. *The World Bank*, *5430*(September), 1–29.

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020a). A bibliometric analysis of

board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/j.jbusres.2019.11.025

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020b). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/J.JBUSRES.2019.11.025

Khatib, S. F. A., Abdullah, D. F., Elamer, A. A., & Abueid, R. (2021). Nudging toward diversity in the boardroom: A systematic literature review of board diversity of financial institutions. *Business Strategy and the Environment*, *30*(2), 985–1002. https://doi.org/10.1002/BSE.2665

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys and Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Kiesow Cortez, E., & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation*, *January*, 1–23. https://doi.org/10.1017/err.2022.10

Kiliç, M., Kuzey, C., & Uyar, A. (2015). The impact of ownership and board structure on corporate social responsibility (CSR) reporting in the Turkish banking industry. *Corporate Governance (Bingley)*, *15*(3), 357–374. https://doi.org/10.1108/CG-02-2014-0022

King, M. (2016). Report on corporate governance for South Africa 2016. *King IV Report on Corporate Governance for South Africa*, 1–128.

KOF. (2020). *Globalization Report 2020*.

Konishi, N., & Ali, M. M. (2007). Risk reporting of Japanese companies and its association with corporate characteristics. *undefined*, *4*(3), 263–285. https://doi.org/10.1504/IJAAPE.2007.016281

Kor, Y. Y. (2006). Direct and interaction effects of top management team and board compositions on R&D investment strategy. *Strategic Management Journal*, *27*(11), 1081–1099. https://doi.org/10.1002/SMJ.554

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597–607. https://doi.org/10.1016/J.IM.2003.08.001

Kravet, T., & Muslu, V. (2013). Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies*, *18*(4), 1088–1122. https://doi.org/10.1007/s11142-013-9228-9

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/J.JISA.2014.09.005

Kühn, A. L., Stiglbauer, M., & Fifka, M. S. (2018). Contents and Determinants of Corporate Social Responsibility Website Reporting in Sub-Saharan Africa: A Seven-Country Study. En *Business and Society* (Vol. 57, Número 3).

https://doi.org/10.1177/0007650315614234

La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (1999). Corporate Ownership Around the World. *The Journal of Finance*, *54*(2), 471–517. https://doi.org/10.1111/0022-1082.00115

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., & Vishny, R. (2000). Investor protection and corporate governance. *Journal of Financial Economics*, *58*(1–2), 3–27. https://doi.org/10.1016/s0304-405x(00)00065-9

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. *Journal of Political Economy*, *106*(6), 1113–1155. https://doi.org/10.1086/250042

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., & Vishny, R. W. (1997). Legal Determinants of External Finance. *The Journal of Finance*, *52*(3), 1131–1150. https://doi.org/10.1111/J.1540-6261.1997.TB02727.X

Lajili, K., & Zéghal, D. (2005). A content analysis of risk management disclosures in canadian annual reports. *Canadian Journal of Administrative Sciences*, *22*(2), 125–142. https://doi.org/10.1111/j.1936-4490.2005.tb00714.x

Larmou, S., & Vafeas, N. (2009). *The relation between board size and firm performance in firms with a history of poor operating performance*. https://doi.org/10.1007/s10997-009-9091-z

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*. https://doi.org/10.1109/PCCC.2016.7820663

Lee, R. P., Chen, Q., & Hartmann, N. N. (2016). Enhancing Stock Market Return with New Product Preannouncements: The Role of Information Quality and Innovativeness. *Journal of Product Innovation Management*, *33*(4), 455–471. https://doi.org/10.1111/JPIM.12284

Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, *8*(4), 1–15. https://doi.org/10.3390/risks8040128

Lernia, C. Di, Hardy, C., & Dori, A. (2020). *Cyber-related Risk Disclosure in Australia: Evidence from the ASX200 Journal Title: Company and Securities*. *5*, 23–29.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/J.ACCINF.2018.06.003

Li, W., & Zhang, R. (2010). Corporate Social Responsibility, Ownership Structure, and Political Interference: Evidence from China. *Journal of Business Ethics*, *96*(4), 631–645. https://doi.org/10.1007/s10551-010-0488-z

Liesen, A., Hoepner, A. G., Patten, D. M., & Figge, F. (2015). Does stakeholder pressure influence corporate GHG emissions reporting? Empirical evidence from Europe. *Accounting, Auditing and Accountability Journal*, *28*(7), 1047–1074. https://doi.org/10.1108/AAAJ-12-2013-1547

Lim, S., Matolcsy, Z., & Chow, D. (2007). The Association between Board Composition

and Different Types of Voluntary Disclosure. *European Accounting Review*, *16*(3), 555–583. https://doi.org/10.1080/09638180701507155

Linck, J. S., Netter, J. M., & Yang, T. (2008). The determinants of board structure. *Journal of Financial Economics*, *87*(2), 308–328. https://doi.org/10.1016/J.JFINECO.2007.03.004

Linsley, P. M., & Shrives, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK companies. *The British Accounting Review*, *38*(4), 387–404. https://doi.org/10.1016/J.BAR.2006.05.002

Lippmann, W. (1914). *Drift and mastery : an attempt to diagnose the current unrest*. Prentice-Hall.

Lipton, M., & Lorsch, J. W. (1992). A modest proposal for improved corporate governance: Business source. *Business Lawyer*, *42*(1), 59–78. http://web.a.ebscohost.com.eserv.uum.edu.my/bsi/detail?vid=19&sid=e3a1315c-d940-4744-b224-1ce498b43ead@sessionmgr4005&hid=4114&bdata=JnNpdGU9YnNpLWxpdmU=#db=bth&AN=5963897

Lopes, P. T., & Rodrigues, L. L. (2007). Accounting for financial instruments: An analysis of the determinants of disclosure in the Portuguese stock exchange. *The International Journal of Accounting*, *42*(1), 25–56. https://doi.org/10.1016/J.INTACC.2006.12.002

Loughran, T., & Mcdonald, B. (2011). When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. *Journal of Finance*, *66*(1), 35–65. https://doi.org/10.1111/j.1540-6261.2010.01625.x

Luo, L., Tang, Q., & Lan, Y. C. (2013). Comparison of propensity for carbon disclosure between developing and developed countries: A resource constraint perspective. *Accounting Research Journal*, *26*(1), 6–34. https://doi.org/10.1108/ARJ-04-2012-0024

Luo, Y. (2005). Corporate governance and accountability in multinational enterprises: Concepts and agenda. En *Journal of International Management* (Vol. 11, Número 1 SPEC. ISS., pp. 1–18). Elsevier Inc. https://doi.org/10.1016/j.intman.2004.11.001

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan management review*, *20*(1), 61–74.

Mahmood, M., & Orazalin, N. (2017). Green governance and sustainability reporting in Kazakhstan's oil, gas, and mining sector: Evidence from a former USSR emerging economy. *Journal of Cleaner Production*, *164*, 389–397. https://doi.org/10.1016/J.JCLEPRO.2017.06.203

Mallin, C. (2006). *Handbook on International Corporate Governance*.

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*(3), 435–452. https://doi.org/10.1111/RMIR.12109

Marshall, A., & Weetman, P. (2007). Modelling Transparency in Disclosure: The Case of

Foreign Exchange Risk Management. *Journal of Business Finance & Accounting*, *34*(5–6), 705–739. https://doi.org/10.1111/j.1468-5957.2007.02007.x

Marston, C. L., & Shrives, P. J. (1991). The use of disclosure indices in accounting research: A review article. En *The British Accounting Review* (Vol. 23, Número 3, pp. 195–210). Academic Press. https://doi.org/10.1016/0890-8389(91)90080-L

Masud, M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*. https://doi.org/10.1108/JAEE-07-2021-0237

Mayor Gómez, R. (2016). *Contenido y novedades del reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)*. Gabilex. Revista del gabinete jurídico de Castilla la Mancha.

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/RMIR.12169

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *Geneva Papers on Risk and Insurance: Issues and Practice*, *45*(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Meftah Gerged, A., Beddewela, E. S., Christopher, |, & Cowton, J. (2021). *Does the quality of country-level governance have an impact on corporate environmental disclosure? Evidence from Gulf Cooperation Council countries*. https://doi.org/10.1002/ijfe.2469

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Melis, A. (2006). Corporate Governance in Italy. En *Handbook on international Corporate Governance*.

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security*, *73*, 87–101. https://doi.org/10.1016/J.COSE.2017.10.009

Merriam -Webster. (2021). *Cybersecurity | Definition of Cybersecurity*. Merriam-Webster.com Dictionary, Merriam-Webster. https://www.merriam-webster.com/dictionary/cybersecurity

Meyer, J. W., & Rowan, B. (1977). Slett denne Institutionalized Organizations : Formal Structure as Myth and Ceremony. *American Journal of Sociology*, *83*(2), 340–363.

Middleton, B. (2017). *A History of Cyber Security Attacks 1980 to present* (T. & Francis (Ed.)).

Mintzberg, H. (1984). Who Should Control the Corporation?: *http://dx.doi.org/10.2307/41165115*, *27*(1), 90–115.

https://doi.org/10.2307/41165115

Mirkovic, J., Reiher, P., & Hall, B. (2004). *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms **.

Mitra, S., & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *https://doi.org/10.1287/isre.2015.0587*, *26*(3), 565–584. https://doi.org/10.1287/ISRE.2015.0587

Mokhtar, E. S., & Mellett, H. (2013). Competition, corporate governance, ownership structure and risk reporting. *Managerial Auditing Journal*, *28*(9), 838–865. https://doi.org/10.1108/MAJ-11-2012-0776/FULL/PDF

Moosa, I. A. (2007). Operational Risk: A Survey. *Financial Markets, Institutions & Instruments*, *16*(4), 167–200. https://doi.org/10.1111/J.1468-0416.2007.00123.X

Morse, E. A., Raval, V., & Wingender, J. R. (2018). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. En *Business Lawyer* (Vol. 73, Número 1, pp. 1–34). American Bar Association. https://doi.org/10.2139/ssrn.2711439

Moumen, N., Ben Othman, H., & Hussainey, K. (2016). Board structure and the informativeness of risk disclosure: Evidence from MENA emerging markets. *Advances in Accounting*, *35*, 82–97. https://doi.org/10.1016/J.ADIAC.2016.09.001

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*(1), 11–26. https://doi.org/10.1016/J.DSS.2013.04.004

Muñoz-Izquierdo, N., Segovia-Vargas, M. J., Camacho-Miñano, M. del M., & Pascual-Ezama, D. (2019). Explaining the causes of business failure using audit report disclosures. *Journal of Business Research*, *98*, 403–414. https://doi.org/10.1016/J.JBUSRES.2018.07.024

NACD. (2009). *Report of the NACD blue ribbon commission. Risk governance: balancing risk and reward*. https://www.wlrk.com/docs/1605831_1.pdf

Nader, R., Green, M. J., & Seligman, J. (1976). *Taming the giant corporation*. 312.

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *https://doi.org/10.1080/23738871.2016.1157619*, *1*(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

NCSC. (2022). *Essential Topics - NCSC.GOV.UK*. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious Software Threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 793–813. https://doi.org/10.1007/978-3-319-78440-3_35

NICCS. (2017). *Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies*. Explore terms: a glossary of common cybersecurity terminology. https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C ( 2017 )

Nielsen, S., & Huse, M. (2010). The Contribution of Women on Boards of Directors: Going beyond the Surface. *Corporate Governance: An International Review*, *18*(2), 136–148. https://doi.org/10.1111/J.1467-8683.2010.00784.X

NIST. (2020). NIST Privacy Framework. En *January 16, 2020*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

NITS. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

Ntim, C. G., Lindop, S., & Thomas, D. A. (2013). Corporate governance and risk reporting in South Africa: A study of corporate risk disclosures in the pre- and post-2007/2008 global financial crisis periods. *International Review of Financial Analysis*, *30*, 363–383. https://doi.org/10.1016/j.irfa.2013.07.001

Nwosu, A. U., Goyal, S. B., & Bedi, P. (2020). Blockchain Transforming Cyber-Attacks: Healthcare Industry. *Advances in Intelligent Systems and Computing*, *1372 AISC*, 258–266. https://doi.org/10.1007/978-3-030-73603-3_24

O'Reilly, C. A., Caldwell, D. F., & Barnett, W. P. (1989). Work Group Demography, Social Integration, and Turnover. *Administrative Science Quarterly*, *34*(1), 21. https://doi.org/10.2307/2392984

OAS; ISA. (2020). *Manual de supervisión de riesgos cibernéticos para juntas corporativas*. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

OAS. (2019). Challenges of cyber risk in the financial sector for Colombia and Latin America. *Asobancaria*, 170. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Ocasio, W., & Joseph, J. (2005). Cultural adaptation and institutional change: The evolution of vocabularies of corporate governance, 1972–2003. *Poetics*, *33*(3–4), 163–178. https://doi.org/10.1016/J.POETIC.2005.10.001

OCDE. (2004). Directrices de la OCDE para la seguridad de sistemas y redes de información. En *Directrices de la OCDE para la seguridad de sistemas y redes de información*. https://doi.org/10.1787/9789264065819-es

OCDE. (2016). *Principios de Gobierno Corporativo de la OCDE y del G20*. https://doi.org/10.1787/9789264259171-es

OCIE. (2020). *OCIE Cybersecurity and Resiliency Obervations 2020*. www.sec.gov/spotlight/cybersecurity.

OECD. (1999). *OECD Principles of Corporate Governance Principles of*.

OECD. (2011). *OECD Guidelines for Multinational Enterprises 2011 Edition*. https://doi.org/10.1787/9789264115415-en

OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity. En *Digital Security Risk Management for Economic and Social Prosperity*. https://doi.org/10.1787/9789264245471-en

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/J.1539-6924.2010.01478.X

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011). Risk-related disclosures by non-finance companies: Portuguese practices and disclosure characteristics. *Managerial Auditing Journal*, *26*(9), 817–839. https://doi.org/10.1108/02686901111171466

Oliveira, J., Serrasqueiro, R., & Mota, S. N. (2018). Determinants of risk reporting by Portuguese and Spanish non-finance companies. *European Business Review*, *30*(3), 311–339. https://doi.org/10.1108/EBR-04-2017-0076/FULL/PDF

Oliver, C. (1991). *Strategic Responses to Institutional Processes*. *16*(1), 145–179.

ONU. (2011). *Developing countries most vulnerable to cyberattacks – UN*. https://news.un.org/en/story/2011/12/397922

Orman, H. (2003). The Morris worm: a fifteen-year perspective. *IEEE Security & Privacy*, *1*(5), 35–43. https://doi.org/10.1109 / MSECP.2003.1236233

Ortiz, E., & Clavel, J. G. (2006). Disclosures indexes: a propose to improve the metodology applied to the case of Human Resources disclosure included in Form 20-F. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, *35*(128), 87–113. https://doi.org/10.1080/02102412.2006.10779574

Packard, N. (2020). Three kinds of demand pull for the ARPANET into the Internet. *http://www.editorialmanager.com/cogentsocsci*, *6*(1). https://doi.org/10.1080/23311886.2020.1720565

Parker, D. B. (2007). The dark side of computing: SRI International and the study of computer crime. *IEEE Annals of the History of Computing*, *29*(1), 3–15. https://doi.org/10.1109/MAHC.2007.15

Patelli, L., & Prencipe, A. (2007). The relationship between voluntary disclosure and independent directors in the presence of a dominant shareholder. *European Accounting Review*, *16*(1), 5–33. https://doi.org/10.1080/09638180701265820

PCAOB. (2014). *Standing Advisory Group meeting cybersecurity*.

Perez-Batres, L. A., Miller, V. V, & Pisani, M. J. (2010). CSR, Sustainability and the Meaning of Global Reporting for Latin American Corporations. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-010-0614-y

Pfeffer, Jeffrey; Salancik, G. (1978). *The External Control of Organizations: A Resource Dependence Perspective by :: SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496213

Pitrakkos, P., & Maroun, W. (2019). Evaluating the quality of carbon disclosures. *Sustainability Accounting, Management and Policy Journal*, *11*(3), 553–589. https://doi.org/10.1108/SAMPJ-03-2018-0081

Plumlee, M., Brown, D., Hayes, R. M., & Marshall, R. S. (2015). Voluntary environmental disclosure quality and firm value: Further evidence. *Journal of Accounting and*

*Public Policy*, *34*(4), 336–361. https://doi.org/10.1016/J.JACCPUBPOL.2015.04.004

Porrúa, M., & Contreras B. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*.

Power, M. (2004). The risk management of everything. *Journal of Risk Finance*, *5*(3), 58–65. https://doi.org/10.1108/eb023001

Prado-Lorenzo, J. M., Rodríguez-Domínguez, L., Gallego-Álvarez, I., & García-Sánchez, I. M. (2009). Factors influencing the disclosure of greenhouse gas emissions in companies world-wide. *Management Decision*, *47*(7), 1133–1157. https://doi.org/10.1108/00251740910978340

Pucheta-Martínez, M. C., & Gallego-Álvarez, I. (2019). An international approach of the relationship between board attributes and the disclosure of corporate social responsibility issues. *Corporate Social Responsibility and Environmental Management*, *26*(3), 612–627. https://doi.org/10.1002/CSR.1707

PwC. (2022). *2022 Global Digital Trust Insights*.

PWC. (2018a). *2018 Global Investor Survey 2018: Anxious Optimism in a Complex World*.

PWC. (2018b). *Better Oversee Cyber Risk*. *November*.

PWC. (2018c). *Rethinking cybersecurity disclosures to investors - What executives and boards need to know about the SEC's guidance: June 2018*. www.pwc.com/cybersecurity

PWC. (2018d). *US2018-07: SEC issues interpretive guidance on cybersecurity disclosures*. https://viewpoint.pwc.com/dt/us/en/pwc/in_briefs/2018/2018__7_US/us201807_sec_issues__US.html

PWC. (2021). *Encuesta Global Digital Trust Insights 2021 Contenido*.

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Rel ated Disclosure. *Journal of Business Ethics*, *1*, 3. https://doi.org/10.1007/s10551-020-04717-9

RAE ASALE. (2020). *Diccionario de la lengua española*. Edición 2020. https://dle.rae.es/cibernético?m=form

Rainer, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, *8*(1), 129–147. https://doi.org/10.1080/07421222.1991.11517914

Rajgopal, S. (1999). Early evidence on the informativeness of the SEC's market risk disclosures: The case of commodity price risk exposure of oil and gas producers. *Accounting Review*, *74*(3), 251–280. https://doi.org/10.2308/accr.1999.74.3.251

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rankin, M., Windsor, C., & Wahyuni, D. (2011). An investigation of voluntary corporate greenhouse gas emissions reporting in a market governance system: Australian evidence. *Accounting, Auditing and Accountability Journal*, *24*(8), 1037–1070. https://doi.org/10.1108/09513571111184751

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121–139. https://doi.org/10.1287/ISRE.1080.0174

Reid, R., & Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies. *Information Security South Africa (ISSA)*, 1–7. https://doi.org/978-1-4799-3383-9

Renn, B. O. (2008). Risk Governance new & Forthcoming Titles. En *Sustainable Development*. https://www.routledge.com/Risk-Governance-Coping-with-Uncertainty-in-a-Complex-World/Renn/p/book/9781844072927

Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering and System Safety*, *59*(1), 49–62. https://doi.org/10.1016/S0951-8320(97)00119-1

Rennekamp, K. (2012). Processing Fluency and Investors' Reactions to Disclosure Readability. *Journal of Accounting Research*, *50*(5), 1319–1354. https://doi.org/10.1111/J.1475-679X.2012.00460.X

Reverte, C. (2009). Determinants of corporate social responsibility disclosure ratings by Spanish listed firms. *Journal of Business Ethics*, *88*(2), 351–366. https://doi.org/10.1007/s10551-008-9968-9

Rhodes, M. J. (2010). Information Asymmetry and Socially Responsible Investment. *Journal of Business Ethics*, *95*(1), 145–150. https://doi.org/10.1007/s10551-009-0343-2

Ripley, W. Z. (1927). *Main Street and Wall Street*. https://www.amazon.es/Main-Street-Wall-William-Ripley/dp/0914348078

Rivera-Arrubla, Y. A., Zorio-Grima, A., & García-Benau, M. A. (2017). Integrated reports: Disclosure level and explanatory factors. *Social Responsibility Journal*, *13*(1), 155–176. https://doi.org/10.1108/SRJ-02-2016-0033

RobecoSAM. (2018). *The sustainability yearbook 2018*. https://www.comunicarseweb.com/sites/default/files/the_sustainability_yearbook_2018_spanish.pdf

Roberts, L. G. (1988). The ARPANET & Computer Networks. *Proceedings of the ACM Conference on The history of personal workstations*. https://doi.org/10.1145/12178

Rodríguez-Ariza, L., Frías Aceituno, J. V., & García Rubio, R. (2014). The board of directors and the sustainability report. *Revista de Contabilidad-Spanish Accounting Review*, *17*(1), 5–16. https://doi.org/10.1016/j.rcsar.2013.02.002

Rogers, E. (2003). Review Diffusion of Innovations, by Everett Rogers (1995). *Stanford University*, *1995*, 5. http://web.stanford.edu/class/symbsys205/Diffusion of Innovations.htm

Rose, C. (2007). Does female board representation influence firm performance? The Danish evidence. *Corporate Governance: An International Review*, *15*(2), 404–413. https://doi.org/10.1111/J.1467-8683.2007.00570.X

Ross, S. A. (1977). Determination of financial structure: the incentive- signalling approach. *Bell J Econ*, *8*(1), 23–40. https://doi.org/10.2307/3003485

Roundtable, B. (1978). The Role and Composition of the Board of Directors of the Large Publicly Owned Corporation — Statement of the bussiness Roundtable. *The Roundtable*, *33*(4), pp . 2083-2113. https://www.jstor.org/stable/40685901?seq=1

Rowe, D. C., Ekstrom, J. J., & Lunt, B. M. (2012). Cyber-Security, IAS and the Cyber Warrior. *The Colloquium for Information Systems Security Education*.

Rupley, K. H., Brown, D., & Marshall, S. (2017). Evolution of corporate reporting: From stand-alone corporate social responsibility reporting to integrated reporting. *Research in Accounting Regulation*, *29*(2), 172–176. https://doi.org/10.1016/J.RACREG.2017.09.010

S&P. (2020). *América Latina*.

Salet, H. A. (2004). *Delaware ' s Good Faith*. *89*(2).

Sánchez, I. M. G., Domínguez, L. R., & Álvarez, I. G. (2011). Corporate governance and strategic information on the internet: A study of Spanish listed companies. *Accounting, Auditing and Accountability Journal*, *24*(4), 471–501. https://doi.org/10.1108/09513571111133063

Santiago Castro, M., Brown, C. J., & Baéz, A. (2009). Prácticas de Gobierno Corporativo en América Latina. *Revista Latinoamericana de Administración*, *43*, 26–40. http://revistaacademia.cladea.org

Sargent, John & Ghaddar, S. (2001). *International Success of Business Groups as an Indicator of National Competitiveness The Mexican Example*. https://www.tandfonline.com/doi/abs/10.1300/J140v02n03_05

SASB. (2021a). *Estándares SASB*. https://www.sasb.org/standards/download/

SASB. (2021b). *SASB Materiality Map*. https://materiality.sasb.org/

Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *Proceedings - International Conference on Distributed Computing Systems*, *2016-August*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Scaltrito, D. (2016). Voluntary disclosure in Italy: Firm-specific determinants an empirical analysis of Italian listed companies. *EuroMed Journal of Business*, *11*(2), 272–303. https://doi.org/10.1108/EMJB-07-2015-0032

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition

of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/https://doi.org/10.15394/jdfsl.2017.1476

Schubert, D; Cedarbaum, J and Schloss, W. (2015). The SEC's Two Primary Theories in Cybersecurity Enforcement Actions. *The Cybersecurity Law Report*, *1*(1), 39–70.

Scott, W. R. (2008). Approaching adulthood: The maturing of institutional theory. *Theory and Society*, *37*(5), 427–442. https://doi.org/10.1007/s11186-008-9067-z

SEC. (1997). Disclosure of Accounting Policies for Derivative Financial Instruments, and Derivative Commodity Instruments and Disclosure of Quantitative and Qualitative Information about Market Risk Inherent in Derivative Financial Instruments, Other Financial Instrum. *Federal Register*, *62*(27), 6044–6079. https://www.federalregister.gov/documents/1997/02/10/97-2991/disclosure-of-accounting-policies-for-derivative-financial-instruments-and-derivative-commodity

SEC. (2005a). *Release #33-8591: Securities Offering Reform (Section VII: Additional Exchange act Disclosure Provisions)* (Número 1294).

SEC. (2005b). *Staff Statement on Management's Report on Internal Control Over Financial Reporting*. https://www.sec.gov/info/accountants/stafficreporting.htm

SEC. (2017). *Prospectus summary, risk factors § 229.503 (Item 503)*. 473–475. https://doi.org/10.4135/9781608712380.n519

SEC. (2018a). *Federal Register Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures

SEC. (2018b). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

SEC. (2020). *17 CFR § 229.105 - (Item 105) Risk factors*. https://www.law.cornell.edu/cfr/text/17/229.105

SEC. (2021a). *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures*. https://www.sec.gov/news/press-release/2021-169

SEC. (2021b). *SEC Charges Issuer With Cybersecurity Disclosure Controls Failures*. https://www.sec.gov/news/press-release/2021-102

SEC. (2022). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. *13*(34), 1–204.

Security Boulevard. (2021). *How Offensive AI Can Disarm Cybersecurity*. https://securityboulevard.com/2021/06/how-offensive-ai-can-disarm-cybersecurity/

Shankar, K. S. (1977). *The Total Computer Security Problem: An overview*.

Shleifer, A., Vishny, R. W., Diamond, D., Easterbrook, F., Harris, M., Hellwig, M., Hines, J., Jonsson, T., Kaplan, S., Porta, R. La, Lopez-De-Silanes, F., Rajan, R., Scharfstein, D., Stulz, R., & Zingales, L. (1997). A Survey of Corporate Governance. *The Journal*

*of Finance*, *52*(2), 737–783. https://doi.org/10.1111/J.1540-6261.1997.TB04820.X

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Security Management Handbook, Sixth Edition*, 357–380. https://doi.org/10.1201/9781420072419-28

Sinha, T., & Vaughan, E. J. (1994). Fundamentals of Risk and Insurance. En *The Journal of Risk and Insurance* (Vol. 61, Número 2). https://doi.org/10.2307/253725

Siponen, M. T., & Oinas-Kukkonen, H. (2007). *A Review of Information Security Issues and Respective Research Contributions*.

Skinner, D. J. (1997). Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics*, *23*(3), 249–282. https://doi.org/10.1016/S0165-4101(97)00010-4

Slovic, P. (1987). Perception of Risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/SCIENCE.3563507

Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations. Oxford: UK: Clarendon Press.*

Sofistic, C. (2017). *Breve historia de la Ciberseguridad*. https://www.sofistic.com/blog-Ciberseguridad/la-breve-historia-de-la-Ciberseguridad/

Solomon, J. (2010). *Corporate governance and accountability*. 414.

Solomon, J. F., Solomon, A., Norton, Si. D., & Joseph, N. L. (2000). A conceptual framework for corporate risk disclosure emerging from the agenda for corporate goverance reform. *The British Accounting Review*, *32*(4), 447–478. https://doi.org/10.1006/bare.2000.0145

Solomon, Jill. (2019). *Corporate Governance and Accountability* (5TH ed.). John Wiley.

Souppaya, M., & Scarfone, K. (2013). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. https://doi.org/10.6028/NIST.SP.800-83R1

Spence, M. (1973). Job Market Signaling. En *The Quarterly Journal of Economics* (Vol. 87, Número 3). https://www.sciencedirect.com/science/article/pii/B9780122148507500255

Spence, M. (2002). La señalización y la estructura informativa de los mercados. *RAE: Revista Asturiana de Economía*, *25*, 49–94.

Srinidhi, B., Gul, F. A., & Tsui, J. (2011). Female Directors and Earnings Quality*. *Contemporary Accounting Research*, *28*(5), 1610–1644. https://doi.org/10.1111/J.1911-3846.2011.01071.X

Stapledon, G. (2006). The development of corporate governance in Australia. En *Handbook on International Corporate Governance*.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29.

https://doi.org/10.1016/j.aos.2018.04.005

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. En *Politics and Governance* (Vol. 6, Número 2, pp. 1–4). Cogitatio Press. https://doi.org/10.17645/pag.v6i2.1569

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/J.SSCI.2020.105143

Subcommittee of Capital Markets; Capital Markets Committee, Capital Financial and, & Federation Japan Business. (2022). *Improve the effectiveness of the revised Corporate Governance Code*. https://www.keidanren.or.jp/policy/2022/047.pdf

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review*, *20*(3), 571. https://doi.org/10.2307/258788

Superintendencia del Mercado de Valores. (2013). *Código De Buen Gobierno Corporativo Para Las Sociedades Peruanas 2013*.

SuperSociedades, Confecámaras, & CCB. (2020). *Guía de Buenas Prácticas de Gobierno Corporativo para Empresas Competitivas, Productivas y Perdurables*.

Szegö, G. (2002). Measures of risk. *Journal of Banking & Finance*, *26*, 1253–1272. https://doi.org/10.1016/S1548-5315(11)70388-6

Szulc, T., & American Assembly. (1970). *The United States and the Caribbean*. 212.

Tabassum, N., & Singh, S. (2020). Corporate governance and organisational performance: The impact of board structure. En *Corporate Governance and Organisational Performance: The Impact of Board Structure*. https://doi.org/10.1007/978-3-030-48527-6

Taiwo, O. J., Owowlabi, B. A., Adedokun, Y., & Ogundajo, G. (2021). Sustainability reporting and market value growth of quoted companies in Nigeria. *Journal of Financial Reporting and Accounting*, *20*(3/4), 542–557. https://doi.org/10.1108/JFRA-05-2020-0143/FULL/PDF

Taylor, G., Tower, G., & Neilson, J. (2010). Corporate communication of financial risk. *Accounting & Finance*, *50*(2), 417–446. https://doi.org/10.1111/j.1467-629X.2009.00326.x

TCFD. (2021). *TCFD Status Report*. *October*.

Terjesen, S., Sealy, R., & Singh, V. (2009). Women directors on corporate boards: A review and research agenda. *Corporate Governance: An International Review*, *17*(3), 320–337. https://doi.org/10.1111/j.1467-8683.2009.00742.x

Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments 2020 7:2*, *7*(2), 69–84. https://doi.org/10.1007/S40860-020-00115-0

Toronto Stock Exchange. (2014). Corporate Governance in Canada. *The International Corporate Governance System*, *December*, 90–100.

https://doi.org/10.1057/9781137360014_7

Trend Micro; OEA. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. 60. https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend Micro Reporte Seguridad Cibernetica y Porteccion de la Inf Critica.pdf

Tricker, R. (1978). *The independent director : a study of the non-executive director and of the audit committee*. 104. https://books.google.com/books/about/The_Independent_Director.html?hl=es&id=8aAjAQAAMAAJ

Tricker, R. (2020). The evolution of corporate governance. En *The SAGE Handbook of Corporate Governance* (Vol. 7175). https://doi.org/10.4135/9781446200995.n1

UIT. (2012). *UIT-IMPACT organizan un cibersimulacro transfronterizo para la región de los Estados Árabes*.

Unión Europea. (2016a). *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo*. Unión Europea.

Unión Europea. (2016b). Reglamento (UE) 2016/ 679. *Diario Oficial de la Unión Europea*.

Unión Europea. (2019). *REGLAMENTO (UE) 2019/881*. Diario Oficial de la Unión Europea.

Unión Internacional de Telecomunicaciones. (s. f.). *LA AGENDA SOBRE CIBERSEGURIDAD GLOBAL – ACTUALIZACION*.

Unión Internacional de Telecomunicaciones. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. *Unión Internacional de Telecomunicaciones*, *1205*, 66.

United Nations General Assembly. (2009). *Resolución 64/25*.

United States Department of Justice. (2001). The USA PATRIOT Act : Preserving Life and Liberty. *USA Department of Justice*. http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

Urrutia, F. D. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Van der Walt, N., & Ingley, C. (2003). Board Dynamics and the Influence of Professional Background, Gender and Ethnic Diversity of Directors. *Corporate Governance: An International Review*, *11*(3), 218–234. https://doi.org/10.1111/1467-8683.00320

Vaughan, E. (1997). *Risk Management*. Wileyl.

Veblen, T. (1904). *The Theory of Business Enterprise*.

Velte, P., & Stawinoga, M. (2016). Integrated reporting: The current state of empirical research, limitations and future research implications. *Journal of Management Control 2016 28:3*, *28*(3), 275–320.

https://doi.org/10.1007/S00187-016-0235-4

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*(C), 179–194. https://doi.org/10.1016/0165-4101(83)90011-3

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, L., & Tuttle, B. (2014). Using corporate social responsibility performance to evaluate financial disclosure credibility. *https://doi.org/10.1080/00014788.2014.922408*, *44*(5), 523–544. https://doi.org/10.1080/00014788.2014.922408

Wang, M. C. (2017). The relationship between firm characteristics and the disclosure of sustainability reporting. *Sustainability (Switzerland)*, *9*(4). https://doi.org/10.3390/SU9040624

Wang, T., & Hsu, C. (2013). Board composition and operational risk events of financial institutions. *Journal of Banking and Finance*, *37*(6), 2042–2051. https://doi.org/10.1016/j.jbankfin.2013.01.027

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Wang, T., Ulmer, J. R., & Kannan, K. (2013). The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities. *Journal of Organizational Computing and Electronic Commerce*, *23*(3), 200–223. https://doi.org/10.1080/10919392.2013.807712

WEF. (2017). Advancing Cyber Resilience - Principles and Tools for Boards. *World Economic Forum*, *January*, 40.

WEF. (2020a). A New Paradigm for Business of Data: Briefing paper. *World Economic Forum*, 15. http://www3.weforum.org/docs/WEF_New_Paradigm_for_Business_of_Data_Report_2020.pdf

WEF. (2021a). *Centre for Cybersecurity > Platforms | World Economic Forum*. https://www.weforum.org/platforms/the-centre-for-cybersecurity

WEF. (2021b). *Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico | foro Economico Mundial*. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

WEF. (2021c). *The Global Risks Report 2021: 16th Edition*.

WEF. (2022). *The Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022

WEF. (2023). *The Global Risks Report 2023 18th Edition*.

WEF, W. E. F. (2020b). *The Global Risks Report 2020*. https://es.weforum.org/reports/the-global-risks-report-2020

Wells, H. (2010). The Birth of Corporate Governance The traditional view dates them to 1932 with the publication of Adolf A . *Seattle University Law Review*, *33*(4), 1247–1292.

Werder, Axel ; Talaulicar, T. (2006). Corporate governance developments in Germany. En *Handbook on International Corporate Governance*.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. En *Cengage Learning*.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt. *USENIX Security Symposium*, 679–702. http://www.doug-tygar.com/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf

Williams, T. D. (2020). Epistemological Questions for Cybersecurity. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*, 1–4. https://doi.org/10.1109/CyberSecurity49315.2020.9138884

Woollacott, P. (2007). Cybercrime comes of age. *ITNOW*, *49*(2), 6–7. https://doi.org/10.1093/COMBUL/BWL110

Wuerges, A. F. E., & Borba, J. A. (2014). Fraudes contábeis: Uma estimativa da probabilidade de detecção. *Revista Brasileira de Gestao de Negocios*, *16*(52), 466–483. https://doi.org/10.7819/rbgn.v16i52.1555

Yang, A., Kwon, Y. J., & Lee, S. Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, *120*(9), 1777–1794. https://doi.org/10.1108/IMDS-10-2019-0536

Yermack, D. (1996). Higher market valuation of companies with a small board of directors. *Journal of Financial Economics*, *40*(2), 185–211. https://doi.org/10.1016/0304-405X(95)00844-5

Yeung, W. H., & Lento, C. (2018). Ownership structure, audit quality, board structure, and stock price crash risk: Evidence from China. *Global Finance Journal*, *37*, 1–24. https://doi.org/10.1016/J.GFJ.2018.04.002

Zeller, G., & Scherer, M. (2020). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*. https://doi.org/10.1007/s13385-021-00290-1

# CAPÍTULO 5. INCIDENCIA DE LAS CARACTERÍSTICAS PAÍS EN LA DIVULGACIÓN DE INFORMACIÓN SOBRE RIESGOS DE CIBERSEGURIDAD EN AMÉRICA LATINA

Según WEF (2023) los ataques cibernéticos a infraestructuras críticas, los ciberdelitos financieros, el ciber espionaje, la ciber interferencia, las ciberamenazas contra dispositivos de Internet de las cosas, los ciberataques contra sistemas de automatización y el control industrial son riesgos identificados como graves por su potencial para causar daño a la economía, la sociedad y la seguridad nacional. Según ITU (2020) corresponde al gobierno nacional tomar medidas para mitigar estos riesgos a través de la creación de políticas y regulaciones, el fomento de la cooperación intergubernamental, la mejora de la capacitación y la conciencia cibernética, el fortalecimiento de la infraestructura de seguridad y la promoción de la investigación y el desarrollo.

La medición de estos compromisos nacionales en el ámbito internacional se realiza a través del Índice Global de Ciberseguridad. El objetivo de esta iniciativa de reconocimiento mundial es ayudar a los países a mejorar el nivel de la Ciberseguridad nacional, a fin de promover las estrategias gubernamentales y el intercambio de información sobre los esfuerzos entre industrias y sectores, y ayudar a fomentar una cultura global de Ciberseguridad y su integración en el núcleo de las TI y la comunicación (ITU, 2015).

Los gobiernos de todo el mundo reconocen que la transformación digital tiene el poder de promover la prosperidad y el bienestar de sus ciudadanos (ITU, 2017). No obstante, cada país presenta un avance de acuerdo a sus condiciones nacionales particulares. Estas características institucionales reflejan diferencias entre países con respecto a la transferencia del riesgo de Ciberseguridad entre gobiernos y empresas (Falco et al., 2019). Asimismo, mantener un buen clima, con una buena gobernanza, entendida como la institucionalidad, supone que existe una gobernabilidad que, entre otros, se basa en la rendición de cuentas y en la transparencia (Young et al., 2020).

Se espera que las empresas que cotizan en bolsa, especialmente, establezcan sus prácticas de divulgación de Ciberseguridad en función de su contexto institucional (Barry et al.,2021). Desde esta perspectiva, siguiendo a estos autores y con base en la teoría institucional, se argumenta que las diferencias en el entorno institucional inciden en las revelaciones de Ciberseguridad.

En este capítulo, a partir de la aplicación del Índice de Divulgación de Ciberseguridad propuesto en el capítulo tres, se efectúa la revisión de contenido de los informes anuales y

del formulario 20 F SEC reportado por las empresas de América Latina emisoras durante el período 2016- 2020, presentando evidencia que comprueba que las características a nivel de país relacionadas con el Índice Global de Ciberseguridad, el Índice de Gobernanza Mundial (por siglas en inglés, WEF), el Índice de Globalización y el Índice de Desarrollo Humano, son determinantes en la divulgación del ciber riesgo corporativo.

Respecto a los indicadores considerados en este capítulo, primero se incorpora el Índice Global de Ciberseguridad, ya utilizado por Krishna & M.P (2021) como variable independiente para, desde la perspectiva institucional, examinar las relaciones entre el desarrollo del gobierno electrónico, el compromiso con la seguridad cibernética, el uso comercial y la prosperidad económica del país. Seguidamente, se vincula la variable de Gobernanza Nacional, en tanto que se presume que el efecto de aumento de las revelaciones de Ciberseguridad podría verse reforzado por un entorno representado con una buena gobernanza, lo que sugiere que los mecanismos de gobierno a nivel de empresa y de país ejercen efectos complementarios en las divulgaciones corporativas (Ernstberger & Grüning, 2013). La literatura precedente coincide en emplear la noción de gobernanza nacional a partir del Índice de Gobernanza Mundial WGI (Baldini et al., 2018; Barakat, AhmedBank; Hussainey, 2013; Barakat et al., 2015; Elamer et al., 2020; Ellimäki et al., 2021; Ernstberger & Grüning, 2013; Gerged et al., 2021; Meftah Gerged et al., 2021). Otros estudios han evaluado el entorno normativo e institucional (Hope, 2003; Jaggi & Low, 2000). Como tercera variable se relaciona el Índice de Globalización Mundial, respecto a la incidencia de la globalización de un país en las revelaciones corporativas. En este sentido, Ellimäki et al. (2021) obtienen que una mayor globalización aumenta la divulgación ambiental de una empresa. Por último, la variable Índice de Desarrollo Humano se convierte en un factor determinante de la divulgación de riesgos (Elamer et al., 2020; Gerged et al., 2021), por lo que también la hemos considerado en esta parte de nuestro trabajo.

