UNIVERSIDAD DE GRANADA

ANÁLISIS DE LA EDUCACIÓN EN CIBERSEGURIDAD: SITUACIÓN ACTUAL, ESTRATEGIAS Y RETOS

Alberto Beltrán Muñoz
Director: Manuel Gabriel Jiménez Torres

TESIS DOCTORAL 2020/2023
PROGRAMA DE DOCTORADO EN CRIMINOLOGÍA
ESCUELA INTERNACIONAL DE POSGRADO (UGR)

albertobeltran@correo.ugr.es

Editor: Universidad de Granada. Tesis Doctorales
Autor: Alberto Beltrán Muñoz
ISBN: 978-84-1195-357-3
URI: https://hdl.handle.net/10481/92804

Indice

Agradecimientos

Me gustaría mostrar mi más sincero agradecimiento a Manuel Gabriel Jiménez Torres, director y tutor de esta tesis, por todo el apoyo proporcionado a lo largo de estos 3 años. También a la Universidad de Granada y a la Escuela Internacional de Posgrado, institución en la que he realizado este trabajo. Dar las gracias al Centro Crímina de Elche y todo su equipo por acogerme en mi estancia de investigación. Además, agradecer especialmente a Neus y a toda mi familia por el apoyo incondicional que me han brindado a lo largo de todo este camino.

I. INTRODUCCIÓN Y JUSTIFICACIÓN

1.1. La importancia de la educación en ciberseguridad

Desde los años 90, con el uso de internet de manera masiva y la mayor interconexión de los equipos informáticos, los criminales han atacado los ordenadores para cometer delitos financieros. Este sería el caso, por ejemplo, del fraude por tarjetas de crédito, pero también han aparecido el spam, el fraude usando correos electrónicos de forma masiva, los troyanos, keyloggers y ataques de denegación de servicio (Amaro-López & Rodríguez, 2016). Es por lo anterior que inicia la idea de que, cuando un usuario utiliza internet, se le debe proveer de una seguridad para protegerse de nuevas amenazas. Posteriormente, aumenta hasta niveles de ser considerado un tema de seguridad nacional y, ya a raíz de eso, surgen estrategias orientadas a coordinación y colaboración, esfuerzos diplomáticos y hasta estrategias nacionales de ciberseguridad.

Vivimos en un mundo digital y en constante transformación en el que las identidades, las transacciones, los contenidos, etc. son datos que se pueden reproducir y transmitir fácilmente, situación aprovechada por ciberdelincuentes. De este modo, el ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor (DSN, 2019). Además, las mismas cualidades que hacen del ciberespacio un valor en sí mismo, se convierten en un arma de doble filo al poderse usar para una finalidad distinta y perjudicial. Las cualidades como anonimato y la amplificación son especialmente útiles a los ciberdelincuentes.

Como dato, alrededor de un millón de personas más se conectan a Internet cada día. Se estima que en 2022 serán unas 6.000 millones de personas las que estén conectadas a Internet frente a los 5.000 millones de 2020. Incluso se estima que en 2030 esta cifra llegue a 7.500 millones (Morgan, 2020). El crecimiento exponencial de la economía digital también ha supuesto problemas de seguridad, como la captura de contraseñas que ha llevado a robo de dinero o de usurpación de identidad (Fundación Telefónica, 2016). Existen datos preocupantes, como el hallazgo de que la mitad de los estudiantes universitarios habían sido víctimas de ciberdelitos, siendo el malware, la piratería y el phishing los delitos cibernéticos más habituales (Bigdoli et al.,2016).

“Es enorme el crecimiento que están teniendo cualitativa y cuantitativamente los incidentes de seguridad. El número de amenazas se multiplica y cada vez son más complejas y esto está creando una sensación de inseguridad que puede frenar el desarrollo tecnológico si no se toman cartas en el asunto” (Pulido & Rosell, 2017:Pg.221).

Algunas organizaciones, como el Center for Strateic &International Studies (Zhanna & Lostri, 2020), estiman que las pérdidas monetarias derivadas de la ciberdelincuencia alcanzaron en 2020 los 945.000 millones de dólares (1% del PIB mundial). A esto se sumaría el gasto mundial en ciberseguridad, que se estima en 145.000 millones de dólares en el mismo año. En total, entre las pérdidas y los gastos, supondría un lastre de 1 billón de dólares a nivel global en un solo año. La tendencia es al alza con un fuerte ascenso ya que, en 2018 (2 años antes), se encontró que el coste de la ciberdelincuencia era de 600.000 millones de dólares. Los costes de la ciberdelincuencia incluyen: el dinero robado, el daño y la destrucción de datos, la interrupción de los negocios, la pérdida de productividad, el robo de propiedad intelectual, el robo de datos personales y financieros, la malversación, la investigación forense, la restauración y la eliminación de los datos y sistemas pirateados, además del daño a la reputación de la organización o empresa (Morgan, 2020).

A todos los costes anteriores, habría que sumar otros que se encuentran más ocultos (Zhanna & Lostri, 2020): los costes de oportunidad, el tiempo y el dinero invertidos en la toma de decisiones en materia de ciberseguridad, el efecto del tiempo de inactividad cuando se producen los incidentes, la pérdida de productividad que supone ser víctima y el daño a la marca y la imagen corporativa. Además, tal y como se señala, muchos de esos costes son difíciles de cuantificar, pero deben ser tenidos en cuenta a la hora de evaluar el efecto de la ciberdelincuencia. También se estima que los costes de la ciberdelincuencia mundial crecerán un 15% al año durante los próximos cinco años, hasta alcanzar los 10,5 billones de dólares anuales en 2025, frente a los 3 billones de dólares de 2015 (Morgan, 2020).

Para tener una referencia, será más rentable que el comercio mundial de todas las principales drogas ilegales juntas. De hecho, si se midiera como un país, la ciberdelincuencia sería la tercera mayor economía del mundo después de Estados Unidos y China (Morgan, 2020). El 60% de la ciudadanía en España afirma haber sufrido un incidente de seguridad en el último semestre de 2021, un aumento de 4,4% respecto al primer semestre de 2021 (ONTSI, 2022). En cuanto al fraude en la red, el porcentaje de quienes aseguran haberlo sufrido aumentó al 71%, lo que supone una subida de 6,3% sobre el semestre anterior.

En cuanto al impacto de la pandemia, la irrupción del COVID-19 ha provocado en la ciudadanía, las instituciones públicas y las empresas un aumento de los riesgos en la ciberseguridad. Las medidas de protección, diseñadas para un crecimiento progresivo, se han visto casi desbordadas por la exposición a nuevos fenómenos como el del teletrabajo, la educación o el ocio masivos. Todos ellos, aumentaron su superficie de

exposición en un corto periodo de tiempo. Además, los ciberdelincuentes han aprovechado la pandemia para aumentar sus ataques contra infraestructuras críticas, como las de los hospitales, quienes se han visto obligados al teletrabajo y que también ha sufrido una campaña de fakenews relacionados con el COVID19 (Arteaga, 2020).

La multiplicación de lugares de trabajo domésticos, sin las adecuadas medidas corporativas de protección, ha sido otro blanco rentable para ciberataques y estafas. Los ciberataques han buscado los puntos débiles de las cadenas ampliadas de teletrabajo. Estas han aumentado la superficie de exposición de las Administraciones y empresas con multitud de aplicaciones, equipos y procedimientos de trabajo a distancia, sin la debida supervisión de los responsables de la seguridad de las organizaciones para las que trabajan (Arteaga, 2020). Esta proliferación del teletrabajo masivo desencadenó una oleada de ciberataques sobre los protocolos para acceder al control remoto de los ordenadores de trabajo. Aprovechando la confusión y las dificultades para parchear los terminales conectados remotamente, los ciberataques pasaron de algunos centenares de miles por día a rozar el millón y superarlo en países como España y Estados Unidos (Galov, 2020). Como dato, el tráfico de spam malicioso se incrementó en más del 6.000% en el mes de abril de 2020 (IBM, 2020).

En el mismo sentido, Google reconoció que había tenido que filtrar y bloquear una cantidad ingente de correos (18 millones diarios) y spam (240 millones diarios) de Gmail que trataban de suplantar la identidad de agencias, organizaciones y empresas de reparto (Huntley, 2020). En cuanto a los hábitos de los usuarios, desde el Covid, el 26% de los usuarios incrementaron sus relaciones a través de Internet, incluso con gente desconocida. También el 14% asegura confiar más en desconocidos a través de Internet, aumentando su vulnerabilidad ante delitos de fraude o abusos (ONTSI, 2022). La vulnerabilidad en el ciberespacio llega a ser calificada en la Estrategia Nacional de Ciberseguridad como uno de los principales riesgos para nuestro desarrollo como nación *"la seguridad en el ciberespacio es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental"* (DSN, 2019:Pg.10).

De acuerdo con un gran número de estudios en los últimos años, se señala que un elemento clave para ser víctima en el ciberespacio, viene determinado por el comportamiento de los propios usuarios. Por ese motivo, los esfuerzos en ciberseguridad no deben ir únicamente encaminados a la creación de nuevos programas antivirus, sino también a hacer comprender a los usuarios los riesgos que conlleva realizar determinadas actividades y enseñarles claves muy sencillas para mantener su

seguridad (Guilabert-García, 2016). Además, se señala que es fundamental para la prevención de la ciberdelincuencia el comprender el rol que desempeña el usuario. Se hace más necesario que nunca asumir el reto de crear, desarrollar y promover las competencias y aptitudes digitales para ser capaz de dotar de las herramientas necesarias a los usuarios.

También será importante, en este punto, tratar de garantizar el uso correcto y responsable de la red (García-Valcárcel et al., 2014). Por lo tanto, debemos transitar como sociedades y Estados de la aplicación de sanciones, a un sistema más funcional, adoptando medidas preventivas en el caso de los ciberdelitos (Avila, 2018). *"Nos encontramos en un momento en el que la mayoría de la sociedad comienza a ser consciente de que la tradicional manera de abordar la seguridad en el mundo digital empieza a no ser suficiente, pues no ofrece soluciones ante las nuevas situaciones"* (Fundación Telefónica, 2016:Pg.3).

Se están hallando datos que demuestran que los usuarios ya toman ciertas precauciones a la hora de compartir los datos. De este modo, estudios realizados por Telefónica (2016) muestran que muchos usuarios están adaptando sus comportamientos, por ejemplo, no accediendo desde ordenadores públicos a sus cuentas bancarias. En otros casos, algunos usuarios han llegado a suprimir ciertos comportamientos como dejar ciertos comentarios en medios sociales. Estas actitudes son una muestra de que los usuarios empiezan a tener una conciencia respecto a los datos que comparten y que se generan en su actividad en Internet.

"Los ciudadanos digitales deben estar concienciados en esta materia. Para proteger la sociedad es, por tanto, necesario que todo ciudadano o empleado de una organización pública o privada tome conciencia de los riesgos a los que se enfrenta la sociedad en su conjunto" (Pulido & Rosell, 2017: Pg.220). Más allá de las diferencias, está claro que todos los usuarios deberán tener un mínimo conocimiento de los riesgos que suponen las amenazas, pero no solo eso, sino que también tienen que saber los medios existentes para hacerles frente. La tendencia actual se asemeja a una carrera armamentística en lo que respecta a atacar y defender activos en línea, alcanzando el éxito aquellos que tengan y conozcan las herramientas y técnicas más actualizadas (Thackray et al.,2016).

Los programas de prevención para el uso seguro y responsable de Internet son fundamentales y necesarios (Fernández-Montalvo et al., 2015). El objetivo de las instituciones, por lo tanto, será el de dar formación y empoderar a esta población para poder tener una capacidad crítica y autónoma de enfrentar las distintas situaciones en

Internet y los peligros que alberga. Paralelamente, las personas y organizaciones han ido adquiriendo mayor conciencia de esta situación a medida que el número de actividades que se realizan de forma digital ha ido aumentando, y sobre todo, han ido adquiriendo una naturaleza más económica. Por arrojar algunos datos, ya en 2015, un 43% de los internautas hacen sus compras por Internet y un 96% de los trámites que las empresas realizan con la Administración se llevan a cabo utilizando el formato electrónico (Fundación Telefónica, 2016).

Mientras que los datos revelan que el acceso a internet es cada vez más precoz, algunos autores como Gamito et al. (2020), señalan que los recursos que se están poniendo y las iniciativas para alcanzar esos objetivos no responden a esas necesidades. Algunos de esos proyectos sobre el uso seguro de internet se están implementando en centros y entidades educativas, pero en gran parte lo hacen sobre alumnado de educación secundaria, descuidando a los más pequeños. Se vuelve, por lo tanto, un hecho de especial atención mantener una observación constante sobre ese aumento del uso de internet en niños cada vez más pequeños (INE, 2018). *"La ciudadanía del siglo XXI necesita de nuevas alfabetizaciones y estrategias para el empoderamiento en línea. Es por ello que la escuela debe afrontar los nuevos retos del contexto digital y trabajar el uso seguro de Internet en el aula desde edades tempranas y otorgando un papel activo al alumnado*" (Gamito et al., 2020: Pg.233).

Nos encontraríamos con una dualidad en cuanto al uso, o mejor dicho, mal uso de las redes sociales, ya que su diseño y fácil acceso, permiten a los menores acceder a ellas y usarlas de un modo sencillo. Al mismo tiempo, no establecen unos límites bien definidos para su uso y, en gran medida, aunque tienen capacidad de emplearla por su sencillez, no tienen la preparación ni conocimientos necesarios para manejarlas de un modo seguro (Vanderhoven et al., 2014). En algunos estudios (Drew, 2020), las víctimas estudiadas todavía desconocen los tipos de estrategias de autoprotección que deberían usar, o existen otros factores que limitan las herramientas y comportamientos de prevención.

Para no verse perjudicado por estos ciberdelitos, la importancia de una educación para protegerse de ellos es cada vez más crítica. Sin embargo, la educación existente hasta ahora en ciberseguridad no ha sido suficiente para hacer frente a los crecientes ciberdelitos (Kim et al., 2016). Sarre, Yui-Chung & Chang (2018) también concluyen que la educación es una de las mejores respuestas al ciberdelito, específicamente la educación de aquellos que son vulnerables a la victimización. La relevancia del ámbito va en aumento, como señala un estudio bibliométrico sobre educación y ciberseguridad (Valencia-Arias, 2020). Encontraron que del año 2001 al 2019 el interés por investigar

en este estudio aumentó notablemente, dando cuenta de preocupación por los riesgos a los cuales nos enfrentamos. También hallaron que hay pocos estudios con metodologías novedosas que se orienten hacia la enseñanza de soluciones prácticas de los riesgos en el tratamiento de la ciberseguridad.

1.2. Objeto de estudio, hipótesis y pregunta de investigación

Las hipótesis planteadas para esta investigación son las siguientes:

- H1: La educación en nociones básicas de ciberseguridad y ciberamenazas es un elemento clave para mejorar la protección de las potenciales víctimas.
- H2: La educación en ciberseguridad actualmente estaría descompensada, debido a que se habría centrado más en aquella dirigida a un nivel avanzado, para personal cualificado o que vaya a tener un desempeño en el ámbito, atendiendo a individuos que tienen competencias en ciberseguridad o que necesitan de conocimientos técnicos para su trabajo. Sin embargo, habría tenido un menor impacto aquella enfocada a explorar la educación básica en la población en general (población no-técnica). Consecuencia de ello, sería que la amplitud de la oferta educativa en ciberseguridad se configura en especializaciones, másteres, y cursos para personas en puestos clave y no a la ciudadanía, a un a nivel básico, para poder prevenir la cibervictimización.
- H3: Las víctimas presentan desconocimiento de elementos claves de ciberseguridad, además de una menor percepción de la amenaza frente a otros delitos, lo que las hace más vulnerables; Por lo tanto, los que han sido víctimas, tendrán alta correlación con vulnerabilidad y relación inversa con conocimientos en ciberseguridad. Las personas que tengan altas puntuaciones en conocimientos, tendrán menor vulnerabilidad y será más probable que no sean víctimas de ciberdelitos frente a los que tienen bajas puntuaciones en conocimientos.

A continuación, se enumeran la pregunta general y las 4 preguntas específicas planteadas para esta investigación:

Pregunta general:

- ¿Se está consiguiendo prevenir a la población general ante la ciberdelincuencia mediante la educación en ciberseguridad?

Preguntas específicas:

1. ¿Cuál es la situación de la educación en ciberseguridad orientada a la población en general?
2. ¿Cómo se está educando en ciberseguridad, qué técnicas didácticas y proyectos educativos se están poniendo en marcha?
3. ¿Las víctimas tienen conocimientos sobre la ciberdelincuencia y nociones de ciberseguridad?
4. ¿Cómo se podría mejorar la estrategia de educación en ciberseguridad?

1.3. Objetivos

Objetivo general:

-Analizar las estrategias de educación en ciberseguridad dirigidas a la población general.

Objetivos específicos:

1. -Explorar los distintos proyectos implementados y los resultados obtenidos, atendiendo a la diferencia entre educación a nivel básico y avanzado.
2. -Realizar un análisis descriptivo mediante la recopilación de bibliografía y análisis sistemático, analizar la evolución de la cuestión objeto de estudio, los principales autores, teorías y estudios realizados.
3. -Recopilación y análisis de la literatura reciente sobre la educación en ciberseguridad y el análisis bibliométrico de los mismos.
4. -Identificar las estrategias y técnicas didácticas para la educación en ciberseguridad.
5. -Determinar las diferencias de conocimientos en ciberseguridad entre personas que han sido víctimas de ciberdelitos y personas que no: se utilizarán métodos de investigación correlacional para investigar las diferencias entre población víctima de ciberdelitos y los no-víctimas.
6. -Obtener información sobre la capacidad y conocimientos de la población general en ciberseguridad.

1.4. Metodología

En cuanto a los métodos empleados, se ha decidido usar diversos medios y técnicas, con un enfoque interdisciplinar. Se han puesto en marcha diseños: no experimentales, cualitativos y cuantitativos. El diseño está dividido en 4 líneas, organizadas en fases y cada una con una técnica distinta:

- Primera línea: Análisis Bibliométrico.

Análisis de tipo documental y longitudinal del periodo 2001 a 2020, utilizando como fuente documental artículos procedentes de Web of Science y Scopus. Para este análisis bibliométrico se han empleado las herramientas digitales bibliometrix, Vosviewer y el propio analizador de resultados de las bases de datos. El método permite realizar un mapeo de la bibliografía y un análisis de las tendencias, evolución en el tiempo, áreas temáticas y autores más relevantes. Además, la técnica permite expresar los datos hallados de un modo gráfico mediante las herramientas usadas.

- Segunda línea: estado del arte y revisión sistemática.

Posteriormente a una recopilación de material (artículos, bibliografía, información institucional, proyectos implantados, etc.), se ha procedido a realizar una revisión de la literatura de artículos, conferencias, los proyectos desarrollados, investigaciones, instituciones, iniciativas, etc. además de datos y análisis estadístico de las variables objeto de estudio. En primer lugar, con un carácter más amplio y general: Educación en ciberseguridad y ciberdelincuencia. En segundo lugar, un estudio bibliográfico más específico sobre la capacidad de prevención de la ciberdelincuencia mediante la educación en población no-técnica. Se incluyeron aquellos estudios relevantes en la materia, proyectos e informes de instituciones.

En tercer lugar, se ha puesto en marcha dentro de esta línea una revisión sistemática, que consiste en un procedimiento integrador de artículos de investigación. Es retroactivo, ya que hace referencia a un tiempo pasado (hasta Junio de 2022) y cualitativo, puesto que sintetiza los resultados de múltiples investigaciones para un estudio exhaustivo. También arroja datos y resultados cuantitativos, con información sobre resultados de técnicas y tendencias. Esta revisión permitió obtener una radiografía de la situación actual en relación con el problema, identificando las principales técnicas y sus resultados.

-Tercera línea: Consulta a jueces expertos.

Análisis cualitativo mediante consulta a Jueces expertos sobre la materia objeto de estudio. Se empleó un cuestionario con preguntas estandarizadas para analizar las

respuestas y la elaboración final de un informe de resultados. Las preguntas referían a cuestiones en torno a la vulnerabilidad de la sociedad general ante la ciberdelincuencia, el rol de las ciencias sociales y el papel de la educación en ciberseguridad para prevenirlo. El número objetivo de expertos a consultar se fijó en 15, aunque finalmente participaron 10. Se incluyó a Jueces expertos en la materia de la ciberseguridad, miembros de instituciones y organismos con competencias en el área, investigadores, personal técnico, etc. que pudieron aportar conocimientos desde distintos enfoques sobre la cuestión objeto de estudio.

- Cuarta línea: Estudio empírico.

Técnica de investigación correlacional, de encuesta y transversal (en un único momento). Se desarrolló y aplicó un instrumento consistente en un cuestionario virtual para evaluar la capacidad del individuo para proteger dispositivos, evaluar conocimientos en ciberseguridad y ciberdelincuencia, medir el nivel de vulnerabilidad y educación, además de indicar si ha sido o no víctima de ciberdelitos.

El instrumento se basó en la herramienta “Google formularios” para poder diseñar, crear, compartir y tomar datos de forma telemática, sencilla, rápida y ágil, así como poder automatizar el proceso. Esta herramienta permite enviar un enlace por Whatsapp, redes sociales, correo electrónico, etc. y abrir desde cualquier dispositivo móvil, ordenador o Tablet, de forma rápida y sin tener que iniciar sesión ni darse de alta en ninguna plataforma. También el ahorro de material y tener en cuenta el medioambiente (sin consumo innecesario de papel)

Los datos son enviados inmediatamente a la cuenta de Google y son descargables en distintos formatos (Excel y gráficas). Una vez recogidos los datos, se procedió a su análisis mediante SPSS para su posterior interpretación y valoración.

II. MARCO TEÓRICO Y REVISIÓN DE LA LITERATURA

1. La ciberdelincuencia

La cibercriminalidad o ciberdelincuencia, representa una de las amenazas más extendidas y generalizadas, se materializa de forma continua y victimiza cada vez a miles de instituciones, empresas y ciudadanos. El término hace referencia al *"conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo"* (DSN, 2019: Pg. 25).

Es de especial transcendencia la evolución que ha sufrido el fenómeno de la cibedelincuencia en relación a la delincuencia general, ya que 1 de cada seis crímenes registrados en España (15,6% del total) en todo el 2021 son ciberdelitos. Dentro de ellos, el malware y el phishing ha sido una de las prácticas preferidas por los delincuentes. (López et al., 2021). Aunque la naturaleza de la ciberdelincuencia evolucionará a la par que la tecnología, en términos generales, se puede hacer una primera distinción entre 2 categorías (Clough, 2011; Clough, 2015):

1. Delitos en los que el ordenador o la red informática es el objetivo de la actividad delictiva, por ejemplo, la piratería informática, los programas maliciosos y los ataques de denegación de servicio.

2. Delitos existentes en los que el ordenador es una herramienta utilizada para cometer el delito; por ejemplo, la pornografía infantil, el ciberacoso, la infracción de los derechos de autor, el fraude, etc.

Por su parte, la Estrategia de Seguridad Nacional de 2019 diferencia entre las ciberamenazas y las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas (DSN, 2019). Según este documento, abarcan un amplio abanico de acciones que se caracterizan por su diversidad, tanto en lo que concierne a las capacidades como a las motivaciones, convirtiéndose en un problema de seguridad ciudadana de primer orden y representando una de las amenazas más extendidas y generalizadas. Además, victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. En cuanto a los datos estadísticos de las ciberamenazas, la ciberdelincuencia, la magnitud del impacto, la cibervictimización, los tipos y modos en que se muestra, es a través del Estudio sobre la Cibercriminalidad en

España (Cerceda et al., 2019) que podemos obtener una radiografía de todos esos aspectos. En estos estudios se detalla a nivel estadístico cómo ha ido evolucionando y en qué modo.

Como datos a destacar en este informe del año 2021 (López et al., 2021):

- 2021, se han conocido un total de 305.477 hechos, lo que supone un 6,1% más con respecto al año anterior. De esta cifra, el 87,4 % corresponde a fraudes informáticos (estafas) y el 5,7% a amenazas y coacciones
- Las fuerzas y cuerpos de seguridad registraron, en 2020, 287.963 hechos delictivos relacionados con TIC, lo que supone un incremento del 32% desde el 2019.
- Si en 2016 había 92.000 hechos detectados (4,6 por ciento del total de los delitos) , en 2020 la cifra ascendía a 288.000 denunciados, un (16,3% del total).
- Los fraudes informáticos (estafas) representan el 89,6% del total de ciberdelitos, con un total de 257.907 casos, seguidos de las ciberamenazas y coacciones cometidas a través de Internet, que alcanzaron los 14.066 casos (4,9% del total).

En cuanto a la distribución de la Cibercriminalidad desde el punto de vista geográfico, se sitúa a Madrid, Cataluña, Andalucía y Comunitat Valenciana entre las Comunidades Autónomas que concentran más ciberdelitos (López et al., 2021). A nivel provincial, se encuentran a la cabeza del ránking: Madrid, Barcelona, Valencia, Sevilla, Alacant, Bizkaia y Málaga. Las formas de ciberdelincuencia que suponen mayores costes a nivel económico son: el espionaje económico, el robo de propiedad intelectual, los delitos financieros y el ransomware (Zhanna & Lostri, 2020). De hecho, se estima que el robo de propiedad intelectual y los delitos financieros representan dos tercios de las pérdidas monetarias y suponen la mayor amenaza para las empresas. Sin embargo, detrás de la cifra principal se esconden otros costes menos obvios que pagan las empresas y los consumidores de diferentes maneras (Zhanna & Lostri, 2020).

1.1. Las formas de ciberdelincuencia que afectan a la población general

Aunque todas las formas de ciberdelincuencia afectan a la sociedad en su conjunto, ya sea directa o indirectamente, cuando hablamos de educación en ciberseguridad y ciberdelincuencia orientada a la población general, se entiende que es de especial transcendencia aquellos tipos de ciberdelincuencia que les afectan directamente.

Quedarían fuera aquellas formas de ciberdelincuenicia orientadas a instituciones públicas, infraestructuras críticas, grandes empresas, etc. En este punto, se debe puntualizar que la ciudadanía, como población general, también desempeñarán puestos de trabajo en organizaciones y empresas. Esta cualidad de la ciudadanía como fuerza de trabajo, hace que la educación general también repercuta en la debilidad o fortaleza de todo el tejido empresarial e industrial para poder protegerse de la ciberdelincuencia en sus distintas formas.

En un estudio realizado por Telefónica (2016), encontraron que muchos usuarios no son capaces de identificar cuáles son los peligros y, por tanto, no saben cómo enfrentarse a ellos. Este hecho es de especial relevancia ya que el conocer cómo el malware llega hasta nuestros sistemas condicionará el comportamiento de los usuarios: no seguir cadenas de correos, utilizar software de fuentes seguras, tener cuidado al introducir USB de terceras personas, etc. También falta actualización de conceptos e información, puesto que los usuarios desconocen cómo han ido evolucionando en el tiempo los ciberataques. Un ejemplo de ello, es el objetivo de los ciberdelincuentes de acceder a los recursos del usuario y aprovechar el poder de procesamiento de sus dispositivos, o también el de acceder a su sistema para que actúe como un zombi dentro de una botnet y poder ejecutar ataques masivos.

Por otra parte, Vanderhoven et al. (2014), plantea 3 tipos de peligro en internet muy similares: contenido, contacto y comercial. El de contenido se referiría a los mensajes que puedan ser de odio o que puedan perjudicar de un modo negativo nuestra niñez y juventud. El segundo, de contacto, haría referencia al uso de medios de coumunicación como mensajería instantánea, chats, RRSS, y en donde pueden darse casos como ciberbullying, acoso en línea, acoso sexual, sustracción de datos personales, phishing, estafa, grooming, etc. Finalmente, el comercial, se referiría al empleo de información y datos personales, como fotografías personales, e incluso la realización de seguimientos a menores *"mensajes de odio y mensajes diversos, que podrían influenciar negativamente a nuestra niñez y juventud, ciberbulling, acoso sexual, riesgos de privacidad, donde los datos y fotos personales puedes ser sustraídos, uso indebido de la información y fotos personales y uso de los datos para hacer seguimiento del comportamiento de la niñez y la adolescencia"* (Vanderhoven et al., 2014: Pg. 124).

En cuanto a los delitos que amenazan a uno de los colectivos más vulnerables, los niños, habría algunos riesgos más habituales frente a la población adulta. Según Lievens (2015) existen tres tipos de riesgos online para los niños: los riesgos de contenido, en los que el niño es un receptor; los riesgos de contacto, en los que es un participante; y los riesgos de conducta, donde el niño es un actor que incumple

determinadas normas de comportamiento o incluso son conductas ilegales. Entre los mayores peligros para los menores de edad que se encuentran en las redes sociales tenemos el ciberbullying, sexting y el grooming (Astorga-Aguilar & Schmidt-Fonseca, 2019). Destacar que, según estos autores, es la educación en ciberseguridad lo que les defiende ante estos riesgos, y su ausencia, lo que les hace más vulnerables.

Ciberbullying

En español “Ciber-Acoso” es el traslado de un fenómeno, ampliamente conocido en criminología y las ciencias sociales, al mundo del ciberespacio. Como consecuencia de este traslado, se ha roto el espacio físico, el tiempo y la interacción directa entre los agentes implicados, pasando a ser un fenómeno asíncrono y deslocalizado. Es más, se potencia debido a factores como la sensación de anonimato que permite internet, el carácter masivo que pueda tener y la diversidad de medios a través de los que se puede reproducir. Como se afirma en Astorga-Aguilar & Schmidt-Fonseca (2019) las formas de delito están cambiando ya se hace necesario que víctima y el criminal se encuentren al mismo tiempo en el mismo espacio virtual.

Algunos ejemplos serían aquellos casos en los que se divulga información falsa para dañar a alguien, difundirla por redes sociales, realizar montajes y enviarlos a personas del entorno, etc. Es un fenómeno especialmente dañino por la rapidez con la que se puede producir la difusión. Como consecuencias, señalar: problemas emocionales, académicos y de comportamiento, hasta baja autoestima, depresión e incluso intentos suicidas u homicidas. Según García-Maldonado et al. (2011), se estima que uno de cada cuatro estudiantes está involucrado en este problema, ya sea como cibervíctima, ciberagresor, o en cualquiera de los 2 roles. Es más, afirma que el peligro de sufrir ciberbullying frente al bullying tradicional es el doble.

Grooming

Según Del Fresno et al. (2016: Pg.257), las redes sociales son “*plataformas tecnológicas en línea que se centran, síncrona y asíncronamente, en las interacciones humanas de manera local y global*”. Internet y su estructura permiten el desarrollo y uso de estas herramientas con gran impulso, las cuales han sido diseñadas para interaccionar con otros usuarios y permitir la comunicación entre ellos. Existe un gran número de redes sociales, en algunos casos donde las fotografías y el audiovisual son el principal elemento, en otras el texto, y en otras la combinación de distintos formatos. En todo caso, su utilización en la población es exponencial y masivo. Una de las formas delictivas que más ha aprovechado las redes para proliferar es el Grooming.

El Grooming se refiere a aquel conjunto de estrategias que una persona adulta pone en marcha para poder ganarse la confianza de un menor de edad. Esta estrategia se realiza mediante internet, ya que permite más posibilidades de anonimato, y también un empleo de un control progresivo sobre la víctima hasta alcanzar la fase final de abuso sexual (Arab & Diaz, 2015). Es frecuente el uso de perfiles falsos para poder acercarse a las víctimas menores de edad y conseguir así ganarse su confianza (Astorga-Aguilar & Schmidt-Fonseca, 2019). Un ejemplo, sería hacerse pasar por una menor de edad con complejos que contacta con la víctima, le expone su caso y sus complejos, y luego le pide fotos de ella para ver cómo es. Una vez conseguido el material, se emplea como chantaje para obtener más material, agravando el problema y los chantajes.

Las etapas que se distinguen son:

- Amistad: En la que el delincuente se hace pasar por una persona joven para ganarse la confianza de la víctima. Es también una fase de obtención de datos.
- Engaño: Se finge la vinculación emocional, enamoramiento, complejos, etc. para conseguir material de la víctima (fotografías, videos, etc.)
- Chantaje: Se producen amenazas empleando los materiales previos, principalmente de divulgarlos, para poder seguir obteniendo nuevos materiales.

Malware

El malware permite la entrada de los ciberdelincuentes a la red privada a través de nuestros dispositivos personales, ya que cada vez tenemos más equipos dependientes de esta red en el mismo entorno virtual. En el segundo semestre de 2021 se produjo un porcentaje del 51,5% en el número de ordenadores infectados con malware, aunque con un descenso del 7,6% (López et al., 2021). Dentro del malware, las categorías que tienen mayor peligrosidad son los troyanos, el ramsomware y rogueware. Un 65% de los ordenadores y un 58% de los dispositivos Android infectados sufrieron ataques por malware de alta peligrosidad. En el caso de los troyanos, un 33,3% de los ordenadores analizados contenía troyanos, por lo que ha disminuido respecto al semestre anterior.

Principales formas de Malware:

Virus informático: es un malware diseñado para alterar el correcto funcionamiento de un dispositivo. Infecta los ficheros de un ordenador mediante un código malicioso y oculto, pero necesita la intervención del usuario para ser ejecutado. Una vez que tiene el control, se propaga a otros equipos (Caro & Moreno, 2022).

Gusanos informáticos: Tiene como principal objetivo propagarse por el sistema, pero la principal diferencia es que los gusanos no necesitan de la intervención del usuario

para infectar a un equipo (Hornetsecurity, 2020). Son capaces de autorreplicarse y expandirse a través de las redes. En la actualidad, el principal empleo de los gusanos es crear las llamadas botnets, en donde una red de ordenadores “zombies” actúan simultáneamente cuando el ciberdelincuente quiera.

Ransomware: es un malware que infecta distintos tipos de dispositivos y restringe su acceso a los archivos, a menudo amenazando con la destrucción permanente de los datos a menos que se pague un rescate. Ha alcanzado proporciones epidémicas en todo el mundo y es uno de los métodos de ataque preferido por los ciberdelincuentes. Según un informe de Cybersecurity Ventures (Morgan, 2020), se calculó que el aumento de 2015 a 2017 aumentó 15 veces, pasando de 325 a 5.000 millones de dólares. La estimación de 2021 a nivel global alcanzan los 20.000 millones de dólares, lo que supone 57 veces más que en 2015. Un modo de evadir este tipo de cibedelitos consiste en generar copias de seguridad periódicas para evitar la pérdida de la información.

Rogueware: consiste en una aplicación que intenta semejarse a otra, por apariencia o nombre, para engañar y timar a los usuarios (López et al., 2021). En algunos casos, incluso simula ser un antivirus u otro tipo de herramienta de seguridad. Este malware lanza una alerta, indicando algún riesgo en el equipo que requiere la atención del usuario. Se trata de un aviso falso, que en caso de querer solucionarlo ejecutando el rogueware que simula ser un antimalware, procederá a instalar software malicioso en el sistema. (Soto, 2021)

Rootkit: malware que proporciona al atacante los privilegios de administrador en el sistema que infecta, una vez conseguido, puede alterar el comportamiento habitual de un dispositivo (Caro & Moreno, 2022).

Troyano: Los troyano funcionan pasando desapercibido para conseguir emprender acciones sin que el usuario se percate. Se infiltra en el dispositivo y puede atacar de forma encubierta (Caro & Moreno, 2022). En algunos casos lo consigue haciéndose pasar por algún software y se usa para crear una puerta trasera que proporcione acceso al atacante. Gracias a los troyanos, los ciberdelincuentes pueden luego robar información o para instalar otros tipos de malware.

Spyware: Es un tipo de malware que trabaja de forma encubierta, recaba información sobre los dispositivos o redes, y una vez obtenida la información, la envía al atacante (Soto, 2021). Además, trata de ocultar su rastro con la finalidad de que el usuario no detecte el spyware y actúe con normalidad. Gracias a este tipo de malware, los ciberdelincuentes pueden monitorizar el dispositivo, y a su vez recopilar todos datos,

archivos, listado de programas instalados, historial de navegación, etc. (Caro & Moreno, 2022).

Keylogger: es un tipo de malware diseñado para grabar todas las pulsaciones de teclas del teclado. Puede ser un dispositivo físico o virtual. Almacena la información recopilada y se la envía al ciberdelincuente. Su principal función es obtener credenciales, passwords, información confidencial o datos financieros (Hornetsecurity, 2020). También puede ir acompañado de un sistema en el que se crea una captura de pantalla con cada clic, por lo que también serían vulnerables los teclados web en los que se deben seleccionar los números con el ratón.

Sexting

Este término hace referencia a la práctica de compartir fotografías, vídeos u otro contenido de tipo sexual a otras personas empleando medios digitales, teléfonos, mensajería instantánea, etc. (Arab & Díaz, 2015) Supone un gran riesgo porque las imágenes pueden ser publicadas o mostradas a terceras personas sin permiso del emisor. La consecuencia posible del sexting es que se pierde el control de las fotografías, que una vez divulgadas, no pueden ser eliminadas de la red por el emisor. Supone un ataque directo contra la intimidad, y un delito de mayor calado en el caso de que haya menores implicados. Las consecuencias pueden ser muy diversas, desde psicológicas (pudiendo llegar al suicidio) como otras de tipo social (necesidad de traslado de centro escolar, entorno, problemas familiares, etc.).

Fraude informático

Los fraudes informáticos (estafas) representan el 89,6% del total de ciberdelitos, con un total de 257.907 casos, seguidos de las ciberamenazas y coacciones cometidas a través de Internet, que alcanzaron los 14.066 casos (4,9% del total) (López et al., 2021). El fraude en internet es más efectivo cuanta más información conocen los ciberdelincuentes sobre las potenciales víctimas, aunque también tiene un gran peso la confianza de la víctima. En la última década, el fraude informático ha recibido un creciente interés de parte de la doctrina penal. Esta forma de ciberdelito constituye el protagonista indiscutido de la cibercriminalidad y ha continuado siendo el centro de los ciberdelitos, principalmente por el impacto económico que presenta y la frecuencia práctica que la caracteriza. Además, ha resultado enormemente potenciada por el auge del comercio electrónico (Mayer & Oliver, 2020).

En cuanto a la legislación, es en el artículo 248.2 del Código Penal donde podemos encontrar su definición: "*el delito de estafa informática o fraude informático, en el que se sustituye la exigencia de engaño personal por la manipulación informática, se define*

como la alteración de los elementos físicos que permiten la programación de un ordenador, o por la introducción de datos falsos" (Ley Orgánica 10/1995).

Suplantación de identidad (Fraude a empresarios y autónomos)

Este tipo de delitos no lo es tanto de cara a la población general, sin embargo, es un tipo de delito que puede afectar a muchas empresas y negocios. Teniendo en cuenta que España es un país que alberga numerosas PYMES es un problema que puede afectar a un gran número de personas de forma indirecta. Además, puede poner en riesgo muchos negocios perjudicando a todavía a más población, por ejemplo, si obliga al cierre de un negocio que no pueda afrontar la pérdida económica. Esta suplantación de identidad consiste en el envío de correo electrónico personalizado, tras un análisis exhaustivo de la víctima, para que realice una transferencia, modifique la cuenta de pago de la factura de un proveedor, etc. a una cuenta controlada por los delincuentes. (López et al., 2021).

2.2. El Phishing

El phishing es un ciberdelito en el que los atacantes suelen hacerse pasar por una fuente de confianza. Los atacantes normalmente envían un correo electrónico que contiene un enlace que les permite robar la información personal del receptor. En algunos países como Estados Unidos, el phishing es el número uno de los ciberdelitos por número de víctimas (Abdelhamid, 2020) y está usualmente vinculado con el concepto de hurto o robo de identidad (identity theft). A pesar de la investigación y los planes para aumentar la conciencia y las capacidades de defensa de los usuarios ante estos ataques, el éxito de estos ataques sigue aumentando a un ritmo elevado. Según Mayer & Oliver (2020) el phishing implica una obtención fraudulenta de datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito orientada a ejecutar transacciones electrónicas a favor del agente o de terceros.

Por su parte, el Informe de ciberseguridad de 2021 (López et al., 2021), consiste principalmente en la recepción por parte de la víctima de un correo electrónico destinado a engañarla y que comparta, normalmente, a través de un enlace a una web fraudulenta, credenciales, datos personales, números de cuenta bancaria, datos de tarjetas de crédito o cualquier otro dato confidencial. Terminológicamente, el phishing evoca la «pesca» de información o el intento de que las eventuales víctimas «muerdan el anzuelo» y proporcionen los datos que busca el cibedelincuente (Mayer & Oliver, 2020). Se encuentra en plena expansión, tal y como señala el informe de Microsoft, que calificó 2019 como un año de evolución del phishing. En ese año, los atacantes realizaron innovaciones tanto en tácticas técnicas como sociales (Abdelhamid, 2020). Mientras que

empresas, expertos e investigadores siguen desarrollando nuevos métodos para detectar los ataques de phishing y mejorar la resistencia a ser víctima del phishing, los atacantes avanzan y mejorando los ataques de phishing a un ritmo mayor y más exitoso ritmo (Abdelhamid, 2020).

2. La ciberseguridad

Según el diccionario del National Initiative for Cybersecurity Careers and Studies, la ciberseguridad se define como "*actividad o proceso, habilidad/capacidad o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso no autorizado, modificación o explotación*" (NICCS, 2019). Otra definición es la aportada por el Observatorio Nacional para la Seguridad de la Información y la Ciberseguridad: "*la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de la tecnología de la información o seguridad de la información electrónica*" (OSIC, 2019). Por lo tanto, la ciberseguridad es la práctica de proteger los sistemas, la información digital y los dispositivos ante ciberataques. Las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones.

En cuanto al Ciberespacio, es un concepto más amplio que el propio Internet, ya que se entiende como aquella realidad simulada implementada dentro de los ordenadores y redes digitales existentes a nivel mundial (Alarcón, 2017). El ciberespacio se define en la Estrategia de Ciberseguridad Nacional (DSN, 2019) como el dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, las redes y los sistemas de información y de telecomunicaciones. Esta Estrategia desarrolla el concepto indicando que el ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. Tiene como particularidad una ausencia de soberanía, débil jurisdicción, facilidad de acceso y dificultad de atribución de las acciones. Por todo ello, crea un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad.

El ciberespacio también posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Pero, por otro lado, el ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo. En 2004, el mercado mundial de la ciberseguridad tenía un valor de 3.500 millones de dólares, y en 2017 superaba los 120.000 millones. Por lo tanto, creció aproximadamente 35 veces durante ese período de apenas 13 años. A

pesar de todo, los datos indican que es insuficiente, por ejemplo, en Estados Unidos, la mayoría de las organizaciones estadounidenses están aumentando de forma lineal o plana los presupuestos, pero los ciberataques crecen de forma exponencial (Morgan, 2020).

2.1. Concienciación en ciberseguridad

Cuando se habla de educación en ciberseguridad y ciberdelincuencia, no se habla solamente de la transmisión de conocimiento a las personas que la reciben. Para que la educación encuentre un encaje correcto y sea aplicada por parte de los usuarios de internet, es necesario generar un nivel mínimo de concienciación. Es precisamente esta la que genera unos niveles de atención y motivación de cara a la ciberseguridad y las ciberamenazas que permitirá absorber y asimilar mejor los contenidos. También es de especial importancia que, una vez que los contenidos se han adquirido, sean interiorizados y aplicados, de lo contrario, no valdría de nada tener ese aprendizaje. Un claro ejemplo sería conocer la mejor forma de crear contraseñas seguras, pero luego seguir usando unas fáciles y breves que no sean seguras. Se señala desde la Estrategia de Ciberseguridad para la Unión Europea que "*los usuarios finales contribuyen de forma decisiva a garantizar la seguridad de las redes y los sistemas de información: es preciso que sean conscientes de los riesgos que corren en línea y sean capaces de adoptar medidas sencillas para protegerse de ellos*" (Comisión Europea, 2013: Pg.8).

En esta línea, según Drew & Farrell (2018), la educación para prevenir la cibedelincuencia sería limitada en su eficacia, ya que hace hincapié solamente en aumentar el conocimiento y éste a menudo no se traduce en el uso real de los comportamientos y estrategias de prevención. De ello, se desprende la importancia de que toda formación y transmisión de conocimiento debe ir acompañado siempre de concienciación, conformando los elementos indispensables de la educación como idea general. El caso contrario, concienciar sin enseñar los conocimientos necesarios, tampoco tendría sentido alguno, ya que no sería fructífero. Sobre la autoeficacia contra los ciberdelitos, se encontró que es un requisito importante para que los participantes tomen el control de su protección (Drew & Farrell, 2018). Inevitablemente, conducirá a una disminución en el miedo a la ciberdelincuencia.

Ya en 2013, La Escuela de Altos Estudios de la Defensa (2013), expresaba la necesidad de crear una conciencia nacional de ciberseguridad debido a los cambios que se estaban produciendo en el ciberespacio. Actualmente, los usuarios perciben la seguridad principalmente como una interrupción o molestia en sus tareas. Es necesario que la seguridad no sea percibida como una molestia, sino como un servicio. Es por ello

que se hace necesario comunicar los objetivos y métodos de seguridad de forma atractiva y comprensible, desarrollando un sentimiento de seguridad el mundo digital (Benenson et al., 2011). Para entender las necesidades y vulnerabilidades de la población sobre la que se debe intervenir, se hace relevante conocer las medidas de protección adoptadas y rechazadas por la población, así como su motivación para aceptarlas o prescindir de ellas.

Los motivos por los que se renuncia a poner en marcha medidas de seguridad están relacionados, principalmente, con la percepción de que no son necesarias, pero también con el desconocimiento. Por ejemplo, se observó que está perdiendo popularidad el uso de antivirus debido a la confianza que les aporta a las personas usuarias la capa de seguridad del sistema operativo (ONTSI, 2022). En cuanto a las medidas y actitudes, los cambios no están siendo interiorizadas por los usuarios, con falta de medidas activas como cambios en los hábitos. La excepción más reseñable de comportamiento activo con respecto a la seguridad es desconectar o tapar la webcam, hábito que llega al 43 % de los internautas (Fundación Telefónica, 2016)

A todo lo anterior, se suma que existe una distorsión de las medidas implementadas por los propios usuarios. En un estudio donde se analizaron los dispositivos de los participantes con un software para contrastar la autopercepción de protección con el estado real de las medidas de seguridad, se encontraron incoherencias entre las opiniones recogidas y los datos arrojados por los dispositivos (ONTSI, 2022). Como dato, el 56% de las personas que se percibían como totalmente preparadas en ciberseguridad, resultaron tener sus dispositivos infectados. De este modo, autopercepción de eficacia y conocimientos reales pueden no estar vinculados a efectos reales, por lo que, a la hora de educar, se debe hacer un esfuerzo en tratar de determinar hasta qué punto la persona tiene esa capacidad real de protegerse y no solo percibirse como capaz.

Sobre la percepción de eficacia, existen estudios que lo relacionan con los conocimientos en ciberseguridad. En Wash & Rader (2015) se encontró que los usuarios que tienen los conocimientos para mitigar la victimización por ciberdelincuencia son, al mismo tiempo, más propensos a participar en comportamientos de riesgo. Una posible explicación sería el hecho de que esa percepción de autoeficacia les provoca falta de miedo y, por lo tanto, una conducta más imprudente (Bigdoli et al.,2016). Tal y como se ha mostrado por medio de la investigación, el miedo a la victimización es un factor clave a la hora de que las potenciales víctimas pongan en marcha la autoprotección (Chadee & Ng Ying, 2013).

También existen otros factores implicados como la percepción de la incidencia en el entorno. Rader et al. (2012) realizaron una encuesta a 301 estudiantes universitarios para ver cómo los usuarios no-expertos usan las historias que escuchan de otros para tomar decisiones de seguridad. Surgieron seis tipos diferentes de historias: tener problemas con una PC debido a un problema de seguridad; piratería, virus o robo (a través de phishing, dinero o personal); robo de datos personales, spam y otras historias que no encajaban en una categoría en particular. Muchos encuestados mencionaron haber escuchado historias de familiares o amigos y ello, a su vez, condujo a un cambio en los comportamientos de ciberseguridad de más de la mitad de los encuestados. Las historias autobiográficas, las historias contadas por personas con más conocimientos y las historias que producen emociones (particularmente ansiedad e ira) tenían más probabilidades de conducir a un cambio en los comportamientos de seguridad.

De este estudio se desprende que pueden ser enormemente útiles medidas de concienciación: contenidos multimedia en el que se narren anécdotas autobiográficas de victimización, acompañadas de historias contadas por expertos y con contenido emocional. Se podría plantear el desarrollo de un vídeo en el que se incluyan los 3 elementos, o bien como elemento de apoyo en clases o sesiones educativas, o bien como elemento único para colgar en webs. El empleo de estas técnicas incidirían en la parte perceptiva y motivacional para tratar de generar cambios comportamentales que, sumados a la previa adquisición de conocimientos, podría disminuir la probabilidad de ser víctima en el futuro. Además, incluiría elementos importantes en el factor humano como son las emociones, ya que, erróneamente, se suele atribuir una excesiva “racionalidad” al usuario/a en su comportamiento cotidiano. En este modo de comportarse rutinario, están presentes los heurísticos y los razonamientos rápidos, que serán oportunidades para los delincuentes al poder aprovechar este bajo esfuerzo cognitivo.

En Drew (2020), entre los hallazgos relevantes, encontró que es un error pensar que las víctimas se motivarían a sí mismas para educarse y protegerse después de ser víctimas. Por lo tanto, defiende que es tan relevante dirigir la educación a los que fueron víctimas de ciberdelitos como a los que no. Pero, además, de dicha idea se desprende que la concienciación debe ser fundamental, ya que la falta de motivación se daría incluso en aquellos individuos que han sido víctimas de la ciberdelincuencia. Otros estudios previos apuntan en dirección opuesta señalando que, aquellos que han sido victimizados previamente, alteraron sus comportamientos y estrategias de protección. Por lo tanto, estos individuos utilizan en mayor medida las estrategias la ciberdelincuencia para evitar volver a ser víctimas (Turanovic & Pratt, 2014).

En el caso de estudios realizados en otros países como México, según el estudio infochannel (Rincón & Prieto, 2020), el 80% de los ciberdelitos se pueden evitar con medidas de concienciación. Para ello, se están llevando a cabo acciones de concienciación mediante instituciones de diverso tipo, especialmente en aquellos ciberdelitos con más incidencia en la ciudadanía. En ese país también están llevando a cabo campañas con recomendaciones para prevenirlas, unidades de apoyo, servicios de orientación técnica y legal (incluyendo mecanismos de denuncia). La concienciación, por lo tanto, se muestra un elemento imprescindible en la protección, y es que el número de ciberataques está aumentando exponencialmente debido, en parte, a la falta de concienciación de los usuarios sobre las prácticas de riesgo en línea (Alqahtani & Kavakli-Thorne, 2020).

Finalmente, en la misma línea apuntan algunos de los datos que arroja el "Estudio sobre percepción y nivel de confianza en España" (ONTSI, 2022) realizado en el último semestre de 2021:

- El 41% de las personas consultadas declara realizar alguna conducta de riesgo a sabiendas y el 40% reconoce no saber con seguridad si su equipo está actualizado
- El 33% afirma que hace clic en enlaces aun sin saber a qué sitio web le redirige.
- El 17% indica abrir ficheros de remitentes desconocidos,
- El 18% afirma deshabilitar el antivirus conscientemente.

2.2. Cultura de ciberseguridad

Se puede definir la cultura en ciberseguridad como el conjunto de conocimientos y habilidades que permiten a un ser humano desenvolverse en el ciberespacio de una manera segura (Pulido & Rosell, 2017). La importancia de esta cultura general en ciberseguridad consiste en elevar el nivel de comprensión de cada miembro de la cadena de ciberseguridad. Es por ello que son necesarias las medidas a nivel nacional y los esfuerzos educativos e inversiones para educar y formar a todos los miembros de la sociedad (Ghernaouti-Helie, 2009). Debe basarse en una visión y una voluntad políticas adecuadas y en asociaciones privadas y públicas eficaces. Si estos 2 sectores no apoyan conjuntamente estas iniciativas, se producirá un efecto negativo a largo plazo en el desarrollo económico y en la capacidad de garantizar la seguridad en el ciberespacio y los bienes y las personas y organizaciones. Ante esta situación, que se agrava día a día, es necesario fomentar una cultura de ciberseguridad global adecuada a través de estrategias de concienciación (Pulido & Rosell, 2017).

El papel de los Estados como protectores del ciberespacio y de la ciudadanía, implica el proporcionar información sobre los riesgos que entraña, teniendo como objetivo tanto las empresas e instituciones públicas, como los propios ciudadanos. Esta función tiene como máximo exponente la creación de lo que viene siendo la "cultura de ciberseguridad" y que viene recogida tanto en nuestra Estrategia Nacional de Ciberseguridad como en la de otros países. Esta cultura permitirá, entre otras cosas, una mayor concienciación pública, elemento clave en todo el proceso de protección de la sociedad. (Peña & Segura, 2014). La necesidad de avanzar en esas políticas educativas para instaurar una cultura de ciberseguridad general vienen reforzadas por algunos estudios que señalan que las fuentes de conocimientos de la población no son las instituciones, sino otras fuentes más informales. En un estudio de Bigdoli et al., (2016), hallaron que la principal fuente de conocimiento sobre la ciberdelincuencia de los participantes, fueron personas conocidas del entorno que han sido víctimas de ciberdelitos y también los medios de comunicación.

Existen efectivamente planes en desarrollo, como el "Plan de cultura de ciberseguridad, concienciación, sensibilización y educación" (Pulido & Rosell, 2017), cuyo objetivo es la promoción de la cultura de ciberseguridad entre ciudadanos, profesionales, empresas y Administraciones Públicas españolas mediante el desarrollo de actividades y mecanismos para la sensibilización, concienciación, formación y educación que renueven y doten de nuevos conocimientos sobre los riesgos derivados del ciberespacio y el uso seguro y responsable de las TIC. El Plan se articula en tres ejes de acción: sensibilización, concienciación y conocimiento; normativa y buenas prácticas. Cada eje tiene asignado un organismo de la Administración pública como responsable y otros como colaboradores. Asimismo, se contemplan unos recursos financieros y humanos para poderlo llevar a cabo.