Dada la inexistencia de estudios previos sobre el tema en América Latina, en este capítulo tratamos de, a partir de la teoría institucional, cerrar esta brecha y ampliar la literatura relacionada con la divulgación de información de Ciberseguridad y su relación con las características del país de pertenencia de las empresas. Para lograrlo, vinculamos variables que no se han tenido en cuenta en estudios previos sobre divulgación de información. Concretamente, consideramos el Índice Global de Ciberseguridad y el Índice de Globalización. Las variables Índice de Gobernanza Mundial y Índice de Desarrollo Humano

han sido tenidas en cuenta como variables explicativas de la divulgación de información en general, más no en Ciberseguridad.

De esta manera, el desarrollo de este capítulo se estructura, en un primer momento, a partir de la descripción de la situación actual de América Latina en torno al panorama de la Ciberseguridad, la Gobernanza, la Globalización y el Desarrollo Humano. Seguidamente, analizamos el efecto de las características del país en el nivel de divulgación de información sobre Ciberseguridad. Para ello, presentamos el marco teórico en el que se sustenta nuestra investigación a partir de la teoría institucional y la literatura previa relacionada con el tema. Enseguida se realiza la formulación de las hipótesis. La metodología precede a la exposición de los resultados y la discusión de los mismos y por último, se presentan las conclusiones de este estudio.

### 5.1. Panorama de la Ciberseguridad Nacional

El panorama mundial de la seguridad cibernética presenta unas circunstancias complejas debido a las características del fenómeno que se intenta contrarrestar y la amplia esfera de actuación en todos los sectores e industrias; esto involucra una perspectiva micro y macro, tanto en el ámbito público como privado. Según WEF (2022), a medida que las amenazas a la Ciberseguridad se multiplican, aumentan y se fusionan, es imperativo que la comunidad mundial trate a este riesgo como un desafío sistémico que requiere una toma de decisiones colectiva y una acción coordinada entre los gobiernos, el sector privado y la sociedad civil. La Ciberseguridad es un punto central que las organizaciones y las naciones atraviesan para lograr una gobernanza digital efectiva (ITU, 2018). Es un elemento fundamental que sustenta el logro de los objetivos socioeconómicos de las economías modernas (ITU, 2021).

Actualmente, la gobernanza de la transformación digital es un tema fundamental de política pública (OCDE, 2019). Existen normas internacionales y directrices para desarrollar la seguridad cibernética de una sola organización, pero es difícil encontrar herramientas integrales para los gobiernos nacionales (Vaks et al., 2020). Permitir el desarrollo de las capacidades nacionales requiere, por lo tanto, la inversión de las fuerzas políticas, económicas y sociales (ITU, 2015). Se necesitan mecanismos y estructuras institucionales eficaces a nivel nacional para hacer frente a los riesgos e incidentes cibernéticos de manera confiable (ITU, 2020). En general, “para contrarrestar las amenazas cibernéticas en rápida

evolución, se debe contar con políticas, legislación y capacitación, así como con equipos de respuesta a emergencias informáticas y unidades de ciberdelincuencia en todos los países del mundo"(IDB; OAS, 2020). Dado que Internet es transfronterizo, la legislación y la estrategia de seguridad cibernética no pueden desarrollarse de forma aislada, sino que deben tener en cuenta las tendencias en otros países (Vaks et al., 2020).

Las Conferencias de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (Busan, 2014; International Telecommunication Union, 2018) invitan a los países a apoyar las iniciativas de la UIT sobre seguridad cibernética, incluido el Índice Global de Ciberseguridad, para promover estrategias gubernamentales y el intercambio de información sobre los esfuerzos entre industrias y sectores. Precisamente, dedicamos el siguiente epígrafe al Índice Global de Ciberseguridad.

### 5.1.1. Índice Global de Ciberseguridad

El Índice Global de Ciberseguridad tiene como objetivo comprender mejor los compromisos de los países con la seguridad cibernética, identificar brechas, fomentar la incorporación de buenas prácticas y proporcionar información útil para que los países mejoren sus posturas de seguridad cibernética (ITU, 2020). El Índice, a través de un cuestionario, mapea preguntas sobre los compromisos de seguridad cibernética de los Estados miembros en cinco pilares (ITU, 2020): medidas legales; medidas técnicas; medidas organizativas; medidas de desarrollo de capacidades; medidas de cooperación. A continuación, presentamos las versiones del índice contempladas en este estudio.

**Índice Global de Ciberseguridad 2015.** A partir del trabajo conjunto de la Unión Internacional de Telecomunicaciones (UIT) con ABI Research en el período 2013-2014, se obtiene la primera iteración del Índice Global de Ciberseguridad (ITU, 2015). El proyecto es el resultado de una intensa investigación primaria y secundaria. En octubre de 2013 se envió una carta de información y un cuestionario a todos los Estados Miembros de la UIT. Tras las respuestas recibidas, con el apoyo de todos y cada uno de los Estados Miembros, la UIT publicó un informe sobre la situación mundial de la Ciberseguridad para 2014 (ITU, 2015). El modelo estadístico utilizado se basó en un análisis multicriterio, que establecía preferencias entre opciones por referencia a un conjunto explícito de objetivos identificados,

y para los cuales existen criterios medibles establecidos para evaluar la medida en que se han logrado los objetivos. Se aplicó un modelo de evaluación aditivo lineal simple. La matriz de rendimiento describe las opciones y el rendimiento de las opciones frente a cada criterio. La evaluación del desempeño individual es numérica (ITU, 2015). La puntuación de referencia se basó en los siguientes indicadores, se asignan 0 puntos donde no hay actividades; 1 punto es asignación para acción parcial; y 2 puntos para una acción más integral (ITU, 2015).

**Índice Global de Ciberseguridad 2017.** Tras los comentarios recibidos de varias comunidades, se planificó y llevó a cabo una segunda iteración del GCI esta versión (ITU, 2017). Se formuló en torno a una participación ampliada de los Estados miembros, expertos y partes interesadas de la industria como socios contribuyentes es decir, el Banco Mundial y Red Team Cyber como nuevos socios de GCI que se unen al Instituto de Política Estratégica de Australia, FIRST, Universidad de Indiana, INTERPOL, UIT-Árabe Regional Cybersecurity Center en Omán, Korea Internet & Security Agency, NTRA Egypt, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica y UNODC, quienes brindaron apoyo con el suministro de datos secundarios, activación de respuesta, análisis estadístico y apreciación cualitativa, entre otros (ITU, 2017). De acuerdo con ITU (2017) la diferencia clave en la metodología entre GCI 2015 y GCI Versión 2017 es el uso de un sistema binario en lugar de un sistema de tres niveles. El sistema binario evalúa la existencia o ausencia de una determinada actividad, departamento o medida. A diferencia de la versión 2015 de GCI, no tiene en cuenta medidas 'parciales'. La posibilidad de que los encuestados carguen documentos de respaldo y URL es una forma de proporcionar más información para corroborar la respuesta binaria. Además, se han agregado varias preguntas nuevas en cada uno de los cinco pilares para refinar la profundidad de la investigación (ITU, 2017).

**Índice Global de Ciberseguridad 2018.** En su tercera versión (ITU, 2018), el cuestionario utilizado para el GCI 2018 proporciona un valor para los 25 indicadores construidos a través de 50 preguntas binarias, precodificadas y abiertas. Esto logra el nivel requerido de granularidad y mejora la precisión y calidad de las respuestas. La diferencia clave en la metodología de las encuestas anteriores de GCI es que la estructura se modificó a preguntas con respuestas predefinidas que incluyen texto libre y preguntas abiertas en cada sección del cuestionario. Se incluyeron preguntas de opción múltiple (respuestas múltiples), y también

se proporcionó la opción de agregar más detalles para que los Estados miembros complementaran información específica que podría no haber sido capturada en las respuestas predefinidas (ITU, 2018).

**Índice Global de Ciberseguridad 2020.** En la cuarta versión (ITU, 2020) el Índice Global de Ciberseguridad se estructura en un cuestionario de 82 preguntas que proporciona un valor para los 20 indicadores. Esto aumenta aún más el nivel requerido de granularidad, y mejora de forma importante la precisión y calidad de las respuestas. Se formula en torno a los datos proporcionados por los miembros de la UIT, incluidas las personas interesadas, los expertos y las partes interesadas de la industria como socios contribuyentes. Seguidamente, se presenta una descripción de los ítems del índice, agrupados en cinco pilares.

**Pilar 1. Medidas legales.** Este pilar hace referencia a las medidas basadas en la existencia de instituciones y marcos legales que se ocupan de la ciberseguridad y el cibercrimen (ITU,2018). Según ITU (2015), estas medidas jurídicas permiten que un Estado nación establezca los mecanismos básicos de respuesta de infracciones: mediante la investigación y la persecución de los delitos y la imposición de sanciones por falta de conformidad o incumplimiento de la ley. Como afirma Vaks et al. (2020), en cada país se debe considerar cuánto está dispuesta la sociedad a ceder, y ceder el derecho a la privacidad en el ejercicio de su función de protección, es una cuestión de confianza y de orden jurídico. El ordenamiento jurídico así diseñado proporcionará los mecanismos y herramientas suficientes para generar confianza y máxima seguridad en la sociedad (Vaks et al., 2020). En este contexto, en el ámbito mundial, según el Informe ITU (2020), 167 países cuentan con algún tipo de legislación sobre Ciberseguridad, 133 con reglamento de protección de datos y 97 presentan normatividad relacionada con infraestructuras críticas. Este pilar está compuesto de dos ítems: derecho sustantivo del ciberdelito y regulación de Ciberseguridad relacionada con protección de datos e infraestructuras críticas:

(1) **Derecho sustantivo del ciberdelito.** La medición de este ítem en cada país hace referencia a la legislación relacionada con la conducta a ser definida como delito en torno a la Ciberseguridad en el ámbito nacional.
(2) **Regulación de Ciberseguridad relacionada con protección de datos e infraestructuras críticas.** Se hace referencia a la adopción legislativa del Reglamento General de Protección de Datos en el ámbito nacional.

**Pilar 2. Medidas técnicas.** Hace referencia a medidas basadas en la existencia de instituciones y marcos técnicos relacionados con la ciberseguridad (ITU,2018). Según ITU (2015) la tecnología es la primera línea de defensa contra las ciberamenazas y los agentes maliciosos en línea , y sin las medidas técnicas adecuadas y las capacidades para detectar y responder a los ciberataques, los estados nacionales y sus respectivas entidades siguen siendo vulnerables a las ciberamenazas. Entre estas medidas, se incluyen, el establecimiento de CIRT nacionales, CIRT regionales y la protección infantil. El pilar técnico se ha reestructurado para reflejar mejor cómo funcionan los CIRT (ITU, 2020). En el ámbito mundial se cuenta con 131 CIRT activos, 104 países involucrados en CIRT regional, 101 mecanismos de denuncia de protección infantil en línea. Este pilar está compuesto de cuatro ítems (CERT/CIRT/ CSIRT nacional, CERT/CIRT/ CSIRT regional, protección Infantil en línea y el marco nacional para la implementación de estándares de Ciberseguridad), a los que nos referimos a continuación.

(3) **CERT/CIRT/ CSIRT nacional.** Esta medida técnica hace referencia al establecimiento de un CIRT (Equipo de Respuesta a Incidentes Informáticos), CERT (Equipo de Respuesta a Emergencias Informáticas) o CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) nacional que proporcione las capacidades para identificar, defender, responder y gestionar amenazas cibernéticas y mejorar la seguridad del ciberespacio en el estado nación .

(4) **CERT/CIRT/ CSIRT regional.** Se considera un centro físico ubicado en un país que actúa como punto focal regional de asuntos de Ciberseguridad y entrega servicios de Ciberseguridad a los países de la región.

(5) **Protección Infantil en línea.** Este indicador mide la existencia de una agencia nacional dedicada a la Protección de la Infancia en Línea, la disponibilidad de un número de teléfono nacional para reportar problemas asociados con la niñez en línea, cualquier mecanismo técnico y capacidad implementada para ayudar a proteger a la niñez en línea, y cualquier actividad por parte del gobierno o no instituciones gubernamentales para brindar conocimiento y apoyo a las partes interesadas sobre cómo proteger a los niños en línea.

(6) **Marco nacional para la implementación de estándares de Ciberseguridad.** Este ítem evalúa la adopción de un marco (o marcos) nacional para la implementación de estándares de seguridad cibernética reconocidos internacionalmente dentro del sector público (agencias gubernamentales) y dentro de la infraestructura crítica

(incluso si es operada por el sector privado) . Estos estándares incluyen, entre otros, los desarrollados por las siguientes agencias: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, entre otros.

**Pilar 3. Medidas organizacionales**. Comprende las medidas basadas en la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a nivel nacional (ITU,2018). Según ITU (2015) las medidas organizativas y procedimentales son necesarias para la adecuada implantación de cualquier tipo de iniciativa nacional, sin una estrategia nacional, un modelo de gobernanza y un organismo supervisor, la labor de los diferentes sectores se dispersa y queda inconexa, frustrando el intento de lograr la armonixzación nacional del desarrollo de la capacidad de ciberseguridad. Este pilar se compone los siguientes tres ítems.

(7) **Estrategia Nacional de Ciberseguridad.** Una estrategia nacional para la Seguridad de las Redes y los Sistemas de Información debe mantener una infraestructura de información resistente y confiable y apuntar a garantizar la seguridad de los ciudadanos; proteger los bienes materiales e intelectuales de los ciudadanos, las organizaciones y el Estado; prevenir ciberataques contra infraestructuras críticas; y minimizar los daños y los tiempos de recuperación de los ciberataques.

(8) **Agencia Nacional de Ciberseguridad.** Las agencias nacionales deben estar presentes para implementar la estrategia y evaluar el éxito o el fracaso del plan. Una agencia responsable de implementar una estrategia/política nacional de seguridad cibernética puede incluir comités permanentes, grupos de trabajo oficiales, consejos asesores o centros interdisciplinarios .

(9) **Métricas de Ciberseguridad.** De acuerdo con el cuestionario , éste evalúa como métricas de Ciberseguridad la existencia de cualquier ejercicio de benchmarking o referencial nacional o específico del sector oficialmente reconocido que se utilice para medir el desarrollo de la Ciberseguridad, las estrategias de evaluación de riesgos, las auditorías de Ciberseguridad y otras herramientas y actividades para calificar o evaluar el desempeño resultante para futuras mejoras.

**Pilar 4. Medidas de creación de capacidades.** Medidas basadas en la existencia de programas de investigación y desarrollo, educación y capacitación, profesionales certificados y agencias del sector público que fomentan el desarrollo de capacidades (ITU, 2018). Las medidas de creación de capacidades se componen de los siguientes ítems: campañas públicas de concientización sobre seguridad cibernética, capacitación para profesionales de seguridad cibernética, apoyo a programas educativos o currículos académicos en seguridad cibernética.

(10) **Campañas públicas de concientización sobre seguridad cibernética.** Un marco de creación de capacidad para promover la Ciberseguridad debe incluir la concienciación y la disponibilidad de recursos.

(11) **Capacitación para profesionales de seguridad cibernética.** Este ítem indaga sobre la capacitación y preparación para los profesionales en Ciberseguridad.

(12) **Apoyo a programas educativos o currículos académicos en seguridad cibernética.** Los gobiernos están reconociendo la necesidad de programas educativos específicos del sector y capacitación para profesionales de Ciberseguridad.

(13) **Programas de investigación y desarrollo. Según** ITU (2020), 94 países cuentan con programas de I+D en Ciberseguridad concientización cibernética.

(14) **Industria nacional de seguridad cibernética.** Este ítem incluye acciones como la creación de portales y sitios web para promover la concienciación, la difusión de material de apoyo para educadores y el establecimiento (o incentivo) de cursos de formación profesional y programas educativos.

(15) **Desarrollo de estandarización.** Este indicador mide la existencia de un marco (o marcos) aprobado (o respaldado) por el gobierno para la implementación de estándares de seguridad cibernética reconocidos internacionalmente dentro del sector público (agencias gubernamentales) y dentro de la infraestructura crítica (incluso si es operada por el sector privado).

**Pilar 5. Medidas de Cooperación Internacional.** La cooperación internacional hace referencia a las medidas en la existencia de asociaciones, marcos cooperativos y redes de intercambio de información (ITU, 2018). Según ITU (2018), la cooperación nacional e internacional se evalúa en función del número de asociaciones, marcos de cooperación y redes de intercambio de información. Entonces, cuanto más fuertes seamos globalmente en promedio, más seguro es el ciberespacio. Además de compartir información sobre la base de

consultas, también es relevante que la cooperación se lleve a cabo a nivel operativo y técnico (Vaks et al., 2020). Debido al nivel sin precedentes de interconexión entre los estados, la Ciberseguridad es una responsabilidad compartida y un desafío transnacional. ITU (2015) define la cooperación intraestatal como cualquier asociación nacional o específica de un sector oficialmente reconocida para compartir activos de seguridad cibernética a través de las fronteras con otros estados nacionales. Una mayor cooperación puede permitir el desarrollo de capacidades de seguridad cibernética mucho más sólidas, lo que ayuda a mitigar los riesgos cibernéticos y permite una mejor investigación, aprehensión y enjuiciamiento de agentes malintencionados (ITU, 2020). La cooperación intraestatal también incluye iniciativas a nivel regional, como las implementadas por la Unión Europea, el Consejo de Europa, el Grupo de Estados del G8, la Cooperación Económica del Pacífico Asiático (APEC), la Organización de los Estados Americanos (OEA), la Asociación de Naciones del Sudeste Asiático (ASEAN), la Liga Árabe, la Unión Africana, la Organización de Cooperación de Shanghái (SCO) y los Grupos de Operaciones de Red (NOG), entre otras (ITU, 2015). Por su parte, los acuerdos bilaterales de cooperación en Ciberseguridad con otros paísesse refieren a cualquier asociación nacional o específica de un sector oficialmente reconocida para compartir información o activos de seguridad cibernética a través de las fronteras por parte del gobierno con otro gobierno extranjero, entidad regional o una organización internacional (ITU, 2018). Los datos extraídos muestran que 90 países tienen un acuerdo bilateral en Ciberseguridad, y para 37 países, sus acuerdos bilaterales incluyen tanto el intercambio de información como medidas de desarrollo de capacidades, pero no abordan la asistencia legal mutua (ITU, 2020). Específicamente, las medidas de cooperación internacional incorporan los siguientes ítems.

(16) **Participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad.** Dentro de estos mecanismos internacionales se puede incluir la ratificación de acuerdos internacionales en materia de Ciberseguridad, como el Convenio de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, o el Convenio de Budapest sobre Ciberdelincuencia.

(17) **Acuerdos multilaterales de Ciberseguridad.** Los acuerdos multilaterales se refieren a cualquier programa nacional o específico de un sector oficialmente reconocido para compartir información o activos de seguridad cibernética a través de las fronteras por parte del gobierno con múltiples gobiernos extranjeros u

organizaciones internacionales. El Informe (ITU, 2020), reporta 112 países con acuerdos multilaterales de Ciberseguridad.

(18) **Alianzas con el sector privado.** Las asociaciones público-privadas se refieren a emprendimientos entre el sector público y privado. Este indicador de rendimiento mide el número de alianzas nacionales o sectoriales oficialmente reconocidas para compartir información y activos de Ciberseguridad (personas, procesos, herramientas) entre el sector público y el privado, ya sea a nivel nacional o internacional.

(19) **Asociaciones Interinstitucionales.** Las asociaciones interinstitucionales hacen referencia a cualquier asociación entre las diversas agencias gubernamentales dentro del estado nación. Esto puede designar asociaciones para compartir información o activos entre ministerios, departamentos, programas y otras instituciones del sector público.

(20) **Acuerdos bilaterales de cooperación en materia de Ciberseguridad con otros países.** Designan alianzas nacionales o sectoriales reconocidas oficialmente y destinadas a compartir información y recursos sobre Ciberseguridad. Son concluidos por un gobierno y otro gobierno extranjero, entidad regional u organización internacional (por ejemplo, cooperación o intercambio de información, conocimientos expertos, tecnología y otros recursos). Este indicador mide también si se comparte información sobre amenazas.

### 5.1.2. Índice Global de Ciberseguridad en la esfera internacional

Dado que el resultado del Índice Global de Ciberseguridad es un índice a nivel de país y una clasificación mundial sobre la preparación para la Ciberseguridad, a partir de los informes de los años 2015, 2017, 2018 y 2020 elaborados por la Unión Internacional de Telecomunicaciones (UIT) se puede observar que el nivel de desarrollo de los diferentes pilares varía de un país a otro y que, aunque el compromiso en Europa sigue siendo muy alto, la difícil situación en las regiones de África y las Américas muestra la necesidad de un apoyo y compromiso continuo (ITU, 2017). En general, los compromisos relacionados con la Ciberseguridad a menudo se distribuyen de manera desigual, ya que los países se desempeñan bien en algunos pilares y menos en otros (ITU, 2017). Según el informe ITU (2020), los países que ocupan los primeros diez lugares en el ranking de Ciberseguridad,

son: Estados Unidos, Reino Unido, Arabia Saudita, Estonia, Corea, Singapur, España, Rusia, Emiratos Árabes, Malasia, Lituania, Japón, Canadá, Francia e India.

La medición de la Ciberseguridad, a partir de la aplicación del Índice Global de Ciberseguridad en el ámbito mundial permite observar algunos resultados a nivel nacional y regional. El informe Global Cybersecurity Index ITU (2020) muestra que muchos países promulgaron nuevas leyes y regulaciones de Ciberseguridad para abordar áreas como la privacidad, el acceso no autorizado y la seguridad en línea.

La puntuación de referencia se basó en los siguientes indicadores, cada uno de los cuales tiene la misma ponderación:

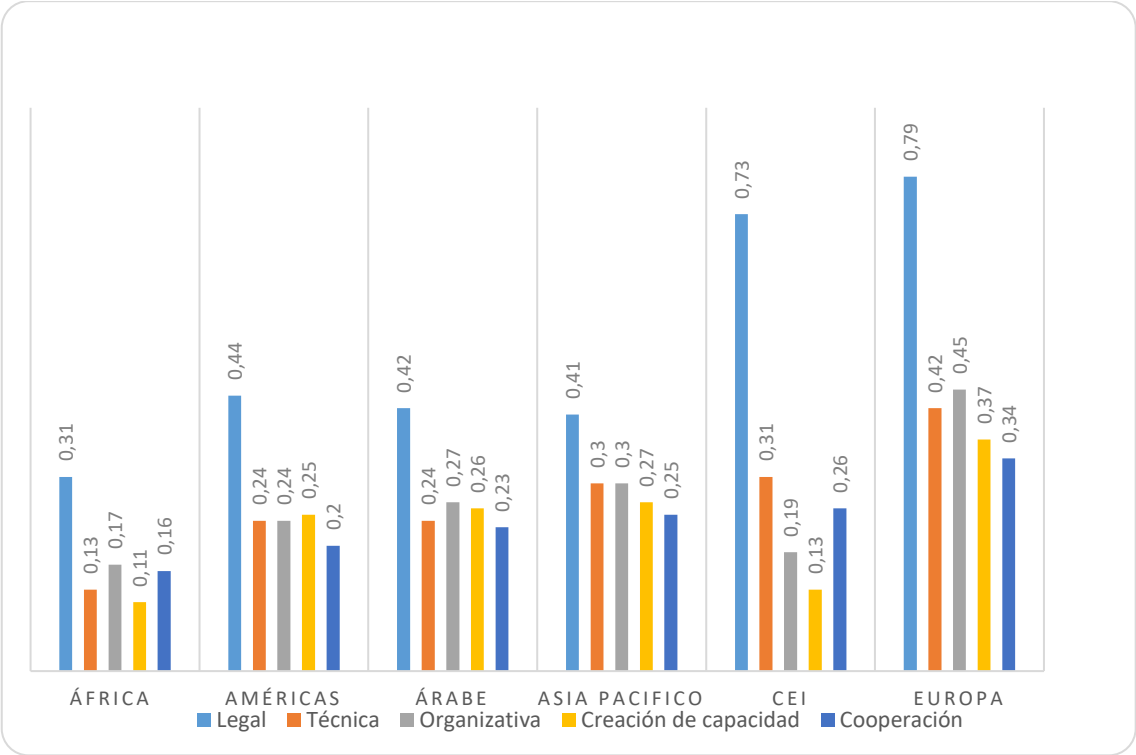
**Medidas legales** (4): legislación penal (2), regulación y cumplimiento (2).
**Medidas Técnicas** (6): CERT CIRT SCIRT (2), Estándares (2) y Certificación (2).
**Medidas Organizacionales** (6): Hoja de ruta para la gobernanza (2), Agencia Responsable (2), Benchmarking nacional (2).
**Desarrollo de capacidades** (8)**:** Desarrollo de estandarización (2), Desarrollo de mano de obra (2), Certificación profesional (2), Certificación de la agencia (2).
**Cooperación** (6): Cooperación intraestatal (2), Cooperación intra agencial (2) Asociaciones público-privadas (2).

El punto de referencia utilizado será el puntaje del país hipotético que maximiza los puntos de preparación general (30). El índice compuesto resultante oscilará entre cero (la peor preparación posible) y 1 (el punto de referencia): se asignan 0 puntos donde no hay actividades; 1 punto es asignación para acción parcial; y 2 puntos para una acción más integral.

A continuación, se presenta la información consolidada de forma comparativa por región y por cada uno de los pilares. La Figura 21, a partir del informe ITU (2015), nos deja ver que Europa presentó el índice más alto en la totalidad de pilares evaluados, mientras África reportó la ponderación más baja. También se observa, como desde el ámbito global el pilar de aspectos legales repunta en todas las regiones y las dimensiones de desarrollo de capacidades y cooperación, obtienen los valores más bajos. En general, el puntaje más alto

lo alcanza Europa con el pilar de aspectos legales (0,79) y el más bajo, África con el desarrollo de capacidades (0,11).

**Figura 21. Puntajes promedio de los pilares por región 2015**

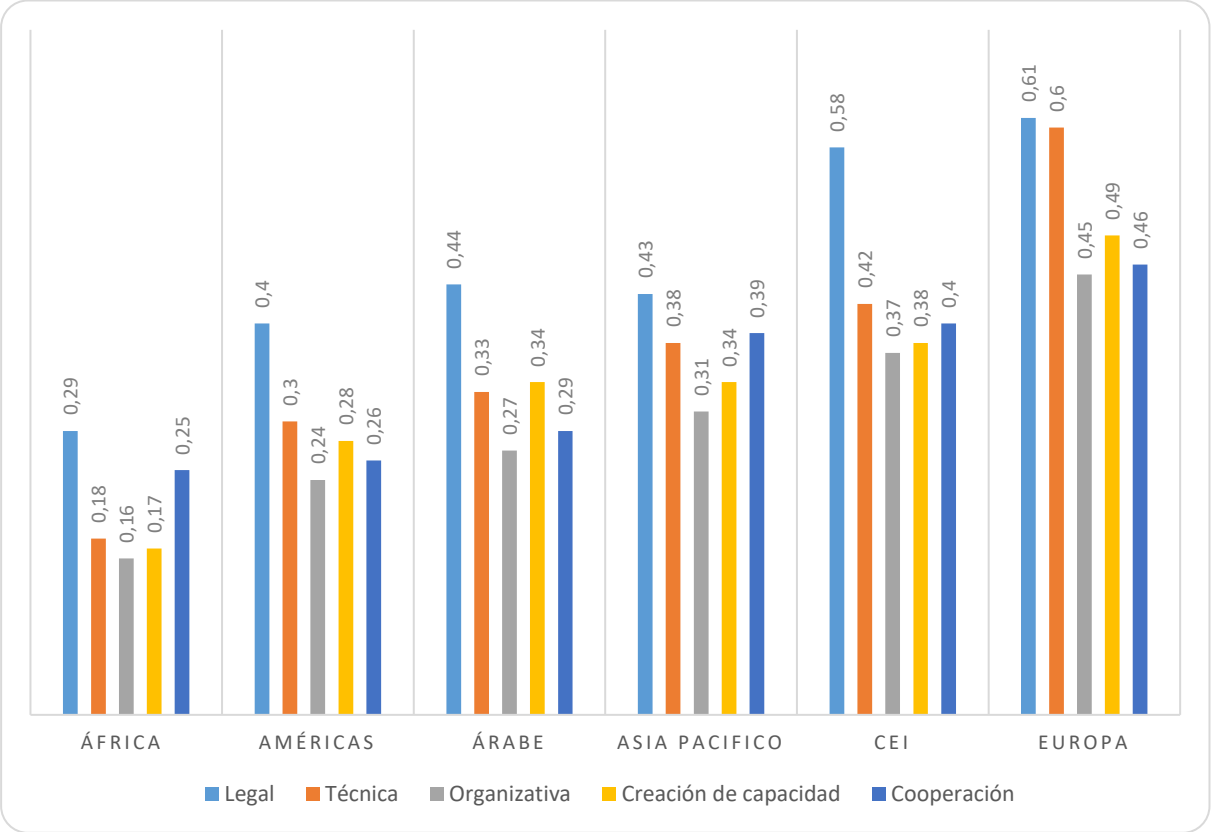



Nota. Elaborado con base en conjunto de datos edición ITU (2015)

Dos años después, el Informe ITU (2017) presenta algunos avances como lo ilustra la Figura 22. Gran parte de las regiones presentan una puntuación media para los diferentes pilares, mientras Europa refleja una puntuación más alta, por lo tanto, un avance importante y diferenciador. El puntaje más alto lo registra Europa (0,61) en el pilar de medidas legales y el más bajo África (0,16) en medidas organizacionales. Con estas diferencias entre regiones existe un gran abismo en la preparación cibernética en todo el mundo. Esta brecha existe entre y dentro de las regiones (ITU, 2017). Como se puede observar la segunda posición la ocupa la Comunidad de Estados Independientes, seguida de Asia Pacífico. Ahora bien, para América podemos ver cómo el pilar más alto lo representa el aspecto legal (0,44), tecnología y medidas organizativas tienen el mismo puntaje (0,24), yel pilar de cooperación presenta la valoración más baja (0,20). En general, la región de América Latina se ubica en el penúltimo

lugar con un índice global de (0,26), mientras África reporta (0,16), la región árabe (0,23), Asia Pacifico (0,25), CEI (0,26) y Europa (0,34).

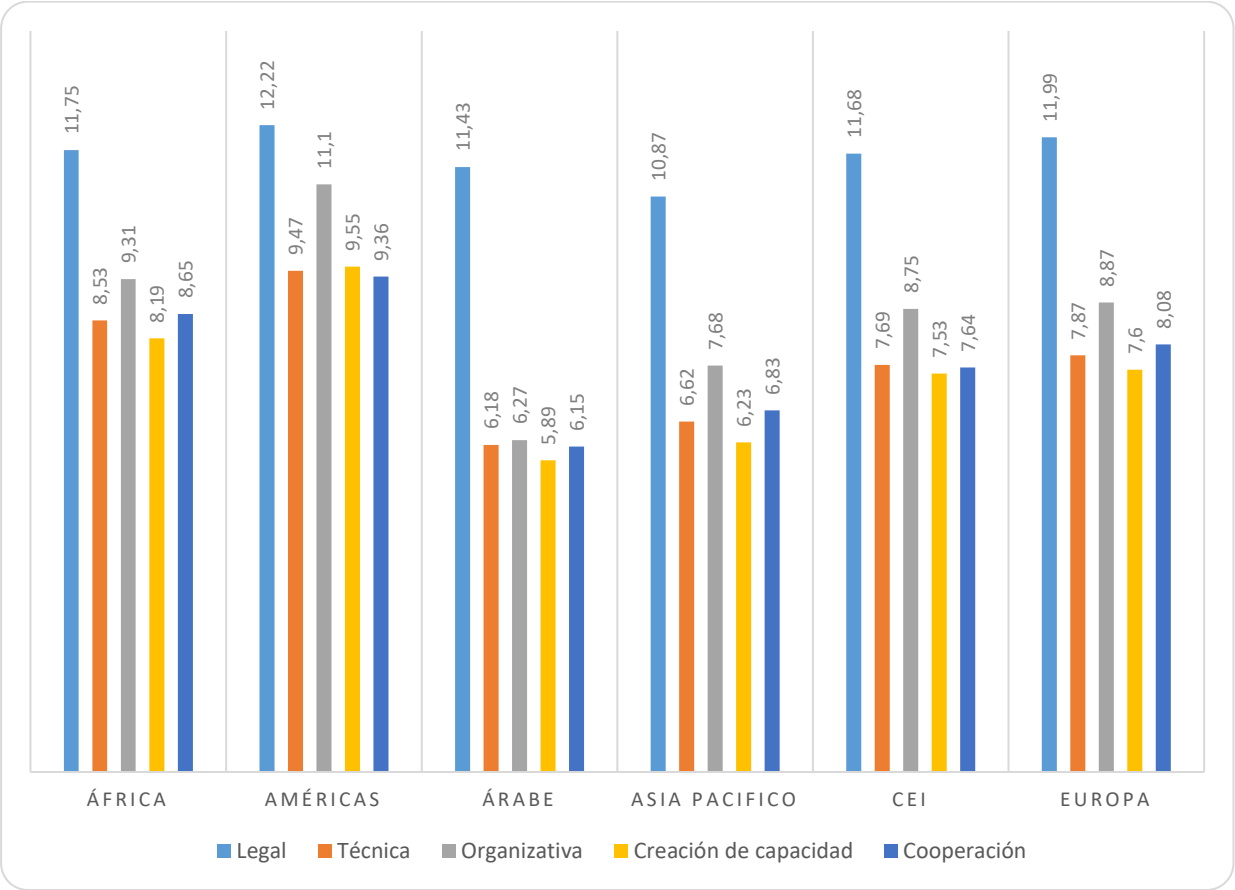
**Figura 22. Puntajes promedio de los pilares por región 2017**




Nota. Elaborado con base en conjunto de datos edición ITU (2017).

En el Informe ITU (2018) (Figura 23), Europa refleja la puntuación más alta y, por lo tanto, un avance importante y diferenciador. El ítem con mejor puntaje lo registra Américas (12,22) en el pilar de medidas legales y el más bajo Región Arabe pilar desarrollo de capacidades (5,89).

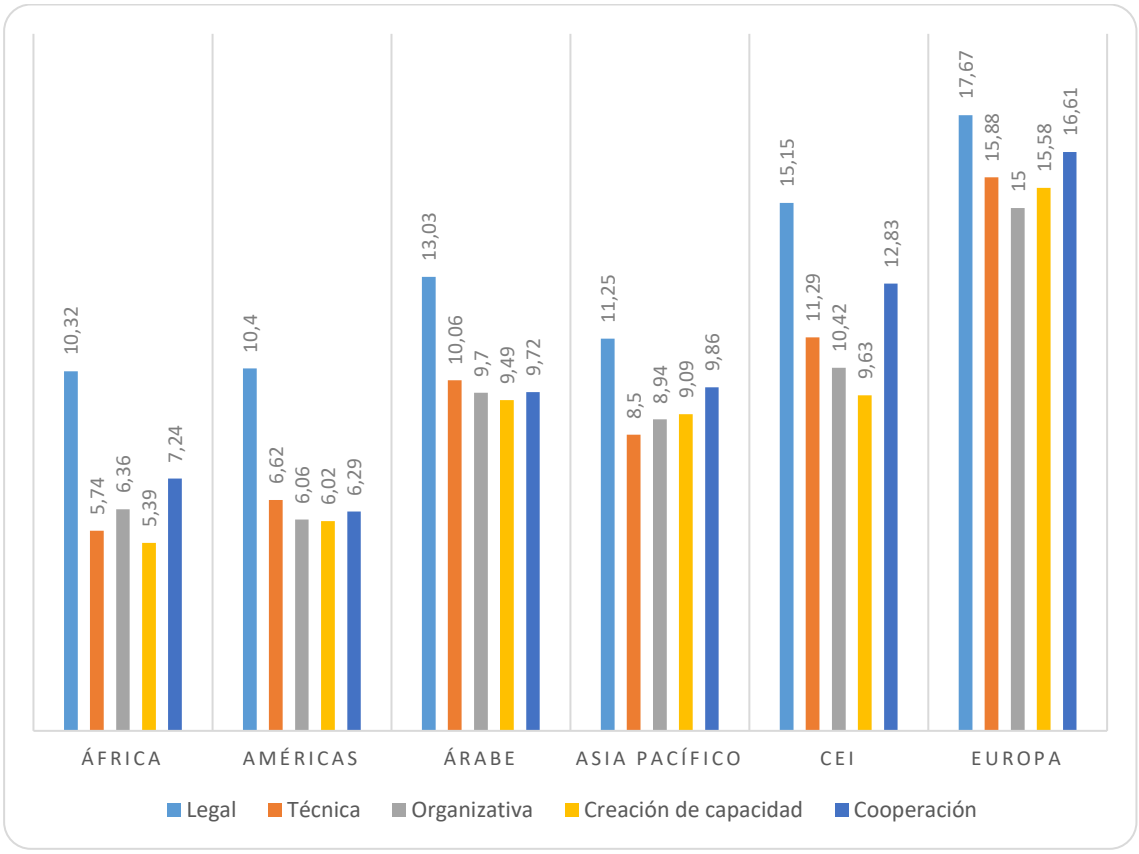
**Figura 23. Puntajes promedio de los pilares por región 2018**




Nota. Elaborado con base en conjunto de datos edición ITU (2018).

Por su parte, el Informe ITU (2020) expone como uno de los mayores desafíos de la pandemia de COVID-19 ha sido encontrar formas de conectarse de manera significativa, a pesar de la incertidumbre, la ansiedad y el cambio. Bajo este panorama (Figura 24), Europa se reporta nuevamente, como la región con la mayor puntuación en todos los pilares y las regiones de África y América continúan presentando los puntajes más bajos. La dimensión de aspectos legales ocupa el primer lugar en la totalidad de las regiones, y las dimensiones de medidas organizacionales y la creación de capacidad presentan indistintamente los menores puntajes.

**Figura 24. Puntajes promedio de los pilares por región 2020**




Nota. Elaborado con base en conjunto de datos edición ITU (2020).

En términos generales ITU (2020) reporta avances importantes en Ciberseguridad. Respecto a los ´CERT Nacional´ definidos como los equipos que permiten que los países respondan a incidentes a nivel nacional utilizando un punto de contacto centralizado que promueva una acción rápida y sistemática, empoderando a los países para aprender de la experiencia y desarrollar resiliencia en Ciberseguridad (ITU, 2020). A finales de 2020, 131 países habían establecido CIRT nacionales, incluidos 10 nuevos CIRT instaurados desde el Índice de Ciberseguridad Global de 2018. Actualmente, se están desarrollando otros cuatro CIRT nacionales (ITU, 2020). El nombre 'CERT' está protegido internacionalmente y requiere el permiso de su propietario, la Universidad Carnegie Mellon, razón por la cual cada vez más equipos utilizan el nombre 'CSIRT' (Vaks et al., 2020). Los CIRT nacionales a menudo se desarrollan e implementan siguiendo la legislación o la política nacional. Los CIRT pueden ser parte de una institución gubernamental o estar bajo el paraguas de un ministerio específico u otra entidad. Cuando los países carecen de tiempo, conocimientos o recursos

para establecer un CIRT nacional, algunos subcontratan las responsabilidades del CIRT a un tercero (ITU, 2020).

En relación con los CIRT Regional, según (ITU, 2020), 104 países se han involucrado en un CIRT regional. Como centros CERT regionales se pueden citar: APCERT (Asia del Pacífico), AFRICACERT (África), EGobierno Corporativo (Gobierno Europeo), OIC (Cooperación Islámica), OAS (América). Otro aspecto que avanza es la protección infantil en línea, que se ha convertido en un desafío mundial y requiere un enfoque holístico y una respuesta global, cooperación internacional y coordinación nacional para proteger a los niños de los riesgos y daños potenciales en línea y empoderarlos para que se beneficien plenamente de las oportunidades (ITU, 2020).

De acuerdo con el cuestionario ITU (2020), 86 países de 194 informaron haber tomado medidas para proteger a los niños en línea. Sin embargo, los datos recopilados muestran que solo el 13 por ciento de 194 países tienen una estrategia independiente dedicada a la protección de los niños en línea. Por otro lado, el 30 por ciento tiene iniciativas para proteger a los niños en línea integradas en estrategias, legislación o iniciativas más amplias sobre el delito cibernético. En la actualidad 101 países cuentan con protección infantil en línea y mecanismos de denuncia (ITU, 2020).

Respecto a la estrategia nacional de Ciberseguridad, ITU (2020) señala que es a menudo la piedra angular clave de las medidas organizativas a nivel nacional de Ciberseguridad. Esta se convierte en un marco o estrategia integral que debe desarrollarse, implementarse y ejecutarse con un enfoque de múltiples partes interesadas (Vaks et al., 2020). Aborda la acción coordinada para la prevención, preparación, respuesta y recuperación de incidentes por parte de las autoridades gubernamentales, el sector privado y la sociedad civil (Vaks et al., 2020). Uno de los compromisos más fuertes es delinear una estrategia de Ciberseguridad que describa cómo el país se preparará y responderá a los ataques contra sus redes digitales (ITU, 2017). Según ITU (2020), 127 países tienen una estrategia nacional de seguridad cibernética, ya sea actual, con más de cinco años o en proceso de redacción, 60 países han demostrado progreso en el establecimiento de objetivos más claros a través de la revisión y el desarrollo de nuevas estrategias de seguridad cibernética o mediante la actualización de su plan de acción. En la actualidad ITU (2020) reporta 136 agencias nacionales de Ciberseguridad.

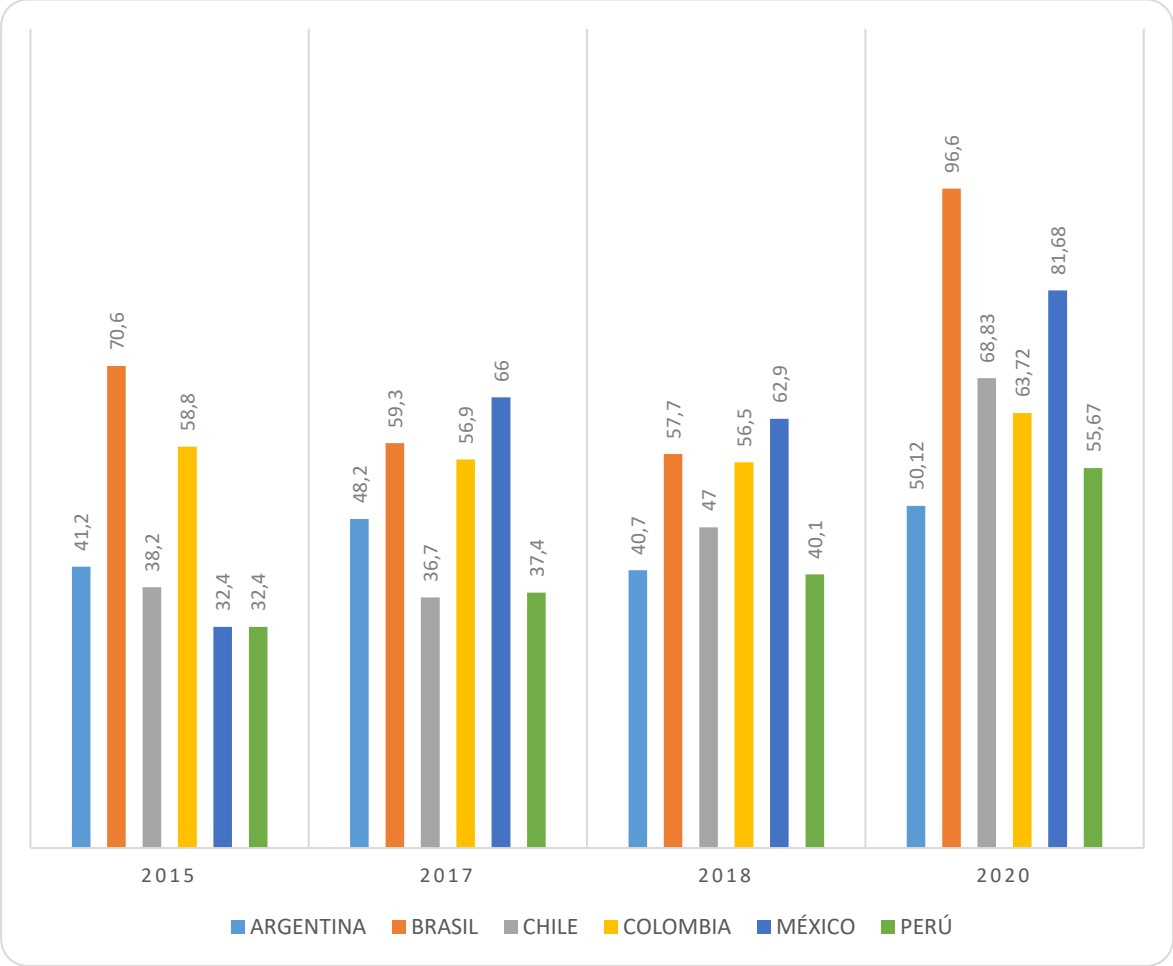
Las métricas buscan evaluar los riesgos asociados al ciberespacio a nivel nacional como un proceso que comprende la identificación, el análisis y la evaluación de riesgos (ITU, 2020). Según ITU (2020), 142 países llevan a cabo iniciativas de concientización cibernética, programas de investigación y desarrollo, industria nacional de seguridad cibernética. En relación con la cooperación internacional el intercambio de información se refiere al intercambio de inteligencia sobre amenazas, mientras que los activos designan el intercambio de profesionales, instalaciones, equipos y otras herramientas y servicios (ITU, 2018). Para esta iteración (ITU, 2020) del Índice de Ciberseguridad Global, los acuerdos multilaterales fueron aquellos entre tres o más partes, incluidos gobiernos y organizaciones regionales, pero excluyendo convenciones internacionales, como la Convención de Budapest sobre Ciberdelincuencia. El Informe (ITU, 2020) señala que es más probable que los países tengan un acuerdo multilateral que un acuerdo bilateral, con casi el 57 por ciento de los países que firmaron un acuerdo multilateral, en comparación con el 46 por ciento de los países que firmaron un acuerdo bilateral. Además, muchos países (99) firmaron o ratificaron un acuerdo multilateral sobre intercambio de información y desarrollo de capacidades (ITU, 2020).

### 5.1.3. Índice Global de Ciberseguridad en América Latina

Los gobiernos de la región de América Latina han dado importantes pasos en el desarrollo y la eficacia de sus estrategias nacionales de seguridad cibernética, también han servido como vehículos para mejorar la cultura y las prácticas nacionales de Ciberseguridad (IDB; OAS, 2020). La región cuenta con CSIRT Américas, que actúa como el impulsor principal del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados americanos en el fortalecimiento de las capacidades de respuestas ante incidentes cibernéticos de los CSIRTs de la región. Cuenta con el apoyo de la OEA, el Gobierno de Estados Unidos y Canadá.

La Figura 25 presenta los resultados de la aplicación del Índice Global de Ciberseguridad en los países objeto de estudio. Estos puntajes deben ser analizados de forma independiente (cada año) debido a que la metodología presenta variaciones importantes en cada versión. De esta forma podemos observar como Brasil repunta en 2015 y 2020. Mientras Perú, obtiene el puntaje más bajo de manera recurrente durante el período de estudio. México inicia con un índice global bajo y los años 2017 y 2018 se ubica en el primer lugar.

**Figura 25. Índice Global de Ciberseguridad por país**




Nota. Elaborado con base en ITU (2015,2017,2018,2020)

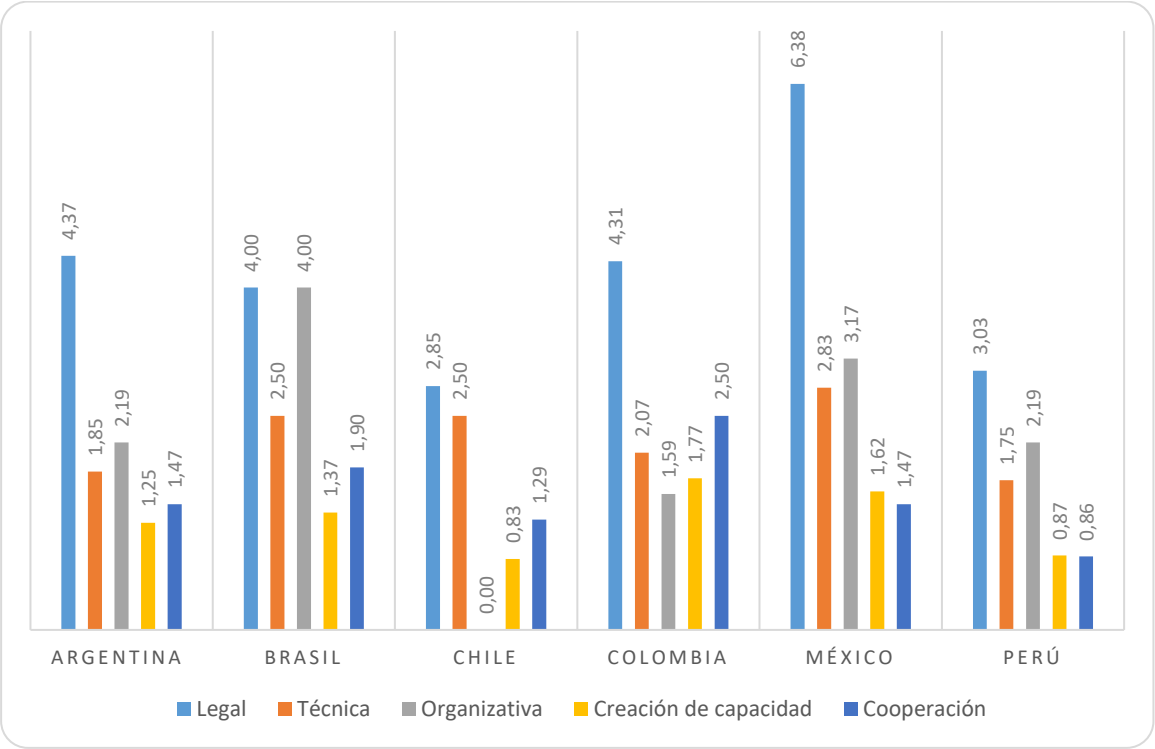
En los seis países objeto de nuestro estudio, según el Informe ITU (2015) la legislación sobre ciberdelincuencia está incorporada en el Código Penal. Colombia se convirtió en uno de los primeros países del mundo en promulgar una ley dirigida específicamente al ciberespacio, Ley 1273 de 2009 "Por la cual se modifica el Código Penal, se crea un nuevo derecho legal - llamado 'protección de la información y datos'- y los sistemas que utilizan TI y la comunicación son íntegramente conservados". En Argentina, bajo la Resolución JGM N°580/2011, se ha establecido un Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC), para crear y adoptar un marco regulatorio orientado a definir y proteger la infraestructura estratégica y crítica de los sectores público y privado, así como organizaciones interjurisdiccionales (IDB; OAS, 2020). En Chile, el Reporte ITU

(2015) revela que la normatividad sobre delito cibernético se ha hecho a través de la Ley de Ciberdelincuencia. En México, la legislación y regulación específica relacionada con la Ciberseguridad se contempla en la Ley de firmas Electrónicas Avanzadas (ITU, 2015).

Respecto a las medidas técnicas, según ITU (2015) Argentina tiene un CIRT nacional oficialmente reconocido como Equipo de Respuesta a Emergencias Informáticas de Argentina (ArCERT). Al respecto, Brasil ha reconocido oficialmente un CERT nacional, un CSIRT del gobierno y un SCIRT específico del sector. Chile cuenta con un CIRT nacional oficialmente reconocido CL CERT, este ha existido y funcionado dentro del gobierno, pero no como una entidad institucional formal, su capacidad y estructura operativa es liderada por el Ministerio del Interior y Seguridad Pública. México cuenta con un CIRT nacional oficialmente reconocido como CERT-MX. En México se requiere el cumplimiento de los requisitos de la norma ISO 27001 para un sistema de gestión de seguridad de la información de todas las instituciones gubernamentales. Perú cuenta con un CIRT nacional oficialmente reconocido como PeCERT. No existe un marco de Ciberseguridad nacional o específico del sector aprobado oficialmente para implementar estándares de Ciberseguridad reconocidos internacionalmente. El país cuenta con un marco de Ciberseguridad para la certificación y acreditación de organismos nacionales y profesionales del sector público.

La Figura 26 ilustra el comportamiento de los pilares del Índice Global de Ciberseguridad en el Informe ITU (2017). México obtiene la mejor puntuación en el pilar legal con un conjunto completo de legislación cibernética que cubre la criminalidad, la protección de datos, la privacidad de datos y las transacciones electrónicas (ITU, 2017). Mientras que Chile reporta un puntaje (0) en medidas organizacionales. A continuación, los puntajes promedio de los pilares por país 2017 presentan como la dimensión de medidas legales obtiene el mayor puntaje en todos los años. Es de resaltar que según la clasificación de este informe los cinco países se clasifican en el nivel ´madurando´; esto significa que hay un avance intermedio, entre la categoría iniciando y la principal. En 2017, Argentina a partir del Decreto 577/2017 crea el “Comité de Ciberseguridad” con el objetivo de desarrollar una estrategia nacional de seguridad cibernética. Brasil presenta una Norma complementaria N° 17/IN01/DSIC/GSIPR que establece lineamientos para la certificación y acreditación de profesionales de seguridad de la información y las comunicaciones.

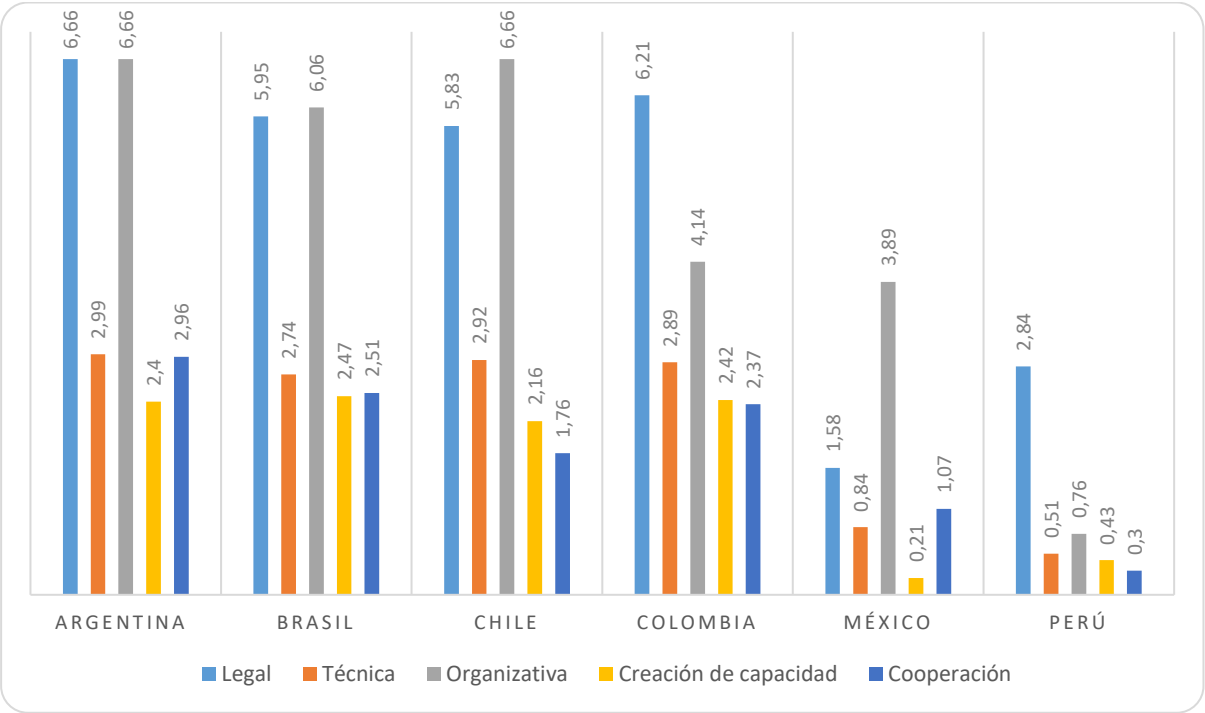
**Figura 26. Puntajes promedio de los pilares por país 2017**




Nota. Elaborado con base en ITU (2017)

El Informe ITU (2018), resalta el proyecto de Ley de protección de datos de Brasil, que incluyen disposiciones sobre notificación de incumplimiento aprobado por la Cámara de Diputados el 29 de mayo de 2018. En 2018 también se aprobó una reforma al numeral 4 del artículo 19 de la Constitución Política de la República de Chile, el cual reconocía el derecho a la honra y vida privada, y se introdujo la protección de datos personales. La Figura 27 nos permite observar cómo los puntajes promedio de los pilares por país presentan un alto puntaje en medidas organizativas y continúan los logros en medidas legales. Mientras tanto los avances en creación de capacidad y cooperación son muy poco alentadores. También se observa el rezago general de México y Perú.

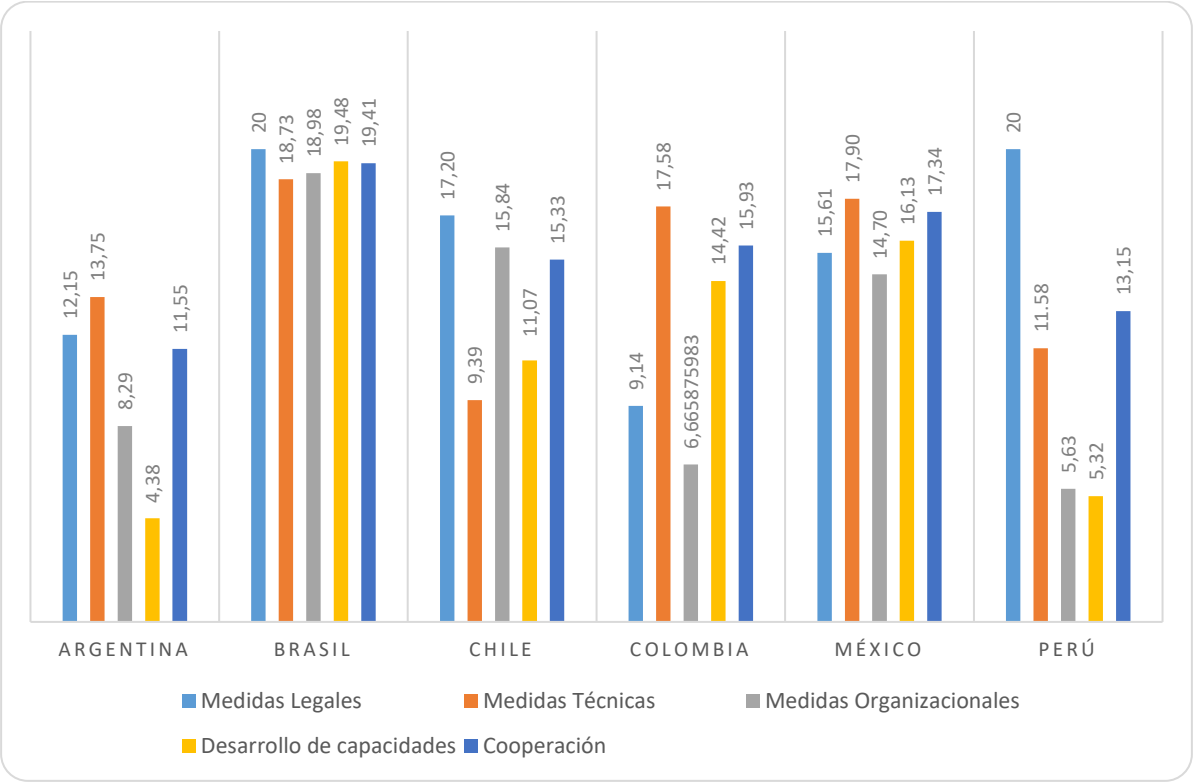
**Figura 27. Puntajes promedio de los pilares por país 2018**




Nota. Elaborado con base en ITU (2018)

Terminando con los puntajes promedio de los pilares por país, la Figura 28 nos permite observar los resultados del Informe ITU (2020). Se destacan altos puntajes de Brasil en los diferentes pilares, seguido de México. En el pilar de medidas legales lideran Brasil y Perú. En medidas técnicas Brasil, Colombia y México. Medidas organizacionales Brasil y Chile. En el pilar desarrollo de capacidades y cooperación Brasil y México obtienen los mayores puntajes.

**Figura 28. Puntajes promedio de los pilares por país 2020**




Nota. Elaborado con base en ITU (2020)

A continuación, a partir del conjunto de datos de la Edición ITU 2020, proporcionados por correo electrónico por la Unión Internacional de Telecomunicaciones obtuvimos la información pormenorizada por cada dimensión de las ediciones anteriores (2017, 2018 y 2020). La Figura 29 detalla los puntajes de la dimensión ´medidas legales´ en el Informe ITU 2020. Éste reporta cómo Brasil y Perú obtienen el puntaje máximo establecido, mientras Colombia obtiene el puntaje más bajo. Al respecto, según IDB; OAS (2020) en Argentina en los últimos años se han tomado numerosas medidas para implementar políticas y realizar cambios administrativos y regulatorios para los sectores de telecomunicaciones, Internet y tecnología.

El informe ITU (2020) da una puntuación a las medidas legales de Argentina de 12,15. Esta puntuación se obtiene a partir de un modelo ponderado que reporta las siguientes puntuaciones individuales: (0,80) por la Ley sustantiva de Ciberseguridad y (0,44) por la regulación relacionada con Ciberseguridad.

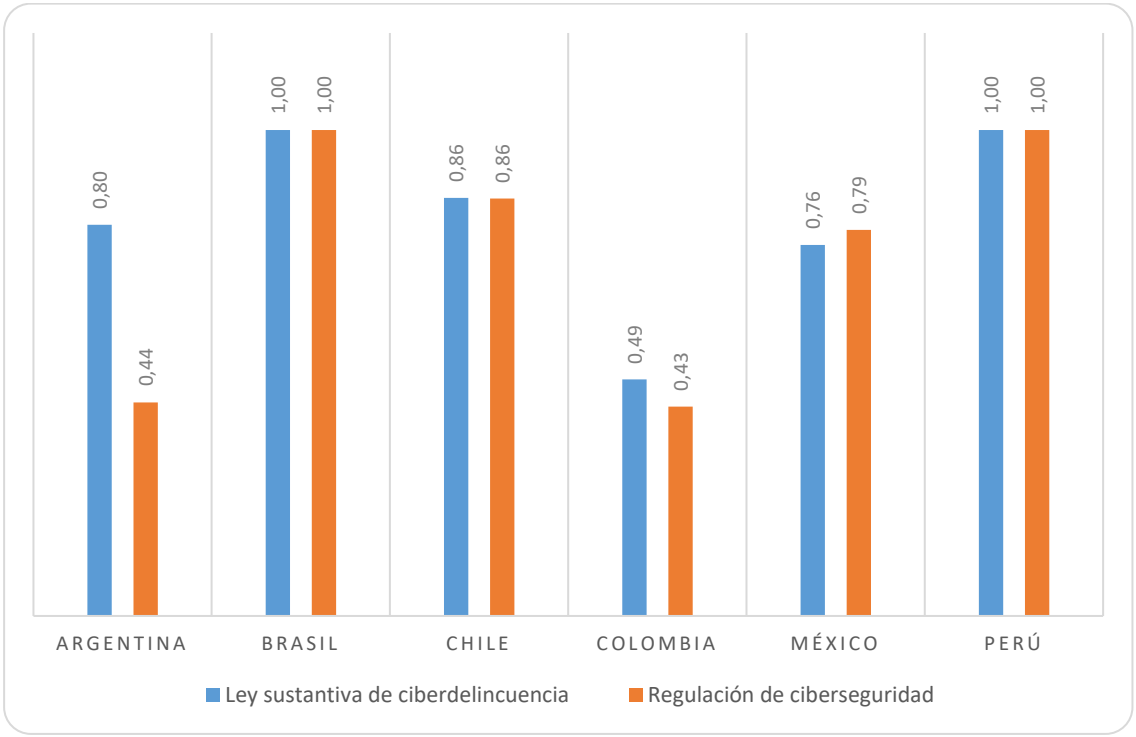
Por su parte Brasil, obtiene una valoración de 20 para las medidas legales, resultado del compromiso del país con la ley sustantiva de Ciberseguridad (1) y la regulación relacionada con Ciberseguridad (1). Chile obtiene una calificación de 17,20, así: ley sustantiva de Ciberseguridad (0,86) y regulación de Ciberseguridad relacionada con Ciberseguridad (0,86). En cuanto a Colombia, concede a las medidas legales del país un puntaje de (9,14) así: Ley sustantiva de Ciberseguridad (0,49) y regulación de Ciberseguridad relacionada con Ciberseguridad (0,43).

En el caso de México según (IDB; OAS, 2020) el país no cuenta con una ley dedicada al delito cibernético, pero el artículo N° 211 del Código Penal prevé el delito informático. Sin embargo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen. En términos de protección de datos y privacidad, existen dos leyes por separado: una para las bases de datos públicas y la otra para bases de datos privadas. (ITU, 2020)) concede a las medidas legales del país un puntaje de (15,61), así: ley sustantiva de Ciberseguridad (0,76) y la regulación de Ciberseguridad relacionada con Ciberseguridad (0,79).

Por último, Perú cuenta con la Ley Nº 30.096 de 2013 sobre delitos informáticos, que brinda disposiciones sustantivas sobre dicho tipo de delito y la Ley Nº 27.309, que incorporó el delito informático al Código Penal del país. La Ley Nº 29.733 de 2011 sobre protección de datos personales se aplica tanto a bases de datos públicas como privadas. (ITU, 2020)), evalúa las medidas legales del país con un puntaje de 20, así: ley sustantiva de Ciberseguridad (1) y la regulación de Ciberseguridad relacionada con Ciberseguridad (1).

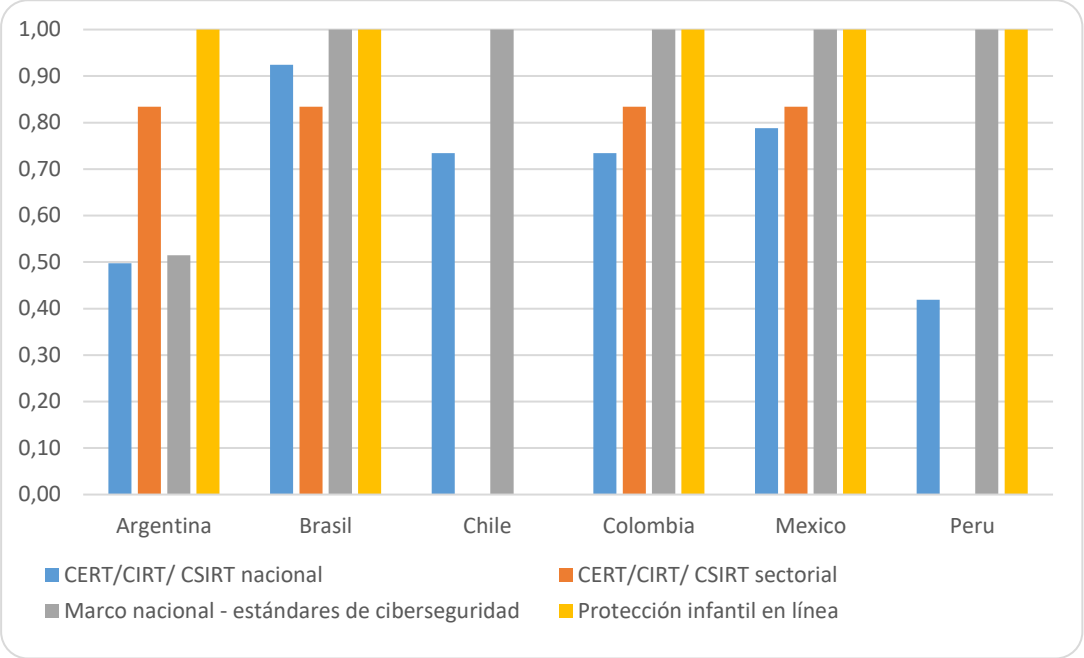
En general, respecto al pilar de medidas legales podemos ver que Brasil y Perú obtienen el mayor puntaje posible, debido a su esfuerzo y compromiso frente a la ley sustantiva y la regulación de Ciberseguridad.

**Figura 29. Medidas legales en los países objeto de estudio Informe (ITU, 2020)**




Nota. Elaborado con base en conjunto de datos de edición ITU (2020)

**Figura 30. Medidas técnicas en los países objeto de estudio Informe (ITU, 2020)**




Nota. Elaborado con base en conjunto de datos de edición ITU (2020)

La puntuación obtenida sobre la aplicación de medidas técnicas en cada país se representa en la Figura 30. Al respecto cabe mencionar que Argentina establece el primer CSIRT nacional en 1994, y desde 2011 ha realizado sus funciones bajo ICIC. ICIC-CERT elabora un registro de todos los incidentes y amenazas de Ciberseguridad existentes. Aunque el ICIC-CERT no es miembro de CSIRT Américas, que nuclea los esfuerzos liderados por la OEA, BA-CSIRT (CSIRT de la ciudad de Buenos Aires) es miembro y puede beneficiarse de la red (IDB; OAS, 2020). Argentina obtiene una valoración de los siguientes ítems que lo componen: ítem CERT/CIRT/CSIRT nacional con un puntaje de (0,50), CERT/CIRT/CSIRT sectorial una puntuación de (0,83), el marco nacional para la implementación de estándares de Ciberseguridad presenta una evaluación de (0,51) y la protección infantil en línea presenta un puntaje de (1).

En Brasil, existen políticas y procedimientos claramente definidos que todas las instituciones públicas deben seguir en función de la información proporcionada por la herramienta de conciencia situacional que posee el CERT nacional. El CERT nacional (CERT.br) continúa siendo la principal entidad responsable de manejar los informes de incidentes a nivel nacional y las actividades en las redes brasileñas (IDB; OAS, 2020). El país ha aprobado oficialmente marcos de seguridad cibernética nacionales y específicos del sector para

implementar estándares de Ciberseguridad reconocidos internacionalmente. Según el Informe ITU 2020, el pilar de medidas técnicas reporta un puntaje de 18,73. Una puntuación de (0,92) por CERT/CIRT/ CSIRT nacional, (0,83) por CERT/CIRT/ CSIRT sectorial, un puntaje de (1) por el Marco nacional para la implementación de estándares de Ciberseguridad y de (1) también para la Protección infantil en línea.

Según ITU (2020), el pilar de medidas técnicas de Chile presenta una puntuación de 9,39: CERT/CIRT/ CSIRT nacional (0,73), CERT/CIRT/ CSIRT sectorial (0) porque no existe una institución con estas características, Marco nacional para la implementación de estándares de Ciberseguridad (1) y Protección infantil en línea (0) se carece de un marco relacionado con este tipo de protección.

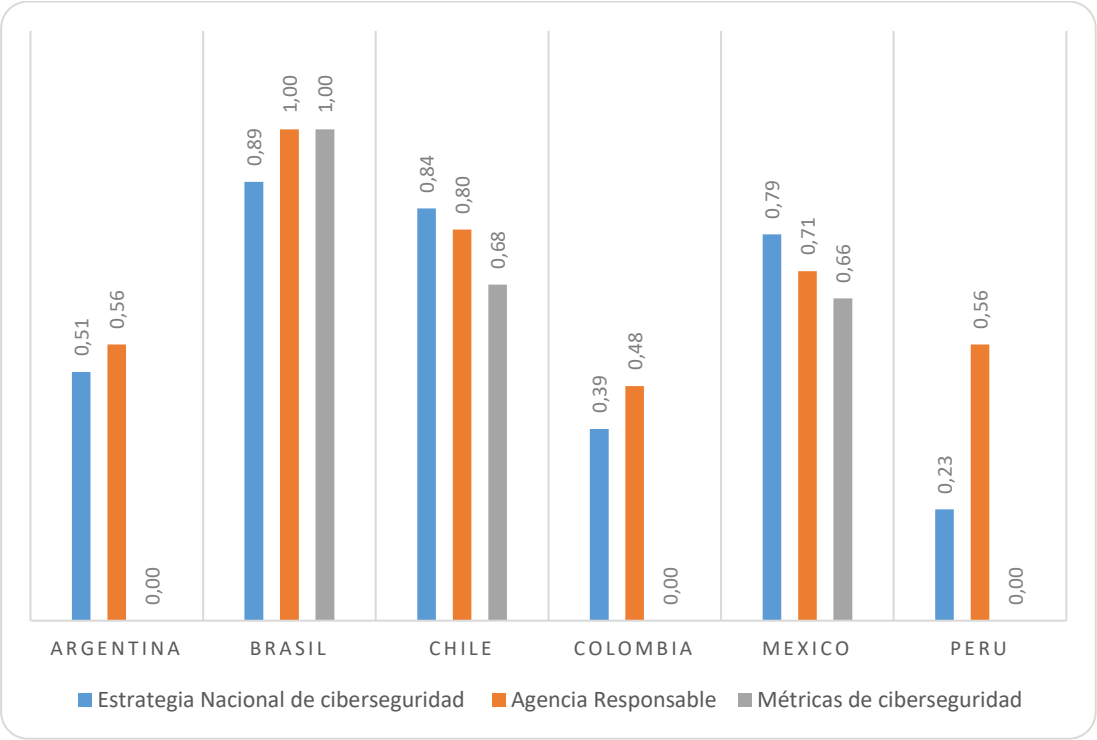
Colombia cuenta con los siguientes CIRT nacionales y sectoriales: ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia dependiente del Ministerio de Defensa. CSIRT ETB. Equipo de Respuesta a Incidentes. CSIRT Ponal: Cuartel General temático de la Policía Nacional. DigiCSIRT: Equipo de respuesta a incidentes de seguridad informática de DigiSOC. SIRT CCIT: Equipo de Respuesta a incidentes de Seguridad Informática de la Cámara Colombiana de Informática y Telecomunicaciones. SOC CCOC: Operaciones de Seguridad. Centro Operaciones Cibernéticas conjunto de mando. Colombia presenta marcos de seguridad cibernéticas nacionales (y específicos del sector) oficialmente reconocidos para implementar estándares de seguridad cibernética internacionales a través del Modelo de seguridad de la información para la estrategia en línea del gobierno y CONPES 3701 Lineamientos para la Política Nacional de Planificación de la Ciberseguridad y la Defensa. En Colombia ITU (2020), da una puntuación de 17,58 al pilar de medidas técnicas: CERT/CIRT/ CSIRT nacional (0,73), CERT/CIRT/ CSIRT sectorial (0,83), marco nacional para la implementación de estándares de Ciberseguridad (1) y protección infantil en línea (1).

Éste es el marco reconocido a nivel nacional para implementar estándares de seguridad cibernética reconocidos internacionalmente. No existe un marco de Ciberseguridad para la certificación y acreditación de organismos nacionales y profesionales del sector público en México. ITU (2020) propone una puntuación de 17,90 para las medidas técnicas de esa manera México obtiene (0,79) por CERT/CIRT/ CSIRT nacional, (0,83) por CERT/CIRT/ CSIRT sectorial, (1) por el marco nacional para la implementación de estándares de

Ciberseguridad y (1) por la protección infantil en línea. Perú tiene un CSIRT nacional, PeCERT cuya misión es coordinar la prevención, el tratamiento y la respuesta a incidentes de seguridad cibernética de instituciones del sector público, así como elaborar estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad de la información del Estado (IDB; OAS, 2020). La evaluación ITU (2020), reporta un puntaje de (11,58) en medidas técnicas, distribuido así: CERT/CIRT/ CSIRT nacional (0,42), CERT/CIRT/ CSIRT sectorial (0), Marco nacional para la implementación de estándares de Ciberseguridad (1) y Protección infantil en línea (1).

La Figura 31 representa los puntajes obtenidos sobre medidas organizacionales en cada país. En 2019 Argentina lanza la Estrategia Nacional de Ciberseguridad (OCDE et al., 2020) a la vez crea la Unidad Ejecutora, en el marco del Comité de Ciberseguridad y bajo la autoridad de la Secretaría de Modernización de la Nación invita a las Provincias y Ciudad Autónoma de Buenos Aires para adherirse a la Estrategia (IDB; OAS, 2020). A nivel nacional también se fijan los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales. El país ha avanzado en la transformación digital del Estado, situándose entre los países más avanzados de América Latina y el Caribe (ALC) en cuanto a políticas de datos abiertos de organismos públicos, según el índice OURdata de la OCDE (OCDE et al., 2020). Según ITU (2020), Argentina obtiene un puntaje de (8,29) por el pilar de medidas organizacionales: respecto al ítem de estrategia nacional de Ciberseguridad obtiene una puntuación de (0,51), por el ítem de Agencia Responsable de (0,56) y reporta un puntaje de (0) en el ítem métricas de Ciberseguridad.

**Figura 31. Medidas organizacionales en los países objeto de estudio Informe (ITU, 2020)**




Nota. Elaborado con base en conjunto de datos de edición ITU (2020)

Por su parte Brasil aprueba su Estrategia Nacional de Ciberseguridad en febrero de 2020 (OCDE et al., 2020). Brasil tiene una política nacional de Ciberseguridad reconocida oficialmente a través de instrumentos legislativos. Brasil tiene una agencia nacional o específica del sector responsable de implementar una estrategia, política y hoja de ruta nacional de seguridad cibernética. En ITU (2020), Brasil consigue una puntuación por el pilar de medidas organizativas de (18,98): en estrategia nacional obtiene una puntuación de (0,89), en los ítems de agencia responsable (1) y métricas de Ciberseguridad obtiene el mayor puntaje (1).

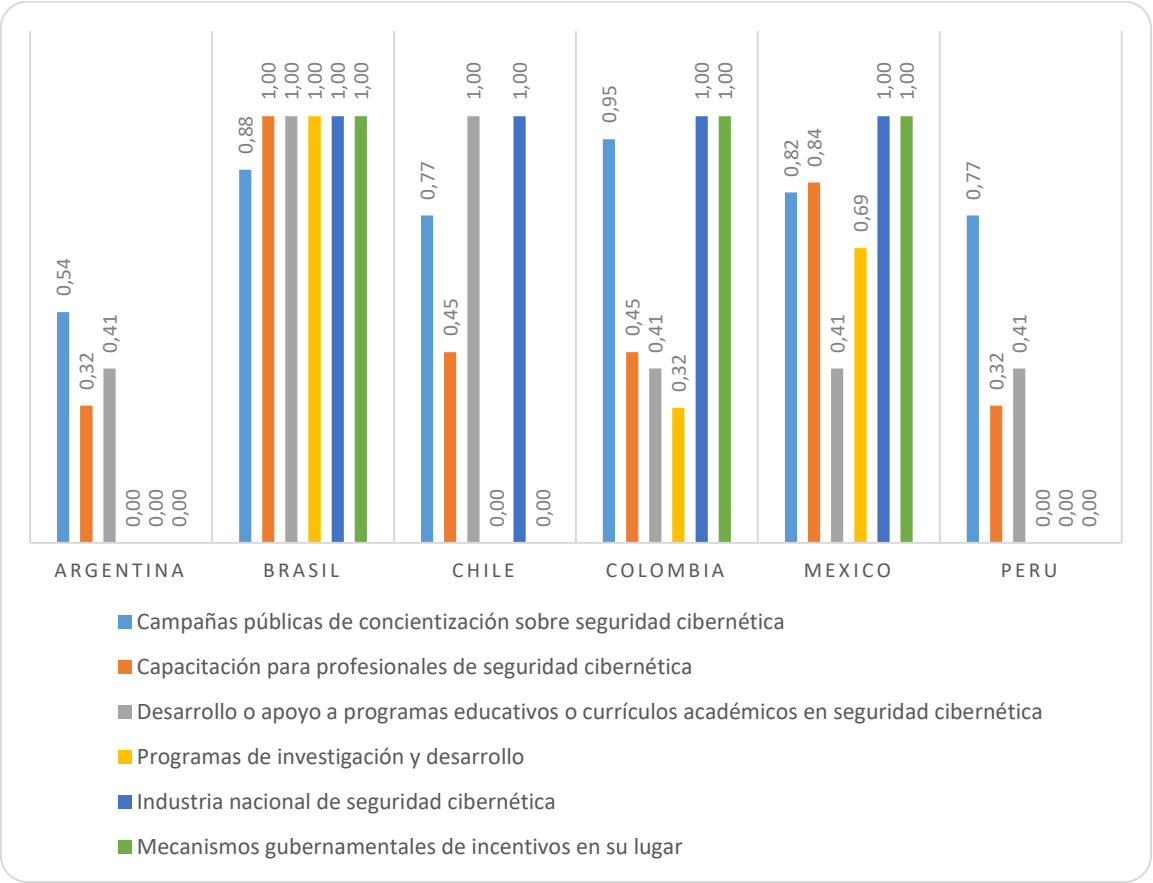
En el caso de Chile su estrategia nacional de seguridad cibernética es creada en abril de 2017. En ITU (2020) en el pilar de medidas organizacionales Chile presenta un puntaje de (15,84), a partir de los siguientes ítems: estrategia de Ciberseguridad obtiene una puntuación de (0,84), el de agencia responsable de (0,80) y el de métricas de Ciberseguridad obtiene de (0,68). Colombia también cuenta con una estrategia nacional de Ciberseguridad reconocida oficialmente a través del CONPES 3701 de 2011.

En Colombia el Departamento Nacional de Planeación y el Ministerio de TI y las Comunicaciones (MINTIC) son las agencias oficialmente reconocidas responsables de implementar una estrategia, política y hoja de ruta nacional de Ciberseguridad. Colombia no cuenta con ningún ejercicio de benchmarking o referencial nacional o sectorial oficialmente reconocido para medir el desarrollo de la Ciberseguridad (ITU, 2020). Así, Colombia obtiene un puntaje de (6,67) Estrategia Nacional de Ciberseguridad (0,39), Entidad Responsable (0,48), Métricas de Ciberseguridad (0).