3. Educación en ciberseguridad y ciberdelincuencia orientada a la población general

Cuando se plantea la educación en ciberseguridad y ciberdelincuencia orientado a la ciudadanía como forma de prevención, cabría preguntarse por qué no hacerlo de cara al delincuente como en muchos otros tipos de delitos. Según el informe sobre la cibercriminalidad en España de 2021 (López et al., 2021), con respecto a los 305.477 hechos conocidos (presuntos ciberdelitos), las 1671 sentencias condenatorias solo representan el 0,5% de los casos. O dicho de otra forma: en España la impunidad de los ciberdelitos (conocidos) es del 99,5%. Si además se tiene en cuenta que algunas

fuentes hacen una estimación de los ciberdelitos conocidos alrededor del 20% de los cometidos y que el 80% no se llega a denunciar ni a conocer.

Estos datos reflejan la dificultad y complejidad de averiguación de la identidad de delincuente. El carácter transnacional de gran parte de estos hechos hacen que ese modo tradicional de operar de la justicia quede obsoleto. En muchas ocasiones, los delincuentes se encuentran en otros países, como China o Rusia, lo que implica que su persecución será muy complicada. Deben tener mayor peso las otras estrategias de cara a prevenir la delincuencia, por ejemplo, orientarse de cara al "control social", implementando estrategias con personal técnico especializado para proteger infraestructuras críticas, redes públicas, mecanismos de control en las plataformas de mensajería, etc.

También existe otra vía complementaria que permitiría reducir el porcentaje de incidencia, que no es otra que la intervención sobre las potenciales víctimas para protegerlas. Esta estrategia orientada a la víctima tiene como principal instrumento a su disposición la educación para protegerse. Mientras que en otros tipos de delitos tradicionales los conocimientos pueden no jugar un papel relevante en la disminución del porcentaje de probabilidad de ser victimizado, en el caso de la ciberseguridad los conocimientos y la concienciación darán pie a una mayor protección. Por todo ello, esta estrategia de prevención de la víctima basada en la educación en ciberseguridad debe tener un amplio respaldo científico sobre el mejor modo de llevarla a cabo.

3.1. Educación en ciberseguridad y ciberdelincuencia

Cuando se hace referencia a la importancia de la educación en ciberseguridad, se debe desgranar su relevancia en 2 corrientes fundamentales. Por una parte, la educación orientada a las medidas de protección, medios para tener una conexión segura, hábitos seguros, acciones para responder a ciberataques o incluso cómo reaccionar ante un delito que hemos sufrido. Todos estos elementos y contendidos serían parte de la educación en ciberseguridad. Por otro lado, el conocimiento relativo a cuáles son las ciberamenazas, los peligros que corremos en la red, cuáles son las formas de ciberdelitos más comunes, dónde y cuándo están presentes, pasarían a formar parte de la educación en ciberdelincuencia. Este componente, aunque no es una medida de protección en sí, permitiría mejorar la concienciación y complementar a los concocimientos en ciberseguridad.

La necesidad de una educación para protegerse de la ciberdelincuencia es cada vez más crítica. Sin embargo, la educación existente hasta ahora en ciberseguridad no ha sido suficiente para hacer frente a los crecientes ciberdelitos (Kim et al., 2016). La

educación en ciberseguridad es un enfoque a largo plazo y eficaz para una sociedad de la información sostenible, segura e inclusiva. (Ghernaouti-Helie, 2009). Sobre cómo debe ser esta educación, algunos autores señalan que tiene que plantearse como "*Una educación consistente, continua y oportuna a los individuos, que puede permitirles mejorar su conciencia y transformar su comportamiento*" (Alqahtani & Kavakli-Thorne, 2020). También lo defiende Adelhamid (2020), especialmente en el caso del phishing, cuando afirma que la única manera de mitigar los ataques de phishing es adelantarse a los ciberdelincuentes mediante la formación en las potenciales víctimas. La formación en phishing debe incluir un equilibrio de material personalizado y enfoques que se ajusten a las características del receptor.

Sobre el tipo de medidas que deben incluir la educación, existirían algunas sobre las que no se podría educar como tal. Este sería el caso de las medidas automatizables, que no son otra cosa que aquellas que no dependen de la intervención de las personas que las usan (ONTSI, 2022). Algunos ejemplos serían el uso de programas antivirus, cortafuegos (firewall), tener actualizado el sistema operativo, programas de bloqueo de pop-up y publicidad, programas y aplicaciones anti-spam, anti-espía, o plugins de seguridad para el navegador. Sí que sería posible incluir conocimientos básicos de las aplicaciones para las personas usuarias puedan integrarla, mejorando su protección y reduciendo su probabilidad de ser víctima de un ciberdelito. Por otra parte, estarían las medidas activas o no automatizables, que son las que quieren intervención manual por parte de las personas usuarias: creación de contraseñas seguras, gestión de archivos temporales e instalación de certificados digitales. Es en esta línea donde tendrá un mayor peso este tipo de educación.

En estrecha relación a esta educación en ciberseguridad y ciberdelincuencia, podemos encontrar un término que cada día cobra más peso, la "ciberresiliencia". La podemos definir como "*la capacidad de anticiparse, resistir, recuperarse y adaptarse a condiciones hostiles consecuencia de condiciones ambientales adversas, estrés de los sistemas por distintas causas o ciberataques"* (Bodeau & Graubart, 2016). La ciberresiliencia, por lo tanto, sería el objetivo último de la educación, consiguiendo mediante la misma una capacidad de defensa contra el cibercrimen. Esa habilidad de anticiparse, responder y adaptarse será un elemento de prevención de la ciberdelincuencia en toda regla que podría tener efectos en el incremento exponencial de las tasas de ciberdelincuencia que se ven en las estadísticas.

Para educar y concienciar y finalmente adquirir ciberresiliencia, será necesario establecer los métodos más adecuados, desde las grandes estrategias europeas y nacionales, pasando por los planes educativos a distintos niveles y las formas técnicas

y específicas de cómo transmitir ese conocimiento. También elaborar contenidos que sean homogéneos en los distintos territorios y organizaciones que los vayan a llevar a cabo. La investigación de todos estos aspectos se hace fundamental, sobre todo en lo que se refiere a cuáles son las brechas existentes y los errores que comente la ciudadanía que permiten una mayor victimización.

- Dentro de los contenidos, además de las técnicas y medidas para protegerse, también se encuentra la cuestión de la información que generamos cada día y la privacidad de dicha información. No todo lo que se comparte en la utilización de los medios digitales se hace conscientemente, de hecho, algunas veces es imposible evitar el compartir gran cantidad de información cuando nos conectamos a Internet. Existirían tres tipos de información que se producen por la actividad en la red (Fundación Telefónica, 2016). En los 3 casos, los usuarios tienen importantes dudas respecto a cuál es su destino final y quién tiene acceso a ellos.
- Información que se comparte por defecto. Solamente los usuarios avanzados conocen que la mera interacción con diferentes dispositivos y plataformas y actividades sencillas como realizar búsquedas generan información que queda registrada.
- Información que se comparte de forma forzada. Cuando se introduce información con la intención de acceder a los beneficios que ofrece la web, hacer transacciones u obtener servicios, por ejemplo, firmar en plataformas, compartir datos personales o proporcionar un número de cuenta bancaria. Los usuarios creen que esta información se queda en la plataforma o website que ofrece el servicio, que es responsable de su uso gracias a las leyes que aseguran la privacidad de los datos. Sin embargo, la mayoría de los usuarios no son conscientes de los términos que la mayoría de los servicios y aplicaciones obligan a firmar respecto a la utilización de sus datos.
- Información que se comparte de forma voluntaria. Va asociada generalmente con el contenido generado por el usuario, como pueden ser fotos y comentarios en redes sociales, foros, emails, etc. Los usuarios son conscientes de que es información que queda expuesta a los. Sin embargo, no conocen cuál es el ciclo de vida de dicha información ni las reglas que aplican para proteger su privacidad.

De este modo, aunque se ha dividido la educación en dos líneas: educación en ciberseguridad (medidas de protección propiamente) y educación en ciberdelincuenia

(conocimiento de las ciberamenazas), cabría añadir ese tercer elemento complementario, pero no irrelevante, “la protección de datos”. La concienciación sobre la gran cantidad de información que generamos en el ciberespacio, ya que pueden suponer, en determinados momentos, una mayor vulnerabilidad ante las ciberamenazas. Algunos ejemplos a señalar, serían la de suplantación de identidad mediante documentos, certificados digitales, robo mediante datos bancarios, etc. e incluso estrategias mixtas en la que los ciberdelincuentes aprovechan datos obtenidos mediante el ciberespacio para cometer robos de forma física (saber por RR.SS. cuando se está de vacaciones para realizar un robo en el domicilio).

También se ha concebido el concepto de “ciberhigiene” de los usuarios finales. El término se refiere a los hábitos cotidianos en materia de seguridad en la red, por ejemplo, emplear cortafuegos y aplicaciones antivirus. Esta ciberhigiene desempeñaría un papel importante en la victimización por ciberdelitos (Cain et al., 2018). Aquellas personas que tengan una buena ciberhigiende mantendrán hábitos, conductas y prácticas encaminadas a proteger su seguridad y su información privada. Estos autores descubrieron que la mayoría de los usuarios disponen de software antivirus (47% y el 78%) y lo actualizan con regularidad, pero también que la mayoría de los usuarios no realizan análisis con la frecuencia suficiente. La mayoría de los usuarios utilizan un cortafuegos, entre el 68% y el 92%, pero no lo cambian cuando es necesario. Muchos usuarios, tanto mayores como jóvenes, comparten demasiada información personal en las redes sociales, como su dirección y sus números de teléfono, y no comprueban su configuración de privacidad.

Los hombres presentan más conocimientos sobre ciberhigiene que las mujeres. Ellas crean contraseñas más débiles y actualizaban el software con menos frecuencia. Sin embargo, a pesar de tener más conocimientos, los hombres no se diferenciaban de las mujeres en su comportamiento de ciberhigiene. También encontraron que haber sufrido ataques en el pasado no influye en su ciberhigiene actual. Otro hallazgo interesante es que los usuarios que se autodefinen como "expertos en ciberseguridad" demostraron tener comportamientos de mayor riesgo y tenían menos conocimientos sobre ciberhigiene. En consonancia con investigaciones anteriores, descubrieron que los usuarios no utilizan las mejores prácticas para proteger sus contraseñas ni para defenderse de los ataques de phishing (Cain et al., 2018). Esta idea de ciberhigiene va muy unida a la ciberresiliencia. A su vez, estas 2 cualidades que deben estar presentes en la población, pueden venir de la mano de la educación en ciberseguridad y ciberdelincuencia.

3.2. Educación en la Población General

Un punto en común entre gran parte de los ciberdelitos es que para que el delito tenga éxito, en una gran parte, la víctima debe participar de alguna manera (Drew, 2020). La víctima favorece su propia victimización cuando realiza alguna solicitud, tiene alguna interacción con un delincuente o no tiene la protección adecuada. También cuando abre un email fraudulento, no identifica el phishing, descarga material pirata o sencillamente clica en un enlace donde, sin querer, descargará malware. Por ese motivo, es necesario comprender el papel de las víctimas en el delito cibernético, y especialmente, intervenir sobre ellas independientemente de los medios de prevencion tradicionales. Existe un reconocimiento en la literatura de que los factores de comportamiento humano son la clave para combatir el ciberdelito (Hadlington & Chivers, 2018).

Como se ha expuesto anteriormente, este enfoque sobre la víctima debe tener por necesidad un enfoque generalista de la población, donde se haga un esfuerzo por tratar de llegar a la mayor cantidad de ciudadanos/as posible. Para ello, se debe adaptar la educación a múltiples variables, con especial atención a la edad del colectivo al que se dirige, el nivel socioeducativo o incluso la pertenencia a algún colectivo de especial vulnerabilidad. La enseñanza generalizada tendrá como consecuencia que los hackers desistirían más fácilmente de lanzar un ataque basándose en el principio de "yo sé que tú sabes". Al saber que la potencial víctima tiene los conocimientos necesarios para reconocer el ciberataque, se replantearía hacerlo al tener en cuenta que las posibilidades de éxito son mínimas (Árpád, I., 2013). Por lo tanto, los riesgos del factor humano pueden mitigarse o reducirse educando a los usuarios finales sobre cómo defenderse de las ciberamenazas, especialmente en casos como el phishing (Aggarwaly et al., 2012; Brody et al., 2007; De Bona & Paci, 2020; Purkait, 2012; Robila & Ragucci, 2006)

Aunque la tecnología de la información es de amplio uso, es necesario enseñar los temas de seguridad de la información para evitar que se conviertan en víctimas de la ciberdelincuencia. (Ismailova & Muharnetjanova, 2016). Tal y como plantea Ghernaouti-Helie (2009), los programas educativos específicos deben ser eficaces y estar disponibles para cada tipo de población objetivo, por un lado, a responsables políticos, profesionales de la justicia y la policía, gestores, profesionales de las TIC y, por otra parte, a los usuarios finales (incluidos niños y ancianos). Los cursos de formación en ciberseguridad deberían integrarse en los distintos niveles de enseñanza, desde la escuela hasta la universidad, en los ámbitos jurídico, científico y social. Tampoco debe omitirse la formación continua, con el fin de preparar a los profesionales para hacer

frente al contexto evolutivo y dinámico de la tecnología y las amenazas. Diversos autores defienden esta introducción de conocimientos relacionados con la seguridad informática en los planes de estudio de todos los niveles educativos (Árpád, I., 2013)

Algunos expertos, como Nieva (2020), señalan que es fundamental que la sociedad tenga unas nociones básicas en ciberseguridad, es por ello necesario enseñarles a los menores conceptos clave y básicos de ciberseguridad para que ellos mismos puedan evitar los peligros. Apunta, además, que en España apenas existen sistemas de formación en ciberseguridad dentro del programa educativo. Es importante resolver esta cuestión dado que una parte de la sociedad carece de conocimientos básicos de seguridad. Complementariamente a que una pequeña parte de la población tenga un conocimiento avanzado, es también importante que la gran mayoría tenga una mínima capacidad de defenderse de los ciberataques. De hecho, esta cuestión se está convirtiendo en un área de creciente preocupación en muchos países desarrollados.

Coughlin (2017), estudió la educación en ciberseguridad dirigida a adolescentes y a adultos no-técnicos. Afirma que existen innumerables aspectos del comportamiento de los usuarios finales que crean o agravan las vulnerabilidades (contraseñas débiles, abrir correos no seguros, no mantener actualizados el sistema operativo, las aplicaciones y el software antivirus). Encontró que aunque los usuarios finales son conscientes de los peligros, los conocimiento que tienen se limita a conocer los términos, pero ni tan siquiera son capaces de definirlos. Al mismo tiempo, advierte que la naturaleza insegura de la tecnología actual, significa que el resultado de esta educación a población no-técnica será la mitigar el problema, pero no la eliminación de las ciberamenazas.

También para Ghernaouti-Helie (2009), hay que educar a la población no-técnica, y para ello, es necesario que exista un modelo de seguridad centrado en el usuario final dentro de un marco técnico y jurídico determinado. Adicionalmente se hace necesario una responsabilidad global de crear una ciudadanía responsable en su comportamiento online y provista de medidas de ciberseguridad adecuadas. La concienciación y educación ayudarán prevenir comportamientos incorrectos y a desarrollar herramientas técnicas, procedimientos legales apropiados para poder construir una confianza razonable en las infraestructuras, servicios, mecanismos de seguridad y controles de las TIC. Por último, debe construirse un modelo que no sea excluyente de aquellas personas con un nivel adquisitivo más bajo, por lo tanto, debe ofrecerse un nivel mínimo de seguridad para las TIC a un coste asequible.

Es de especial relevancia el carácter general que debe tener la educación también en el ámbito laboral. Los trabajadores de las empresas son parte de esa ciudadanía que

debe poseer ya un mínimo de conocimientos previos a formar parte de la empresa, y por lo tanto, la capacidad mínima vendrá marcada por la capacidad mínima del trabajador que menos conocimientos tenga. Es por todo ello, que la educación generalizada a la población también repercutirá a nivel empresarial, y aque las empresas se beneficiarán indirectamente de esta mejora en las capacidades de autoprotección. En esta misma línea apuntan Pulido & Rosell (2017) cuando hablan de la seguridad de las organizaciones. Afirman que es fundamental la implicación de las personas, y no solo implantar medidas técnicas.

El factor humano es un pilar vital en la seguirdad. La falta de conocimientos y cultura de seguridad por parte de los empleados es aprovechada por los ciberdelincuentes, por lo tanto, prácticas inseguras en red pueden poner en riesgo la seguridad de cualquier organización. Cuando perseguimos un riesgo asumible mediante la educación, es especialmente relevante el hecho de que no todo el mundo requiere un mismo nivel seguridad. Según (Pulido & Rosell, 2017), dependerá de la relación, personal o profesional, que el individuo tenga con el ciberespacio. Tal y como exponen, una persona que accede de manera ocasional con su dispositivo a una red social y un directivo de una organización que maneja información sensible con multitud de dispositivos, tendrán requisitos de seguridad diferentes. Es por todo ello, que las necesidades educativas y formativas van a ser diversas.

En este sentido, uno de los momentos de especial relevancia fueron los cambios que se produjeron en 2013, cuando los principales objetivos pasaron de ser las empresas, a ser las personas (Check Point, 2015). Independientemente de que haya personal especializado en las organizaciones y empresas, cada trabajador hará de “cortafuegos” para poder prevenir su propia victimización pero, también, la de la organización en la que trabaja. Un ejemplo de todo esto es, cuando mediante suplantación de identidad, un ciberdelincuente engaña a un administrativo para realizar una transferencia bancaria a una cuenta falsa haciéndose pasar por un proveedor. También cuando se hacen pasar por otro empleado o incluso un superior para efectuar un pago o transferencia de forma urgente. Aunque la afectada será la organización, el ciberdelincuente pondrá en el punto de mira al empleado raso para poder cometer dicho ataque. Sin embargo, señalar en este punto que las pequeñas y medianas empresas, en muchas ocasiones, carecen de los recursos financieros y de los conocimientos necesarios para combatir las ciberamenazas (Morgan, 2020).

Otra prueba de la importancia de esta educación en la población general la arroja la ONTSI. En una encuesta realizada en 2021, al consultar si se cree que es necesaria formación en ciberseguridad (ONTSI, 2022) el 53% manifestó que es necesaria mucha

o bastante, y el 38% afirmó que es necesaria algo de formación. Por lo tanto, el 91% de internautas ven necesaria la formación en ciberseguridad. Ya no es solamente que la población carezca de estos conocimientos, sino que llega a reconocer y admitir tal falta de preparación. Esta brecha digital específica es un obstáculo que se debe superar para poder adaptar la sociedad al Siglo XXI y sus nuevas amenazas en seguridad. "*La digitalización sin ciberseguridad supone una clara barrera tecnológica muy difícil o imposible de afrontar sin la formación adecuada, adaptada a diferente público o conjuntos poblacionales*" (ONTSI, 2022: Pg.57).

El "analfabetismo" informático también tiene como consecuencia que las personas no puedan reconocer efectivamente si son víctimas de un hackeo (Van Wilsem, 2013). Por lo tanto, van a existir víctimas de ciberdelitos que no saben que experimentaron ciberdelitos (Wall, 2008) y que a su vez nunca lleguen a interponer una denuncia ni llegar a visibilizarse en las estadísticas oficiales. A esto se añade que Drew (2020) encontró que es un error pensar que las víctimas se motivarían a sí mismas para educarse y protegerse después de ser víctimas.

Abordando la cuestión en un enfoque comparado, debemos acudir en primer lugar a la primera potencia mundial en el ámbito de la ciberseguridad, tanto en el área de la investigación como en la implementación educativa, Estados Unidos. En dicho país, encontramos la denominadaa NICE (National Initiative for Cybersecurity Education), que busca promover el desarrollo de recursos humanos en el ámbito de la ciberseguridad. Se caracteriza por un alto nivel de planificación, desarrollo y recursos relacionados con la educación y la ciberseguridad, todo ello a un nivel que ningún otro país ha logrado hasta el momento. De hecho, es una prueba más de la preponderancia de EEUU en ámbito de la ciberseguridad. En su caso, el Department of Homeland Security el que busca promover el uso responsable de internet por parte de la población general, todo ello mediante campañas publicitarias públicas (Peña & Segura, 2014). Estas acciones buscan incorporar programas de ciberseguridad en todos los niveles educativos, entre los que se incluye preescolar, además de desarrollar personal especializado en ciberseguridad y ciberdenfensa (por lo tanto, a un nivel avanzado).

En el caso de Reino Unido, el enfoque está más orientado hacia un nivel avanzado. Busca la promoción de expertos en ciberseguridad dentro del sector privado. Recomienda fortalecer la oferta educativa a nivel de posgrado, diseñar una agenda de investigación multidisciplinaria y la creación de un instituto de investigación en ciberseguridad (Peña & Segura, 2014). También cuentan con la Office of Cyber Security & Information Assurance (OCSIA) para coordinar tdas las actividades orientadas a este

fin. En cuanto a la educación más allá de la avanzada, cuentan con la creación de una asignatura a nivel de secundaria sobre seguridad.

Es de destacar también el caso de Australia, el cual desarrolla su Estrategia en 7 prioridades estratégicas. Una de ellas se enfoca en la educación, el empoderamiento de la ciudadanía mediante la información, confianza y herramientas prácticas que necesitan para evitar ser víctimas en el ciberespacio. Para ello, implementa diversas acciones, entre las que se incluyen la creación de un portal estatal orientado a la ciberseguridad (consejos y alertas para ciudadanos y empresas), la incorporación de módulos educativos sobre ciberseguridad en primaria y secundaria, y por último, la celebración con carácter anual de una semana dedicada a la concienciación en ciberseguridad ("Cyber Security Awareness Week"), en la que además, participan empresarios y organizaciones comunitarias (Peña & Segura, 2014).

Estos enfoques en otros países incluyen la formación en ciberseguridad orientada a la población general, al igual que se incluye en España, sin embargo, no es señal de que los mayores esfuerzos se estén dedicando a dicha ciudadanía. Existe asimetría y con un mayor peso de la formación especializada a personal técnico. Uno de los elementos que puede ser explicativo de la asimetría de formación orientada a personal cualificado, o que vaya a desempeñar funciones relacionadas en ciberseguridad, es que se está produciendo un gran déficit de mano de obra. Por lo tanto, ante este déficit de mano de obra cualificada, el sistema educativo se ha readaptado para satisfacer esa necesidad.

Como es lógico, existe una oferta y demanda que se trata de equilibrar, sin embargo, cuando nos referimos a educación a nivel general, quizá ese elemento equilibrador se diluya. Si, por ejemplo, una Universidad, institución académica o similar comienza a ofrecer cursos, masteres, etc. para desarrollo de personal, tendrá una gran demanda, se realizarán matrículas y además se producirá un flujo al mundo laboral. Por otra parte, cuando hablamos de población general, de la ciudadanía en su conjunto, esta idea se convierte en un proyecto a mayor escala, donde la finalidad no es tanto la formación de personas para un puesto de trabajo concreto como podría ser el de cualquier otra titulación profesional, sino un interés general, una idea más social y por lo tanto, donde el Estado y las instituciones públicas, juegan un papel clave (Gonzalez-Manzano & Fuentes, 2019). Definitivamente, se debe destacar la inversión de las instituciones y la voluntad política para tratar de cubrir esta necesidad, que responden, en último caso, a un interés general de la seguridad ciudadana.

Las universidades ofrecen masteres en ciberseguridad, sin embargo, habría un nivel más básico para principiantes. Una educación de forma más masiva con 2 modalidades:

laboratorios virtuales con formación de tipo experimental y, por otro lado, otros de base teórica y práctica. EdX y Coursera son plataformas que están ofreciendo estas alternativas, con un gran éxito y una adopción más generalizada (Gonzalez-Manzano & Fuentes, 2019). De los 32 cursos, 12 son para principiantes. Sin embargo, son específicos de subcategorías de ciberseguridad, y con una orientación profesional (Criptografía, software específico, hardware de seguridad, etc.). No son, por lo tanto, cursos genéricos orientados a la población general. El resto de cursos, son intermedios (12) y avanzados (7). El diseño y constante actualización de estos cursos puede, y debe, ser una base de gran aportación para la elaboración de cursos orientados a la población general. Sus técnicas didácticas y pedagógicas (no tanto a nivel de contenido) pueden ser fuente de conocimiento sobre cómo transmitir el conocimiento en materia de ciberseguridad.

En una revisión sistemática en la que se analizaron artículos de educación en ciberseguridad (Svabensky et al., 2020), encontraron que de los términos en los que se centraban dichos artículos, los aspectos humanos estaban en el 4° lugar, siendo los primeros los programas, las redes de seguridad y conceptos relacionados con el cibercrimen. Además, de 71 artículos, 54 estaban orientados a universitarios, 17 técnicos educativos y 7 a niños. Por lo tanto, es reflejo de la desproporción que existe en la orientación hacia perfiles avanzados frente a la población general, así como la preponderancia de aspectos técnicos frente a los factores humanos.

De los artículos que describían técnicas de intervención, los más comunes fueron los “hands-on learning” (51), o aprendizaje experiencial durante el tiempo en clase o estudio. Consiste en el proceso de aprender a través de experiencia, y se define más específicamente como "aprender a través de la reflexión sobre el hacer”. Incluía talleres de laboratorio, ejercicios, tareas prácticas, juegos educativos y otras actividades para practicar en los términos seleccionados. Otras formas frecuentes de técnicas eran las lecturas (24 artículos), proyectos de larga duración que ocupaban todo el semestre (10 artículos) y debates (8 artículos). La mitad del total de las técnicas implicaban que los alumnos se involucrasen en grupos o por parejas (Svabensky et al., 2020).

En cuanto a las condiciones de uso de las RRSS, también tendrán su papel en la ciberseguridad y la ciberdelincuencia, ya que si no se configuran adecuadamente, el usuario puede dar acceso abierto a su información personal, dispositivo, contenidos que accede, ubicación, contactos, cámara, etc. (Astorga-Aguilar & Schmidt-Fonseca, 2019). La mayoría de las RRSS permiten configurar las normas de privacidad y seguridad, pero de forma predeterminada, permiten posibilidades como de ser encontrada fácilmente, ver su actividad o recibir mensajes de cualquier persona. Es por todo ello que es

fundamental conocer las opciones de cada red social y saber controlar la información que se genera, y sobre todo, quiénes pueden recibirla o verla.

3.3. Brecha digital

Se conoce como brecha digital a la desigualdad en el acceso a Internet y las TIC, es decir, la diferencia que existe entre aquellas poblaciones o colectivos que tienen acceso a dispositivos digitales e Internet y aquellos que por diversas circunstancias tendrían un acceso más limitado o incluso no tendrían dicho acceso. Incluye diversas brechas: disponibilidad, asequibilidad, interés y competencia digital (Vasconcelos & Muller, 2022). Existen diversos factores que provocan esta brecha digital, como puede ser la edad o la región geográfica. Ha sido objeto de diversas políticas públicas, que tratan de combatirla y reducir esa distancia entre poblaciones. Entre todas ellas, es de especial relevancia la diferencia entre zonas urbanas y zonas rurales. En comunidades rurales la brecha digital es muy grande (brecha por zona geográfica). En las regiones más urbanas se posee una mayor cantidad de dispositivos y acceso a internet frente a las zonas rurales que sufren una situación de desventaja. Esta brecha, a su vez, tendrá como consecuencia un mayor desconocimiento del peligro sobre las redes sociales, ciberamenazas, medidas de ciberseguridad y privacidad (Amador, 2017).

El problema no es solamente en España, sino que está presente en gran parte de los países a nivel mundial. En un estudio realizado por Martínez-López y Martínez-López (2018) para conocer la información que tienen los jóvenes de educación media-superior en zonas rurales (Oxaca, México) con respecto a temas de ciberseguridad, se encontró que, en las comunidades rurales dónde el uso de las TIC es limitado, los conocimientos sobre la seguridad de la información y el derecho sobre la protección de los datos personales es casi desconocida. Desde el punto de vista de los autores, se considera que la educación en ciberseguridad en el contexto rural, es el factor clave para iniciar con una cultura de la protección de la información.

Encontraron que existen estudiantes de zonas rurales que desconocen qué es la seguridad de la información, cómo proteger sus datos personales y a que instituciones acudir en caso de ser necesario para garantizar sus derechos a la privacidad y seguridad de su información. *"De aquí la importancia de un plan de estudios en los bachilleratos rurales que contemple una asignatura acerca de la seguridad informática para contribuir a que los jóvenes tengan noción acerca de cómo protegerse en Internet, en cuanto a la seguridad y privacidad de su información. De la misma manera, que tengan información acerca de la protección de datos personales"* (Martínez-López & Martínez-López, 2018).

La edad es otro factor generador de la brecha digital, en este caso, de forma intergeneracional, pudiendo encontrarnos que las personas mayores presentan menores conocimientos y capacidades para defenderse en el ámbito digital frente a las más jóvenes. Es de destacar en este punto la existencia de los llamados “nativos digitales”, que serían aquellas personas que han crecido y adoptado las nuevas tecnologías en edades muy tempranas y, por lo tanto, tendrán más soltura para el uso de estas. Por otra parte, los “inmigrantes digitales” son los que se han ido adaptado al mundo digital ya de adultos. También destacar la dificultad de la tercera edad para acceder a estas tecnologías y, más aún, de un modo seguro. Es por todo ello, que la edad se presenta como una barrera digital que debe ser tenida en cuenta a la hora de diseñar e implementar estrategias para educar en ciberseguridad.

4. Enfoques

4.1. Enfoque Derecho Penal

El Derecho penal es el saber jurídico que establece los principios para crear, interpretar y aplicar las leyes penales, ayudando a orientar a los jueces en sus decisiones. El Derecho penal no se reduce al listado de las conductas consideradas delitos y la penas que a cada uno corresponde, sino que su objetivo prioritario es proteger a la sociedad en su conjunto. “Derecho” significa que es un conjunto coordinado (sistema) de reglas (normas) relativas al comportamiento. El adjetivo “Penal” hace referencia al contenido de esas reglas, es decir, a la tipología de conductas al que se refieren (Bacigalupo et al., 2019). El Derecho Penal, a su vez, se plasma en el Código Penal, que es el conjunto de normas jurídicas punitivas del Estado, en donde se recoge las penas aplicables a toda persona que cometa algún delito y los actos que están tipificados como delitos (Letslaw, 2021). El Código Penal español actual fue aprobado por la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Este código ha sufrido multitud de modificaciones a lo largo de los años.

La importancia del Código Penal en relación con la ciberdelincuencia, reside en que es esta ley la que establece cuáles son los ciberdelitos y cuáles son las penas que llevan aparejadas. Por lo tanto, su persecución y su condena tendrán una dependencia total de lo que establezca esta norma. A su vez, las leyes penales también van incluidas por los cambios sociales y políticos que establecen las modificaciones oportunas. Su importancia también se señala en la Estrategia Nacional de Ciberseguridad, cuando establece como una de las medidas para reforzar las capacidades de investigación y persecución de la cibercriminalidad: “*Reforzar el marco jurídico para responder*

eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación" (DSN, 2019).

En el Código Penal español los ciberdelitos se dividieron en dos grupos: los Ciberdelitos Propios y los Ciberdelitos como vía para la comisión de delitos tradicionales. Se encuentran tipificados en los artículos 197 bis y siguientes como Delitos de Acceso no Autorizado a Sistemas Informáticos, tipificándose los siguientes delitos principales: Delito de Intrusión Informática y Delito de Interceptación Informática. El primero persigue las conductas consistentes en el acceso o facilitación del acceso a un Sistema Informático, vulnerando sus sistemas de seguridad o explotando sus vulnerabilidades. El segundo tiene por objeto la interceptación deliberada e ilegítima de datos comunicados en transmisiones no públicas efectuadas entre sistemas informáticos o dentro de un mismo sistema. El otro grupo de Ciberdelitos son los mediales, que consisten en delitos tradicionales apoyados en las TIC para su comisión(Letslaw, 2021). Los ciberdelitos mediales más habituales son:

- Fraude Informático (phishing, suplantación de identidad, robo y uso de tarjetas de créditos, Art. 248 del Código Penal)
- Daños Informáticos (Art.263 del Código Penal)
- Delitos contra la intimidad y la propia imagen (Art. 197. 2 del Código Penal).
- Defraudación de conexión a internet (Art. 256 del Código Penal, robar Wi-Fi al vecino es delito).
- Delitos contra la libertad – Amenazas y extorsiones a través de internet (Arts. 169 y ss. del Código Penal.
- Delitos contra el honor – Injurias y Calumnias en medios electrónicos (Art. 205 del Código Penal).

En cuanto a la base internacional, el año 2001 tuvo lugar el Convenio sobre la Ciberdelincuencia (Convenio de Budapest de 2001), que se convirtió en el instrumento jurídico que vertebra la definición y tipificación del cibercrimen en cuatro grupos:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Delitos Informáticos referidos al fraude y falsedad.
- Delitos relacionados con el contenido.
- Delitos contra la Propiedad Intelectual y derechos afines.

También desde el Derecho Penal Europeo se han ido aprobando directivas que tratan de armonizar la legislación de los países miembro en relación con la ciberdelincuencia. Algunos ejemplos son la Directiva 2013/40 sobre Integridad de Sistemas y la Directiva 2011/92 contra la explotación sexual y la pornografía infantil (Eynde, 2021). Por lo tanto, tanto desde una perspectiva internacional como nacional, el derecho penal es quien regula y establece cuáles son los delitos en lo que se refiere a la ciberdelincuencia y las penas a las que debe ir asociado. El enfoque Penal se convierte así en un enfoque necesario a la hora de abordar la ciberdelincuencia y su prevención.

4.2. Enfoque Criminología

El estudio de la victimización es uno de los cuatro objetos de estudio de la criminología, junto con el delito, el delincuente y el control social. Por lo tanto, cuando hablamos de cibervictimización o victimización por ciberdelitos, estaríamos encuadrándonos dentro de un objeto de estudio de la criminología. La criminología tiene un largo recorrido en el estudio de esta victimización, sin embargo, han surgido nuevas líneas de estudio y nuevas formas de analizar estos fenómenos. También han surgido diversas adaptaciones y reformulaciones de las teorías clásicas para aplicar a esta nueva forma de delincuencia. Incluso se ha acuñado términos como “Cybercriminology” para denominar a esta nueva criminología con su propio objeto de estudio y su propio glosario de conceptos.

No sería posible un estudio y una posterior intervención en el ámbito sin unos conocimientos criminológicos y legales adecuados. Todo ello hace la criminología sea una rama de estudio clave para aportar conocimientos sobre de las tipologías ciberdelictivas, la prevención, el comportamiento de los ciberdelincuentes, los conocimientos técnico-forenses, de investigación y descubrimiento del delito y el delincuente, victimización y políticas públicas de ciberseguridad. También tiene un gran abanico de teorías clásicas adaptadas a las nuevas realidades presentes en el ciberespacio y la aparición de nuevas para explicar todo el fenómeno delictivo. Entre otras teorías, cabría destacar la Teoría de Actividades Rutinarias o Actividades Cotidianas de Cohen y Fehlson (Cohen & Felson, 1979), que posteriormente tuvo su adaptación al ciberespacio en la CyberTAR o CyberRAT (en inglés). (Yar, 2005; Choi, 2008; Choi & Lee, 2017).

En cuanto a la victimología (uno de los pilares de la criminología) tendrá un peso importante a la hora de diseñar estrategias para mejorar la ciberresiliencia, tan necesaria en la ciudadanía para poder empoderar a las víctimas y hacerlas partícipes. También para analizar cómo se comportan estas y buscar posibles necesidades y puntos

vulnerables. En cuanto al enfoque de la criminología como análisis y prevención del crimen, tendrá su papel fundamental en mejorar las estrategias preventivas, todo el proceso alrededor del ciberdelincuente, la reeducación del mismo, la mejora de los sistemas de control (instituciones, FCSE, legislación, etc.) y también el análisis del modus operandi y técnicas puestas en marcha por los ciberdelincuentes.

4.3. Enfoque Psicología

Se puede definir la psicología como la ciencia que analiza los procesos mentales y de la conducta, que es su manifestación externa. La Psicología es el estudio científico de la conducta y la experiencia, de cómo los seres humanos sienten, piensan, aprenden y conocen para adaptarse al medio que les rodea (Sotelo, 2016). Según Taylor-Jackson et al. (2020), el campo de la psicología puede tener una importante contribución a la educación y la práctica de la ciberseguridad, permitiendo trabajar de forma interdisciplinar, y dotando a los individuos de las habilidades y los conocimientos necesarios para afrontar los retos de la ciberseguridad. El beneficio que pueda aportar la psicología a la industria de la ciberseguridad es enorme, especialmente en una industria que es demasiado dependiente de las soluciones técnicas (Glenny, 2011). De hecho, el principal punto débil de la seguridad de los sistemas informáticos está pasando de la tecnología a la psicología (Benenson et al., 2011).

Para el esfuerzo que implica la educación en ciberseguridad y la prevención de la ciberdelincuencia, es esencial cubrir esta necesidad de colaboración entre la psicología y las TIC. En primer lugar, se debe introducir la psicología en los programas de ciberseguridad para garantizar que los profesionales tengan una comprensión del comportamiento. Este conocimiento de la conducta humana, a su vez, se debe relacionar con sus conocimientos específicos y habilidades técnicas. Los incidentes de ciberseguridad se componen de una secuencia de acciones de comportamiento, cada una de las cuales está determinada por una serie de factores psicológicos. Los programas de educación y formación en ciberseguridad a menudo no abordan plenamente los componentes psicológicos de la ciberseguridad (Taylor-Jackson et al., 2020).

Otra prueba más de la importancia de la psicología viene de los resultados encontrados en el año 2015, cuando se llevó a cabo una encuesta sobre la concienciación en ciberseguridad. Los resultados han puesto de relieve dos hechos clave: En primer punto, en general, los equipos de concienciación no tienen el apoyo, tiempo y recursos que necesitarían para tener éxito. En segundo lugar, los equipos de concienciación suelen tener buenas habilidades técnicas, pero les suelen faltar habilidades de comunicación

interpersonales (Sans, 2016). Los equipos de concienciación ideales deberían estar compuestos por un buen comunicador y un buen técnico. El primero para hacer llegar los mensajes clave y el segundo para apoyarle y poder realizar demostraciones técnicas que tengan el impacto necesario (Pulido & Rosell, 2017).

Thackray et al. (2016) va precisamente en esta línea cuando defiende el uso de la psicología social en el ámbito cibernético, exponiendo la enorme utilidad que puede resultar de la unión de la ciberseguridad y la psicología social para informar y promover los intentos de educar a la ciudadanía, pero también para analizar a los potenciales ciberdelincuentes. Según estos autores, la concienciación y la educación, conducirán a una mayor comprensión de los riesgos y las consecuencias, tanto para los potenciales ciberatacantes como para los defensores. El enfoque no está centrado solamente en la educación para las víctimas, sino que la utilidad de la fusión de las dos disciplinas puede incidir sobre los potenciales delincuentes, disuadiéndolos de comenzar las actividades. Por otra parte, este conocimiento que se genere, también será de gran utilidad para los especilistas, concretamente para entender el perfil de los ciberdelincuentes, sus motivaciones y los procesos psicológicos que se producen en los grupos (cohesión, liderazgo, influencia, etc.) Por lo tanto, defiende la fusión interdisciplinaria como medio de solución.

Dentro de la psicología, también se debe destacar la rama que estudia el aprendizaje y el desarrollo humano en el ámbito de la educación: la psicología de la educación. Su principal objetivo como área de estudio es optimizar el aprendizaje y el rendimiento. Tiene importantes aportaciones para diseñar y desarrollar técnicas y estrategias educativas eficaces, programas de intervención más novedosos y mejor adaptados a las distintas circunstancias y poblaciones. Por lo tanto, la psicología de la educación tendrá, dentro de la corriente general, un especial peso en lo que se refiere a la educación en ciberseguridad. Su enfoque es de especial relevancia para mejorar estas técnicas con las que se pretende mejorar la preparación y capacidad de ciberresiliencia de las personas usuarias. La aplicación de todo el conocimiento que aporta esta rama de estudio podrá mejorar la implementación de la educación, con una atención especial en la infancia y la adolescencia, población que requiere de una mayor adaptación educativa.

Entre las aportaciones que se pueden encontrar en la literatura de investigación en el área de psicología y que tiene una incidencia directa en torno a la ciberdelincuencia y las víctimas, se pueden destacar: análisis y comprensión de la motivación de los ciberdelincuentes, predicción de las acciones futuras, diseño de políticas públicas atendiendo a factores individuales, desarrollo de aplicaciones centradas en el ser

humano, ingeniería social (manipulación y engaño), estudio de los heurísticos, cambios de comportamiento en los usuarios e intervención en la cultura organizativa (Taylor-Jackson et al., 2020). Se tratan de temas propios de la psicología y que aportan importantes elementos para poder prevenir la ciberdelincuencia. Además, existe un conocimiento pedagógico basado en la investigación y la experiencia sobre la mejor manera de educar a la gente. Este conocimiento podría ser utilizado para la educación de los estudiantes y profesionales de la ciberseguridad, que a su vez, tendrán una mejor capacitación para educar a la población general no-técnica. Por lo tanto, la aportación no es solamente sobre el contenido, sino también sobre el cómo educar.

Además, el papel de la psicología incluye la comprensión de las capacidades, habilidades, intenciones y motivaciones de los ciberdelicuentes. Las motivaciones de los piratas informáticos se han redefinido y actualizado constantemente (Seebruck, 2015) Entre ellas cabe destacar:

• Recreación: aquellos que piratean por placer, como la curiosidad intelectual, la emoción o la travesura;

• Prestigio: ganancias no materiales, como la notoriedad. Sería el caso de los denominados piratas informáticos de sombrero blanco, Whitehat.

• Venganza: venganza personal y problemas más amplios de justicia social (por ejemplo, movimientos de crowdsourcing en línea);

• Beneficio: ganancia material, la principal motivación para criminales;

• Ideología: activistas políticos o sociales. También se les denomina hacktivistas.

En cuanto al enfoque de la psicología aplicado a la víctima, se han realizado muchos intentos de promover comportamientos positivos en materia de ciberseguridad, sea en ámbito doméstico como en el lugar de trabajo. Se basan en animar a los usuarios a adoptar siempre un enfoque más lento, racional y minucioso en las actividades relacionadas con la ciberseguridad. Sin embargo, los psicólogos argumentan que esto no es sostenible y que es importante aceptar que la tendencia de los individuos a tomar decisiones rápidas (heurísticos) es una necesidad evolutiva, no un defecto inherente de las personas(Taylor-Jackson et al., 2020). Se plantea entonces el reto de cómo conseguir un análisis profundo, lento, racional en el ámbito de la ciberseguridad, y al mismo tiempo, que encaje con esta cualidad propia de las personas a funcionar en un modo rápido basándose en heurísticos.

El uso de estos heruísticos tiene un papel especialmente relevante en el phishing, el cual se caracteriza por una gramática pobre y, en muchas ocasiones, por intentos

burdos de manipulación. Se ha observado una tendencia al empleo de un lenguaje y unas técnicas cada vez más sofisticadas y persuasivas, prueba de ello es que los más convincentes engañan a los usuarios hasta un 45% de las veces (Zen Protocol, 2017). El phishing se aprovecha de la heurística para la toma de decisiones (atajos mentales) que los individuos utilizan fruto de la necesidad de interactuar con un entorno complejo. El estudio y análisis de los heurísticos es un objeto de estudio de la Psicología, la cual estudia cómo los individuos emplean estos "razonamientos simples" o "atajos mentales" para reducir los recursos cognitivos. Son útiles para disminuir la sobrecarga que supone resolver problemas o abordar cuestiones diariamente. Sería imposible dedicar una atención total y realizar un análisis profundo de todos los estímulos y circunstancias que nos rodean, provocaría un sobreesfuerzo cognitivo constante a la hora de interactuar con el mundo complejo en el que vivimos.

Esta idea del uso de heurísticos como forma de reducir recursos cognitivos se puede aplicar al ciberespacio, ya que el individuo debe interactuar constantemente con distintos elementos, problemas, estímulos, etc. Ejemplos de ello serían abrir correos electrónicos, acceder a información o descargar y subir archivos. Comprender cómo el phishing aprovecha los heurísticos para poder acceder a la víctima es un gran avance en la prevención enfocada en la víctima y, especialmente, si la comprensión de ese proceso es retransmitido en la educación en ciberseguridad. El empleo de la heurística y los sesgos a menudo se basa en información relativamente limitada, así que el éxito de toda esta ingeniería social se orienta a animar a los objetivos a tomar decisiones más rápidas. Otros procesos psicológicos relevantes para el caso del phishing incluyen la teoría de la protección-motivación (Taylor-Jackson et al., 2020), en la que se utiliza una apelación al miedo o un elemento de urgencia. Ejemplo de todo lo anterior sería cuando, a través de un correo electrónico falso, se informa que la cuenta bancaria fue hackeada para engañar a un usuario a realizar acciones que le harán caer en la trampa del ciberdelincuente.

También en Psicología encontramos teorías con cierta aplicación al mundo de la prevención de ciberdelincuencia. La teoría de la motivación de la protección (PMT) fue desarrollada en su origen con el propósito de aclarar las apelaciones al miedo, pero se ha empleado como un modelo más general para estudiar las decisiones relacionadas con el riesgo. Actualmente, la PMT se ha podido aplicar al ámbito de la ciberseguridad proporcionando oportunidades para estudiar la motivación de los usuarios finales. Concretamente, para llevar a cabo un comportamiento de precaución en línea, convirtiéndose en un enfoque importante en la literatura actual de seguridad de la información y su relación con el miedo (Jansen & Van Schaik, 2019). A pesar de todo,

existirían algunas visiones contrarias, que plantean que es contraproducente construir una seguridad basada en el miedo. El miedo es un argumento de venta cuando se trata de cuestiones de seguridad, pero no es racional y no conduce a la mejor eficacia en materia de seguridad (Ghernaouti-Helie, 2009).

Existen también estudios que han tratado de comprobar hasta qué punto un modelo conceptual sobre los determinantes de las conductas preventivas no digitales puede aplicarse al estudio de las conductas de ciberseguridad. En Dodel & Mesch (2017), han aplicado las teorías cognitivas de la conducta sanitaria a la ciberseguridad. Estas teorías son un grupo de perspectivas relacionadas que sostienen que un pequeño número de creencias y actitudes son los mejores determinantes próximos de la conducta preventiva. Según este punto de vista, los seres humanos son tomadores de decisiones racionales que sopesan los costes de tomar precauciones frente a los beneficios que podrían obtenerse de ellas (Weinstein, 1987). Suponen una versión limitada de la racionalidad en la que los individuos están orientados al futuro y evalúan los costes y los beneficios de un comportamiento, pero de forma no óptima; pueden tener creencias incorrectas y actuar con intenciones basadas en información antigua o falsa.

Dentro de ellos, el Modelo de Creencias en Salud (MFS), considera dos factores principales como los determinantes de los comportamientos relacionados con la salud (Rosenstock, 1974):

1. Las percepciones sobre las amenazas.

2. Las expectativas sobre el comportamiento.

La primera se compone de dos conjuntos de percepciones sobre el peligro: la susceptibilidad percibida al riesgo y la gravedad percibida de las consecuencias de esas amenazas. Los autores encontraron que el modelo de creencias sobre la salud parece funcionar de forma más que razonable como marco para predecir el comportamiento preventivo de ciberseguridad (uso de antivirus).

En cuanto a los métodos en las organizaciones que utilizan la psicología para hacer frente a los riesgos de ciberseguridad, se centran en la formación HATCH (Hacking and Tricking Capricious Humans) que utiliza escenarios en tiempo real para ayudar a los empleados a aprender diferentes situaciones de ciberataque y los procesos para hacerles frente. Este método ha resultado especialmente eficaz para reducir los ataques relacionados con el phishing, el ransomware, las manipulaciones físicas y el spear phishing. Los aspectos de gamificación dentro de este tipo de formación, se centran en la evaluación del comportamiento de hipotéticas víctimas de ciberataques mediante manipulaciones psicológicas. Se encontró que esto tiene un gran impacto en el aumento

del nivel de concienciación sobre los riesgos de ciberseguridad entre los empleados. Por lo tanto, es de destacar que esta colaboración entre las empresas tecnológicas y los investigadores en psicología, mejora el conocimiento y la calidad de la educación en ciberseguridad. También optimizará la intervención para conseguir cambios de comportamiento entre los usuarios finales (Skinner et al., 2018).

Además, algunas organizaciones consideran cada vez más crucial aplicar la psicología para potenciar la ciberseguridad, centrándose en limitaciones de comportamiento específicas como: la influencia cultural, los sesgos, las preferencias cognitivas, los comportamientos de seguridad irresponsables, así como el sesgo de sobrestimar la propia capacidad de seguridad (Taylor-Jackson et al., 2020). Los resultados de algunos ensayos indican seis requisitos para este tipo de aprendizaje que combina factores de psicología y ciberseguridad (Steptoe & Wardle, 2001; Taylor-Jackson et al., 2020; Power & Kirwan, 2014):

1. El aspecto inmersivo del enfoque a través de vídeos y simulaciones parece ser especialmente eficaz con el alumnado más jóven. Tienen menos distracciones y mejora la motivación;
2. La integración de un diseño de juego bien ejecutado, respaldado psicológicamente con retos intelectuales y técnicas de refuerzo positivo, consigue mejorar la motivación y compromiso de los/as alumnos/as. Además, se consigue fomenta cambios de comportamiento y la retención de los conocimientos;
3. El alumnado demostró el deseo de tener control sobre su ritmo de aprendizaje y sobre y la plataforma de los materiales educativos. Esta idea está directamente relacionada con los resultados de algunas investigaciones en psicología, que sugiere que dar a la gente una sensación de control sobre su propio proceso de cambio conductual aumentará la eficacia en los resultados.
4. El alumnado responde mejor cuando hay una combinación de vídeos, cuestionarios y sesiones interactivas, por lo tanto, es necesario mantener un equilibrio entre las actividades. Cuando los individuos encuentran alguna actividad demasiado extensa, intentan engañar al sistema para pasar a la siguiente actividad;
5. La concienciación y sensibilización no son elementos suficiente por sí mismos. Según la Teoría de motivación a la protección (Power & Kirwan, 2014), los individuos que tienen demasiado miedo a una posible amenaza, pueden no intentar siquiera evitarla si creen que dicha evitación no es posible. La educación

en ciberseguridad, por lo tanto, debe mitigar este riesgo mediante la introducción inmediata de un módulo que ayuda al usuario a protegerse frente a la ciberamenaza;

6. El alumnado necesita feedback, conocer cuáles están siendo sus resultados y poder obtener una autoevaluación. Además, necesita que esa evaluación sea a intervalos regulares durante todo el proceso educativo, incluso se puede añadir la posibilidad de recibir datos comparativos sobre su rendimiento frente al resto del grupo. La finalidad sería mejorar la motivación externa y progresivamente la motivación interna (el entusiasmo por el propio aprendizaje).

También algunos ejemplos de implementación de educación en ciberseguridad donde la psicología tuvo un peso importante, han sido los puestos en marcha en Reino Unido (Taylor-Jackson et al., 2020). Haciendo uso de la teoría del aprendizaje cognitivo social (McLeod, 2016; Ewen, 2010), se pidió a los empleados que considerasen cómo las acciones podrían conducir/facilitar los ataques de ciberseguridad, de manera similar a los ejercicios de toma de perspectiva utilizados con los estudiantes. Se efectuaron simulaciones interactivas inmersivas con ejemplos de incidentes de ciberseguridad realistas, seguidas de cuestionarios interactivos para evaluar los conocimientos.

Se puede considerar, por lo tanto, a la psicología, como ciencia que estudia el comportamiento humano, una herramienta fundamental para poder comprender todo el fenómeno de la ciberdelincuencia y su victimización, especialmente a la hora de prevenirla. Sus teorías y conocimientos, pueden (y deben) enriquecer todas las estrategias y técnicas a la hora de educar y concienciar a la población general. Su rama de la psicología de la educación también tendrá un papel central para la mejora de la transmisión del conocimiento necesario, y la optimización del tiempo y los recursos necesarios para educar. Por último, todo el lenguaje, terminología y conceptos que genera la psicología, serán imprescindibles para poder dar un constructo teórico a la prevención de la ciberdelincuencia mediante la educación en ciberseguridad.

4.4. Enfoque Pedagogía / Ciencias de la Educación

No se puede concebir una educación adecuada y optimizada sin tener en cuenta todo el conocimiento creado y desarrollado por las ciencias de la educación. Se entiende por Ciencias de la Educación a todas las disciplinas que complementan y nutren la educación por medio de diferentes conocimientos (Campos, 2007). Entre estas ciencias destacarían la sociología, psicología, biología, política y pedagogía. Las Ciencias de la Educación, por lo tanto, son un conjunto de disciplinas que explican el fenómeno educativo en sus múltiples dimensiones. Cada una de ellas trata de estudiar, analizar y

comprender las diferentes situaciones y contextos existentes en el ámbito educativo, ya sea una situación formal o informal, para luego abordarlas desde distintas perspectivas. Todas estas ciencias abordan la complejidad del acto educativo y la importancia que tiene, convirtiéndose en un sistema circular y de comunicación formado por diversas dimensiones. Gracias todo este sistema circular formado por conocimientos acerca de la educación, se puede hablar y postular la existencia de la Teoría de la Educación, de carácter eminentemente integrador (Colom, 1996). Por lo tanto, las ciencias de la educación dan pie a obtener aportes de las diferentes ciencias que las forman, y conseguir el beneficio de una continua actualización y optimización en su funcionamiento (Perez, 1978).