México crea el Comité Especializado de Seguridad de la Información (CESI) con el objetivo de desarrollar una Estrategia Nacional de Seguridad de la Información (ENSI), que orienta todas las acciones que deben emprender las entidades del gobierno federal para prevenir, identificar, neutralizar o contrarrestar los riesgos y amenazas a la seguridad de la información. El Informe ITU (2020) reporta en el pilar de medidas organizacionales un puntaje de (14,70) distribuido, así: (0,79) estrategia de Ciberseguridad, (0,71) agencia responsable y (0.66) métricas de Ciberseguridad.

En Perú el PeCERT y la División de Delitos de Alta Tecnología (DIVINDAT) son los encargados de la Ciberseguridad en el país. ITU (2020) presenta en el pilar de medidas organizacionales un puntaje de (5,63) distribuido, así: (0,23) estrategia de Ciberseguridad, (0,56) agencia responsable y (0,00) métricas de Ciberseguridad.

**Figura 32. Medidas de creación de capacidad en los países objeto de estudio Informe (ITU, 2020)**




Nota. Elaborado con base en conjunto de datos de edición ITU (2020).

La Figura 32 destaca las medidas de creación de capacidad según el Informe (ITU, 2020) por cada país. Para el caso de Argentina diferentes oportunidades para que los argentinos continúen su educación en Ciberseguridad, en universidades públicas y privadas, y también ofrecidos por la sociedad civil (IDB; OAS, 2020). Además, BA-CSIRT brinda capacitaciones y charlas de sensibilización para enseñar a los interesados sobre seguridad cibernética y el uso de las TIC (IDB; OAS, 2020). Según ITU (2020), las medidas de creación de capacidad en Argentina obtienen un puntaje de (4,38) y presentan las siguientes puntuaciones: campañas públicas de concientización sobre seguridad cibernética (0,54), capacitación para profesionales de seguridad cibernética (0,32), desarrollo o apoyo a programas educativos o currículos académicos en seguridad cibernética (0,41), programas de investigación y desarrollo (0), Industria nacional de seguridad cibernética (0), mecanismos gubernamentales de incentivos en su lugar (0).

En Brasil se ofrecen cursos especializados en informática a nivel universitario (IDB; OAS, 2020). Los profesionales del sector público asisten a las cualificaciones profesionales de las TI en el extranjero y reciben certificados de TIC registrados por instituciones internacionales como el Certificado de Seguridad de Sistemas de Información Profesional (CISSP) o el de Gerente de Seguridad de Información Certificado (CISM) (IDB; OAS, 2020). En ITU (2020), Brasil obtiene una puntuación por el pilar creación de capacidad de 19,48: campañas públicas de concientización sobre seguridad cibernética (0,88), capacitación para profesionales de seguridad cibernética (1,00), desarrollo o apoyo a programas educativos o currículos académicos en seguridad cibernética (1,00), programas de investigación y desarrollo (1,0), Industria nacional de seguridad cibernética (1,00), mecanismos gubernamentales de incentivos en su lugar (1,00).

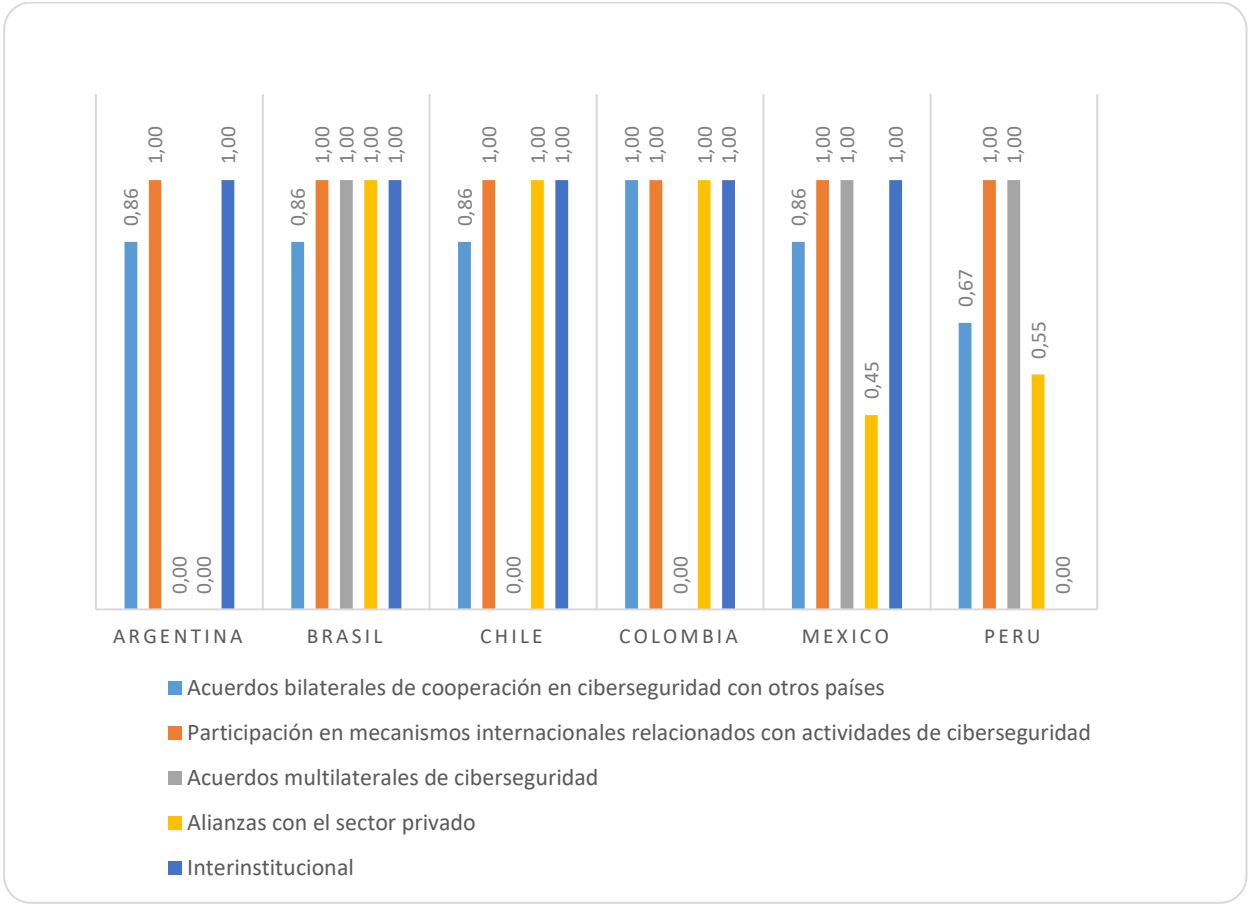
Por lo que respecta a Chile, las universidades, tanto públicas como privadas, ofertan carreras de grado, así como posgrados y diplomados de especialización relacionados con la Ciberseguridad (IDB; OAS, 2020). En ITU (2020), Chile obtiene una puntuación del pilar de creación de capacidad (11.07) a partir de los siguientes ítems: campañas públicas de concientización sobre seguridad cibernética (0,77), capacitación para profesionales de seguridad cibernética (0,454), desarrollo o apoyo a programas educativos o currículos académicos en seguridad cibernética (1.00), programas de investigación y desarrollo (0), Industria nacional de seguridad cibernética (1.00), mecanismos gubernamentales de incentivos en su lugar (0).

En apoyo a la transformación digital en Colombia, a finales de 2018 el BID aprobó el "Programa para la mejora de la conectividad y digitalización de la economía" a través de un "Préstamo Basado en Políticas" (IDB; OAS, 2020) este programa concreta iniciativas de fortalecimiento de las capacidades nacionales en Ciberseguridad. Los colombianos tienen amplias oportunidades de continuar con estudios en seguridad cibernética tanto a nivel de grado como de posgrado. ITU (2020) reporta una puntuación de (14,42) para el pilar de creación de capacidad, por los resultados de los siguientes ítems: campañas públicas de concientización sobre seguridad cibernética (0,95), capacitación para profesionales de seguridad cibernética (0,45), desarrollo o apoyo a programas educativos o currículos académicos en seguridad cibernética (0,41), programas de investigación y desarrollo (0,32), Industria nacional de seguridad cibernética (1.00), mecanismos gubernamentales de incentivos en su lugar (1,00).

En México desde la educación superior, hay suficientes oportunidades para que los mexicanos realicen estudios tanto de grado como de posgrado centrados en la seguridad cibernética (IDB; OAS, 2020). ITU (2020) reporta una puntuación de (16,13) para el pilar de creación de capacidad, por los resultados de los siguientes ítems: campañas públicas de concientización sobre seguridad cibernética (0,82), capacitación para profesionales de seguridad cibernética (0,84), desarrollo o apoyo a programas educativos o currículos académicos en seguridad cibernética (0,41), programas de investigación y desarrollo (0,69), Industria nacional de seguridad cibernética (1.00), mecanismos gubernamentales de incentivos en su lugar (1,00).

Finalmente, en Perú también algunas universidades brindan la oportunidad de que se continúe la educación en seguridad cibernética, y además se han realizado eventos para tratar las temáticas organizadas por asociaciones independientes (IDB; OAS, 2020). ITU (2020) informa una puntuación de (5,32) para el pilar de creación de capacidad, a partir de los siguientes ítems: campañas públicas de concientización sobre seguridad cibernética (0,77), capacitación para profesionales de seguridad cibernética (0,32), desarrollo o apoyo a programas educativos o currículos académicos en seguridad cibernética (0,41), programas de investigación y desarrollo (0,00), Industria nacional de seguridad cibernética (0,0), mecanismos gubernamentales de incentivos en su lugar (0,00).

**Figura 33. Medidas de cooperación en los países objeto de estudio ITU (2020)**




Nota. Elaborado con base en conjunto de datos de edición ITU (2020).

La Figura 33 ilustra el puntaje de las medidas de cooperación en los países objeto de estudio. Al respecto cabe destacar que Argentina realiza alianzas estratégicas de cooperación internacional para la seguridad cibernética con Estados Unidos, España y Chile. Según ITU (2020), el pilar de medidas de cooperación presenta una puntuación de (11,55), a partir de los siguientes ítems: acuerdos bilaterales de cooperación en Ciberseguridad con otros países (0,86), participación en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,0), acuerdos multilaterales de Ciberseguridad (0,0), alianzas con el sector privado (0,0), interinstitucional (1,0). La estabilidad cibernética global se basa en la capacidad local y nacional de todos los países para prevenir y reaccionar ante incidentes cibernéticos e investigar y procesar casos de delitos cibernéticos (IDB; OAS, 2020).

Brasil es miembro de la iniciativa ITU-IMPACT y tiene acceso a servicios relevantes de Ciberseguridad. ITU (2020), reporta una puntuación de (19,41) por medidas de cooperación.

A partir del buen puntaje de sus ítems: acuerdos bilaterales de cooperación en Ciberseguridad con otros países (0,86), participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,00), acuerdos multilaterales de Ciberseguridad (1,00) alianzas con el sector privado (APP) (1,00), Interinstitucional (1,00). En noviembre de 2021, el Senado de Brasil aprobó la adhesión de su país a la Convención sobre Delitos Cibernéticos, celebrada en Budapest, Hungría. Dicha convención tiene como objetivo la cooperación internacional para combatir el crimen cibernético de manera con Junta(González, 2021). Según ITU (2020), Brasil reporta una puntuación de (15,33) por medidas de cooperación. A partir del buen puntaje de sus ítems: acuerdos bilaterales de cooperación en Ciberseguridad con otros países (0,85), participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,00), acuerdos multilaterales de Ciberseguridad (0,00), alianzas con el sector privado (APP) (1,00), Interinstitucional (1,00).

En Chile ITU (2020), reporta una puntuación de (15,33) por medidas de cooperación. A partir de los siguientes puntajes de sus ítems: acuerdos bilaterales de cooperación en Ciberseguridad con otros países (0,86), participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,00), acuerdos multilaterales de Ciberseguridad (0,00) alianzas con el sector privado (APP) (1,00), Interinstitucional (1,00).

En Colombia existen empresas a nivel nacional que brindan cursos especializados que abordan frentes de Ciberseguridad. También cuenta con 11 programas académicos ofrecidos por instituciones de seguridad a nivel nacional. Colombia no cuenta con ningún programa nacional o sectorial oficialmente reconocido para compartir activos de Ciberseguridad dentro del sector público. Según IDB; OAS (2020) Colombia es miembro tanto de Interpol como de Europol y ha priorizado su participación en escenarios internacionales. Además, mediante la Ley N° 1.928 del 24 de julio de 2018, se aprobó el Convenio sobre la Ciberdelincuencia (Convenio de Budapest, 2001) y depositó su instrumento de adhesión el 16 de marzo de 2020. Según ITU (2020), reporta una puntuación de (15,93) por medidas de cooperación. A partir del puntaje de sus ítems: acuerdos bilaterales de cooperación en

Ciberseguridad con otros países (1,00), participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,00), acuerdos multilaterales de Ciberseguridad (0,00), alianzas con el sector privado (APP) (1,00), Interinstitucional (1,00).

Por lo que respecta a México, según ITU (2020) reporta una puntuación de (17,34) por medidas de cooperación, y ello a partir de la siguiente puntuación otorgada a cada uno de los ítems: acuerdos bilaterales de cooperación en Ciberseguridad con otros países (0,86), participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,00), acuerdos multilaterales de Ciberseguridad (1,00), alianzas con el sector privado (APP) (0,45) e interinstitucional (1,00). Finalmente, Perú consigue una puntuación de 13,15 por medidas de cooperación. A partir del puntaje de sus ítems: acuerdos bilaterales de cooperación en Ciberseguridad con otros países (0,67), participación del gobierno en mecanismos internacionales relacionados con actividades de Ciberseguridad (1,00), acuerdos multilaterales de Ciberseguridad (1,00), alianzas con el sector privado (APP) (0,55) e interinstitucional (0,00).

### 5.2. Panorama de la Gobernanza Nacional: Índice de Gobernanza Mundial

Las cuestiones relativas a la gobernanza del sector público y la lucha contra la corrupción siguen ocupando de manera constante los primeros puestos entre las prioridades de desarrollo más importantes (World Bank, 2022). Bajo este panorama, la comunidad empresarial global clasificó el "fracaso de la gobernanza nacional" como el sexto riesgo más preocupante para hacer negocios durante los próximos diez años. El fracaso de la gobernanza nacional se refiere a la incapacidad para gobernar una nación de importancia geopolítica, como resultado de un estado de derecho débil, corrupción o estancamiento político (WEF, 2020). En este nuevo, complejo y cambiante entorno, con múltiples actores, el Estado, garante del bien público, no puede por sí solo solucionar los problemas de la sociedad actual (Meuleman, 2010).

Una buena gobernanza se convierte en el mecanismo clave para el éxito (Young et al., 2020). De acuerdo con Kaufmann et al. (2010), la gobernanza nacional hace referencia a las tradiciones e instituciones mediante las cuales se ejerce la autoridad en un país. Éste es un

concepto alineado con la propuesta del Banco Mundial sobre la buena gestión de los asuntos públicos o buena gobernanza (good governance), concebida como la relación entre las instituciones y el desarrollo (Von Haldenwang, 2005). Existe la creencia generalizada de que la mala calidad de la gobernanza obstaculiza el crecimiento económico y el desarrollo financiero. En otras palabras, la buena gobernanza y las instituciones son sin duda requisitos previos para el desarrollo de los mercados financieros (Low et al., 2015).

Aunque otros organismos internacionales tienen carteras de proyectos y perspectivas diferentes sobre ciertos aspectos clave de la relación entre Estado y sociedad, puede sostenerse que el concepto de gobernanza del Banco Mundial es una visión básica compartida por la mayor parte de las organizaciones internacionales (Von Haldenwang, 2005). Durante la última década, las clasificaciones internacionales se han convertido en una herramienta crítica utilizada por los actores internacionales involucrados en la gobernanza global (Cooley, 2015). Un ejemplo de estas clasificaciones, lo constituye el Índice de Gobernanza Mundial.

El Índice de Gobernanza Mundial (por sus siglas en inglés, WGI), publicado por el Banco Mundial, presenta el estado de la gobernanza en los países objeto de estudio. Este indicador combina las opiniones de un gran número de encuestados: empresas, ciudadanos y expertos en países industrializados y en desarrollo. Se basa en más de 30 fuentes de datos individuales producidos por una variedad de institutos de encuestas, grupos de expertos, organizaciones no gubernamentales, organizaciones internacionales y empresas del sector privado (World Bank, 2022). Esta metodología, producida para el Banco Mundial con una cobertura de más de doscientos países y territorios, da un gran paso adelante al pensar en la gobernanza en conjunto (Devarajan & Johnson, 2008). Construye dos medidas de gobernabilidad correspondiente a cada una de las siguientes tres áreas, dando como resultado un total de seis dimensiones de gobernabilidad (Baldini et al., 2018):

(a) El proceso por el cual los gobiernos son seleccionados, monitoreados y reemplazados:
    1. Voz y rendición de cuentas (VA): captura las percepciones de la medida en que los ciudadanos de un país pueden participar en la selección de su gobierno, así como la libertad de expresión, la libertad de asociación y la libertad de prensa.
    2. Estabilidad política y ausencia de violencia/terrorismo (PV): captura las percepciones de la probabilidad de que el gobierno sea desestabilizado o derrocado

por medios inconstitucionales o violentos, incluida la violencia y las motivaciones políticas.

(b) La capacidad del gobierno para formular e implementar efectivamente políticas sólidas:

3. Efectividad del gobierno (GE): captura las percepciones de la calidad de los servicios públicos, la calidad del servicio civil y el grado de su independencia de las presiones políticas, la calidad de la formulación e implementación de políticas y la credibilidad del compromiso del gobierno para tales políticas.
4. Calidad regulatoria (RQ): captura las percepciones de la capacidad del gobierno para formular e implementar políticas y regulaciones sólidas que permitan y promuevan el desarrollo del sector privado.

(c) El respeto de los ciudadanos y el Estado por las instituciones que rigen las interacciones económicas y sociales entre ellos:

5. Estado de derecho (RL): captura las percepciones de la medida en que los agentes confían en las reglas de la sociedad y las cumplen, y en particular la calidad de la ejecución de contratos, los derechos de propiedad, la policía y los tribunales, así como la probabilidad de delincuencia y violencia. Generado por expertos.
6. Control de la corrupción (CC): captura las percepciones de la medida en que el poder público se ejerce, para beneficio privado, incluidas formas de corrupción menores y mayores, así como la "captura" del estado por parte de élites e intereses privados.

Las seis medidas del índice WGI son útiles como herramienta para comparaciones amplias entre países y para evaluar tendencias generales a lo largo del tiempo (World Bank, 2022). En 2020 los países con los mejores índices de gobernanza mundial, según WGI (2021), fueron: Singapur (0,891), Nueva Zelanda (0.876), Finlandia (0,864), Noruega (0,859), Liechtenstein (0,858), Dinamarca (0,854), Luxemburgo (0,854), Suiza (0.843), Suecia (0.842) y Países Bajos (0,830).

### 5.2.1. Índice de Gobernanza Mundial en América Latina

La restricción de las libertades, del poder estatal, de la tergiversación de la democracia y de sus componentes esenciales, mantiene anclada a América Latina en encrucijadas complejas, en culturas de dominación y opresión, que requieren ser superadas, instaurando medios democráticos y legítimos para hacerlo (Barraza et al., 2022).

Al mismo tiempo, tras un impulso legitimador inicial debido al cambio de régimen, muchas de las democracias latinoamericanas han tenido serias dificultades para mejorar su gobernanza (Von Haldenwang, 2005). Según diversos estudios, ésta es la región más desigual del mundo (Chaves, 2019). De acuerdo con la Comisión Económica para América Latina y el Caribe (CEPAL, 2016), la desigualdad se debe principalmente a la estructura heterogénea de los sistemas económicos y productivos, donde coexisten sectores de alta y baja productividad, muchas veces en grandes centros metropolitanos. La corrupción, los privilegios, la falta de garantías legales y de acceso a la toma de decisiones políticas, así como la mala gestión, han sido características constantes y han causado una amplia desilusión con el modelo democrático y de mercado (Von Haldenwang, 2005).

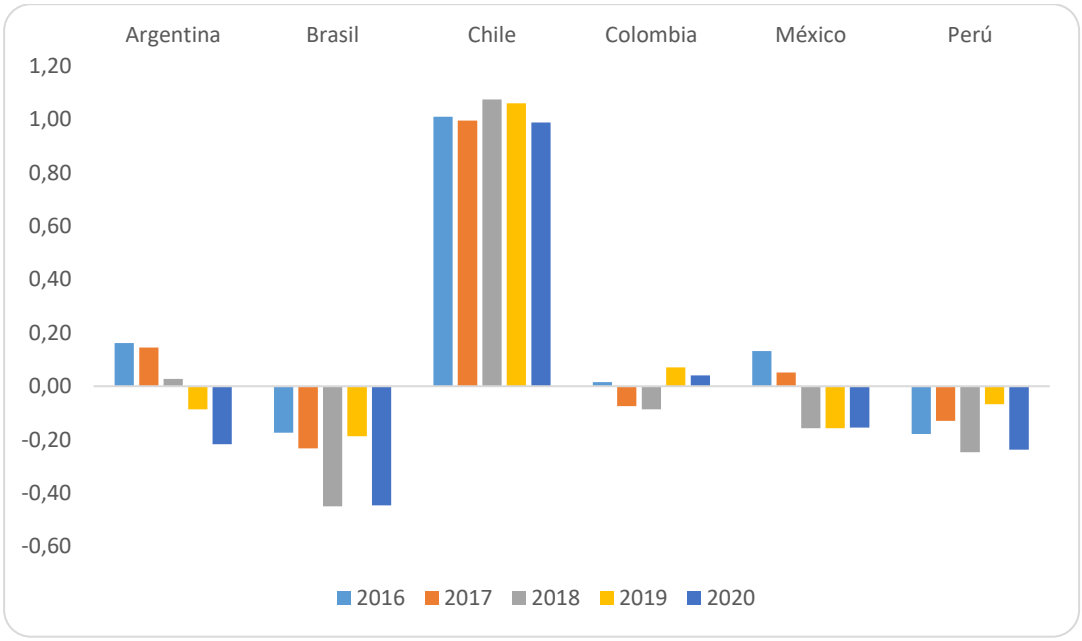
Las experiencias analizadas en América Latina han demostrado que la transferencia de los formatos de gobernanza, por parte de los organismos internacionales, no tuvieron los resultados esperados en términos de lograr políticas públicas más eficaces, eficientes y democráticas (Zurbriggen, 2011). En términos generales, la gobernanza nacional en América Latina ha estado definida por una situación política, económica y social marcada en algunos países por la corrupción, el clientelismo político y la falta de transparencia en la toma de decisiones. Respecto al sistema político, la región ha enfrentado diversas formas de gobierno, desde democracias hasta regímenes autoritarios. Algunos países, como Chile, han logrado estabilizar su sistema político, mientras que otros, como Brasil, Colombia, México y Perú, siguen presentando problemáticas relacionadas con la inestabilidad política y la violencia. Bajo este panorama presentamos el estado de la gobernanza en los países objeto de estudio durante el período 2016-2020 en América Latina.

La Figura 34 presenta los resultados de la aplicación del Índice de Gobernanza Mundial para los países objeto de estudio durante el período 2016-2020. En línea con el panorama descrito en América Latina, podemos observar que Chile es el país que reporta la mejor gobernanza. En general, el país presenta una gobernanza estable y robusta, con aspectos por mejorar según las demandas crecientes en términos sociales. Argentina presenta la segunda mejor gobernanza, si bien el país cuenta con una democracia representativa y un sistema de división de poderes; los problemas económicos y políticos (con un alto nivel de corrupción y una estabilidad en los cambios de gobierno) representan un desafío significativo. Enseguida encontramos la puntuación de Colombia, país con problemas de corrupción y desplazamiento forzado. Este país firma el Acuerdo de Paz con grupos ilegales en septiembre

de 2016, como un esfuerzo importante para su gobernanza en términos de democracia y los derechos humanos. No obstante, hay problemáticas como la corrupción y la violencia que se deben superar.

Por su parte, Perú presenta en el periodo analizado problemas de corrupción, crisis política y económica. Tres presidentes han sido destituidos por corrupción, lo que ha empeorado la crisis política. El país, a través de sucesivas reformas, ha buscado mejorar la transparencia y el problema de la corrupción, pero es necesario que esta nación continúe mejorando la seguridad y la economía, y fortalezca la justicia y los derechos humanos. La gobernanza nacional en Brasil, como lo refleja la puntuación en el período 2016-2020, presentó una serie de problemas originados por la polarización entre partidos políticos y la corrupción. La destitución del presidente en 2016 por escándalo de corrupción y su sucesor enfrentaron una serie de acusaciones de corrupción durante su mandato. Por último, México es el país que obtiene la menor puntuación con valores negativos muy altos. En 2016 el nuevo presidente recibió un país con un alto nivel de violencia y criminalidad, violación de derechos humanos, corrupción y polarización de los partidos políticos.

**Figura 34. Gobernanza en América Latina 2016- 2020**




Nota. Elaborado con base en ITU (2016, 2017, 2018, 2019, 2020).

Con respecto al Pilar 1, “Voz y responsabilidad”, como se observa en la Tabla 30 Chile reporta la mayor puntuación, seguido de Argentina, Brasil, Colombia, Perú y México. Los seis países objeto de estudio cuentan con un sistema electoral democrático que les permite a los ciudadanos elegir a sus gobernantes.

**Tabla 30. Voz y Responsabilidad**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Argentina | 0,49 | 0,53 | 0,53 | 0,57 | 0,59 |
| Brasil | 0,45 | 0,45 | 0,37 | 0,30 | 0,30 |
| Chile | 1,00 | 1,00 | 1,02 | 0,98 | 1,00 |
| Colombia | 0,12 | 0,11 | 0,16 | 0,21 | 0,15 |
| México | -0,07 | -0,08 | -0,02 | 0,01 | -0,03 |
| Perú | 0,27 | 0,27 | 0,21 | 0,27 | 0,25 |

Como se presenta en la Tabla 31, en lo que se refiere al Pilar 2, “Estabilidad Política y Ausencia de Violencia/Terrorismo”, Chile obtiene las puntuaciones positivas más altas, seguido de Argentina y Brasil. Por su parte, Perú y Colombia les siguen en la lista con puntajes más bajos y México reporta valores negativos muy por debajo de los demás países objeto de estudio.

**Tabla 31. Estabilidad Política y Ausencia de Violencia/Terrorismo**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Argentina | 0,20 | 0,17 | 0,01 | -0,09 | -0,08 |
| Brasil | -0,38 | -0,47 | -0,44 | -0,71 | -0,43 |
| Chile | 0,41 | 0,42 | 0,43 | 0,01 | 0,07 |
| Colombia | -0,88 | -0,77 | -0,80 | -0,95 | -0,66 |
| México | -0,63 | -0,80 | -0,65 | -0,84 | -0,86 |
| Perú | -0,20 | -0,26 | -0,27 | -0,15 | -0,36 |

En la Tabla 32 se presentan los resultados del Pilar 3, denominado ´Eficacia del gobierno´. Según los puntajes Chile experimenta una estabilidad política durante los últimos años, seguido de Argentina país que reporta valores positivos. Los demás países presentan cifras negativas.

**Tabla 32. La Eficacia del Gobierno**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Argentina | 0,25 | 0,16 | 0,05 | -0,10 | -0,22 |
| Brasil | -0,22 | -0,29 | -0,50 | -0,21 | -0,44 |
| Chile | 0,86 | 0,84 | 0,94 | 0,89 | 0,74 |
| Colombia | -0,01 | -0,11 | -0,11 | 0,06 | 0,04 |
| México | 0,06 | -0,03 | -0,26 | -0,28 | -0,24 |
| Perú | -0,23 | -0,18 | -0,30 | -0,10 | -0,26 |

Respecto a la dimensión denominada ´Calidad regulatoria´, la Tabla 32 presenta los resultados obtenidos por la aplicación del índice. La calidad regulatoria de Chile es considerada como una de las mejores de América Latina. El país ha implementado medidas para mejorar la eficacia y eficiencia de su sistema regulatorio, incluyendo la creación de una Agencia de Calidad Regulatoria (ARC) en 2002, que tiene como objetivo mejorar la calidad de las regulaciones y reducir los costos para las empresas y los ciudadanos. Además, Chile cuenta con un sistema de evaluación de impacto regulador que busca medir el impacto de las regulaciones en el mercado, la economía y la sociedad.

La calidad regulatoria en Argentina, Brasil, Colombia, México y Perú han enfrentado problemas en la aplicación y el cumplimiento de las regulaciones. Los gobiernos han establecido agencias reguladoras independientes para supervisar sectores clave como la energía, las telecomunicaciones, y los servicios públicos.

**Tabla 33. Calidad Regulatoria**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Argentina | -0,34 | -0,18 | -0,18 | -0,44 | -0,48 |
| Brasil | -0,18 | -0,12 | -0,28 | -0,11 | -0,10 |
| Chile | 1,37 | 1,33 | 1,31 | 1,17 | 0,96 |
| Colombia | 0,35 | 0,27 | 0,24 | 0,33 | 0,24 |
| México | 0,21 | 0,19 | 0,10 | 0,03 | 0,00 |
| Perú | 0,48 | 0,36 | 0,45 | 0,53 | 0,49 |

La Tabla 34 presenta la puntuación de la dimensión ´Estado de derecho´. Esta dimensión presenta avances importantes en Chile. Además, el estado de derecho ha sido afectado por

la corrupción y la falta de transparencia en el sector público, y por la inestabilidad política y económica em los países de América Latina.

**Tabla 34. Estado de Derecho**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Argentina | -0,39 | -0,25 | -0,24 | -0,43 | -0,47 |
| Brasil | -0,16 | -0,25 | -0,25 | -0,18 | -0,18 |
| Chile | 1,13 | 1,15 | 1,09 | 1,07 | 1,07 |
| Colombia | -0,28 | -0,36 | -0,41 | -0,42 | -0,49 |
| México | -0,56 | -0,56 | -0,64 | -0,66 | -0,67 |
| Peru | -0,48 | -0,50 | -0,53 | -0,49 | -0,34 |

La Tabla 35 presenta los resultados de la dimensión ´Control de la corrupción´. En Chile pese a que el país cuenta con un sistema legal y regulaciones para prevenir y combatir la corrupción, ha habido críticas sobre la falta de cumplimiento y efectividad de estas medidas. En los seis países objeto de estudio, el sector público ha sido criticado por la falta de transparencia y la falta de rendición de cuentas, lo que ha llevado a la corrupción y el abuso de poder. En Brasil la corrupción ha sido un problema histórico, y ha sido objeto de críticas por parte de organismos internacionales y organizaciones no gubernamentales. Uno de los casos más notorios de corrupción en Brasil fue la operación Lava Jato. En Perú, es de resaltar que los presidentes han sido encarcelados o procesados por casos de corrupción, casi todos vinculados a la investigación Lava Jato. En el caso de México el escepticismo respecto a la efectividad de las instituciones encargadas de procurar la justicia se da en el entorno de una creciente percepción de inseguridad (IEEM, 2020).

**Tabla 35. Puntajes percepción sobre corrupción**

| | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|
| Argentina | -0,27 | -0,28 | -0,07 | -0,08 | -0,14 |
| Brasil | -0,42 | -0,54 | -0,46 | -0,39 | -0,41 |
| Chile | 1,06 | 1,03 | 0,99 | 1,01 | 1,13 |
| Colombia | -0,36 | -0,41 | -0,32 | -0,26 | -0,23 |
| México | -0,83 | -0,93 | -0,93 | -0,90 | -0,90 |
| Perú | -0,41 | -0,54 | -0,58 | -0,49 | -0,50 |

Una vez revisados los puntajes del Índice de Gobernanza para América Latina, y al contrastar estas puntuaciones con la realidad de cada país, se puede evidenciar la problemática de gobernanza que envuelve a la región.

### 5.3. Panorama de la Globalización: Índice de la Globalización

La globalización mundial ha experimentado cambios significativos en el período comprendido entre 2016 y 2020. Durante estos años, se ha producido una desaceleración en el comercio mundial debido a la incertidumbre económica, la volatilidad financiera y el creciente proteccionismo.

Según el Índice de Globalización del Instituto de Investigación Económica Konjunkturforschungsstelle KOF (KOF Globalization Index), Japón es el campeón de la globalización (KOF, 2020). Este informe también reporta cómo dos países de la UE altamente desarrollados, bien conectados y relativamente pequeños lideran la clasificación con un margen generoso. Concretamente, los Países Bajos e Irlanda, que logran más de 90 puntos. Los siguientes diez rangos también los ocupan los estados miembros de la UE y Suiza, que también está estrechamente integrada en las estructuras del Mercado Único Europeo a través de numerosos acuerdos bilaterales. Los países no europeos más fuertemente globalizados siguen en los lugares 13 (Canadá) y 21 (Australia). La mayor dependencia del comercio exterior se encuentra en pequeños países europeos como Luxemburgo, Irlanda y Bélgica (KOF 2020).

El Índice de Globalización del Instituto de Investigación Económica KOF (KOF Globalization Index) es una medida cuantitativa desarrollada por el KOF Swiss Economic Institute en la Universidad de Zurich, Suiza, encargada en evaluar el grado de globalización de un país o región. El índice se basa en tres dimensiones: económica, política y social. La dimensión económica se refiere a las relaciones comerciales y financieras internacionales, la dimensión política se refiere a las relaciones políticas y de seguridad internacionales, y la dimensión social se refiere a las relaciones culturales y de movilidad humana. Los países con un índice de globalización más alto son considerados más globalizados. El índice es actualizado anualmente y se utiliza ampliamente en investigaciones académicas y en la toma de decisiones de políticas públicas. Luego de un análisis econométrico, establece la relación

entre la globalización en los países individuales y su respectivo crecimiento económico. Los cambios en el desempeño económico en cada país debido a la globalización se trasfieren a una clasificación. Finalmente se elige el campeón de la globalización. Este es el país que exhibe el mayor crecimiento absoluto en el ingreso per cápita (KOF, 2020).

El Índice general de globalización contiene los tres subíndices económicos (ponderado 60%), social y político (ponderado 20%, respectivamente) (KOF, 2020). En general la globalización económica se compone de la globalización comercial y financiera cada uno con un peso del 50 por ciento. La globalización social consiste en el contacto personal, los flujos de información y la proximidad cultural donde cada subíndice aporta un tercio y la globalización política considera aspectos como el número de tratados internacionales o la pertenencia a organizaciones internacionales (KOF, 2020).

### 5.3.1. Índice de la Globalización de América Latina

En muchos mercados emergentes, los mercados financieros y de capital en particular están mucho menos integrados internacionalmente que los de la mayoría de los países industrializados (KOF, 2020). América Latina ha conseguido un nivel de globalización en las últimas décadas, pero en general ha tenido un índice de globalización más bajo en comparación con otros países desarrollados o en desarrollo. Según KOF (2020), los países de América Latina con un mayor índice de globalización son: Chile, México, Costa Rica, Panamá y Perú. También ha enfrentado desafíos en la protección del medio ambiente y en la promoción de políticas sostenibles.

La Figura 35 representa la evolución del Índice de Globalización en los países objeto de análisis en el presente estudio, durante el periodo 2016 a 2020. Según este índice, Argentina, después de una disminución continua del grado de globalización de 1995 a 2014, comenzó a crecer nuevamente en 2014. En 2016, primer año de la serie temporal analizada, Argentina obtuvo un índice de globalización de 0.54, ubicándose en el puesto número 93 a nivel mundial. Sin embargo, en los años siguientes, el índice de globalización de Argentina ha disminuido, alcanzando su punto más bajo en 2020 con un índice de 0.45, ubicándose en el puesto número 97 a nivel mundial.

En 2016 Brasil obtuvo un índice de globalización de 0.63, ubicándose en el puesto número 72 a nivel mundial. Sin embargo, en los años siguientes, el índice de globalización de Brasil ha disminuido, alcanzando su punto más bajo en 2020 con un índice de 0.59, ubicándose en el puesto número 78 a nivel mundial.

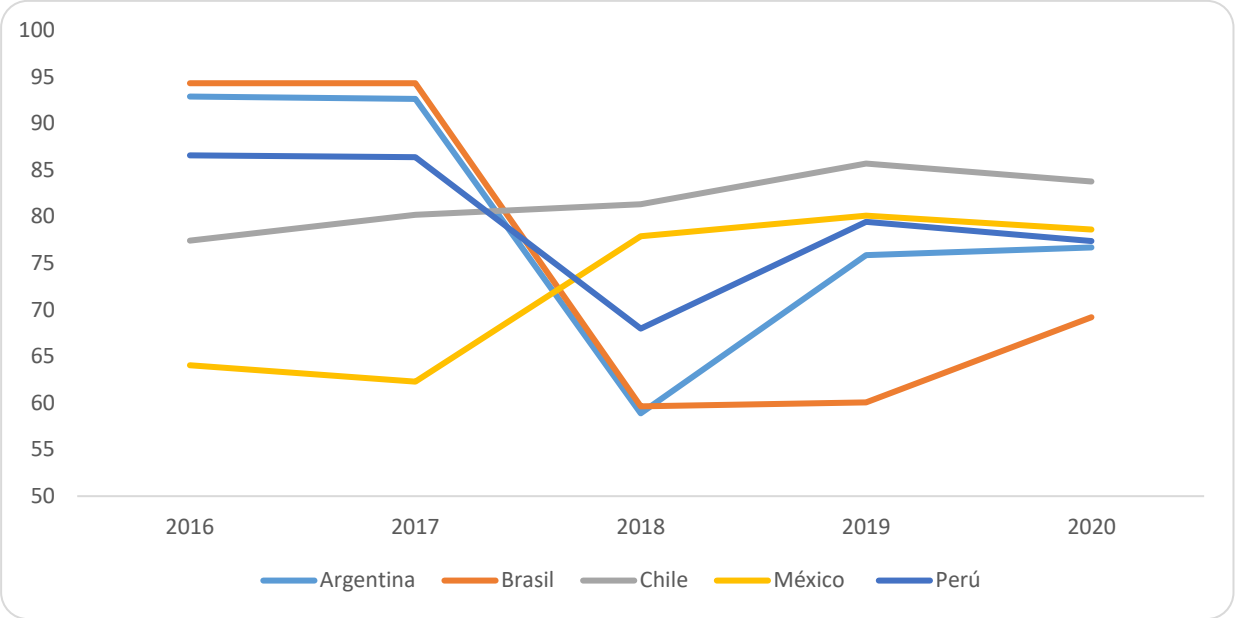
En 2016 Chile obtuvo un índice de globalización de 0.73, ubicándose en el puesto número 54 a nivel mundial. En los años siguientes, el índice de globalización de Chile ha mantenido un nivel similar, con un índice de 0.74 en 2017, 0.75 en 2018, 0.73 en 2019 y 0.72 en 2020, ubicándose en los puestos número 52, 51, 55 y 55 respectivamente a nivel mundial. Chile ha aumentado constantemente su integración en la economía mundial desde 1990 hasta 2007. Desde entonces, ha estado aproximadamente en la mediana de los países informantes. Ningún otro país emergente se ha beneficiado más de la globalización en términos de aumento de ingreso per cápita (KOF, 2020).

Colombia presentó un índice de globalización de 0.58, ubicándose en el puesto número 80 a nivel mundial. En los años siguientes, el índice de globalización de Colombia ha mantenido un nivel similar, con un índice de 0.59 en 2017, 0.58 en 2018, 0.57 en 2019 y 0.56 en 2020, ubicándose en los puestos número 78, 79, 83 y 84 respectivamente.

México logra en 2016 un índice de globalización de 0.68, ubicándose en el puesto número 61 a nivel mundial. En los años siguientes, el índice de globalización de México ha mantenido un nivel similar, con un índice de 0.69 en 2017, 0.68 en 2018, 0.67 en 2019 y 0.65 en 2020, ubicándose en los puestos número 59, 59, 63 y 65. Ocupa uno de los lugares más bajos en el ranking del índicey, aunque el país experimentó un aumento de la globalización de 2004 a 2011, sus ganancias de ingreso per cápita son bastante bajas debido al aumento tardío de la integración global.

Por último, Perú reporta un índice de globalización de 0.68, ubicándose en el puesto número 61 a nivel mundial. En los años siguientes, el índice de globalización de Perú ha mantenido un nivel similar, con un índice de 0.68 en 2017, 0.69 en 2018, 0.67 en 2019 y 0.66 en 2020, ubicándose en los puestos número 59, 59, 63 y 64.

**Figura 35. Índice de Globalización países de América Latina**

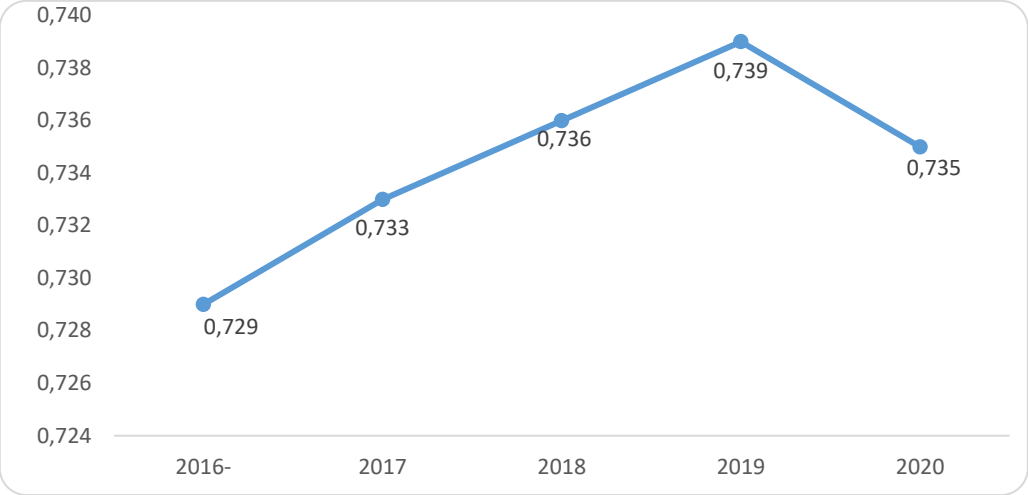



Nota. Elaborado con base en KOF 2016, 2017, 2018, 2019 y 2020.

## 5.4. Panorama Económico y Social: Índice de Desarrollo Humano

El Desarrollo Humano es un enfoque promovido por el Programa de las Naciones Unidas para el Desarrollo (PNUD) centrado en la calidad de vida de las personas y su bienestar general. Desde esta perspectiva, el Índice de Desarrollo Humano (IDH), introducido en 1990, se creó para enfatizar que las personas y sus capacidades deberían ser el criterio fundamental para evaluar el desarrollo de un país, sin limitarlo al crecimiento económico (PNUD, 2023). Este índice incorpora medidas relacionadas con la esperanza de vida al nacer (salud), la tasa de alfabetización y de matriculación (educación) y el ingreso nacional bruto per cápita ajustado según la paridad del poder adquisitivo (nivel de vida digno). En general, para nuestro estudio podemos decir que el Índice de Desarrollo Humano ofrece un enfoque multidimensional que va más allá de la producción económica de un país, a partir de la inclusión de aspectos sociales, consideración de la desigualdad con un enfoque centrado en las personas y comparabilidad internacional. Entre los países con el mayor Índice de Desarrollo Humano se encuentra Suiza, Noruega, Islandia, Hong Kong, China (RAE) y Australia. El Índice de Desarrollo Humano presenta un aumento sostenido de 2016 a 2019. Sin embargo, en el 2020, debido a la pandemia de COVID-19, el índice registra un decrecimiento (Figura 36).

**Figura 36. Índice de Desarrollo Humano Mundial 2016-2020**

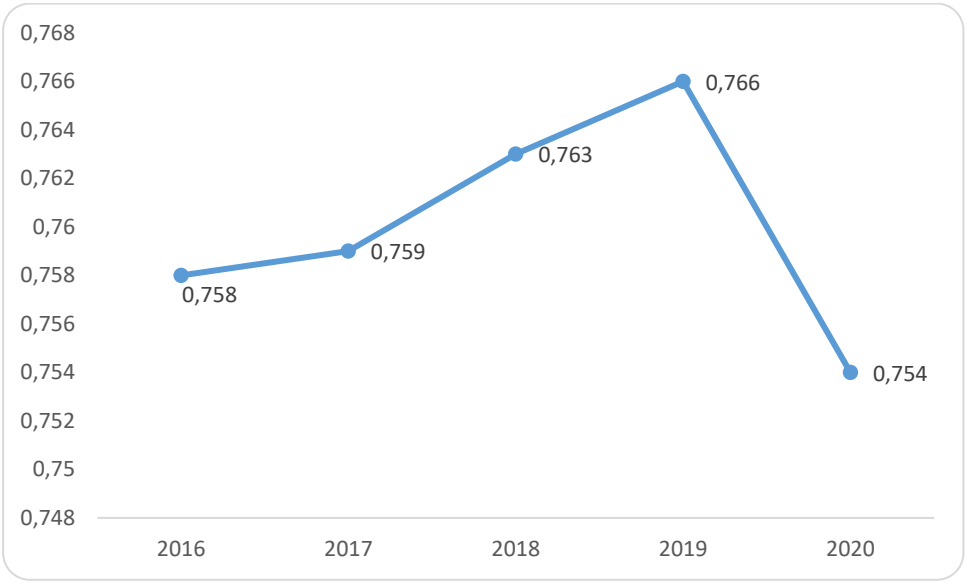



Nota. Elaborado con base en Informes PNUD 2016-2020

### 5.4.1. Índice de Desarrollo Humano en América Latina

En los albores del nuevo milenio, la mayor parte de las economías de América Latina pasaron de un desarrollo dirigido por el Estado a uno impulsado por el mercado, pero la correspondiente adaptación de las instituciones políticas y sociales ha sido lenta, despareja y conflictiva (Von Haldenwang, 2005). Según BID (2023) los gobiernos de la región presentan dificultades para encontrar recursos públicos para promover intervenciones que reduzcan la pobreza y la desigualdad, o mejoren la productividad. Si bien América Latina y el Caribe está casi exclusivamente constituida por países de renta media, se caracteriza también por ser la región más desigual del mundo. (Gaudin & Pareyón, 2020). La Figura 37 revela que el Desarrollo Humano en América Latina presenta una ligera disminución desde 2016 hasta 2020, en general, se mantiene estable. Brasil, no experimenta cambios significativos. Chile reporta un aumento permanente, sin alteraciones notables. Colombia también notifica un aumento gradual. México experimenta una pequeña disminución durante el período objeto de estudio. Por su parte, Perú registra un progreso en el desarrollo humano del país.

**Figura 37. Índice de Desarrollo Humano en América Latina 2016-2020**




Nota. Elaborado con base en PNUD 2016 – 2020. Fuente: https://report.hdr.undp.org/es/intro/

## 5.5. Investigación sobre variables país como factor de divulgación de riesgos

A partir del panorama descrito en aspectos de nivel macro como Ciberseguridad, gobernanza, globalización y crecimiento económico de los países objeto de estudio. A continuación, presentaremos el marco teórico de la investigación que relaciona los factores institucionales como determinantes país de la divulgación de información y la literatura previa relacionada, será bajo este panorama que formularemos las hipótesis del presente estudio.

### 5.5.1. Marco teórico

Algunos estudios precedentes que tienen como objetivo relacionar la divulgación de información corporativa con los determinantes a nivel país, han tomado como referente la teoría institucional (Baldini et al., 2018; Barakat et al., 2015; Barry,et al., 2021; Ellimäki et al., 2021; Gerged et al., 2021). Según Bhatia & Makkar (2020) se ha descubierto que el entorno de gobernanza, la globalización son determinantes significativos de la divulgación de la RSE para los países en desarrollo. En esta investigación la teoría institucional se refiere a la idea de que las instituciones (relacionadas con la Ciberseguridad nacional, el sistema de gobernanza, la globalización y el sistema económico de un país) tienen un gran impacto en

un tema de importancia para todos los grupos de interés ´la divulgación de información sobre el riesgo de Ciberseguridad´. Las bondades de esta teoría incluyen una mejor comprensión de cómo las instituciones influyen en la economía, la política y la sociedad en general, y cómo pueden ser cambiadas para mejorar la vida de las personas. También puede ayudar a identificar problemas institucionales y proponer soluciones para ellos. Además, permite comprender mejor como se establecen las normas y los valores y cómo estos influyen en la conducta humana.

En resumen, la teoría institucional es una herramienta valiosa para entender y mejorar las estructuras sociales y económicas. Según la teoría institucional, las empresas modifican su comportamiento para adaptarse a la guía y expectativas de las instituciones (Campbell, 2007; Roe, 1991). Por la palabra 'institución', usualmente tenemos en mente ciertas 'tipificaciones' donde bajo ciertas condiciones X, se espera que un tipo particular de actor Y haga Z (Berger et al, 2016). Como afirma Bebbington et al. (2009), no solo una o dos instituciones, sino una combinación de todas las instituciones, darán forma a los requisitos organizacionales para la legitimidad social. Una idea que a menudo se olvida es el hecho de que el proceso de institucionalización está ligado a la historia (Brammer et al., 2012). Las instituciones son el resultado de luchas históricas sobre los entendimientos y las reglas del juego prevalecientes (Thelen, 2003).

Las instituciones a nivel del país proponen elementos formales e informales que brindan modelos y estándares legítimos de comportamiento social aceptable. Campbell (2007), Doh & Guay (2006), Hiss (2009), Judge et al., (2008) y North (1994), reconocen la influencia tanto de las instituciones formales (leyes, políticas, organismos y acuerdos formales), como de las instituciones informales (normas de comportamiento, entidades y códigos morales) creados por diferentes creencias culturales, religiosas o políticas que residen en diferentes áreas geográficas; es así como en ambos entornos institucionales, las organizaciones tienden a promover intereses colectivos (Matten & Moon, 2008). Las instituciones formales, como los organismos reguladores, pueden influir en la presentación de reportes por parte de las empresas al proporcionar incentivos tangibles para cumplir con las normas de presentación de informes (Yang & Rivers, 2009) y penalizar el incumplimiento (Momin & Parker, 2013). En esta dinámica, la investigación previa ha revelado que las organizaciones que operan dentro de contextos sociales similares tienden a adoptar características y normas de

comportamiento análogos (Campbell, 2007; Claessens & Fan, 2002; DiMaggio & Powell, 1983; Filatotchev & Nakajima, 2014; La Porta et al., 1998).

La teoría institucional asume que las organizaciones empresariales están influenciadas por estructuras sociales más amplias, como la regulación pública y privada y la presencia de organizaciones no gubernamentales y otras organizaciones independientes que monitorean el comportamiento corporativo (Campbell, 2007; DiMaggio & Powell, 1983; Skouloudis et al., 2012). Estas estructuras sociales afectan la actividad y el modo de operación de la empresa (Baldini et al., 2018). Así, la perspectiva institucional ve a las corporaciones como obligadas a cumplir con sus marcos institucionales (Campbell, 2007; Ioannou & Serafeim, 2012; Matten & Moon, 2008).

Según DiMaggio & Powell (1983) la teoría institucional sostiene que las empresas muestran isomorfismo cuando buscan alinear sus prácticas organizacionales, como la divulgación con normas, creencias y estructuras institucionalizadas en un campo organizacional. Estas prácticas corporativas tienen su origen en decisiones de parecerse a otras empresas modelo –isomorfismo mimético– de hacer lo profesionalmente correcto –isomorfismo normativo– o de cumplir con reglas impuestas por fuerzas externas –isomorfismo coercitivo (Frías-Aceituno et al., 2013). El isomorfismo mimético se presume como un tipo de presión de comportamiento comparativo, mediante el cual las organizaciones siguen las prácticas de sus competidores, especialmente los líderes dentro del campo organizacional. Por su parte, el isomorfismo normativo, implica la alineación de las prácticas organizacionales con las normas sociales colectivas o los comportamientos esperados promovidos por los interesados institucionales, como las ONG y las asociaciones profesionales. Por último, el isomorfismo coercitivo ocurre cuando las empresas se ven obligadas a adherirse a ciertas prácticas organizacionales impuestas por partes interesadas externas poderosas, generalmente en forma de regulación dura o blanda (Castello & Lozano, 2011; DiMaggio & Powell, 1983; Meyer & Rowan, 1977; Sonpar et al., 2010; Suchman, 1995).

Los teóricos institucionales han comenzado recientemente a abogar por un mayor enfoque en la relación entre los factores a nivel institucional y la divulgación de información. En el caso de las revelaciones sobre Ciberseguridad, las características institucionales reflejan diferencias entre países con respecto a la transferencia del riesgo cibernético entre gobiernos y empresas (Falco et al., 2019). En todo el mundo, los enfoques gubernamentales de la

Ciberseguridad varían significativamente (Barry et al., 2021). Para nuestro estudio es importante señalar que América Latina, como región en sí, presenta un contexto institucional único.

Respecto a la divulgación de información sobre Ciberseguridad reportada por las organizaciones latinoamericanas, el isomorfismo coercitivo estará definido por la participación de un actor institucional, como el gobierno nacional de un país; el isomorfismo normativo por los entes de vigilancia y control, las bolsas de valores y demás organismos reguladores nacionales e internacionales que intervengan en la dinámica corporativa; y por último, el isomorfismo mimético estará dado por la dinámica de las empresas líderes en los diferentes sectores.

### 5.5.2. Literatura Previa

Atendiendo a la literatura previa sobre divulgación de riesgos de Ciberseguridad (Barry et al., 2021) y revelaciones de información en general (Baldini et al., 2018; Barakat et al., 2015; Ellimäki et al., 2021; Gerged et al., 2021), y tomando como base la teoría y la lógica institucionales, pretendemos analizar la medida en que los entornos nacionales contribuyen al alcance de la divulgación de información sobre Ciberseguridad en América Latina.

De acuerdo con Hitchens & Goren (2017), la Ciberseguridad trasciende las fronteras nacionales de muchas maneras, ya que la infraestructura técnica de Internet tiene un alcance global, los actores de amenazas basados en un país pueden disfrazar sus identidades tomando el control de los computadores en otros países, y las consecuencias de un ataque disruptivo pueden extenderse mucho más allá de la víctima inicial. En este panorama, la actividad de intercambio cibernético entre las naciones también presenta diferencias en ideología y objetivos geopolíticos. Según el objeto de este estudio revisaremos algunos determinantes país y su influencia en específico con la divulgación de información de Ciberseguridad.

Según nuestra búsqueda, la literatura previa presenta un único estudio que se acerca al tema (Barry et al., 2021) (Tabla 36). En él, los investigadores exploran las diferencias en las revelaciones cualitativas entre las empresas chinas que cotizan en los Estados Unidos y sus contrapartes nacionales del país norteamericano. Las diferencias institucionales entre los dos países son sustanciales: en China la participación del gobierno presenta un sólido marco

regulatorio que externaliza la Ciberseguridad y, por lo tanto, reduce la necesidad de divulgar la conciencia de Ciberseguridad por parte de las empresas; mientras que en los Estados Unidos la responsabilidad de divulgación se traslada directamente a las compañías. Los resultados del estudio proporcionan evidencia sobre la visión del mercado de la conciencia de Ciberseguridad de las empresas y su susceptibilidad frente a los cambios en las percepciones del entorno institucional de las empresas.

**Tabla 36. Estudio previo sobre los efectos de las características institucionales a nivel país y la divulgación de información de Ciberseguridad**

| Autor | País | Años | Variables | Muestra |
|---|---|---|---|---|
| (Barry et al., 2021) | China y Estados Unidos | 2012-2018 | Variables del modelo diferencias transversales en las revelaciones:<br>**Dependiente**:<br>Divulgación de Ciberseguridad<br>**Independiente:**<br>- Dicotómica empresa con sede en China (1) o fuera (0).<br>**Control:**<br>Tamaño de la empresa, rentabilidad, el apalancamiento, la relación mercado-valor contable, oportunidades de crecimiento y el gasto de capital e intensidad de capital, la competencia, la longitud total del archivo, la propiedad institucional total. | **Teoría** Institucional |

En razón a la escasa literatura que vincula los factores a nivel país y la divulgación en particular de Ciberseguridad, relacionamos algunos estudios que en esta misma línea han investigado la incidencia de variables de gobernanza país y la divulgación de información en general, a los efectos de contar con referentes cercanos a nuestra investigación.

El primero de estos factores es el que hace referencia a la gobernanza a nivel país, normalmente a partir del Índice de Gobernanza Mundial, publicado por el Banco Mundial. Los gobiernos deben mejorar la gobernanza y los servicios públicos para poder responder a las expectativas cambiantes y las demandas crecientes (OECD, 2019). A continuación, la Tabla 36 presenta los estudios previos sobre los efectos de las variables de Gobernanza

Nacional en la divulgación de información corporativa. Barakat; Hussainey (2013) investigan los efectos directos y conjuntos de la gobernanza, la regulación y la supervisión bancaria sobre la calidad de la divulgación de riesgos operativos en los bancos europeos. Sus hallazgos recomiendan mantener la independencia de la Junta, mejorar la actividad del comité de auditoría, facilitar la entrada a los requisitos bancarios y promover un papel más proactivo para los supervisores bancarios. Por su parte, Ernstberger & Grüning (2013) evaluan la incidencia del entorno regulatorio de un país y su efecto en la divulgación de información, encontrando una relación positiva entre la fortaleza del sistema legal con respecto a la divulgación en términos de la información que una empresa proporciona a las partes interesadas en su informe anual. Usando tres medidas derivadas del Índice de Gobernanza Mundial (WGI), examinan hasta qué punto los tres factores de gobernanza durante un período de cinco años inciden en la divulgación de información. Los resultados en el desarrollo institucional del país de origen influye en la relación entre las estrategias internacionales y ambientales de una empresa. Barakat et al. (2015) evalúan los factores institucionales formales que pueden influir en la divulgación de riesgos de Ciberseguridad el contexto legal y la existencia de mecanismos de control. Encuentran también una asociación positiva entre la divulgación de riesgos y el sistema legal, las características de la firma de auditores externos y el Gobierno Corporativo. Baldini et al. (2018) proporcionan evidencia de que las características a nivel de país, como un sistema político (marco legal y corrupción), el sistema laboral y el sistema cultural afectan significativamente las prácticas de divulgación de información ambiental de las empresas. Los resultados de las características a nivel de empresa relacionadas con la visibilidad de una empresa (cobertura de analistas, cotización cruzada, apalancamiento y tamaño) demuestran un efecto positivo y homogéneo en la divulgación de Ambiental, Social y de Gobernanza y cada pilar. Elamer et al. (2020) examinan el impacto de la supervisión de la Junta y las estructuras de gobierno en el alcance de las divulgaciones de riesgo operativo. Encuentran que la propiedad del bloque, la independencia de la Junta, la calidad de la gobernanza a nivel de país y la globalización progresiva de una empresa aumenta la divulgación, estas variables son estadísticamente significativas y se asocian positivamente con la divulgación de riesgos. Por otra parte, Ellimäki et al. (2021) demuestran que la globalización progresiva de una empresa aumenta su divulgación ambiental. Meftah Gerged et al. (2021) examinan la influencia de la gobernanza a nivel de país en la divulgación entre los sectores no financieros Los datos confirman una tendencia creciente en la información ambiental publicada en los informes anuales de las empresas.

**Tabla 37. Estudios previos sobre los efectos de las variables de gobernanza nacional en la divulgación de información corporativa**

| Autor | País | Años | Variables | Muestra |
|---|---|---|---|---|
| (Barakat; Hussainey, 2013) | UE | 2008-2010 | **Dependiente:**<br>Índice de calidad divulgación de riesgos operativos.<br>**Independiente:**<br>Requisitos de ingreso a la banca<br>Los poderes oficiales y la independencia de las autoridades de supervisión bancaria<br>- Proporción de directores externos que forman parte del directorio<br>- Proporción de derechos de voto que posee el primer accionista.<br>- Tenencia en bloque gubernamental.<br>- Proporción de derechos de voto.<br>- Frecuencia de las reuniones del Comité de Auditoría.<br>- Regulaciones bancarias<br>**Control:**<br>Tamaño del banco, efectos de la cotización cruzada, medición cuantificar el capital regulatorio por riesgo operativo, la fortaleza de los derechos de los accionistas, el entorno legal a nivel de país, grado de concentración bancaria nacional. | **Teorías**<br>de la legitimidad, de la dependencia de los recursos y de las partes interesadas |
| (Ernstberger & Grüning, 2013) | 16 países europeos | 2007 | **Dependiente**: índice de divulgación de la empresa, índice de Gobierno Corporativo de la empresa<br>**Independiente:**<br>- Índice anti - director aplicado,<br>- Estado de derecho del país (WGI).<br>**Control:**<br>Tamaño, rentabilidad, estructura accionaria, apalancamiento, número de países en los que cotiza. | **Teoría**<br>Agencia |
| (Barakat et al., 2015) | Palestina y Jordania | 2011 | **Dependiente:**<br>Índice de divulgación del nivel de responsabilidad social corporativa.<br>**Independiente**:<br>- Sistema legal<br>- Empresas de auditoría<br>- Gobierno Corporativo (tamaño, comités de la Junta, independencia de la Junta.<br>**Control:**<br>Tamaño, industria, rentabilidad y años. | **Teoría**<br>Institucional |
| (Baldini et al., 2018) | Países de Asia, Europa, África, América y Oceanía. La mayoría de las observaciones corresponden a Japón, Estados Unidos, Reino Unido, Australia. | 2005-2012 | **Dependientes:**<br>Divulgación de ESG, ambientales, sociales y de gobernanza.<br>**Independientes:**<br>Legal Framework nivel de "institución formal", Corrupción WGI, Protección laborales, Tasa de desempleo, Individualismo, Distancia de poder, Leverage, Cobertura de analistas, N° de marcados en los que cotiza la empresa, Tamaño LN del valor de mercado.<br>**Control:**<br>Ley de RSC, PIB de capitalización de mercado, Rentabilidad, Crecimiento de las ventas. | **Teoría**<br>Institucional, Legitimidad |
| (Elamer et al., 2020) | Bahréin, Egipto, Jordania, Kuwait, Líbano, Omán, | 2006-2013 | **Dependientes:**<br>ORD Divulgación de riesgo operativo<br>**Independientes:** | **Teorías**<br>Agencia, Señalización, |

| | | | | |
|---|---|---|---|---|
| | Qatar, Arabia Saudita, Siria y los Emiratos Árabes Unidos | | Existencia de SSB, miembros de SSB, reuniones de SSB, propiedad del bloque, tamaño de la Junta, directores no ejecutivos, gobernanza a nivel de país WGI (6 dimensiones de Kaufmann).<br>**Control:**<br>Tamaño del banco, ROA, Diversidad de ingresos, Eficiencia de las operaciones, crisis financiera, Inflación, PIB per cápita y Dummies para los años fiscales. | Legitimidad y dependencia de recursos. |
| (Ellimäki et al., 2021) | Empresas de energía y servicios públicos de Asia, Europa, América, África del ser, Australasia. | 2011-2018 | **Dependientes:**<br>Divulgación ambiental, desempeño ambiental<br>Internacionalización interregional representa el porcentaje de ventas de las empresas fuera de sus regiones de origen.<br>Moderadora:<br>Desarrollo institucional del país de origen WGI,<br>**Control:**<br>Tamaño de la empresa, ventas totales, ROA, Industria, Origen. | **Teoría**<br>Institucional |
| (Gerged et al., 2021) | Países del Consejo de Cooperación del Golfo | 2010-2014 | **Dependientes:**<br>EDI Índice de divulgación no ponderado, WEDI Índice de divulgación ponderado, SUB-EDI1 Subíndice política ambiental, SUB-EDI2 Contaminación ambiental, SUB-EDI3 energía ambiental, SUB-EDI4 financiero ambiental, SUB-EDI5 otro subíndice ambiental.<br>**Independientes:**<br>Virginia: Puntuación de voz y rendición de cuenta WGI; Efectividad del gobierno WGI; Control de la corrupción WGI.<br>**Control:**<br>Activos totales; apalancamiento; sector; tipo de auditor; PIB | **Teoría**<br>Institucional |

### 5.5.3 Hipótesis del Estudio

## Índice Global de Ciberseguridad (GCI)

Según nuestra búsqueda, Krishna & M.P (2021) utilizan el Índice Global de Ciberseguridad como variable explicativa desde la perspectiva institucional para examinar las relaciones entre el desarrollo del gobierno electrónico, el compromiso con la seguridad cibernética, el uso comercial y la prosperidad económica del país. Bajo este panorama, se presume que los países que presentan un mayor índice de Ciberseguridad responden a un compromiso y a la incorporación de buenas prácticas frente a la seguridad cibernética, como es el caso de la divulgación de información de Ciberseguridad. Según ITU (2020) “el objetivo del IGC es ayudar a los países a determinar los aspectos susceptibles de mejora en el campo de la ciberseguridad e instarles a tomar medidas al respecto” p.133. Estas iniciativas son aplicables al contexto organizacional por lo tanto objeto de divulgación en sus informes y

comunicaciones corporativas. Destacamos el hecho de que la literatura previa no ha considerado esta variable en los estudios de difusión de la Ciberseguridad.

En consecuencia, consideramos la siguiente hipótesis:

***H1:*** *Existe una relación significativa y positiva entre el Índice Global de Ciberseguridad y el nivel de divulgación de información de Ciberseguridad de las empresas cotizantes de América Latina.*

**Gobernanza Nacional**

La gobernanza a nivel país es un concepto muy amplio y multidimensional que se puede estudiar desde diferentes ópticas. Según Hirst (2010), los economistas reconocen que las instituciones importan, que las economías dinámicas se sustentan en leyes, instituciones sociales y valores apropiados. El buen gobierno, por lo tanto, significa crear un marco político efectivo que conduzca a la acción económica privada: regímenes estables, el estado de derecho, una administración estatal eficiente adaptada a los roles que los gobiernos pueden desempeñar y una sociedad civil fuerte e independiente del Estado (Pierre, 2000). En general, la gobernanza se reconoce como el proceso por el cual los gobiernos son seleccionados, monitoreados y reemplazados; la capacidad del gobierno para formular e implementar efectivamente políticas sólidas; y el respeto de los ciudadanos y el Estado por las instituciones que rigen las interacciones económicas y sociales entre ellos (World Bank, 2022).

Según Elamer et al. (2020) se puede argumentar que las prácticas de gobierno a nivel de país pueden cumplir una función de control en entornos de Gobierno Corporativo débiles en comparación con el caso de sus contrapartes fuertes. En los últimos años, varios países han intentado asegurar estos beneficios potenciales de una mayor divulgación imponiendo requisitos de revelación más estrictos a las empresas (Ernstberger & Grüning, 2013). Los estudios previos han tomado la variable gobernanza a nivel nacional en la divulgación de información (Baldini et al., 2018; Elamer et al., 2020, Ellimäki et al., 2021; Ernstberger & Grüning, 2013; Gerged et al., 2021; Li & Zhang, 2010).

La confianza en el gobierno es esencial para la cohesión social y el bienestar, incluida la reducción de la desigualdad, ya que afecta la capacidad del gobierno para implementar reformas (BID, 2020). En este sentido, los países con una mejor gobernanza pueden incentivar la divulgación de información sobre los riesgos de Ciberseguridad porque "tienen instituciones sólidas más resilientes, están en mejores condiciones para facilitar el crecimiento del sector privado, reducir la pobreza, prestar servicios valiosos, abordar el cambio climático, ganarse la confianza de los ciudadanos y, en última instancia, prevenir los conflictos y la fragilidad (WGI, 2023). En América Latina, las debilidades institucionales en varias dimensiones de la gobernanza pública pueden explicar la vulnerabilidad de muchos países de la región frente a ineficiencias causadas por el desperdicio, el mal uso y la captura por parte de grupos de interés, así como frente a los shocks económicos exógenos (BID, 2020). En este contexto, los formuladores de políticas en los países emergentes deben hacer hincapié en mejorar las características de gobernanza del país para mejorar la divulgación de las empresas (Bhatia & Makkar, 2020).

Bajo este panorama, y basándonos en la teoría institucional, planteamos la siguiente hipótesis:

***H2:*** *Existe una relación significativa y positiva entre el Índice de Gobernanza Mundial y el nivel de divulgación de información de Ciberseguridad de las empresas cotizantes de América Latina.*

**Índice de Globalización**

La globalización ha resultado en un aumento de las redes entre las naciones debido a la movilidad de la mano de obra, el capital, los bienes y la tecnología (Bhatia & Makkar, 2020). El Índice de Globalización es una herramienta útil para medir el grado en que un país está integrado en la economía global. Según KOF (2020) el índice combina varios factores, como la conectividad, integración e interdependencia global de los países en las ésferas culturales, ecológicas, económicas, políticas, sociales y tecnológicas. Si bien la literatura previa no ha considerado el Índice de Globalización como variable de estudio en la divulgación de Ciberseguridad, consideramos que puede ayudar en la divulgación de Ciberseguridad, al proporcionar una medida de la integración económica, política y tecnológica de un país con el resto del mundo. Países más globalizados tienden a tener una

mayor interconexión con el resto del mundo, lo que significa una mayor propensión a la exposición a las amenazas cibernéticas. Mientras tanto, los países en desarrollo deben respetar y ajustarse a las normas y reglamentos mientras se globalizan (Bhatia & Makkar, 2020).

Según Chapple & Moon (2005), para ser parte de los negocios globales e internacionales, los países en desarrollo siguen requisitos de divulgación mejorados impuestos por las naciones desarrolladas y, por lo tanto, la divulgación tiende a mejorar aún más. Según Jamali et al. (2008), la globalización y el comercio internacional se ha reflejado en una mayor complejidad comercial y nuevas demandas de mayor transparencia y ciudadanía corporativa. La globalización y la expansión de las transacciones entre países han sensibilizado a las corporaciones en los países desarrollados y en vías de desarrollo Chapple & Moon (2005) observaron acertadamente que las empresas con exposición internacional, que puede ser en términos de propiedad extranjera o ventas internacionales, tienen mayores niveles de divulgación de RSE. Según Fifka & Pobizhan (2014), la creciente conciencia entre los consumidores globales y los inversores globales en relación con las prácticas comerciales responsables ha estimulado la divulgación de la de aspectos de responsabilidad social empresarial.

Por lo tanto, la comprensión de la globalización y su índice puede ayudar a identificar los países con una mayor necesidad de información y educación en materia de Ciberseguridad. Además, el índice de globalización puede ser utilizado para dirigir esfuerzos de divulgación de Ciberseguridad, asegurando un mayor alcance e impacto en la promoción de la seguridad cibernética. En este sentido, desde la teoría institucional, suponemos que un mayor grado de integración en la economía global incide en el alcance de la divulgación de Ciberseguridad.

La variable globalización ha sido utilizada por Bhatia & Makka (2020) con el propósito de investigar el impacto de este factor de nivel país en el grado de divulgación de la responsabilidad social corporativa (RSC) en un grupo de países en desarrollo y naciones desarrolladas. Este estudio considera la inversión extranjera directa (IED) bruta como porcentaje del PIB como proxy para medir la globalización, y sus resultados muestran que la globalización es un determinate significativopara los países en desarrollo.
Bajo estas consideraciones, planteamos la siguiente hipótesis:

***H3:*** *Existe una relación significativa y positiva entre la puntuación del Índice de Globalización por país y el nivel de divulgación de información de Ciberseguridad de las empresas cotizantes de América Latina.*

**Índice de Desarrollo Humano**

El Índice de Desarrollo Humano se ha empleado en estudios previos como un factor determinante del alcance de la divulgación de información (Asare et al., 2022; Birry., 2020; Duho, 2020; Yu et al., 2021). En el caso de América Latina han propuesto el Índice de Desarrollo Humano como una variable a relacionar con estas revelaciones Cuevas., et al (2013). En este sentido, el Índice de Desarrollo Humano (IDH) puede influir en la divulgación de información corporativa debido a que los países con un mayor IDH pueden representar una mejor calidad de vida por parte de los ciudadanos y por ende un país con mejor salud, mayores ingresos y mejor educación gestionará de una mejor manera los riesgos corporativos en este caso los relacionados con fallas de ciberseguridad. Según BID (2023), la región se enfrenta a un reto social con cerca del 18% de la población viviendo con menos de USD 3,1 por día, los niveles de pobreza de la región superan los de hace una década.

Desde esta perspectiva, formulamos esta nueva hipótesis:

***H4:*** *Existe una relación significativa y positiva entre el Índice de Desarrollo Humano por país influye de forma significativa y positiva en el alcance de la divulgación de información de Ciberseguridad de las empresas cotizantes de América Latina.*

## 5.6. Metodología

### 5.6.1. Población y Muestra

La población objeto de estudio esta compuesta por las empresas listadas en los principales índices bursátiles de los países latinoamericanos de mayor capitalización de la región: Argentina, Brasil, Chile, Colombia, México y Perú de cuatro sectores económicos distintos: energía, financiero, consumo discrecional y materiales. La muestra final presenta un total de 85 empresas equivalente a 425 observaciones durante el período 2016-2020. La recopilación de la información, se lleva a cabo a partir del análisis de contenido de los informes anuales

publicados en los sitios web de las empresas y del informe 20 F en el caso de las empresas emisoras reguladas por SEC.

### 5.6.2. Variables

**Variable dependiente**

Esta variable se obtiene a través de la aplicación del Índice de Divulgación de Información sobre Ciberseguridad que se ha diseñado en el capítulo tres. Nuestra variable dependiente mide el alcance de la divulgación de Ciberseguridad en los informes anuales y en los reportes presentados en el Formulario 20 F de las empresas latinoamericanas.

**Variables independientes**

El Índice de Ciberseguridad como una medida multidimensional se estructura por la evaluación de las medidas legales, técnicas, organizacionales, de desarrollo de capacidades y de cooperación a nivel nacional. Utilizado por Krishna & M.P (2021).

El Índice Mundial de Gobernanza, instrumento de medición multidimensional, se estructura en seis pilares. Variable independiente en investigaciones previas (Baldini et al., 2018; Elamer et al., 2020, Ellimäki et al., 2021; Ernstberger & Grüning, 2013; Gerged et al., 2021; Li & Zhang, 2010).

El Índice de Globalización es una medida cuantitativa que incorpora tres dimensiones económica, política y social utilizado por (Bhatia & Makka, 2020) como variable independiente asociada a la divulgación de información

El Índice de Desarrollo Humano (IDH), introducido en 1990, se creó para enfatizar que las personas y sus capacidades deberían ser el criterio fundamental para evaluar el desarrollo de un país, sin limitarlo al crecimiento económico (PNUD, 2023).

**Variables de control**

La literatura indica que algunas variables podrían influir en la divulgación de empresas cotizadas, y que deberían ser controladas. Según Barry et al. (2021), las variables de control incluyen una gama de probables determinantes de las divulgaciones de seguridad cibernética como el tamaño de la empresa, el apalancamiento, la rentabilidad y los activos intangibles.

Tamaño de la Empresa. Incluimos el tamaño de la empresa como variable de control, ya que estudios previos han encontrado que está relacionada con la divulgación de información corporativa y las variables institucionales a nivel de país (Baldini et al., 2018; Barakat et al., 2015: Barry et al., 2021; Elamer et al., 2020; Ellimäki et al., 2021; Meftah Gerged et al., 2021). Medimos el tamaño de la empresa utilizando el logaritmo natural de los activos totales (Barry et al., 2021). De acuerdo con Barakat et al. (2015) el tamaño de la empresa podría determinar el volumen de información divulgada, las grandes empresas podrían buscar nuevos inversores y divulgar más información para atraer a posibles nuevos inversores. Las grandes empresas divulgan más información para demostrar que sus acciones son consistentes con una buena ciudadanía corporativa (Brammer & Pavelin, 2006). Elamer et al. (2020) y Gerged et al. (2021) encuentran que la variable tamaño de la empresa es considerada un factor significativo en la divulgación.

Intangibles. La variable de control ´activos intangibles´ permite presumir que una mayor proporción de estos, puede sugerir una mayor inversión en software para combatir los riesgos cibernéticos, lo que puede disminuir los riesgos de Ciberseguridad e incidir en el alcance de las divulgaciones.

Apalancamiento. El apalancamiento ha sido una variable de control utilizada por (Baldini et al., 2018; Barakat et al., 2015; Barry et al., 2021; Ernstberger & Grüning, 2013; Gerged et al., 2021). Rentabilidad. Se incluyó como variable control en el modelo porque el mejor desempeño financiero se ha relacionado previamente con la divulgación de información corporativa (Barry et al., 2021; Barakat et al., 2015; Elamer et al., 2020; Ellimäki et al., 2021). Según Barakat et al. (2015) los buenos resultados permiten a las empresas utilizar recursos en nuevas políticas y nuevas estrategias. Utilizamos el rendimiento de los activos (ROA) como indicador de la rentabilidad. Una empresa con buenos resultados tiene que

satisfacer las demandas de información de los grupos de interés (Barakat et al., 2015; Baldini et al., 2018).

**Tabla 38. Resumen de las medidas utilizadas para las variables**

| Variables | Concepto | Signo esperado |
|---|---|---|
| | **Variable dependiente** | |
| Divulgación de Ciberseguridad | Alcance de la divulgación medida obtenida a partir de la aplicación del Índice de Divulgación de Información sobre Ciberseguridad. | |
| | **Variables independientes** | |
| Índice Global de Ciberseguridad | Mide el compromiso de los Estados miembros a UIT con la Ciberseguridad. | *Positivo* |
| Índice de Gobernanza Mundial | Es un indicador de evaluación de la gobernanza mundial. | *Positivo* |
| Índice de Globalización | Es una medida de apertura de una economía a las interacciones comerciales, financieras y culturales con el resto del mundo. | *Positivo* |
| Índice de Desarrollo Humano | Es una medida utilizada para evaluar y comparar el nivel de desarrollo humano de los distintos países del mundo. | *Positivo* |
| | **Variables de control** | |
| Tamaño | Medido por el logaritmo natural de los activos totales | |
| Intangibles | Medido por el valor total de activos intangibles entre el valor total de activos. | |
| Apalancamiento | Porcentaje de la deuda total sobre el patrimonio total. | |
| ROA | Rentabilidad de la empresa (medido por el valor de ingresos totales entre el valor de activos totales). | |

### 5.6.3. Modelo

Se estimó un modelo Data Panel para controlar los efectos fijos específicos de cada empresa. Dado que las variables independientes en nuestro modelo son índices multidimensionales que pueden tener diferencias en su cálculo anual, se ha llevado a cabo un proceso de normalización en concordancia con los resultados obtenidos a través de la aplicación de la Prueba de Hauman tomando como referente el único estudio que relaciona la divulgación de información de ciberegurudad y las características a nivel país (Barry et al., 2021). Esto se ha hecho con el propósito de garantizar que todas las variables tengan una escala y un rango similares. Esta investigación se llevará a cabo a partir del análisis de contenido de los

informes anuales y demás comunicaciones reportadas por las compañías cotizadas de Argentina, Brasil, Chile, Colombia, México y Perú para el intervalo de tiempo 2016-2020.

**Ecuación 1. Modelo data panel por efectos fijos**

$$CyberDiscl_{it} = \beta_0 + \beta_1 GCI_{it} + \beta_2 WGI_{it} + \beta_3 IG_{it} + \beta_4 IDH_{it} + \beta_8 Tamaño_Compañía_{it} + \beta_5 Intangibles_{it} + \beta_6 ROA_{it} + \beta_7 Apalancamiento_{it} + \varepsilon_{it}$$

## 5.7. Resultados y Discusión

La Tabla 39 reporta las estadísticas descriptivas de las variables independientes y de control utilizadas en este estudio. Cada variable independiente presenta un promedio de los puntajes obtenidos por la muestra en el período objeto de estudio. El Índice Global de Ciberseguridad reporta un promedio de (56,61) este resultado muestra una puntuación que apenas supera la media y refleja, en general, la situación de la región entorno al ranking mundial. El valor mínimo corresponde a Perú en 2016 y el máximo a Brasil en 2020. El Índice Mundial de Gobernanza reporta una media de (0,138) valor que refleja el promedio de la muestra, es un valor bajo respecto al obtenido por otras regiones. El valor mínimo corresponde a Brasil en 2016 y el máximo es de Chile en 2018. El Índice Mundial de Globalización (76,70) supera el 76% durante 2019 y especialmente en 2020 describe la realidad desatada por la pandemia COVID-19. El valor mínimo se atribuye a Argentina en 2018 y el máximo a Brasil en 2016. El Índice de Desarrollo Humano presenta una media en el período 2016-2020 de 0,796 valor que refleja el impacto económico de la pandemia COVID-19. El valor mínimo corresponde a Brasil en 2016 y el máximo a Chile en 2019.

**Tabla 39. Estadísticas descriptivas de variables**

| Variable | Obs | Mean | Std Dev | Min | Max |
|---|---|---|---|---|---|
| GCI | 425 | 56,61 | 15,23 | 32,35 | 96,6 |
| WGI | 425 | 0,14 | 1,29 | -4,06 | 2,51 |
| IGM | 425 | 76,70 | 10,85 | 58,89 | 94,31 |
| IDH | 425 | 79,6 | 0,041 | 75,5 | 86,1 |
| Tamaño de la Compañía | 425 | 9,18 | 1,61 | 4,13 | 12,98 |
| Intangibles | 425 | 0,06 | 0,09 | 0,00 | 0,50 |
| Apalancamiento | 425 | 133,36 | 315,09 | 0,00 | 6135,80 |
| ROA | 425 | 4,19 | 4,50 | -11,49 | 26,70 |

La Tabla 40 muestra los coeficientes de correlación entre las variables del modelo. En general, según la matriz de correlación podemos colegir que no existe una asociación significativa entre las variables individuales objeto de estudio.