De los aportes de todo este conjunto de ciencias y disciplinas, psicología, filosofía, sociología, etc. se nutre la pedagogía. Su objeto de estudio es la formación del individuo, con un conocimiento práctico y una intencionalidad formativa. Se define como "*el conjunto de conocimientos que están orientados hacia la educación, entendida como un fenómeno que pertenece intrínsecamente a la especie humana y que se desarrolla de manera social*" (Perez & Merino, 2008). Tiene características psicosociales y se considera una ciencia aplicada. Se diferencia con la didáctica en que la pedagogía estudia la educación y la didáctica, por su parte, es la disciplina que favorece el aprendizaje. Se puede entender entonces a la didáctica como una parte de la pedagogía. Su aportación a la educación en ciberseguridad es principalmente en el carácter técnico. Debe ser tenida en cuenta a la hora de diseñar las intervenciones educativas en ciberseguridad, dado que estudia la metodología y las técnicas que se aplican a la enseñanza y la educación, especialmente la infantil. Sobre todo, cuando se trata de la infancia y sus peculiaridades y necesidades en el aprendizaje.

Dentro de este conocimiento, herramientas y técnicas que aportan las ciencias de la educación, cabría destacar aquellas que se enfocan en la adaptación a los distintos perfiles diana. La forma de educar no es igual en la infancia que en los adultos, la tercera edad, personas inmigrantes con dificultades del idioma y falta de alfabetización digital o las personas con diversidad de cualquier tipo. Por lo tanto, cuando se decide educar, se deben tener en cuenta estas cualidades propias de la población con la que se trabaja. En cuanto al enfoque de las ciencias educativas, es que no solo es necesario adquirir conocimientos (Seas, 2016), también será necesario interiorziar dicho aprendizaje. La información debe fluir desde estructuras cognitivas con la finalidad de prevenir la victimización, siendo capaces de identificar y detectar las ciberamenazas, comprender los peligros que implican las RRSS e internet en general. Esta interiorización involucra un aprendizaje en todos los aspectos cognitivos, como pueden ser las expectativas, las

emociones (especialmente el miedo) la sensibilidad, la percepción de las distintas situaciones y circunstancias, los heurísticos, etc. Tener en cuenta todos estos factores, objeto de estudio de las ciencias de la educación, pueden potenciar en su conjunto la motivación, el interés y la necesidad por aprender.

Como prueba del valor de las ciencias educativas, encontramos las conclusiones de Livingstone, Mascheroni y Staksrud (2015). Estas muestran que la mediación de los educadores es un primer factor determinante para limitar los potenciales riesgos que conlleva el uso de tecnología online. Por lo tanto, si deseamos conseguir la prevención mediante la educación, es necesario plantear un cambio estructural que redefina las competencias de los educadores en el marco de un proceso de innovación pedagógica (Howard, Yang, Ma, Maton, & Rennie, 2018; Redecker, 2017). Por el contrario a como debería ser, las ciencias de la educación están poco presente en la investigación en esta área en la actualidad. La mayor parte de los/as autores/as perteneces a ciencias computacionales o vinculadas a la informática. La incorporación de personal proveniente de las ciencias de la educación, tanto para la investigación, como para la implementación de las políticas educativas en ciberseguridad, sería un activo de enorme interés y con una gran aportación para mejorar el conocimiento y la optimización del aprendizaje.

4.5. Enfoque Ciencias Políticas

Se conoce como ciencia política a la disciplina que estudia y analiza los fenómenos políticos. Forma parte de las ciencias sociales y permite conocer, explicar, estudiar y analizar la realidad en torno al Estado y las políticas que se dan en la sociedad. También estudia el ejercicio, distribución y organización del poder en una sociedad, analizando los hechos políticos y la conducta política (Torreblanca, 2006). Dentro de esta disciplina, es de especial interés los conocimientos que puede aportar de cara a la planificación de políticas públicas de seguridad, las estrategias nacionales y la gestión de recursos dirigidos a prevenir y combatir la ciberdelincuencia. Por lo tanto, este enfoque debe estar presente en cualquier mesa de decisión a la hora de implementar políticas de prevención mediante la educación, más aún teniendo en cuenta el papel fundamental del Estado y las instituciones educativas, de fuerzas y cuerpos de seguridad, de justicia, etc.

La ciberseguridad aborda un amplio abanico de cuestiones como la seguridad nacional, la soberanía de los Estados, la protección de infraestructuras críticas, riesgos para las organizaciones que dependen de las TIC, la seguridad de los valores materiales e inmateriales y la protección de los datos personales entre otras. Estos son los principales retos y desafíos a los que deben enfrentarse los gobiernos a la hora de

desarrollar una política, un plan de estudios y una cultura de ciberseguridad nacional en relación con las necesidades locales e internacionales. Además, las políticas eficaces de ciberseguridad deben responder a las necesidades individuales, no solo a las de las grandes instituciones públicas o privadas (Ghernaouti-Helie, 2009). Por lo tanto, ciberseguridad y política van estrechamente entrelazadas, siendo la segunda la que permita el fomento e implantación de la primera.

4.6. Enfoque STEAM

El STEM es el acrónimo bajo el cual se engloban las siglas “Science, Technology, Engineering & Mathematics”. Su variante es la STEAM, donde se añaden las artes, dando espacio también al conocimiento relacionado con el arte y el diseño (Santillán et al., 2019). Bajo este término STEAM, se genera un marco para la educación a través de las disciplinas científicas, que plantea la ciencia y la tecnología a través de la ingeniería y de las artes. Bajo ese esquema, los nuevos modelos de investigación educativa deberían de considerar la progresiva integración del marco de las disciplinas científicas (Resnick & Rosenbaum, 2013). Diversas investigaciones confirman que las STEAM se presentan como un enfoque eficaz para aumentar la creatividad, la motivación y la autoeficacia del alumnado en los procesos de enseñanza aprendizaje. También se destaca que debe haber interdisciplinariedad y estar conectado con los contenidos. Por lo tanto, para el enfoque educativo, las STEAM tienen una interesante aportación propia e interdisciplinar, que enriquecería a los conocimientos aportados por las Ciencias Sociales.

Dentro de las STEAM destacarían, en relación con la ciberseguridad, la tecnología, la ciencia y la ingeniería. Si miramos el origen de los/as autores/as de la mayor parte de investigaciones en el área de la ciberseguridad, podemos encontrar a personal perteneciente a la informática, ciencias computacionales, sistemas, ingenierías, etc. y es que ciberseguridad ante todo es ciencia y computación. Es evidente la pertenencia de la ciberseguridad a la informática y las ciencias computacionales, por lo que carecería de sentido que no estuviese en cualquier abordaje interdisciplinar sobre el objeto de estudio. Sin embargo, tal y como se expondrá en otras secciones, más bien cabría destacar una desproporción de las STEAM a la hora plantear la problemática de la ciberdelincuencia y la educación en la población general. Aunque el diseño de sistemas seguros, cortafuegos, técnicas de machine learning, aplicaciones y software de ciberseguridad es objeto de la informática y las ciencias computacionales, se quedaría falto de soporte conductual sin las ciencias sociales y vinculadas.

Una de las subáreas de mayor relevancia es la de Seguridad de la Información. Su objeto de estudio son las tecnologías para el tratamiento de la información digital, que se encargan de la protección de los sistemas sobre los que la información se almacena y transmite, convirtiendo la infraestructura tecnológica en otro activo a proteger. El enfoque consiste en proteger la información y sistemas informáticos ante las amenazas para las que son vulnerables, seleccionando e implementando controles o contramedidas que ayuden a reducir el riesgo que representan dichas vulnerabilidades. Si para la seguridad informática el activo a proteger son los sistemas tecnológicos y para la seguridad de la información es la información junto con la tecnología subyacente, para la ciberseguridad el objetivo principal claramente no es proteger el ciberespacio, sino más bien proteger a aquellos que funcionan en el ciberespacio, ya sean personas, organizaciones o naciones (Sánchez et al., 2022).

La capacitación en estas áreas a un nivel básico también serán un elemento de empoderamiento de la ciudadanía. Cada vez se habla más de alfabetización digital y se ponen en marcha políticas y estrategias para que todo el mundo tenga unos mínimos conocimientos de informática, redes, ordenadores y nuevas tecnologías en general. Desde este punto de vista, la implantación de la informática en momentos iniciales de la educación, como la escuela o la secundaria, serán claves para el fomento de la capacitación. Por lo tanto, cuanto más conocimientos informático, mayor es el nivel de conocimiento de las amenazas del ciberespacio (Ismailova & Muharnetjanova, 2016). Por otra parte, fuera de un nivel básico, gran parte de los estudios en ciberseguridad en STEAM suelen ser a un nivel avanzado y dirigido a personal técnico que se dedica a la ciberseguridad. Este personal perteneciente a las ciencias más puras, las vinculadas a nuevas tecnologías y las ingenierías serán ese conjunto de profesionales que se dedicarán a proteger a la sociedad en su conjunto.

4.7. La interdisciplinariedad

La promoción de un ciberespacio seguro y fiable, debe llevarse a cabo desde distintos enfoques, sin centrarse únicamente en aspectos puramente técnicos. Es por ello que se hace más necesario que nunca buscar un conocimiento amplio y comprensión abierta sobre las distintas formas de cibedelincuencia a las que se enfrenta nuestra sociedad, especialmente aquellas nuevas y emergentes (DSN, 2019). Por lo tanto, para profundizar sobre la ciberdelincuencia y para aportar soluciones eficaces de seguridad en la población no-técnica, es necesario un enfoque global e interdisciplinario (Ghernaouti-Helie, 2009).

La ciberseguridad y la ciberdelincuencia es un punto de encuentro entre los campos tecnológico, jurídico, psicológico, criminológico, sociológico, económico y político, por lo que la seguridad de la información es interdisciplinaria por naturaleza. También debe reflejar las particularidades y características propias según el país, la visión y la cultura de una nación, así como responder a las necesidades específicas de ciberseguridad del contexto local donde se implementa. No implica cuestiones meramente técnicas ya que, al evolucionar del campo técnico al campo de la gestión, el concepto de seguridad de las TIC dio paso a la gestión de los riesgos tecnológicos e informáticos.

Hoy en día, una parte importante de los usuarios finales de las TIC, simplemente no entienden las cuestiones de ciberseguridad y no tienen la habilidad o las herramientas para protegerse correctamente. Deben confiar en productos y mecanismos que no dominan, en soluciones que les han sido impuestas por razones comerciales y la seguridad se hace en el desconocimiento. El desarrollo de un enfoque interdisciplinario de la seguridad de la información permitirá un mejor enfoque integrador y global, que aportará un valor añadido en el dominio de los riesgos informáticos (Ghernaouti-Helie, 2009). En el caso concreto de la educación en ciberseguridad y ciberdelincuencia, ese carácter interdisciplinar se hace más necesario que nunca, sobre todo reforzando los conocimientos desde las perspectivas sociales (psicología, criminología, educación y ciencias políticas).

La actividad social no es determinista, el comportamiento humano es extremadamente variable e incluso impredecible y difícil de anticipar y controlar. Hay que añadir que los equipos y expertos encargados de la ciberseguridad tienen un perfil técnico, con una alta preparación en informática, pero no sobre el comportamiento humano, la incidencia de la cultura y la formación. En la actualidad se requieren también expertos de otras disciplinas capaces de analizar el comportamiento de los usuarios y colaborar en el análisis y diseño de soluciones a los problemas de la ciberseguridad. Las nuevas tecnologías de la información y el ciberespacio están penetrando sobre la vida cotidiana de la ciudadanía, lo que obliga a la ciberseguridad a ir más allá de los aspectos técnicos. Debe convertirse en una disciplina multidisciplinar donde participen expertos en comportamiento que aporten una perspectiva sociocultural, psicológica y de la educación (Sánchez et al., 2022).

5. Políticas públicas en materia de ciberseguridad en España.

"*Es responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más*

vulnerables y que permita el adecuado desarrollo socioeconómico de España" (DSN, 2019).

Aunque la ciberseguridad es algo extendido en toda la sociedad y las ciberamenazas afecta a toda la ciudadanía, es claro que el papel del Estado como principal promotor en la función de proteger, y así lo defiende la Estrategia Nacional de Ciberseguridad (de ahora en adelante ENC). La forma que tiene dicho estado en dar forma a ello, es mediante las políticas públicas que creen normas e instituciones encargadas de velar por la seguridad. Son distintas las instituciones públicas y los niveles en los que se desarrolla: A nivel nacional, autonómico y local. Adicionalmente, existe un contexto Internacional, con un subnivel europeo, en el encontramos distintas instituciones que tienen competencias y objetivos relacionados con la materia de estudio.

A nivel Europeo, surge también la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 con relación a la utilización de datos y la protección del derecho a la intimidad. Se refiere a la protección de las personas físicas en materia de tratamiento de datos personales y su libre circulación. Este texto constituye un pilar básico sobre la que se asienta la protección de datos a un nivel europeo (Valls-Prieto, 2016). En cuanto a la Ley de Ciberseguridad de la UE (Eur-Lex, 2019), refuerza la Agencia de la UE para la ciberseguridad (ENISA) y establece un marco de certificación de la ciberseguridad. La agencia europea ENISA tiene el mandato de aumentar la cooperación operativa a nivel de la UE, ayudando a los Estados miembros de la UE que deseen solicitarla a manejar sus incidentes de ciberseguridad, y apoyando la coordinación de la UE en caso de ciberataques y crisis transfronterizas a gran escala.

Posteriormente, el 18 de abril de 2023, la Comisión propuso una modificación específica de dicha Ley para la adopción de sistemas de certificación europeos que ayuden a las empresas y organizaciones a prevenir, detectar, responder o recuperarse de incidentes (Comisión Europea, 2023). Por otra parte, en diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior anunciaron la Estrategia de Ciberseguridad de la UE. El objetivo de esta estrategia es "*reforzar la resiliencia de Europa frente a las ciberamenazas y garantizar que todos los ciudadanos y empresas puedan beneficiarse plenamente de servicios y herramientas digitales seguros y fiables*" (Consejo Europeo, 2023). La estrategia incluye propuestas para la implantación de instrumentos normativos, de actuación y de inversión.

El sentido de que existan directivas europeas y normas jurídicas que regulen la ciberseguridad, reside en que es más efectivo y práctico que los distintos países

compartan normas comunes. Además, muchos de los ciberdelitos se cometen desde y hacia varios países. Como consecuencia, esta base legislativa europea permite mayores facilidades a la hora de perseguir la ciberdelincuencia y ayudar a prevenirla. Se ha avanzado mucho con la creación de instituciones específicas de cooperación internacional, como Europol o Eurojust, que luchan contra la ciberdelincuencia. En cuanto a la clasificación europea de gestión de ciberseguridad, España se sitúa en cuarta posición respecto al resto de estados miembros (ONTSI, 2022). La mejora en esta clasificación en el futuro puede venir de la mano de la formación y la educación, ya que dotaría al país de mejores herramientas para proteger a sus instituciones, empresas y ciudadanos. Por otro lado, las entidades organizadas de ciberdelincuencia están uniendo sus fuerzas. Aun con todo, se estima que su probabilidad de detección y persecución es tan baja como el 0,05% en Estados Unidos, el país con mayor desarrollo en la ciberseguridad (Morgan, 2020).

A un nivel inferior al internacional y el europeo, nos encontramos con las políticas públicas a nivel nacional, donde es de destacar la ENC, que será desarrollada en el siguiente apartado. Es el Gobierno y, concretamente, el Ministerio del Interior, quienes tendrán un mayor protagonismo a la hora de combatir la ciberdelincuencia, aun sin dejar de lado el importante labor que puede tener el Ministerio de Educación a la hora de abordar la educación en ciberseguridad propiamente. El principal eje de las políticas públicas en materia de educación en ciberseguridad, fue la creación de instituciones específicas como el OSI o el INCIBE, que tienen la educación y concienciación de la ciudadanía como objetivos fundamentales.

Además de la creación de instituciones, se han puesto en marcha otros planes y políticas públicas. Como ejemplos concretos, encontramos que, durante 2021 y el primer semestre de 2022, se ha dado un impulso crucial a las inversiones del Plan de Recuperación en el ámbito digital en conectividad, I+D, digitalización de la Administración y de las pymes. Por su parte, la Agenda 2030 para el Desarrollo Sostenible, es un plan de acción en distintos ámbitos para la mejora de la sociedad. Este plan estratégico prevé actuaciones dirigidas a mejorar la digitalización para la mejora de la eficacia de las actuaciones y la lucha contra la brecha digital. Todas estas políticas de carácter general suelen incluir elementos de ciberseguridad dentro de eliminar esta brecha digital. (MDSA2030, 2021). En cuanto a la Instrucción 1/2021 del Secretario de Estado de Seguridad, recoge el Plan Estratégico contra la Cibercriminalidad, en el que se establecen funciones y competencias para organismos relacionados con la ciberseguridad (Congreso, 2021).

Con el Plan de Recuperación, Transformación y Resiliencia se han puesto en marcha proyectos y ayudas para la digitalización donde se incluyen medidas de educación en ciberseguridad, tanto para empresas y autónomos, como para proyectos en Entidades del Tercer Sector (Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G). También podemos encontrar la agenda España Digital, que es la hoja de ruta para la transformación digital del país, una estrategia ambiciosa para aprovechar plenamente las nuevas tecnologías y lograr un crecimiento económico más intenso y sostenido.

En el siguiente nivel, el autonómico, se ha llevado a cabo una importante transferencia a las Comunidades Autónomas y ayuntamientos para la digitalización del sector público y el impulso de las competencias digitales a la ciudadanía, incluidas la educación en ciberseguridad y concienciación en ciberdelincuencia. Algunos ejemplos son la creación de AMTEGA (Axencia para a Modernización Tecnolóxica de Galicia), la Ley para crear una Agencia de Ciberseguridad en la Comunidad de Madrid, el CSIRT-CV de la Comunidad Valenciana con iniciativas como el Concienciat, el Centro de Seguridad de la Información de Cataluña, la Agencia Vasca de Ciberseguridad, etc.

Finalmente, a la hora de abordar la cuestión de la ciberseguridad, se hace necesario tener en cuenta también la cultura local y no solo los contextos y marcos jurídicos nacionales (Ghernaouti-Helie, 2009). Por lo tanto, cualquier estrategia global para desarrollar una cultura de ciberseguridad debe adaptarse a dichas necesidades. Antes de desarrollar/diseñar la cultura de la ciberseguridad, el principal reto es identificar correctamente cuáles son los problemas globales/internacionales y cuáles son las necesidades locales específicas de una cultura de la ciberseguridad. Los municipios, son las instituciones más cercanas para la ciudadanía, de más fácil acceso, y que a su vez, pueden ser las que mejor puedan hacer de puente desde las nacionales y autonómicas de cara a la población general.

5.1. Estrategia Nacional de Ciberseguridad

El Estrategia Nacional de Ciberseguridad de 2019 fue publicada por el Consejo de Seguridad Nacional con el objetivo de garantizar la seguridad, las infraestructuras y la tecnología que integran el ciberespacio. La estrategia supone una actualización de las amenazas y desafíos (la anterior se remonta a 2013) proponiendo un conjunto de Líneas de Acción y medidas más dinámicas que permiten una rápida adaptación del ecosistema de ciberseguridad nacional. Sin embargo, este documento solo se limita a emitir unas directrices generales y técnicas a las que tendrán que seguir decisiones políticas concretas para ejecutar las líneas de actuación recogidas en ella.

El objetivo principal de esta ENC es garantizar un uso seguro de la red para proteger las libertades y derechos de los ciudadanos y promover el desarrollo socioeconómico. La estrategia establece unas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio; impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional (DSN, 2019).

Los objetivos específicos serían son los siguientes:

- Seguridad y resiliencia de las redes y sistemas de información y comunicaciones del las entidades públicas.
- Uso fiable y seguro del ciberespacio frente al uso malicioso.
- Protección de los ciudadanos y del sector empresarial y social.
- Compromiso y cultura de ciberseguridad y fortalecimiento de las capacidades tecnológicas y humanas.
- Seguridad internacional del ciberespacio.

Dentro de todos los objetivos, cabe a destacar con relación a la educación en ciberseguridad el Objetivo IV. Este objetivo hace referencia al fomento de la cultura de ciberseguridad que, según señala, ha de ser uno de los ejes centrales para contar con una sociedad más conocedora de las amenazas y desafíos a las que se enfrenta. También habla de "*potenciación de las capacidades humanas y tecnológicas, mejorar la ciberseguridad colectiva, difundiendo la cultura de la ciberseguridad con la ayuda de organismos públicos y privados y medios de comunicación, potenciando mecanismos de información y asistencia a los ciudadanos y fomentando espacios de encuentro entre la sociedad civil, administraciones y empresas*" (DSN, 2019). Por lo tanto, hace referencias claras a la educación en ciberseguridad dirigida a la población no-técnica.

Dentro de los objetivos, es de destacar que la estrategia aporta una definición de lo que se considera ciberamenazas. Según la ENC, las ciberamenazas son todas aquellas

disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Se caracterizan por una amplia diversidad de acciones, capacidades y motivaciones. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas. También destaca el carácter internacional y sin fronteras que supone este tipo de fenómeno. Al ser esta la estrategia principal desde el Estado en materia de ciberseguridad, de ella se desprende el objeto de las políticas a otros niveles y un punto de partida para el diseño de las políticas públicas en la materia.

La estrategia también señala que “es responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España”. No establece quienes son los más vulnerables, ni tampoco señala en este punto precisamente a la población que precisamente carece de educación en ciberseguridad. Sí que añade en referencia a las obligaciones y responsabilidades que “*todos los usuarios del ciberespacio deben hacer un uso responsable de la tecnología a su alcance*” y también posteriormente “*El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea, es una responsabilidad compartida”* (DSN, 2019),

La estrategia establece una serie de líneas de acción. Es de especial interés la Línea de Acción 7, que es aquella destinada a desarrollar una cultura de ciberseguridad, directamente encuadrada con el objetivo IV anteriormente descrito. Esta línea de acción se compone de varios puntos entre los que varios tienen una relación directa e indirecta con la educación y cultura en ciberseguridad orientada a la población general:

- Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.
- Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.
- Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.
- Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.
- Promover un espíritu crítico en favor de una información veraz y de calidad y

- que contribuya a la identificación de las noticias falsas y la desinformación Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.
- Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.
- Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

Se desprende de estos puntos que cuando se diseñó la Estrategia y concretamente esta línea, el Estado tiene una clara intencionalidad de usar como soporte para la cultura en ciberseguridad a las entidades privadas, ya sean empresas, organizaciones y medios de comunicación.

El papel de las Estrategias Nacionales

Según Peña & Segura (2014), 31 países incorporan expresamente el componente educativo dentro de sus Estrategias de Ciberseguridad. Sin embargo, cada una tiene distintos enfoques, ya que algunos países buscan más la concienciación en ciberseguridad en personal administrativo y militar. Las estrategias nacionales de ciberseguridad, orientadas a la coordinación y colaboración, tienen un especial énfasis en aspectos a nivel avanzado. Quizás pueda ser debido a esto que la seguridad informática se ha orientado en gran medida a ese nivel.

- Las Estrategias Nacionales de Ciberseguridad existentes basan su funcionamiento en una serie de pilares básicos y líneas de actuación que son (Coz, 2015):
- Un liderazgo desde el Estado en materia de Ciberseguridad.
- La creación de una estructura organizativa de control.
- El desarrollo de foros de comunicación para la formación y concienciación.
- El impulso económico público-privado a la Ciberseguridad.
- La política exterior en materia de Ciberseguridad.
- La normalización y legislación de la Ciberseguridad.
- La gestión del I+D+i sobre Ciberseguridad.

En el caso de Estados Unidos, las estructuras y capacidades desarrolladas para la defensa de su Ciberespacio han tomado la delantera al resto de países. Desde la primera década del siglo XXI se han ido elaborando diferentes propuestas gubernamentales tomaron forma con la aprobación de la Estrategia de Seguridad Nacional en el Ciberespacio (2003). Posteriormente, en 2009, se revisó la política estadounidense en el Ciberespacio, desde la cual surgieron un conjunto de líneas de actuación urgentes, entre las que destaca la siguiente: Realizar campañas nacionales de concienciación y formación. En 2010, el Department of Homeland Security (DHS) lanzó la campaña “Stop, think, connect”. Esta campaña tiene un carácter estatal y tiene como objetivo fomentar la formación y concienciación en materia de Ciberseguridad en todos los ámbitos de la sociedad estadounidense (Coz, 2015).

5.2. Instituciones

Las instituciones que se encuentran implicadas en materia de Ciberseguridad son amplias y abarcan varios niveles. Algunas se centran más en la coordinación, otras en la persecución del ciberdelito, en la prevención o en el análisis del ámbito. En primer lugar, las instituciones internacionales en las que España participa con relación a la ciberseguridad son las siguientes:

- Unión Europea (ENISA, Eurojust y Europol)
- Organización del Tratado del Atlántico Norte (OTAN)
- Naciones Unidas y en sus foros derivados como el Foro de Gobernanza de Internet (IGF)
- Organización para la Seguridad y la Cooperación en Europa (OSCE),
- Organización de Estados Americanos (OEA)
- Foro Global de Expertos en Ciberseguridad (GFCE)
- Coalición por la Libertad en Internet (FOC)
- Centro Europeo de Excelencia para contrarrestar las Amenazas Híbridas (Hybrid CoE)
- Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCD CoE).

A nivel Estatal, la estructura orgánica en materia de ciberseguridad venía ya establecida en la Estrategia Nacional de Ciberseguridad de 2013 y en la Ley de Seguridad Nacional. La Estrategia de 2019 (DSN, 2019) lo que hace es complementar el organigrama con las políticas de la UE:

- Consejo de Seguridad Nacional
- Comité de Situación
- Consejo Nacional de Ciberseguridad
- Comisión Permanente de Ciberseguridad
- Foro Nacional de Ciberseguridad
- Autoridades públicas competentes y CSIRT de referencia.

A estas instituciones y organismos habría que añadir el INCIBE, la OSI, IS4K, el ONTSI, el Mando Conjunto de Ciberdefensa, las FCSE, Unidad de Coordinación de Ciberseguridad (UCCIBER), el Gabinete de Coordinación de Estudios y la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad.

INCIBE

Según su página web, el Instituto Nacional de Ciberseguridad de España (INCIBE), es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (INCIBE, 2023). Es una institución de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. También es una entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Por lo tanto, el INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. En cuanto a su misión, viene fijada en su Consejo de Administración de acuerdo a la estrategia general del Gobierno de España y la legislación vigente en materia de ciberseguridad. Sus principales objetivos son:

- Mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España.
- Proteger y defender a los ciudadanos, menores y empresas privadas de España.
- Potenciar la industria española de ciberseguridad.
- Impulsar la I+D+i española en ciberseguridad.
- Identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad.

Con relación a la educación, destacan que su misión es "*ser un motor para la transformación digital de la sociedad, protegiendo a ciudadanos, menores y empresas privadas en España*" y que "*el nivel de ciberseguridad de ciudadanos y empresas se sitúe entre los cinco mejores del mundo*". El INCIBE incluye el INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España. Se encuentra coordinado con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información (INCIBE, 2023). El INCIBE gestionó un total de 109.126 incidentes de ciberseguridad en España durante el año 2021. Los incidentes tipo malware son los más frecuentes, con un porcentaje del 29,88%, respecto del total; seguido de los fraudes, con un 28,60% (López et al., 2021).

Oficina de Seguridad de Internauta

La Oficina de Seguridad del Internauta (OSI) es un servicio del Gobierno para proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectarnos al navegar por Internet. Este organismo que depende actualmente del INCIBE y del Ministerio de Asuntos Económicos y Transformación Digital. Su principal función es ofrecer información y servicios de ciberseguridad a sus visitantes, utilizando para ello un lenguaje accesible, para que cualquier ciudadano pueda entender sus contenidos, independientemente de la edad, la formación el grado de conocimientos (Grupo Atico34, 2020).

Su objetivo es elevar la cultura de seguridad, prevenir, concienciar y formar, proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en Internet. Al mismo tiempo, impulsan la detección y denuncia de nuevas amenazas en la red, de fraudes, estafas online o de cualquier otro tipo de ataque de Seguridad Informática. Entre los servicios que ofrece la OSI, encontramos la sección "Protégete"; aquí tenemos varios apartados con artículos y posts para saber cómo protegernos de las principales amenazas respecto ciberseguridad.

Internet Segura for Kids

Dentro de la OSI, existe el denominado Internet Segura for Kids (IS4K), un portal especializado en infancia y juventud y los riesgos que pueden encontrar y enfrentar en Internet. Esta web, también depende del INCIBE, ofrece diferentes recursos y guías tanto para familias como para educadores. Cuenta con su propio blog de actualidad, con artículos enfocados a los riesgos que acechan en la Red, especialmente para niños y adolescentes, cómo reconocerlos y evitarlos, así como recursos y programas propios (Grupo Atico34, 2020).

CERT

Por otro lado, los CERT de ámbito autonómico (CSIRT-CV, CESICAT, ANDALUCIA-CERT), en el ámbito de sus funciones, también han desarrollado programas de concienciación basados en portales donde se puede encontrar información relativa a riesgos y buenas prácticas. Merece la pena destacar la gran labor desarrollada por el CSIRT-CV en este ámbito. Es un centro muy activo que cuenta con numerosos cursos (26) e informes (27) que han tenido muy buena aceptación en la Comunidad Valenciana (CSIRT-CV, 2023).

A pesar de todo, según (Pulido & Rosell, 2017), para tener éxito y mejorar nuestra cultura global de ciberseguridad hay que pensar que trabajamos con personas, disponer del apoyo institucional y los recursos para desarrollar todos los planes que son necesarios, alinearlos con los intereses del Estado y aglutinar en a todos los interesados (empresas, Administración y empresas específicas de ciberseguridad) para definir las líneas de trabajo más apropiadas para garantizar el éxito. Sin embargo, la descoordinación entre los diferentes organismos nacionales es una debilidad para la defensa del Ciberespacio del país (Coz, 2015).

Observatorio Nacional de Tecnología y Sociedad (ONTSI)

Su fin es analizar los ciberriesgos a los que se enfrentan la ciudadanía, las empresas y las estrategias de gestión de ciberseguridad y privacidad (ONTSI, 2022). También tiene como prioridad conocer el nivel de confianza digital y seguridad en España.

Analizando los datos del estudio realizado por la ONTSI (2022) sobre la percepción de la ciudadanía sobre este tipo de instituciones, encontramos que el 81% de los individuos consultados creen que las entidades administrativas han de implicarse más en mejorar la seguridad en Internet. Otro dato muy significativo es que solamente el 18,4% de quienes han tenido algún problema de ciberseguridad en el segundo trimestre de 2021 han recurrido a los mecanismos de ayuda (teléfono 017 del INCIBE). El semestre anterior solo el 13% las personas que aprovecharon este mismo mecanismo. También es de destacar que el 42% de usuarios/as sienten dificultades para poder acceder a la información de cómo navegar de una forma segura.

Algunas campañas emitidas desde las instituciones como el INCIBE para concienciar sobre ciberamenazas apenas llegan a la población, de hecho, el 49% de las personas encuestadas en 2021 no conoce ninguna en concreto. Por ejemplo, la campaña "*Hoy es un anuncio, mañana no*" dirigida a concienciar sobre el ransomware tan solo ha sido reconocida por el 10,8% de las personas encuestadas. Otros ejemplos serían la del IS4K sobre el ciberacoso en la infancia (25%); "*Estate atento*", del SEPE, para prevenir

el phishing (18,6%); De control parental de IS4K (15,7%); El servicio 017 para ayuda sobre ciberseguridad, del INCIBE, es conocido por el 15,4% de los individuos encuestados. El único dato positivo es el aumento del uso de estos servicios en el año 2021, que pasó del 13% en el primer semestre al 18,4% en el segundo semestre.

Mando Conjunto de Ciberdefensa

En cuanto al Mando Conjunto de Ciberdefensa, tiene como misión, definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa del propio Ministerio de Defensa. En base a este cometido, ha coordinado y puesto en marcha, el Plan de Concienciación en Ciberdefensa (CONCIBE) y ha explorado programas dirigidos a su ámbito de actuación y basados en cursos de sensibilización en la plataforma e-learning del MINISDEF, que incluso incorporan técnicas de gamificación orientadas a mejorar los resultados prácticos (Pulido & Rosell, 2017).

Fuerzas y Cuerpos de Seguridad del Estado

la Policía Nacional y la Guardia Civil han puesto en marcha diversas iniciativas durante años en materia de educación y concienciación en ciberseguridad. Han tratado de concienciar a los niños en los colegios sobre los peligros que encierra la red mediante visitas y charlas a centros públicos. En ellas, se exponían las amenazas existentes y las medidas de seguridad básicas para poder proteger a los menores. La finalidad no es solamente concienciar y sensibilizar a los niños y adolescentes, sino también que adquieran herramientas para poder defenderse.

En el caso de la Guardia Civil, en su Plan de Acción Operativo, se desarrolla, diferentes líneas de acción para el desarrollo y fomento de la cultura de ciberseguridad (Congreso, 2021):

- Elaboración de un Plan Permanente de Divulgación para la Prevención contra la Cibercriminalidad.
- Promoción del desarrollo de campañas específicas de información y divulgación sobre determinadas tipologías de delitos cometidos a través de la red.
- Impulso de las campañas de sensibilización y actuación sobre la prevención de la cibercriminalidad en empresas, en especial PYMES y MICROPYMES.
- Renovación y actualización de los planes dirigidos a concienciar acerca de los riesgos que presenta el uso del ciberespacio en los centros educativos, en centros sociales y otros colectivos vulnerables cibernéticamente que se detecten.

Además, la Guardia Civil, a través de sus redes sociales, realiza campañas específicas de difusión de contenidos acerca de aquellas modalidades delictivas que presentan una mayor incidencia. Estas acciones permiten identificar inquietudes, amenazas y problemáticas presentes en el sector empresarial, aportando medidas eficaces para la prevención y mitigación de los ciberdelitos con mayor impacto. También se están adecuando los planes específicos de la Secretaría de Estado de Seguridad a la actual realidad delictiva, de forma que la ciberseguridad se perciba como un elemento esencial a tener en cuenta por los ciudadanos.

Gabinete de Coordinación de Estudios

Es el órgano de apoyo y asesoramiento para la coordinación y supervisión de actividades relacionadas con la protección, de infraestructuras críticas, coordinación con instituciones europeas y canal de comunicación entre los CSIRT (Centros de Respuesta e Incidentes Cibernéticos) y la Secretaria de Estado de Seguridad (H50DigitalPolicial, 2023).

Unidad de Coordinación de Ciberseguridad (UCCIBER)

Con respecto a las actividades de formación en este ámbito de la Unidad de Coordinación de Ciberseguridad, se han desarrollado las siguientes (Congreso, 2021):

- Curso in Company de redes informáticas.
- Curso in Company de Sistemas Operativos. Estructura de ficheros de audio y administración y auditoría.
- Planificación y dirección de actividades de inteligencia de fuentes abiertas en el Ciberespacio.
- Curso de Auxiliar de Estadística de la Guardia Civil.
- Curso de Radio tecnología hacking UCB.
- Curso de introducción a la investigación de delitos relacionados con el uso de la informática.
- Curso de Blockchain.
- Curso de Esquema Nacional de Seguridad

5.3. Iniciativas y Proyectos implementados

Las campañas para reducir la percepción de barreras relacionadas con la seguridad digital y el refuerzo de la creencia en la eficacia del antimalware, parecen ser medidas políticas claras y rentables para aumentar el compromiso con la ciberseguridad (Dodel

& Mesch, 2017). Se recomienda aumentar la circulación de la información relativa a las ciberamenazas (sobre todo en la gravedad de las consecuencias), reforzar las creencias en la confianza de los usuarios en sus capacidades para protegerse y, especialmente, en el antimalware como estrategias preventivas de bajo coste y poco disruptivas, ya que han demostrado aumentar la seguridad y funcionar contra estas amenazas.

También se han ido implementando planes y estrategias para combatir la Brecha digital, que se configura como un elemento significativo en las regiones rurales fuera de las ciudades. Surge según la zona geográfica, separando urbes y áreas rurales. Existe en las primeras una mayor posesión de tecnologías (Astorga-Aguilar & Schmidt-Fonseca, 2019). Estas diferencias, también tendrán su influencia en la formación, uso responsable y la incidencia en ciberdelincuencia. Según Amador (2017) también los niveles de educación en ciberseguridad van ligados a ello, por lo que el nivel de conocimiento de los peligros y la capacitación para hacerles frente será menor en el rural que en las ciudades. Las estrategias institucionales dirigidas a combatir la brecha digital serán, por lo tanto, necesarias para poder equilibrar esta asimetría entre el mundo rural y urbano.

Durante 2021 y el primer semestre de 2022 se ha dado un impulso fundamental a las inversiones del Plan de Recuperación en el ámbito digital en conectividad, I+D, digitalización de la Administración y de las pymes. Se ha llevado a cabo una importante transferencia a las Comunidades Autónomas y ayuntamientos para la digitalización del sector público y el impulso de las competencias digitales a la ciudadanía. También podemos encontrar la agenda España Digital, que es la hoja de ruta para la transformación digital del país, una estrategia ambiciosa para aprovechar plenamente las nuevas tecnologías y lograr un crecimiento económico más intenso y sostenido, rico en empleo de calidad, con mayor productividad y que contribuya a la cohesión social y territorial. Por su parte, la Agenda 2030 para el Desarrollo Sostenible, es un plan de acción en distintos ámbitos para la mejora de la sociedad. Este plan estratégico prevé actuaciones dirigidas a mejorar la calidad del empleo y una clara apuesta por la digitalización para la mejora de la eficacia de las actuaciones.

A través de las Agendas Digitales, los distintos Gobiernos europeos están encaminando la sociedad a una nueva era de digitalización e implementando las TIC en todos los ámbitos de la sociedad. Sin embargo, también surge esta necesidad de conseguir este espacio seguro que acompañe al desarrollo tecnológico de la sociedad digital, por todo ello, las Agendas Digitales también están incluyendo la seguridad como un pilar base. Por su parte, en la Agenda Digital europea, se incluye como tercer campo de acción (de los 7 que la constituyen), el fomento de la confianza y seguridad en Internet, la acción clave “conseguir una política de seguridad reforzada y de alto nivel” y “medidas para

combatir los ciberataques (UE, 2010). Se muestra un interés claro de los distintos estados europeos por encaminar a la sociedad hacia un uso seguro en el ámbito digital.

En cuanto a la Agenda Digital Española, tiene como objetivo impulsar acciones concretas para "*Reforzar la confianza en el ámbito digital*", en donde se apuesta la concienciación y sensibilización de la sociedad en la ciberseguridad con un enfoque hacia las personas. En el ámbito de actuación de la agenda se desarrolla el «Plan de confianza en el ámbito digital», que a su vez tiene cinco ejes estratégicos: Experiencia digital segura; Oportunidad para la industria TIC; Nuevo contexto regulatorio; Capacidades para la resiliencia; Programa de excelencia en ciberseguridad (Gobierno de España, 2013). Se configura de este modo, una base Estatal que servirá de guión para definir las grandes líneas de la educación en ciberseguridad. Además, esta agenda va en consonancia con un marco europeo que permitirá homogeneizar este esfuerzo en los distintos países implicados.

También habría que destacar el kit de concienciación desarrollado por el INCIBE (2020) y que ha puesto a disposición de las empresas. El kit propone una serie de prácticas y materiales a distribuir. La primera fase, consistiría en lanzar un ciberataque dirigido, dentro de la empresa, con un fichero infectado con malware inocuo y cuyo vector de infección sería el correo electrónico o una memoria USB. INCIBE incluso recomienda los mensajes y ficheros a utilizar. Una vez realizada esta primera fase, ya se pasaría una fase formativa en la que se distribuyen materiales como pósteres o trípticos, que también han sido preparados por INCIBE. Se daría continuidad posteriormente a esta tarea mediante consejos de ciberseguridad de periodicidad mensual.

Por otra parte, desde el tercer sector, iniciativas como cibervoluntarios han desplegado talleres, seminarios, cursos y formaciones sobre ciberseguridad en todo el territorio. Son una ONG centrada en impulsar una transición digital inclusiva y eliminar la brecha digital. Se centran en la creación y gestión de una red de voluntariado tecnológico, facilitando formación gratuita en competencias digitales. Cuentan con una red de más de 2800 personas cibervoluntarias y colaboran con más de 1600 organizaciones (Cibervoluntarios, 2023). También mediante fondos públicos, tanto del FSE, como desde el Gobierno y las Comunidades Autónomas, distintas ONGs han financiado proyectos para combatir la brecha digital, incluyendo dentro de sus programas, capacitación en ciberseguridad en población general. Cada una de ellas, centrándose en su población objetivo (población migrante, con discapacidad, personas de especial vulnerabilidad, menores de edad, etc.)

Un ejemplo de intervención del tercer sector en el área de la brecha digital es el caso del PILOTEM. El proyecto, desarrollado en la Comunidad Valenciana e iniciado en agosto de 2022, implica a más de 100 entidades del tercer sector y tiene como eje principal la lucha contra la brecha digital (Generalitat Valenciana, 2022). Se configura como un proyecto de investigación y de intervención social. En el proyecto, técnicos de diversos perfiles del ámbito social están poniendo en marcha talleres, cursos formativos e intervenciones individuales. En ellos, un eje fundamental es la formación y educación para reducir la brecha digital. Entre los contenidos mínimos, se ha incluido la ciberseguridad para poder educar en medidas de protección. Por ejemplo, la Comisión Española de Ayuda al Refugiado adapta estos contenidos a su población objetivo: personas migrantes, solicitantes de asilo y refugiadas. Lo mismo sucede con otras como Secretariado Gitano, ACCEM, CEPAIM, Cruz Roja, Cáritas, etc.

En cuanto a las medidas preventivas que existen en el ámbito internacional para proteger a los menores de edad de los ciberdelitos, se han adoptado, tanto a nivel global, por la Organización de Naciones Unidas, como por otras organizaciones y Estados. Los instrumentos se centran más en la respuesta y sanción, sin embargo, han surgido algunas medidas preventivas que protegen a menores de edad contra ciberdelitos: Declaración de Río 2008; SaferNet; programa ThinkUKnow; Línea de ayuda a los menores a través del número de teléfono, etc. las cuales han sido impulsadas por la Organización de Naciones Unidas; Brasil; Reino Unido y la organización internacional I-Safe4; Unión Internacional de Telecomunicaciones y la Cumbre Mundial sobre la Sociedad de la Información (CMSI) celebrada en Túnez en noviembre de 2005. (Avila, 2018)

En relación a los riesgos para los menores de edad en el ciberespacio, se han creado estrategias en las que han participado directamente los menores de edad. Tejedor-Calvo & Pulido-Rodriguez (2012), señalan el programa ThinkUKnow del Reino Unido y la organizacion internacional I-Safe4. Estos dos, son ejemplos que pueden ser utiles para el profesorado, ya que se puede consultar los contenidos diseñados para los padres, profesores, educadores y menores de diferentes edades y establecerlos como modelos.

6. Medios para educar

6.1. Agentes responsables en la educación

Tal y como se ha expuesto, es el Estado el que tiene las competencias en materia de seguridad y el que debe garantizar la protección de la sociedad ante las ciberamenazas y la ciberdelincuencia. No obstante, el tejido público que tiene responsabilidad en la protección y la prevención es mayor que el que forman las Fuerzas y Cuerpos de

Seguridad del Estado. Desde las distintas administraciones como son las comunidades autónomas, los ayuntamientos, colegios e institutos públicos, universidades, etc. también pueden implementar proyectos y planes educativos para prevenir a la ciudadanía. En cada una de estas instituciones se debe realizar un mayor esfuerzo por preparar a sus trabajadores (que son los conectan a las instituciones con la ciudadanía) en transmitir los conocimientos y la concienciación en las ciberamenazas y la protección en la red. Como se desarrollará más adelante, jugarán un papel clave los centros de primaria y secundaria, con el profesorado como protagonista y agente necesario en la tarea. Por lo tanto, es claro el papel primordial que tiene el sector público en la educación en ciberseguridad y ciberdelincuencia, sin embargo, no es el único.

El sector privado, en coordinación con el sector público (Pulido & Rosell, 2017) se muestra un excelente aliado en el objetivo de educar para prevenir. Las empresas y autónomos son los grandes afectados en la ciberdelincuencia, por lo que también efectúan inversiones en preparar y educar a sus plantillas y personal para estar protegidos. Esta protección no solo se limitaría a tener personal técnico especializado, sino en que la totalidad, o parte de ella, conozca los riesgos y las medidas básicas de protección. Por poner un ejemplo, un empleado al que hacen phishing y le engañan para efectuar una transferencia a la cuenta de un ciberdelincuente en vez de a un proveedor legítimo. Este tarea educativa repercutiría en la población general al tener un enorme tejido empresarial dedicado a prevenir la ciberdelincuencia, teniendo beneficios en la ciudadanía que podrá usar esos conocimientos para su autoprotección no solo en el puesto de trabajo, sino en su ámbito privado y doméstico.

Este sector privado no es el único aliado de las instituciones públicas, el tercer sector, formado por un gran número de organizaciones y entidades, intervienen de forma directa con diversos colectivos y poblaciones. Este contacto que ejerce una función social básica podría tener un mayor rol en lo que se refiere a la educación en ciberseguridad. Muchas de ellas ya se encuentran implementando contenidos educativos dirigidos a reducir la brecha digital y la alfabetización digital. Un ejemplo de ello es el ya mencionado Proyecto Pilotem de la Comunidad Valenciana. Ha sido financiado por el FSE y que ha puesto en marcha proyectos sociales en más de 100 entidades del tercer sector (Generalitat Valenciana, 2022). Las entidades pertenecen a diversos sectores segun la población con la que trabajan: población con discapacidad, migrante, enfermedades mentales, personas sin recursos, etc. La coordinación entre tercer sector y las instituciones fue clave para poder transmitir toda la información y metodologías adecuadas en materia de educación en ciberseguridad.

Finalmente, tal y como se ha desarrollado en el apartado de políticas públicas en materia de ciberseguridad, existen diversas instituciones especializadas que tienen como su objetivo primordial la educación en ciberseguridad, por ejemplo el INCIBE o la OSI. También las FCSE imparten charlas en escuelas y centros educativos para concienciar y educar. Sin embargo, más allá de las iniciativas y proyectos puestos en marcha por todas estas instituciones, la función de educar en ciberseguridad debe ser transversal y estar presente en todas las instituciones educativas con menores. Es por ello que habrá 2 agentes clave responsables de la educación, son las madres y padres en primer lugar, y los docentes de centros educativos de primaria y secundaria.

Padres

La formación en ciberseguridad enfocada en el uso correcto de redes sociales, tanto en la infancia y la adolescencia, recae en diferentes entes participantes en la acción didáctica: personal docente, estudiantes, padres y madres de familia, comunidad educativa e integrantes del contexto. (Pérez, 2016). Son los que deben poner en marcha las acciones educativas, familiares y comunitarias que promuevan el uso seguro en internet y el ciberespacio. La formación debe estar integrada en el día a día en el hogar, de forma integrada y llevando a cabo el ejemplo. Incluso, bajo esta idea, también señalan un elemento interesante, y es la idea de que los propios niños también sean partícipes en la educación. El modo de llevarlo a cabo sería que los menores enseñen a los adultos y no solo los adultos a los menores, para que así la eduación no sea vista como algo impuesto y también para mejorar la motivación. Además, esta técnica permitiría que los menores muestren sus intereses y sus capacidades, para que la formación esté más monitorizada y se pueda percibir mejor hacia donde se dirige (Davara-Fernandez, 2019)

También Astorga-Aguilar & Schmidt-Fonseca (2019) señalan que la educación en ciberseguridad, especialmente en redes sociales, debe recaer en distintos actores sociales: el personal docente, los estudiantes, comunidad educativa, integrantes del contexto y padres y madres. Además de la educación, también se deben llevar a cabo campañas comunitarias y educativas para promover la concienciación (Pérez, 2016), lo que es fundamental si lo que se persigue es implementar y fomentar el uso de los medios seguros, y no solamente su conocimiento. Para ello, será fundamental la construcción de una metodología por parte de los padres y madres, de forma que desde el hogar se colabore con el sistema formal de enseñanza en esta temática. Los padres también necesitan recibir la formación, tanto como receptores de la formación, como transmisores a sus hijos (Davara-Fernandez, 2019).

El fenómeno es de especial transcendencia si tenemos en cuenta las edades a las que se comienza a usar Facebook, Snapchat y Whatsapp, que están restringidas a mayores de 13 años, o Instagram, que es de 14 años en adelante (y si no se da el caso de que las creen antes, de modo ilegal y sin supervisión ninguna). También destacar que las grandes compañías se aprovechan del desconocimiento para absorber una enorme cantidad de datos, que si las conocieran detalladamente, quizás no las habrían permitido. Por lo tanto, al peligro en sí del ciberdelito, se suma un problema de la privacidad y los datos personales. Existen cláusulas donde los usuarios dan acceso abiertamente a su información personal, información del dispositivo que se emplea para acceder, información sobre ubicación, contactos, control sobre la cámara, e incluso algunas redes declaran derecho sobre las fotografías que suba a la red, como en el caso de Snapchat (Astorga-Aguilar & Schmidt-Fonseca, 2019).

El caso de la aceptación de las condiciones y cláusulas por parte de menores, se da en parte porque los padres permiten que sus hijos menores de edad otorguen ese derecho, o simplemente por dejadez a la hora de analizar las condiciones. Según Echeburúa y De Corral (2010), la figura de los padres dentro del proceso educativo en ciberseguridad es clave, pero también la de los hijos sobre los padres. Esta relación bidireccional consiste en que los hijos pueden enseñar a los padres el uso de las nuevas tecnologías, que en muchos casos tienen más conocimientos que ellos. Por su parte, los padres a los hijos pueden, y deben, enseñarles a usarlas en su justa medida (y se entiende que también de un modo responsable), a leer y conocer las condiciones y permisos que implica, los peligros existentes, la importancia de configurar la privacidad y en general, a preocuparse por la utilización sensata y responsable de las mismas.

También en Astorga-Aguilar & Schmidt-Fonseca (2019) van en esta dirección cuando afirman que el papel de los padres va en doble dirección. Los jóvenes pueden enseñar a los padres a emplear las TIC y los padres deben enseñar a los jóvenes a usarlas de forma responsable. Por lo tanto, se desprende la idea de que por parte de los jóvenes prima un conocimiento más técnico, ya que en muchas ocasiones se muestran más conocedores y capaces de usar las nuevas tecnologías, pero de un modo inmaduro e irresponsable. Por el contrario, los padres y adultos en general, en muchas ocasiones se ven más limitados en los aspectos técnicos, pero ponen el peso en la responsabilidad, la seguridad y la conciencia sobre los peligros que pueden suponer esas tecnologías. De esa educación bidireccional y retroactiva, se puede dar, por lo tanto, una doble educación, técnica y responsable, de la que puedan beneficiarse ambas partes.

Estos autores afirman que es de suma importancia el acercamiento a los padres para conocer sus medios y conocimientos sobre ciberseguridad, ya que son ellos los que tendrán un papel relevante en la formación y educación de sus hijos. A esta idea se le debería sumar que son ellos, los padres, los que conocen mejor las particularidades de sus propios hijos en cuanto a aprendizaje, ritmos y tiempos. Es por ello que, más que en contenido de aprendizaje, el papel que pueden tener es muy importante en cuanto a la capacidad de educar de una forma más individualizada. En la misma línea van Arab y Díaz (2015) cuando señalan la importancia de que sean los adultos los que se autoeduquen en las nuevas tecnologías para poder llevar a cabo ese monitoreo, acompañamiento y supervisión. También que estos conocimientos sean interiorizados con el aprendizaje, consiguiendo que los menores lo hagan como propio, de este modo, la información pasaría a sus estructuras cognitivas con el fin de identificar peligros en la red (Astorga-Aguilar & Schmidt-Fonseca, 2019).

Los padres también tendrán un papel crucial como mediadores del proceso educativo, ya que pueden facilitarles la construcción de significados e integrar la información para ser asimilada con sus conocimientos previos. Son ellos los que deben analizar las características del entorno y el lugar donde se desarrollan, así como las personas con las que interactúan. Cabría cuestionarse, tras la afirmación de estos autores, cuáles son las herramientas y conocimientos que pueden tener en muchos casos los padres para poder implementar ese control. Si ellos han tenido una formación para poder transmitir conocimientos o, al menos, supervisar a sus hijos.

Es aquí donde llega también la puntualización de Fernández Montalvo et al. (2015), sobre cómo van a poder realizar toda esa supervisión si ni tan siquiera se cuenta en muchos casos unos criterios claros sobre el uso adecuado de internet y los dispositivos. Es más, no se cuenta tampoco en muchos casos con indicadores claros sobre el mal uso de los mismos. señalan la necesidad de "*desarrollar metodologías prácticas y contextualizadas, innovadoras y significativas, que permitan dar solución a problemáticas relacionadas con los peligros en la red a los que se enfrentan*". El papel de los padres, es también de mediador en el proceso, dotando de significado a todo ese conocimiento, e integrarla con los conocimientos previos para una mejor asimilación. Todo esto implica la necesidad de nuevo de los adultos de educarse para educar. Arab y Díaz (2015) recalcan que "*es indispensable por parte de los adultos autoeducarse y aprender todo lo relativo a internet, aplicaciones y redes sociales"*

Como beneficio de esta mediación, pueden mejorar la comprensión y uso de los aprendizajes para transferir la solución de ciertos problemas a otros nuevos o a otros contextos. Esto es interesante desde el punto de vista en que los padres pueden ir más

allá en la mera transmisión de conocimientos sobre ciberseguridad. Pueden ayudar a que esa información sea asentada y "digerida" por sus hijos para una mejor absorción e integración, sobre todo ayudada desde el actor principal en su educación, los padres, quienes conocen mejor que nadie las particularidades individuales de sus hijos y sus capacidades y tiempos en el aprendizaje.

Finalmente, la importancia del rol de los padres en el proceso se visibiliza precisamente por los casos en los que están ausente. Es el caso de los huérfanos digitales, que serían aquellos nativos digitales que no tienen apoyo de sus padres, e incluso sus hijos manejan mejor que su propios padres las herramientas digitales. Es preocupante que incluso en estos casos, tengan gran dominio de las herramientas, pero al mismo tiempo carezcan de la concienciación y de las nociones básicas en materia de seguridad, ya que, por un lado, aumentarán la probabilidad de estar expuestos a los peligros y, por otro lado, carecerán de las herramientas para defenderse. Es por ello, que los padres tienen un papel relevante para que sus hijos no sean huérfanos digitales, sino nativos digitales conscientes y formados (Davara-Fernandez, 2019).

Profesores

Al igual que a los padres, a los profesores se les debe educar como receptores y como emisores, teniendo en cuenta que en algunos casos (especialmente, los de más avanzada edad) no tienen los conocimientos adecuados en la materia e incluso se ven sobrepasados por sus propios alumnos. En Davara-Fernandez (2019) incluso se propone formar a toda la plantilla docente de los centros de forma periódica. Este carácter periódico se debería a la rápida velocidad a la que evoluciona la ciberseguridad, y en cuanto al actor activo que lleve a cabo la formación, puede ser un profesor que tenga la formación necesaria para transmitirla a sus compañeros, o impartirla un experto externo. En este punto, es de destacar que los autores señalan "*que en todo caso, domine el campo de la educación para que personalice los contenidos a la realidad del centro*". Encontramos aquí un elemento imprescindible, la capacidad de personalizar la materia y también la capacidad para educar que debe tener la persona encargada de impartir la formación. Se desprende que, para ellos, no puede ser únicamente una persona experta en ciberseguridad, sino una persona preparada para la enseñanza.

El papel de los profesores del sistema educativo es un punto central ya que son ellos los que tienen más experiencia a la hora de educar, transmitir el conocimiento, diseñar elaborar la programación, usar técnicas y herramientas educativas, pero sobre todo, los que más cercanía tienen a los menores y más saben adaptar los contenidos y materiales a la población objetivo. Cabría en este punto plantear si la mejor herramienta será formar

a los profesores en los contenidos y conocimientos más técnicos, para que luego sean ellos los que desplieguen su "saber hacer" en materia educativa en sus aulas. Por lo tanto, quedarían cubiertos así los 2 principales pilares sobre los que se debe sostener la educación en ciberseguirdad (el carácter técnico y el carácter didáctico/pedagógico). En esta misma línea también advierten en Davara-Fernandez (2019), cuando dicen que es necesario un cambio de mentalidad y un esfuerzo en formar a los profesores en TIC para poder integrar esta área en el currículum escolar, ya que de lo contrario, "*no hacerlo puede salir mucho más caro*"

La reivindicación de una educación en ciberseguridad en la educación secundaria está presente en otros países. Por ejemplo, en Martínez-López & Martínez-López (2018), resaltan la importancia de implementar un plan de estudios con una asignatura orientada a la seguridad informática en México. Proponen que desde las instituciones públicas, y especialmente desde la secretaría de Educación de México, se incorporen a los programas de estudio en los niveles de educación primaria, secundaria y bachillerato, una asignatura enfocada a la "seguridad de la información". Esta propuesta la justifican mediante la incorporación y necesidad de las TIC en la sociedad. Por su parte, a nivel europeo, el informe presentado por la Comisión Europea que establece un Marco europeo para la competencia digital de los docentes, señala que las medidas de protección no pueden limitarse a contemplar barreras externas. La prioridad debería ser empoderar a los usuarios para que dispongan de recursos para identificar y gestionar los riesgos de forma autónoma (Redecker, 2017).

El informe del Centro de Investigación EdWeek Research Center (2020) afirma que los alumnos de K-12 deben conocer conceptos, principios y prácticas de ciberseguridad para protegerse en línea, pero el problema es que muchos estudiantes no están preparados porque sus profesores no tienen conocimientos sobre métodos, prácticas y conceptos de ciberseguridad. En una encuesta realizada por este Centro, el 91% de los profesores indican que saben al menos un poco sobre ciberseguridad, mientras que sólo el 10% sabe mucho. Estos datos son un reflejo de la problemática: los educadores no pueden enseñar a sus alumnos sobre ciberseguridad a menos que ellos mismos sepan algo al respecto. El estudio también señala un punto importante en referencia a las diferencias provocadas por la brecha digital "*Los esfuerzos de creación de conocimiento son especialmente críticos en áreas donde los niveles de conocimiento son más bajos, como los distritos escolares de alta pobreza, los desiertos de ciberseguridad y también entre los profesores, que informan de niveles más bajos de conocimiento que los administradores*" (EdWeek Research Center, 2020).

6.2. Perfiles diana de la educación

"*Identificar a las poblaciones de riesgo es allanar el camino hacia la mejora de la ciberseguridad*" (Livingstone & Helsper, 2013).

Según el informe sobre la cibercriminalidad en España (López et al., 2021), la mayoría de las víctimas de ciberdelincuencia pertenecen son hombres (51,9%), tienen entre 26 a 40 años, y principalmente son víctimas de los delitos de fraudes informáticos, amenazas y coacciones y falsificación informática. Sin embargo, si se analiza la distribución global de incidentes conocidos por ámbito y sexo, las mujeres exceden en porcentaje a las víctimas de sexo masculino cuando se trata de hechos relacionados con la falsificación informática, acceso e interceptación ilícita (descubrimiento y revelación de secretos), contra el honor (injurias) y los delitos sexuales. Todo ello da una primera aproximación hacia donde priorizar el objetivo de educar, tanto en edad como en los tipos de delitos que prevenir.

Por otra parte, se publican datos relativos a las victimizaciones desglosadas por tipología penal. Entre los principales hechos conocidos cometidos se encuentran las estafas, las amenazas y la usurpación de estado civil. En relación con la nacionalidad de la víctima, el 87,5% de ellas son españolas, y el 12,5% restante extranjeras. En el conjunto de estas víctimas de extranjeras, las que aúnan valores más elevados son las procedentes de Marruecos, Rumanía, R. Dominicana, Venezuela y Colombia. Es de gran interés tener las variables sociodemográficas en cuenta a la hora de poder sectorizar la educación, determinar la incidencia que afecta a las distintas poblaciones, y sobre todo, poder adaptar dicha educación al perfil de las personas que la van a recibir. En la tabla se muestra los porcentajes en intervalos de años. Se puede observar que la población adulta, de entre 26 y 65 años, es la que sufre el grueso de la victimización (76,46%).

Edad	N	Porcentaje
Menores de edad	3.733	1,55%
De 18 a 25 años	32.604	13,59%
De 26 a 40 años	69.544	29%
De 41 a 50 años	58.239	24,28%
De 51 a 65 años	55.602	23,18%

Mayores 65 años	20.109	8,38%
TOTAL	239.831	100%

Fuente: Informe sobre la cibercriminalidad en España (López et al., 2021)

En Dodel & Mesch (2018) investigaron cómo las diferencias sociodemográficas se reflejan en las habilidades de ciberseguridad digital y evaluaron si estas diferencias afectan al compromiso con los comportamientos preventivos. Encontraron que las habilidades de ciberseguridad y el compromiso con el comportamiento preventivo están distribuidos de forma desigual según las dimensiones sociales tradicionales de la desigualdad, como el género, la edad y la educación. Por lo tanto, la adopción de acciones para prevenir las ciberamenazas se ve afectada por la posición que uno ocupa en el sistema de estratificación social y las desigualdades sociodemográficas. También que la posición social determina no solo el nivel de conocimientos informáticos y de Internet en general, sino también el nivel de conocimientos de ciberseguridad. El reenfocar el problema de la ciberseguridad en las desigualdades digitales, puede ayudar a los gobiernos y las organizaciones a identificar a las poblaciones en riesgo digital.

Niños y adolescentes

Los menores son identificados como uno de los colectivos más vulnerables tardándose de ciberdelitos. Generalmente, los menores navegan el doble del tiempo que los padres piensan que lo hacen (Avila, 2018). Como elemento relevante de la educación en población infantil, destacar que en una investigación se encontró que casi el 30% del alumnado no había recibido ningún tipo de formación o información previa a la actuación formativa de ciberseguridad y que, al mismo tiempo, la valoraron muy positivamente (Gamito et al., 2020). En cuanto a las fuentes de formación que afirman tener los niños entre 9 y 12 años son principalmente la familia con un 49,82%, amistades 25/64%, profesorado 19,41% e Internet 18,68%. Por su parte, Carceles, M. M. (2015), señala que la prevención debe orientarse en dos sentidos: evitar segundas y posteriores victimizaciones, e intervenir sobre aquellos colectivos que presenten un elevado grado de cibervulnerabilidad. En este caso, serían adoptar las medidas preventivas en favor de los menores debido a su falta de desarrollo y madurez.

Los menores son el grupo de vulnerabilidad por excelencia, tanto por encontrarse en una etapa de desarrollo intelectual y cognitivo, como por su falta de conocimientos en muchas áreas. En el ámbito victimológico son los que se encuentran en el grupo de edad con mayor vulnerabilidad y su victimización es mayor que la de los adultos (Finkelhor, 2008). A esto se le añade que muchas veces ellos mismos no son

conscientes de que están siendo víctimas, lo que les convierte en víctimas ideales (Montiel, 2016). Sufren lo que se viene denominando “cibercriminalidad social” englobando distintas formas de victimización online como el cyberbullying, el acoso online, grooming, sexting, etc. (Miró, 2012). El problema, por lo tanto, ya no es solo la protección, sino el conocimiento de las formas de ciberdelito y también cuáles son las formas de victimización. Educando y concienciando sobre ello, podrán detectar cuándo y cómo han sido víctimas de un ciberdelito.

Dentro de las teorías que apoyan las medidas preventivas para contrarrestar la ciberdelincuencia, García-Guilabert (2014), señala que el menor juega un papel muy importante en su adecuación como víctima en el ciberespacio al introducir sus bienes y al hacerse visible para otros usuarios a partir de sus actividades cotidianas en la Red. Sin embargo, también será decisivo en la victimización del menor, el rol que puedan ejercer los padres y otros familiares como guardianes capaces en el ciberespacio. Todo ello, sin despreciar otro tipo de medidas enfocadas, por ejemplo, en los prestadores de servicio, en los creadores de las herramientas de comunicación, etc.

Por lo tanto, debe considerarse un enfoque integral para educar a los niños en los que se tenga en cuenta no solo al menor en el centro, sino todo lo que le rodea, familia, escuela, grupo de iguales o consideraciones legales que se apliquen al menor. Dentro de este entorno, debe tener una especial consideración la figura de los padres y madres y del apoyo que puedan aportar a la hora de educar a su hijo en la navegación segura. El enfoque educativo de la ciberseguridad debe tener como base la sensibilización de los alumnos en edad escolar de los distintos peligros y riesgos que entrañan las prácticas en internet, teniendo en cuenta también el papel que juegan los distintos actores a su alrededor (padres, organismos especializados y el de telecomunicaciones) (Peña & Segura, 2014).

Por ejemplo, en un estudio realizado en Navarra con menores de edad de entre 10 y 13 años (Fernández-Montalvo et al., 2015), se encontró que la mayor parte de los menores usa Internet en casa y en solitario (sin supervisión de los padres) y también un uso mayoritario de las redes sociales (sin tener la edad legal necesaria). Algunos de los datos que más nos deben poner en alerta son que, un porcentaje del 11%, se comunican con amigos virtuales que no conocen cara a cara. Conductas de riesgo como el envío de fotografías y vídeos a desconocidos, agregar a desconocidos, proporcionar datos personales como número de teléfono e incluso, algunos han quedado presencialmente con desconocidos (5,6%). Se entiende que la educación en ciberseguridad, sea a nivel de conocimientos como en concienciación, disminuiría esas conductas de riesgo en los menores, al distinguir los peligros que corren, y cómo evitarlos.

Los menores en la actualidad forman parte de los nativos digitales, sin embargo, no debe pensarse que por ello tienen un profundo conocimiento sobre el manejo de las TIC y que, por lo tanto, no necesitan formación alguna. La realidad es más bien al contrario. Es necesario que se forme a los menores en un lenguaje adecuado a su edad y con ejemplos prácticos, tratando de evitar las prohibiciones absolutas y la cultura del miedo, que solo muestra los riesgos de la red de redes (Davara-Fernandez, 2019). Los niños no tienen la información ni la capacidad de reaccionar ante un ciberdelito del que puedan ser víctimas, al igual que ante cualquier otro tipo de delito. La educación debe ir dirigida a cubrir también estos aspectos, la ciberresiliencia y la prevención, y a su vez, cubrir de forma transversal la concienciación constante sobre los peligros que implican las redes sociales y la navegación en internet en general.

La relación entre la población más joven y una mayor vulnerabilidad es ampliamente defendida por diversos autores. Mediante una revisión bibliográfica sobre esta cuestión (Astorga-Aguilar & Schmidt-Fonseca, 2019), defienden como, mediante buenas prácticas de ciberseguridad, se puede proteger a menores de edad ante los peligros más habituales que les afectan. Hacen énfasis en las herramientas que proporcionan las propias RRSS (Facebook, Instragram, Whatsapp y SnapChat) para asegurar la privacidad y la seguridad de los datos. También apuntan a la importancia del conocimiento sobre las posibilidades de configurar todas las opciones de seguridad. Este es un elemento de protección ante los peligros a los que están expuestos. En cuanto a los peligros, incluirían aceptar solicitudes de amistad de sujetos desconocidos, no tener público los contenidos que sube en la red social, no subir a la red información personal como direcciones, no publicar fotografías de niños y niñas que muestren sus centros educativos y ubicación de los hogares.

Según el centro Innocenti Insights (UNICEF, 2012), la implicación de los niños en el proceso de toma de medidas implicará: proporcionar a los niños información que les permita tomar decisiones informadas, evitar riesgos y encontrar ayuda cuando sea necesario. También involucrarlos como activistas y defensores de la seguridad en línea. Por lo tanto, aleja su posición de una educación "*a los niños pero sin los niños*", poniendo a éstos en el centro de la participación de todo el proceso. Por otra parte, también señalan la importancia de fortalecer las capacidades de los padres y los profesionales que trabajan con los niños para protegerlos. Según este centro, la capacitación de estos actores (padres y profesionales) sería a través de programas específicos que trabajen sobre: los riesgos asociados a las TIC, las estrategias que los niños y jóvenes pueden adoptar, las posibles fuentes de ayuda y la importancia del diálogo y la participación de los padres en la vida de sus hijos.

En cuanto a Avila (2018), defiende que una de las medidas fundamentales, para la prevención de los ciberdelitos que afectan a los menores, es la adecuada vigilancia de los padres, tanto de la información que comparten, como la que trasmiten a través del ciberespacio. Ejercen un rol decisivo a la hora de que un menor puede o no ser víctima de un ciberdelito. Es trascendental la vigilancia que estos ejercen en el uso de las TICS por parte de menores de edad, ya que es la primera línea de defensa y puede marcar una gran diferencia a la hora de que un menor sea víctima o no de un cibercrimen.Sin embargo, al igual que otros autores, apunta que no todos los padres de familia se encuentran informados acerca del uso adecuado de internet. Tampoco todos los padres conocen las medidas de seguridad con que cuentan algunos sitios para proteger su información y comunicaciones. Para ello, son muchos los países que han elaborado materiales innovadores para comunicarse con los niños, y que a su vez, podrían adaptarse a diferentes contextos nacionales (UNICEF, 2012).

Cuando abordamos este fenómeno, debemos tener en cuenta la particularidad de la población menor de edad y cómo experimentan los procesos de victimización, ya que como es lógico, la cibervictimización también tendrá un impacto diferente en la población joven que en la población adulta. Montiel (2016) señala algunos elementos relevantes en los procesos de victimización como son: "*Comprender y aceptar la gravedad de los hechos, asumir la condición de víctima, reconocer la necesidad de ayuda y además, sentirse merecedor de la misma y solicitarla, liberado de los sentimientos de vergüenza y culpa".* Sin embargo, en el caso de los menores y su mayor vulnerabilidad lo sufrirán de un modo amplificado por los siguientes motivos: "*la tecnofilia, la identificación con el grupo de iguales, la búsqueda de identidad y de autonomía personal y la distancia digital intergeneracional que les separa en muchas ocasiones de las personas adultas que les rodean y tienen el deber de protegerles*" (Montiel, 2016). Es de destacar este último elemento, ya que como indican los autores, aunque lo deseable es la búsqueda de ayuda externa (adultos), no es tan habitual como debería ser. Contrariamente, lo que hacen es acudir al grupo de iguales (amigos) que no van a poder ser un apoyo adecuando como recurso de afrontamiento a diferencia de los adultos, e incluso las autoridades.

Diversos estudios se han centrado en dar luz sobre los hábitos, conocimientos, experiencias y percepciones de los menores en torno al uso de internet. Por ejemplo, Gamito et al. (2020) realizaron un estudio en alumnado de 9 a 12 años para tratar de analizar esas variables y usar la información resultante en la docencia, concretamente para fomentar la ciberseguridad en el aula. El estudio constata el uso de los móviles en menores y sobre todo, testimonios de situaciones conflictivas en la red. Por lo tanto,

encuentran que a su corta edad y su breve experiencia en internet, los alumnos sufrieron estas situaciones conflictivas en la red y son capaces de asociar los riesgos con experiencias personales o de otras personas de su entorno.

También se señala en dicho estudio que las numerosas amenazas a las que están expuestos los menores cuando se habla del ciberespacio: ciberacoso, sextorsión, ciberengaño, grooming, exposición a contenidos inadecuados... A esto hay que añadir, que el número de casos de lo anterior está teniendo un incremento gradual en los menores de edad (Cressato, 2017). Los menores, además, carecen de estrategias para afrontar las diversas situaciones que se pueden dar en el área de la cibercriminalidad (Fernández-Montalvo et al., 2016). El estudio de Gamito et al. (2020) sigue la línea precisamente sobre el colectivo de niños entre 9 y 12 años para detectar sus necesidades formativas en ciberseguridad, encontrando que muchos de ellos son capaces de mencionar riesgos y conflictos relacionados con ciberacoso (267 referencias) y los asocia a experiencias personales o a testimonios de personas del entorno. Es más, parte del alumnado admite haber sido víctima de diferentes tipos de acoso en la red:

"*el 4,39% ha sufrido el robo de identidad en línea, el 4,03% ha recibido o ha visto publicaciones cuyo objetivo era perjudicarle, el 3,66% ha recibido o ha visto publicaciones desagradables sobre familiares y amistades y, por último, el 1,83% ha sido amenazado mediante medios digitales."*

En relación con las necesidades formativas encuentran que los alumnos dicen conocer los riesgos y las medidas para poder prevenirlos (88 referencias), sin embargo, las prácticas de uso en internet hacen dudar de su seguridad. "*El 28,35% no sabe si su cuenta es privada o pública, pero desconocen cuáles son y/o cómo se modifican las opciones de privacidad de las aplicaciones."* Se desprende también de este estudio que aunque saben algo de teoría, no la ponen en práctica, por lo tanto, existe cierta incoherencia entre ese discurso teórico y las prácticas de uso. Son capaces de enumerar las consecuencias de enviar fotos personales pero, al mismo tiempo reconocen hacerlo y no reparar en exceso en cuestiones de privacidad o de cesión de datos personales en RRSS.

En Astorga-Aguilar & Schmidt-Fonseca (2019) se defiende que en la prevención de los riesgos la juventud se debe atender especialmente a los adolescentes. Esta prevención está en base al nivel de ciberseguridad que se tenga, abarcando conceptos de seguridad y privacidad, protección de propiedad y seguridad de su información. Por lo tanto, sería fundamental esa capacitación general en la adolescencia sobre conceptos

clave. Son edades donde las cualidades propias del colectivo les podría hacer más vulnerables a delitos como el ciberacoso, el sexting, la suplantación de identidad o el chantaje. Además de la protección, en la adolescencia tendría un peso de gran importancia la concienciación sobre la privacidad y el envío de datos personales, la verificación de la identidad de las personas con las que se interactúa en la red y, sobre todo, las ciberamenazas a las que pueden enfrentarse.

Educar sobre las mismas y sobre sus consecuencias, son el elemento fundamental para generar la concienciación y la puesta en marcha de las medidas que deben conocer. Cabe señalar aquí, de nuevo, el papel fundamental de los centros educativos y las intervenciones de instituciones públicas a la hora de dar charlas y talleres en materia de ciberseguridad. Por una parte, desde los propios centros y la preparación que pueda tener el personal docente y, por otra parte, las instituciones directamente relacionadas con la ciberseguridad que pueden impartir sesiones didácticas sobre el ámbito (FCSE, Incibe, OSI, etc.).

Adultos

Analizando las cifras del informe sobre la cibercriminalidad en España (López et al., 2021), la población adulta de entre 26 y 65 años es la que sufre el grueso de la victimización (76,46%). Es una generación que incluye a nativos digitales, especialmente aquellos más jóvenes del rango. Estos nativos digitales han nacido y se han formado utilizando las TIC, Internet, las Redes Sociales y el lenguaje digital de juegos por ordenador, vídeo e Internet. Por otra parte, estarían los que no han tenido esa inmersión temprana y poco a poco se han ido adaptando por mera necesidad de estar al día. Este grupo es el que se denomina “Inmigrantes Digitales”. Aunque los nativos digitales tienen más formación y conocimientos en ámbito digital, algunos estudios, como el de Cain et al., (2018), encontró que los usuarios de más edad tendían a comportarse de forma más segura que los más jóvenes. Por lo tanto, se debe tener en consideración que, aunque las personas adultas en algunos casos no presenten los mismos conocimientos que los nativos digitales, cualidades como la responsabilidad o la prevención pueden favorecerles de cara a la navegación segura.

Siguiendo en esa línea, se ha observado que los adultos más jóvenes pueden correr un mayor riesgo de ser engañados por correos electrónicos de phishing, todo ello a pesar de su supuesta mayor familiaridad con las tecnologías de Internet que los adultos de mayor edad (Sheng et al., 2010). Esto está relacionado con los sesgos cognitivos que los individuos pueden demostrar en relación con sus comportamientos de ciberseguridad. Un ejemplo de lo anterior es que los individuos ignoran las advertencias

sobre los riesgos si confían en su capacidad para minimizar las consecuencias de una violación de la seguridad (Rifon, 2005). En un estudio en Finlandia, Oksanen & Keipi (2013) encontraron que la victimización por ciberdelitos es más frecuente en el grupo de edad de 15 a 24 años que en los grupos de mayor edad. El estudio también encontró que la edad y la participación en comunidades en línea estaban fuertemente asociados con la victimización por ciberdelitos.

Otra cualidad diferenciadora que determina la victimización de la población adulta es la actividad. Son personas que se están formando y que participan principalmente en el mundo laboral. A diferencia de los niños y mayores (pensionistas), la población adulta es el motor de la economía, y la que participa en amplia mayoría en la actividad comercial y productiva del país. Son las que tienen mayor nivel adquisitivo y las que gestionan más cantidad de dinero. Además, al gestionar las empresas, compañías y todo el sector privado, son los que presentarán el primer objetivo de los ciberdelincuentes. Al mismo tiempo, esta característica también puede ser una ventaja facilitadora de la protección. El sector privado y el mundo laboral, es actualmente una puerta de acceso a la educación en ciberseguridad. Las empresas reciben asesoramiento y solicitan formación a sus empleados, por lo tanto, una parte importante de la vía de aprendizaje en ciberseguridad viene por medio de estas organizaciones.

La población adulta, como empleados y trabajadores, están en contacto directo con una realidad actualizada. Esto se produce en mayor medida cuando se habla de grandes empresas y organizaciones, que tienen una mentalidad corporativa y donde se hace mayor hincapié en la ciberseguridad. Según Pulido & Rosell (2017) existen diferentes niveles de aprendizaje a la hora de aplicarlos a los miembros de una organización. En primer lugar, tendríamos la concienciación, que es un proceso de aprendizaje destinado a todos los miembros de la empresa. Su meta es cambiar las actitudes individuales y colectivas para comprender la importancia de la seguridad y las consecuencias de su fracaso. En segundo lugar, la formación destinada a trasladar a los empleados de la empresa los conocimientos que les permitan realizar su trabajo con mayor eficacia. Se centra en dar a conocer y hacer que se dominen las habilidades necesarias para desempeñar adecuadamente un rol determinado.

Finalmente, tenemos la educación, que es el proceso de formación en ciberseguridad más avanzado. Se centra en el desarrollo de la capacidad y la visión para llevar a cabo actividades complejas y multidisciplinares, además de las habilidades necesarias para promover el desarrollo profesional en ciberseguridad. El objetivo final desarrollar un entendimiento profundo y capacidad de gestionar el conocimiento en ciberseguridad. Es más, incluso señalan la necesidad de convertir al empleado en un human firewall, o

muro de defensa humano, para que tenga un papel activo y relevante en la información que maneja. Todo ello se traduciría en una estrategia de seguridad más robusta que la simple aplicación de medidas técnicas. En cuanto a los autónomos, también se han puesto en marcha medidas para capacitarles en ciberseguridad a través de programas públicos de digitalización. También sería el caso de los programas formativos de entidades especializadas como la Federación Nacional de Trabajadores Autónomos entre otras.

Personas Mayores

Los perfiles de las personas vulnerables a la que debe dirigirse esta educación no son solamente los menores de edad, también el colectivo de personas mayores es especialmente vulnerable al no haber crecido en el ámbito de las nuevas tecnologías. En Burton et al. (2022) hablan de la desprotección de los mayores ante los riesgos a los que se ven expuestos en uso diario de las nuevas tecnología. Entre los factores de vulnerabilidad encontraron: el aislamiento social, los problemas de salud cognitivos, físicos y mentales; el nivel de riqueza, las habilidades o conocimientos limitados en ciberseguridad. Al mismo tiempo que tienen desconocimiento, también son usuarios de internet y dispositivos, por lo tanto, deberán ser un objetivo de la educación en ciberseguridad. En consecuencia, señalan esta necesidad y desprotección de los mayores ante los riesgos a los que se ven expuestos en uso diario de las nuevas tecnologías.

De forma más concreta se apunta al entorno familiar y las instituciones educativas como las que deben dar una respuesta eficaz ante este problema. También proponen, en esta última línea, el desarrollo de herramientas como medio pedagógico-didáctico, las cuales se articularían dentro de un conjunto de actuaciones en entidades y organismos. En cuanto a dónde se deben integrar estas herramientas, señalan a los programas de inclusión digital para los mayores (Gudiño, 2018). Yendo más allá, también cabría destacar el papel de los centros de mayores y residencias de tercera edad a la hora de hacerles llegar este flujo formativo desde otras instituciones (ayuntamientos y comunidades autónomas). Las entidades e instituciones que trabajan con personas mayores disponen de personal que realiza formación reglada a través de distintos módulos y ciclos. Si se incluyese la educación en ciberseguridad en dicha formación, se podría beneficiar indirectamente a las personas beneficiarias de esas instituciones.

Además de la necesidad de implementar planes en centros públicos y privados que trabajen con estos perfiles, también existe una falta de investigación y datos relacionados con el estudio de la vulnerabilidad que presentan y los mejores métodos

para educarles en ciberseguridad. Las personas ancianas no tienen los mismos estilos de aprendizaje que los de las generaciones más jóvenes. Entre otros factores, se relaciona principalmente con la edad, la disminución de las capacidades cognitivas, limitaciones físicas y perceptivas, como deficiencias visuales y auditivas (Teets & Grimes, 2019). Debido a las peculiaridades de esta población, se hace necesario desarrollar materiales de aprendizaje para ellos, con metodologías de aprendizaje y enseñanza personalizadas. Algunos investigadores sugirieron también que el uso de tabletas digitales puede ayudar a los ancianos a aprender. Se basan en que las personas mayores tienen que estar conectados, ser independientes y autónomos (Gatti et al., 2017).

Para esta población, se han desarrollado programas como el llamado Elderly Empowerment Program (Programa de capacitación de ancianos), creado por los investigadores para evaluar si el vídeo es un método adecuado y eficaz para educar a los ancianos (Ramadhani et al., 2020). El programa usó tres elementos de evaluación: contenidos de educación sobre la salud oral y el rendimiento físico, contenidos visuales atractivos y contenidos de vídeo fácilmente comprensibles. El empleo del vídeo se justifica en que las personas mayores tienen dificultades para recuperar los conocimientos de los libros debido a la disminución de sus capacidades (envejecimiento) (Buja et al., 2021). También se encontró que las personas mayores prefieren realizar algunas actividades con sus amigos y no en solitario.

Se elaboraron vídeos educativos basados en la idoneidad visual y auditiva para aumentar la comprensión y el interés por ver vídeos educativos. El estilo de aprendizaje visual es adecuado para las personas con problemas de audición. Sin embargo, debido a la disminución de la visión, la audición y la memoria, habrían algunos cambios a tener en cuenta. Por ejemplo, aquellos que afectan a la absorción de los colores en la luz que entra en el ojo. Las personas mayores tienden a tener dificultades para distinguir los colores, especialmente el azul, el verde y el morado. Por lo tanto, es importante la selección correcta de los colores. En cuanto al audio, también hay que tener en cuenta la voz utilizada en el vídeo, ya que las personas mayores tardan más tiempo en escuchar con claridad y procesar las voces entrantes. La misma consideración se aplica a la memoria (Ramadhani et al., 2020).

Otro programa desarrollado en Australia ha tenido muy buenos resultados, siendo un programa sencillo, de carácter educativo y diseñado para explicar los conceptos de seguridad (Cook, Szewczyk & Sansurooah, 2011). El funcionamiento se asemeja al aprendizaje que pueda tener un niño del idioma o las matemáticas. Los participantes aprenden las técnicas de seguridad y las medidas de protección desde la base.

Comenzó explicando a personas de la tercera edad sobre cómo y por qué un ciberdelincuente envía estafas de phishing por correo electrónico, es decir, el modus operandi. En la siguiente fase, se enseñó a los participantes una serie de ejemplos de phishing y, por otra parte, correos legítimos haciendo mayor hincapié en los correos electrónicos engañosos. Finalmente, se educó sobre cómo identificar el phishing, consiguiendo buenos resultados en poco tiempo. Por lo tanto, el programa fue un éxito y las personas de la tercera edad fueron capaces de identificar con seguridad los correos legítimos del phishing sin ayuda.

Este tipo de programas son ejemplo de la capacidad que tiene el esfuerzo educativo para la prevención en aquellos tipos de delitos que afectan a la ciudadanía más vulnerable. El caso japonés también incluye este elemento relevante y diferenciador, el de añadir programas de entrenamiento para personas mayores y de tercera edad (NCIRSC , 2013). Este entrenamiento, por tanto, se una herramienta útil y eficiente en esta población que necesita metodologías especiales adaptadas a sus necesidades cognitivas. En el estudio de Burton et al., (2022) identificaron los factores que conducen a la victimización de las personas mayores para mejorar las intervenciones destinadas a reducir los riesgos de victimización. Para ello, analizaron cómo, por qué y en qué circunstancias las personas mayores se convierten en víctimas de la ciberdelincuencia. Descubrieron que aunque la intervención directa con las personas mayores parece reducir los riesgos de ciberdelincuencia, también son necesarias medidas para cambiar las actitudes sociales, reducir la delincuencia y aumentar la protección. Se necesitan protecciones sociales y estructurales para garantizar la seguridad de la tercera edad.

Población migrante, refugiados y solicitantes de protección internacional.

El número de residentes en España nacidos en el extranjero ascendía a 7.506.870 personas (enero de 2022), el 15,8% de la población total (prácticamente una de cada seis personas). Según el informe sobre la cibercriminalidad en España (López et al., 2021), el 12,5% de las personas víctimas de ciberdelitos son extranjeras. Puede parecer una cifra relativamente baja, pero si tenemos en cuenta que existe un cierto porcentaje de personas que, por su situación administrativa, deciden no denunciar, esta cifra podría ser mayor. Es una población que, en muchos casos, tiene miedo a denunciar al ser víctima de cualquier tipo de delito, especialmente por las consecuencias que puedan sufrir ellos mismos (órdenes de expulsión). Además, a ello se suma el desconocimiento de los procedimientos y la legislación en el país, que puede ser muy distinta a la de los países de procedencia.

Según un informe publicado por la fundación CEPAIM (Mendez et al, 2022), existen vacíos legislativos para garantizar la denuncia segura de las víctimas de delitos que están en situación administrativa irregular. Además, se producen deficiencias en la implementación de procedimientos como, por ejemplo, agentes clave que prestan mala información a las víctimas acerca sus derechos, actitudes policiales inadecuadas y falta de protocolos claros entre las Fuerzas y Cuerpos de Seguridad. Teniendo en cuenta la situación personal de la víctima, en muchas ocasiones son perfiles de una gran vulnerabilidad. Se suman también varios factores que pueden impedir su acceso a la justicia, como puede ser el desconocimiento de la normativa, barreras lingüísticas o la desconfianza en las FCSE. Es por todo que estos perfiles requieren una mayor atención personalizada e individualizada a las necesidades específicas que presentan.

En cuanto a los conocimientos que presentan, estas personas en numerosas ocasiones carecen de alfabetización digital y nociones básicas de informática. Tampoco tienen conocimientos básicos de ciberseguridad a pesar de que usan internet, redes sociales, aplicaciones y mensajería instantánea. En algunos países en vías de desarrollo también se encontró que incluso una parte importante de la población no considera la ciberdelincuencia como un delito. En un estudio se les preguntó a los participantes sobre allanamiento de morada y robo a través de una cuenta en Internet, y mientras definían al primero como un ladrón, al hacker lo consideraban un “chico listo” (Ismailova & Muharnetjanova, 2016). Hallaron que el conocimiento sobre la ciberdelincuencia era bastante escaso y los participantes desconocían en su mayoría muchos aspectos de la delincuencia informática.

Vulnerables

Existen diversos perfiles de vulnerablidad en la sociedad, sin embargo, cuando hablamos de delincuencia y de ciberdelincuencia debemos prestar una especial atención a ellos. En Hellems & Bhatia (2022) apuntan a cuatro discapacidades que por su impacto tienen mayor relevancia de cara a la problemática de la ciberseguridad. Las personas ciegas y de discapacidad visual para adquirir aprender conceptos de ciberseguridad (Hairston et al., 2020). También los perfiles con discapacidad intelectual, ya que pueden tener dificultades en el razonamiento y abstracción. Otro perfil es el de las personas que sufren dislexia, debido a la comprensión textual, por ejemplo para la creación de contraseñas. En cuanto al autismo, puede aumentar la susceptibilidad a los ataques phishing. También se apunta, de cara a la educación de estos perfiles, al empleo de técnicas similares a otros perfiles, como por ejemplo la gamificación (Hellems & Bhatia, 2022). No obstante, señalan la falta de una cultura más inclusiva en el campo de la ciberseguridad y la garantía de la educación en estos perfiles.

En cuanto a los/as cuidadores/as que trabajan con perfiles de discapacidad intelectual, actualmente no existen estudios que analicen las estrategias dirigidas a ellos/as. Estos/as trabajadores/as no suelen recibir formación en ciberseguridad ni sobre protección de los datos (Shpigleman, 2017). Esto es de especial relevancia dada la importancia que podrían tener para disminuir las amenazas a las que se enfrentan las personas con estos perfiles. Por lo tanto, es necesaria más investigación para intervenir en la eficacia de los/as cuidadores/as que son parte responsable de la protección de sus usuarios (Rochelau et al., 2021). También existen numerosas entidades del tercer sector que trabajan con estos tipos de perfiles y en donde se podrían implementar actividades formativas dirigidas a educar en ciberseguridad y ciberamenazas.

6.3. Técnicas y métodos para la educación en ciberseguridad

Respondiendo a la pregunta de ¿Cómo educar en ciberseguridad? encontramos las distintas técnicas y métodos educativos. Incluyen un gran repertorio de formas y formatos, como la gamificación o el entrenamiento. Según SEAS (2016), las distintas formas que tomarán el proceso de enseñanza son las estrategias, técnicas y actividades mediadas, ya que son las que generarán esas experiencias más que necesarias y que serán las que permitan el aprendizaje. El objetivo último, por lo tanto, es una educación integral que incluya conocimientos conceptuales, procedimentales y actitudinales, todo ello basado en una rigurosa planificación y contextualización. Seas afirma que se debe generar incertidumbre y deseo de aprender o resolver un problema. Ello se fundamenta en la idea en que percibir mejor las situaciones, elementos y circunstancias generadoras de esa incertidumbre, vienen dadas por los sentidos, emociones que se generan en el proceso de conocimiento y la cognición (Seas, 2016).

Algunos autores defienden que la formación sea “aprobada, adaptada y diseñada por maestros, psicólogos y pedagogos que, con su conocimiento, adecuen la frecuencia, el formato y, en caso de ser necesario, el contenido a la situación real de los destinatarios” (Davara-Fernandez, 2019). Por lo tanto, se debe otorgar un rol fundamental a personas provenientes de áreas sociales y educativas en lo que se refiere a la transmisión del contenido. Incluso atribuirles ese papel de adaptación de los contenidos al destinatario. Esta idea tiene un especial protagonismo en la infancia y los adolescentes. La educación juega un factor sumamente importante como una medida preventiva de ciberdelitos que afectan a menores, por lo que los programas educativos deben ser adaptados en todos los estados para combatir la cibercriminalidad (Avila, 2018).

También con los destinatarios adultos se hace necesario adaptar los modelos educativos para, de este modo, optimizar el esfuerzo e inversión que implica educar a

gran escala. Un ejemplo de ello, son las estrategias corporativas para educar a los trabajadores. Pulido & Rosell (2017) afirman que "*hay empresas que gastan millones en campañas de concienciación pero realmente pocos responsables de la seguridad de las TIC (CISO) están contentos con los resultados*". El motivo aparentemente es que la mayor parte de los programas llevan mucho tiempo, son muy técnicos y esencialmente basados en mensajes negativos. Por tanto, propone aproximarse al problema con una visión más sofisticada, con técnicas de gamificación, ataques simulados e instrucción interactiva en profundidad de las destrezas en ciberseguridad. A continuación se definirán y explicarán cada una de las técnicas existentes.

GAMIFICACION

Romero & Rojas (2013) definen la gamificación como una técnica de aprendizaje basado en las mecánicas y dinámicas de juego para alentar o motivarlo, colaborando en la construcción de nuevas experiencias, convirtiendo algunas actividades consideradas aburridas en innovadoras e interesantes para los participantes. La gamificación aplica los conocimientos de la teoría del juego y la teoría del flujo (Deterding et al., 2011; Silic, 2020) a contextos ajenos al juego, con la finalidad de modificar los comportamientos y resultados. Los principios de esta "ludificación" se han mostrado como un enfoque eficaz para mejorar la capacidad de protección (en un 51,75%), la motivación intrínseca, el aprendizaje, las habilidades de afrontamiento y el cumplimiento de las normas de seguridad. Además, los participantes señalan que los elementos de gamificación son un medio importante para aumentar la concienciación sobre la ciberseguridad (Alqahtani & Kavakli-Thorne, 2020).

La gamificación surge en 2010 con la idea de que los alumnos disfruten del proceso de aprendizaje mediante el juego, reforzano la motivación y la interacción en todo momento. También aporta una mayor implicación y un refuerzo, a diferencia de la educación unidireccional tradicional "*pretende que el alumnado aprenda y/o sea evaluado de manera motivadora e interactiva a través del juego*" (Becerra & Fernández, 2018). Entre las utilidades, destaca que es una metodología atractiva para los más jóvenes, permite el uso de móviles en el aula y al mismo tiempo la adquisición de nuevas habilidades intelectuales y emocionales del alumnado a través del juego. Becerra & Fernández (2018) añaden un elemento más, y es que la gamificación en el aprendizaje permite mejorar la motivación de los alumnos que se encuentran inmersos en el juego, ya que buscan la consecución de un objetivo concreto. Las experiencias realizadas en el Kahoot muestran que el profesorado (en este caso universitario) tiene un buen grado de satisfacción.

Otro recurso de gran utilidad, sería los juegos de autoevaluación a través de dispositivos móviles (Miguez & Dafonte,2018). Se señala que el empleo de los móviles en el aula puede tener un valor motivador, además de efectos positivos sobre la evaluación formativa debido a la retroalimentación inmediata. Es decir, el hecho de que ellos mismos, con una herramienta ampliamente conocida y que les es familiar, puedan plantearse cuestiones formativas, como puede ser en este caso la ciberseguridad, responderlas e inmediatamente saber si conocen o desconocen las respuestas, podrá reforzar y asentar el aprendizaje. El someterse a preguntas e inmediatamente obtener una respuesta, también puede provocar cierta sensación de desconocimiento en caso de que las respuestas sean erróneas, y por lo tanto, crear una concienciación y una cierta “inquietud” al ver que son cuestiones relevantes de seguridad, y que no sabrían responderlas.

El teléfono móvil como apoyo es un elemento que incentiva la participación, ya que es el principal instrumento de ocio en la población joven. Además de motivar la participación, es una herramienta dinamizadora en donde el alumno deberá realizar actividades y la autoevaluación. También existiría otros beneficios como integrar el móvil en el aula para vincularlo a las plataformas virtuales que ya conocen (Vázquez-Cano & Sevillano-García, 2017). Es una herramienta que también tendría una tercera aportación relevante, y es que permite la preparación de textos previamente y luego la respuesta de cuestionarios, lo que se conoce como flipped learning o clase invertida. Lo positivo de este enfoque es que es muy bien valorado por los propios estudiantes de cara a la asimilación y aprendizaje de contenidos (frente a la clase magistral tradicional).

Para que un juego sea efectivo y exitoso, deberá explotar al máximo todos los motivadores para poder producir los niveles necesarios de compromiso, motivación y retención entre los usuarios (Chou, 2015). Por otra parte, autores como Dondlinger (2007) y Sheng et al. (2007) apuntan a otros elementos que deben mantener los juegos: Debe llamar y mantener la atención del jugador, promover y fomentar el aprendizaje, emplear un contexto narrativo para garantizar que el juego sea divertido y entretenido, usar personajes e historia fuertes para ayudar a motivar a los jugadores y hacer hincapié en la habilidad (son necesarios retos para mantener la atención del jugador. En cuanto a los requisitos funcionales, apuntan a los siguientes: el juego debe ser dinámico y fácilmente configurable para diferentes tipos de redes sociales, personalizable para que sea relevante para diferentes tipos de usuarios y que esté disponible para un grupo de usuarios lo más amplio posible.

Dentro de la gamificación podemos encontrar los denominados “Serious Game”, o juego serio en castellano. Tiene como finalidad combinar la diversión y el juego con un aspecto

serio o didáctico (Dorner et al., 2016). La finalidad clásica de los videojuegos del entretenimiento es aprovechada como herramienta para motivar y mantener la atención de la usuaria, todo ello, mientras se le enseñan aspectos sobre ciberseguridad o se le conciencia sobre la ciberdelincuencia (Ritterfeld et al., 2009). Por lo tanto, los juegos serios son videojuegos que tienen una finalidad educativa, y secundariamente, son divertidos. Cuando se habla de este tipo de videojuegos, se hace referencia únicamente a los que emplean plataformas digitales o medios digitales. Existen técnicas de gamificación con juegos de mesa, cartas, etc. pero no serían “videojuegos” en el sentido estricto.

Un ejemplo práctico de gamificación es el de Alqahtani & Kavakli-Thorne (2020). Diseñaron, implementaron y evaluaron los resultados de un serious-game basado en realidad aumentada (RA) llamado CybAR. La gamifición buscaba evitar los ciberataques y mejorar su comportamiento de evitación. Los resultados indicaron que la plataforma basada en RA fue una forma eficaz y divertida de aprender conceptos relacionados con la ciberseguridad. CybAR imitaba el escenario de un problema de ciberseguridad de la vida real, pero de forma amena y comprensible. También motivaba a los jugadores a aprender más sobre conceptos relacionados con la ciberseguridad en el futuro. Por lo tanto, la gamificación se muestra como una técnica completa y eficaz que puede convertir la educación en ciberseguridad en algo ameno y divertido.

Finalmente, como recomendaciones, algunos autores (Nalin et al., 2013) señalan la importancia de incluir en los diseños: los elementos de amenaza percibida, efectividad de salvaguarda, costo de salvaguarda, autoeficacia, gravedad percibida y susceptibilidad percibida. Estos elementos deben incorporarse en el marco de diseño del juego para que los usuarios eviten los ataques de phishing a través de la motivación. En la literatura encontrada, las modalidades de los juegos son múltiples y diversas, pero la inclusión de factores motivacionales y lúdicos es algo en común en todos ellos. Además, también funciona de forma eficiente cuando en un plan educativo se incluye esta gamificación conjuntamente con otras técnicas complementarias como pueden ser la simulación, el entrenamiento o talleres prácticos.

ENTRENAMIENTO

En cuanto al entrenamiento, se considera una estrategia para mejorar la capacidad de discriminación, adecuada para aumentar sensibilidad a las señales visuales de engaño y para producir una mejora de las capacidades discriminativas (Dodge, 2012; Moreno-Fernández, 2017; Lastdrager, 2019). El entrenamiento consiste en la preparación

repetida de diversas situaciones relacionadas con incidencias de seguridad ante las que el usuario debe poner a prueba sus conocimientos para defenderse.

SIMULACION

La simulación consiste en prevenir los ciberdelitos utilizando contenidos relacionados con la vida real, ayudando a los alumnos a mejorar la conciencia de los ciberdelitos, y a darse cuenta de su gravedad a través de la experiencia indirecta (Kim et al., 2016). Por lo general, una simulación pretende permitirnos manipular y experimentar una situación a la que no podemos enfrentarnos en el mundo real (Kim et al., 2016). Por lo tanto, es una herramienta que proporciona una situación similar a la del mundo real para lograr un objetivo educativo (Kang et al., 2011). Permite aprender situaciones peligrosas sin suponer ningún riesgo, de forma segura, controlada, y repitiendo las veces que sea necesario (Im & Yeon, 2009). Dentro de la simulación, a su vez, existirían varios modelos o categorías (Alessi & Trollip, 2001): simulación física, de procedimiento, de situación y de proceso. De todos ellos, la simulación situacional es la que tendría una mayor aplicación a la educación en ciberseguridad (Im & Yeon, 2009). En ella, el alumnado puede adquirir cambios comportamentales o actitudinales mediante la resolución de problemas en contextos simulados, roles y escenarios.

El gran valor de la simulación es que tiene una doble aportación. No solo permite un aprendizaje en el que el alumno tiene un papel activo y dinámico, por lo tanto, no es un sujeto pasivo en el proceso educativo, sino que también permite desarrollar una concienciación de los peligros (Pulido & Rosell, 2017). En las pruebas en entorno de simulación, el participante debe aprender cuáles son las amenazas, las consecuencias, los conocimientos y aplicaciones de ciberseguirdad, los procedimientos, la gestión de las medidas de seguridad entre otros. Se le pone a prueba mejorando su motivación, y reforzando aquellas conductas y soluciones correctas frente a aquellas otras que le llevan al fracaso.

MULTIMETODO

Las tareas multimétodo se refieren al uso mixto de varias técnicas de forma conjunta, aunque casi siempre suelen ser la combinación de las técnicas más habituales como la gamificación, el entrenamiento o la simulación (Chattopadhyay, 2019; Mugayitoglu, 2021; Reinheimer, 2020; Pittman, 2016; Alencar, 2013; Wolf, 2020; Tschakert, 2019; Herzberg, 2011; Baillon, 2019; Wen, 2019). La utilización mixta de técnicas muestra buenos resultados y permite beneficiarse de los beneficios que aporta cada una de ellas. El hecho de que en la mayoría de ocasiones que se emplea el multimétodo se incluya la gamificación, es otra muestra de la versatilidad y efectividad que tiene la misma.

Un ejemplo de combinación de elementos es el “edutainment”, o entretenimiento educativo, surge de la combinación de las palabras inglesas education y entertainment. El edutainment es un concepto que hace referencia al software o plataforma que permite aprender mediante el entretenimiento/diversión, es decir, combinando contenido educativo y elementos lúdicos (Kim, 2002; Kim et al., 2016). Un juego educativo basado en una simulación puede mejor la motivación si se consigue resaltar esa asociación con la vida real. Por lo tanto, el aprendizaje puede ser más efectivo si el alumno resuelve problemas dados a través del edutainment (Kim, 2014). Como resultado, cuando combinamos técnicas de gamificación con simulación, de entrenamiento con simulación o gamificación con entrenamiento, lo que conseguimos es amplificar la capacidad de aprendizaje y motivación.

ESCAPE ROOM

El Escape Room, el tradicional juego que consiste en tratar de escapar de una sala o lugar en un tiempo límite, se ha conseguido aplicar al ámbito de la educación en ciberseguridad (Decusatis, C. 2022; Streiff, 2019). En este tipo de juegos, los participantes deben pasar una serie de pruebas y llaves relacionadas con conceptos de ciberseguridad o ciberamenazas hasta conseguir escapar de la sala. Se puede jugar en un sitio físico o en un lugar virtual. En el caso del Escape Room aplicado a la ciberseguridad, se probaron diseños utilizando el marco de Octalysis (DeCusatis et al., 2022). El enfoque Octalysis se centra en la persona y la incorporación de elementos de juego en contextos que habitualmente no suelen serlo.

Los beneficios pedagógicos han sido documentados y demostrados (Chou, 2015). El caso de Octalysis, organiza ocho elementos de gamificación (impulsores cognitivos) con la que es posible medir el nivel de compromiso y motivación del estudiante Los elementos de gamificación se dividen en "sombrero blanco" o “white hat”, y vienen a ser los motivadores positivos (sensación de dominio de habilidades, creatividad y mayor propósito) y por el contrarío, habría el grupo de los “sombrero negro” o “black hat” (miedo, incertidumbre, codicia y castigo). También se organizan según apelen a motivaciones extrínsecas (lógica, cálculos y propiedad) frente a las intrínsecas (creatividad, autoexpresión y contexto social).

OTRAS

Existen otro tipo de técnicas, como el empleo de Robot o Robot Social (Yett, 2020; Althobaiti, 2018), que apuestan por dar nuevas aplicaciones (educativas en ciberseguridad) a las tecnologías más innovadoras. También existen las clases prácticas, herramienta que se muestra eficaz por la implicación y la atención que

requiere, mejorando la motivación intrínseca (Amo, 2019; Kolb, 2022). Por otra parte, hay voces defensoras de enseñar ciertas técnicas de hacking (Árpád, I., 2013), ya que consideran que esas enseñanzas pueden ayudar a prevenir nuevos ataques. Saber cómo un hacker intentará hackear un sistema puede ser útil para la víctima en dos sentidos: el usuario estará preparado con ciertas contramedidas y le ayudará a reconocer un ataque para poder actuar en consecuencia.

Cada nueva innovación tecnológica que ha surgido, ha abierto nuevas posibilidades para educación y su avance: la imprenta, pizarras, televisores, ordenadores, internet, dispositivos, etc. como sería el caso de las películas (Hammond & Lee, 2010). Las películas y el cine es otro formato más que puede tener importantes aplicaciones a la educación en ciberseguridad. Forman parte de la vida cotidiana de los alumnos, están disponibles en una gran variedad de formatos y pueden reproducirse fácilmente con equipos comunes como los ordenadores. También pueden ofrecer notables opciones pedagógicas y pueden resultar una buena fuente de materiales motivadores para los alumnos (Andreatos, 2020). A pesar de que las películas se han utilizado en otros tipos de cursos, como los idiomas, enseñanza infantil, etc. no es habitual en ciberseguridad.

Taylor et al. (2017) han desarrollado una herramienta de formación en ciberseguridad que utiliza documentales en vídeo de casos reales. También en Andreatos (2020) desarrollan un proyecto piloto para sensibilizar al alumnado sobre los factores humanos de la ciberseguridad y la ciberdelincuencia. Consistió en la proyección de una película en donde los alumnos fueron capaces de identificar la mayoría de los ciberataques relacionados con la base impartida en el curso, además de tener la oportunidad de adquirir algunos conocimientos mientras disfrutaba de la película. El experimento fue evaluado muy positivamente, ya que el uso de una película les resultó un medio agradable y atractivo para introducir a los estudiantes en los temas sociales y psicológicos de la ciberseguridad.

Los MOOC son un formato de cursos masivos pensado para dirigirse a una audiencia numerosa. Mooc es el acrónimo en inglés de Massive Online Open Courses (o cursos online masivos y abiertos) En González-Manzano & Fuentes (2019), analizaron 32 cursos de ciberseguridad. La mayor parte de los alumnos tenían entre 21 y 40 años. En cuanto al nivel educativo, la mayoría son de bachillerato, escuela superior y máster. No se da, en definitiva, un perfil de ciudadanía general, sino uno más específico de universidad y ambiente académico. También se destaca en el propio artículo que el 60% de los participantes de MOOC han completado una licenciatura. Un punto positivo es que los MOOC están pensados para tener contenidos de fácil comprensión, a diferencia de aquellos que persiguen una comprensión profunda o que requieran conocimientos

en informática o titulaciones en el ámbito (Gonzalez-Manzano & Fuentes, 2019). Como punto negativo, cabría decir que es un tipo de educación que requiere un interés activo de la audiencia. Se deben buscar, luego inscribirse y participar. No es un formato que llegue de por sí a la población general.

Por su parte, los campamentos de ciberseguridad o Cybercamp también muestran buenos resultados. Son un tipo de actividad inmersiva, con un fuerte contenido de socialización y trabajo en equipo (Cornel, 2016; Pittman, 2016; Jin, 2018; Wolf, 2020). Por último, se han encontrado resultados positivos en las técnicas de E-Learning (Peker, 2018), los juego de cartas (Wang, 2018), taller grupal/ colaborativo (Kovačević, 2020), mapas conceptuales (Sun, 2016), cómic (Zhang-Kennedy, 2016) y la lectura de consejos/ relatos (Wash, 2018). Merece una especial atención los talleres grupales/colaborativos porque permiten socializar, de una forma transversal a todo el proceso educativo, con el grupo de iguales. En estos talleres, los participantes trabajan en grupo para superar las distintas pruebas y retos educativos

7. Recomendaciones

La literatura científica sobre la educación se ciberseguridad arroja algunas recomendaciones sobre los contenidos que debe incluir, el modo en el que se debe llevar a cabo, factores psicológicos que deben ser tenidos en cuenta y las deficiencias que presentan algunas de las campañas actuales. Las limitaciones en general apuntan a una falta de concienciación, es decir, que en muchos casos no es tanto la falta de conocimientos, sino que es la motivación de poner en marcha dichos conocimientos. También está la desconexión entre esa educación y la ciudadanía de a pie, ya que no llega al grueso de la sociedad. Por lo tanto, es necesario tener en cuenta las limitaciones y defectos encontrados para poder mejorar y desarrollar planes de educación y concienciación.