**Tabla 40. Matriz de correlación**

| | Índice | GCI | WGI | GI | IDH | LN activos | Intangibles | Apalancamiento | ROA |
|---|---|---|---|---|---|---|---|---|---|
| **Índice** | **1,0000** | | | | | | | | |
| **GCI** | 0,1758 | **1,0000** | | | | | | | |
| **WGI** | -0,0267 | -0,3881 | **1,0000** | | | | | | |
| **GI** | -0,0952 | -0,0671 | 0,2741 | **1,0000** | | | | | |
| **IDH** | 0,0739 | -0,4794 | 0,8526 | 0,2166 | **1,0000** | | | | |
| **Tamaño Compañía** | 0,4260 | 0,1488 | 0,0643 | -0,0142 | 0,0174 | **1,0000** | | | |
| **Intangibles** | -0,1279 | 0,0929 | -0,1002 | -0,0284 | -0,1930 | -0,3290 | **1,0000** | | |
| **Apalancamiento** | 0,0379 | -0,0044 | 0,0524 | 0,0952 | 0,0782 | 0,0712 | -0,0825 | **1,0000** | |
| **ROA** | -0,2069 | 0,0018 | -0,1956 | -0,1145 | -0,1623 | -0,4132 | 0,2850 | -0,2021 | **1,0000** |

La Tabla 41 muestra la Prueba de Factor de Inflación de la Varianza VIF, los resultados no se ven afectados por multicolinealidad ya que los factores de inflación de la varianza (VIF) estan dentro del umbral de 10, hallazgos que coinciden con Baldini et al. (2018).

**Tabla 41. Factor de inflación de la varianza VIF**

| Variable | VIF | 1/VIF |
|---|---|---|
| GCI normalizada | 1.35 | 0.740038 |
| WGI normalizada | 3.97 | 0.251669 |
| GI normalizada | 1.10 | 0.908990 |
| IDH normalizada | 4.27 | 0.234135 |
| Tamaño de la compañía | 1.35 | 0.740271 |
| Intangibles | 1.24 | 0.807761 |
| Apalancamiento | 1.05 | 0.948485 |
| ROA | 1.33 | 0.750764 |
| **Mean VIF** | **1.96** | |

Los resultados de la regresión muestran que la variable Índice Global de Ciberseguridad obtiene una relación positiva y fuertemente significativa, respecto al alcance de las divulgaciones de ciberseguridad; hallazgo que coincide con el encontrado por Krishna & M.P (2021) al relacionar el Índice Global de Ciberseguridad con el desarrollo del gobierno electrónico, el compromiso con la seguridad cibernética, el uso comercial y la prosperidad económica del país. En nuestro estudio, esto implica que las empresas ubicadas en países con una puntuación más alta en el índice, tienden a tener un alcance más amplio en sus divulgaciones de ciberseguridad. Se presume que las empresas con mayor Índice Global de Ciberseguridad reflejan "el establecimiento de estrategias y mecanismos para desarrollar capacidades por parte de los gobiernos y las empresas para prepararse mejor y mitigar los crecientes riesgos cibernéticos" (ITU, 2020). Estas compañías corresponden a países que han implementado medidas de seguridad cibernética relacionadas con los aspectos legales, técnicos, organizativos, creación de capacidad y/o cooperación, medidas que seguramente representan información

importante para los grupos de interés porque representan el compromiso con el riesgo cibernético en el quehacer corporativo. En este sentido, nuestros hallazgos suponen un avance sobre la literatura previa al relacionar por primera vez el Índice Global de Ciberseguridad con el alcance de la divulgación sobre seguridad cibernética. Como resultado, se acepta la hipótesis H1.

La variable Índice de Gobernanza Mundial presenta una inversa y fuerte relación con la divulgación de información de ciberseguridad por parte de las empresas cotizantes de América Latina. De esta forma, el efecto de un aumento de las revelaciones de ciberseguridad podría verse afectado por un entorno representado con una buena gobernanza, lo que sugiere que los mecanismos de gobierno a nivel de empresa y de país ejercen efectos complementarios en las divulgaciones corporativas (Baldini et al. 2018; Ernstberger & Grüning, 2013). En relación a este aspecto podemos afirmar que un mayor Índice de Gobernanza Mundial incide de manera importante e inversa en el alcance de las revelaciones de ciberseguridad, se presume que una mayor gobernanza nacional conlleva "un mejor proceso de selección, monitoreo, reemplazo de los gobiernos de un país. Así como la capacidad del gobierno para formular e implementar política sólidas y el respeto de los ciudadanos y el Estado por las instituciones que rigen las interacciones económicas y sociales" (Kaufmann et al., 2010). En este contexto, nuestros hallazgos realizan un aporte novedoso a la investigación al establecer una asociación entre el Índice de Gobernanza Mundial y el alcance de las revelaciones de ciberseguridad. En consecuencia, se confirma la asociación entre las variables de la hipótesis H2 y se presenta la relación opuesta entre el índice de gobernanza y las revelaciones de ciberseguridad.

En cuanto a la variable Índice de Globalización, se observa una asociación directa y significativa con respecto a las revelaciones de ciberseguridad. Estos resultados coinciden con Ellimäki et al (2021) quienes encontraron una relación significativa entre la globalización a nivel nacional y la divulgación de información. Por lo tanto, se acepta la hipótesis H3.

Por último, la variable Índice de Desarrollo Humano presenta una relación significativa e inversa en línea con la divulgación de información. Este hallazgo contrario a estudios

previos (Asare et al., 2022; Birry., 2020; Duho, 2020; Yu et al., 2021) obtiene como resultado que un aumento del Índice se relaciona con una disminución en la divulgación de información de ciberseguridad. Esta situación puede derivar de las características inherentes al entorno latinoamericano, región enmarcada por una escasez de recursos, limitado acceso a internet y tecnología insuficiente.

Es de anotar que en el estudio no se encontró una asociación significativa entre las variables de control y el alcance de la divulgación de ciberseguridad. Por tanto, coincidimos con Barry et al. (2021) que las variables tamaño de la empresa, apalancamiento y rentabilidad no se relacionan de forma significativa con el alcance de la divulgación de ciberseguridad.

**Tabla 42. Resultados del análisis de regresión**

| Variables | Coeficiente<br>(Error Estándar) |
|---|---|
| GCI normalizada | 0.000***<br>(0.066) |
| WGI normalizada | 0.000***<br>(-0.376) |
| GI normalizada | 0.001**<br>(0.161) |
| IDH normalizada | 0.002**<br>(-0.187) |
| Tamaño de la Compañía | 0.194<br>(0.0273) |
| Intangibles | 0.942<br>(0.0130) |
| Apalancamiento | 0.430<br>(0.0000) |
| ROA | 0.595<br>(0.0012) |
| -cons | 0.916<br>(0.0211) |

Los errores estándar corregidos se presentan entre paréntesis

Niveles de significación: *Significancia al 10%, ** Significancia al 5%, *** Significancia al 1%,

## 5.8. Conclusiones

La visión general del panorama de la Ciberseguridad, la gobernanza, la globalización y el desarrollo humano en América Latina se obtiene a partir de la aplicación del índice respectivo: la medición nacional de la Ciberseguridad se consigue a través del Índice Global de Ciberseguridad. Para estudiar la situación de los países de América, hemos revisado los puntajes promedio de los pilares en cada versión del informe GCI 2015, 2017, 2018 y 2020. En general, observamos que Americas ocupa el penúltimo lugar en el ranking por regiones. Europa ocupa el primer lugar, seguido por la Región Arabe, la Comunidad Europea Independiente, Asia Pacífico, Américas y África. Bajo este panorama, podemos señalar que al igual que las demás regiones en la dimensión de medidas legales se obtiene el puntaje más alto. Los demás pilares presentan puntajes que apenas superan la media en medidas técnicas, medidas organizacionales, medidas de creación de capacidad y medidas de cooperación. Respecto a los países de nuestra muestra podemos ver que Brasil presenta las puntuaciones más altas en todas las dimensiones. En la dimensión medidas legales, comparte este primer lugar con Perú. En los demás ítems presenta unas puntuaciones muy altas en comparación con los demás países objeto de este estudio. La aprobación de la Estrategia Nacional de Ciberseguridad por parte de algunos países: Colombia (2016), Chile (2017), México (2017), Argentina (2019) y Brasil (2020) y la expedición de leyes de protección de datos: en Argentina (2016), Brasil (2018), Colombia (2018), Chile (1999), México (2017) y Perú (2011) y los ciberataques del ransomware WannaCry en 2017, del cual, según Creese (2020) CSIRT Americas facilitó la identificación temprana y el aislamiento de puntos críticos de infección en América Latina para detener la propagación de WannaCry dentro de la región.

De acuerdo con Barry et al. (2021), los factores de nivel macrosocial, entre otros la gobernanza nacional, afectan la calidad, la transparencia y la rendición de cuentas. La situación actual de América Latina se deriva de un conjunto complejo de crisis sociales, económicas y políticas interrelacionadas, que se han magnificado con el advenimiento de la pandemia del coronavirus y una ola creciente de aislacionismo y “antiglobalismo” (Merke et al., 2021). De esta manera, si revisamos la medición de la Gobernanza Nacional en la región a través del Índice de Gobernanza Mundial, se evidencia que las puntuaciones de los países objeto de estudio en su mayoría son inferiores a otros países. Es relevante destacar que, a diferencia de Chile, que ha logrado estabilizar su sistema político, Brasil,

Colombia, México y Perú, aún enfrentan desafios relacionados con la inestabilidad política y la violencia.

Respecto al Indice de Globalización, América Latina ha experimentado un cierto grado de globalización en las últimas décadas, no obstante, ha tenido un índice de globalización más bajo en comparación con otros países desarrollados o en desarrollo. En general, América Latina ha experimentado un aumento en el comercio y las inversiones internacionales, pero ha enfrentado desafíos en la integración en la economía global y en la reducción de la pobreza y la desigualdad.

En el ámbito del desarrollo humano en América Latina se habían alcanzado avances significativos en diversos aspectos como la salud, la economía, la educación y el fortalecimiento de la democracia. No obstante, la Pandemia COVID - 19 ha dejado un impacto devastador, generando la necesidad de redoblar esfuerzos en la implementación de políticas públicas nacionales y regionales.

A partir de la teoría institucional, el estudio empírico concluye que las variables explicativas propuestas inciden como factores determinantes, relacionados con las características del país: Índice de Ciberseguridad, de Globalización, de Gobernanza y de Desarrollo Humano respecto a la información revelada sobre los riesgos de Ciberseguridad en América Latina. Estos corresponden a índices multidimensionales que incorporan diferentes factores institucionales del orden nacional. Las empresas que se encuentran en países con un mayor Índice de Ciberseguridad y un Índice de Globalización más alto presentan una asociación positiva y fuertemente significativa, respecto a la variable Índice de Gobernanza Mundial e Índice de Desarrollo Humano se obtiene una relación inversa y significativa.

## 5.9. Referencias

Abbate, J. (2011). Inventing the internet. En *Networks of Innovation*. https://doi.org/10.1093/acprof:oso/9780199269051.003.0003

Abraham, S., & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/J.BAR.2007.06.002

Abraham, S., & Shrives, P. J. (2014). Improving the relevance of risk factor disclosure in corporate annual reports. *British Accounting Review*, *46*(1), 91–107. https://doi.org/10.1016/j.bar.2013.10.002

Abraham, S. the determinants of narrative risk information in U. F. 100 annual reports, & Cox, P. (2007). Analysing the determinants of narrative risk information in UK FTSE 100 annual reports. *The British Accounting Review*, *39*(3), 227–248. https://doi.org/10.1016/J.BAR.2007.06.002

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Adams, R. B., & Ferreira, D. (2007). A Theory of Friendly Boards. *The Journal of Finance*, *62*(1), 217–250. https://doi.org/10.1111/J.1540-6261.2007.01206.X

Adams, R. B., & Ferreira, D. (2009). Women in the boardroom and their impact on governance and performance. *Journal of Financial Economics*, *94*(2), 291–309. https://doi.org/10.1016/j.jfineco.2008.10.007

Adams, R. B., & Funk, P. (2012). Beyond the glass ceiling: Does gender matter? *Management Science*, *58*(2), 219–235. https://doi.org/10.1287/mnsc.1110.1452

Afep Medef. (2015). *Code de gouvernement entreprise revise*.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/CYBSEC/TYY006

Agrawal, A., & Chadha, S. (2005). Corporate governance and accounting scandals. *Journal of Law and Economics*, *48*(2), 371–406. https://doi.org/10.1086/430808/ASSET/IMAGES/LARGE/FG1.JPEG

Agrawal, A., & Knoeber, C. R. (2001). Do some outside directors play a political role? *Journal of Law and Economics*, *44*(1), 179–198. https://doi.org/10.1086/320271

Agrawal, A., & Knoeber, C. R. (2015). Do Some Outside Directors Play a Political Role?*. *https://doi.org/10.1086/320271*, *44*(1), 179–198. https://doi.org/10.1086/320271

Aguilar Antonio, J. M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, *25*.

Agyei-Mensah, B. K. (2017). The relationship between corporate governance

mechanisms and IFRS 7 compliance: evidence from an emerging market. *Corporate Governance (Bingley)*, *17*(3), 446–465. https://doi.org/10.1108/CG-06-2016-0129/FULL/PDF

Ahmed, K., Hossain, M., & Adams, M. B. (2006). The Effects of Board Composition and Board Size on the Informativeness of Annual Accounting Earnings. *Corporate Governance: An International Review*, *14*(5), 418–431. https://doi.org/10.1111/J.1467-8683.2006.00515.X

AICPA. (2017a). *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*. 29. https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/Description-Criteria.pdf%0Ahttps://web.archive.org/web/20170706132715/https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocum

AICPA. (2017b). *Guide Reporting on an Entity´s Cybersecurity Risk Management Program and Controls*.

AICPA. (2018). *Cybersecurity risk management reporting*. 1–4.

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Al-Hadi, A., Hasan, M. M., & Habib, A. (2016). Risk Committee, Firm Life Cycle, and Market Risk Disclosures. *Corporate Governance: An International Review*, *24*(2), 145–170. https://doi.org/10.1111/corg.12115

Al-Sartawi, A. M. A. M., Wadi, R. M. A., & Hannoon, A. (2018). Information Technology Governance and Electronic Financial Disclosure. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11195 LNCS*, 449–458. https://doi.org/10.1007/978-3-030-02131-3_40

Alavi, M., & Weiss, I. R. (1985). Managing the Risks Associated with End-User Computing. *Journal of Management Information Systems*, *2*(3), 5–20. https://doi.org/10.1080/07421222.1985.11517734

Albitar, K., Hussainey, K., Kolade, N., & Gerged, A. M. (2020). ESG disclosure and firm performance before and after IR: The moderating role of governance mechanisms. *International Journal of Accounting & Information Management*, *28*(3), 429–

444. https://doi.org/10.1108/IJAIM-09-2019-0108

Alchian, A., & Demsetz, H. (1972). Linked references are available on JSTOR for this article : Production , Information Costs , and Economic Organization. *The American Economic Review*, *62*(5), 777–795. https://knowledgehub.unsse.org/es/knowledge-hub/relaciones-entre-los-ods-el-plan-para-una-decada-cooperativa-y-el-balance-social-en-cooperativas-2/

Allegrini, M., & Greco, G. (2013). Corporate boards, audit committees and voluntary disclosure: Evidence from Italian Listed Companies. *Journal of Management and Governance*, *17*(1), 187–216. https://doi.org/10.1007/S10997-011-9168-3/TABLES/6

Allini, A., Manes Rossi, F., & Hussainey, K. (2016). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *Public Money & Management*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Allini, A., Manes Rossi, F., & Macchioni, R. (2014). Do Corporate Governance Characteristics Affect Non-Financial Risk Disclosure in Government-owned Companies? The Italian Experience. *FINANCIAL REPORTING*, *1*, 5–31. https://doi.org/10.3280/FR2014-001001

Allini, A., Rossi, F. M., & Hussainey, K. (2015). The board's role in risk disclosure: an exploratory study of Italian listed state-owned enterprises. *http://dx.doi.org/10.1080/09540962.2016.1118935*, *36*(2), 113–120. https://doi.org/10.1080/09540962.2016.1118935

Almazan, A., & Suarez, J. (2003). Entrenchment and Severance Pay in Optimal Governance Structures. *The Journal of Finance*, *58*(2), 519–547. https://doi.org/10.1111/1540-6261.00536

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). *Towards a Taxonomy of Information Security Management Practices in Organisations*. https://openrepository.aut.ac.nz/handle/10292/8174

Althonayan, A., & Andronache, A. (2018). Shifting from information security towards a cybersecurity paradigm. *ACM International Conference Proceeding Series, September 2018*, 68–79. https://doi.org/10.1145/3285957.3285971

Amir, E., & Lev, B. (1996). Value-relevance of nonfinancial information: The wireless communications industry. *Journal of Accounting and Economics*, *22*(1–3), 3–30. https://doi.org/10.1016/S0165-4101(96)00430-2

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Anderson, R. C., Mansi, S. A., & Reeb, D. M. (2004). Board characteristics, accounting report integrity, and the cost of debt. *Journal of Accounting and Economics*, *37*(3), 315–342. https://doi.org/10.1016/j.jacceco.2004.01.004

Andrikopoulos, A., Samitas, A., & Bekiaris, M. (2014). Corporate social responsibility reporting in financial institutions: Evidence from Euronext. *Research in International Business and Finance*, *32*, 27–35. https://doi.org/10.1016/j.ribaf.2014.02.001

Aoki, M., Kim, H.-K., & World Bank. (1995). *Corporate governance in transitional economies : insider control and the role of banks*. 467.

Armstrong, Philip; Segal, Nick; Davis, B. (2006). Corporate Governance in South Africa. En *Handbook on International Corporate Governance*.

Arnum, E. (1995). Doing business on the Internet-A question of balance. *Business Communications Review*.

Asamblea General de las Naciones Unidas. (2001). *Resolución 56/183. Cumbre Mundial sobre la Sociedad de la Información*. 3.

AT&T Cybersecurity. (2021). *What is a Cybersecurity Strategy and How to Develop One*. https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-strategy-explained

ATOS. (2020). *Universal Registration Document Board of Directors 2020*.

Axa. (2020). *AXA Future Risks Report*.

Baginski, S. P., Campbell, J. L., Hinson, L. A., & Koo, D. S. (2018). Do Career Concerns Affect the Delay of Bad News Disclosure? *The Accounting Review*, *93*(2), 61–95. https://doi.org/10.2308/ACCR-51848

Bakker, T. G. (2015). *Beadle Scholar Accuracy of Self-Disclosed Cybersecurity Risks of Large US Banks*. https://scholar.dsu.edu/theses/294

Baldini, M., Maso, L. D., Liberatore, G., Mazzi, F., & Terzani, S. (2018). Role of Country- and Firm-Level Determinants in Environmental, Social, and Governance Disclosure. *Journal of Business Ethics*, *150*(1), 79–98. https://doi.org/10.1007/s10551-016-3139-1

Barakat, AhmedBank; Hussainey, K. (2013). Bank governance, regulation, supervision,

and risk reporting: Evidence from operational risk disclosures in European banks. *International Review of Financial Analysis*, *30*, 254–273. https://doi.org/10.1016/J.IRFA.2013.07.002

Barakat, A., & Hussainey, K. (2013). 0. *International Review of Financial Analysis*, *30*, 254–273. https://doi.org/10.1016/j.irfa.2013.07.002

Barakat, F. S. Q., López Pérez, M. V., & Rodríguez Ariza, L. (2015). Corporate social responsibility disclosure (CSRD) determinants of listed companies in Palestine (PXE) and Jordan (ASE). *Review of Managerial Science*, *9*(4), 681–702. https://doi.org/10.1007/s11846-014-0133-9

Barclay, M. J., & Holderness, C. G. (1991). Negotiated Block Trades and Corporate Control. *The Journal of Finance*, *46*(3), 861–878. https://doi.org/10.1111/J.1540-6261.1991.TB03769.X

Barmpaliou, N. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*.

Barney, J. (2014). Gaining and sustaining a competitive advantage. En P. E. Limited (Ed.), *Introduction to e-Business*. https://doi.org/10.4324/9780080492780-16

Barry, T., Jona, J., & Soderstrom, N. S. (2021). The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3916525

Bartha, Peter; Gillies, J. (2006). Corporate governance in Russia: is it really necessary? En *Corporate governance handbook on international country analysis*.

Bear, S., Rahman, N., & Post, C. (2010). The Impact of Board Diversity and Gender Composition on Corporate Social Responsibility and Firm Reputation. *Journal of Business Ethics 2010 97:2*, *97*(2), 207–221. https://doi.org/10.1007/S10551-010-0505-2

Beattie, V., McInnes, B., & Fearnley, S. (2004). A methodology for analysing and evaluating narratives in annual reports: A comprehensive descriptive profile and metrics for disclosure quality attributes. *Accounting Forum*, *28*(3), 205–236. https://doi.org/10.1016/j.accfor.2004.07.001

Bebbington, J., Kirk, E. A., & Larrinaga, C. (2012). The production of normativity: A comparison of reporting regimes in Spain and the UK. *Accounting, Organizations and Society*, *37*(2), 78–94. https://doi.org/10.1016/j.aos.2012.01.001

Bebbington, J., & Larrinaga-González, C. (2008). Carbon Trading: Accounting and

Reporting Issues. *European Accounting Review*, *17*(4), 697–717. https://doi.org/10.1080/09638180802489162

Berelson, B. (1952). *Content Analysis, Lindzey: Handbook of social psychology*.

Beretta, S., & Bozzolan, S. (2004). A framework for the analysis of firm risk communication. *International Journal of Accounting*, *39*(3), 265–288. https://doi.org/10.1016/j.intacc.2004.06.006

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Berle, A. a, & Means, G. C. (1932). Property in Transaction, The Appearance of the Corporate System, The Concetration of Economic Power. *The Modern Corporation and Private Property*, 24. http://books.google.com/books?id=mLdLHhqxUb4C&pgis=1

Bhatia, A., & Makkar, B. (2020). Stage of development of a country and CSR disclosure – the latent driving forces. *International Journal of Law and Management*, *62*(5), 467–493. https://doi.org/10.1108/IJLMA-03-2020-0068

Biener, C., & Eling, M. (2012). *Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions*. *37*, 77–107. https://doi.org/10.1057/gpp.2011.29

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance: Issues and Practice*, *40*(1), 131–158. https://doi.org/10.1057/gpp.2014.19

BID (2023) Preparar el terreno macroeconómico. Informe maroeconómico de América Latina y el Caribe 2023 para un crecimiento renovado.

Blakley, B., Mcdermott, E., Morganchase, J. P., & Geer, D. (2002). Information Security is Information Risk Management. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*. https://doi.org/10.1145/508171

Bloomfield, R. J. (2002). The "Incomplete Revelation Hypothesis" and Financial Reporting. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.312671

Bogle, J. C. (2005). *The Battle for the Soul of Capitalism*.

Bose, R., & Luo, X. (2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, *22*(3), 194–208. https://doi.org/10.1108/IJAIM-04-2014-0026

Botosan, C. A. (1997). Disclosure level and the cost of equity capital. *Accounting Review*,

*72*(3), 323–349.

Branco, M. C., & Rodrigues, L. L. (2008). Social responsibility disclosure: A study of proxies for the public visibility of Portuguese banks. *The British Accounting Review*, *40*(2), 161–181. https://doi.org/10.1016/j.bar.2008.02.004

Brandeis, L. D. (1914). *Other people's money and how the bankers use it*. https://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-by-louis-d.-brandeis

Bratton, W. W. (1989). *Penn Law : Legal Scholarship Repository The New Economic Theory of the Firm : Critical Perspectives from History The New Economic Theory of the Firm : Critical Perspectives from History*.

Bratton, W. W. (2007). *Hedge Funds and Governance Targets*. https://scholarship.law.upenn.edu/faculty_scholarship://scholarship.law.upenn.edu/faculty_scholarship/862

Brazilian Institute of Corporate Governance. (2020). *Gestión de Riesgos Corporativos* (Brazilian Institute of Corporate Governance (ed.)). https://idbinvest.org/sites/default/files/2021-04/Cuaderno 19 - Gestión de Riesgos Corporativos.pdf

Brennan, N. (2006). Boards of directors and firm performance: Is there an expectations gap? *Corporate Governance: An International Review*, *14*, 577–594.

Brennan, N. M., & Solomon, J. (2008). Corporate governance, accountability and mechanisms of accountability: An overview. *Accounting, Auditing & Accountability Journal*, *21*(7), 885–906. https://doi.org/10.1108/09513570810907401/FULL/PDF

Briano-Turrent, G. D. C., & Poletti-Hughes, J. (2017). Corporate governance compliance of family and non-family listed firms in emerging markets: Evidence from Latin America. *Journal of Family Business Strategy*, *8*(4), 237–247. https://doi.org/10.1016/J.JFBS.2017.10.001

Briano, G. del C. (2012). *Tesis doctoral: Factores institucionales que inciden en la transparencia del Gobierno Corporativo: un estudio en empresas cotizadas*. Universidad de Cantabria.

Brooks, L. (Lily) Z., Cheng, Y., Liu, L., & Yu, M. D. (2021). The timeliness of 10-K filings, early filers, and effects of filing deadline changes. *Journal of Corporate Accounting & Finance*, *32*(2), 169–186. https://doi.org/10.1002/JCAF.22492

Burnap, P. (2021). Risk Management & Governance Knowledge Area. *The Cyber*

*Security Body Of Knowledge*, 19–48.

Bushee, B. J., Carter, M. E., & Gerakos, J. (2014). Institutional investor preferences for corporate governance mechanisms. *Journal of Management Accounting Research*, *26*(2), 123–149. https://doi.org/10.2308/jmar-50550

Bushman, R. M., & Smith, A. J. (2001). Financial accounting information and corporate governance. *Journal of Accounting and Economics*, *32*(1–3), 237–333. https://doi.org/10.1016/S0165-4101(01)00027-1

Business Roundtable. (2018). *Principles of Corporate Governance 2016*. *153*(153), 84–97.

Cabedo, J. D., & Tirado, J. M. (2004). The disclosure of risk in financial statements. *Accounting Forum*, *28*(2), 181–200. https://doi.org/10.1016/j.accfor.2003.10.002

Cadbury. (1992). The Report of the Cadbury Committee on The Financial Aspects of Corporate Governance: The Code of Best Practice. *Corporate Governance: An International Review*, *1*(3), 124–124. https://doi.org/10.1111/j.1467-8683.1993.tb00025.x

CAF. (2013). *Lineamientos para un Código latinoamericano de Gobierno Corporativo* .

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*. https://doi.org/10.1111/RISA.13687

Calder, A. (2008). *Corporate governance : a practical guide to the legal frameworks and international codes of practice* (London).

Calderón, R., Piñero, R., & Redín, D. M. (2018). Can compliance restart integrity? Toward a harmonized approach. The example of the audit committee. *Business Ethics: A European Review*, *27*(2), 195–206. https://doi.org/10.1111/BEER.12182

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing*, *25*(1), 24–39. https://doi.org/10.1111/ijau.12209

Campbell, J. L. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. En *Academy of Management Review* (Vol. 32, Número 3, pp. 946–967). Academy of Management. https://doi.org/10.5465/AMR.2007.25275684

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. min, & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review*

*of Accounting Studies*, *19*(1), 396–455. https://doi.org/10.1007/s11142-013-9258-3

Campbell, K., & Mínguez-Vera, A. (2008). Gender Diversity in the Boardroom and Firm Financial Performance. *Journal of Business Ethics 2007 83:3*, *83*(3), 435–451. https://doi.org/10.1007/S10551-007-9630-Y

Cano, J. (2021). *Ciberseguridad empresarial Reflexiones y retos para los ejecutivos del siglo XXI*.

Carter, D. A., D'Souza, F., Simkins, B. J., & Simpson, W. G. (2010). The Gender and Ethnic Diversity of US Boards and Board Committees and Firm Financial Performance. *Corporate Governance: An International Review*, *18*(5), 396–414. https://doi.org/10.1111/J.1467-8683.2010.00809.X

Carter, D. A., Simkins, B. J., & Simpson, W. G. (2003). Corporate Governance, Board Diversity, and Firm Value. *Financial Review*, *38*(1), 33–53. https://doi.org/10.1111/1540-6288.00034

Castro, S. (2009). Practicas de Gobierno Corporativo en America Latina. *Revista Latinoamericana de Administración*, *43*, 26–40.

Cavelty, M. D. (2010). *Cyber-Security* (Routledge (ed.)). The Routledge Handbook of New Security Studies: 154-162.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

CCB, & OCDE. (2004). *"White paper" sobre Gobierno Corporativo en Latinoamerica*. *7*, 92.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images. December*. http://www.sei.cmu.edu

CEUPE. (2019). Modelos de Gobierno Corporativo. *Centro europeo de postgrado*, 1. https://www.ceupe.com/blog/modelos-de-gobierno-corporativo.html

Chang, H. C. (2016). The Synergy of Scientometric Analysis and Knowledge Mapping with Topic Models: Modelling the Development Trajectories of Information Security and Cyber-Security Research. *http://dx.doi.org/10.1142/S0219649216500441*, *15*(4). https://doi.org/10.1142/S0219649216500441

Chang, L. S., Most, K. S., & Brain, C. W. (1983). The Utility of Annual Reports: An International Study. *Journal of International Business Studies 1983 14:1*, *14*(1), 63–84. https://doi.org/10.1057/PALGRAVE.JIBS.8490507

Chapple, W., & Moon, J. (2005). Corporate social responsibility (CSR) in Asia a seven-country study of CSR Web site reporting. *Business and Society*, *44*(4), 415–441. https://doi.org/10.1177/0007650305281658

Charkham, J. P. (1995). *Keeping good company : a study of corporate governance in five countries*. 389.

Cheffins, B. R. (2012). The History of Corporate Governance. *SSRN Electronic Journal*, *January*. https://doi.org/10.2139/ssrn.1975404

Chen, T.; R. J. (2004). *The Evolution of Viruses and Worms*. 289–310. https://doi.org/10.1201/9781420030884-19

Cheung, Y. L., Jiang, P., & Tan, W. (2010). A transparency Disclosure Index measuring disclosures: Chinese listed companies. *Journal of Accounting and Public Policy*, *29*(3), 259–280. https://doi.org/10.1016/j.jaccpubpol.2010.02.001

Chithambo, L., & Tauringana, V. (2014). Company specific determinants of greenhouse gases disclosures. *Journal of Applied Accounting Research*, *15*(3), 323–338. https://doi.org/10.1108/JAAR-11-2013-0087

Choe, H., Kho, B. C., & Stulz, R. M. (2005). Do domestic investors have an edge? The trading experience of foreign investors in Korea. *Review of Financial Studies*, *18*(3), 795–829. https://doi.org/10.1093/rfs/hhi028

Choi, B.B., Lee, D. and Psaros, J. (2010). An analysis and explanation of Australian company carbon emission disclosures. *Paper presented at 2010 AFAANZ Conference, Christchurch, July 3-5.*

Choi, F. D. S. (1973). Financial Disclosure and Entry to the European Capital Market. *Journal of Accounting Research, 11*(2), 159. https://doi.org/10.2307/2490187

Chong, Alberto; López de Silanes, F. (2007). Investor Protection and Corporate Governance. En S. U. P. (2007) (Ed.), *Investor Protection and Corporate Governance*. The World Bank. https://doi.org/10.1596/978-0-8213-6913-5

Chong, A., & Lopez-de-Silanes, F. (2007). *Investor protection and corporate governance : firm-level evidence across Latin America*. 557.

Chow, C. W., & Wong-Boren, A. (1987). Voluntary Financial Disclosure by Mexican Corporations. *Accounting Review*, *62*(3), 533.

http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=4496048&S=R&D=bth&EbscoContent=dGJyMNLe80SeqLE4y9f3OLCmr0uep7ZSsKi4TLSWxWXS&ContentCustomer=dGJyMPGqtkqxra5Rue3sfefwuY3x2%2FAA%5Cnhttp://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=449604

Chu, C. I., Chatterjee, B., & Brown, A. (2013). The current status of greenhouse gas reporting by Chinese companies: A test of legitimacy theory. *Managerial Auditing Journal*, *28*(2), 114–139. https://doi.org/10.1108/02686901311284531

Clarkson, P. M., Fang, X., Li, Y., & Richardson, G. (2013). The relevance of environmental disclosures: Are such disclosures incrementally informative? *Journal of Accounting and Public Policy*, *32*(5), 410–431. https://doi.org/10.1016/J.JACCPUBPOL.2013.06.008

Clarkson, P. M., Li, Y., Richardson, G. D., & Vasvari, F. P. (2008). Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis. *Accounting, Organizations and Society*, *33*(4–5), 303–327. https://doi.org/10.1016/j.aos.2007.05.003

Clinton, L., & Higgins, J. (2020). *Cyber-Risk Oversight Cyber-Risk Oversight*.

Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405. https://doi.org/10.1111/J.1468-0335.1937.TB00002.X

Coles, J. L., Daniel, N. D., & Naveen, L. (2008). Boards: Does one size fit all? *Journal of Financial Economics*, *87*(2), 329–356. https://doi.org/10.1016/J.JFINECO.2006.08.008

Collier, P., & Institute of Chartered Accountants in England and Wales. Research Board. (1992). *Audit committees in large UK companies.* 203.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems and Decisions 2013 33:4*, *33*(4), 469–470. https://doi.org/10.1007/S10669-013-9484-Z

Comisión Europea. (2022). *Economía justa y sostenible : la Comisión establece normas para que las empresas respeten los derechos humanos y el medio ambiente en las cadenas de suministro mundiales*. https://ec.europa.eu/commission/presscorner/detail/es/ip_22_1145

Comisión Interamericana de Telecomunicaciones. (2004). *Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y*

*multidisciplinario para la creación de una cultura de seguridad cibernética*.

Comisión Nacional de Valores. (2019). *Codigo de Gobierno Societario - Resolucion General 797 2019*. https://www.erreius.com/Legislacion/documento/20190619075647772/resolucion-general-797-2019-comision-nacional-de-valores-codigo-de-gobierno-societario-memoria-informacion-modificacion-normas-nt-2013

Committee Basel. (2015). Standards: Revised Pillar 3 Disclosure Requirements. En *Bank for International Settlements* (Número January). http://www.bis.org/bcbs/publ/d309.pdf

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Consejo coordinador empresarial. (2018). *Código de principios y mejores prácticas de Gobierno Corporativo*.

Convenio de Budapest, | (2001).

Cooke, T. E., & Wallace, R. S. O. (1989). Global Surveys of Corporate Disclosure Practices and Audit Firms: A Review Essay. *Accounting and Business Research*, *20*(77), 47–57. https://doi.org/10.1080/00014788.1989.9729394

COSO. (2017). *COSO II ERM*.

CPMI-IOSCO. (2016). *Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures*. www.bis.org

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/TIMREVIEW/835

Creese, S. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Crowdstrike. (2021). *The evolution of ransomware: how to protect against new adversary trends and methods*. 1–9.

CSA. (2017). *CSA Multilateral Staff Notice 51-347-Disclosure of cyber security risks and*

*incidents*. http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

CSA ACVM. (2013). *CSA Staff Notice 11-326 - Cyber Security*.

CSA ACVM. (2017). *CSA Staff Notice 33-321: Cyber Security and Social Media*. https://lautorite.qc.ca/fileadmin/lautorite/reglementation/valeurs-mobilieres/0-avis-acvm-staff/2017/2017oct19-33-321-avis-acvm-en.pdf

CSA ACVM. (2019). *Disclosure of cyber security risks and incidents*. *2017*, 605–608.

CyBOK. (2019). The Cyber Security Body of Knowledge (CyBoK) 1.0. *CyBoK*, 299. https://www.cybok.org/

CyBOK. (2021). Introduction to CyBOK Knowledge Areas. *The Cyber Security Body of Knowledge*, 22. www.cybok.org

Da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *https://doi.org/10.1080/10580530701586136*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Dalton, D. R., Hitt, M. A., Certo, S. T., & Dalton, C. M. (2007). The Fundamental Agency Problem and Its Mitigation. *The Academy of Management Annals*, *1*(1), 1–64. https://doi.org/10.1080/078559806

Darus, F., Mohd Zuki, H. I., & Yusoff, H. (2019). The path to sustainability: Understanding organisations' environmental initiatives and climate change in an emerging economy. *European Journal of Management and Business Economics*, *29*(1), 84–96. https://doi.org/10.1108/EJMBE-06-2019-0099

Datt, R. R., Luo, L., & Tang, Q. (2019). Corporate voluntary carbon disclosure strategy and carbon performance in the USA. *Accounting Research Journal*, *32*(3), 417–435. https://doi.org/10.1108/ARJ-02-2017-0031

Day, J. (2018). *Privacy and Cybersecurity Developments in Latin America*. https://www.lexology.com/library/detail.aspx?g=c0701531-2665-4e4b-a87b-00434e25d55f

De Villiers, C., Hsiao, P.-C. K., & Maroun, W. (2020). Introduction to the Routledge Handbook of Integrated Reporting : An overview of integrated reporting and this book, which entails different perspectives on a maturing field and a framework for future research. *The Routledge Handbook of Integrated Reporting*, 1–14. https://doi.org/10.4324/9780429279621-1

Deegan, C. (2002). Introduction: The legitimising effect of social and environmental disclosures – a theoretical foundation. En *Accounting, Auditing & Accountability*

*Journal* (Vol. 15, Número 3, pp. 282–311). MCB UP Ltd. https://doi.org/10.1108/09513570210435852

Deloitte. (2012). *Guía Práctica Consejeros del Comité de Auditoría*.

Deloitte. (2015). *Cybersecurity: The changing role of audit committee and internal audit Contents*. 16. http://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

Deloitte. (2016). *Cyber security: The changing role of the Board and the Audit Committee*. *June*, 5. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

Deloitte. (2019a). *Índice Global de Ciberseguridad - 2018*. https://www2.deloitte.com/cl/es/pages/risk/revista-perspectivas-4ta-edicion/seccion-2/Indice-Global-de-Seguridad-2018.html

Deloitte. (2019b). Managing Cyber Risk in a Digital Age. *Coso*, 28. https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf

Deloitte. (2021a). *Business-aligned cyber strategy | Deloitte | Cyber Risk*. https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/business-aligned-cyber-strategy.html

Deloitte. (2021b). *Practicas nacionales versus practicas internacionales Gobierno Corporativo*.

Deloitte. (2021c). *Progress at a snail's pace*. file:///C:/Users/HP/Desktop/gx-women-in-the-boardroom-seventh-edition (1).pdf

Denis, D. K. (2001). Twenty-five years of corporate governance research … and counting. *Review of Financial Economics*, *10*(3), 191–212. https://doi.org/10.1016/S1058-3300(01)00037-4

DeZoort, F. T., Hermanson, D., Archambeault, D., & Reed, S. (2002). Audit Committee Effectiveness: A Synthesis of the Empirical Audit Committee Literature. *Audit Committee Effectiveness: A Synthesis of the Empirical Audit Committee Literature*, *21*. https://digitalcommons.kennesaw.edu/facpubs/1495

Dezsö, C. L., & Ross, D. G. (2012). Does female representation in top management improve firm performance? A panel data investigation. *Strategic Management*

*Journal*, *33*(9), 1072–1089. https://doi.org/10.1002/SMJ.1955

Dimaggio, P. (1982). Cultural Capital and School Success : The Impact of Status Culture Participation on the Grades. *American Sociological Review*, *47*(2), 189–201.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147. https://doi.org/10.2307/2095101

Division of Corporation Finance, & SEC. (2011). *CF Disclosure Guidance: Topic No. 2 - Cybersecurity*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Dobran, B. (2021). *17 Types of Cyber Security Attacks To Protect Against in 2021*. https://phoenixnap.com/blog/cyber-security-attack-types/

Domenech, J. J. G. (2017). La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE. *REVISTA LEX MERCATORIA Doctrina, Praxis, Jurisprudencia y Legislación*, 37–42. https://doi.org/10.21134/LEX.VI.534

Donnelly, R., & Mulcahy, M. (2008). Board Structure, Ownership, and Voluntary Disclosure in Ireland. *Corporate Governance: An International Review*, *16*(5), 416–429. https://doi.org/10.1111/j.1467-8683.2008.00692.x

Dungey, M., Flavin, T., O'Connor, T., & Wosser, M. (2022). Non-financial corporations and systemic risk. *Journal of Corporate Finance*, *72*, 102129. https://doi.org/10.1016/J.JCORPFIN.2021.102129

E&Y. (2018). *Cybersecurity disclosure benchmarking*.

E&Y. (2019). *What Companies are Disclosing About Cybersecurity Risk and Oversight*. 1–7.

E&Y. (2020). *What companies are disclosing about cybersecurity risk and oversight in 2020*. *August*.

Eijkelenboom, E. V. A., & Nieuwesteeg, B. F. H. (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. *Computer Law and Security Review*, *40*, 105513. https://doi.org/10.1016/j.clsr.2020.105513

Eisenberg, M. A. (1976). *The structure of the corporation : a legal analysis*. https://books.google.com/books/about/The_Structure_of_the_Corporation.html?hl=es&id=pxY-AQAAIAAJ

Eisenberg, T., Sundgren, S., & Wells, M. T. (1998). Larger board size and decreasing firm value in small firms. *Journal of Financial Economics*, *48*(1), 35–54.

https://doi.org/10.1016/s0304-405x(98)00003-8

Eisenhardt, K. M. (1985). Control: Organizational and Economic Approaches. *http://dx.doi.org/10.1287/mnsc.31.2.134*, *31*(2), 134–149. https://doi.org/10.1287/MNSC.31.2.134

Elamer, A. A., AlHares, A., Ntim, C. G., & Benyazid, I. (2018). The corporate governance–risk-taking nexus: evidence from insurance companies. *International Journal of Ethics and Systems*, *34*(4), 493–509. https://doi.org/10.1108/IJOES-07-2018-0103

Elamer, A. A., Ntim, C. G., Abdou, H. A., & Pyke, C. (2020). Sharia supervisory boards, governance structures and operational risk disclosures: Evidence from Islamic banks in MENA countries. *Global Finance Journal*, *46*, 100488. https://doi.org/10.1016/J.GFJ.2019.100488

Elgadi, E., & Ghardallou, W. (2022). Gender diversity, board of director's size and Islamic banks performance. *International Journal of Islamic and Middle Eastern Finance and Management*, *15*(3), 664–680. https://doi.org/10.1108/IMEFM-09-2019-0397/FULL/PDF

Eling, M., & Schnell, W. (2016a). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122/FULL/PDF

Eling, M., & Schnell, W. (2016b). What do we know about cyber risk and cyber risk insurance? En *Journal of Risk Finance* (Vol. 17, Número 5, pp. 474–491). Emerald Group Publishing Ltd. https://doi.org/10.1108/JRF-09-2016-0122

Ellimäki, P., Gómez-Bolaños, E., Hurtado-Torres, N., & Aragón-Correa, J. A. (2021). Do global firms increase their environmental disclosure and performance? Symbolic versus effective operations and the moderating role of liability of origin. Legitimation implications. *Industrial Marketing Management*, *92*, 354–363. https://doi.org/10.1016/J.INDMARMAN.2019.10.015

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*(6), 597–603. https://doi.org/10.1016/0167-4048(93)90056-B

Elsayed, M., Elshandidy, T., & Ahmed, Y. (2022). Corporate failure in the UK: An examination of corporate governance reforms. *International Review of Financial Analysis*, *82*, 102165. https://doi.org/10.1016/J.IRFA.2022.102165

Elshandidy, T., & Neri, L. (2015). Corporate Governance, Risk Disclosure Practices, and Market Liquidity: Comparative Evidence from the UK and Italy. *Corporate Governance: An International Review*, *23*(4), 331–356. https://doi.org/10.1111/corg.12095

Elshandidy, T., Shrives, P. J., Bamber, M., & Abraham, S. (2018). Risk reporting: A review of the literature and implications for future research. *Journal of Accounting Literature*, *40*, 54–82. https://doi.org/10.1016/j.acclit.2017.12.001

Elzahar, H., & Hussainey, K. (2012). Determinants of narrative risk disclosures in UK interim reports. *Journal of Risk Finance*, *13*(2), 133–147. https://doi.org/10.1108/15265941211203189/FULL/PDF

ENISA. (2015). Definition of Cybersecurity | Gaps and overlaps in standardisation. En *European Union Agency For Network And Information Security: Vol. v1.0* (Número December).

Enrique, & Bonsón, E. T. (2004). *La difusión voluntaria de información financiera en Internet. Un análisis comparativo entre Estados Unidos, Europa del Este y la Unión Europea*.

Ernst & Young. (2019). *What Boards Are Doing Today to Better Oversee Cyber Risk*. *July*, 1–6.

Ernst & Young. (2021). *EY Global Information Security Survey 2021: Cybersecurity: how do you rise above the waves of a perfect storm?*

Ernstberger, J., & Grüning, M. (2013). How do firm- and country-level governance mechanisms affect firms' disclosure? *Journal of Accounting and Public Policy*, *32*(3), 50–67. https://doi.org/10.1016/J.JACCPUBPOL.2013.02.003

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

EU. (2014). *Directive 2014/95 / EU of the European Parliament and of the Council - of October 22, 2014*.

EU. (2016). *EU general data protection regulation* (Vol. 2014, Número April).

EU. (2019). *Regulation (EU) 2019/881*. Regulation (EU) 2019/881 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

Europea, U. (2015). *Digital Security Risk Management for Economic and Social*

*Prosperity OECD Recommendation and Companion Document*. https://doi.org/10.1787/9789264245471-en

Excelencia, E. E. de. (2022). *Evaluación del riesgo cuantitativa vs cualitativa: ¿cuál escoger?* https://www.escuelaeuropeaexcelencia.com/2020/11/evaluacion-del-riesgo-cuantitativa-vs-cualitativa-cual-escoger/

EY. (2018). *SEC guidance on cybersecurity: board considerations* (Número March). https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cybersecurity/ey-sec-guidance-on-cybersecurity-board-considerations.pdf

EY. (2020). *EY Global Information Security Survey 2020. How does security evolve from bolted on to built-in?* https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf

EY. (2021). *Board Agenda 2021*. *1*(1), 21.

Fakhfakh, I., & Jarboui, A. (2022). Board of director's effectiveness, audit quality and ownership structure: impact on audit risk-Tunisian evidence. *Journal of Accounting in Emerging Economies*, *12*(3), 468–485. https://doi.org/10.1108/JAEE-07-2020-0158/FULL/PDF

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., Wang, S. S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., & Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science*, *366*(6469), 1066–1069. https://doi.org/10.1126/science.aaz4795

Fama, E. F., Fisher, L., Jensen, M. C., & Roll, R. (1969). The Adjustment of Stock Prices to New Information. *International Economic Review*, *10*(1), 1. https://doi.org/10.2307/2525569

Fama, E. F., & Jensen, M. C. (1983). Separation of Ownership and Control. *Journal of Law & Economics*, *26*. https://heinonline.org/HOL/Page?handle=hein.journals/jlecono26&id=313&div=&collection=

Farrell, K. A., & Hersch, P. L. (2005). Additions to corporate boards: the effect of gender. *Journal of Corporate Finance*, *11*(1–2), 85–106. https://doi.org/10.1016/J.JCORPFIN.2003.12.001

FASB. (1994). Statement of Financial Accounting Standards No. 119, Disclosure about

Derivative Financial Instruments and Fair Value of Financial Instruments. *Financial Accounting Standards Board: Norwalk, Connecticut*, *119*.

FASB. (1998). Statement of Financial Accounting Standards No. 133, Accounting for Derivative Instruments and Hedging Activities. *Financial Accounting Standards Board: Norwalk, Connecticut.*, *133*.

Fidler, D. P. (2020). Cybersecurity in the Time of COVID-19. *Council on Foreign Relations*, *2020*, 7–9. https://www.cfr.org/blog/cybersecurity-time-covid-19

Fifka, M. S., & Pobizhan, M. (2014). An institutional approach to corporate social responsibility in Russia. *Journal of Cleaner Production*, *82*, 192–201. https://doi.org/10.1016/j.jclepro.2014.06.091

Financial Standards Foundation. (2011). Achieving Effective Boards. *Global Corporate Governance Forum*, *June*.

Fontaine, David; Reed, J. (2018). *Cybersecurity: The SEC's Wake-up Call to Corporate Directors*. Harvard Law School. https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/

Fortinet. (2022). *Fortinet registró 137 mil millones de intentos de ciberataques en América Latina en la primera mitad del año.* https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e

Francoeur, C., Labelle, R., & Sinclair-Desgagné, B. (2008). Gender Diversity in Corporate Governance and Top Management. *Journal of Business Ethics 2007 81:1*, *81*(1), 83–95. https://doi.org/10.1007/S10551-007-9482-5

Fraser, J. S. B. J. (2010). *Enterprise risk management*.

Freedman, M., & Jaggi, B. (2005). Global warming, commitment to the Kyoto protocol, and accounting disclosures by the largest global public firms from polluting industries. *The International Journal of Accounting*, *40*(3), 215–232. https://doi.org/10.1016/J.INTACC.2005.06.004

Freeman, E. (1984). *Edward Freeman*.

Freeman, R. E., & Mcvea, J. (2001). *A Stakeholder Approach to Strategic Management*.

Freeman, R. E., & Reed, D. L. (1983). Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review*, *25*(3), 88–106. https://doi.org/10.2307/41165018

Frias-Aceituno, J. V., Rodríguez-Ariza, L., & Garcia-Sánchez, I. M. (2014). Explanatory Factors of Integrated Sustainability and Financial Reporting. *Business Strategy and the Environment*, *23*(1), 56–72. https://doi.org/10.1002/bse.1765

Friedman, M. A. (1970). *The social responsibility of business is to increase its profits*. https://www.nytimes.com/1970/09/13/archives/a-friedman-doctrine-the-social-responsibility-of-business-is-to.html

G20/OECD. (2016). Principles of Corporate Governance. En *G20/OECD Principles of Corporate Governance*. https://doi.org/10.1787/9789264257443-tr

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*. https://doi.org/10.1016/j.accinf.2020.100468

García-Sánchez, I. M., Gómez-Miranda, M. E., David, F., & Rodríguez-Ariza, L. (2019). Board independence and GRI-IFC performance standards: The mediating effect of the CSR committee. *Journal of Cleaner Production*, *225*, 554–562. https://doi.org/10.1016/J.JCLEPRO.2019.03.337

Garcia-Sanchez, I. M. of the I. M. C. on the V. D. of C. I., Cuadrado-Ballesteros, B., & Frias-Aceituno, J. V. (2016). Impact of the Institutional Macro Context on the Voluntary Disclosure of CSR Information. *Long Range Planning*, *49*(1), 15–35. https://doi.org/10.1016/J.LRP.2015.02.004

Gelfond, S., Wechsler, J., Cohen, H., & Llp, J. (2017). *Top 10 Practice tips by experts: risk factors*.

Gendron, Y., & Bédard, J. (2006). On the constitution of audit committee effectiveness. *Accounting, Organizations and Society*, *31*(3), 211–239. https://doi.org/10.1016/J.AOS.2005.03.002

German Government Commission. (2022). *Deutscher Corporate Governance Kodex*. https://doi.org/10.1515/zinso-2018-0608

Giner, B. (1997). The influence of company characteristics and accounting regulation on information disclosed by Spanish firms. *https://doi.org/10.1080/096381897336863*, *6*(1), 45–68. https://doi.org/10.1080/096381897336863

Gómez Vieites, A. (2006). *Enciclopedia de la seguridad informática*.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. En *Computer Security Journal* (Vol. 19, Número 2, pp. 1–7). Computer Security Institute.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 567–594. https://doi.org/10.2307/25750692

Gray, R., Kouhy, R., & Lavers, S. (1995). Corporate social and environmental reporting A review of the literature and a longitudinal study of UK disclosure. *Accounting, Auditing & Accountability Journal*, *8*(2), 47–77. https://doi.org/10.1108/09513579510146996

GRI. (2016). GRI 418: Customer privacy 2016 418. *GRI Standards*. www.globalreporting.org

Grossman, B. S. J., & Stiglitz, J. E. (1980). *On the Impossibility of Informationally Efficient Markets Author ( s ): Sanford J . Grossman and Joseph E . Stiglitz Source : The American Economic Review , Jun ., 1980 , Vol . 70 , No . 3 ( Jun ., 1980 ), pp . 393- Published by : American Economic Associ*. *70*(3), 393–408.

GSSB. (2016). GRI 418: Privacidad Del Cliente 2016. *GRI Standards*.

Gul, F. A., Srinidhi, B., & Ng, A. C. (2011). Does board gender diversity improve the informativeness of stock prices? *Journal of Accounting and Economics*, *51*(3), 314–

338. https://doi.org/10.1016/J.JACCECO.2011.01.005

Gunter, O. (2004). The Phishing Guide. *History*.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. En *Managerial Auditing Journal* (Vol. 34, Número 7, pp. 808–834). Emerald Group Publishing Ltd. https://doi.org/10.1108/MAJ-09-2018-2004

Hacienda, M. D. E., & Hacienda, S. D. E. (2022). *Ley 20382*. 1–34.

Haniffa, R. M., & Cooke, T. E. (2002). Culture, Corporate Governance and Disclosure in Malaysian Corporations. *Abacus*, *38*(3), 317–349. https://doi.org/10.1111/1467-6281.00112

Haniffa, R. M., & Cooke, T. E. (2005). The impact of culture and governance on corporate social reporting. *Journal of Accounting and Public Policy*, *24*(5), 391–430. https://doi.org/10.1016/j.jaccpubpol.2005.06.001

Haque, S., & Deegan, C. (2010). Corporate Climate Change-Related Governance Practices and Related Disclosures: Evidence from Australia. *Australian Accounting Review*, *20*(4), 317–333. https://doi.org/10.1111/J.1835-2561.2010.00107.X

Hardiyansah, M., & Agustini, A. T. (2020). Analysis of carbon emissions disclosure and firm value: Type of industry as a moderating model. *International Journal of Scientific and Technology Research*, *9*(2), 1125–1132.

Harrigan, K. R. (2017). Numbers and Positions Of Women Elected to Corporate Boards. *https://doi.org/10.5465/255580*, *24*(3), 619–625. https://doi.org/10.5465/255580

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security*, *73*, 102–113. https://doi.org/10.1016/J.COSE.2017.10.008

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, *3*, 1117–1124. https://doi.org/10.1016/J.PROMFG.2015.07.186

Hermalin, B. E., & Weisbach, M. S. (2003). *Boards of Directors as an Endogenously Determined Institution: A Survey of the Economic Literature*. https://doi.org/10.3386/W8161

Héroux, S., & Fortin, A. (2020a). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S., & Fortin, A. (2020b). Cybersecurity Disclosure by the Companies on the S&P/TSX 60 Index. *Accounting Perspectives*, *19*(2), 73–100.

https://doi.org/10.1111/1911-3838.12220

Hijink, J. B. S. (2010). *Publicatieverplichtingen voor beursvennootschappen*.

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure: Who Cares? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2852519

Hillman, A. J., Cannella, A. A., & Paetzold, R. L. (2000). The Resource Dependence Role of Corporate Directors: Strategic Adaptation of Board Composition in Response to Environmental Change. *Journal of Management Studies*, *37*(2), 235–256. https://doi.org/10.1111/1467-6486.00179

Holland & Knight. (2021). *SEC Issues First-Ever Penalties for Deficient Cybersecurity Risk Controls*. https://www.hklaw.com/en/insights/publications/2021/06/sec-issues-first-ever-penalties-for-deficient-cybersecurity-risk

Holland, L., & Foo, Y. B. (2003). Differences in environmental reporting practices in the UK and the US: The legal and regulatory context. *British Accounting Review*, *35*(1), 1–18. https://doi.org/10.1016/S0890-8389(02)00127-0

Hope, O.-K. (2003). *Disclosure Practices, Enforcement of Accounting Standards, and Analysts' Forecast Accuracy: An International Study - Hope - 2003 - Journal of Accounting Research - Wiley Online Library*. https://onlinelibrary.wiley.com/doi/10.1111/1475-679X.00102

Hope, O. K., Hu, D., & Lu, H. (2016). The benefits of specific risk-factor disclosures. *Review of Accounting Studies*, *21*(4), 1005–1045. https://doi.org/10.1007/s11142-016-9371-1

Hunt, B. (2003). *The Timid Corporation: Why Business is Terrified of Taking Risk*.

IBGC. (2015). Código das Melhores Práticas de Governança Corporativa. En *Instituto Brasileiro de Governança Corporativa*. http://www.ibgc.org.br/userfiles/2014/files/CMPGPT.pdf

ICAWE. (2011). *Reporting Business Risks: Meeting Expectations*.

IDB; OAS. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

International Integrated Reporting Council. (2021). < IR > Framework about the IIRC. *Jo*, *January*, 58. https://integratedreporting.org/wp-

content/uploads/2021/01/InternationalIntegratedReportingFramework.pdf

International Telecommunication Union. (2008). Overview Cybersecurity. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I

Internet Security Alliance and American National Standards. (2010). The Financial Management of Cyber Risk: An Implementation Framework for CFOs. *Order A Journal On The Theory Of Ordered Sets And Its Applications*.

Investor Stewardship Group. (2017). Corporate Governance Principles For US Listed Companies. *Isg*, 1–5. https://isgframework.org/corporate-governance-principles/

IOSCO. (2016). *Cyber Security in Securities Markets – An International Perspective Report on IOSCO ' s cyber risk coordination efforts*.

IRRC. (2016). *The Corporate Risk Factor Disclosure Landscape*. *January*, 27. https://www.weinberg.udel.edu/irrci/research/887

ISO. (2011). ISO 26000. *The Corporate Responsibility code book*, 83–129. https://doi.org/10.4324/9781351278881-5

ISO. (2012). *ISO/IEC 27032: Information technology — Security techniques — Guidelines for cybersecurity*. ISO 27032. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

ISO. (2013). *ISO 27002*.

ISO. (2018). *ISO 31000 Risk management*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO. (2020). *ISO/IEC 27014:2020 - Information security, cybersecurity and privacy protection — Governance of information security*. https://www.iso.org/standard/74046.html

*ISO 37000*. (2021).

ITU. (2007). *ITU Global Cybersecurity Agenda - A Framework for International Cooperation in Cybersecurity*. https://www.itu.int/osg/spuold/cybersecurity/gca/

ITU. (2017). Global Cybersecurity Index (GCI) 2017. En *ITU-D Global*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU. (2018). *Global Cybersecurity Index (GCI) 2018 ITUPublications Studies & research*.

ITU. (2020). *ITU Publications*. Índice Global de Ciberseguridad 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

ITU. (2021a). *About the International Telecommunication Union (ITU)*. https://www.itu.int/es/about/Pages/default.aspx

ITU. (2021b). Global Cybersecurity Index (GCI). En *ITU Publications*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU & ABI Research. (2014). *Global Cybersecurity I N D E X*. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf

Jaggi, B., & Low, P. Y. (2000). Impact of Culture, Market Forces, and Legal System on Financial Disclosures. *The International Journal of Accounting*, *35*(4), 495–519. https://doi.org/10.1016/S0020-7063(00)00076-5

Jamali, D., Safieddine, A. M., & Rabbath, M. (2008). Corporate Governance and Corporate Social Responsibility Synergies and Interrelationships. *Corporate Governance: An International Review*, *16*(5), 443–459. https://doi.org/10.1111/J.1467-8683.2008.00702.X

Jamaludin, N. D., Sanusi, Z. M., & Kamaluddin, A. (2015). Board Structure and Earnings Management in Malaysian Government Linked Companies. *Procedia Economics and Finance*, *28*, 235–242. https://doi.org/10.1016/S2212-5671(15)01105-3

James P. Anderson, Sheila Brand, Li Gong, T. H. (2004). Firewalls: an Expert Roundtable. En *Book Security, Statistical Methods in Computer* (Edition, E, pp. 333–350). CRC Press. https://doi.org/10.1201/9781420030884-21

Jensen, M. C. (1993). The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems. *The Journal of Finance*, *48*(3), 831–880. https://doi.org/10.1111/j.1540-6261.1993.tb04022.x

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: managerial behavior, agency costs and ownership structure. *Journal Of Financial Economics*, *3*, 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Jizi, M. I., Salama, A., Dixon, R., & Stratling, R. (2014). Corporate Governance and Corporate Social Responsibility Disclosure: Evidence from the US Banking Sector. *Journal of Business Ethics*, *125*(4), 601–615. https://doi.org/10.1007/s10551-013-1929-2

Jorion, P. (2002). *The Accounting Review* (Vol. 77).

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019

Kang, H., Cheng, M., & Gray, S. J. (2007). Corporate Governance and Board Composition: diversity and independence of Australian boards. *Corporate Governance: An International Review*, *15*(2), 194–207. https://doi.org/10.1111/J.1467-8683.2007.00554.X

Kanter, R. M. (1977). *Men and women of the corporation*. 348. https://books.google.com/books/about/Men_And_Women_Of_The_Corporation.html?hl=es&id=7L63AAAAIAAJ

Kaplan, J. M., Bailey, T., O'Halloran, D., Marcus, A., & Rezek, C. (2015). *Beyond Cybersecurity: Protecting Your Digital Business*. *Exhibit 1*, 1–9. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1119026849,descCd-buy.html

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Kasznik, R., & Lev, B. (1995). To warn or not to warn: Management disclosures in the face of an earnings surprise. *Accounting review: A quarterly journal of the American Accounting Association*, *70*(1), 113–134.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2010). The Worldwide Governance Indicators: A Summary of Methodology, Data and Analytical Issues. *The World Bank*, *5430*(September), 1–29.

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020a). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/j.jbusres.2019.11.025

Kent Baker, H., Pandey, N., Kumar, S., & Haldar, A. (2020b). A bibliometric analysis of board diversity: Current status, development, and future research directions. *Journal of Business Research*, *108*, 232–246. https://doi.org/10.1016/J.JBUSRES.2019.11.025

Khatib, S. F. A., Abdullah, D. F., Elamer, A. A., & Abueid, R. (2021). Nudging toward diversity in the boardroom: A systematic literature review of board diversity of financial institutions. *Business Strategy and the Environment*, *30*(2), 985–1002. https://doi.org/10.1002/BSE.2665

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys and Tutorials*, *15*(4), 2091–2121.

https://doi.org/10.1109/SURV.2013.032213.00009

Kiesow Cortez, E., & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation*, *January*, 1–23. https://doi.org/10.1017/err.2022.10

Kiliç, M., Kuzey, C., & Uyar, A. (2015). The impact of ownership and board structure on corporate social responsibility (CSR) reporting in the Turkish banking industry. *Corporate Governance (Bingley)*, *15*(3), 357–374. https://doi.org/10.1108/CG-02-2014-0022

King, M. (2016). Report on corporate governance for South Africa 2016. *King IV Report on Corporate Governance for South Africa*, 1–128.

KOF. (2020). *Globalization Report 2020*.

Konishi, N., & Ali, M. M. (2007). Risk reporting of Japanese companies and its association with corporate characteristics. *undefined*, *4*(3), 263–285. https://doi.org/10.1504/IJAAPE.2007.016281

Kor, Y. Y. (2006). Direct and interaction effects of top management team and board compositions on R&D investment strategy. *Strategic Management Journal*, *27*(11), 1081–1099. https://doi.org/10.1002/SMJ.554

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management*, *41*(5), 597–607. https://doi.org/10.1016/J.IM.2003.08.001

Kravet, T., & Muslu, V. (2013). Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies*, *18*(4), 1088–1122. https://doi.org/10.1007/s11142-013-9228-9

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/J.JISA.2014.09.005

Kühn, A. L., Stiglbauer, M., & Fifka, M. S. (2018). Contents and Determinants of Corporate Social Responsibility Website Reporting in Sub-Saharan Africa: A Seven-Country Study. En *Business and Society* (Vol. 57, Número 3). https://doi.org/10.1177/0007650315614234

La Porta, R., Lopez-de-Silanes, F., & Shleifer, A. (1999). Corporate Ownership Around the World. *The Journal of Finance*, *54*(2), 471–517. https://doi.org/10.1111/0022-1082.00115

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., & Vishny, R. (2000). Investor protection and corporate governance. *Journal of Financial Economics*, *58*(1–2), 3–27. https://doi.org/10.1016/s0304-405x(00)00065-9

La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. W. (1998). Law and finance. *Journal of Political Economy*, *106*(6), 1113–1155. https://doi.org/10.1086/250042

La Porta, R., Lopez-De-Silanes, F., Shleifer, A., & Vishny, R. W. (1997). Legal Determinants of External Finance. *The Journal of Finance*, *52*(3), 1131–1150. https://doi.org/10.1111/J.1540-6261.1997.TB02727.X

Lajili, K., & Zéghal, D. (2005). A content analysis of risk management disclosures in canadian annual reports. *Canadian Journal of Administrative Sciences*, *22*(2), 125–142. https://doi.org/10.1111/j.1936-4490.2005.tb00714.x

Larmou, S., & Vafeas, N. (2009). *The relation between board size and firm performance in firms with a history of poor operating performance*. https://doi.org/10.1007/s10997-009-9091-z

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*. https://doi.org/10.1109/PCCC.2016.7820663

Lee, R. P., Chen, Q., & Hartmann, N. N. (2016). Enhancing Stock Market Return with New Product Preannouncements: The Role of Information Quality and Innovativeness. *Journal of Product Innovation Management*, *33*(4), 455–471. https://doi.org/10.1111/JPIM.12284

Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, *8*(4), 1–15. https://doi.org/10.3390/risks8040128

Lernia, C. Di, Hardy, C., & Dori, A. (2020). *Cyber-related Risk Disclosure in Australia: Evidence from the ASX200 Journal Title: Company and Securities*. *5*, 23–29.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/J.ACCINF.2018.06.003

Li, W., & Zhang, R. (2010). Corporate Social Responsibility, Ownership Structure, and Political Interference: Evidence from China. *Journal of Business Ethics*, *96*(4), 631–645. https://doi.org/10.1007/s10551-010-0488-z

Liesen, A., Hoepner, A. G., Patten, D. M., & Figge, F. (2015). Does stakeholder pressure

influence corporate GHG emissions reporting? Empirical evidence from Europe. *Accounting, Auditing and Accountability Journal*, *28*(7), 1047–1074. https://doi.org/10.1108/AAAJ-12-2013-1547

Lim, S., Matolcsy, Z., & Chow, D. (2007). The Association between Board Composition and Different Types of Voluntary Disclosure. *European Accounting Review*, *16*(3), 555–583. https://doi.org/10.1080/09638180701507155

Linck, J. S., Netter, J. M., & Yang, T. (2008). The determinants of board structure. *Journal of Financial Economics*, *87*(2), 308–328. https://doi.org/10.1016/J.JFINECO.2007.03.004

Linsley, P. M., & Shrives, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK companies. *The British Accounting Review*, *38*(4), 387–404. https://doi.org/10.1016/J.BAR.2006.05.002

Lippmann, W. (1914). *Drift and mastery : an attempt to diagnose the current unrest*. Prentice-Hall.

Lipton, M., & Lorsch, J. W. (1992). A modest proposal for improved corporate governance: Business source. *Business Lawyer*, *42*(1), 59–78. http://web.a.ebscohost.com.eserv.uum.edu.my/bsi/detail?vid=19&sid=e3a1315c-d940-4744-b224-1ce498b43ead@sessionmgr4005&hid=4114&bdata=JnNpdGU9YnNpLWxpdmU=#db=bth&AN=5963897

Lopes, P. T., & Rodrigues, L. L. (2007). Accounting for financial instruments: An analysis of the determinants of disclosure in the Portuguese stock exchange. *The International Journal of Accounting*, *42*(1), 25–56. https://doi.org/10.1016/J.INTACC.2006.12.002

Loughran, T., & Mcdonald, B. (2011). When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. *Journal of Finance*, *66*(1), 35–65. https://doi.org/10.1111/j.1540-6261.2010.01625.x

Luo, L., Tang, Q., & Lan, Y. C. (2013). Comparison of propensity for carbon disclosure between developing and developed countries: A resource constraint perspective. *Accounting Research Journal*, *26*(1), 6–34. https://doi.org/10.1108/ARJ-04-2012-0024

Luo, Y. (2005). Corporate governance and accountability in multinational enterprises: Concepts and agenda. En *Journal of International Management* (Vol. 11, Número 1

SPEC. ISS., pp. 1–18). Elsevier Inc. https://doi.org/10.1016/j.intman.2004.11.001

Madnick, S. E. (1978). Management policies and procedures needed for effective computer security. *Sloan management review*, *20*(1), 61–74.

Mahmood, M., & Orazalin, N. (2017). Green governance and sustainability reporting in Kazakhstan's oil, gas, and mining sector: Evidence from a former USSR emerging economy. *Journal of Cleaner Production*, *164*, 389–397. https://doi.org/10.1016/J.JCLEPRO.2017.06.203

Mallin, C. (2006). *Handbook on International Corporate Governance*.

Marotta, A., & McShane, M. (2018). Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review*, *21*(3), 435–452. https://doi.org/10.1111/RMIR.12109

Marshall, A., & Weetman, P. (2007). Modelling Transparency in Disclosure: The Case of Foreign Exchange Risk Management. *Journal of Business Finance & Accounting*, *34*(5–6), 705–739. https://doi.org/10.1111/j.1468-5957.2007.02007.x

Marston, C. L., & Shrives, P. J. (1991). The use of disclosure indices in accounting research: A review article. En *The British Accounting Review* (Vol. 23, Número 3, pp. 195–210). Academic Press. https://doi.org/10.1016/0890-8389(91)90080-L

Masud, M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter? *Journal of Accounting in Emerging Economies*. https://doi.org/10.1108/JAEE-07-2021-0237

Mayor Gómez, R. (2016). *Contenido y novedades del reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)*. Gabilex. Revista del gabinete jurídico de Castilla la Mancha.

McCarthy, D. R. (2018). Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order. *Politics and Governance*, *6*(2), 5–12. https://doi.org/10.17645/pag.v6i2.1335

McShane, M., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/RMIR.12169

McShane, M., & Nguyen, T. (2020). Time-varying effects of cyberattacks on firm value. *Geneva Papers on Risk and Insurance: Issues and Practice*, *45*(4), 580–615. https://doi.org/10.1057/s41288-020-00170-x

Meftah Gerged, A., Beddewela, E. S., Christopher, |, & Cowton, J. (2021). *Does the*

*quality of country-level governance have an impact on corporate environmental disclosure? Evidence from Gulf Cooperation Council countries*. https://doi.org/10.1002/ijfe.2469

Meisner, M. (2018). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63. https://doi.org/10.12775/cjfa.2017.017

Melis, A. (2006). Corporate Governance in Italy. En *Handbook on international Corporate Governance*.

Menges, F., & Pernul, G. (2018). A comparative analysis of incident reporting formats. *Computers & Security*, *73*, 87–101. https://doi.org/10.1016/J.COSE.2017.10.009

Merriam -Webster. (2021). *Cybersecurity | Definition of Cybersecurity*. Merriam-Webster.com Dictionary, Merriam-Webster. https://www.merriam-webster.com/dictionary/cybersecurity

Meyer, J. W., & Rowan, B. (1977). Slett denne Institutionalized Organizations : Formal Structure as Myth and Ceremony. *American Journal of Sociology*, *83*(2), 340–363.

Middleton, B. (2017). *A History of Cyber Security Attacks 1980 to present* (T. & Francis (Ed.)).

Mintzberg, H. (1984). Who Should Control the Corporation?: *http://dx.doi.org/10.2307/41165115*, *27*(1), 90–115. https://doi.org/10.2307/41165115

Mirkovic, J., Reiher, P., & Hall, B. (2004). *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms* *.

Mitra, S., & Ransbotham, S. (2015). Information Disclosure and the Diffusion of Information Security Attacks. *https://doi.org/10.1287/isre.2015.0587*, *26*(3), 565–584. https://doi.org/10.1287/ISRE.2015.0587

Mokhtar, E. S., & Mellett, H. (2013). Competition, corporate governance, ownership structure and risk reporting. *Managerial Auditing Journal*, *28*(9), 838–865. https://doi.org/10.1108/MAJ-11-2012-0776/FULL/PDF

Moosa, I. A. (2007). Operational Risk: A Survey. *Financial Markets, Institutions & Instruments*, *16*(4), 167–200. https://doi.org/10.1111/J.1468-0416.2007.00123.X

Morse, E. A., Raval, V., & Wingender, J. R. (2018). SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. En *Business Lawyer* (Vol. 73, Número 1, pp. 1–34). American Bar Association.

https://doi.org/10.2139/ssrn.2711439

Moumen, N., Ben Othman, H., & Hussainey, K. (2016). Board structure and the informativeness of risk disclosure: Evidence from MENA emerging markets. *Advances in Accounting*, *35*, 82–97. https://doi.org/10.1016/J.ADIAC.2016.09.001

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*(1), 11–26. https://doi.org/10.1016/J.DSS.2013.04.004

Muñoz-Izquierdo, N., Segovia-Vargas, M. J., Camacho-Miñano, M. del M., & Pascual-Ezama, D. (2019). Explaining the causes of business failure using audit report disclosures. *Journal of Business Research*, *98*, 403–414. https://doi.org/10.1016/J.JBUSRES.2018.07.024

NACD. (2009). *Report of the NACD blue ribbon commission. Risk governance: balancing risk and reward*. https://www.wlrk.com/docs/1605831_1.pdf

Nader, R., Green, M. J., & Seligman, J. (1976). *Taming the giant corporation*. 312.

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *https://doi.org/10.1080/23738871.2016.1157619*, *1*(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

NCSC. (2022). *Essential Topics - NCSC.GOV.UK*. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious Software Threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 793–813. https://doi.org/10.1007/978-3-319-78440-3_35

NICCS. (2017). *Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies*. Explore terms: a glossary of common cybersecurity terminology. https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C ( 2017 )

Nielsen, S., & Huse, M. (2010). The Contribution of Women on Boards of Directors: Going beyond the Surface. *Corporate Governance: An International Review*, *18*(2), 136–148. https://doi.org/10.1111/J.1467-8683.2010.00784.X

NIST. (2020). NIST Privacy Framework. En *January 16, 2020*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

NITS. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

Ntim, C. G., Lindop, S., & Thomas, D. A. (2013). Corporate governance and risk

reporting in South Africa: A study of corporate risk disclosures in the pre- and post-2007/2008 global financial crisis periods. *International Review of Financial Analysis*, *30*, 363–383. https://doi.org/10.1016/j.irfa.2013.07.001

Nwosu, A. U., Goyal, S. B., & Bedi, P. (2020). Blockchain Transforming Cyber-Attacks: Healthcare Industry. *Advances in Intelligent Systems and Computing*, *1372 AISC*, 258–266. https://doi.org/10.1007/978-3-030-73603-3_24

O'Reilly, C. A., Caldwell, D. F., & Barnett, W. P. (1989). Work Group Demography, Social Integration, and Turnover. *Administrative Science Quarterly*, *34*(1), 21. https://doi.org/10.2307/2392984

OAS; ISA. (2020). *Manual de supervisión de riesgos cibernéticos para Juntas corporativas*. https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

OAS. (2019). Challenges of cyber risk in the financial sector for Colombia and Latin America. *Asobancaria*, 170. https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Ocasio, W., & Joseph, J. (2005). Cultural adaptation and institutional change: The evolution of vocabularies of corporate governance, 1972–2003. *Poetics*, *33*(3–4), 163–178. https://doi.org/10.1016/J.POETIC.2005.10.001

OCDE. (2004). Directrices de la OCDE para la seguridad de sistemas y redes de información. En *Directrices de la OCDE para la seguridad de sistemas y redes de información*. https://doi.org/10.1787/9789264065819-es

OCDE. (2016). *Principios de Gobierno Corporativo de la OCDE y del G20*. https://doi.org/10.1787/9789264259171-es

OCIE. (2020). *OCIE Cybersecurity and Resiliency Obervations 2020*. www.sec.gov/spotlight/cybersecurity.

OECD. (1999). *OECD Principles of Corporate Governance Principles of*.

OECD. (2011). *OECD Guidelines for Multinational Enterprises 2011 Edition*. https://doi.org/10.1787/9789264115415-en

OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity. En *Digital Security Risk Management for Economic and Social Prosperity*. https://doi.org/10.1787/9789264245471-en

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and

Observability of Self-Protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/J.1539-6924.2010.01478.X

Oliveira, J., Rodrigues, L. L., & Craig, R. (2011). Risk-related disclosures by non-finance companies: Portuguese practices and disclosure characteristics. *Managerial Auditing Journal*, *26*(9), 817–839. https://doi.org/10.1108/02686901111171466

Oliveira, J., Serrasqueiro, R., & Mota, S. N. (2018). Determinants of risk reporting by Portuguese and Spanish non-finance companies. *European Business Review*, *30*(3), 311–339. https://doi.org/10.1108/EBR-04-2017-0076/FULL/PDF

Oliver, C. (1991). *Strategic Responses to Institutional Processes*. *16*(1), 145–179.

ONU. (2011). *Developing countries most vulnerable to cyberattacks – UN*. https://news.un.org/en/story/2011/12/397922

Orman, H. (2003). The Morris worm: a fifteen-year perspective. *IEEE Security & Privacy*, *1*(5), 35–43. https://doi.org/10.1109 / MSECP.2003.1236233

Ortiz, E., & Clavel, J. G. (2006). Disclosures indexes: a propose to improve the metodology applied to the case of Human Resources disclosure included in Form 20-F. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, *35*(128), 87–113. https://doi.org/10.1080/02102412.2006.10779574

Packard, N. (2020). Three kinds of demand pull for the ARPANET into the Internet. *http://www.editorialmanager.com/cogentsocsci*, *6*(1). https://doi.org/10.1080/23311886.2020.1720565

Parker, D. B. (2007). The dark side of computing: SRI International and the study of computer crime. *IEEE Annals of the History of Computing*, *29*(1), 3–15. https://doi.org/10.1109/MAHC.2007.15

Patelli, L., & Prencipe, A. (2007). The relationship between voluntary disclosure and independent directors in the presence of a dominant shareholder. *European Accounting Review*, *16*(1), 5–33. https://doi.org/10.1080/09638180701265820

PCAOB. (2014). *Standing Advisory Group meeting cybersecurity*.

Perez-Batres, L. A., Miller, V. V, & Pisani, M. J. (2010). CSR, Sustainability and the Meaning of Global Reporting for Latin American Corporations. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-010-0614-y

Pfeffer, Jeffrey; Salancik, G. (1978). *The External Control of Organizations: A Resource Dependence Perspective by :: SSRN*.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496213

Pitrakkos, P., & Maroun, W. (2019). Evaluating the quality of carbon disclosures. *Sustainability Accounting, Management and Policy Journal*, *11*(3), 553–589. https://doi.org/10.1108/SAMPJ-03-2018-0081

Plumlee, M., Brown, D., Hayes, R. M., & Marshall, R. S. (2015). Voluntary environmental disclosure quality and firm value: Further evidence. *Journal of Accounting and Public Policy*, *34*(4), 336–361. https://doi.org/10.1016/J.JACCPUBPOL.2015.04.004

Porrúa, M., & Contreras B. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*.

Power, M. (2004). The risk management of everything. *Journal of Risk Finance*, *5*(3), 58–65. https://doi.org/10.1108/eb023001

Prado-Lorenzo, J. M., Rodríguez-Domínguez, L., Gallego-Álvarez, I., & García-Sánchez, I. M. (2009). Factors influencing the disclosure of greenhouse gas emissions in companies world-wide. *Management Decision*, *47*(7), 1133–1157. https://doi.org/10.1108/00251740910978340

Pucheta-Martínez, M. C., & Gallego-Álvarez, I. (2019). An international approach of the relationship between board attributes and the disclosure of corporate social responsibility issues. *Corporate Social Responsibility and Environmental Management*, *26*(3), 612–627. https://doi.org/10.1002/CSR.1707

PwC. (2022). *2022 Global Digital Trust Insights*.

PWC. (2018a). *2018 Global Investor Survey 2018: Anxious Optimism in a Complex World*.

PWC. (2018b). *Better Oversee Cyber Risk. November*.

PWC. (2018c). *Rethinking cybersecurity disclosures to investors - What executives and boards need to know about the SEC's guidance: June 2018*. www.pwc.com/cybersecurity

PWC. (2018d). *US2018-07: SEC issues interpretive guidance on cybersecurity disclosures*. https://viewpoint.pwc.com/dt/us/en/pwc/in_briefs/2018/2018__7_US/us201807_sec_issues__US.html

PWC. (2021). *Encuesta Global Digital Trust Insights 2021 Contenido*.