En una reunión de representantes de la UE y de EEUU (ENISA, 2012), discutieron sobre cómo mejorar la concienciación en ciberseguridad. Algunas de las conclusiones fueron:

- La ciberseguridad supone un reto cultural, pues debe ir encaminada a ciertos cambios en el comportamiento de los usuarios.
- Los ciudadanos son conscientes de alguna manera de que hay medios técnicos para protegerse, pero en muchos casos no saben cómo aplicarlos.
- Para concienciar no es necesario dar excesiva información técnica.
- Los mensajes de concienciación deben estar cuidadosamente estudiados para que vayan dirigidos a una audiencia concreta.

- Los usuarios de las TIC más jóvenes puede ser buenos promotores y llegando a ellos se puede llegar a los padres. Cuanto antes comience la educación, mayores serán los efectos en el comportamiento adecuado de los usuarios en el ciberespacio.

En un estudio sobre las diversas campañas de concienciación hechas en diversos países (Connoty et al., 2011) se dedujeron algunos aspectos que dichas campañas tenían en común. Encontraron que las herramientas dominantes en la mayoría de las campañas eran páginas web y publicaciones; los juegos y test eran bastante escasos; la mayoría de las campañas no incluían un servicio de asesoramiento; el patrocinador de las campañas era normalmente el Gobierno; los temas cubiertos eran muy diversos y no se cubrían todos los aspectos que hubieran sido necesarios; las audiencias objetivo en muchas campañas estaban muy diversificadas; la difusión de folletos, websites y otros medios pasivos tienen un impacto limitado si no vienen seguidas de prácticas, y por último, los mensajes difundidos vía televisión han demostrado ser muy efectivos.

También desde Peña & Segura (2014) se lanzan unas recomendaciones de cara a la implementación de acciones, proyectos e iniciativas educativas en ciberseguridad. En primer lugar, que estén enmarcadas dentro de la propia Estrategia de Ciberseguridad del país, que se abarquen todos los niveles formativos, desde el preescolar hasta el universitario (por lo tanto, dirigiéndose a la ciudadanía general además de a personal especializado), que cuente con participación pública y privada, que sepa absorber la experiencia y conocimiento de otros países y que involucre a los ministerios clave: de educación, cultura, industria, etc. Finalmente, señalan el aspecto crucial que debe regir la educación en ciberseguridad y es implicar el factor educativo a todos los niveles sociales, desde los más especializados como pueden ser los militares y policiales, hasta los más divulgativos para la ciudadanía en general.

No solamente los Gobiernos han establecido códigos de buena conducta en el ciberespacio, también por parte de empresas del sector privado que desarrollan y proveen de tecnologías de información y comunicación. Microsoft (Nicholas, 2015), ha colaborado para formalizar normas entre las instituciones y el sector tecnológico en el ciberespacio. Se proponen las siguientes reglas:

1. El Estado no puede dirigirse a las empresas de ICT para que agreguen vulnerabilidades o lleven acciones que disminuyan la confianza por parte del público en productos o servicios que prevean las empresas.
2. Los Estados deberán informar de vulnerabilidades encontradas en productos a las empresas antes de explotarlas.

3. Los Estados deben restringir la creación de armas cibernéticas y si las desarrollan deben ser elaboradas para un fin muy específico, limitado, preciso y no deben ser reutilizables.
4. Los Estados deben comprometerse a no realizar actividades que fomenten la proliferación de armas cibernéticas.
5. Evitar participar en ofensivas cibernéticas.
6. El Estado debe ayudar a las empresas de este ramo a detectar, contener, responder y recuperarse de eventos en el ciberespacio.

De todo lo anterior, se pueden observar medidas orientadas a estas relaciones entre empresas privadas y los Estados, sobre todo, con relación a evitar la creación de armas cibernéticas. Sin embargo, no están incluidas las medidas en relación a la ciudadanía. No vale únicamente el desarrollo de sistemas de transferencia segura si luego lo que falla es el factor humano, en donde una persona es engañada para ceder su información. Son los/as usuarios/as quienes tienen también la responsabilidad de asegurar su propia seguridad mediante buenas prácticas. De hecho, defiende que además de las relaciones diplomáticas para evitar los ataques y mejorar las relaciones estados-empresas, se debe hacer hincapié en el papel de la ciudadanía (Amaro-López & Rodríguez, 2016).

Sobre los programas educativos de ciberseguridad, Beuran et al. (2016) señalan unas condiciones/requisitos:

1. Debe ser apropiado para el público objetivo en términos de conocimientos y niveles de habilidad.
2. Su contenido debe estar de acuerdo con las habilidades previstas.
3. Debe llegar a una audiencia lo más amplia posible.
4. Debe ser sostenible a largo plazo (es decir, buen costo / desempeño).

Además, se recomienda que se tengan en cuenta los antecedentes y el perfil de la audiencia, ya que la cultura de la audiencia tiene un impacto en la forma de aprender en los cursos en línea (Wang, 2007). Bashir et al. (2015), van más allá, proponiendo desarrollar previamente un perfil demográfico, psicológico, cultural y vocacional de los participantes en concursos de ciberseguridad. Por su parte, Dodel & Mesch (2018) defienden la creación de programas de educación en ciberseguridad para las personas socialmente desfavorecidas y con menos conocimientos tecnológicos, especialmente cuando este puede afectar a la calidad de vida de una persona.

En Davara-Fernández (2019), se apuntan consejos y recomendaciones de cómo debe ser la formación en ciberseguridad.

- La formación ha de ser 100 % personalizada.
- La formación deberá ser impartida por un usuario activo de internet y de todas sus funcionalidades –conocedor, por tanto, de las ventajas, de la potencialidad de su uso y, por supuesto, de los riesgos.
- La formación deberá impartirse de manera práctica, contando cada alumno con un dispositivo en el que pueda llevar a la práctica las técnicas, las medidas y las acciones que el formador le vaya dando.
- La formación incluirá casos reales contados tanto por el propio formador, como, por ejemplo, por usuarios que ofrezcan su testimonio sobre su experiencia en la red (tanto positiva como negativa).
- La formación deberá estar apoyada por un documento sencillo y práctico, con recursos e información de interés, así como remarcando las ideas clave que se trasladará a los menores, tanto en formato electrónico como en papel.

Proporciona información sobre lo que puede ser eficaz para animar a las personas a hacer un mayor uso de las estrategias que pueden influir en la victimización (Drew, 2020). Indica que educar a los individuos sobre el daño causado por la ciberdelincuencia puede ser un método útil para fomentar la autoprotección y un mayor uso de los métodos de prevención de la delincuencia. Señalan que una comunicación clara a las personas sobre el daño potencial causado por la ciberdelincuencia puede motivarlas a autoprotegerse mejor cuando participan en el entorno en línea. La educación debe incluir no solo las consecuencias financieras, sino también psicológicas y emocionales de la ciberdelincuencia (Leukfeldt, 2018; Modic & Anderson, 2015). Dado que el daño percibido se asoció con las estrategias de prevención del delito, es probable que la capacidad de influir en esta percepción tenga un impacto particularmente importante en la eficacia de la educación para la prevención de la delincuencia en línea y, a su vez, reducir la victimización.

A la hora de implementar educación en ciberseguridad usando el formato MOOC, Gonzalez-Manzano & Fuentes (2019) señalan que es fundamental para el buen diseño de los cursos en ciberseguridad, que tras los mismos, se revisen los resultados para el rediseño. Las calificaciones y el compromiso de los estudiantes son la base para la toma de decisiones en torno al contenido del curso. Analizando medidores como comentarios realizados, tiempo de seguimiento, finalización, o tiempo que han visto los vídeos, se

pueden saber si los contenidos son adecuados. En caso de que se tengan altas tasas de suspensos en alumnos que han seguido el curso, se pueden detectar fallos en el contenido, así como tasas de abandono excesivamente altas. También se deben analizar las actividades concretas efectuadas en los cursos ya que, individualizándolas, es más sencillo detectar qué partes fallan y cuáles no.

Para ello conseguir esa individualización, se deben seguir indicadores diferenciales como calificaciones, resultados, comentarios, dudas, tasa de seguimiento y tasa de abandono. Además, señalan como elemento principal el compromiso por parte de los profesores, por ejemplo, atendiendo a los comentarios en etapas iniciales de los cursos. Si se atienden desde el principio, las dudas disminuyen a lo largo de las partes restantes del curso. Se debe tener en consideración en los cursos el diseño de la interacción, ya que si queremos que haya participación o interactividad, se debe tener en cuenta la audiencia, tanto por rangos de edades como por regiones. Según este estudio, los alumnos más comprometidos son los que se encuentran entre 20 a 40 años y los mayores de 60.

En cuanto a los factores de protección de los niños, Crescendzi-Lanna et. Cols (2019) proponen una idea de protección de forma amplia. A través de una observación sistemática de 200 apps para menores de ocho años, sugiere una definición multidimensional de protección que no se limita a detallar los riesgos potenciales, sino que también considera aspectos relacionados con el potencial educativo e inclusivo de los recursos digitales. Los cinco factores a considerar para seleccionar estos recursos y contribuir a la competencia digital de docentes y alumnos son: El uso de mecanismos de protección y la existencia de interferencias externas; presencia de herramientas de adaptación; la exposición a estereotipos corresponde; conocimientos previos requeridos y por último, el componente verbal de las apps.

Además, también existen recomendaciones de cara a la educación de los menores por parte de los padres. Se indican como buenas prácticas para los padres con relación a la ciberseguridad de sus hijos las siguientes: "*conocer las políticas de uso de las redes sociales a que accedan sus hijos/as investigar y configurar la seguridad y privacidad de la cuenta o perfil y delimitar quiénes pueden acceder a los contenidos y publicaciones que hacen, así como a la información que dejan abierta. El monitoreo, el acompañamiento y la supervisión sobre el uso correcto de las redes sociales en línea debe ser constante*" (Astorga-Aguilar & Schmidt-Fonseca, 2019: Pg.20). En definitiva, es fundamental desarrollar programas de formación más eficaces y en formas de animar a los usuarios más jóvenes a comportarse de forma más segura (Cain et al., 2018).

Es de destacar la importancia también del flujo de noticias como forma de concienciación, y a su vez, como forma de transmisión de conocimiento. Ante la necesidad de fomentar la ciberseguirdad en la población, algunos autores (Rincón & Prieto, 2020) plantean el desarrollo de un sistema web para poder hacer un seguimiento de noticias y luego difundirla mediante un portal de ciberseguridad. De este modo, se permitía obtener información acerca de ciberseguridad y, a su vez, retransmitirla de cara a fomentar la ciberseguridad en la sociedad. Como ventajas de automatizar esta información, los autores señalan que permitirá tener un mejor control. El beneficio viene dado en que primero se van a registrar las noticias que se consideren importantes en el sistema. Una vez hecho esto, se podrá integrar la información en tiempo real para, posteriormente, dejar a disoposición a cualquier ciudadano la información respecto a la ciberseguridad que desee.

Aunque este concepto es importante, también es cuestionable el acceso que la ciudadanía de a pie tendría a este portal centralizado. La limitación no vendría tanto sobre la dificultad de acceder a él, ya que funcionaría como cualquier Web, sino por la falta de interés general en consultar esa información. La utilidad de este instrumento como promotor de la cultura de ciberseguridad y educación en ciberseguridad sería más realista si, como herramienta de retransmisión, se le dotara de acceso a otro medios públicos de acceso masivo. Los medios pueden ser la televisión, radio, periódico (en papel y digital), que llegan a una mayor cantidad de personas. Por lo tanto, debería darse un flujo desde ese portal centralizado de noticias de ciberseguiridad para luego retransmitirse en la medida de lo posible al público general por los “mass media”, ya que normalizar las noticias de este ámbito, podrían despertar el interés y la concienciación sobre nuestra protección y privacidad en el ciberespacio.

Plantean que las personas que aún no tienen dicha cultura de la seguridad de la información, tiendan a estar más expuestas a que sus datos sean utilizados con distintos fines. También que la falta de seguridad digital implica que estemos expuestos a ataques de ciberdelincuentes y espionaje. Como datos, en el estudio se obtuvo solo el 57.1% conoce a qué se refiere la seguridad de la información en Internet, el 56.3% desconoce las medidas básicas de la seguridad de la información, y finalmente, el 75.9% no sabe a quién acudir en caso de que terceros hagan mal uso de sus datos personales (Rincón & Prieto, 2020).

III. INVESTIGACIONES REALIZADAS

Tras una revisión de la literatura científica sobre el ámbito de estudio, se ha procedido a llevar a cabo las distintas lineas de investigación para responder a las preguntas de investigación plantadas, cumplir los objetivos de investigación y confirmar o rechazar las hipótesis planteadas. La pregunta general planteada es la siguiente ¿Se está consiguiendo prevenir a la población general ante la ciberdelincuencia mediante la educación en ciberseguridad?. En cuanto a las 4 preguntas específicas planteadas para esta investigación son:

1. ¿Cuál es la situación de la educación en ciberseguridad orientada a la población en general?
2. ¿Cómo se está educando en ciberseguridad, qué técnicas didácticas y proyectos educativos se están poniendo en marcha?
3. ¿Las víctimas tienen conocimientos sobre la ciberdelincuencia y nociones de ciberseguridad?
4. ¿Cómo se podría mejorar la estrategia de educación en ciberseguridad? Apartado Recomendaciones y Análisis de expertos.

Para responder a dichas cuestiones, se han establecido unos objetivos específicos y un objetivo general. El general es analizar las estrategias de educación en ciberseguridad dirigidas a la población general. En cuanto a los específicos son:

1. Explorar los distintos proyectos implementados y los resultados obtenidos, atendiendo a la diferencia entre educación a nivel básico y avanzado.
2. Realizar un análisis descriptivo mediante la recopilación de bibliografía , analizar la evolución de la cuestión objeto de estudio, los principales autores, teorías y estudios realizados.
3. Recopilación y análisis de la literatura reciente sobre la educación en ciberseguridad y el análisis bibliométrico de los mismos.
4. Identificar las estrategias y técnicas didácticas para la educación en ciberseguridad.
5. Determinar las diferencias de conocimientos en ciberseguridad entre personas que han sido víctimas de ciberdelitos y personas que no: se utilizarán métodos de investigación correlacional para investigar las diferencias entre población víctima de ciberdelitos y los no-víctimas.

6. Obtener información sobre la capacidad y conocimientos de la población general en ciberseguridad.

Las hipótesis que se plantearon para esta investigación fueron las siguientes:

H1: La educación en nociones básicas de ciberseguridad y ciberamenazas es un elemento clave para mejorar la protección de las potenciales víctimas.

H2: La educación en ciberseguridad actualmente estaría descompensada, debido a que se habría centrado más en aquella dirigida a un nivel avanzado, para personal cualificado o que vaya a tener un desempeño en el ámbito, por lo tanto, a individuos que tienen competencias en ciberseguridad o que necesitan de conocimientos técnicos para su trabajo. Sin embargo, habría tenido un menor impacto aquella enfocada a explorar la educación básica en la población en general (población no-técnica). Consecuencia de ello, sería que la amplitud de la oferta educativa en ciberseguridad se configura en especializaciones, másteres, y cursos para personas en puestos clave y no a la ciudadanía, a un a nivel básico, para poder prevenir la cibervictimización.

H3: Las víctimas presentan desconocimiento de elementos claves de ciberseguridad, además de una menor percepción de la amenaza frente a otros delitos, lo que las hace más vulnerables; Por lo tanto, los que han sido víctimas, tendrán alta correlación con vulnerabilidad y relación inversa con conocimientos en ciberseguridad. Las personas que tengan altas puntuaciones en conocimientos, tendrán menor vulnerabilidad y será más probable que no sean víctimas de ciberdelitos frente a los que tienen bajas puntuaciones en conocimientos.

Finalmente, las líneas de investigación que se llevaron a cabo en base a estas preguntas, objetivos e hipótesis fueron: un análisis de la Teoría de Actividades Rutinarias aplicada al ciberespacio (Cyber-TAR), una revisión bibliométrica, una revisión sistemática sobre las técnicas educativas, una consulta a expertos y un estudio basado en cuestionario que se administró a 229 participantes.

Estudio 1. Teoría de las Actividades Rutinarias

1. CyberTAR – Teoría de las Actividades Rutinarias en el Ciberespacio

RESUMEN

La CyberTAR o CybeRAT en inglés (Cyber-Routine Activities Theory), es la integración de los conceptos de la Teoría de las Actividades Rutinarias (TAR) a los delitos informáticos y al ciberespacio. Según esta teoría, los ciberdelitos se basan en las redes

informáticas para conectar a los delincuentes motivados con objetivos potenciales de victimización en ausencia de una tutela capaz. La idea de relacionar la TAR con el mundo virtual consiste en que la organización del hecho delictivo tiene una equivalencia en los entornos virtuales y los escenarios físicos. Por lo tanto, considera las oportunidades delictivas como la causa última de los hechos delictivos.

TEMAS RELACIONADOS: Teorías criminológicas; Actividades rutinarias; Cibercrimen; Internet; Oportunidad.

DEFINICIÓN Y ORIGEN

La Teoría de las Actividades Rutinarias (de ahora en adelante TAR) fue formulada por Cohen y Felson para explicar cómo los cambios sociales modificaban los hábitos y las actividades cotidianas de las personas. A su vez, estas creaban entornos de oportunidad para cometer delitos (Cohen & Felson, 1979). Desde la TAR encontramos múltiples estudios que han analizado la victimización online. Esta teoría se fundamenta en 3 elementos: un delincuente motivado, una víctima adecuada, y un guardián eficaz (cuya presencia disuada el delito y su ausencia lo facilite). También se sostiene que el delito es equivalente en escenarios físicos y virtuales y, en consecuencia, la cibervictimización puede ser tratada apropiadamente a la luz de la propuesta de Cohen y Felson (Yar, 2005).

La TAR tiene como premisa la convergencia física de los delincuentes y las víctimas en tiempo y espacio, pero en el ciberespacio esto quedaría obsoleto, es por ello que se necesita una redefinición de la teoría más exacta y precisa para poder explicar los comportamientos online. Choi (2008) propuso la teoría CyberTAR (CyberRAT en inglés) integrando los conceptos de la TAR a los delitos informáticos "*Cyber-Routine Activities Theory*" o "*Cyberlifestyle-Routine Activities Theory*". Dentro de la criminología, forma parte de la perspectiva de la oportunidad que considera las oportunidades delictivas como la causa última de los hechos delictivos. Según esta teoría, los ciberdelitos se basan en las redes informáticas para conectar a los delincuentes motivados con objetivos potenciales de victimización en ausencia de una tutela capaz. La CyberTAR sostiene que la separación de los delincuentes motivados y los objetivos adecuados en el tiempo puede conciliarse considerando su interacción como "retrasada en el tiempo" (Reyns, 2017).

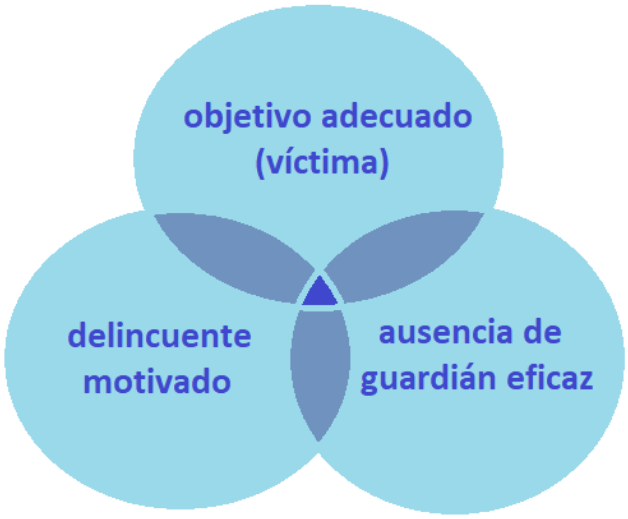


Figura 1 Convergencia en el espacio de los 3 elementos de la TAR Clásica.

La idea de relacionar la TAR con el mundo virtual consiste en que la organización del hecho delictivo tiene una equivalencia en los entornos virtuales y los escenarios físicos. Es por ello, que autores como Yar (2005) establecen que la civervictimización puede ser tratada apropiadamente a través de la TAR. El ciberespacio cumple el criterio ecológico de la RAT en el que se crea un espacio-temporal (virtual) en el que convergen los elementos al igual que en el mundo físico. Proximidad, lugar distancia y orden temporal. En esta línea, autores como Rodríguez (2017) ejemplifican el paralelismo con situaciones: enseñar el dinero en una taquilla de pagos y dar información en Facebook sobre nuestro banco; tener un antivirus en el ordenador y un que haya un vigilante de seguridad en la tienda a la que vamos todos los días.

En la CyberTAR, diversos autores se han centrado en identificar de manera empírica cada uno de los elementos que conforman el triángulo del delito. Sin embargo, no existe un acuerdo sobre cómo deben ser conceptualizados y medidos los elementos de la TAC en el ciberespacio (García-Guilabert, 2014). Por otra parte, a través de sus estudios, se puede obtener una serie de factores considerados de riesgo, ya que aumentan la probabilidad de convertirse en víctimas en el ciberespacio. A su vez, todos los factores de riesgo pueden ser agrupados de acuerdo con las características que hacen a un objetivo adecuado en el ciberespacio. Esta misma argumentación sirve para tratar de explicar cómo las TIC y, más que estas, las actividades de los usuarios a través de ellas, generan oportunidades para realizar cibercrímenes (Guilabert-García, 2016). En el caso de la CyberTAR, habría también un cambio en los tres componentes, que según algunos

autores pasarían a ser: un delincuente potencial, un objetivo potencial y una red virtual (Eck & Clarke, 2003). Estos componentos no coinciden con los defendidos por otros autores, que sí añaden el “guardian” como elemento central.

Varios estudios han demostrado la asociación predictiva entre los comportamientos en línea de riesgo, la exposición a delincuentes potenciales y los factores de visibilidad en línea con los resultados de victimización (DeKimpe et al., 2018). De hecho, se encontró que el comportamiento de compra en línea y copia digital estaba asociado con una mayor victimización (objetivo de phishing). En el caso de Choi (2008), los dos factores que seleccionó Choi para sus estudios son: el guardián digital o guardían eficaz “digital guardianship” que es la ciberseguridad, y por otra parte las actividades rutinarias, en referencia a aquellas actividades vocacionales y de ocio. Choi plantea que las actividades rutinarias y la ausencia de este guardián digital eficaz son los que contribuyen a la cibervictimización (Choi 2008).

La relevancia de la aportación de Choi es que hace una evaluación empírica del modelo de victimización por delitos informáticos aplicando la TAR. Tras poner a prueba los componentes de la TAR , hace un modelo de ecuaciones estructurales para ver si existen relaciones significativas entre las actividades cotidianas online, los niveles de seguridad informática y los de victimización individual por ciberdelitos. Tras administrar una encuesta de autoinforme con medidas de riesgo y victimización, halla un apoyo empírico para estos componentes, dibujando unos patrones de victimización por delitos informáticos (Choi, 2010). Se defiende que los estilos de vida en línea imprudentes (abrir adjuntos y enlaces web enviados por correos electrónicos desconocidos o ingresar en mensajes pop-up) aumentan la probabilidad de victimización por infección de virus. Y, al contrario, disponer de un guardián digital (programas antivirus, antispyware y firewall), disminuye tal probabilidad (Choi, 2008).

Estas barreras o protecciones desplegadas por el usuario vendrían a ser fruto de la capacidad del ciudadano. Si bien es cierto que algunas medidas vienen de serie y son ajenas al propio usuario (servicios de protección), otras serán proporcionales a los conocimientos que tenga (Miró, 2011). El modo en que desarrolla sus actividades en el ciberespacio también serán un reflejo de sus capacidades para protegerse cuando navega en él. Por lo tanto, la idea del guardián eficaz tendría una doble vertiente, la externa, o proveniente de los Sistemas operativos, antivirus, navegadores, etc. y en la el conocimiento no tiene ningún papel. Y por otro lado la interna, que son aquellas medidas implementadas por la potencial víctima para evitar ser vulnerable (contraseñas seguras, comprobación de enlaces, detección de phishing...,) (Yar, 2005).

Algunos autores apuntan a algunas prácticas online que hacen más probable la exposición a delincuentes motivados (uso de correo electrónico, mensajería instantánea, salas de chat y redes sociales) y la idoneidad del objetivo (información personal compartida en redes sociales), que se relacionaron con la victimización por exposición a material sexual, acoso y proposición sexual no deseados (Rodríguez, 2017). Un estudio más reciente en esta línea se orientó a identificar algunos predictores de la victimización cibernética mediante una encuesta de victimización, donde encontraron que “el guardián eficaz” (software antimalware) mostró tener el efecto más fuerte y estable sobre las distintas formas de victimización cibernética, en especial sobre las de acoso en línea.

También existen algunos pasos preparatorios realizados por los ciberdelincuentes para llegar a sus víctimas: La recepción de correos electrónicos de spam, la recepción de correos electrónicos de phishing y la infección por malware, que se conceptualizan como “tipos de aproximación llevados a cabo por los delincuentes”. Además, son los tipos de ciberataques que más comúnmente experimentan las víctimas potenciales dentro de las actividades rutinarias de los usuarios (Miró-Llinares et al., 2020).

Además del hecho de que algunas personas son más vulnerables que otras a los ciberataques, también hay que tener en consideración el factor geográfico, ya que la vulnerabilidad varía nivel transnacional. Por ejemplo, en un estudio comparativo entre España y Australia se encontró que el mayor riesgo para los participantes españoles es la compra en línea, mientras que para los australianos es la descarga de archivos (Miró-Llinares et al., 2020). También se encontraron diferencias en el uso de antivirus, software pirata, contacto con extraños y participación en videoconferencias. Por lo tanto, las estrategias de prevención deben tener en cuenta las diferencias en los comportamientos habituales en las distintas zonas geográficas.

En cuanto a esta variable “espacio” (ciberespacio), no es del todo neutral ya que le corresponde una realidad social. Sin embargo, es un lugar de encuentro más diluido que la realidad física, separada en paises, guetos, urbano rural, y que hace difícil un punto de encuentro como sí lo hace en el mundo virtual. También hay que tener en cuenta que las diferencias existentes en el ciberespacio en el año 2005 que es cuando se menciona esta diferencia (Yar, 2005) ya no es la misma que en el año 2021. Vivimos en un mundo más globalizado en donde el acceso a Internet es generalizado, donde el peso de conomías emergentes como China hay redibujado el mapa internacional y más aún si tenemos en cuenta que gran parte de los ciberataques se generan en países como Rusia y China.

La teoría del TAR tiene como presupuesto la capacidad del infractor de predecir cuándo poder actuar sobre la víctima, por lo tanto incluyen no solo la concurrencia del espacio, sino también del tiempo. Es el ordenamiento de carácter temporal en una secuencia ordenada lo que permite a los delincuentes la capacidad de anticipación. Esta idea en el mundo físico es bien distinta del ciberespacio, donde no hay un orden temporal claro. El ciberespacio es atemporal, globalizado y con una zona horaria a nivel mundial, por lo tanto este traspaso de sincronicidad temporal del mundo real al ciberespacio es dificil en términos de TAR. Tal y como se expone en Yar (2005) las actividades rutinarias en el ciberespacio se producen en el trabajo, hogar, ocio, y no limitadas a un momento concreto y delimitado, y por lo tanto dificil de anticipar para los infractores. "*el ritmo y la sincronización como propiedades estructurantes de las actividades rutinarias se vuelven problemáticos para los infractores, para los posibles objetivos y para los tutores. Dada la naturaleza "desordenada" de las espacio-temporales virtuales, la identificación de patrones de convergencia entre los elementos criminógenos se vuelve especialmente difícil"* (Yar, 2005: Pg.16).

No obstante, lo que no tiene en cuenta esta afirmación, es que una de las principales cualidades de la red es que en gran medida es asíncrona. Envío de mails que son posteriormente leídos, creación de contenidos para páginas web a los que se acceden en cualquier momento, mensajes y contenidos de redes sociales a los que se accede cuando se desea, etc. Ello no quiere decir que el delincuente pueda anticipar que el contenido será abierto, que le mensaje será leído o que la acción de la persona será realizada. La sincronización temporal de la TAR queda desdibujada aquí, pero no el fondo explicativo, ya que se dan los elementos necesarios: un infractor que predice una situación, un objetivo que será víctima en un momento determinado (no necesariamente en el momento de realizar la acción el delincuente) y la ausencia de un guardián necesario.

En cuanto al grupo de factores relacionados con la visibilidad del usuario en Internet, se debe tener en cuenta que, en el ciberespacio, hay más probabilidad de convertirse en un blanco potencial para el delincuente cuanto más visible sea. La visibilidad se define como el grado de interacción y exposición que tiene la víctima a los ciberataques (Miró-Llinares et al., 2020). Existirían una serie de conductas a partir de los cuales los usuarios se hacen más visibles: la interacción, realizar compras y reservas por internet, descargar videojuegos, música, películas, abrir archivos adjuntos, abrir enlaces recibidos por correo electrónico o por mensajería instantánea, empleo de redes sociales, contactar con personas desconocidas y empleo de banca electrónica (Miró, 2011; Leukfeldt et al., 2016; Yar, 2005). Los estudios de cibervictimización deben incluir la idoneidad y la

visibidad del objetivo, es decir, en aquellos comportamientos que hacen a las víctimas potenciales más visibles y más accesibles a los ciberataques. Se debe a que ambas presentan fuertes correlaciones de victimización (Miró-Llinares et al., 2020; Drew & Farrell, 2018).

Sobre la ausencia de elementos de autoprotección de sus sistemas para defenderse de los ciberataques, correspondería con la ausencia de guardián eficaz. Sería el caso, por ejemplo, de antivirus, antiespías (Antispy) , cortafuegos o la gestión correcta de contraseñas (Miró, 2012). Finalmente, el grupo de factores relacionado con los bienes personales consistiría en aquellos factores relacionados con la introducción de bienes en el ciberespacio, ya que una vez en el mismo, pueden estar disponibles para ser atacados. Algunos ejemplos son la publicación de información personal o tener información personal (como contraseñas) en los dispositivos (Guilabert-García, 2016). Por este motivo son necesarios los conocimientos informáticos, ya que cuanto mayores sea este, mayor es también el nivel de conocimiento de las amenazas del ciberespacio (Ismailova & Muharnetjanova, 2016).

Por su parte, Alalwan (2018) defiende que el efecto funcional del miedo a los ciberdelitos puede desempeñar un papel importante en la adhesión de los individuos a la política de seguridad de la organización en la que trabajan. La literatura sobre el miedo a la delincuencia concluye que el miedo a la delincuencia puede tener efectos funcionales y disfuncionales. Por lo tanto, se puede desgranar en 4 posibilidades: el individuo estará preocupado o despreocupado por ser víctima de la ciberdelincuencia y será funcional o disfuncional en cuanto al cumplimiento de la política organizativa de seguridad (Alalwan, 2018). Es también importante tenerlo en consideración ya que el miedo al ciberdelito no siempre será funcional. Bigdoli et al. (2016) creen que las percepciones de los usuarios es importante porque, su miedo a los ciberdelitos y su capacidad percibida para mitigar la victimización (la autoeficacia), puede influir en que se tomen medidas preventivas, se eviten conductas de riesgo en línea y se denuncien las victimizaciones. También estudiaron el origen del conocimiento sobre los ciberdelitos para poder explicar el cómo los perciben y cómo lidian con la victimización.

INVESTIGACIÓN EMPÍRICA

La CyberTAR fue aplicada en un modelo de victimización por delitos informáticos. Su evaluación dio como resultado un apoyo empírico para esta teoría en el mundo del ciberespacio y, además, señalar patrones de victimización. Las variables que contribuyen a la victimización por delitos informáticos son las variables de estilo de vida, o lo que es lo mismo, los patrones diarios de las Actividades Rutinarias de las personas.

También incluyen de nuevo el papel fundamental del guardián eficaz en el ciberespacio como un factor contra la victimización. Choi (2008), señala la falta de concienciación sobre los delitos informáticos como explicación para que los patrones de estilo de vida aumenten significativamente las oportunidades delictivas. También se evaluó si el guardián digital y el estilo de vida en línea influyen directamente en la victimización por delitos informáticos empleando modelos de ecuaciones estructurales. Por otra parte, se sugiere que los usuarios que pasan por alto su estilo de vida orientado a la computadora en el ciberespacio, o que descuidan la presencia de software de seguridad informática en su computadora, probablemente sean victimizados. Como resultado de la evaluación, cabe destacar que el estilo de vida en línea y la tutela digital son aspectos importantes de un modelo que delinea patrones de victimización por ciberdelitos, y también que la presencia de seguridad informática es el componente más crucial para proteger a las potenciales víctimas (Choi, 2008).

Un estudio más reciente en esta línea (Rodriguez, 2017) se orientó a identificar algunos predictores de la victimización cibernética mediante una encuesta de victimización. Encontraron que “el guardián eficaz” (software antimalware) mostró tener el efecto más fuerte y estable sobre las distintas formas de victimización cibernética, en especial sobre las de acoso en línea. Hubo algunas relaciones contrarias a las expectativas de la CyberTAR, como señalan propiamente los autores, pudieron ser consecuencia de que no se tuvo en cuenta el orden temporal de las relaciones. Sería el ejemplo de una persona que fue víctima de algún tipo de ciberdelito luego comienza a tener conductas de control, restringir la entrada en webs extrañas, configurar privacidad de redes sociales, instalar software como antivirus, etc.

Siguiendo el enfoque de la CyberTAR sobre la probabilidad de cibervictimización , en Rodríguez (2017) analizaron estadísticamente si la exposición a un delincuente motivado, la idoneidad del objetivo/víctima y la falta de vigilancia efectiva tienen correspondencia con el hacking y el acoso en línea. Como resultados, se halló que el guardián eficaz el que tiene un efecto fuerte y estable sobre las distintas formas de victimización cibernética, en especial sobre las de acoso en línea. La exposición a un delincuente motivado presentó una predicción más inestable. Hubo tres medidas estadísticamente relacionadas con algunos de los cinco indicadores de cibervictimización conforme la TAR. Las personas que pasaron más tiempo en internet fueron más propensos a ser victimizados por acoso online. El uso de software antimalware hacía disminuir la cibervictimización y la solicitud de eliminación de datos en registros de Internet (la cual disminuyó el riesgo tanto de hacking como de online harassment (Rodriguez, 2017).

Otro autor también a favor de la aplicación de la TAR en ciberseguridad es McQuade (2006). Afirmó que "*la teoría de las actividades rutinarias tiene importantes implicaciones para comprender los delitos cometidos o prevenidos con computadoras, otros dispositivos informáticos o sistemas de información*". Afirma que promover un estilo de vida en línea adecuado reducirá la victimización, y a su vez, destaca el empleo de la seguridad informática eficiente para conseguir ese mismo objetivo. McQuadeDefiende que una gran oportunidad para minimizar los delitos informáticos a través de una mayor seguridad de la información es a través de la "conciencia pública, educación formal y capacitación profesional", reafirmando así su apuesta por el papel de la educación en ciberseguridad, concienciación y capacitación para minimizar delitos informáticos. Además, un programa educativo en ciberseguridad, también debe incluir estilos de vida en línea adecuados, alertando al individuo sobre comportamientos de riesgo (Moitra, 2005).

En el caso de Choi (2008), se le atribuyen como hallazgos empíricos en favor de esta teoría, que los estilos de vida online imprudentes aumentan la probabilidad de victimización en red, incluyendo conductas como abrir correos de desconocidos, ingresar en pop-up o archivos adjuntos que no sean de confianza. Además, en referencia al guardián digital disminuiría la probabilidad de ser víctima, entendiendo al guardián digital como el conjunto de programas antivirus, antispyware y firewall.

Alshalan (2009) aplica la CybeTAR para determinar cómo afecta el uso de Internet a la victimización, específicamente, los factores que afectan al miedo al ciberdelito. Descubre que el 80% de los usuarios encuestados están "muy preocupados", y que existe un alto nivel de miedo a la ciberdelincuencia entre las mujeres, los que han sido víctimas anteriormente y los que consideran que la ciberdelincuencia es grave. Algunas investigaciones hallaron que cuanto mayor es la amenaza percibida, las víctimas potenciales estarán más motivadas para poner en marcha las medidas de seguridad (Sommestad et al., 2015; Thompson et al., 2017; Marten et al., 2019). También que la percepción de la prevalencia de la cibercriminalidad tiene impacto en la decisión de usar estrategias de autoprotección (Martens et al., 2019; Drew, 2020).

También en Choi & Lee (2017) se continúa el legado de la TAR aplicada al ciberespacio para realizar un estudio que determine si los factores de riesgo en los estilos de vida en línea y la gestión de la ciberseguridad influyen en los ciberdelitos contra las personas. Como variable determinante, plantean que son los individuos que llevan a cabo comportamientos más arriesgados y que no administran eficanzmente la configuración de seguridad, serán los que tienen más probabilidad de ser víctimas. También plantea un punto intermedio entre la propia TAR clásica de Cohen y la versión CyberRAT de

Choi, en la que existiría un uso del ciberespacio para poder cometer delitos en el mundo físico, por ejemplo "*Cuando una persona publica información sobre sus vacaciones en internet y esto es aprovechado por los delincuentes para robar en su casa*". En relación con ello, Liang & Xue (2010) encuentran que las creencias sobre la vulnerabilidad personal son un factor motivacional clave que aumenta la probabilidad de adoptar conductas de ciberprevención.

Analizan la victimización y el delito de violencia ciber-interpersonal utilizando los tres componentes por excelencia de Cyber-RAT: un delincuente potencial, un objetivo potencial y una red virtual. En ella, se respalda empíricamente la CyberRAT en el sentido de que los estilos de vida arriesgados se relacionan con los riesgos de victimización por acoso cibernético interpersonal. También la gestión deficiente de la ciberseguridad se relacionó positivamente con la cibervictimizción. Por lo tanto, aquellas personas que se involucran en conductas de riesgo online y no manejan adecuadamente la ciberseguridad, tendrán una mayor probabilidad de experimentar la victimización por acoso cibernética interpersonal.

El estudio aporta importantes hallazgos para la CyberTAR, ya que amplía sus capacidades explicativas de los delitos informáticos como el hackeo, a otro tipo de delitos informáticos como el acoso online (ciberacoso). Por lo tanto, refuerza la idea de que la teoría del CyberTAR es apropiada y capaz de dar cuenta de distintos comportamientos online (Choi & Lee, 2017). También lanzan la siguiente recomendación: "La esperanza es que la educación sobre los peligros potenciales de Internet y la violencia cibernética interpersonal induzca una actividad online y un compromiso más responsables".

Por su parte, Guilabert-García (2016) realizó un estudio para analizar el alcance de victimización de malware entre la población juvenil y, también, para determinar qué actividades de las que realizan los jóvenes de manera cotidiana en Internet inciden en la probabilidad de sufrirlo. Concluye que se puede confirmar la importancia del comportamiento del usuario en la probabilidad de que sean víctimas de cibercrimen. Existirían, por lo tanto, determinadas actividades que los jóvenes realizan de manera cotidiana que aumentan el riesgo de que sus dispositivos se infecten de códigos maliciosos.

En cuanto a Drew (2020), existiría una relación entre la victimización previa y la percepción del daño causado con esas medidas de autoprotección. El estudio buscaba comprender mejor cómo la victimización previa, la percepción de la prevalencia del ciberdelito y la percepción del daño causado se relacionan con el uso de estrategias de

prevención. Hallaron que esos factores son fundamentales en el uso de estrategias de prevención por parte de las víctimas. Al comprender qué factores están asociados con la decisión de un individuo de utilizar comportamientos de prevención/autoprotección, se podrían integrar en el diseño de iniciativas y programas de prevención del ciberdelito (Drew, 2020).

Una de las críticas al modelo de RAT es que no es de fácil aplicación en delitos que no son de tipo racional, como pueden ser asesinatos, delitos pasionales, etc. sin embargo, en la ciberdelincuencia, es difícil salir de un esquema explicativo que no incluya un autor que actúe de forma racional y a sabiendas de lo que hace. Los delitos de tipo racionales, de tipo económicos contra el patrimonio, vendrían a se explicados por modelos similares (Yar, 2005). Expone que algunos conceptos son iguales, pero existirían ciertas diferencias requiriendo así un nuevo marco explicativo, con vocabulario y terminología propia (CyberTAR). En la misma línea están Capeller (2001) y Snyder (2001) que defienden la idea de aplicar la misma teoría pero con modificaciones de los conceptos "*Lo de siempre pero con nuevo molde".* Por otro lado, están los que defienden la idea de que sería posible adaptar los esquemas clásicos a estas nuevas formas de delincuencia. Es para estos últimos posible, por lo tanto, explicar y analizar el ciberdelito mediante las teorías orientadas a la criminología "terrestre" como pueden ser la RAT.

En el estudio de Miró-Llinares et al. (2020) se descubrió que el riesgo de sufrir spam, estafas y malware aumenta en función de la cantidad de compromiso que tienen las víctimas potenciales, pero está asociado a tipos específicos de actividades en el ciberespacio. Por otra parte, la participación en foros/blogs online, mensajería instantánea, redes sociales y videojuegos no tenía influencia en ningún tipo de victimización en las muestras estudiadas. En cuanto a los esfuerzos en educación, plantean que deben centrarse en gran medida en el riesgo de descargar archivos, ya que la descarga de archivos está asociada tanto a la victimización por spam como por estafa.

Finalmente, como limitación al enfoque, señalar que algunos autores como Ngo & Paternoster (2011) analizaron la capacidad predictiva de la TAR en algunas formas de victimización online, pero los resultados no consiguieron dar respaldo empírico a la teoría (Rodríguez, 2017). También se ha concluido en relación a la limitación actual de la TAR que "*la comprensión actual de la idoneidad de los objetivos, la visibilidad de los mismos y el papel de los comportamientos de autoprotección y tutela en el ciberespacio es limitada"* (Miró-Llinares et al., 2020).

Referencias bibliográficas

Alalwan, J.A. (2018). Fear of cybercrime and the compliance with information security policies: a theoretical study. Proceedings of the 9th International Conference on E-Education, E-Business, E-Management and E-Learning. 85–87. https://doi.org/10.1145/3183586.3183590

Alshalan, A. (2009). Cyber-Crime Fear and Victimization: An Analysis of a National Survey.

Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016). When cybercrimes strike undergraduates. ECrime Researchers Summit, ECrime, 2016-June, 42–51. https://doi.org/10.1109/ECRIME.2016.7487948

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. Social & Legal Studies 10, 229–42.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology, 2(1), 308e333

Choi, K. (2010). Risk Factors in Computer-Crime Victimization. LFB Scholarly Publishing LLC. Retrieved from https://www.perlego.com/book/2028086/risk-factors-in-computercrime-victimization-pdf

Choi,K., & Lee, J.R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory, Computers in Human Behavior. DOI: 10.1016/j.chb.2017.03.061

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review 44: 588-608.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. Telematics & Informatics, 35, 1277-1287.

Drew, J.M., & Farrell, L. (2018). Online victimisation risk and self-protective strategies: Developing police-led cyber fraud prevention programs. Journal of Police Practice and Research: An International Journal, 19, 537-549.

Eck, J. E. & Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. Theory and Practice in Situational Crime Prevention, Crime Prevention Studies, 16, 7e39.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. Int. J. Cyber Criminol., vol. 5, no. 1, p. 773

Garcia-Guilabert, N. (2014). Victimizacion de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio. Escuela Internacional de Posgrado.

García-Guilabert, N. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. IDP. Revista de Internet, Derecho y Política, (22),48-61. Disponible en: https://www.redalyc.org/articulo.oa?id=78846481005

Ismailova, R., & Muhametjanova, G. (2016): Cyber crime risk awareness in Kyrgyz Republic, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2015.1132800

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394-413.

Martens, M., DeWolf, R., & DeMarez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior, 92, 139-150.

McQuade, S.C. (2006). Understanding and managing cyber crime. Boston:Pearson/Allyn and Bacon. Vol.1 No.3.

Miró, F. (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología, núm. 13-07.

Miró-Llinares, F., Drew, J., & Townsley, M. (2020). Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. International Journal of Cyber Criminology, 14(1), 139-155. Retrieved from https://www.proquest.com/scholarly-journals/understanding-target-suitability-cyberspace/docview/2404395082/se-2

Moitra, S. (2005) Developing policies for cyber crime. European Journal of Crime, Criminal Law and Criminal Justice, 13(3), 435-464

Reyns, B.W. (2017). Routine Activity Theory and Cybercrime: A Theoretical Appraisal and Literature Review. Technocrime and Criminological Theory. ISBN 9781315117249.

Rodríguez, J.A., Oduber, J., & Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20),63-79.[fecha de Consulta 10 de Febrero de 2021]. ISSN:

1390-3691. Disponible en: https://www.redalyc.org/articulo.oa?id=5526/552656641006

Snyder, F. (2001). Sites of criminality and sites of governance. Social & Legal Studies 10, 251–6.

Sommestad, T., Karzen, H. & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International Journal of Information Security, 9(1), 26-46.

Thompson, N., Mcgill, T.J., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behaviour. Computers & Security, 70, 376-391.

Leukfeldt, E.R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behaviour, 37(3), 263-280.

Yar, M. (2005). «The Novelty of "Cybercrime" An Assessment in Light of Routine Activity Theory». European Journal of Criminology, Vol. 4, núm. 2, págs. 407-427. http://dx.doi.org/10.1177/147737080556056

2. CyberTAR y educación en ciberseguridad

El encaje de la educación en ciberseguridad y ciberdelincuencia dentro de este marco teórico viene a ser que, si se refuerzan los conocimientos en ciberseguridad y las distintas formas de ciberdelincuencia, la probabilidad de victimización disminuirá. En primer lugar, el guardián eficaz (ciberseguridad) se verá reforzado, al igual que la concienciación y los conocimientos, que vendrán reflejados en las actividades rutinarias. Los esfuerzos en educación deben centrarse en gran medida en el riesgo de descargar archivos, ya que dicha conducta es de las que está más asociada tanto a la victimización por spam como por estafa.

Las conductas imprudentes, como abrir adjuntos y enlaces web enviados por correos electrónicos desconocidos o ingresar en mensajes pop-up, aumentan la probabilidad de victimización por infección de virus. Por el contrario, disponer de un guardián digital (programas antivirus, antispyware y firewall) disminuye tal probabilidad (Choi, 2008). Estas son variables que guardarían relación con la educación en ciberseguridad, ya que esta incide directamente con los modos en como interactuamos con las TIC, y sobre todo, en cómo nos protegemos externamente adquiriendo software de seguridad.

El elemento central que resultaría de mayor interés de esta teoría explicativa es la idoneidad del objetivo. Este elemento se relacionaría directamente con la educación en ciberseguridad ya que está encaminado a proveer a la persona de conocimientos y mecanismos para evitar ser víctima de ciberdelitos. Esas capacidades serán las que harán disminuir la idoneidad y, por lo tanto, reducir la probabilidad de ser víctima. La idoneidad del objetivo en la nueva versión de la TAR juega un papel crucial como lo hacía en la TAR clásica. Se suele decir que en ciberseguridad, el eslabón más débil es el factor humano y, en consecuencia, un trabajador de una empresa que es engañado con un email falso y termina realiza pagos a una cuenta de los ciberdelincuentes, deja por tierra los esfuerzos técnicos en materia de ciberseguridad. Es ahí donde reside la fuerza de la CyberTAR como corriente explicativa y el valor de la educación en ciberseguridad en relación con el objetivo idóneo.

Las barreras o protecciones desplegadas por el usuario, vendrían a ser fruto de la capacidad del ciudadano, capacidad desarrollada gracias a la educación en ciberseguridad. Como señala Yar (2005) la protección interna, que son aquellas medidas implementadas por la potencial víctima para evitar ser vulnerable (contraseñas segura, comprobación de enlaces, detección de phishing) son las que concuerdan con la educación en ciberseguridad. En cuanto a los esfuerzos en educación, Miró-Llinares et al. (2020) plantean que deben centrarse en gran medida en el riesgo de descargar archivos, ya que descarga de archivos está asociada tanto a la victimización por spam como por estafa. Descubrió que el riesgo de sufrir spam, estafas y malware aumenta en función de la cantidad de compromiso que tienen las víctimas potenciales, pero está asociado a tipos específicos de actividades en el ciberespacio.

Otro punto donde jugaría un papel relevante la educación en ciberseguridad, y especialmente en ciberdelincuencia, es en el otro elemento protector: la concienciación. McQuade (2006) afirma que una gran oportunidad para minimizar los delitos informáticos a través de una mayor seguridad de la información. Al mismo tiempo, defiende que es a través de la “conciencia pública, educación formal y capacitación profesional”, reafirmando así su apuesta por el papel de la educación en ciberseguridad, concienciación y capacitación para minimizar delitos informáticos. Además, un programa educativo en ciberdelincuencia, también debe inlcuír estilos de vida en línea adecuados, alertando al individuo sobre comportamientos de riesgo (Moitra 2005). En la misma línea Choi & Lee (2017) afirman que la esperanza reside en que la educación sobre los peligros potenciales de Internet y la violencia cibernética interpersonal induzca una actividad online y un compromiso más responsables. Por lo tanto, también señalan

a la educación como una variable determinante de cara a incidir en las condutas de riesgo y la autodefensa de los usuarios.

Por otra parte, diversos estudios han aplicado la exposición del estilo de vida a la cibervictimización en el contexto del ciberacoso y el cyberbullying (Marcum et al., 2010; Vakhitova et al., 2016; Kokkinos & Saripanidis, 2017). Otros han aplicado la teoría a ciberdelitos como estafas en línea y phishing (DeKimpe et al., 2018). Estudios, como el de Marcum et al. (2010) han dado un respaldo empírico para la transferibilidad de la teoría de la exposición del estilo de vida al cibersespacio, demostrando la relación entre un estilo de vida arriesgado (compartir información privada en internet) con el aumento de la victimización. Las conductas analizadas tienen un componente educativo en el sentido de que pueden ser modificadas a través del ya expuesto sumatorio de conocimientos y concienciación.

Entre las principales conductas de riesgo a las que se debe orientar la educación es en el acceso a contenidos gratuitos, cuya descarga puede esconder riesgos de seguridad. Otra fuente adicional de riesgo reside en las actividades relacionadas con el comercio online y la realización de transacciones electrónicas, debido al evidente factor económico implicado en dichas actividades. También está el exceso de confianza en la banca electrónica, ya que da pie a que no se compruebe si tienen una conexión segura antes de realizar las transacciones (ONTSI, 2022). No se deben ignorar tampoco el hecho de que después de ser víctima de un ciberdelito, es habitual que existan ciertas modificaciones en el comportamiento para evitar que se vuelva a producir ese tipo de incidentes. Por ejemplo, haciendo copias se seguridad periódicas después de sufrir un ataque de ramsomware (ONTSI, 2022).

Sobre los hábitos, los últimos datos arrojan que el 41% de las personas que han sufrido incidencias de ciberseguridad, no han llevado a cabo ningún tipo de cambio en dichos hábitos. Entre las restantes que sí han cambiado sus conductas (59%), han comenzado principalmente a cambiar contraseñas, usar gestores de contraseñas, a actualizar el software y a efectuar copias de seguridad. También estaría entre los cambios de conductas, el dejar de usar software sin autorización (21%). Este cambio potencial del comportamiento de los/as usuarios/as puede, y debe, ser potenciado por la educación. A través de esta victimización, la educación podría incidir en la concienciación y a su vez en la adquisición de conocimientos.

Bidgoli et al. (2016) descubrieron que el conocimiento sobre ciberdelitos de los estudiantes universitarios proviene predominantemente de los medios de comunicación y del conocimiento personal de alguien que ha sido víctima. Este factor, junto con el

autocontrol en línea, influyeron en sus percepciones de miedo y autoeficacia. A su vez, estas percepciones influyeron en los comportamientos de los participantes en términos de medidas preventivas y comportamientos habilitadores. La educación no se debe dejar en manos únicamente de los medios de comunicación y a las experiencias personales, por lo que la institucionalización en distintos niveles se hace más que necesaria. Por su parte, al señalar el estudio que las percepciones un factor de cambio comportamental (especialmente el miedo y la autoeficacia), permite resaltar la importancia de esa capacidad que pueden tener las instituciones sobre la población objetivo a la hora de poner en marcha mecanismos de cambio. Un ejemplo serían las campañas de concienciación, pero también lo serían los cursos de ciberseguridad en los que se añade un componente de concienciación de cara a las ciberamenazas.

En un estudio (Bossler & Holt, 2010) realizado con una muestra de 573 estudiantes universitarios encontraron que, el bajo autocontrol, aumenta la probabilidad de tres tipos de victimización por ciberdelincuencia: acceso a contraseña, cambio de información de la computadora y ciberacoso. En la misma línea, van Wilsem (2013) halló que, los individuos que presentan un bajo autocontrol, tendrán una mayor probabilidad de ser víctimas de piratería, ciberacoso y victimización mixta. También que los individuos con un bajo autocontrol tienen un mayor riesgo de ser víctimas de fraude en Internet (Wilsen, 2013). En relación con ello, las creencias sobre la vulnerabilidad personal son un factor motivacional clave que aumenta la probabilidad de adoptar conductas de ciberprevención (Liang & Xue, 2010). Por lo tanto, si la educación consigue llegar al objetivo de mejorar el autocontrol y la creencias de vulnerabilidad a través del conocimiento y la concienciación, podrá alcanzar también el objetivo de reducir el riesgo.