Radu, C., & Smaili, N. (2021). Board Gender Diversity and Corporate Response to Cyber

Risk: Evidence from Cybersecurity Rel ated Disclosure. *Journal of Business Ethics*, *1*, 3. https://doi.org/10.1007/s10551-020-04717-9

RAE ASALE. (2020). *Diccionario de la lengua española*. Edición 2020. https://dle.rae.es/cibernético?m=form

Rainer, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems*, *8*(1), 129–147. https://doi.org/10.1080/07421222.1991.11517914

Rajgopal, S. (1999). Early evidence on the informativeness of the SEC's market risk disclosures: The case of commodity price risk exposure of oil and gas producers. *Accounting Review*, *74*(3), 251–280. https://doi.org/10.2308/accr.1999.74.3.251

Ramirez, R., & Choucri, N. (2016). Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, *4*, 2216–2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rankin, M., Windsor, C., & Wahyuni, D. (2011). An investigation of voluntary corporate greenhouse gas emissions reporting in a market governance system: Australian evidence. *Accounting, Auditing and Accountability Journal*, *24*(8), 1037–1070. https://doi.org/10.1108/09513571111184751

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*(1), 121–139. https://doi.org/10.1287/ISRE.1080.0174

Reid, R., & Van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies. *Information Security South Africa (ISSA)*, 1–7. https://doi.org/978-1-4799-3383-9

Renn, B. O. (2008). Risk Governance new & Forthcoming Titles. En *Sustainable Development*. https://www.routledge.com/Risk-Governance-Coping-with-Uncertainty-in-a-Complex-World/Renn/p/book/9781844072927

Renn, O. (1998). The role of risk perception for risk management. *Reliability Engineering and System Safety*, *59*(1), 49–62. https://doi.org/10.1016/S0951-8320(97)00119-1

Rennekamp, K. (2012). Processing Fluency and Investors' Reactions to Disclosure Readability. *Journal of Accounting Research*, *50*(5), 1319–1354. https://doi.org/10.1111/J.1475-679X.2012.00460.X

Reverte, C. (2009). Determinants of corporate social responsibility disclosure ratings by Spanish listed firms. *Journal of Business Ethics*, *88*(2), 351–366.

https://doi.org/10.1007/s10551-008-9968-9

Rhodes, M. J. (2010). Information Asymmetry and Socially Responsible Investment. *Journal of Business Ethics*, *95*(1), 145–150. https://doi.org/10.1007/s10551-009-0343-2

Ripley, W. Z. (1927). *Main Street and Wall Street*. https://www.amazon.es/Main-Street-Wall-William-Ripley/dp/0914348078

Rivera-Arrubla, Y. A., Zorio-Grima, A., & García-Benau, M. A. (2017). Integrated reports: Disclosure level and explanatory factors. *Social Responsibility Journal*, *13*(1), 155–176. https://doi.org/10.1108/SRJ-02-2016-0033

RobecoSAM. (2018). *The sustainability yearbook 2018*. https://www.comunicarseweb.com/sites/default/files/the_sustainability_yearbook_2018_spanish.pdf

Roberts, L. G. (1988). The ARPANET & Computer Networks. *Proceedings of the ACM Conference on The history of personal workstations*. https://doi.org/10.1145/12178

Rodríguez-Ariza, L., Frías Aceituno, J. V., & García Rubio, R. (2014). The board of directors and the sustainability report. *Revista de Contabilidad-Spanish Accounting Review*, *17*(1), 5–16. https://doi.org/10.1016/j.rcsar.2013.02.002

Rogers, E. (2003). Review Diffusion of Innovations, by Everett Rogers (1995). *Stanford University*, *1995*, 5. http://web.stanford.edu/class/symbsys205/Diffusion of Innovations.htm

Rose, C. (2007). Does female board representation influence firm performance? The Danish evidence. *Corporate Governance: An International Review*, *15*(2), 404–413. https://doi.org/10.1111/J.1467-8683.2007.00570.X

Ross, S. A. (1977). Determination of financial structure: the incentive- signalling approach. *Bell J Econ*, *8*(1), 23–40. https://doi.org/10.2307/3003485

Roundtable, B. (1978). The Role and Composition of the Board of Directors of the Large Publicly Owned Corporation — Statement of the bussiness Roundtable. *The Roundtable*, *33*(4), pp . 2083-2113. https://www.jstor.org/stable/40685901?seq=1

Rowe, D. C., Ekstrom, J. J., & Lunt, B. M. (2012). Cyber-Security, IAS and the Cyber Warrior. *The Colloquium for Information Systems Security Education*.

Rupley, K. H., Brown, D., & Marshall, S. (2017). Evolution of corporate reporting: From stand-alone corporate social responsibility reporting to integrated reporting. *Research in Accounting Regulation*, *29*(2), 172–176.

https://doi.org/10.1016/J.RACREG.2017.09.010

S&P. (2020). *América Latina*.

Salet, H. A. (2004). *Delaware ' s Good Faith*. *89*(2).

Sánchez, I. M. G., Domínguez, L. R., & Álvarez, I. G. (2011). Corporate governance and strategic information on the internet: A study of Spanish listed companies. *Accounting, Auditing and Accountability Journal*, *24*(4), 471–501. https://doi.org/10.1108/09513571111133063

Santiago Castro, M., Brown, C. J., & Baéz, A. (2009). Prácticas de Gobierno Corporativo en América Latina. *Revista Latinoamericana de Administración*, *43*, 26–40. http://revistaacademia.cladea.org

Sargent, John & Ghaddar, S. (2001). *International Success of Business Groups as an Indicator of National Competitiveness The Mexican Example*. https://www.tandfonline.com/doi/abs/10.1300/J140v02n03_05

SASB. (2021a). *Estándares SASB*. https://www.sasb.org/standards/download/

SASB. (2021b). *SASB Materiality Map*. https://materiality.sasb.org/

Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, *2*(2), 17–32.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *Proceedings - International Conference on Distributed Computing Systems*, *2016-August*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Scaltrito, D. (2016). Voluntary disclosure in Italy: Firm-specific determinants an empirical analysis of Italian listed companies. *EuroMed Journal of Business*, *11*(2), 272–303. https://doi.org/10.1108/EMJB-07-2015-0032

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8. https://doi.org/https://doi.org/10.15394/jdfsl.2017.1476

Schubert, D; Cedarbaum, J and Schloss, W. (2015). The SEC's Two Primary Theories in Cybersecurity Enforcement Actions. *The Cybersecurity Law Report*, *1*(1), 39–70.

Scott, W. R. (2008). Approaching adulthood: The maturing of institutional theory. *Theory and Society*, *37*(5), 427–442. https://doi.org/10.1007/s11186-008-9067-z

SEC. (1997). Disclosure of Accounting Policies for Derivative Financial Instruments, and

Derivative Commodity Instruments and Disclosure of Quantitative and Qualitative Information about Market Risk Inherent in Derivative Financial Instruments, Other Financial Instrum. *Federal Register*, *62*(27), 6044–6079. https://www.federalregister.gov/documents/1997/02/10/97-2991/disclosure-of-accounting-policies-for-derivative-financial-instruments-and-derivative-commodity

SEC. (2005a). *Release #33-8591: Securities Offering Reform (Section VII: Additional Exchange act Disclosure Provisions)* (Número 1294).

SEC. (2005b). *Staff Statement on Management's Report on Internal Control Over Financial Reporting*. https://www.sec.gov/info/accountants/stafficreporting.htm

SEC. (2017). *Prospectus summary, risk factors § 229.503 (Item 503)*. 473–475. https://doi.org/10.4135/9781608712380.n519

SEC. (2018a). *Federal Register Commission Statement and Guidance on Public Company Cybersecurity Disclosures*. https://www.federalregister.gov/documents/2018/02/26/2018-03858/commission-statement-and-guidance-on-public-company-cybersecurity-disclosures

SEC. (2018b). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

SEC. (2020). *17 CFR § 229.105 - (Item 105) Risk factors*. https://www.law.cornell.edu/cfr/text/17/229.105

SEC. (2021a). *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures*. https://www.sec.gov/news/press-release/2021-169

SEC. (2021b). *SEC Charges Issuer With Cybersecurity Disclosure Controls Failures*. https://www.sec.gov/news/press-release/2021-102

SEC. (2022). *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. *13*(34), 1–204.

Security Boulevard. (2021). *How Offensive AI Can Disarm Cybersecurity*. https://securityboulevard.com/2021/06/how-offensive-ai-can-disarm-cybersecurity/

Shankar, K. S. (1977). *The Total Computer Security Problem: An overview*.

Shleifer, A., Vishny, R. W., Diamond, D., Easterbrook, F., Harris, M., Hellwig, M., Hines, J., Jonsson, T., Kaplan, S., Porta, R. La, Lopez-De-Silanes, F., Rajan, R., Scharfstein, D., Stulz, R., & Zingales, L. (1997). A Survey of Corporate Governance.

*The Journal of Finance*, *52*(2), 737–783. https://doi.org/10.1111/J.1540-6261.1997.TB04820.X

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Security Management Handbook, Sixth Edition*, 357–380. https://doi.org/10.1201/9781420072419-28

Sinha, T., & Vaughan, E. J. (1994). Fundamentals of Risk and Insurance. En *The Journal of Risk and Insurance* (Vol. 61, Número 2). https://doi.org/10.2307/253725

Siponen, M. T., & Oinas-Kukkonen, H. (2007). *A Review of Information Security Issues and Respective Research Contributions*.

Skinner, D. J. (1997). Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics*, *23*(3), 249–282. https://doi.org/10.1016/S0165-4101(97)00010-4

Slovic, P. (1987). Perception of Risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/SCIENCE.3563507

Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations. Oxford: UK: Clarendon Press.*

Sofistic, C. (2017). *Breve historia de la Ciberseguridad*. https://www.sofistic.com/blog-Ciberseguridad/la-breve-historia-de-la-Ciberseguridad/

Solomon, J. (2010). *Corporate governance and accountability*. 414.

Solomon, J. F., Solomon, A., Norton, Si. D., & Joseph, N. L. (2000). A conceptual framework for corporate risk disclosure emerging from the agenda for corporate goverance reform. *The British Accounting Review*, *32*(4), 447–478. https://doi.org/10.1006/bare.2000.0145

Solomon, Jill. (2019). *Corporate Governance and Accountability* (5TH ed.). John Wiley.

Souppaya, M., & Scarfone, K. (2013). *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. https://doi.org/10.6028/NIST.SP.800-83R1

Spence, M. (1973). Job Market Signaling. En *The Quarterly Journal of Economics* (Vol. 87, Número 3). https://www.sciencedirect.com/science/article/pii/B9780122148507500255

Spence, M. (2002). La señalización y la estructura informativa de los mercados. *RAE: Revista Asturiana de Economía*, *25*, 49–94.

Srinidhi, B., Gul, F. A., & Tsui, J. (2011). Female Directors and Earnings Quality*.

*Contemporary Accounting Research*, *28*(5), 1610–1644. https://doi.org/10.1111/J.1911-3846.2011.01071.X

Stapledon, G. (2006). The development of corporate governance in Australia. En *Handbook on International Corporate Governance*.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. En *Politics and Governance* (Vol. 6, Número 2, pp. 1–4). Cogitatio Press. https://doi.org/10.17645/pag.v6i2.1569

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/J.SSCI.2020.105143

Subcommittee of Capital Markets; Capital Markets Committee, Capital Financial and, & Federation Japan Business. (2022). *Improve the effectiveness of the revised Corporate Governance Code*. https://www.keidanren.or.jp/policy/2022/047.pdf

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review*, *20*(3), 571. https://doi.org/10.2307/258788

Superintendencia del Mercado de Valores. (2013). *Código De Buen Gobierno Corporativo Para Las Sociedades Peruanas 2013*.

SuperSociedades, Confecámaras, & CCB. (2020). *Guía de Buenas Prácticas de Gobierno Corporativo para Empresas Competitivas, Productivas y Perdurables*.

Szegö, G. (2002). Measures of risk. *Journal of Banking & Finance*, *26*, 1253–1272. https://doi.org/10.1016/S1548-5315(11)70388-6

Szulc, T., & American Assembly. (1970). *The United States and the Caribbean*. 212.

Tabassum, N., & Singh, S. (2020). Corporate governance and organisational performance: The impact of board structure. En *Corporate Governance and Organisational Performance: The Impact of Board Structure*. https://doi.org/10.1007/978-3-030-48527-6

Taiwo, O. J., Owowlabi, B. A., Adedokun, Y., & Ogundajo, G. (2021). Sustainability reporting and market value growth of quoted companies in Nigeria. *Journal of Financial Reporting and Accounting*, *20*(3/4), 542–557. https://doi.org/10.1108/JFRA-05-2020-0143/FULL/PDF

Taylor, G., Tower, G., & Neilson, J. (2010). Corporate communication of financial risk. *Accounting & Finance*, *50*(2), 417–446. https://doi.org/10.1111/j.1467-629X.2009.00326.x

TCFD. (2021). *TCFD Status Report*. *October*.

Terjesen, S., Sealy, R., & Singh, V. (2009). Women directors on corporate boards: A review and research agenda. *Corporate Governance: An International Review*, *17*(3), 320–337. https://doi.org/10.1111/j.1467-8683.2009.00742.x

Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments 2020 7:2*, *7*(2), 69–84. https://doi.org/10.1007/S40860-020-00115-0

Toronto Stock Exchange. (2014). Corporate Governance in Canada. *The International Corporate Governance System*, *December*, 90–100. https://doi.org/10.1057/9781137360014_7

Trend Micro; OEA. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. 60. https://www.sites.oas.org/cyber/Certs_Web/OEA-Trend Micro Reporte Seguridad Cibernetica y Porteccion de la Inf Critica.pdf

Tricker, R. (1978). *The independent director : a study of the non-executive director and of the audit committee*. 104. https://books.google.com/books/about/The_Independent_Director.html?hl=es&id=8aAjAQAAMAAJ

Tricker, R. (2020). The evolution of corporate governance. En *The SAGE Handbook of Corporate Governance* (Vol. 7175). https://doi.org/10.4135/9781446200995.n1

UIT. (2012). *UIT-IMPACT organizan un cibersimulacro transfronterizo para la región de los Estados Árabes*.

Unión Europea. (2016a). *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo*. Unión Europea.

Unión Europea. (2016b). Reglamento (UE) 2016/ 679. *Diario Oficial de la Unión Europea*.

Unión Europea. (2019). *REGLAMENTO (UE) 2019/881*. Diario Oficial de la Unión Europea.

Unión Internacional de Telecomunicaciones. (s. f.). *LA AGENDA SOBRE CIBERSEGURIDAD GLOBAL – ACTUALIZACION*.

Unión Internacional de Telecomunicaciones. (2008). Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad. *Unión Internacional de Telecomunicaciones, 1205*, 66.

United Nations General Assembly. (2009). *Resolución 64/25*.

United States Department of Justice. (2001). The USA PATRIOT Act : Preserving Life and Liberty. *USA Department of Justice*. http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

Urrutia, F. D. (2020). *Cybersecurity: risks, progress, and the way forward in Latin America and the Caribbean*. https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

Van der Walt, N., & Ingley, C. (2003). Board Dynamics and the Influence of Professional Background, Gender and Ethnic Diversity of Directors. *Corporate Governance: An International Review*, *11*(3), 218–234. https://doi.org/10.1111/1467-8683.00320

Vaughan, E. (1997). *Risk Management*. Wileyl.

Veblen, T. (1904). *The Theory of Business Enterprise*.

Velte, P., & Stawinoga, M. (2016). Integrated reporting: The current state of empirical research, limitations and future research implications. *Journal of Management Control 2016 28:3*, *28*(3), 275–320. https://doi.org/10.1007/S00187-016-0235-4

Verrecchia, R. E. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, *5*(C), 179–194. https://doi.org/10.1016/0165-4101(83)90011-3

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, L., & Tuttle, B. (2014). Using corporate social responsibility performance to evaluate financial disclosure credibility. *https://doi.org/10.1080/00014788.2014.922408*, *44*(5), 523–544. https://doi.org/10.1080/00014788.2014.922408

Wang, M. C. (2017). The relationship between firm characteristics and the disclosure of sustainability reporting. *Sustainability (Switzerland)*, *9*(4).

https://doi.org/10.3390/SU9040624

Wang, T., & Hsu, C. (2013). Board composition and operational risk events of financial institutions. *Journal of Banking and Finance*, *37*(6), 2042–2051. https://doi.org/10.1016/j.jbankfin.2013.01.027

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Wang, T., Ulmer, J. R., & Kannan, K. (2013). The Textual Contents of Media Reports of Information Security Breaches and Profitable Short-Term Investment Opportunities. *Journal of Organizational Computing and Electronic Commerce*, *23*(3), 200–223. https://doi.org/10.1080/10919392.2013.807712

WEF. (2017). Advancing Cyber Resilience - Principles and Tools for Boards. *World Economic Forum*, *January*, 40.

WEF. (2020a). A New Paradigm for Business of Data: Briefing paper. *World Economic Forum*, 15. http://www3.weforum.org/docs/WEF_New_Paradigm_for_Business_of_Data_Report_2020.pdf

WEF. (2021a). *Centre for Cybersecurity > Platforms | World Economic Forum*. https://www.weforum.org/platforms/the-centre-for-cybersecurity

WEF. (2021b). *Future Series: Ciberseguridad, tecnología emergente y riesgo sistémico | foro Economico Mundial*. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

WEF. (2021c). *The Global Risks Report 2021: 16th Edition*.

WEF. (2022). *The Global Risks Report 2022*. https://www.weforum.org/reports/global-risks-report-2022

WEF. (2023). *The Global Risks Report 2023 18th Edition*.

WEF, W. E. F. (2020b). *The Global Risks Report 2020*. https://es.weforum.org/reports/the-global-risks-report-2020

Wells, H. (2010). The Birth of Corporate Governance The traditional view dates them to 1932 with the publication of Adolf A . *Seattle University Law Review*, *33*(4), 1247–1292.

Werder, Axel ; Talaulicar, T. (2006). Corporate governance developments in Germany. En *Handbook on International Corporate Governance*.

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. En *Cengage Learning*.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt. *USENIX Security Symposium*, 679–702. http://www.doug-tygar.com/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf

Williams, T. D. (2020). Epistemological Questions for Cybersecurity. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*, 1–4. https://doi.org/10.1109/CyberSecurity49315.2020.9138884

Woollacott, P. (2007). Cybercrime comes of age. *ITNOW*, *49*(2), 6–7. https://doi.org/10.1093/COMBUL/BWL110

Wuerges, A. F. E., & Borba, J. A. (2014). Fraudes contábeis: Uma estimativa da probabilidade de detecção. *Revista Brasileira de Gestao de Negocios*, *16*(52), 466–483. https://doi.org/10.7819/rbgn.v16i52.1555

Yang, A., Kwon, Y. J., & Lee, S. Y. T. (2020). The impact of information sharing legislation on cybersecurity industry. *Industrial Management & Data Systems*, *120*(9), 1777–1794. https://doi.org/10.1108/IMDS-10-2019-0536

Yermack, D. (1996). Higher market valuation of companies with a small board of directors. *Journal of Financial Economics*, *40*(2), 185–211. https://doi.org/10.1016/0304-405X(95)00844-5

Yeung, W. H., & Lento, C. (2018). Ownership structure, audit quality, board structure, and stock price crash risk: Evidence from China. *Global Finance Journal*, *37*, 1–24. https://doi.org/10.1016/J.GFJ.2018.04.002

Zeller, G., & Scherer, M. (2020). A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*. https://doi.org/10.1007/s13385-021-00290-1

# CAPÍTULO 6. CONCLUSIONES, IMPLICACIONES, LIMITACIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN

## 6.1. Conclusiones

El desarrollo de esta investigación nos ha permitido evidenciar que la Ciberseguridad es un tema fundamental en el mundo actual. La presencia latente de este riesgo en el mundo corporativo y las connotaciones económicas que representa, lo convierten en una amenaza de rápido crecimiento y quizás la más peligrosa a la que se enfrentan las organizaciones en la actualidad. El recuento de hechos históricos que hemos relacionado nos permite concluir que la Ciberseguridad en los últimos treinta años ha obtenido un posicionamiento mundial sin precedentes, razón por la cual es de gran importancia que la comunidad mundial enfrente el riesgo de Ciberseguridad como un compromiso de múltiples partes.

Ratificamos que no existe un consenso sobre lo que los investigadores, educadores y profesionales ven como conocimiento fundamental en Ciberseguridad. El conflicto por regular y gobernar este campo de conocimiento se evidencia en el escaso panorama de su teoría y en los limitados métodos para comprender su quehacer e interpretar las decisiones políticas que enmarcan sus problemáticas. En general, concluimos que esta área temática requiere propuestas novedosas que amplíen la frontera del conocimiento relacionado.

Los resultados de nuestra búsqueda nos permiten afirmar que en la actualidad no existe un concepto único de aceptación mundial del término ´Ciberseguridad´, ni un pronunciamiento de aceptación internacional sobre el mismo. En este contexto, creemos necesario que la comunidad mundial trate el riesgo de Ciberseguridad como un desafío sistémico, una toma de decisiones colectiva y una acción coordinada entre los gobiernos, el sector privado y la sociedad civil.

De acuerdo con el estudio de la literatura previa, el concepto de Ciberseguridad a través del tiempo ha venido sumando componentes, solicitando la protección de tres aspectos que necesariamente se adhieren a su definición: la protección de las personas, la protección de las cualidades de la seguridad de la información y la protección de los activos físicos e infraestructuras que se encuentran en el ciberespacio. El análisis que hemos realizado a las definiciones de Ciberseguridad planteadas por organismos internacionales enmarca la falta de uniformidad en torno al concepto y el reducido alcance frente a los elementos que deben constituir actualmente su definición. Sería necesario, por tanto, consensuar una definición a nivel internacional que contemple los componentes

de protección en los tres aspectos mencionados y que sea aplicable a cualquier ámbito geográfico.

Dos características, multidimensionalidad e interdisciplinariedad, enmarcan el significado de Ciberseguridad y son ratificadas por el estudio de origen inglés CYBOK (2021), quienes atribuyen 21 áreas del conocimiento. En la misma línea, la Agencia Europea de Seguridad de las Redes y de la Información ENISA (2015), le asignan cinco dominios a la Ciberseguridad desde el ámbito nacional: seguridad de las comunicaciones, seguridad de las operaciones, seguridad de la información, seguridad militar y seguridad física. Estos dominios igualmente representan la amplitud del alcance global del término.

Por su parte, la geopolítica y la cooperación internacional han definido el marco normativo internacional sobre Ciberseguridad. El análisis realizado nos ha permitido constatar que el Convenio de Budapest, la Recomendación de la Unión Internacional de Telecomunicaciones en 2008, la Recomendación OCDE (2004), la Directiva 2016/1148, el Reglamento General para la Protección de Datos (RGPD) y la Ley de Ciberseguridad para la UE son las iniciativas legislativas más importantes por su impacto en el ámbito internacional. Es de anotar que la búsqueda de acuerdos internacionales para perseguir al cibercrimen es fundamental e imprescindible para mitigar su impacto a nivel mundial, escenario sin fronteras para este tipo de delitos.

Dado que no existe unanimidad en el establecimiento de dimensiones temáticas que estructuren y agrupen los aspectos de Ciberseguridad en el ámbito empresarial, a partir de nuestro estudio proponemos las siguientes dimensiones temáticas: gobernanza, como base para la toma de decisiones por parte de la Junta Directiva o la alta gerencia sobre las estrategias de las organizaciones, con el objetivo de lograr la supervisión y liderazgo para el manejo del riesgo cibernético; estrategia corporativa, ya que como estrategia de Ciberseguridad se compone de planes de alto nivel sobre cómo una organización va a asegurar sus activos y minimizar el riesgo cibernético; gestión de riesgos, considerando un sistema de gestión de riesgo empresarial en el que se priorizan, mitigan e informan los principales riesgos de la organización; y evaluación de las implicaciones financieras, ya que la afectación económica que traen consigo las pérdidas económicas y de reputación

por posibles ciberataques o incidentes cibernéticos, requieren ser evaluadas y valoradas dentro de la información financiera de la organización.

Según nuestro estudio, encontramos que en la actualidad la definición de riesgo consignada en la última versión ISO 31000 (2018) presenta una serie de elementos que dejan ver el avance de este concepto. El repaso histórico del riesgo corporativo muestra cómo las crisis económicas han sido las impulsoras de su desarrollo. Es de anotar que el primer Estándar de Gestión de Riesgos se propone en Australia AS/NZS 4360:1995 (revisado desde 1999 y 2004), y reúne por primera vez diferentes subdisciplinas. Este Estándar es seguido de esfuerzos similares en Canadá, Japón y el Reino Unido.

Desde los hallazgos de nuestro estudio, proponemos que las revelaciones sobre riesgos se construyan desde una óptica prospectiva que mejore la rendición de cuentas y las asimetrías de acceso a la información corporativa, al mejorar la medición y divulgación de los asuntos relacionados con el riesgo. Concluimos que un referente internacional para América Latina en la divulgación de riesgos, lo constituyen los Principios de Gobierno Corporativo del G20 y de la OCDE. Además, nos parece importante mencionar que en el ámbito internacional gozan de un reconocimiento muy marcado las divulgaciones financieras establecidas por el Grupo de Trabajo sobre Divulgaciones Financieras relacionadas con el riesgo de Cambio Climático (TCFD).

Nuestra busqueda, ratifica cómo Estados Unidos presenta avances importantes en la divulgación de información de riesgos de Ciberseguridad. La emisión de las guías SEC (2011; 2018) recomiendan que en el informe se incluyan las divulgaciones sobre riesgos e incidentes de Ciberseguridad para el caso de empresas extranjeras reguladas por la SEC en el artículo 3. D del Formulario 20-F. Esta medida va dirigida para todos los “emisores privados extranjeros” con acciones de capital inscritas en las bolsas de Estados Unidos, por lo que podemos decir que ésta es una exigencia con repercusiones en el contexto internacional.

Respecto a la divulgación de información sobre los riesgos de Ciberseguridad podemos afirmar que estas revelaciones se presentan especialmente en el informe anual, el cual se ha convertido en el medio de comunicación de las corporaciones con sus diferentes partes interesadas. Desde la responsabilidad social que se atribuye a las organizaciones, la

sociedad interpela cada vez con mayor frecuencia el comportamiento organizacional, por lo que se exige transparencia, responsabilidad e información estratégica que conecte el pasado con los riesgos y oportunidades futuras. Las revelaciones sobre Ciberseguridad expuestas en el informe anual mejoran las relaciones con los actores del mercado, reguladores y autoridad de protección de datos y la organización interna de la empresa. En la actualidad, la preparación de los informes anuales reportados por las organizaciones se efectúa a partir de algunos estándares de aceptación internacional. Concretamente, por su importancia, destacamos los siguientes como referentes de primer orden:

- Las directrices GRI 2016 emitidos por la Junta de Estándares de Sostenibilidad Global (GSSB). Los aspectos de Ciberseguridad a revelar en el informe de sostenibilidad se pueden relacionar en especial con el ítem GRI 418 Privacidad de cliente GRI 418 – 1 "Reclamaciones fundamentadas relativas a violaciones de la privacidad del cliente y pérdida de datos del cliente".

- Los estándares emitidos por el American Sustainability Accounting Standard Board (SASB) que divulgan información a los inversores sobre la materialidad financiera de aspectos relacionados con sostenibilidad entre las empresas registradas ante la Securities Exchange Commission (SEC). La información sobre Ciberseguridad se divulga en la dimensión de capital social (SASB, 2021b).

- En el marco del International Integrated Reporting Council (IIRC), el informe integrado es una comunicación resumen sobre cómo la estrategia, gobernanza, rendimiento y perspectivas de una organización desde el contexto de su medio ambiente, conducen a la creación, preservación o deterioro del valor sobre el corto, medio y largo plazo.

- Presentaciones 10-K en EDGAR, que es el formulario oficial del informe anual requerido por la Comisión de Bolsa y Valores de EE. UU, en el que se presenta un resumen completo del desempeño financiero de una compañía.

- Presentaciones 20-F en EDGAR, formulario anual que deben presentar los titulares privados extranjeros que emiten acciones de acuerdo con la Ley de la Bolsa de Valores en los Estados Unidos 1934.

Según nuestra búsqueda, este estudio concluye la inexistencia de un índice que permita evaluar el alcance de la divulgación de información sobre Ciberseguridad en los países objeto de estudio. El Índice de Divulgación de Información sobre Ciberseguridad propuesto en este trabajo tiene como objetivo obtener una herramienta que, tomando como base para su elaboración los principales estándares de aceptación global, permita evaluar el alcance de la divulgación de la información sobre Ciberseguridad por parte de las empresas. Está compuesto por 27 elementos individuales, asociados con una de las cuatro dimensiones siguientes: gobernanza (5), estrategia (6), gestión de riesgos (13) e implicaciones financieras (3). La selección de los ítems que componen el Índice de Ciberseguridad se hizo a partir de literatura previa, estudios de firmas internacionales de contabilidad y auditoría, estándares internacionales, como ISO y GRI, guías SEC (2011; 2018), la Norma General de Protección de Datos Reglamento (GDPR) de la Unión Europea, y otros documentos propuestos por entidades con amplio reconocimiento internacional, como la OCDE, el BID, la OEA y el Global Reporting Iniciative (GRI), entre otros.

Dado que el instrumento de medición propuesto ha sido elaborado con base en estos estándares internacionales relacionados con el riesgo cibernético corporativo, puede ser aplicable en futuras investigaciones a empresas que desarrollan su actividad en otras áreas geográficas. De esta forma, se espera que este índice se convierta en un punto de partida para el análisis comparativo en otros países en diferentes períodos de tiempo, lo que permitirá conocer las tendencias en la divulgación de información de Ciberseguridad desde diferentes perspectivas. Creemos que el instrumento de medición propuesto constituye un instrumento novedoso que permite evaluar el alcance de la divulgación de información sobre Ciberseguridad. Teniendo en cuenta que la Ciberseguridad se ha convertido en una responsabilidad empresarial, la información que revela este índice puede constituir un punto de referencia para la valoración de las organizaciones por parte de los diferentes grupos de interés.

En cuanto al análisis longitudinal por países, la aplicación del instrumento permite verificar que las empresas que constantemente divulgaron más información sobre Ciberseguridad durante el período 2016-2020 fueron las argentinas. Según nuestros resultados, el 86% de las empresas de la muestra de este país reportaron a la SEC. En su mayoría, estas empresas pertenecen al sector financiero, situación que puede generar un

aumento en la divulgación de Ciberseguridad. La medición de la divulgación por sector muestra cómo el sector financiero obtuvo liderazgo durante los cinco años del estudio. En este sentido, podemos señalar que en los países objeto de estudio, y a nivel internacional, la normativa para este sector se ha incrementado y es más exigente, debido a que estas organizaciones presentan una mayor vulnerabilidad a los ciberataques. De esta forma, constatamos que las prácticas de divulgación de información sobre Ciberseguridad han evolucionado a la luz de las expectativas de los reguladores financieros. Dadas las implicaciones de las amenazas de Ciberseguridad en todas las industrias es necesario potenciar el desarrollo de las revelaciones de Ciberseguridad en los demás sectores económicos.

Los resultados del estudio comparativo por dimensiones indican cómo la dimensión de estrategia obtuvo el puntaje más alto durante el período 2016-2020. En concreto, a partir de los resultados obtenidos, podemos concluir que, en términos generales, las empresas analizadas revelaron información sobre las acciones diseñadas a largo plazo, como las estrategias de Ciberseguridad, y se han interesado en comunicar las medidas relacionadas con los ciberiesgos de gestión, concretando cómo este riesgo emergente se va vinculando, poco a poco, con otros riesgos corporativos. Las revelaciones también permiten visualizar cómo la Junta Directiva y la gerencia se vinculan gradualmente en la supervisión de los asuntos de Ciberseguridad.

Respecto al panorama de la Ciberseguridad en América Latina, podemos sintetizar que las acciones en materia de Ciberseguridad son impulsadas por la OEA con diferentes iniciativas que promueven la Ciberseguridad y la cooperación internacional para la región. A nivel nacional, los países se han adherido gradualmente a las medidas de política internacional. Algunas han tenido avances importantes, como la ratificación del Convenio de Budapest, la aprobación de la estrategia nacional y la creación de leyes de protección de datos, entre otras. Es por ello que la medición del compromiso nacional en Ciberseguridad en 2020 muestra un mejor puntaje, en comparación con años anteriores, en las diferentes dimensiones que componen el Índice Global de Ciberseguridad: medidas legales, técnicas, organizacionales, de desarrollo de capacidades y de cooperación.

El mayor nivel de desarrollo se encontró en Brasil (97,68), seguido de México (81,68), Uruguay (75,15), República Dominicana (75,07), Chile (68,83), Costa Rica (67,46),

Colombia (63,74), Perú (55,68) y Argentina (50,12). Pero, a pesar de los logros alcanzados hasta la fecha, el rezago de la región en algunos frentes obliga a tomar medidas para mejorar su capacidad de respuesta ante riesgos y amenazas cibernéticas.

Desde la cronología que realizamos sobre el origen y el desarrollo del Gobierno Corporativo, enfatizamos la relación entre la organización y la sociedad. Los hechos evidencian la incorporación de nuevos elementos que han ampliado su perspectiva y cobertura en aras de superar los problemas generados por la crisis de confianza. Además, constatamos que se han incorporado conceptos que van más allá de la protección del accionista individual e institucional, como el manejo y vigilancia de nuevos riesgos corporativos de alta probabilidad e impacto. En consecuencia, independiente del modelo, desde la gobernanza corporativa se entregan mayores responsabilidades a la Junta Directiva entorno a la supervisión como mecanismo de control. En este sentido, la Junta Directiva puede tener un papel importante en la divulgación de información sobre Ciberseguridad, razón por la cual se ha estudiado para las empresas latinoamericanas.

Dado el objeto de este estudio, hemos retomado para la presente investigación algunos mecanismos de control relacionados con la estructura de la Junta Directiva como factor determinante de la divulgación de información: tamaño de la Junta, independencia, diversidad de género, Comité de Auditoría y Comité de Ciberseguridad.

Es importante resaltar que las condiciones en Latinoamérica relacionadas con el problema de la agencia se trasladan a los inversionistas mayoritarios, quienes se suponen se benefician de los minoritarios. El Gobierno Corporativo podría constituir una herramienta para alinear estos intereses. Según la revisión que hemos hecho de códigos y normativa de los países objeto de estudio, en lo relacionado con las prácticas de Gobierno Corporativo los seis países latinoamericanos contemplan: ´la implementación de una visión estratégica por parte del consejo de administración´, ´la creación de un Comité de Auditoría´ y 'la supervisión de la gestión de riesgos y los sistemas de control interno´. Respecto a la inclusión de temas como ´involucramiento de consejeros independientes´, Chile es el único país que no lo considera. En cuanto a temas como ´la responsabilidad social', tan solo México y Perú no lo contemplan. Y, en relación a ´las Tecnologías de la Información´, el tema se vincula en los códigos de Colombia y México.

Con base en los resultados descriptivos de capítulo cuatro, concluimos la necesidad de recomendar a reguladores y entes de vigilancia y control de la región ampliar la diversidad de las juntas directivas de las empresas. Los resultados descriptivos relacionados con la conformación de la Junta Directiva confirman la limitada participación con tan solo un 11% de las mujeres en los directorios de las empresas listadas en Latinoamérica, estos reportan que tan solo una de cada diez miembros del directorio es mujer. Respecto a los directores independientes en promedio tan solo el 42% del total de los miembros del directorio se clasifican como directores independientes. El 70% de las empresas cuentan con un Comité de Auditoria, mientras que el 12% cuentan con un Comité de Ciberseguridad en particular.

En cuanto a los resultados del estudio empírico plasmado en el capítulo cuatro, éstos denotan cómo la estructura del Gobierno Corporativo es un factor determinante en la divulgación de información relacionada con los riesgos de Ciberseguridad en América Latina. Respecto a la estructura de los consejos de administración, las empresas con juntas directivas más pequeñas o con menos miembros presentan un mayor alcance en sus revelaciones sobre Ciberseguridad. La participación de un mayor número de miembros independientes en los consejos de administración también se relaciona de forma significativa con la divulgación. Contrario a los resultados esperados en estudios previos, la participación de las mujeres en la divulgación sobre Ciberseguridad presenta una asociación no significativa, situación que puede obedecer a la baja participación femenina en las juntas corporativas en América Latina. Sobre la delegación de los riesgos de Ciberseguridad al Comité de Auditoría, concluimos que no afecta de forma importante la divulgación de Ciberseguridad. Por el contrario, la designación de estas funciones a un comité dedicado exclusivamente a los riesgos de Ciberseguridad presenta una relación significativa y directa frente a la divulgación.

Aumentar la divulgación de los riesgos de Ciberseguridad puede verse como una decisión ética por parte de las organizaciones, ya que la información divulgada sobre riesgos cibernéticos es informativa y útil para las partes interesadas al momento de evaluar la probabilidad de futuros incidentes. Este estudio, basado en la teoría de la agencia y la teoría de las partes interesadas, contribuye a la limitada investigación.

En el capítulo cinco desde la teoría institucional se analizan variables a nivel de país que inciden como factores determinantes en la divulgación de información sobre Ciberseguridad. Los principales avances respecto a investigaciones anteriores están relacionados con la incorporación de variables que evalúan el efecto del Índice de Ciberseguridad, de Globalización, de Gobernanza y de Desarrollo Humano respecto a la divulgación de riesgos de Ciberseguridad. Estos corresponden a índices multidimensionales que incorporan diferentes factores institucionales del orden nacional.

La información descriptiva nos confirma que la situación de América Latina requiere mejoras importantes en aspectos de ciberseguridad, gobernanza, globalización y desarrollo humano. De acuerdo al estudio empírico del capítulo cinco, las variables Índice de Ciberseguridad e Índice de Globalización reportan una asociación directa y significativa con respecto a las revelaciones de Ciberseguridad. Por su parte, el Índice de Gobernanza Mundial y Índice de Desarrollo Humano presentan una relación significativa e inversa.

Los hallazgos de nuestro trabajo contribuyen a la literatura que brinda una comprensión general de las tendencias y perspectivas actuales de la divulgación de la Ciberseguridad, pudiendo concluir que los gerentes deben evaluar las fuerzas políticas, sociales y económicas del país, y no solo confiar en los indicadores a nivel de la empresa que afectan la divulgación.

### 6.2. Implicaciones

Nuestros hallazgos mejoran el entendimiento sobre el estado del arte en relación al concepto de Ciberseguridad, fijando los componentes que enmarcan su actual definición. Contribuimos al campo de investigación sobre Ciberseguridad, ampliando la escasa literatura sobre divulgación de Ciberseguridad y cerrando la brecha de la inexistente literatura sobre divulgación de Ciberseguridad en América Latina.

Aportamos nuevo conocimiento a la literatura emergente sobre Ciberseguridad al proponer un novedoso instrumento de medición del alcance de la ivulgación de Ciberseguridad, denominado ´Índice de Divulgación de Ciberseguridad´. Los

reguladores, inversores y otras partes interesadas podrán utilizar nuestros resultados para evaluar el alcance de la divulgación de información sobre Ciberseguridad.

Pese a que nuestros hallazgos proporcionan evidencia empírica de que el aumento de la diversidad de género en la composición de la Junta no afecta de forma estadísticamente significativa a la divulgación de información sobre Ciberseguridad, respaldamos la necesidad de aumentar la representación de las mujeres en los directorios.

Contribuimos a la literatura previa sobre divulgación de información de Ciberseguridad, pues nuestro estudio refleja el nivel de incidencia de la composición de la Junta y de los factores institucionales a nivel país en el alcance de las revelaciones sobre Ciberseguridad. Estos resultados presentan a los legisladores y reguladores la oportunidad de mejorar sus actuaciones para incrementar los niveles de divulgación de Ciberseguridad de la región.

Los hallazgos resaltan la necesidad de incorporar el riesgo cibernético en la gestión de riesgos, así como en delegar el control de este riesgo a un comité experto dentro de la Junta. Nuestros resultados recomiendan para la ampliación de los niveles de divulgación, la creación de un Comité de Ciberseguridad con dedicación exclusiva al control del riesgo cibernético en particular y, a ser posible, no encargar esta función al Comité de Auditoría.

Finalmente, aportamos a la literatura previa sobre determinantes de la divulgación de Ciberseguridad novedosas variables a nivel macro, tales como el Índice Global de Ciberseguridad o el Índice de Gobernanza Mundial.

### 6.3. Limitaciones y futuras líneas de investigación

Este estudio tiene algunas limitaciones que podrían solventarse en futuras investigaciones. Entre ellas, cabe destacar que el índice propuesto muestra una importante inclinación hacia el contexto estadounidense, ya que gran parte de la literatura previa presenta los mayores avances en la difusión de información sobre Ciberseguridad empresarial en este ámbito geográfico. Las características específicas de este entorno podrían dificultar su generalización a otras regiones del mundo, pero dado que nuestra muestra está compuesta por empresas cotizadas en los principales índices bursátiles de

los países objeto de estudio, entendemos que nuestros hallazgos son relevantes para este tipo de empresas.

En el estudio empírico sobre la incidencia de las variables país en el alcance de la divulgación de Ciberseguridad se han tomado los índices globales. Sin embargo, futuras investigaciones podrían considerar el efecto de las dimensiones particulares de cada índice.

Nuestra investigación toma como objeto de estudio las empresas listadas de los países de mayor cotización bursátil de América Latina. No obstante, se podrían analizar empresas no cotizadas o de menor dimensión.

Se han estudiado empresas de sectores en concreto. En este sentido, futuras investigaciones podrían considerar otros sectores de actividad e, incluso, actividades específicas dentro de cada sector económico.

Finalmente, nuestra investigación centra su atención en países emergentes del ámbito latinoamericano. Sin embargo, se podrían analizar otros ámbitos geográficos, y realizar estudios comparativos entre países o regiones de países emergentes y/o desarrollados.

### 6.4. Referencias


ENISA. (2015). Definition of Cybersecurity | Gaps and overlaps in standardisation. En *European Union Agency For Network And Information Security: Vol. v1.0* (Número December).

ISO. (2018). *ISO 31000 Risk management*. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

OCDE. (2004). Directrices de la OCDE para la seguridad de sistemas y redes de información. En *Directrices de la OCDE para la seguridad de sistemas y redes de información*. https://doi.org/10.1787/9789264065819-es

SASB. (2021). *SASB Materiality Map*. https://materiality.sasb.org/