Además de los factores expuestos, algunas investigaciones encontraron otros factores claves con relación a la víctima (objetivo adecuado). Hallaron que cuanto mayor es la amenaza percibida, las víctimas potenciales estarán más motivadas para poner en marcha las medidas de seguridad (Sommestad et al., 2015; Thompson et al., 2017; Marten et al., 2019). También que la percepción de la prevalencia de la cibercriminalidad tiene impacto en la decisión de usar estrategias de autoprotección (Martens et al., 2019; Drew, 2020). La antigüedad del acceso a Internet es otro elemento determinante tanto de las habilidades de seguridad digital como del uso de antivirus. (Dodel & Mesch, 2018). Aunque la antigüedad no es un factor desde el que se pueda incidir desde la educación, sí se puede sobre la percepción de las amenazas y la prevalencia mediante la formación enfocada a las ciberamenazas.

Finalmente, señalar que algunos autores como Ngo y Paternoster (2011) analizaron la capacidad predictiva de la TAR en algunas formas de victimización online y los

resultados no consiguieron dar respaldo empírico a la teoría (Rodriguez, 2017). No obstante, a pesar de que en algunos estudios efectivamente no consiguiesen ese repaldo, es abundante la literatura científica que si da ese soporte empírico para defender la CyberTar como una teoría válida en su explicación de la ciberdelincuencia.

Tomando estos resultados en su conjunto, encontramos que existen elementos que se encuentran del lado de la víctima y sobre los que se deberá incidir para tratar de reducir su riesgo. La educación se presenta en este punto como una estrategia fundamental para que la víctima sea empoderada en su protección y no como mero sujeto pasivo en lo que se refiere a la lucha contra la delincuencia. Falta de conocimientos debe ser entendida como sinónimo de vulnerabilidad y, en especial, cuando esa falta de conocimientos va acompañada de los elementos que se han señalado anteriormente en el desarrollo de la CyberTar. Deberían aumentarse los estudios que estudiasen la correlación entre conocimientos, vulnerabilidad y victimización para señalar cuáles son los aspectos clave para reducir la incidencia.

Esta educación, sin embargo, no se debe enfocar como un elemento único por si solo, sino como un complemento y una línea de actuación más añadida a aquellas puestas en marcha por las instituciones. Por ejemplo, al igual que se deben establecer mecanismos para luchar contra el phishing desde las empresas de mensajería, debe haber un siguiente filtro que lo ponga el propio usuario o usuaria. Terminar con la ciberdelincuencia es una tarea que la realidad señala como imposible, no obstante, una vez segmentados como establece la CyberTar, debemos ser conscientes que actuar sobre un elemento dejaría fuera la oportunidad de actuar directamente sobre factores que ayudarían a disminuir la probabilidad de victimización.

Existen también estudios que han tratado de comprobar hasta qué punto un modelo conceptual sobre los determinantes de las conductas preventivas no digitales puede aplicarse al estudio de las conductas de ciberseguridad. En Dodel & Mesch (2017), han aplicado las teorías cognitivas de la conducta sanitaria a la ciberseguridad. Estas teorías son un grupo de perspectivas relacionadas que sostienen que un pequeño número de creencias y actitudes son los mejores determinantes próximos de la conducta preventiva. Según este punto de vista, los seres humanos son tomadores de decisiones racionales que sopesan los costes de tomar precauciones frente a los beneficios que podrían obtenerse de ellas (Weinstein, 1987). Suponen una versión limitada de la racionalidad en la que los individuos están orientados al futuro y evalúan los costes y los beneficios de un comportamiento, pero de forma no óptima; pueden tener creencias incorrectas y actuar con intenciones basadas en información antigua o falsa.

Dentro de ellos, el Modelo de Creencias en Salud (MFS), considera dos factores principales como los determinantes de los comportamientos relacionados con la salud (Rosenstock, 1974):

1. Las percepciones sobre las amenazas

2. Las expectativas sobre el comportamiento.

La primera se compone de dos conjuntos de percepciones sobre el peligro: la susceptibilidad percibida al riesgo y la gravedad percibida de las consecuencias de esas amenazas. Los autores encontraron que el modelo de creencias sobre la salud parece funcionar de forma más que razonable como marco para predecir el comportamiento preventivo de ciberseguridad (uso de antivirus).

Finalmente, la educación y la capacitación pueden ser muy útiles en formas concretas de cibervictimización. En un estudio sobre el perfil de cibervictimización ante violencias de género, se ha hallado que estas tienen menos competencias digitales protectoras como conocimientos de condiciones de privacidad de las redes sociales. Además, perciben en menor medida riesgo de sus conductas en los entornos online (Donoso y cols., 2016). Por lo tanto, esta capacitación puede tener también implicaciones en formas concretas de delincuencia como es la violencia de género, siendo necesario implementarlas en los programas de prevención generales y en los protocolos establecidos.

Estudio 2: Analisis bibliométrico

Análisis Bibliométrico de la Educación en Ciberseguridad y Ciberdelincuencia.

Resumen

En esta investigación se ha realizado un estudio mediante análisis bibliométrico y de contenido sobre la educación en ciberseguridad y la ciberdelincuencia. En segundo lugar, se hizo una comparativa entre la que va dirigida a la población general y aquella más técnica orientada al ámbito especializado. También una comparativa entre los dos elementos, ciberseguridad y ciberdelincuencia, para observar cómo varían sus resultados. Paralelamente, se han evaluado las diferencias y similitudes entre las 2 bases de datos empleadas (*Scopus* y *Web of Science*). Por último, se realizó un análisis de contenido de una muestra bibliográfica para profundizar en el análisis comparativo. Como resultados se encontró un crecimiento exponencial en las publicaciones, la preponderancia de EEUU frente a otros países, una mayor producción orientada a nivel técnico/avanzado frente a la dirigida a población general y una tendencia cronológica más favorable en la primera. Por último, se halló una mayor producción desde las ciencias (Computacionales, ingenierías, informática, etc.) frente a las Ciencias Sociales.

Palabras clave: Ciberseguridad; Ciberdelincuencia; Educación; Bibliometría; Revisión Bibliográfica

1. Introducción

El objetivo que se establece en este estudio es mostrar un mapa de la literatura científica de la educación en ciberseguridad y ciberdelincuencia. Además, se busca proporcionar información sobre las tendencias, autores, evolución, producción por países, principales revistas, diferencias de producción en base a la población a la que se dirije o en base a los distintos campos de investigación. Esta información es útil para predecir las tendencias y movimientos futuros en la investigación, pudiendo también identificar los países, autores y medios clave. Por lo tanto, se busca responder a ¿Cómo es la evolución cronológica en este ámbito? ¿Cuáles son las diferencias entre países? ¿Cuáles son las diferencias entre las áreas de estudio (ciencias y ciencias sociales) desde las que se aborda esta cuestión? ¿Hacia dónde se orienta más según objetivo de la educación, hacia personal cualificado o a la población en general?

En cuanto a la problemática, la ciberdelincuencia es un problema que ha aumentado en los últimos años y especialmente desde la situación excepcional surgida por el COVID-19. Solamente en España aumentó un 31,9% de 2019 a 2020 (Secretaria de Estado de

Seguridad, 2021). Se hace más necesario que nunca la promoción de un ciberespacio seguro y fiable, incluyendo aspectos más allá de los puramente técnicos. Además, victimiza de un modo cada vez más importante a miles de instituciones, empresas y ciudadanos (Departamento de Seguridad Nacional, 2019). Según un informe de McAfee y el Centro de Estudios Estratégicos e Internacionales, los delitos cibernéticos le costaron a la economía mundial más de 1 billón de dólares (1 % del PIB mundial). En 2018 (el año anterior) la cifra era algo más de la mitad, 600 000 millones de dólares (Smith, 2020).

En el caso de España, según un estudio realizado (Cerceda et al., 2019), se puede observar el aumento de la cibercriminalidad en los últimos años. Por ejemplo, en 2016, tenemos 92.716 delitos registrados, mientras que en el año 2019 asciende a 218.302. Otro hecho es el peso proporcional que va adquiriendo dentro del conjunto de la criminalidad, ya que hemos pasado del 4,6% en el año 2016, al 9,9% en el año 2019. Afecta a estructuras críticas, ciberdefensa, Instituciones, grandes empresas, pero también a la sociedad en su conjunto, ya que según muestran los datos, en 2019 hubo 166.152 víctimas de ciberdelitos de diverso tipo.

Frente a este fenómeno, surge la ciberseguridad como modo de protegerse y defenderse. Para ello, los gobiernos han implementado distintas estrategias que incluyen el fomento de la educación en ciberseguridad y la cultura de ciberseguridad (Departamento de Seguridad Nacional, 2019). Paralelamente, en el ámbito de la investigación, se está generando una producción científica para dar luz sobre todas estas cuestiones. Es por ello que este estudio pretende mostrar una imagen global de la producción en torno a esta educación en ciberseguridad y ciberdelincuencia. Además de la educación en ciberseguridad, también se ha incluido la educación en ciberdelincuencia entendiéndola como la orientada a las distintas amenazas a la que se enfrenta la sociedad actual (phishing, malware, ramsonware, etc.).

Para definir la ciberseguridad, según el diccionario del National Initiative for Cybersecurity Careers and Studies, se entiende como “actividad o proceso, habilidad/capacidad o estado por el cual los sistemas de información y comunicaciones, y la información contenida en ellos están protegidos y/o defendidos contra daños, uso no autorizado, modificación o explotación” (NICCS, 2019). Otra definición, es la aportada por el Observatorio Nacional para la Seguridad de la Información y la Ciberseguridad. En su Ciberpedia define la ciberseguridad como “la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de la tecnología de la información o seguridad de la información electrónica” (OSIC, 2019).

La ciberseguridad y la ciberdelincuencia son áreas recientes para los que se han generado grandes esfuerzos por conseguir conocimientos científicos. Por su naturaleza son multidisciplinares, ya que son investigadas desde campos como la psicología, criminología, sociología, victimología, ciencias computacionales, ciencias de la información y ciencias de la comunicación (Payne & Hadzhidimova, 2020). Debido a ello, no es extraño encontrar que a la hora de estudiar la educación en ciberseguridad y ciberdelincuencia las áreas de investigación sean amplias. Es por este motivo que también se incluyen en este estudio comparativas entre las áreas que abordan el objeto de estudio, diferenciando el volumen de producción en Ciencias Sociales (de ahora en adelante CCSS) frente a las ciencias.

También es un área de investigación en auge y crecimiento. En estudios bibliométricos previos sobre educación en ciberseguridad, encontraron que del año 2001 al 2019 el interés por investigar en este estudio aumentó notablemente, dando cuenta de preocupación por los riesgos a los cuales nos enfrentamos. También hallaron que hay pocos estudios con metodologías novedosas que se orienten hacia la enseñanza de soluciones prácticas de los riesgos en el tratamiento de la ciberseguridad. Por último, resaltaron la preponderancia de EEUU en el mapa científico mundial sobre este área (Valencia-Arias et al., 2020). Como novedad ante ese estudio, en éste artículo se analizarán más cuestiones, se emplearán más técnicas (VOSViewer, Bibliometrix y análisis de contenido) y también la base de datos WoS y no solo Scopus.

La educación en ciberseguridad y la creación de una cultura global son los nuevos retos de la sociedad. Aunque no todo el mundo requiere un mismo nivel de seguridad, los usuarios del ciberespacio deben tener un mínimo conocimiento del riesgo que suponen las amenazas que se encuentran en el ciberespacio. Para alcanzar este objetivo, y poder proteger a la sociedad, es necesario que todo ciudadano o empleado de una organización pública o privada tome conciencia de los riesgos a los que se enfrenta la sociedad en su conjunto. Por lo tanto, es necesario fomentar una cultura de ciberseguridad mediante estrategias de concienciación, ya que es preciso que los usuarios sean conscientes de los riesgos que corren en línea y sean capaces de tomar medidas básicas para protegerse (Pulido & Rosell, 2017).

También desde el Centro de Estudios Superiores para la Defensa (Cayón & García, 2014) se apunta en esta dirección cuando se afirma que la ciberseguridad debe abarcar todos los niveles formativos: desde prescolar hasta universitario, que cuente con la participación de la academia tanto privada como pública, así como involucrar directamente a los principales ministerios relacionados: educación, cultura, industria,

etc. y a aquellas personas especializadas como con un carácter divulgativos para el público general.

La importancia de lo anterior se demuestra en los resultados de diversos estudios. Por ejemplo, en una investigación los encuestados informaron tener insuficientes conocimientos y habilidades con respecto a la seguridad y protección de la banca en línea, además de la dificultad de evaluar cómo las medidas de protección les ayudan a protegerse contra ataques fraudulentos. Todo ello es relevante teniendo en cuenta que la capacitación sobre cómo aplicar medidas de protección es fundamental para un uso seguro de la banca en línea (Jansen, 2016). En otro estudio se ha constatado que casi el 30% del alumnado de 9 a 12 años participante no había recibido ningún tipo de formación o información previa a la acción formativa en relación con la ciberseguridad (Gamito et al., 2020).

La educación en ciberseguridad y la ciberdelincuencia incluye en muchos casos aumentar la concienciación sobre los riesgos presentes. Los conocimientos en ciberseguridad y las actividades delictivas en Internet tienen una relación positiva con la concienciación (Nzeakor, 2020) por lo que la educación en este área es doblemente útil. También la educación y la capacitación pueden ser muy útiles en formas concretas de cibervictimización. En un estudio sobre el perfil de cibervictimización ante violencias de género, se ha hallado que éstas tienen menos competencias digitales protectoras, conocimientos de condiciones de privacidad de las redes sociales o ausencia de algún antivirus en el ordenador que avisa o bloquea las páginas peligrosas. Además, perciben en menor medida el riesgo de sus conductas en los entornos online (Donoso et al., 2016). Es por todas estas cuestiones que es necesario ampliar el conocimiento científico en esta materia.

2. Metodología

Para lograr los objetivos de la investigación se ha realizado un estudio mixto mediante análisis bibliométrico y de contenido. A lo largo del estudio, se hicieron comparaciones entre la educación dirigida a la población general y aquella más técnica orientada al ámbito especializado. También comparativas entre los dos elementos, ciberseguridad y ciberdelincuencia, para observar cómo varían sus resultados. Por útlimo, se han evaluado las diferencias y similitudes entre las 2 bases de datos empleadas (*Scopus* y *Web of Science*).

La bibliometría se puede describir como un conjunto de métodos matemáticos y estadísticos que se utilizan para analizar y medir la cantidad y calidad de libros, artículos y otras formas de publicaciones (Durieux & Gevenois, 2010). Existen varios tipos de

indicadores bibliométricos, pero en este caso usaremos los indicadores estructurales, que miden las conexiones entre publicaciones, autores y áreas de investigación.

Los indicadores bibliométricos son especialmente importantes para los investigadores y las organizaciones, ya que estas medidas se utilizan a menudo en las decisiones de financiación, nombramientos y promociones de investigadores. En cuanto a la citación de un artículo es característica de las publicaciones científicas y, generalmente, se acepta que el número de citas de un artículo en particular es un reflejo de su impacto en la comunidad científica. (Durieux & Gevenois, 2010). La bibliometría también permite realizar un seguimiento de tendencias, evoluciones y cambios asociados, dando luz de este modo sobre el panorama del objeto de estudio y una ruta de trabajo más clara (Arenas & Santillán-Rivero, 2002).

Se utiliza a menudo para evaluar la investigación científica y las publicaciones de investigación mediante métodos cuantitativos. Se basan en el supuesto que la mayoría de los descubrimientos científicos y los resultados de la investigación eventualmente se publican en revistas científicas internacionales donde puedan ser leídas y citadas por otros investigadores. Entre las variables de análisis están los años de publicación, que permiten mostrar las tendencias y la cantidad de publicaciones producida cronológicamente; análisis de títulos por revista, que muestran una visión de los patrones de publicación; el análisis de autores, cómo se relacionan, la cantidad de producción de cada uno, su impacto e incluso diferenciar según países de procedencia (Rhen & Kronman, 2006).

Las 4 fases en las que se desarrolló el presente estudio fueron:

- Elección de la fuente de información y selección de datos.

- Visualización de los datos mediante el uso de técnicas bibliométricas.

- Análisis del contenido: Título y Abstract.

- Informe de resultados.

En primer lugar, para el desarrollo del primer punto se seleccionaron 2 bases de datos: *Scopus* y *Web of Science*. Se delimitó la búsqueda entre el año 2001 y 2020. Seguidamente se realizaron distintas combinaciones de búsqueda para valorar las mejores opciones. Finalmente para la búsqueda general se emplearon las de la tabla 1. Todas las graficas analizadas en el apartado de resultados corresponden a las búsquedas de esta tabla 1 a excepción del apartado de áreas de investigación y colecciones, y el análisis de contenido. Por otro lado, las búsquedas para la

comparación entre educación en ciberseguridad y ciberdelincuencia fueron las de la Tabla 2.

Tabla 1. Búsqueda general

Scopus:
TITLE-ABS-KEY(CYBERCRIME OR CYBERSECURITY OR CYBER-SECURITY OR "CYBER SECURITY") AND TITLE-ABS-KEY(EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY)
Resultados: 4073
Web of Science:
TS=(CYBERCRIME OR CYBERSECURITY OR CYBER-SECURITY OR "CYBERSECURITY") AND TS=(EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY)Resultados: 2385

*TS: Titulo- Abstract- Keywords.

Tabla 2. Búsquedas específicas

Scopus:
TITLE-ABS-KEY (cybercrime) AND TITLE-ABS-KEY (education OR learning OR teaching OR pedagogy) AND (EXCLUDE (PUBYEAR , 2021))
Resultados: 391
TITLE-ABS-KEY (cybersecurity OR cyber-security OR "CYBER SECURITY") AND TITLE-ABS-KEY (education OR learning OR teaching OR pedagogy)
Resultados: 3770
Web of Science:
TS=(CYBERCRIME) AND TS= (EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY)
Resultados: 251
TS= (CYBERSECURITY OR CYBER-SECURITY OR "CYBER SECURITY") AND TS= (EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY)
Resultados: 2195

Obtenidos todos los resultados de las búsquedas (a fecha de 26/2/2021), se emplearon los propios instrumentos de análisis de *Web of Science* y *Scopus* para obtener gráficas. También se descargaron en formato ".txt" ".bib" y "CSV" para su análisis en Biblioshiny y VOSviewer. Estos software permitieron obtener gráficas sobre la situación de este área de estudio que se han ido comentando y analizando. Las variables estudiadas fueron: año, país, términos y tendencias, áreas de investigación, revistas y autores.

Para el análisis de contenido,se seleccionaron 900 artículos entre las dos bases de datos (Tabla 3) y las búsquedas de la Tabla 2:

Tabla 3. Selección de artículos de cada base de datos y tipo de búsqueda

450 de *Scopus*	225 búsqueda de ciberdelincuencia y educación
	225 búsqueda de ciberseguridad y educación
450 de *Web of Science*	225 búsqueda de ciberdelincuencia y educación
	225 búsqueda de ciberseguridad y educación.

Se introdujeron en Mendeley para una gestión más sencilla por carpetas. A continuación se reordenaron los artículos de las 2 bases de datos en 2 categorías de búsqueda: Ciberdelincuencia y Educación; Ciberseguridad y Educación. Se depuraron las bases de datos eliminando duplicidades. Los resultados fueron: 385 de Ciberdelincuencia y Educación; 426 en Ciberseguridad y Educación (Tabla 7).

A continuación se analizaron los títulos y abstracts de cada artículo para poder clasificarlo en las categorías de población a la que están dirigidos:

-Educación a nivel general: orientada a ciudadanía sin conocimientos ni formación avanzada que no desempeñen funciones específicas de ciberseguridad.

-Educación a nivel avanzado: orientada a personal con funciones clave en ciberseguridad, en puestos relacionados, estudiantes de titulaciones relacionadas,

ámbito académico/investigador o que tengan competencias relacionadas con el ámbito de ciberseguridad.

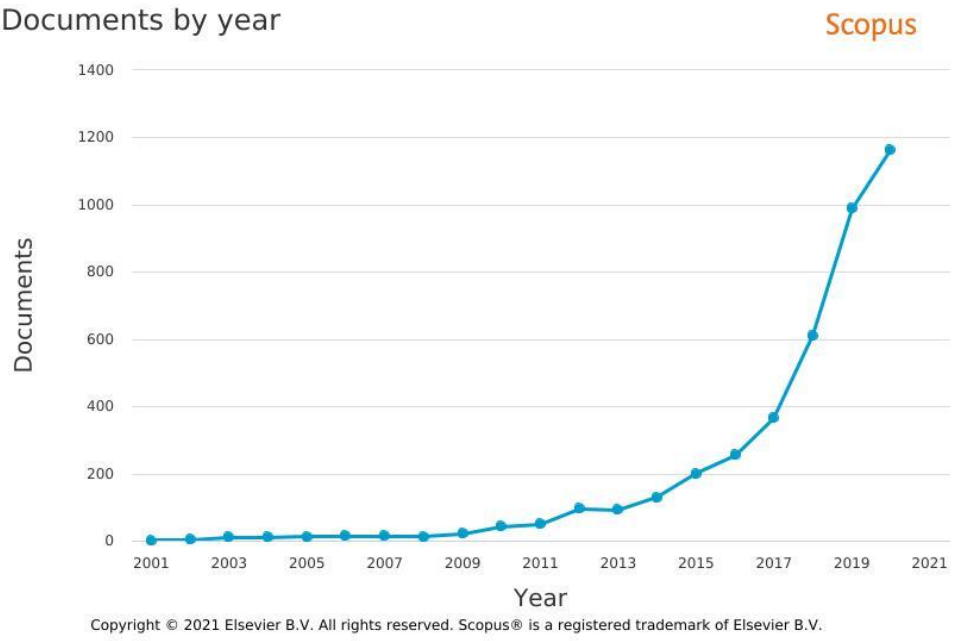
-Otros: artículos sobrantes que no se encuadran en ninguno de los 2 ámbitos y no se encuentran específicamente dentro del objeto de estudio.

3. Resultados

3.1. Publicaciones por año

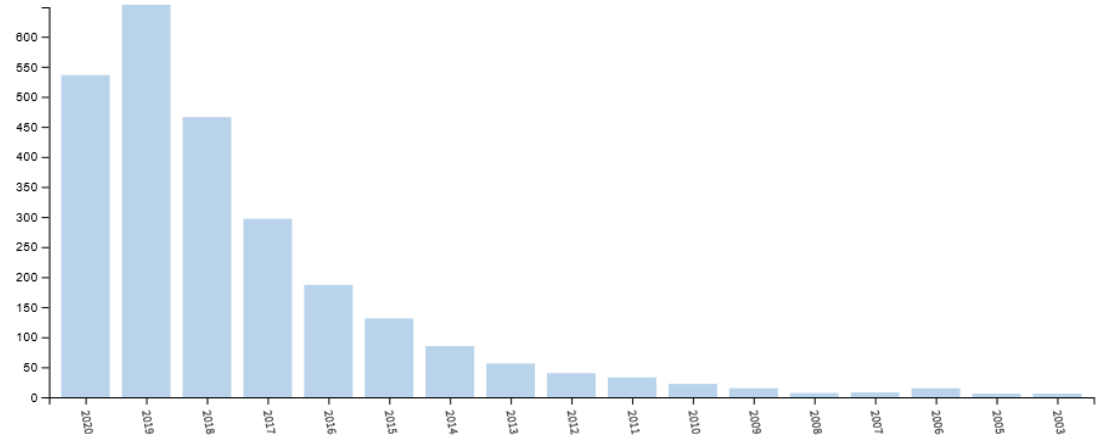
En la figura 1 se puede observar que la producción se mantiene constante desde el año 2001 hasta el año 2009. Es a partir de ese año cuando comienza a aumentar más rápidamente hasta 2013. A partir de ese mismo año, se dispara el crecimiento y se vuelve exponencial hasta llegar a 2020, en donde se alcanzan las mayores cifras. Por lo tanto, la tendencia es creciente y más acelerada en la última década.

Figura 1. Documentos por año en Scopus



En el caso de *Web of Science* (figura 2) también se aprecia como el crecimiento fue bajo pero constante hasta el año 2013/2014, cuando comienza un aumento significativo hasta el 2019, donde se alcanza la cifra más alta (649). En el año 2020 se produce un descenso llegando hasta los 532 coincidente con la crisis del COVID-19. Por lo tanto, la tendencia es ascendente y con una evolución constante, únicamente interrumpida en el último año.

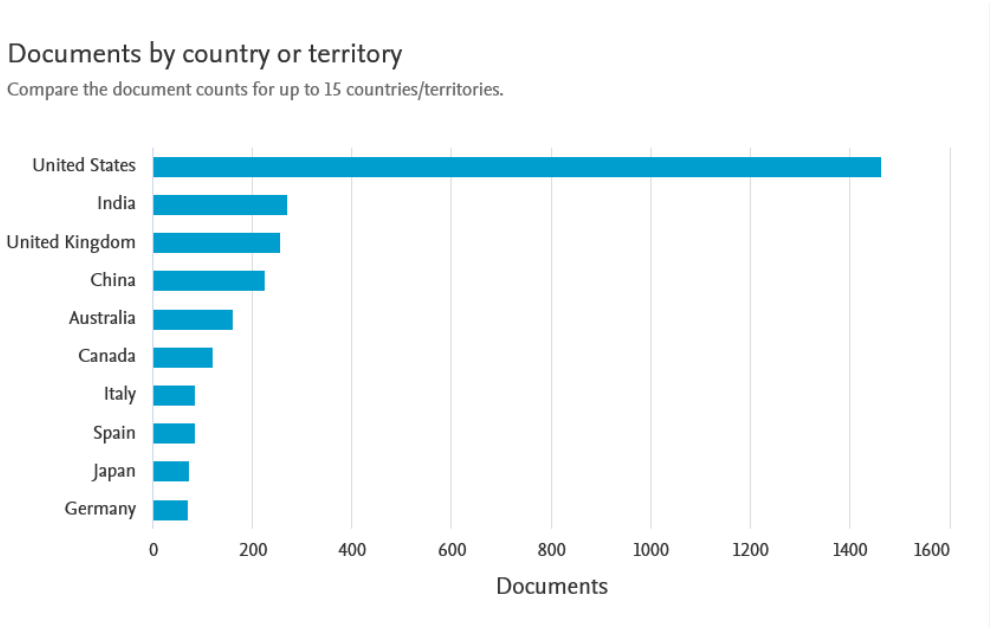
Figura 2. Documentos por año en Web of Science



3.2. Publicaciones por país

En esta figura 3 se puede apreciar la preponderancia de Estados Unidos en la producción científica (1450), siendo mucho mayor que los siguientes 9 países en el ranking. Siguiendo la lista se encuentran India, Reino Unido, China, Australia, Canadá, Italia, España, Japón y Alemania.

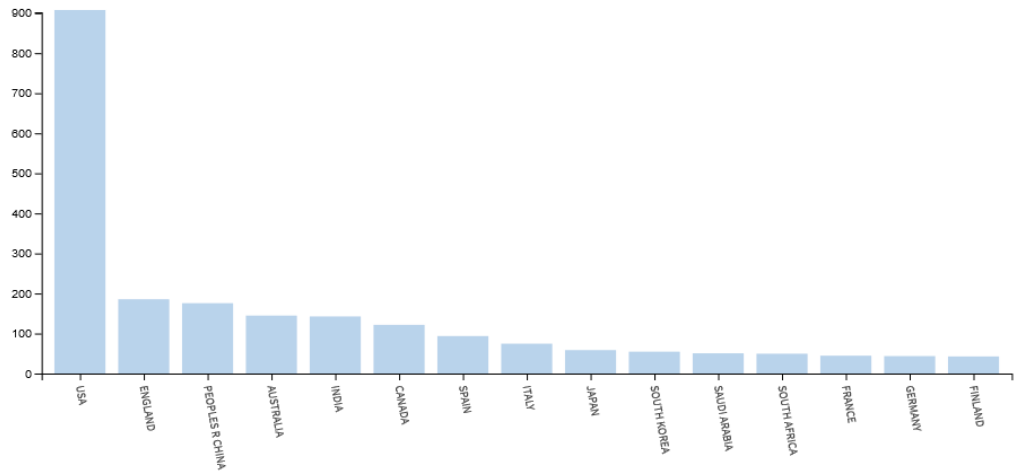
Figura 3. Documentos por año en Scopus



En el caso de *Web of Science (figura 4)*, podemos observar de nuevo los mismos resultados, presentando Estados Unidos la mayor producción muy por encima del resto de países (900). A diferencia de *Scopus*, aquí India se encuentra en el quinto puesto. El

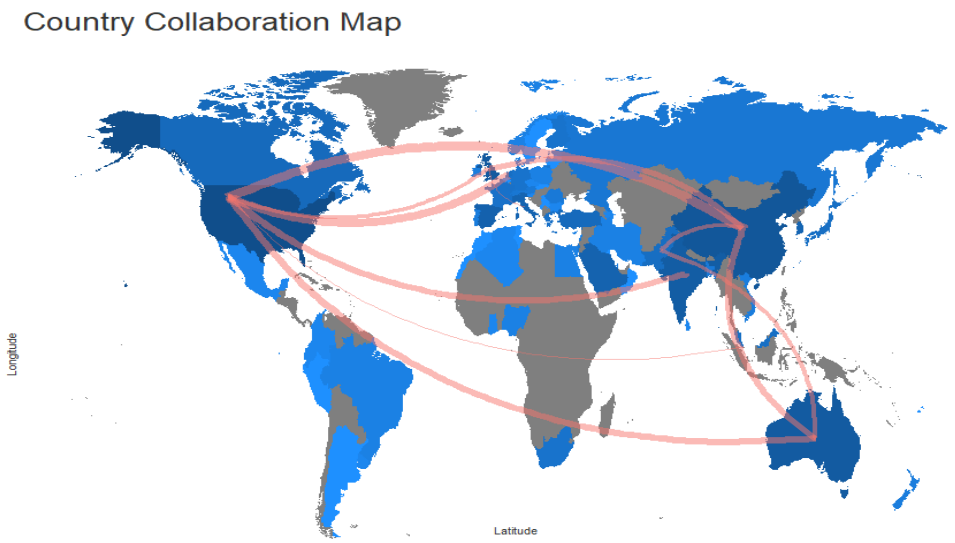
resto de países muestran posiciones muy similares en el ranking: Reino Unido, China, Australia, India, Canadá, España, Italia, Japón, Corea del Sur, Sudáfrica, Francia, Alemania y Finlandia.

Figura 4. Documentos por año en Web of Science



En cuanto al mapa global de colaboración, se puede observar en la figura 5 cómo se establecen las principales líneas a nivel mundial. Las mayores se observan desde Estados Unidos con el resto de países (India, China, Australia, Reino Unido y Alemania). Aunque también China presenta numerosas conexiones con Australia, Reino Unido y Pakistán.

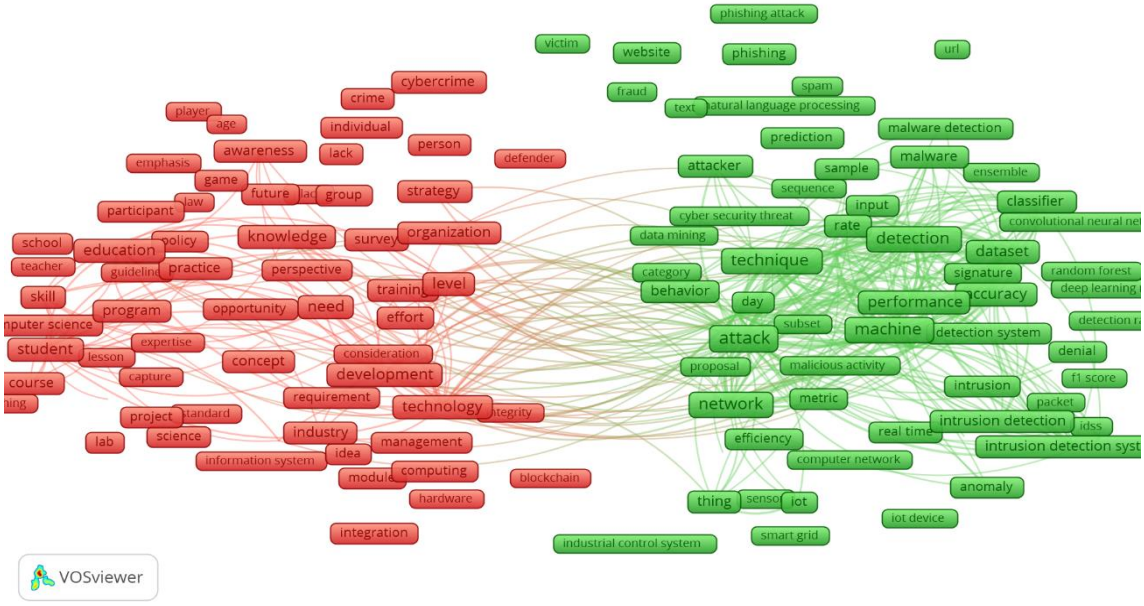
Figura 5. Mapa de colaboración por países



3.3. Tendencias de investigación

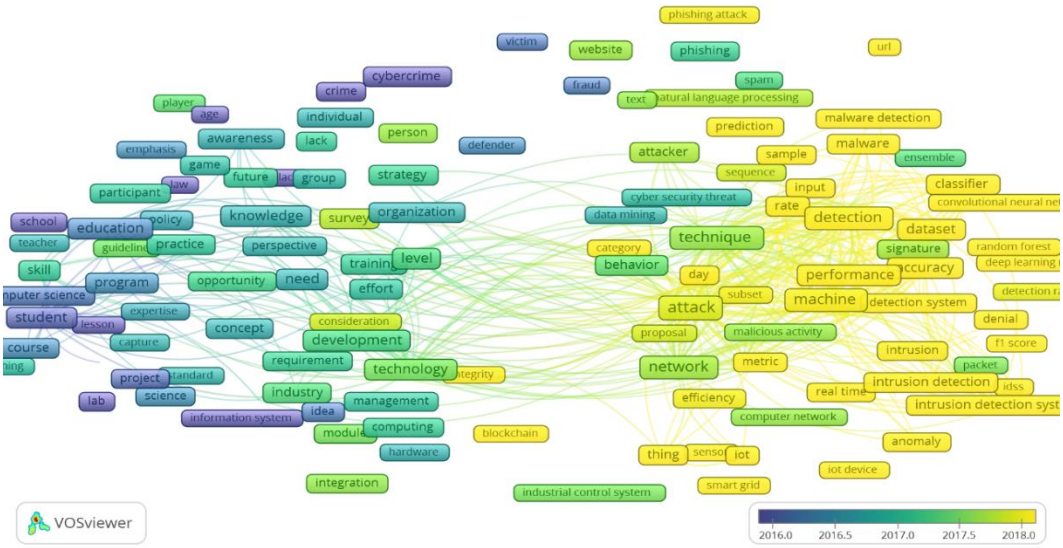
En este mapa de términos de VOSviewer (figura 6) se puede observar los resultados de analizar los títulos y abstarct de los artículos recopilados en *Scopus*. El sistema formó 2 clústeres interrelacionados (verde y rojo). En el clúster verde se pueden observar términos más orientados a un área técnica y computacional: técnica, detección, máquina, actividad maliciosa, detección de intrusos, sistemas de detección, malware, dataset, phishing, anomalía, métricas, eficiencia, sensores, IoT (Internet of Things), deep learning, etc. mientras que en el clúster rojo los términos muestran una tendencia más hacia la educación, la enseñanza y variables de tipo social: educación, conocimiento, industria, escuela, profesor, habilidades, estudiante, lecciones, integración, cursos, guías, edad, jugador, persona, oportunidad, necesidad, carencias, estrategia, énfasis, organización, entrenamiento, desarrollo, idea, etc.

Figura 6. Mapa de términos en Scopus



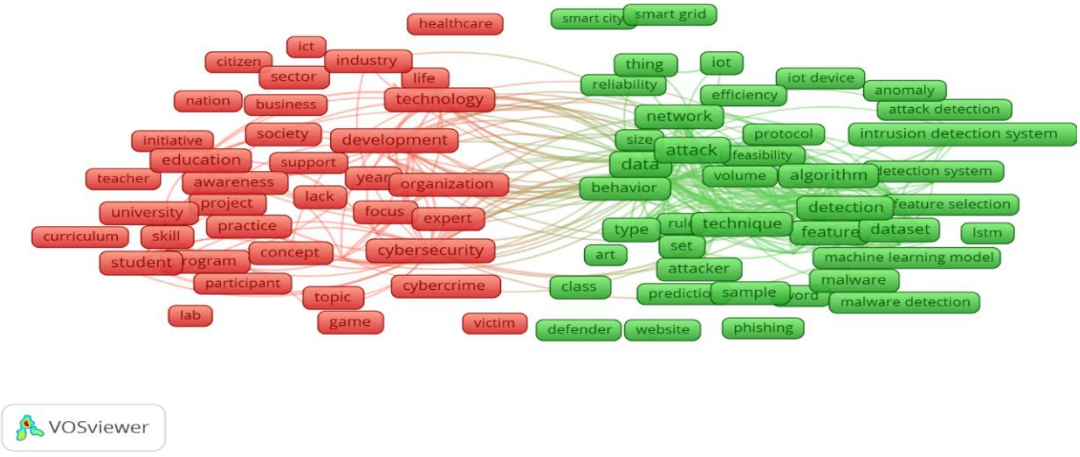
En la figura 7 se pueden ver los mismos conceptos de la figura 6, pero introduciendo la variable cronológica. Se puede observar un mayor color amarillo (más actual) en el clúster derecho (vinculado a cuestiones técnicas y computacionales) que en el clúster izquierdo (educativo), el cual se muestra más azul (antiguo). Por lo tanto, se muestra de un modo gráfico cómo está evolucionando la literatura científica en una producción orientada a aspectos técnicos y computacionales más que a cuestiones educativas y de tipo didáctico.

Figura 7 Mapa de términos en Scopus por criterio cronológico



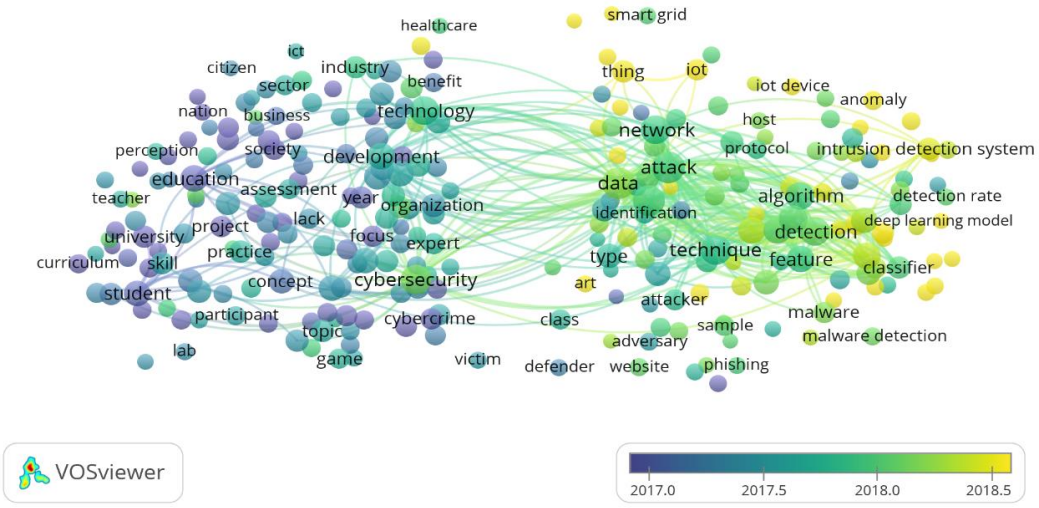
En el caso de *Web of Science (*figura 8), los resultados son similares al de *Scopus*. Tenemos como resultado 2 clústeres, siendo el derecho (verde) orientado a aspectos técnicos, computacionales, vinculados a ingeniería e informática, mientras que el izquierdo (rojo) incluye conceptos de tipo social y educativo. En el verde nos encontramos: Algoritmo, detección, técnica, ataque, protocolo, sistemas de detección de intrusiones, machine learning, malware, phishing, predicción, defensor, anomalía, IoT, set de datos, etc. y por otro lado, en el rojo, tenemos conceptos como: educación, concienciación, carencia, ciberseguridad, cibercrimen, estudiante, curriculum, universidad, profesor, participación, victima, juego, sociedad, negocios, ciudadanos, nación, vida, salud, experto, organización, etc.

Figura 8. Mapa de términos en Web of Science



En la figura 9, introduciendo un análisis cronológico a los conceptos obtenidos en la figura 8, podemos obervar que se repiten los mismos resultados que en el caso de *Scopus*. En el lado derecho predomina el amarillo, por lo que la tendencia de producción científica a lo largo del tiempo se orienta hacia ese lado. Contrariamente, del lado izquierdo predomina el azul, ya que esos términos están cada vez más en desuso y se encuentran en artículos más antíguos. Por lo tanto, tenemos que la evolución de producción científica avanza hacia aspectos más técnicos y de áreas computacionales más que en las categorías relacionadas con la educación y la sociedad.

Figura 9. Mapa de términos en Web of Science por criterio cronológico



3.4. Colecciones, áreas de investigación y temáticas

En estas tablas (4 y 5) se pueden observar las diferencias de producción científica según las distintas colecciones en Web of Science. Las 2 categorías de colecciones son ciencias y CCSS, siendo el resultado de las ciencias mayor frente a las CCSS. Se puede apreciar en los datos que están descompensadas (476 CCSS; 2717 ciencias). También se pueden observar las diferencias por categorías de búsqueda: Ciberseguridad frente Ciberdelincuencia. En la categoría Ciberseguridad la proporción de la diferencia es mayor que en el caso de la categoría Ciberdelincuencia (diferencia entre CCSS y ciencias: Ciberdelincuencia: 64 (143 -79); Ciberseguridad: 2177 (2574 - 397).

Tabla 4. Producción científica en colecciones de Ciencias Sociales

Colecciones Ciencias Sociales	
TS=**(CYBERCRIME**) AND TS=(EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY) Social Sciences Citation Index (SSCI) --1900-presente Conference Proceedings Citation Index- Social Science & Humanities (CPCI-SSH) --1990-presente Book Citation Index– Social Sciences & Humanities (BKCI-SSH) --2005-presente	**79**
TS=(**CYBERSECURITY** OR CYBER-SECURITY OR CYBER SECURITY) AND TS=(EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY) Social Sciences Citation Index (SSCI) --1900-presente Conference Proceedings Citation Index- Social Science & Humanities (CPCI-SSH) --1990-presente Book Citation Index– Social Sciences & Humanities (BKCI-SSH) --2005-presente	**397**
TOTAL	**476**

Tabla 5. Producción científica en colecciones de Ciencias

Colecciones Ciencias	
TS=(**CYBERCRIME**) AND TS=(EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY) Science Citation Index Expanded (SCI-EXPANDED) --1900-presente Conference Proceedings Citation Index- Science (CPCI-S) --1990-presente Book Citation Index– Science (BKCI-S) --2005-presente	**143**
TS=(**CYBERSECURITY** OR CYBER-SECURITY OR CYBER SECURITY) AND TS=(EDUCATION OR LEARNING OR TEACHING OR PEDAGOGY) Science Citation Index Expanded (SCI-EXPANDED) --1900-presente Conference Proceedings Citation Index- Science (CPCI-S) --1990-presente Book Citation Index– Science (BKCI-S) --2005-presente	**2.574**
TOTAL	**2717**

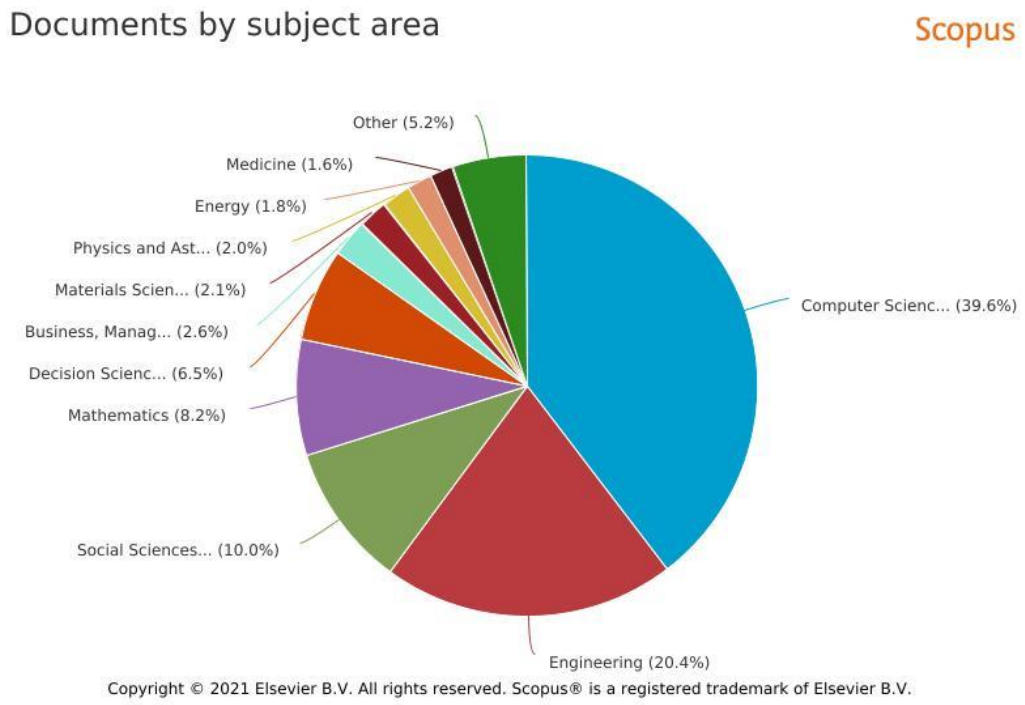
En cuanto a las áreas de investigación (Tabla 6), de nuevo nos encontramos con un fuerte contraste entre ciencias y CCSS. También hay diferencias según si centramos la búsqueda de educación en cibercrimen o ciberseguridad (cibercrimen 253; ciberseguridad 2225). En el primer caso, las ciencias duplican a las CCSS (ciencias 164; CCSS 81), en el segundo caso es 8 veces mayor (ciencias 1815; CCSS 244). Finalmente, la diferencia total entre ciencias y CCSS es de: ciencias 1979; 325 CCSS.

Tabla 6. Documentos por áreas de investigación

BUSQUEDA	RESULTADOS	Áreas de investigación	RESULTADOS
Ed. en cibecrimen	253	Ciencias Sociales	**81**
		Ciencias	**164**
Ed. en ciberseguridad	2.225	Ciencias Sociales	**244**
		Ciencias	**1815**
		Total Ciencias Sociales	**325**
		Total Ciencias	**1979**

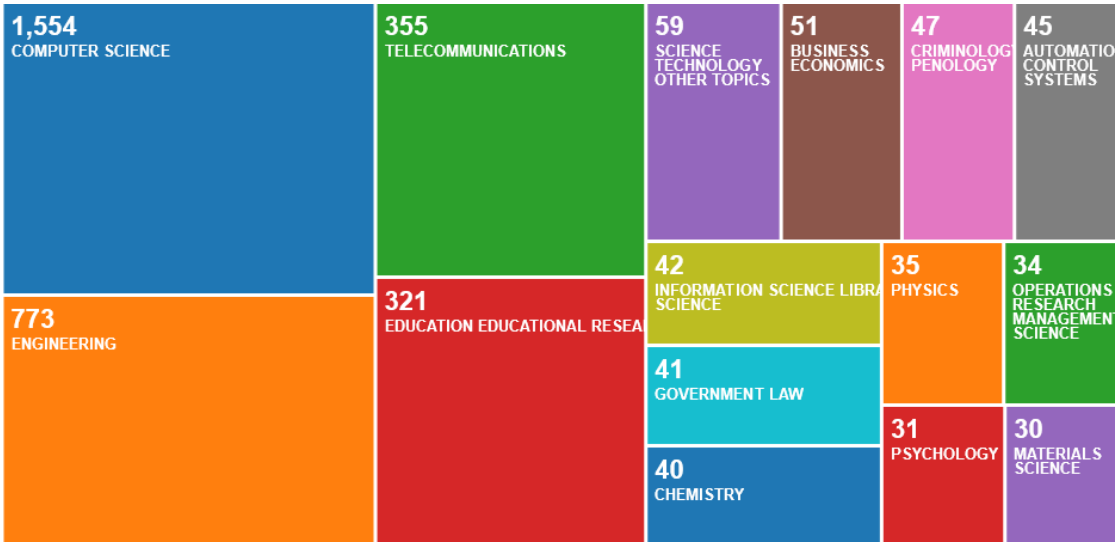
En esta figura 10 se pueden observar las áreas temáticas de resultados tras la búsqueda principal en *Scopus* (Tabla1). Las Ciencias Computacionales (39,6%) y las Ingenierías (20,4%) suman el 60%. Las CCSS se encuentran en el tercer puesto con tan solo un 10% y seguidas de otras áreas temáticas alejadas del ámbito social y educativo (matemáticas, económicas, ciencias de los materiales, física, energía, etc.).

Figura 10. Documentos por área temática en Scopus



En el caso de *Web of Science* (figura 11) de nuevo nos encontramos con una descompensación en el área temática, ya que tenemos en los 3 primeros puestos las ciencias Computacionales, Ingenierías y Telecomunicaciones con un sumatorio de 2682. En cuarto lugar está Educación e Investigación Educativa, con 321 publicaciones. Las siguientes áreas siguen principalmente la línea de ciencias, como ciencias tecnológicas, ciencias de la Información, Química, Economía, Física, Investigación de Operaciones, Sistemas de control automático y ciencias de los Materiales. Aquellas más vinculadas al área social serían Psicología, Criminología y Penología, y Leyes Gubernamentales.

Figura 11. Documentos por área temática en Web of Science

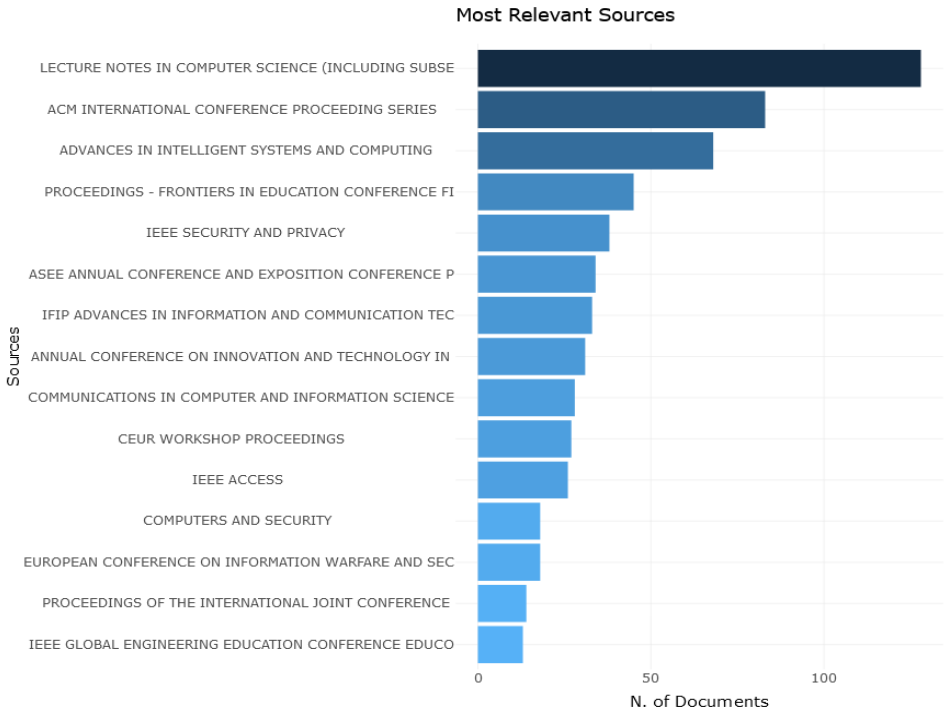


3.5. Revistas

En referencia a las fuentes más relevantes (figura 12), tenemos en primer *lugar Lecture Notes in Computer Science* (LNCS) Esta serie de actas de congresos publica los últimos avances en investigación en todas las áreas de la informática. Seguidamente *ACM International Conference Prodeeding Series, Advanaces in Intelligent Systems and Computin, Frontiers in Education Conference, IEEE Security and Privacy, ASEE Conference and Exposition Conference, IFIP Advances in Information and Comunication Tecnologies, Annual Conference of Innovation and Technology, Comunications in Computer and Information Science, CEUR Workshop Preceedings, IEEE ACCESS, Computers and Security, European Conference on Information Warfare and Security, Proceedings of the International Joint Conference y IEEE Global Engineering Education Conference EDUCO.*

De todo este ranking de las 15 principales de *Scopus*, tan solo 1 es propiamente de ámbito educativo (*Frontiers in educations*); mientras que el resto están vinculadas a las áreas computacionales, tecnológicas, ingenierías, comunicaciones y sistemas.

Figura 12. Fuentes más relevantes en Scopus



En *Web of Science* (Figura 13) tenemos en primer lugar *IEEE ACCESS*. Es una revista multidisciplinaria de acceso abierto, totalmente electrónica, que presenta continuamente los resultados de la investigación o el desarrollo original en todos los campos de interés propios de la IEEE. Seguidamente, se encuentran *Lecture Notes in Computres Science, Frontiers in Education Conference, Computer Security, IEEE International Conference of Big Data, Advances in Intelligent Systems and Computing, Inted Proceedings*...

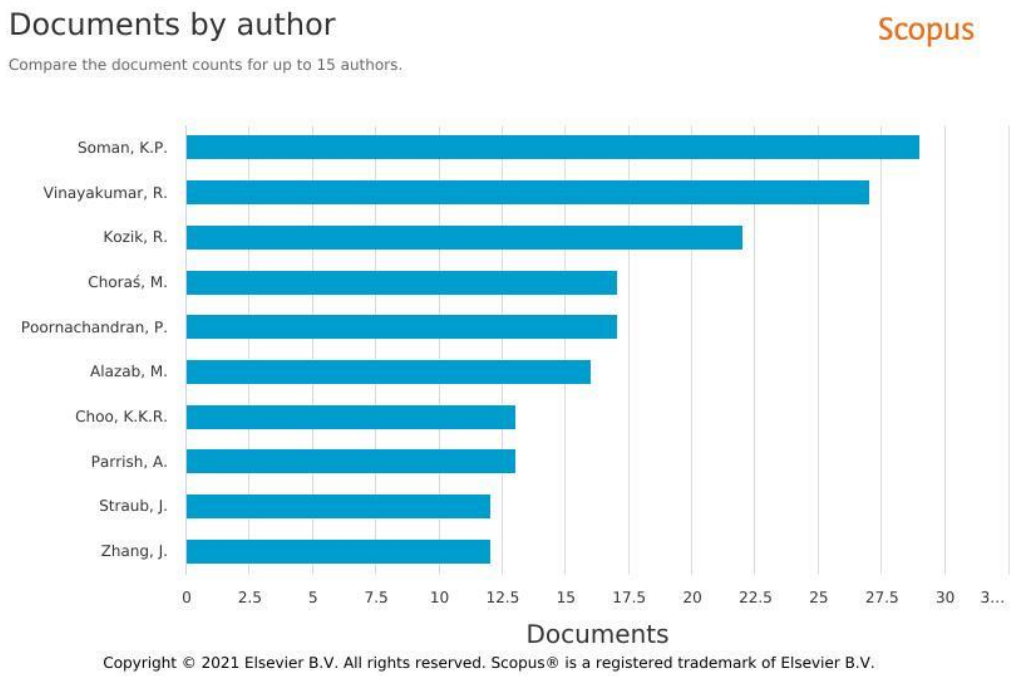
Al igual que en *Scopus*, tan solo 1 es de educación propiamente mientras que el resto son de nuevas tecnologías o de educación en esas áreas específicas.

Figura 13. Fuentes más relevantes en Web of Science

3.6. Autores

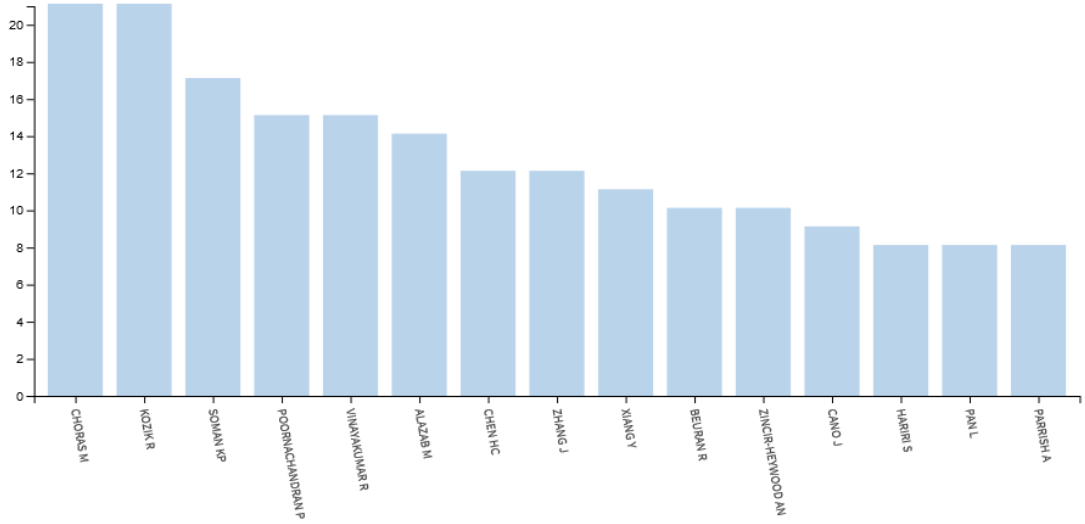
En la figura 14 se pueden ver los 10 autores que mayor cantidad de aportes generan en la temática (*Scopus*). El ranking lo lideran Soman K.P. (29), Vinayakumar R. (27) y Kozik, R. (22). Se aprecian coincidencias con el listado de *Web of Science* aunque en distinto orden: Soman K.P., Vinayakumar R., Kozik R, Choras M., Poornachandran P., Alazab M., Parrish A. y Zhang J.

Figura 2. Documentos por autor en Scopus



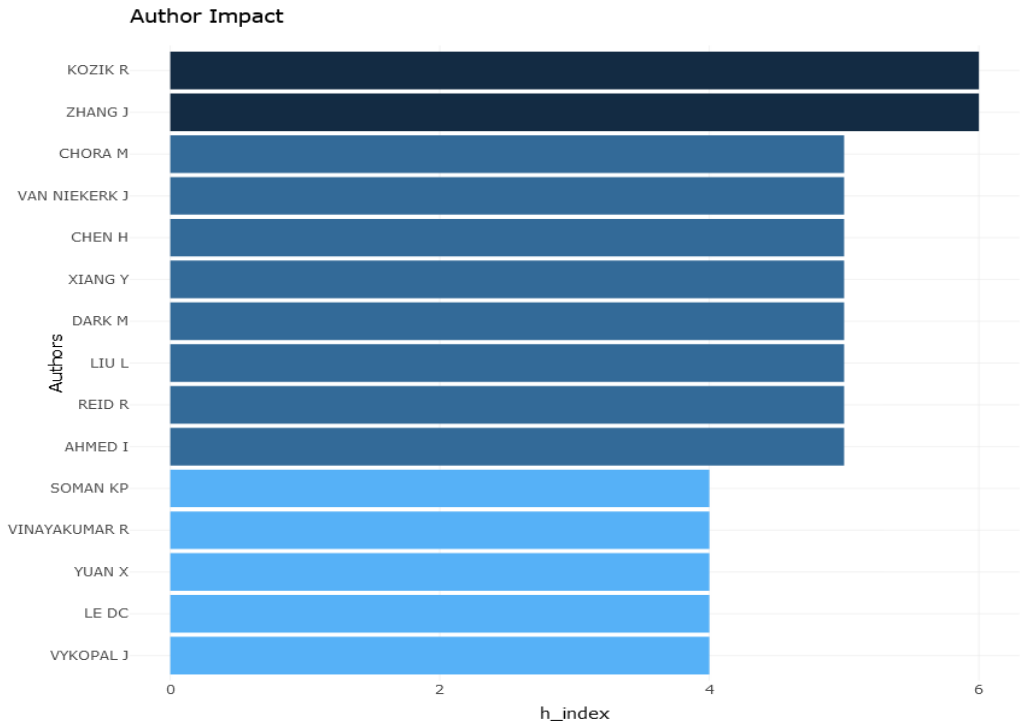
En la figura 15 se puede observar el ranking de los 15 autores con mayor número de publicaciones en *Web of Science*. Lideran el Ranking: Choras M. (21), Kozik (21)y Soman K.P. (17).

Figura 15. Documentos por autor en Web of Science



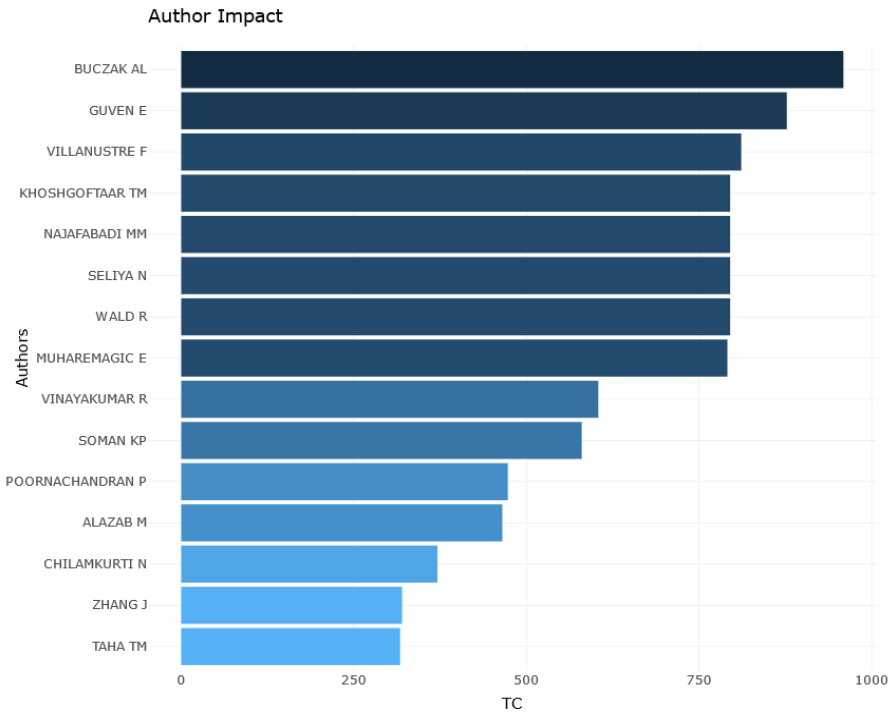
En esta figura 16 se observan los autores con mayor impacto en el objeto de estudio siguiendo el índice H. El índice H es un sistema de medición de la calidad profesional de los científicos, se basa en la relevancia de su producción científica teniendo en cuenta el conjunto de los trabajos más citados del investigador y el número de citas de cada uno de estos trabajos. Lo encabezan Kozik R. (6) y Zhang J. (6).

Figura 3. Autores con mayor impacto según índice H



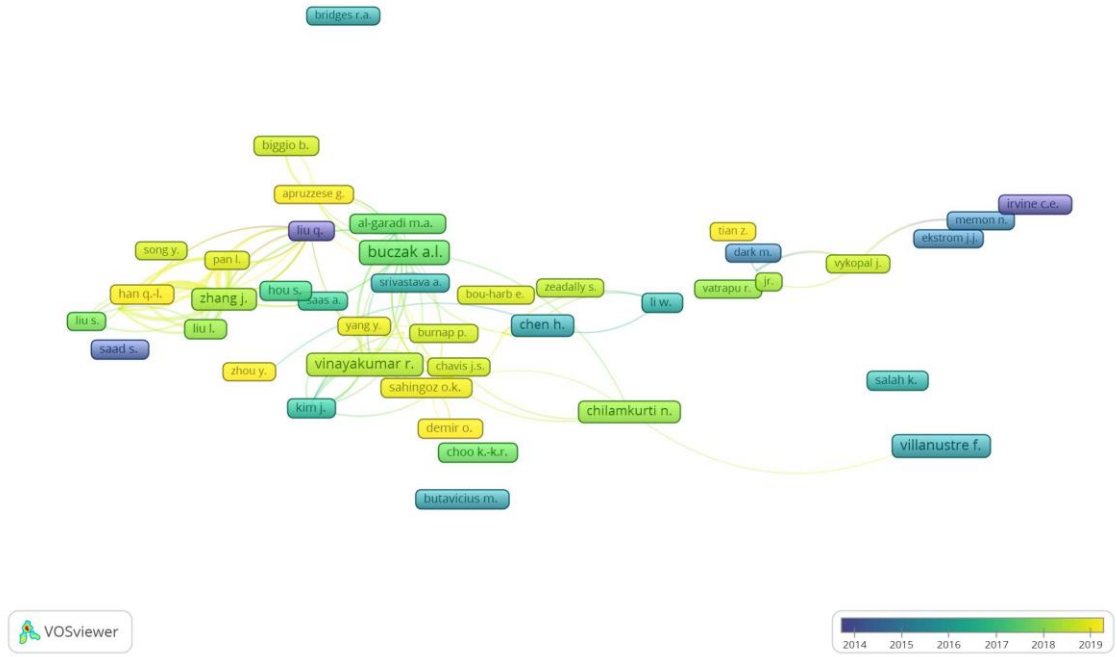
En esta figura 17 se muestran los autores con mayor impacto según el número de citaciones. Como se puede comprobar, la lista la lidera Buczak A.L., Guven E. y Villanustre F. En el listado se incluyen algunos de los que estaban presentes por nivel de producción (figuras 14 y 15) y por el índice H (figura 16): Soman K.P., Poornachandran P., Alazab M., Zhang J. y Vinayakumar R.

Figura 17. Autores con mayor impacto según citaciones



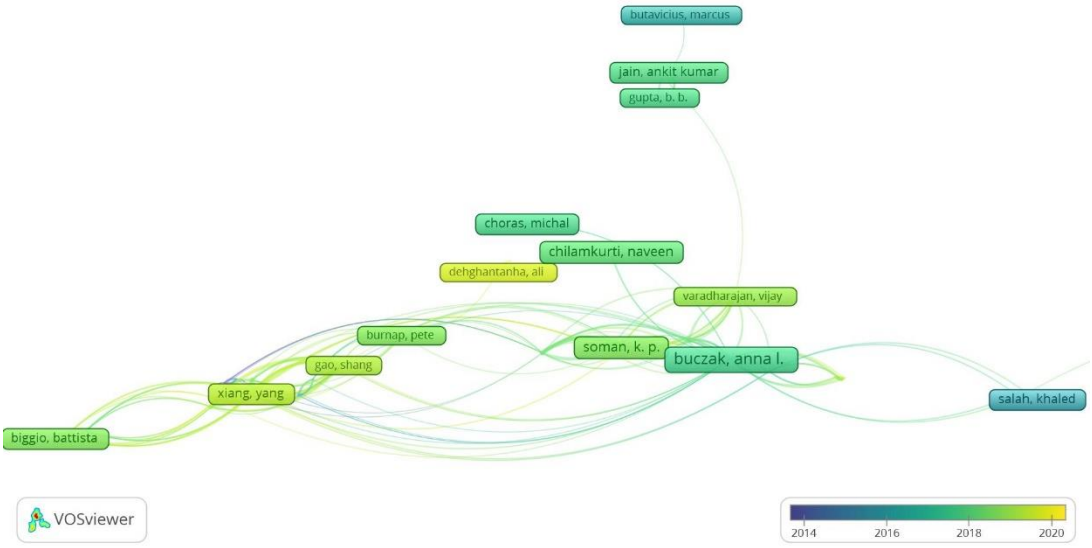
En esta figura 18 se puede observar mediante VOSviewer los datos de citaciones de los autores (fuente:*Scopus*) . Se muestran de distintos colores en base a criterios cronológicos, dando como resultado un mapa de aquellos más actuales frente a los que antiguos. Se aprecian varios de los principales autores anteriormente mencionados (Buczack A.L., Vinayakumar R., Zhang J., Dark M., Liu L. y Chen H.). Aunque existe un grupo central que muestra mayor actualidad (amarillo), algunos se remontan a 2014 y 2015.

Figura 18. Citaciones de autores en Scopus



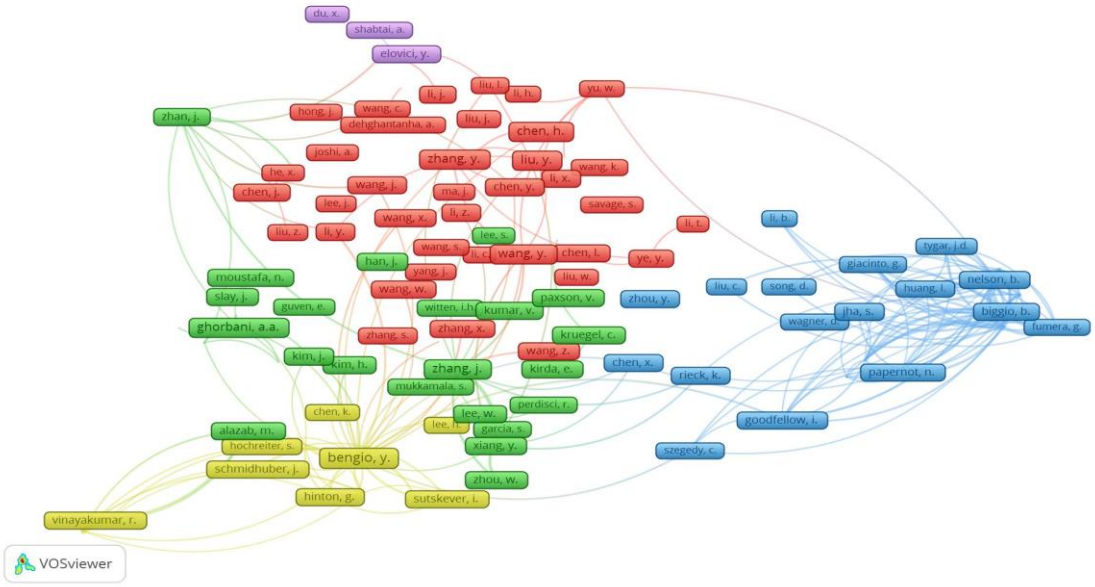
En esta figura 19 se puede observar mediante VOSviewer los datos de citaciones de los autores, pero en este caso obtenidos de Web of Sicence. Vemos que en general los autores presentes tienen una mayor actualidad que en el caso de *Scopus*.

Figura 19. Citaciones de autores en Web of Science



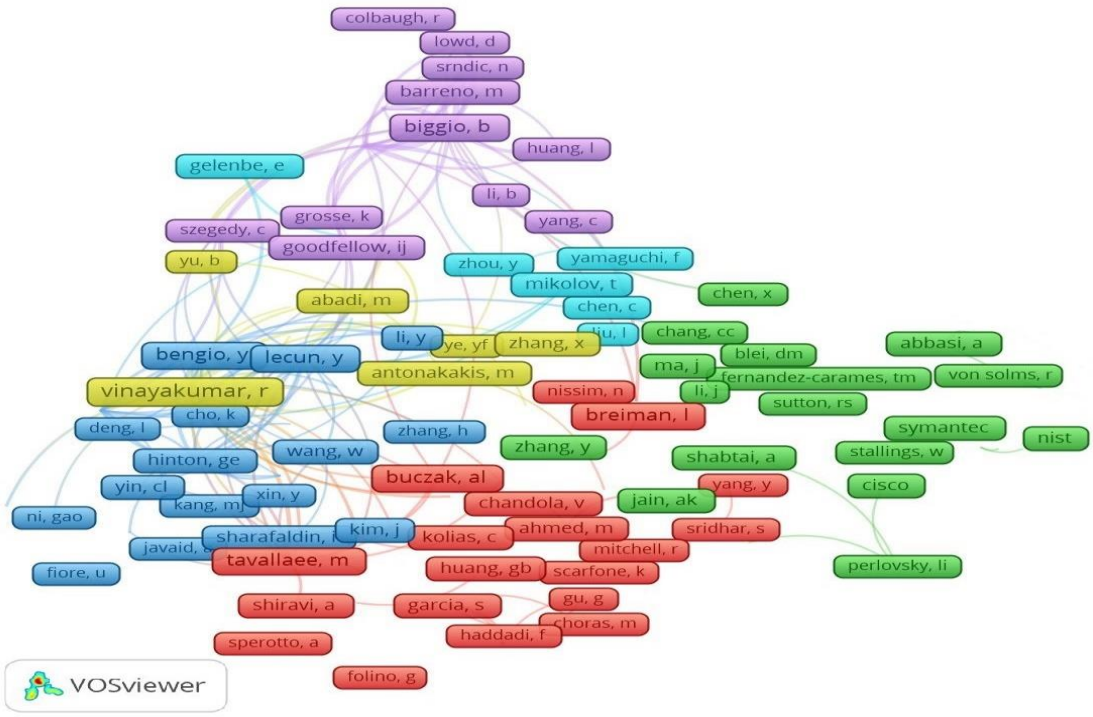
En la figura 20 tenemos el mapa de autores por cocitación para poder observar una imagen de las interrelaciones que se establecen (fuente: *Scopus*). Se han formado 5 clústeres correspondiente a aquellos grupos con mayor conexión.

Figura 20. Interrelación de autores en Scopus



Por último, en la figura 21, tenemos el resultado correspondiente a la cocitación de los autores obtenida en *Web of Science*. Se muestra mucho más amplia que en *Scopus* y con 6 clústeres en vez de 5.

Figura 21. Interrelación de autores en Web of Science



3.7. Análisis de Contenido

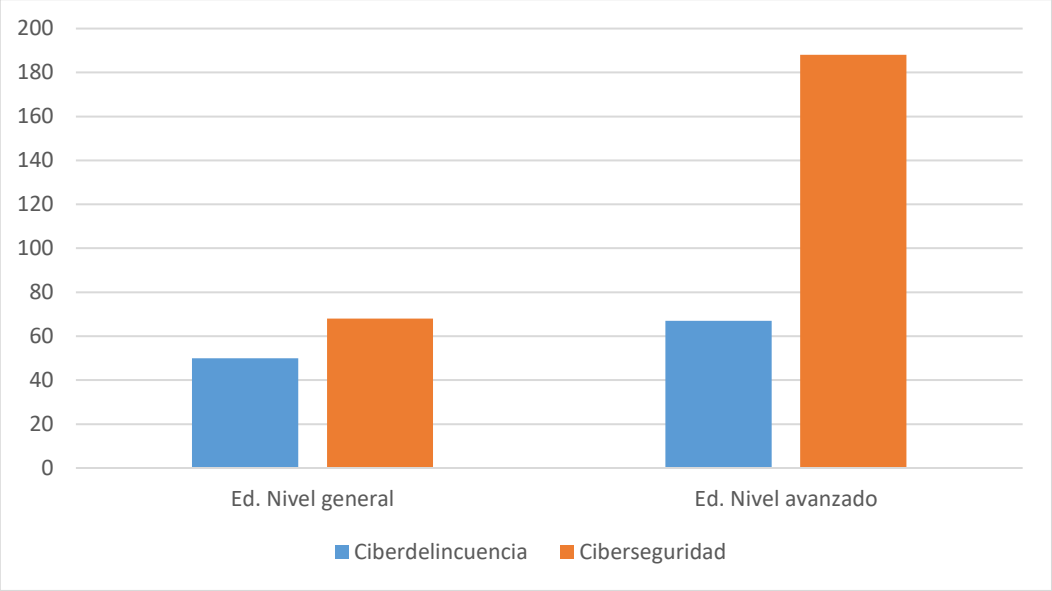
Tras el análisis de la muestra de artículos descrita en el apartado de metodología (tabla 3) se han obtenido los resultados depurados en la tabla 7. En la figura 22, creada a partir de estos resultados, se aprecia desequilibrios entre las búsquedas de ciberseguridad y de ciberdelincuencia. También que los artículos orientados a personas con un nivel avanzado (255) son más abundantes que aquellos dirigidos a la ciudadanía general (118). Finalmente, se puede apreciar que esta diferencia de nivel avanzado frente a nivel general es mayor en el área de educación en ciberseguridad (diferencia de 120) que en el de educación en ciberdelincuencia (diferencia de 17).

De los artículos clasificados en nivel general, gran parte estaban orientados a estudiar los conocimientos, vulnerabilidades y concienciación en la población. Por otra parte, los dirigidos a un nivel avanzado, estaban más orientados al ámbito universitario o de las empresas en donde es necesario niveles formativos de alto nivel.

Tabla 7. Resultados de análisis de contenido

	Ciberdelincuencia	Ciberseguridad	
Ed. Nivel general	50	68	118
Ed. Nivel avanz.	67	188	255
Otros	268	170	438
Total	385	426	811

Figura 22. Resultados de análisis de contenido



4. Discusión

Con los resultados obtenidos se pueden afirmar varias premisas. En primer lugar, que es una materia que cuenta con un gran crecimiento, especialmente en los últimos 10 años como se ha podido constatar en el apartado 3.1. Cabe pensar que la tendencia sea positiva ya que es una temática que cuenta con gran impacto en la sociedad actual y que ha evolucionado rápidamente. Este aumento se podría explicar debido al aumento paralelo de la ciberdelincuencia, que en los últimos años ha aumentado exponencialmente. Por lo tanto, la educación en ciberseguridad y ciberdelincuencia es un área de estudio moderno y emergente con grandes posibilidades de cara al futuro y que implicará una mayor producción científica e investigadora.

También en base a los resultados (apartado 3.2), se puede afirmar que EEUU es el mayor país en esta materia con una gran producción en comparación al resto de países. De los restantes, la mayor parte son países occidentales a excepción de India, China y Japón. Además de liderar la lista con mayor producción, también es la que establece más y mejores conexiones en el mapa global de colaboraciones.

En referencia a las tendencias de investigación (apartado 3.3), se puede interpretar un cambio de objetivos a lo largo del tiempo. Con el paso de los años, el interés ha ido centrándose en aspectos más técnicos y específicos de ciberseguridad, con conceptos relacionados con ciencias computacionales, nuevas tecnologías, comunicación o ingenierías, frente a materias más relacionadas con educación y sociedad, que han ido quedando más anticuadas. Estas tendencias pueden explicarse por un mayor

desinterés en “cómo educar”, es decir, técnicas pedagógicas, didácticas y de enseñanza. Paralelamente, ha aumentado el interés sobre “el qué educar”, es decir, los contenidos sobre técnicas en materia de ciberseguridad.

En cuanto a las colecciones y áreas de investigación (apartado 3.4), el desequilibrio de la aportación por parte de las ciencias y CCSS es incuestionable, especialmente en el área específica de “educación en ciberseguridad”. Los datos mostrados en la figura 10 y las tablas 4, 5 y 6 muestran claramente esta desigualdad, que se interpreta como una escasez de atención en el objeto de estudio por parte de áreas pertenecientes a CCSS como ciencias de la Educación, Psicología o Criminología frente a las ciencias. Este hecho es importante teniendo en cuenta que estas disciplinas de CCSS pueden realizar una gran aportación al objeto de estudio: técnicas didácticas, pedagógicas, para adaptar la educación en ciberseguridad a distintos públicos (especialmente en menores), relación con la victimización o incluso las aportaciones que pueda tener la psicología sobre la ingeniería social presente en el phishing.

También si observamos las revistas científicas podemos ver esta asímetría, ya que en los principales rankings de publicaciones en la materia objeto de estudio solo hay una revista perteneciente al área de educación. Se puede decir por lo tanto que existe una preponderancia de las revistas de ciencias cuando tratamos la educación en ciberseguridad y ciberdelincuencia.

En cuanto al análisis de contenido (apartado 3.7), los datos reflejan una gran asimetría entre la educación orientada a pesonal especializado y de nivel avanzado frente a la educación para la población general (figura 22). Además, también se muestran diferencias entre la educación en ciberseguridad y la educación en ciberdelincuencia. El hecho de que la educación en ciberdelincuencia esté más orientada a la población general que la educación en ciberseguridad, puede deberse a que se oriente a mejorar la comprensión de riesgos y por lo tanto sea percibida como más adecuada para ciertos colectivos. También que este tipo de educación se enfoque para concienciar y alertar de los peligros presentes en la red, tratando de prevenir la victimización en la población. Un ejemplo de esto serían aquellos artículos de la educación en escuelas e institutos, donde se estudia la concienciación y los conocimientos sobre riesgos.

En cuanto a la educación ciberseguridad, en gran medida trataría de mejorar la educación del personal que va a desempeñar funciones en la materia (alumnos universitarios de másters especializados, ingenierías o áreas relacionadas con la computación) y no tanto de dirigirse a la población general como sí lo hace la educación en ciberdelincuencia. Cabría cuestionarse si esta falta de producción en torno a la

educación en ciberseguridad orientada a la población general podría tener relación con las altas tasas de víctimización. Esta cuestión es todavía más importante si tenemos en cuenta la tendencia observada en las figuras 7 y 9, que muestra precisamente la dirección contraria, una educación orientada a la especialización avanzada y no hacia la cultura de ciberseguridad como se promueve en la Estrategia Nacional de Ciberseguridad (Departamento de Seguridad Nacional, 2019).

Las limitaciones encontradas fueron principalmente relacionadas con los términos de búsqueda y el análisis de contenido. A la hora de analizar los titulos+abstracts se encontró que algunos de los artículos que aparecieron en las búsquedas no tenían relación directa con el objeto de estudio. Por ejemplo, aparecieron términos como “machine learning” entre los artículos, sin embargo, no tienen relación directa con la enseñanza (“learning”) que es uno de los términos del objeto de este estudio incluido en la búsqueda. Este efecto de artículos incluidos y no relacionados directamente con el objeto de estudio tendrían un efecto distorsionador. A pesar de ello, en el análisis de contenidos han sido controlados y aún así los resultados han sido similares a aquellos sin controlar.

5. Conclusiones

En el presente estudio se ha realizado una investigación mediante análisis bibliométrico y de contenido sobre la educación en ciberseguridad y la ciberdelincuencia. El periodo de estudio fue de 2001 a 2020 y las bases de datos fueron *Scopus* y *Web of Science*. Los resultados mostraron la preponderancia de EEUU frente a otros países y el rápido crecimiento de la producción científica en la última década. También se encontró un aumento del interés en aspectos técnicos frente a educativos y sociales en los últimos años.

En cuanto a las diferencias de producción desde CCSS y ciencias se halló una gran asimetría, siendo las ciencias las que más investigaciones generaron. También las propias diferencias entre la educación orientada a personal especializado (con funciones en ciberseguridad o estudiantes de ramas vinculadas al ámbito computacional) frente a la educación orientada a la población general. Finalmente, se encontraron diferencias entre la educación en ciberseguridad y la educación en ciberdelincuencia, siendo la primera más abundante y dirigido a un perfil más avanzado que la segunda.

Los resultados obtenidos permiten plantear ciertas cuestiones sobre si la producción científica está actuando de un modo acorde a las recomendaciones de muchas estrategias nacionales de seguridad. Estas estrategias defienden la creación de una

cultura de ciberseguridad, en donde la población general tenga conocimientos y medios para autoprotegerse de la ciberdelincuencia, y no solo formar a un reducido colectivo de especialistas en ciberseguridad. Además, la ciudanía también debe tener conciencia de los peligros en la red, es aquí en donde juega un papel crucial la educación en ciberdelincuencia. Es por ello que los resultados obtenidos, en donde se observa que la tendencia es contraria, pueden ser motivo de preocupación.

6. Referencias

Arenas, J. & Santillán-Rivero, E. (2002) Bibliometría ¿Para qué?. Biblioteca Universitaria Nueva Época. 5(1). 3-10. Disponible: https://rdudemo.unc.edu.ar/handle/123456789/715?locale-attribute=es

Cayón Peña, J., & García Segura, L. A. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. *Estudios En Seguridad Y Defensa*, *9*(18), 5-13. https://doi.org/10.25062/1900-8325.9

Cerceda, J.; Sanchez, F., & Herrera, D. (2019). Estudio sobre la Cibercriminalidad en España. Gabinete de Coordinación y Estudios. Ministerio del Interior, España.

Coz, J. & Fojón, E. (2011). Un modelo educativo para una estrategia nacional de ciberseguridad. Ingeniería de Sistemas para la Defensa de España.

Departamento de Seguridad Nacional, España. (2019). Estrategia Nacional de Ciberseguridad 2019. Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Donoso Vázquez, Trinidad.; Vilà Baños, R.; Rubio Hurtado, M. & Prado Soto, M. (2016). Perfil de cibervictimización ante las violencias de género 2.0. *FEMERIS* Vol.1, Núm. 1/2. Recuperado de: https://e-revistas.uc3m.es/index.php/FEMERIS/article/view/3226

Durieux, V. & Gevenois, P. A. (2010). Bibliometric Indicators: Quality Measurements of Scientific Publication. *Radiology*, 255(2). 342-351. https://doi.org/10.1148/radiol.09090626

Jansen, J., & Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, Vol. 10(1), 79–91. http://doi.org/10.5281/zenodo.58523

National Initiative for Cybersecurity Careers and Studies (NICCS). (2019). Official website of the Department of Homeland Security. Glossary. Consultado el 31/12/2019. Recuperado de https://niccs.us-cert.gov/about-niccs/glossary#C

Nzeakor, O., Bonaventure N., & Ezeh, P. (2020). Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment*. International Journal of Cyber Criminology*, Vol. 14(1): 283–299. http://doi.org/10.5281/zenodo.3753223

Observatorio Nacional para la Seguridad de la Información y la Ciberseguridad (OSIC). (2019) *Ciberpedia*. Consultado el 31/12/2019. Recuperado de https://observatoriociber.org/recursos/ciberpedia/#letra-c

Payne, B. K. & Hadzhidimova, L. (2020). Disciplinary and Interdisciplinary Trends in Cybercrime Research: An examination. *International Journal of Cyber Criminology, 14*, 81-105. doi:10.5281/zenodo.3741131

Pulido, G. M., & Rosell, R. R. (2017). Cooperación Público-Privada en el fomento de la cultura de ciberseguridad. *Cuaderno de Estrategia IEEE 185*, 217-246 http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2017/Cuaderno_185.html

Rhen, C. & Kronman, U. (2006). **Bibliometric handbook for Karolinska Institutet.** *Karolinska Institutet*.

Secretaría de Estado de Seguridad. (2021). Estudio sobre la cibercriminalidad en España. *Ministerio del Interior. Gobierno de España*. Consultado el 31/10/2021. Recuperado de

http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Ciber criminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3

Smith, Z.M., Lewis, J. A., & Lostri, E. (2020). The Hidden Costs of Cybercrime. *White Papers* & Webcasts. https://www.csis.org/analysis/hidden-costs-cybercrime

Valencia-Arias, A., Giraldo, M., Acevedo-Correa, Y., Garcés-Giraldo, L., Quiroz-Fabra, J., Benjumea-Arias, M., & Patiño-Vanegas, J. (2020). Tendencias investigativas en educación en ciberseguridad: Un estudio bibliométrico. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *E29*(05), 225–239.

Estudio 3: Revisión Sistemática

Métodos y efectos de la educación en ciberseguridad: Una revisión sistemática

Artículo publicado en Revista Electrónica de Criminología el 30/12/23.
Beltrán, A., Jiménez-Torres, M.G., & Sampayo, S. (2023). Métodos y efectos de la educación en ciberseguridad: Una revisión sistemática. *Revista Electrónica de Criminología, 14-07*. 1-19

RESUMEN

Este estudio tiene como objetivo analizar las técnicas educativas en el área de ciberseguridad y ciberdelincuencia, concretamente, las dirigidas a población no-técnica. Se llevó a cabo una revisión sistemática de la literatura científica empleando las bases de datos Scopus, Web of Science y Proquest. Tras analizar 79 artículos, se encontró que la gamificación, el entrenamiento, la simulación, el multimétodo y los medios audiovisuales son las técnicas más habituales y con mejores resultados de efectividad. También se encontró que los estudios se centran más en la ciberseguridad y las herramientas de protección que en educar en las ciberamenazas y concienciar. Por otra parte, se halló un reparto equitativo de los estudios siguiendo el criterio edad, con la excepción de la educación dirigida a la tercera edad, que resultó ser escasa. Finalmente, se encontró que existe fuerte predominancia de las ciencias STEAM, como ciencias computacionales e informática, frente a las ciencias sociales (psicología, criminología o ciencias de la educación), existiendo una grave falta de interdisciplinariedad en el área de estudio.

Palabras clave: Educación, ciberseguridad, ciberdelito, revisión sistemática, población no-técnica.

1. Introducción

La ciberdelincuencia es una problemática que va en aumento, y en el caso de España, las cifras son muy preocupantes. En el “Estudio sobre percepción y nivel de confianza en España” (ONTSI, 2022) se encontró que, en tan solo un año, del 2019 al 2020, la ciberdelincuencia aumentó un 31,9% llegando a los 287.963 hechos conocidos. Directamente relacionado con esta cuestión, en el mismo estudio se afirma que “*las costumbres online determinan en gran medida la exposición a los ataques*” (ONTSI, 2022: Pg. 16). Los factores de comportamiento humano son la clave para combatir el ciberdelito (Hadlington & Chivers, 2018). Por lo tanto, a la hora de prevenir la ciberdelincuencia, se debe incidir en la educación para poder cambiar dichos

comportamientos. Dentro de la educación, son de especial importancia las técnicas educativas y su relación con la vulnerabilidad y capacidad de los usuarios no-técnicos (Choi, 2008). Estas se pueden dividir en dos objetivos distintos y compatibles: la educación en ciberseguridad, dirigida a formar en herramientas y capacidades para protegerse, y la educación en ciberdelincuencia, orientada a conocer las ciberamenazas y formas que toma el ciberdelito. Actualmente se están investigando distintas formas de educar, técnicas, metodologías, estrategias, etc., por lo que también se han realizado distintas revisiones sobre aspectos concretos dentro del ámbito.

En Coenraad et al. (2020), se realizó una revisión sistemática de los juegos digitales relacionados con la ciberseguridad. Identificaron 181 juegos y tras probarlos 1 hora cada uno, expusieron sus características. En Svabensky et al. (2020)m examinaron 71 documentos centrándose en la educación en ciberseguridad. Discuten cursos, herramientas, ejercicios y enfoques de enseñanza y evaluaron las percepciones subjetivas de los estudiantes a través de cuestionarios. En cuanto a Zhang-Kennedy & Chiasson (2021), realizaron una revisión que cubría publicaciones académicas y productos de la industria relacionados con la educación en ciberseguridad dirigidas a usuarios finales no expertos. Identificaron 119 herramientas que catalogan en cinco categorías. También exploraron las tendencias actuales, evaluaron su uso y revisaron la evidencia empírica de la efectividad de las herramientas.

En Mendivil et al. (2022), se elaboró una revisión sistemática con el objetivo de explorar el uso de modelos de competencias para la elaboración de programas de formación y concienciación en ciberseguridad. Aldawood & Skinner (2018), consiguieron identificar algunas amenazas de ciberseguridad relacionadas con la ingeniería social en diversos entornos. Detallaron cómo los programas innovadores de educación en seguridad de la información pueden aumentar de manera efectiva la conciencia de los usuarios/empleados y, en última instancia, reducir los incidentes de seguridad cibernética. También se centra en empleados de organizaciones Jampen (2020), quien analiza la formación y entrenamiento en antiphishing y su eficacia. Al-Daeef et al. (2017), revisan el enfoque de capacitación de los usuarios como una solución no-técnica para mitigar las amenazas de seguridad en general y el problema de phishing en particular. Estudian factores como la atención de los usuarios, la concienciación y la retención de los conocimientos adquiridos durante más tiempo. Encuentran que las actividades de capacitación deben considerar los aspectos de adquisición, retención y transferencia de conocimientos.

Existe un amplio repertorio de técnicas y herramientas que presentan diversos resultados (Coenraad et al., 2020; Zhang-Kennedy & Chiasson, 2021) y que, en general,

consiguen mejorar los conocimientos y la concienciación ante formas concretas de ciberdelitos (Aldawood & Skinner, 2018; Al-Daeef et al., 2017). Por lo tanto, es de especial relevancia analizar los beneficios que muestra cada una de esas técnicas en la población. Este estudio permitiría saber con más precisión cuáles de ellas son más adecuadas y efectivas. A esto se añade la importancia de conocer cuáles son los perfiles específicos a los que se dirige y las diferencias que hay en las técnicas empleadas. Es por todo ello que, un análisis de los resultados de las técnicas educativas puede ser de gran utilidad para seleccionar las más adecuadas en cada caso. También es de especial interés saber si se educa sobre las distintas formas de ciberdelito o si solo se educa en las medidas para protegerse.

Otro punto relevante es analizar cuál es la disciplina de trabajo de los autores implicados en los estudios, para así conocer el peso de las aportaciones desde distintas áreas (Ingenierías, Ciencias Sociales, etc.) y valorar si se está produciendo una desproporción, tal y como señalan algunos autores (Thackray et al., 2016). Por último, se busca determinar si se incluye la educación en ciberdelincuencia en la educación en ciberseguridad, ya que permite concienciar sobre las amenazas y riesgos del ciberespacio. Actualmente, no hay disponible una revisión sistemática y/o meta-análisis reciente que evalúe todas estas cuestiones presentadas. En el caso de este estudio, la relevancia reside en poder seleccionar las mejores técnicas de educación en ciberseguridad a la hora de proteger a población no-técnica. Con todo ello, la educación se podría optimizar y también los recursos necesarios que implica.

En la siguiente sección, se explicará la metodología del trabajo, que consiste en una revisión sistemática, las bases de datos empleadas, la estrategia de búsqueda, el proceso de selección y codificación. En la tercera sección, se describirán los resultados sobre las técnicas encontradas, su efectividad comparada, perfiles diana y áreas de estudio. En la cuarta sección, se discutirán los resultados y sus implicaciones, además de su relación con la literatura científica. En la última, resumiremos los contenidos y expondremos las principales conclusiones.

2. Método

El método empleado para este estudio ha sido la revisión sistemática, consultando las bases de datos SCOPUS, Web of Science y Proquest. Las revisiones sistemáticas de la evidencia científica son estudios que sintetizan la evidencia científica disponible, de forma eficiente (Tricco et al., 2015). Usan métodos explícitos y rigurosos para identificar, seleccionar, evaluar, analizar y sintetizar los estudios empíricos que permitirán responder a cuestiones específicas (Perestelo-Pérez, 2013). Permiten analizar áreas

emergentes y son útiles para responder preguntas de investigación (Sucharew & Macaluso, 2019). Mediante este procedimiento, se han seleccionado 79 artículos relacionados con la educación en ciberseguridad dirigida a población no-técnica. Estos artículos se eligen de revistas de referencia, altamente citadas y revisadas por pares. Además, en todo momento se ha seguido el protocolo PRISMA (Liberati et al., 2009; Hutton et al., 2016) para revisiones sistemáticas, con criterios de inclusión y exclusión de los artículos, y sus fases de identificación, selección, elegibilidad e inclusión.

La pregunta, claramente definida, sigue el formato PICOS: descripción de los participantes (P), las intervenciones (I), las comparaciones (C) y las medidas de resultado de la revisión sistemática (O), así como el tipo de estudio (S). Además, este tipo de técnicas son cada vez más empleadas para facilitar la toma de decisiones (Bosch-Capblanch et al., 2012). Se hace necesario enfocar cuidadosamente la pregunta y usar estrategias de búsqueda (Grant & Booth, 2009). En cuanto a la Pregunta de investigación que se plantea en este estudio es la siguiente: ¿Cuáles son los efectos de las distintas técnicas y herramientas utilizadas en educación en ciberseguridad/ciberdelincuencia orientada a usuarios no-técnicos?.

A partir de dicha pregunta de investigación se determinan los siguientes objetivos de investigación:

Objetivo 1: Identificar cuáles son las principales técnicas y herramientas para educar en ciberseguridad/ciberdelincuencia.

Objetivo 2: Comparar los efectos de las diferentes técnicas y herramientas utilizadas en la educación en ciberseguridad/ciberdelincuencia sobre usuarios no-técnicos.

Objetivo 3: Averiguar si la educación se centra únicamente en la educación en ciberseguridad o, por lo contrario, también incluye nociones de ciberdelincuencia y sus amenazas.

Objetivo 4: Estudiar cuáles son las poblaciones específicas a las que se dirige esta educación.

Objetivo 5: Identificar los perfiles científicos o áreas de estudio de los/as autores/as en dichas investigaciones.

2.1. Protocolo PICO

Se ha aplicado el protocolo PICO para la delimitación del estudio. Se utiliza el acrónimo PICO para la construcción de la pregunta (Villasís-Keever et al., 2020), en la cual se incluyen los cuatro componentes principales: población de estudio; intervención por

evaluar; comparación de la intervención; outcome measures (efectos). Una vez finalizado, se ha procedido a codificar y analizar los artículos resultantes para la elaboración del análisis de resultados. En nuestro estudio los componentes son los siguientes:

(P) Población: La población objetivo del estudio es la población general, entendiendo esta como usuarios no-técnicos. Se excluye del estudio aquella educación dirigida a la siguiente población: Personas que por su rol o función tengan encomendadas tareas de ciberseguridad; profesionales de ciberseguridad; personas de tecnologías de la información en organizaciones y empresas; alumnos de titulaciones vinculadas a la ciberseguridad; Trabajadores públicos relacionados con la ciberseguridad o la ciberdelincuencia.

(I) Intervención: Recibir educación en el área de la ciberseguridad y/o sobre la ciberdelincuencia en sus distintas modalidades.

(C) Comparativo: Se comparan las distintas técnicas educativas en ciberseguridad/ciberdelincuencia sobre la población objetivo (usuarios no-técnicos).

(O) Resultados: Los efectos de la educación sobre la población objeto de estudio.

2.2. Estrategia de búsqueda

Para las búsquedas se han utilizado los términos “educación“, “ciberseguridad“, “ciberdelincuencia“ junto con términos referentes a las consecuencias y efectos de dicha educación. Además, se han añadido términos relacionados con la población objetivo (población no técnica), se emplearon términos equivalentes y los conectores lógicos “Y“ y “O“ de acuerdo a la búsqueda booleana. Se seleccionaron únicamente artículos en lengua inglesa. Se han delimitado el tipo de literatura a aquellos que sean: artículos o artículos de conferencias.

El análisis de las bases de datos se llevó a cabo el 3 de junio del año 2022. Después de un examen de las bases de datos existentes, se seleccionaron como fuentes de búsqueda de datos primarios Web of Science, SCOPUS y Proquest.

2.3. Fórmula de búsqueda

TITLE-ABS-KEY (cybersecurity OR cyber-security OR cybercrime OR phishing) AND TITLE-ABS-KEY (educat* OR pedagog* OR teach* OR train* OR intervention OR gamification OR simulation) AND TITLE-ABS-KEY (result* OR benefit* OR capabilit* OR effect* OR skill* OR knowledge* OR victimisation OR victimization OR awareness) AND TITLE-ABS-KEY (non-tech* OR “non technical” OR “high school” OR high-school

OR teen* OR teenage* OR child* OR youth OR k-12 OR “young people” OR citizenship OR elderly OR “elder population” OR user*)

Fecha de búsqueda 03/06/2022 (Aplicando inclusión de textos: en inglés ; artículos; artículos de conferencias)

Resultados de búsqueda : SCOPUS 1180 + WOS 923 + PROQUEST 334 = 2437

Resultado de Búsqueda tras el volcado en Zotero y eliminado de duplicados = 1537

2.4. Proceso de selección de los artículos

En primer lugar, los estudios recuperados se revisaron por título, keywords y resumen. Solo aquellos estudios preseleccionados en esta primera criba (teniendo en cuenta los criterios de inclusión/exclusión) pasaron a revisarse a texto completo. Fueron dos los revisores que procedieron a seleccionar las referencias relevantes de forma independiente. Para realizar un procedimiento exhaustivo se ha empleado el protocolo PRISMA (Liberati et al., 2009). La Figura 1, muestra el diagrama de flujo del proceso de búsqueda y selección según viene establecido en PRISMA y cuya finalidad es garantizar trasparencia y claridad.

En cuanto a los criterios de inclusión, fueron los siguientes:

a) Estudios primarios relativos a la educación en ciberseguridad y/o educación en cibercrimen y sus efectos en población no-técnica: beneficios, conocimientos, concienciación, habilidades, y reducción de la victimización.

b) Artículos de revistas y artículos de conferencias.

c) Revisión por pares (peer review).

d) Estudios observacionales: Diferencias en los resultados de capacitación/vulnerabilidad frente a ciberdelitos y ciberamenazas en función de haber recibido las técnicas de educación en ciberseguridad.

e) Estudios quasi y experimentales: Diferencias pre y post en los resultados de test, simulaciones o pruebas de capacitación y/o vulnerabilidad ante ciberamenazas, según hayan recibido educación en ciberseguridad y/o ciberdelincuencia.

Los criterios de exclusión:

a) Artículos duplicados.

b) Literatura gris como blogs y noticias.

c) Revisiones sistemáticas y meta-análisis.

d) Artículos cuya población a la que se dirige la educación quede fuera del objeto de estudio: Personas que por su rol o función tengan encomendadas tareas de ciberseguridad; profesionales de ciberseguridad; personas TI de organizaciones y empresas; alumnos de titulaciones vinculadas a la ciberseguridad; Trabajadores públicos relacionados con la ciberseguridad o la ciberdelincuencia.

e) Artículos fuera de objeto de estudio; artículos sobre cuestiones relacionadas pero no tengan intervención.

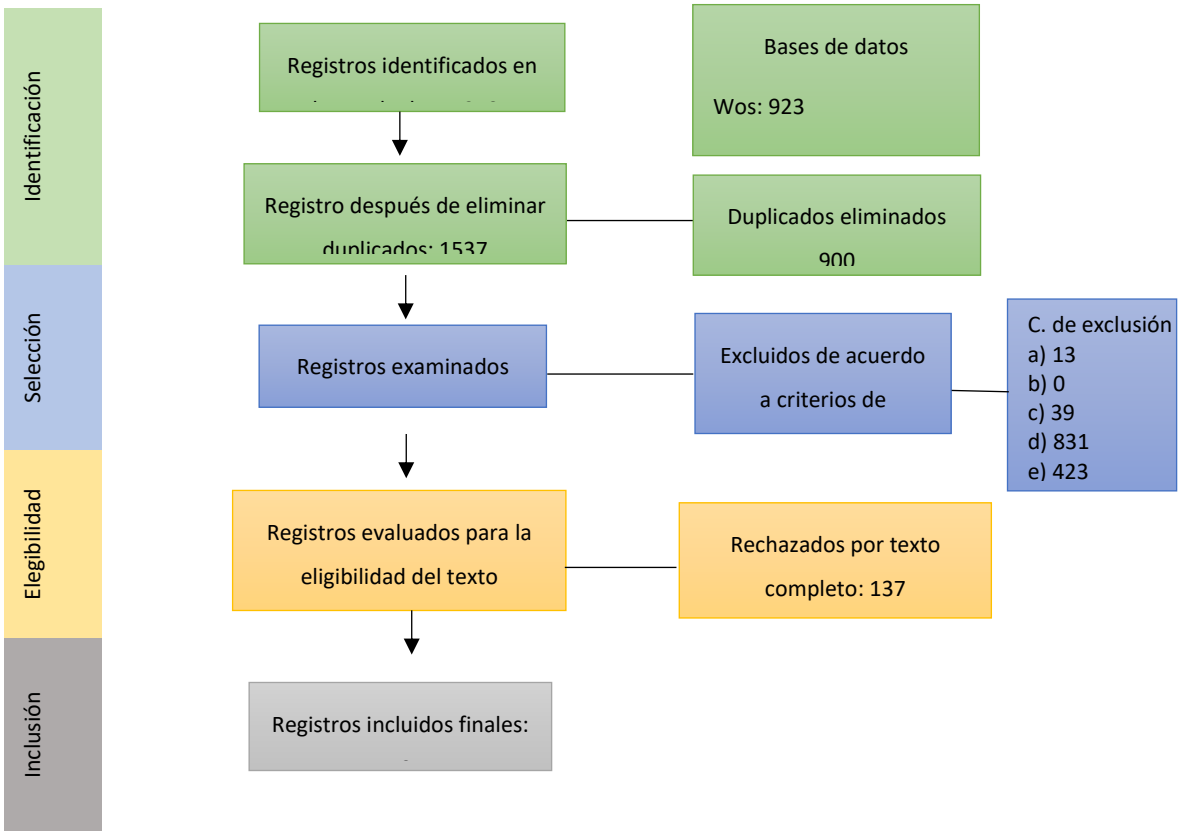


Figura 1. Diagrama de flujo PRISMA

Tabla 1. Artículos incluidos en fase final

Ar.	1° AUTOR Y AÑO	Ar.	1° AUTOR Y AÑO	Ar.	1° AUTOR Y AÑO	Ar.	1° AUTOR Y AÑO
1	Giannakas, F. 2019	21	Shen, L.W. 2021	41	Moreno-Fernández, M. 2017	61	Gokul, C.J. 2018
2	Reid, R. 2015	22	Giannakas, F. 2015	42	Herzberg, A. 2011	62	Newbould, M. 2009
3	Decusatis, C. 2022	23	Qusa, H. 2021	43	Jin, G. 2018	63	Visoottiviseth, V. 2018
4	Cornel, C. 2016	24	Amo, L. C. 2019	44	Scholefield, S. 2019	64	Kumaraguru, P. 2007
5	Yett, B. 2020	25	Veneruso, S.V. 2020	45	Kumaraguru, P. 2007	65	Neo, H.F. 2021
6	Al-Hamar, Y. 2020	26	Huynh, D. 2017	46	Chen, T. 2020	66	Kaabi, L.A. 2022
7	Chattopadhyay, A. 2019	27	Alqahtani, H. 2020	47	Beckers, K. 2016	67	Kovačević, A. 2020
8	Tsokkis, P. 2018	28	Septiana, R. 2020	48	Alwanain, M. 2021	68	Kumaraguru, P. 2009
9	Saito, T. 2019	29	Lim, I. 2016	49	Lastdrager, E. 2019	69	Giannakas, F. 2016
10	De Bona, M. 2020	30	Maqsood, S. 2021	50	Cuchta, T. 2019	70	Olano, M. 2014
11	Mugayitoglu, B. 2021	31	Mikka-Muntuumo, J. 2021	51	Rastenis, J. 2020	70	Ganesh, A. 2022
12	Burris, J. 2018	32	Volkamer, M. 2018	52	Baillon, A. 2019	72	Baslyman, M. 2016

13	Plachkinova, M. 2019	33	Sercombe, A.A. 2012	53	Wolf, S. 2020	73	Reid, R. 2014
14	Reinheimer, B. 2020	34	Sookhanaphibarn, K. 2020	54	Davinson, N. 2010	74	Quinkert, F. 2021
15	Pittman, J.M. 2016	35	Tschakert, K.F. 2019	55	Kumaraguru, P. 2008	75	Zhang-Kennedy, L. 2016
16	Sheng, S. 2007	36	Sun, J.C. 2016	56	Kunz, A. 2016	76	Weaver, B.W. 2021
17	Alencar, G.D. 2013	37	Dodge, R. 2012	57	Zielinska, O.A. 2014	77	Silic, M. 2020
18	Wang, Y.-J. 2018	38	Salazar, M. 2013	58	Peker, Y.K. 2018	78	Wen, Z.A. 2019
19	Wolf, S. 2020	39	Streiff, J. 2019	59	Schoebel, S. 2021	79	Wash, R. 2018
20	Kolb, C. 2022	40	Althobaiti, K. 2018	60	Alwanain, M. 2020		

2.5. Codificación

Posteriormente, se procedió a la codificación de los 79 estudios que fueron finalmente incluidos en la revisión sistemática (Tabla 1) y se evaluó su calidad metodológica y/o riesgo de sesgo (González et al., 2012). Todo el proceso de selección de los estudios se realizó por pares, resolviendo las posibles discrepancias por consenso y con la intervención de una tercera autora. Las tablas de codificación se han incluido en el anexo. En ellas se encuentra toda la información completa empleada para el estudio. Durante la codificación de los estudios, se extrajo de cada uno de ellos los siguientes datos:

a) Publicación: cita completa, año, revista y país.

b) Tipo de técnicas empleadas.

c) Tipo de educación incluida: Ciberseguridad; ciberdelincuencia+ciberseguridad; ciberdelincuencia.

d) Población diana.

e) Área/disciplina de los/as autor/es

f) Resultados: Efectos de la educación en la población objeto de estudio. Mejora, disminución o ausencia de cambios sobre la vulnerabilidad/capacitación frente a la ciberdelincuencia.

- Ef.1: La mejora de la capacidad para protegerse en el ciberespacio/ disminución de la vulnerabilidad;
- Ef.2: La mejora de la capacidad para protegerse en el ciberespacio/ disminución de la vulnerabilidad frente a un grupo control;
- Ef.3: Disminución de la capacidad / aumento de la vulnerabilidad;
- Ef.4: Disminución de la capacidad / aumento de la vulnerabilidad frente a un grupo control;
- Ef.5: Ausencia de cambios o cambios no significativos.

- Ef.6: Ausencia de cambios / resultados idénticos al grupo control.

3. Resultados

Los resultados se han dividido en un primer apartado de variables geográficas con el análisis por países. Un segundo apartado con los tipos de educación y las técnicas empleadas, en el que se exponen los efectos de la educación y se comparan según las técnicas. Por último, un apartado con las poblaciones diana a las que se dirige la educación y las áreas de estudio de los autores con una comparativa por disciplinas.

3.1. Países

Tal y como se puede observar en la Figura 2, la predominancia de Estados Unidos es clara, con un total de 45 artículos de los 79 incluidos en el estudio. La mayor parte de las revistas de ciberseguridad en las que se publicaron los artículos de esta revisión, tienen su origen en los Estados Unidos. Le siguen muy de lejos Alemania con 11 artículos y Reino Unido con 7. Los demás países aportan entre 1 y 4 de esta revisión. En cuanto a España, ninguno de los 79 artículos proceden de dicho país.

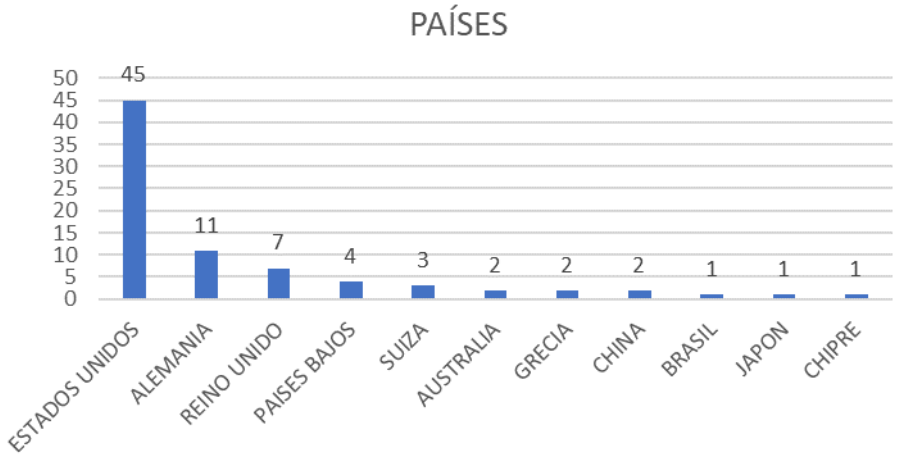


Figura 2**.** N° de artículos por país

3.2. Tipos de educación y de técnicas empleadas

En la Tabla 2 se muestra el listado resultante de las técnicas encontradas en los 79 artículos. Se ha incluido en la primera columna el listado de técnicas y en la segunda columna el número de artículos de cada una. En la tercera se muestra el porcentaje de los artículos en relación al total (79). Entre las tres primeras técnicas están: Gamificación (31; 39,24%), Entrenamiento (14; 17,72%) y Multimétodo (10; 12,65%). Suman el 70% del total de las técnicas. El resto son menos frecuentes, encabezadas por la Simulación (6,33%) y los Medios audiovisuales (5,6%). También están presentes los campamentos

de ciberseguridad o Cybercamp, robots, clases prácticas, escape room, e-learning, juego de cartas, talleres colaborativos, mapas conceptuales, comics y lectura de consejos y relatos.

A continuación, se han expuesto las distintas posibilidades planteadas de los efectos tras recibir educación en ciberseguridad/ciberdelincuencia. En los casos del Ef. 3 y Ef. 4 no hay ningún registro ya que no se encontraron estudios en los que los resultados post-tratamiento fuesen peores que los pre-tratamiento. Son ampliamente mayoritarios los que tuvieron Ef. 1 (La mejora de la capacidad) y Ef. 2 (Mejora frente al grupo control). En cuanto a los que presentaron los efectos Ef.5 (Ausencia de cambios) y Ef.6 (Ausencia de cambios frente a grupo control) son minoritarios, únicamente 5 artículos del total de 79.

Tabla 2. Técnicas educativas, n° de artículos y % de mejora tras la intervención.

Técnica	N° art.	% del total	Ef. 1	Ef. 2	Ef. 3	Ef. 4	Ef. 5	Ef. 6	% Mejora*
Gamificación	31	39,24%	20	10			1		51,75%
Entrenamiento	14	17,72%	4	8			1	1	29,25%
Multimétodo	10	12,65%	7	3					59,5%
Simulación	5	6,33%	3	1			1		47,16%
Medios audiovisuales	4	5,6%	3	1					67,5%
Cybercamp	3	3,79%	3						49,5%
Robot	2	2,53%	1	1					33%
Clases prácticas	2	2,53%	1					1	-
Escape Room	2	2,53%	2						-
E-Learning	1	1,27%	1						58%
Juego de cartas	1	1,27%	1						
Taller grupal/ colaborativo	1	1,27%	1						82%
Mapas conceptuales	1	1,27%		1					-
Cómic	1	1,27%	1						42%
Lectura de consejos/ relatos	1	1,27%		1					21%

Nota. El % medio de mejora tras recibir educación en ciberseguridad/ciberdelincuencia.

Por último, tras recopilar los datos de los resultados que presentaron los participantes de los estudios y armonizar los datos en % de mejora, se elaboró una tabla (Tabla 3) en donde poder comparar los % de dichos estudios organizados por técnica. Las mejoras en algunos casos se obtuvieron mediante pretest y postest tras la intervención. En otros casos, mediante la comparativa de distintas técnicas en diferentes grupos. En algunos estudios no fue posible obtener esos datos porque, o bien no se mostraba ese dato en el artículo, o bien no fue posible transformar en % de mejora. Una vez realizada la tabla, se procedió a hacer la media total de mejora de todos los estudios de cada técnica empleada. Esa media de % de mejora se muestra en la última columna (% Mejora).

Tabla 3. Porcentajes de mejora tras la intervención

Técnica	Efecto	Porcentaje de mejora tras la intervención/tratamiento educativo															Media	
Gamificación	Ef.1 %	70	24	76	80	75	80	78	75	20	12	29	76	24	35		53,85%	51,75%
	Ef.2 %	81	18	77	20	30	72										49,66%	
Entrenamiento	Ef.1 %	49	9														29%	29,25%
	Ef.2 %	18	67	14	50	28											29,5%	
Multimétodo	Ef.1 %	37															37%	59,5%
	Ef.2 %	82															82%	
Simulación	Ef.1 %	80	27	14													40,33%	47,16%
	Ef.2 %	54															54%	
M. Audiovisuales	Ef.1 %	37	98														67,5%	67,5%
Cybercamp	Ef.1 %	44	55														49,5%	49,5%
Robot	Ef.1 %	33															33%	33%
Clases prácticas	-	-															-	-
Escape Room	-	-															-	-
E-Learning	Ef.1 %	58															58%	58%
Juego de cartas	-	-															-	-
Taller grupal/ colaborativo	Ef.1 %	82															82%	82%
Mapas conceptuales	-	-															-	-
Cómic	Ef.1 %	42															42%	42%
Lectura de consejos/ relatos	Ef.2%	21															21%	21%

Si ordenamos las técnicas por % de mejora tras la intervención educativa, encontramos entre las 5 primeras: el taller colaborativo (82%) (solamente 1 estudio), seguido de Medios Audiovisuales (67,5%), la técnica Multimétodo (59,5%), E-Learning (58%) y la Gamificación (51,75%). De estas 5 primeras técnicas con mejor % de mejora, la Gamificación y el Multimétodo se encuentran también entre las 5 primeras en número de artículos totales. Se puede afirmar que estas 2 técnicas, Gamificación y Multimétodo, son las que presentan mejores puntuaciones de aprendizaje siendo las mejores a nivel de respaldo empírico. La técnica de entrenamiento, aunque se encuentra en el segundo puesto en número total de artículos, tiene el penúltimo resultado en % de mejora. Por lo tanto, se muestra como una de las técnicas que menores beneficios proporciona frente a otras técnicas. A esto se añade que, si la comparamos con las otras que tienen mayor respaldo científico en número de artículos, se encuentra en el último puesto a nivel de % de mejora.

En cuanto a los tipos de educación según los contenidos incluidos (ver Figura 3), existe una gran diferencia entre aquellas que se orientan únicamente a la ciberseguridad, frente a las que incluyen también aspectos sobre ciberdelincuencia. Las primeras se centran en las herramientas, medios, capacidades y conocimientos para defenderse de posibles ciberamenazas, mientras que las segundas incluyen nociones sobre cuáles son las ciberamenazas: formas de ciberdelitos, conceptos teóricos y prácticos sobre phishing, malware, grooming, sexting, smishing, rootkit, etc. Tal y como se puede observar en la Figura 3, las que se orientan fundamentalmente a la ciberseguridad (53) son mayores que las que contienen conocimientos también en

ciberdelincuencia (26). No se han encontrado artículos que solamente contengan conocimientos sobre las ciberamenazas sin incluir ciberseguridad.

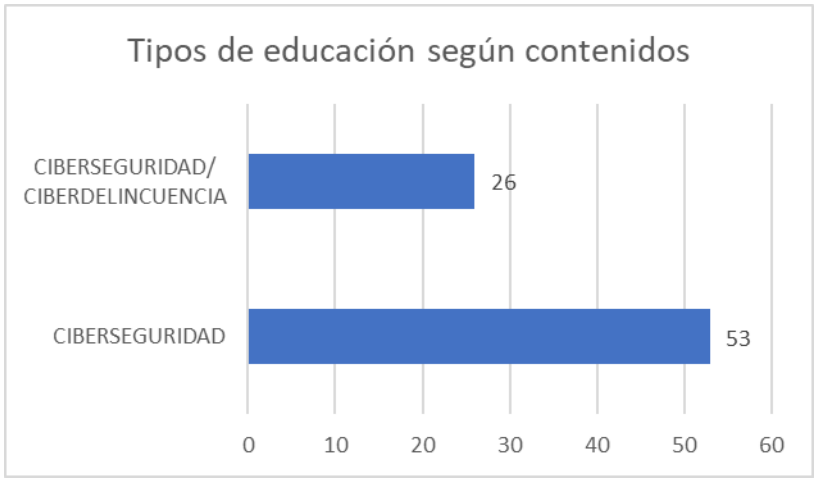


Figura 3**.** Gráfica de barras de los distintos tipos de educación según sus contenidos

3.3. Población diana y áreas de estudio

En la Tabla 4 se muestran los datos relacionados con los colectivos objetivo de intervención según su edad. Tal y como se puede observar, siguen una progresión numérica desde la infancia hasta los adultos, con la excepción de la tercera edad en donde hay 1 solo artículo (0,94%). Este dato resalta la falta de investigaciones que estudien la educación en ciberseguridad orientada a la tercera edad. La mayor parte de las intervenciones educativas se centran en adultos (31,13%) y en los jóvenes (26,41%), que juntos suman 57,54% del total. También cabe destacar que parte de los estudios orientados a estos grupos, estaban dirigidos específicamente a empleados de organizaciones, instituciones y empresas. Por último, los niños (18,86%) y los adolescentes (22,64%) acumulan el 41,5% del total de las investigaciones.

Tabla 4. Tabla de colectivos por edades y área de estudio de autores/as

Colectivo por edad	Rango de edades	N°Artículos	porcentaje
Niños	0-12	20	18,86%
Adolescentes	12-18	24	22,64%
Jóvenes	18-30	28	26,41%
Adultos	30-65	33	31,13%
Ancianos	+65	1	0,94%

En cuanto a las áreas de estudio de los autores, los datos son muy claros en la supremacía de las ciencias (STEAM) frene a otras áreas como son las ciencias sociales (ver Figura 4). Los artículos que fueron elaborados exclusivamente por autores/as procedentes de ciencias STEAM forman el 82% del total, mientras que los elaborados en exclusiva por autores/as de ciencias sociales (en adelante CC.SS) apenas alcanzan

el 4%. Dentro del área STEAM, predominan las Ciencias Computacionales, ya que un gran número de autores/es pertenecen a esa rama de estudio. Otro dato relevante es la falta de interdisciplinariedad: de todos los estudios, tan solo el 13% estuvieron formados por miembros procedentes de áreas de STEAM y CC.SS conjuntamente.

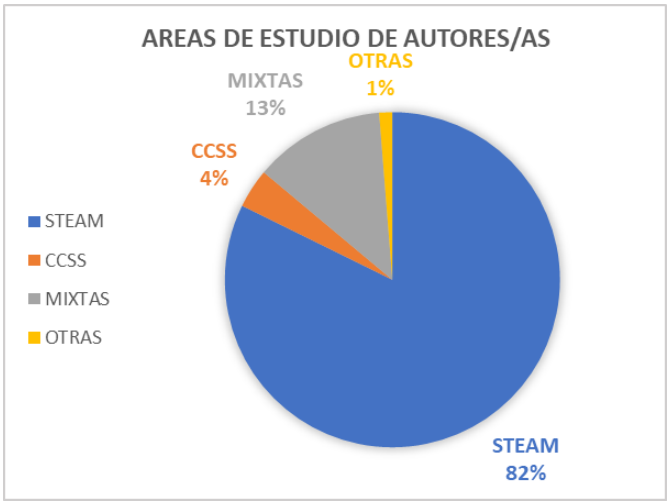


Figura 4. Áreas de estudio de autores/as

4. Discusión

Tras los resultados hallados, se puede afirmar que las principales técnicas que se están empleando en el ámbito de la educación en ciberseguridad son la gamificación, el entrenamiento, las técnicas multimétodo, la simulación y los medios audiovisuales. Este conjunto de técnicas va más allá de la educación expositiva tradicional y enfocan la educación como un proceso interactivo en el que la persona participante debe implicarse activamente. Por su parte, la gamificación aplica los conocimientos de la teoría del juego y la teoría del flujo (Deterding et al., 2011; Silic, 2020) a contextos ajenos al juego, con la finalidad de modificar los comportamientos y resultados. Los principios de esta "ludificación" se han mostrado como un enfoque eficaz para mejorar la capacidad de protección (51,75%), la motivación intrínseca, el aprendizaje, las habilidades de afrontamiento y el cumplimiento de las normas de seguridad.

En cuanto al entrenamiento, se considera una estrategia para mejorar la capacidad de discriminación, adecuada para aumentar sensibilidad a las señales visuales de engaño y para producir una mejora de las capacidades discriminativas (Dodge, 2012; Moreno-Fernández, 2017; Lastdrager, 2019). No obstante, tal y como se muestra en los resultados, es de las técnicas que tiene una tasa de mejora más baja frente a las demás (29,25%). De esto se desprende que quizás fuese una buena técnica para combinar con otras dentro del multimétodo. Las tareas multimétodo se refieren al uso mixto de varias técnicas de forma conjunta, aunque habitualmente consisten en la combinación de las

técnicas más habituales como la gamificación, el entrenamiento o la simulación (Chattopadhyay, 2019; Mugayitoglu, 2021; Reinheimer, 2020; Pittman, 2016; Alencar, 2013; Wolf, 2020; Tschakert, 2019; Herzberg, 2011; Baillon, 2019; Wen, 2019). El uso mixto de técnicas muestra buenos resultados (59,5% de mejora) y permite beneficiarse de los beneficios que aporta cada una de ellas. El hecho de que en la mayoría de ocasiones que se emplea el multimétodo se incluya la gamificación, es otra muestra de la versatilidad y efectividad que tiene la misma. De los resultados obtenidos se desprende que esta opción resulta de las mejores a la hora de educar en ciberseguridad.

Los campamentos de ciberseguridad o Cybercamp también muestran buenos resultados (49,5%), siendo un tipo de actividad inmersiva, con un fuerte contenido de socialización y trabajo en equipo (Cornel, 2016; Pittman, 2016; Jin, 2018; Wolf, 2020). Otras técnicas, como el empleo de Robot o Robot Social (Yett, 2020; Althobaiti, 2018) apuestan por dar nuevas aplicaciones (educativas en ciberseguridad) a las tecnologías más innovadoras. Las Clases prácticas son otra herramienta que se muestra eficaz por la implicación y la atención que requiere, mejorando la motivación intrínseca (Amo, 2019; Kolb, 2022). El Escape Room, el tradicional juego que consiste en tratar de escapar de una sala o lugar en un tiempo límite, también se ha conseguido aplicar al ámbito de la educación en ciberseguridad (Decusatis, C. 2022; Streiff, 2019).

Por último, se han encontrado resultados positivos en las técnicas de E-Learning (Peker, 2018), los juego de cartas (Wang, 2018), taller grupal y colaborativo (Kovačević, 2020), mapas conceptuales (Sun, 2016), cómic (Zhang-Kennedy, 2016) y la lectura de consejos y relatos (Wash, 2018). Merece una especial atención los talleres grupales y colaborativos (mejora del 82%) porque permiten socializar, de una forma transversal a todo el proceso educativo, con el grupo de iguales. Señalar que la literatura a este respecto es escasa, ya que solo se ha podido incluir un estudio. En estos talleres, los participantes trabajan en grupo para superar las distintas pruebas y retos educativos.

En base a los resultados encontrados, se confirma que son más numerosas las técnicas que se orientan únicamente a la ciberseguridad frente a las que incluyen también aspectos sobre ciberdelincuencia. La relevancia de este hecho radica en que, la ciberseguridad como elemento único, puede no ser suficiente a la hora de prevenir la ciberdelincuencia en la población. Si solamente se da formación en medios y herramientas para poder protegerse, pero no se informa lo suficiente de cuáles son las amenazas reales en el ciberespacio, no estaremos completando totalmente la prevención de los individuos. Esto va en la misma línea que diversos autores, los cuales señalan que la clave de la prevención es la es la concienciación ciberdelito (Aldawood & Skinner, 2018; Hadlington & Chivers, 2018; Huynh, 2017). Otro motivo es que, tal y

como señala la literatura (Chadee & Ng Ying, 2013), cuando se informa a la población sobre cuáles son las amenazas existentes, también estamos apelando a una cierta preocupación o miedo moderado. Este motivará al individuo y conseguirá que ponga en marcha esos conocimientos de ciberseguridad.

Los datos arrojan que la educación se dirige de una forma muy equilibrada a los colectivos poblacionales siguiendo el criterio de edad. Se reparten entre niños, adolescentes, jóvenes y adultos en un rango del 18% al 31%. La única excepción es la de la tercera edad (Alwanain, 2020), para la que apenas se han puesto en marcha estudios de cómo adaptar la educación en ciberseguridad. En cuanto a niños y adolescentes, las técnicas empleadas más habituales son las técnicas de gamificación, en algunos casos adaptadas de modo específico para esos colectivos (Giannakas, 2015; Giannakas, 2016; Giannakas, F. 2019; Shen, 2021; Qusa, 2021; Maqsood, 2021; Schoebel, 2021; Neo, 2021; Reid, 2014). El empleo de juegos tiene un componente motivador muy grande en estos colectivos y, sobre todo, consigue un equilibrio necesario entre aprendizaje y entretenimiento.

También son especialmente útiles los materiales audiovisuales (Reid, 2015) y los cybercamps (Cornel, 2016; Pittman, 2016; Jin, 2018; Wolf, 2020). Los materiales audiovisuales fomentan la activación de distintos sentidos y crean estímulos visuales y auditivos. Estas cualidades permiten mejorar la motivación y la atención en la infancia frente a la exposición oral o los textos. En el caso de los cybercamps, éstos permiten crear un entorno educativo completo con inmersión educativa prolongada y compartida. En cuanto al entrenamiento aplicado a niños, Saito (2019), Alwanain (2021) y Lastdrager (2019), han tenido buenos resultados, con mejoras del 49%, 50% y 14% respectivamente. Esto demuestra que siempre que sean técnicas que requieran una respuesta constante y participativa, será útil y efectiva en los/as niños/as.

En lo que respecta a los jóvenes y adultos, gran parte de las técnicas que se han implementado han seguido la línea de la gamificación (Sheng, 2007; Veneruso, 2020; Huynh, 2017; Alqahtani, 2020; Sercombe, 2012; Sookhanaphibarn, 2020; Salazar, 2013; Scholefield, 2019; Chen, 2020; Beckers, 2016; Cuchta, 2019; Kunz, 2016; Gokul, 2018; Newbould, 2009; Kumaraguru, 2009; Baslyman, 2016; Silic, 2020). La media de mejora conseguida con esta técnica es un 51,75% (Tabla 3), por lo que emplear esta técnica es garante de buenos resultados, aunque un elemento imprescindible a tener en cuenta es procurar adaptar siempre la gamificación a la población diana a la que se dirige.

Siguiendo con el colectivo de jóvenes y adultos, también nos encontramos el entrenamiento (Moreno-Fernández, 2017; Kumaraguru, 2007; Rastenis, 2020;

Davinson, 2010; Kumaraguru, 2008; Zielinska, 2014; Quinkert, 2021; Weaver, 2021) y la simulación (De Bona, 2020; Burris, 2018 Septiana, 2020; Lim, 2016) como las grandes apuestas para poder educar y proteger a estos colectivos. El entrenamiento y la simulación van muy unidos, suelen incluir ejemplos de ciberataques ante los que el participante debe protegerse. Mediante ensayo y error y con mensajes de feedback, se van mejorando los conocimientos y la capacidad de defensa. También permiten al usuario/a habituarse al lenguaje del ámbito, al modus operandi de los ciberdelincuentes, identificar y detectar contenidos sospechosos o fraudulentos y aprender a reaccionar ante ellos.

Los resultados muestran claramente la supremacía de los perfiles procedentes de ciencias STEAM, especialmente de ciencias computacionales e informática. Se ha encontrado que son perfiles muy técnicos centrados en cuestiones de programación, diseño y ciberseguridad a un nivel avanzado. Por otra parte, los perfiles procedentes de CC.SS. son escasos, como sería el caso de psicología, criminología, sociología o ciencias de la educación. Esta falta de interdisciplinariedad va en línea con lo que señalan algunos autores (Ghernaouti-Helie, 2009), que apuntan a una falta de diversidad científica en los perfiles dedicados a la educacióne en ciberseguridad. La importancia de lo que está sucediendo reside en que, cuando hablamos de educación en ciberseguridad, deberían estar presentes perfiles con conocimientos en pedagogía y aprendizaje.

También son necesarios perfiles relacionados con el comportamiento humano, como psicología o criminología. Cuando se habla de víctimas, delincuentes, heurísticos, factor del miedo, vulnerabilidad, capacitación, ciberresiliencia, error humano, etc. estamos dentro del área de estudio de estas ciencias. En línea de lo que señala la literatura (López et al., 2021), la riqueza de disponer de distintas visiones, metodologías, enfoques y conocimientos permitirá abordar la cuestión de la educación en ciberseguridad orientada a población no-técnica de un modo completo y más adaptado a la realidad. Adicionalmente, es de destacar que ninguno de los 79 artículos proceda de España, lo que pueda ser señal de una falta de inversión, de medios y de revistas de impacto en el área de la ciberseguridad. Se debe tener en cuenta el efecto distorsionador del idioma, ya que el inglés es el idioma predominante, y tanto EEUU como Reino Unido son de habla inglesa.

5. Conclusiones

La principal contribución de este estudio es dar una visión global de las técnicas educativas en el área de ciberseguridad y ciberdelincuencia. Se ha encontrado que la

gamificación, el entrenamiento, la simulación, el multimétodo y los medios audiovisuales son las técnicas más habituales. De ellas, las que obtienen mejores resultados de eficacia son la gamificación y el multimétodo. Todas estas técnicas consiguen mejorar la protección, los conocimientos en ciberseguridad y en ciberdelincuencia, y sobre todo, defenderse de ciberamenazas como el phishing. En líneas generales, los beneficios de emplear estas técnicas son: la mejora de la motivación intrínseca, asentar los conocimientos, conseguir valoraciones muy positivas de los participantes y mejorar la atención frente a la educación tradicional (expositiva).

En cuanto a los contenidos, se ha hallado que los estudios se enfocan principalmente en las herramientas y medidas para protegerse, frente a aquellos otros que incluyen contenidos para educar sobre la ciberdelincuencia. Estas diferencias son relevantes por la enorme utilidad que tiene aprender cuáles son las ciberamenazas, especialmente de cara a la concienciación y la puesta en marcha de las medidas de autoprotección. También se analizó la literatura científica atendiendo a las poblaciones diana en función de la edad, encontrando un reparto equitativo entre los distintos colectivos con la excepción de la tercera edad. Esta última apenas tiene estudios que la hayan abordado, por lo que sería necesario un mayor trabajo en esta dirección.

Finalmente, se ha encontrado que existe fuerte predominancia de las ciencias STEAM (especialmente ciencias computacionales) frente a las CC.SS. Todo ello a pesar de la importancia que tienen los enfoques interdisciplinares, con la presencia de ciencias del comportamiento como pueden ser la psicología, criminología, sociología o las ciencias de la educación. En cuanto a las limitaciones, se debe señalar que los porcentajes de mejora se han obtenido de estudios que emplearon distintas muestras. También que la cantidad de artículos de las distintas técnicas fueron distintos, por ejemplo, los de gamificación fueron más numerosos que los de talleres colaborativos. Otra limitación sería las propias de las revisiónes sistemáticas, ya que se han empleado bases de datos como Scopus y Web of Science, sin embargo, existen artículos en la literatura gris o en otras bases de datos que podrían aportar importantes estudios para el análisis.

Las implicaciones de esta investigación pueden ser especialmente relevantes en el ámbito aplicado de la educación en ciberseguridad. El motivo es que existe un gran esfuerzo por parte de las instituciones públicas y entidades privadas en mejorar la protección y conocimientos en la ciudadanía. Se están poniendo en marcha campañas y estrategias para poder empoderar a la población en estas capacidades, así que es de especial transcendencia poder conocer cuáles son las mejores técnicas y qué efectos tienen. Por esta razón, los resultados hallados en este estudio deberían ser tenidos en cuenta a la hora de diseñar los planes educativos en la materia. Para futuras

investigaciones, sería interesante profundizar en cuáles han sido los puntos fuertes y débiles de cada una de esas técnicas. También sería enriquecedor el poder ampliar la información de efectos y resultados en algunas técnicas de las que apenas se han realizado estudios, como sería el caso de uso de cómics, talleres colaborativos, lectura de consejos y relatos, etc.

.

6. Referencias

Al-Daeef, M.M., Basir, N., & Saudi, M.M. (2017). Security awareness training: A review. Lecture Notes in Engineering and Computer Science, 2229, 446–451

Al-Hamar, Y., & Kolivand, H. (2020). A New Email Phishing Training Website. *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, *2020-December*, 263-268. https://doi.org/10.1109/DeSE51703.2020.9450238 *

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In Lee, MJW and Nikolic, S and Shen, J and Lei, LCU and Wong, GKW and Venkatarayalu, N (Ed.), PROCEEDINGS OF 2018 IEEE INTERNATIONAL CONFERENCE ON TALE, (pp. 62–68).

Alencar, G. D., de Lima, M. F., & Firmo, A. C. A. (2013). BEHAVIORAL ANALYSIS AS A MEANS TO PREVENT SOCIAL ENGINEERING AND PHISHING. *RESI Revista Electronica de Sistemas de Informacao*, *12*(3), 1. Advanced Technologies & Aerospace Collection. *

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information (Switzerland)*, *11*(2). https://doi.org/10.3390/info11020121 *

Althobaiti, K., Vaniea, K., & Zheng, S. (2018). Faheem: Explaining URLs to people using a Slack bot. *Proceedings of AISB Annual Convention 2018*, 1-8. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051426851&partnerID=40&md5=c56d6bb6162bb263e3b69498131e3c8a *

Alwanain, M., I. (2020). Phishing Awareness and Elderly Users in Social Media. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, *20*(9), 114-119. https://doi.org/10.22937/IJCSNS.2020.20.09.14 *

Alwanain, M., I. (2021). How Do Children Interact with Phishing Attacks? *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, *21*(3), 127-133. https://doi.org/10.22937/IJCSNS.2021.21.3.17 *

Amo, L. C., Liao, R., Frank, E., Rao, H. R., & Upadhyaya, S. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on*

Education, *62*(2), 134-140. Social Science Premium Collection. https://doi.org/10.1109/TE.2018.2877182 *

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PLOS ONE*, *14*(12). https://doi.org/10.1371/journal.pone.0224216 *

Baslyman, M., & Chiasson, S. (2016). «smells Phishy?»: An educational game about online phishing scams. *eCrime Researchers Summit, eCrime*, *2016-June*, 91-101. https://doi.org/10.1109/ECRIME.2016.7487946 *

Beckers, K., Pape, S., & Fries, V. (2016). HATCH: Hack and trick capricious humans – A serious game on social engineering. *Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016*, *2016-July*. https://doi.org/10.14236/ewic/hci2016.94 *

Bosch-Capblanch X., Lavis, J.N., Lewin, S., Atun, R., Røttingen, J.A., Dröschel D., Beck, L., Abalos, E., El-Jardali, F., Gilson, L., Oliver, S., Wyss, K., Tugwell, P., Kulier, R., Pang, T., & Haines, A. (2012). Guidance for evidence-informed policies about health systems: rationale for and challenges of guidance development. PLoS Med, 9(3), e1001185. https://doi.org/10.1371/journal.pmed.1001185

Burris, J., Deneke, W., & Maulding, B. (2018). Activity simulation for experiential learning in cybersecurity workforce development. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10923 LNCS*, 17-25. https://doi.org/10.1007/978-3-319-91716-0_2 *

Chadee, D., & Ng Ying, N.K. (2013). Predictors of fear of crime: general fear verses perceived risk. *Journal of Applied Psychology*, 43(1), 1896-1904.

Chattopadhyay, A., Christian, D., Oeder, A., & Budul, I. (2019). A Novel Visual-Privacy Themed Experiential- Learning Tool for Human-Privacy Societal-Security Awareness in Middle-School and High-School Youth. *Proceedings - Frontiers in Education Conference, FIE*, *2019-October*. https://doi.org/10.1109/FIE43999.2019.9028375 *

Chen, T., Stewart, M., Bai, Z., Chen, E., Dabbish, L., & Hammer, J. (2020). Hacked time: Design and evaluation of a self-efficacy based cybersecurity game. *DIS 2020 - Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 1737-1749. https://doi.org/10.1145/3357236.3395522 *

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. International Journal of Cyber Criminology 2 (1): 308–333. Recuperado de: https://www.researchgate.net/publication/238621672_Computer_Crime_Victimization_and_Integrated_Theory_An_Empirical_Assessment

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation and Gaming, 51(5), 586–611. https://doi.org/10.1177/1046878120933312

Cornel, C., Cornel, C. M., Rowe, D. C., & Moses, S. (2016). A cybersecurity camp for girls. *ASEE Annual Conference and Exposition, Conference Proceedings*, *2016-June*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84983347749&partnerID=40&md5=bd701a49eabb23972b48d3b95806f211 *

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human risk factors in cybersecurity. *SIGITE 2019 - Proceedings of the 20th Annual Conference on Information Technology Education*, 87-92. https://doi.org/10.1145/3349266.3351407 *

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739-1747. APA PsycInfo®. https://doi.org/10.1016/j.chb.2010.06.023

De Bona, M., & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3407023.3409179 *

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining gamification. 15th international academic MindTrek conference: Envisioning future media environments. pp. 9-15.

Decusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D., & Mah, B. (2022). A Cybersecurity Awareness Escape Room using Gamification Design Principles. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, 765-770. https://doi.org/10.1109/CCWC54503.2022.9720748 *

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical benefits of training to phishing susceptibility. *IFIP Advances in Information and Communication Technology*, *376 AICT*, 457-464. https://doi.org/10.1007/978-3-642-30436-1_37 *

Ganesh, A., Ndulue, C., & Orji, R. (2022). Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13213 LNCS*, 89-100. https://doi.org/10.1007/978-3-030-98438-0_7 *

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). CyberAware: A mobile game-based app for cybersecurity education and awareness. *Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL 2015*, 54-58. https://doi.org/10.1109/IMCTL.2015.7359553 *

Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security education and awareness for K-6 going mobile. *International Journal of Interactive Mobile Technologies*, *10*(2), 41-48. https://doi.org/10.3991/ijim.v10i2.5473 *

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal*, *28*(3), 81-106. https://doi.org/10.1080/19393555.2019.1657527 *

Gokul, C. J., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). Phishy—A serious game to train enterprise users on phishing awareness. *CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 169-181. https://doi.org/10.1145/3270316.3273042 *

González, J., Buñuel, J.C., & González, P. (2012). Listas guía de comprobación de estudios observacionales: declaración STROBE. Evid Pediatr. 8:65

Grant, M.J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health Information and Libraries Journal, 26(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Hadlington, L., & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. Policing: A Journal of Policy and Practice, April, 1-14.

Herzberg, A., & Margulies, R. (2011). Forcing Johnny to login safely: Long-term user study of forcing and training login mechanisms. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture*

Notes in Bioinformatics), *6879 LNCS*, 452-471. https://doi.org/10.1007/978-3-642-23822-2_25 *

Hutton, B., Catalá-López, F., & Moher, D. (2016). La extensión de la declaración PRISMA para revisiones sistemáticas que incorporan metaanálisis en red: PRISMA-NMA. *Medicina Clinica*, *147*(6), 262–266. https://doi.org/10.1016/j.medcli.2016.02.025

Huynh, D., Luong, P., Iida, H., & Beuran, R. (2017). Design and evaluation of a cybersecurity awareness training game. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10507 LNCS*, 183-188. https://doi.org/10.1007/978-3-319-66715-7_19 *

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. In *Human-centric Computing and Information Sciences* (Vol. 10, Issue 1). Springer Berlin Heidelberg. https://doi.org/10.1186/s13673-020-00237-7

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game based cybersecurity training for High School Students. *SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, *2018-January*, 68-73. https://doi.org/10.1145/3159450.3159591 *

Kaabi, L. A., Ketbi, W. A., Khoori, A. A., Shamsi, M. A., & Alrabaee, S. (2022). Safe: Cryptographic Algorithms and Security Principles Gamification. *IEEE Global Engineering Education Conference, EDUCON*, *2022-March*, 1169-1178. https://doi.org/10.1109/EDUCON52537.2022.9766526

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26.

Kolb, C., Strouse, J., Palmer, J., Ford, V., & Turygina, V. (2022). Cyber Securing the Future. *AIP Conference Proceedings*, *2425*. https://doi.org/10.1063/5.0081419

Kovačević, A., & Radenković, S. D. (2020). SAWIT—Security Awareness Improvement Tool in the Workplace. *Applied Sciences*, *10*(9), 3065. Advanced Technologies & Aerospace Collection; Earth, Atmospheric & Aquatic Science Collection; ProQuest One Academic; Publicly Available Content Database. https://doi.org/10.3390/app10093065

Kunz, A., Volkamer, M., Stockhardt, S., Palberg, S., Lottermann, T., & Piegert, E. (2016). NoPhish: Evaluation of a web application that teaches people being aware of

phishing attacks. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, *P-259*, 509-518. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020702971&partnerID=40&md5=4e91989eb224aacf8f160041c1eb053e

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *Conference on Human Factors in Computing Systems - Proceedings*, 905-914. https://doi.org/10.1145/1240624.1240760 *

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *ACM International Conference Proceeding Series*, *269*, 70-81. https://doi.org/10.1145/1299015.1299022 *

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. *eCrime Researchers Summit, eCrime 2008*. https://doi.org/10.1109/ECRIME.2008.4696970 *

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security*. https://doi.org/10.1145/1572532.1572536 *

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2019). How effective is anti-phishing training for children? *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017*, 229-239. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075917140&partnerID=40&md5=c509892b8cff514dd540a70a3f0bffd2 *

Levy, Y., & Ellis, T.J. (2006), “A systems approach to conduct an effective literature review in support of information systems research”, Informing Science Journal, Vol. 9 No. 1, pp. 181-212

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gotzsche, P. C., Ioannidis, J. P. A., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: Explanation and elaboration. *British Medical Journal*, *339*, b2700. doi: https://doi.org/10.1136/bmj.b2700

Lim, I., Park, Y.-G., & Lee, J.-K. (2016). Design of Security Training System for Individual Users. *Wireless Personal Communications*, *90*(3), 1105-1120. Advanced

Technologies & Aerospace Collection. https://doi.org/10.1007/s11277-016-3380-z *

Maqsood, S., & Chiasson, S. (2021). Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security*, *24*(4). https://doi.org/10.1145/3469821 *

Mikka-Muntuumo, J., & Peters, A. N. (2021). Designing an Interactive Game for Preventing Online Abuse in Namibia. *2021 3rd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2021*. https://doi.org/10.1109/IMITEC52926.2021.9714592 *

Moreno-Fernández, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior*, *69*, 421. Advanced Technologies & Aerospace Collection.*

Mugayitoglu, B., Borowczak, M., Burrows, A., Carson, A., Person, C., Finch, A., & Kennedy, C. (2021). A university's developmental framework: Creating, implementing, and evaluating a K-12 teacher cybersecurity micro-credential course. *ICSIT 2021 - 12th International Conference on Society and Information Technologies, Proceedings*, 35-40. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105867054&partnerID=40&md5=4d3140888267c6189eb1d76ae1c896ad *

Neo, H.-F., Teo, C.-C., & Peng, C. L. (2021). Safe Internet: An Edutainment Tool for Teenagers. *Lecture Notes in Electrical Engineering*, *739 LNEE*, 53-70. https://doi.org/10.1007/978-981-33-6385-4_6 *

Newbould, M., & Furnell, S. (2009). Playing safe: A prototype game for raising awareness of social engineering. *Proceedings of the 7th Australian Information Security Management Conference*, 24-30. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84864552106&partnerID=40&md5=c35c02b54b3c5929bc9cdb6fffd4c843 *

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J., Sohn, I., & Thomas, D. (2014). SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, 3GSE 2014*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85040226944&partnerID=40&md5=78b3676884e4e3fb2e7c4ecbfe3d4725 *

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2022). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. Observaciber. Recuperado de https://www.observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

Peker, Y. K., Ray, L., da Silva, S., & IEEE. (2018). *Online Cybersecurity Awareness Modules for College and High School Students* (WOS:000463185700004). 24-33. https://doi.org/10.1109/NCS.2018.00009 *

Perestelo-Pérez, L. (2013). Standards on how to develop and report systematic reviews in Psychology and Health. International Journal of Clinical and Health Psychology, 13, 49–57.

Pittman, J. M., & Pike, R. E. (2016). An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp. *Information Systems Education Journal*, *14*(3), 4-13. ERIC. *

Plachkinova, M., & Menard, P. (2019). An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09970-6 *

Quinkert, F., Degeling, M., & Holz, T. (2021). Spotlight on Phishing: A Longitudinal Study on Phishing Awareness Trainings. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12756 LNCS*, 341-360. https://doi.org/10.1007/978-3-030-80825-9_17 *

Qusa, H., & Tarazi, J. (2021). Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 677-682. https://doi.org/10.1109/CCWC51732.2021.9375847 *

Rastenis, J., Ramanauskaitė, S., Janulevičius, J., & Čenys, A. (2020). Impact of information security training on recognition of phishing attacks: A case study of vilnius gediminas technical university. *Communications in Computer and Information Science*, *1243 CCIS*, 311-324. https://doi.org/10.1007/978-3-030-57672-1_23 *

Reid, R., & Van Niekerk, J. (2014). Snakes and ladders for digital natives: Information security education for the youth. *Information Management & Computer Security*, *22*(2), 179-190. Advanced Technologies & Aerospace Collection; ProQuest One

Academic; ProQuest One Business; Social Science Premium Collection. https://doi.org/10.1108/IMCS-09-2013-0063 *

Reid, R., & Van Niekerk, J. (2015). A cyber security culture fostering campaign through the lens of active audience theory. *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, 34-44. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85026347994&partnerID=40&md5=90f8bac7ab485818b4265a118ea60ba0 *

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020*, 259-284. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091852889&partnerID=40&md5=6643e561a062c251360023104af547b7 *

Saito, T., Yashiro, S., Tanabe, K., & Saito, Y. (2019). A Proposal and the Evaluation of a Hands-On Training System for Cyber Security. En Barolli, L and Leu, FY and Enokido, T and Chen, HC (Ed.), *ADVANCES ON BROADBAND AND WIRELESS COMPUTING, COMMUNICATION AND APPLICATIONS, BWCCA-2018* (Vol. 25, pp. 339-349). https://doi.org/10.1007/978-3-030-02613-4_30 *

Salazar, M., Gaviria, J., Laorden, C., & Bringas, P. G. (2013). Enhancing cybersecurity learning through an augmented reality-based serious game. *IEEE Global Engineering Education Conference, EDUCON*, 602-607. https://doi.org/10.1109/EduCon.2013.6530167 *

Schoebel, S., Roepke, R., & Schroeder, U. (2021). Phishing Academy: Evaluation of a Digital Educational Game on URLs and Phishing. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13134 LNCS*, 44-53. https://doi.org/10.1007/978-3-030-92182-8_5 *

Scholefield, S., & Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11594 LNCS*, 191-203. https://doi.org/10.1007/978-3-030-22351-9_13 *

Sercombe, A. A., & Papadaki, M. (2012). Education in the «virtual» community: Can beating Malware Man teach users about social networking security? *Proceedings of the 6th International Symposium on Human Aspects of Information Security*

and Assurance, HAISA 2012, 33-39. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84926306106&partnerID=40&md5=f1644a3a54a362b2832d3bbb04d16e84 *

Septiana, R., & Julian, R. K. (2020). Design of Phishing Simulation Dashboard Using Analytic Data Concepts. *Journal of Physics: Conference Series*, *1577*(1). Advanced Technologies & Aerospace Collection; ProQuest One Academic; Publicly Available Content Database. https://doi.org/10.1088/1742-6596/1577/1/012041 *

Shen, L. W., Mammi, H. K., & Din, M. M. (2021). Cyber Security Awareness Game (CSAG) for Secondary School Students. *2021 International Conference on Data Science and Its Applications, ICoDSA 2021*, 48-53. https://doi.org/10.1109/ICoDSA53588.2021.9617548 *

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *ACM International Conference Proceeding Series*, *229*, 88-99. https://doi.org/10.1145/1280680.1280692 *

Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance: JMIS. *Journal of Management Information Systems*, *37*(1), 129-161. Advanced Technologies & Aerospace Collection; ProQuest One Academic; ProQuest One Business; Social Science Premium Collection. https://doi.org/10.1080/07421222.2019.1705512 *

Sookhanaphibarn, K., & Choensawat, W. (2020). Educational games for cybersecurity awareness. *2020 IEEE 9th Global Conference on Consumer Electronics, GCCE 2020*, 424-428. https://doi.org/10.1109/GCCE50665.2020.9291723 *

Streiff, J., Justice, C., & Camp, J. (2019). Escaping to cybersecurity education: Using manipulative challenges to engage and educate. *Proceedings of the European Conference on Games-based Learning*, *2019-October*, 1046-1050. https://doi.org/10.34190/GBL.19.183 *

Sucharew, H., & Macaluso, M. (2019). Methods for Research Evidence Synthesis: The Scoping Review Approach. Journal of Hospital Medicine 14, 416-418. https://doi.org/10.12788/jhm.3248

Sun, J. C.-Y., & Chen, A. Y.-Z. (2016). Effects of integrating dynamic concept maps with Interactive Response System on elementary school students' motivation and

learning outcome: The case of anti-phishing education. *COMPUTERS & EDUCATION*, *102*, 117-127. https://doi.org/10.1016/j.compedu.2016.08.002 *

Svabensky, V., Vykopal, J., & Celeda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. *SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2–8. https://doi.org/10.1145/3328778.3366816

Thackray, H., McAlaney, J., Dogan, H., Taylor, J., & Richardson, C. (2016). Social psychology: An under-used tool in cybersecurity. Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016, 2016-July. https://doi.org/10.14236/ewic/HCI2016.64

Tricco, A.C., Antony, J., Zarin, W., Strifler, L., Ghassemi, M., Ivory, J., Perrier, L., Hutton, B., Moher, D., & Straus, S.E. (2015). A scoping review of rapid review methods. BMC Medicine, 13(224). https://bit.ly/2ZT1PUN

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), 1. MEDLINE®. https://doi.org/10.1016/j.heliyon.2019.e02010

Tsokkis, P., & Stavrou, E. (2018). A password generator tool to increase users' awareness on bad password construction strategies. *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018*. https://doi.org/10.1109/ISNCC.2018.8531061 *

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3399715.3399860 *

Villasís-Keever, M.A., Rendón-Macías, M.E., García, H., Miranda-Novales., M.G., & Escamilla-Núñez, A. (2020). La revisión sistemática y el metaanálisis como herramienta de apoyo para la clínica y la investigación. Rev Alerg Mex.; 67(1):62-72.

Visoottiviseth, V., Sainont, R., Boonnak, T., & Thammakulkrajang, V. (2018). POMEGA: Security game for building security awareness. *Proceeding of 2018 7th ICT International Student Project Conference, ICT-ISPC 2018*. https://doi.org/10.1109/ICT-ISPC.2018.8523965 *

Volkamer, M., Renaud, K., Reinheimer, B., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A., & Gerber, N. (2018). Developing and evaluating a five minute phishing awareness video. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11033 LNCS*, 119-134. https://doi.org/10.1007/978-3-319-98385-1_9

Wang, Y.-J., Tseng, S.-S., Yang, T.-Y., & Weng, J.-F. (2018). Building a frame-based cyber security learning game. *Communications in Computer and Information Science*, *797*, 32-41. https://doi.org/10.1007/978-981-10-7850-7_4 *

Wash, R., & Cooper, M. M. (2018). Who provides phishing training? Facts, stories, and people like me. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3173574.3174066 *

Weaver, B. W., Braly, A. M., & Lane, D. M. (2021). Training Users to Identify Phishing Emails. *Journal of Educational Computing Research*, *59*(6), 1169-1183. https://doi.org/10.1177/0735633121992516 *

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300338 *

Wolf, S., Burrows, A. C., Borowczak, M., Johnson, M., Cooley, R., & Mogenson, K. (2020). Integrated outreach: Increasing engagement in computer science and cybersecurity. *Education Sciences*, *10*(12), 1-23. https://doi.org/10.3390/educsci10120353 *

Wolf, S., Cooley, R., Johnson, M., Burrows, A. C., & Borowczak, M. (2020). Constructing and refining engaging computer science outreach. *ASEE Annual Conference and Exposition, Conference Proceedings*, *2020-June*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85095780473&partnerID=40&md5=05052e69cca875c069c9f7b96122cb68 *

Yett, B., Hutchins, N., Stein, G., Zare, H., Snyder, C., Biswas, G., Metelko, M., & Ledeczi, A. (2020). A hands-on cybersecurity curriculum using a robotics platform. SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education, 1040-1046. https://doi.org/10.1145/3328778.3366878 *

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal*

of Human-Computer Interaction, *32*(3), 215-257. APA PsycInfo®. https://doi.org/10.1080/10447318.2016.1136177 *

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. ACM Computing Surveys, 54(1), 1–39. https://doi.org/10.1145/3427920 *

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. *Proceedings of the Human Factors and Ergonomics Society*, *2014-January*, 1466-1470. https://doi.org/10.1177/1541931214581306

7. ANEXO

Tabla de codificación con cita completa.

	TITULO	PRIMER AUTOR Y AÑO	REVISTA	PAÍS
1	A comprehensive cybersecurity learning platform for elementary education	Giannakas, F. 2019	Information Security Journal	GRECIA
2	A cyber security culture fostering campaign through the lens of active audience theory	Reid, R. 2015	Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance	GRECIA
3	A Cybersecurity Awareness Escape Room using Gamification Design Principles	Decusatis, C. 2022	2022 IEEE 12th Annual Computing and Communication Workshop and Conference	ESTADOS UNIDOS
4	A cybersecurity camp for girls	Cornel, C. 2016	ASEE Annual Conference and Exposition	ESTADOS UNIDOS
5	A hands-on cybersecurity curriculum using a robotics platform	Yett, B. 2020	SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education	ESTADOS UNIDOS
6	A New Email Phishing Training Website	Al-Hamar, Y. 2020	Proceedings - International Conference on Developments in eSystems Engineering	REINO UNIDO
7	A Novel Visual-Privacy Themed Experiential- Learning Tool for Human-Privacy Societal-Security Awareness in Middle-School and High-School Youth	Chattopadhyay, A. 2019	Proceedings - Frontiers in Education Conference	ESTADOS UNIDOS
8	A password generator tool to increase users' awareness on bad password construction strategies	Tsokkis, P. 2018	2018 International Symposium on Networks	CHIPRE
9	A Proposal and the Evaluation of a Hands-On Training System for Cyber Security	Saito, T. 2019	ADVANCES ON BROADBAND AND WIRELESS COMPUTING	JAPON
10	A real world study on employees' susceptibility to phishing attacks	De Bona, M. 2020	ACM International Conference Proceeding Series	ESTADOS UNIDOS
11	"A University's Developmental Framework: Creating, Implementing, and			
12	Evaluating a K-12 Teacher Cybersecurity Micro-credential Course"	Mugayitoglu, B. 2021	implementing	ESTADOS UNIDOS
13	Activity simulation for experiential learning in cybersecurity workforce development	Burris, J. 2018	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ESTADOS UNIDOS
14	An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs	Plachkinova, M. 2019	Information Systems Frontiers	PAISES BAJOS
15	An investigation of phishing awareness and education over time: When and how to best remind users	Reinheimer, B. 2020	Proceedings of the 16th Symposium on Usable Privacy and Security	AUSTRALIA
16	An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp	Pittman, J.M. 2016	Information Systems Education Journal	ESTADOS UNIDOS
17	Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish	Sheng, S. 2007	ACM International Conference Proceeding Series	ESTADOS UNIDOS
18	BEHAVIORAL ANALYSIS AS A MEANS TO PREVENT SOCIAL ENGINEERING AND PHISHING	Alencar, G.D. 2013	RESI Revista Electronica de Sistemas de Informacao	BRASIL
19	Building a frame-based cyber security learning game	Wang, Y.-J. 2018	Communications in Computer and Information Science	ALEMANIA
20	Constructing and refining engaging computer science outreach	Wolf, S. 2020	ASEE Annual Conference and Exposition	ESTADOS UNIDOS
21	Cyber Securing the Future	Kolb, C. 2022	AIP Conference Proceedings	ESTADOS UNIDOS
22	Cyber Security Awareness Game (CSAG) for Secondary School Students	Shen, L.W. 2021	2021 International Conference on Data Science and Its Applications	ESTADOS UNIDOS

23	CyberAware: A mobile game-based app for cybersecurity education and awareness	Giannakas, F. 2015	Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning	ESTADOS UNIDOS
24	Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students	Qusa, H. 2021	2021 IEEE 11th Annual Computing and Communication Workshop and Conference	ESTADOS UNIDOS
25	Cybersecurity Interventions for Teens: Two Time-Based Approaches	Amo, Laura C. 2019	IEEE Transactions on Education	ESTADOS UNIDOS
26	CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues	Veneruso, S.V. 2020	ACM International Conference Proceeding Series	ESTADOS UNIDOS
27	Design and evaluation of a cybersecurity awareness training game	Huynh, D. 2017	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
28	Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)	Alqahtani, H. 2020	Information (Switzerland)	SUIZA
29	Design of Phishing Simulation Dashboard Using Analytic Data Concepts	Septiana, R. 2020	Journal of Physics: Conference Series	REINO UNIDO
30	Design of Security Training System for Individual Users	Lim, I. 2016	Wireless Personal Communications	PAISES BAJOS
31	Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens	Maqsood, S. 2021	ACM Transactions on Privacy and Security	ESTADOS UNIDOS
32	Designing an Interactive Game for Preventing Online Abuse in Namibia	Mikka-Muntuumo, J. 2021	2021 3rd International Multidisciplinary Information Technology and Engineering Conference	ESTADOS UNIDOS
33	Developing and evaluating a five minute phishing awareness video	Volkamer, M. 2018	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ESTADOS UNIDOS
34	Education in the 'virtual' community: Can beating Malware Man teach users about social networking security?	Sercombe, A.A. 2012	Proceedings of the 6th International Symposium on Human Aspects of Information Security and Assurance	ESTADOS UNIDOS
35	Educational games for cybersecurity awareness	Sookhanaphibarn, K. 2020	2020 IEEE 9th Global Conference on Consumer Electronics	ESTADOS UNIDOS
36	Effectiveness of and user preferences for security awareness training methodologies.	Tschakert, K.F. 2019	Heliyon	PAISES BAJOS
37	Effects of integrating dynamic concept maps with Interactive Response System on elementary school students' motivation and learning outcome: The case of anti-phishing education	Sun, J.C. 2016	COMPUTERS & EDUCATION	REINO UNIDO
38	Empirical benefits of training to phishing susceptibility	Dodge, R. 2012	IFIP Advances in Information and Communication Technology	ESTADOS UNIDOS
39	Enhancing cybersecurity learning through an augmented reality-based serious game	Salazar, M. 2013	IEEE Global Engineering Education Conference	ESTADOS UNIDOS
40	Escaping to cybersecurity education: Using manipulative challenges to engage and educate	Streiff, J. 2019	Proceedings of the European Conference on Games-based Learning	ALEMANIA
41	Faheem: Explaining URLs to people using a Slack bot	Althobaiti, K. 2018	Proceedings of AISB Annual Convention 2018	REINO UNIDO
42	Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud	Moreno-Fernández, M. 2017	Computers in Human Behavior	REINO UNIDO
43	Forcing Johnny to login safely: Long-term user study of forcing and training login mechanisms	Herzberg, A. 2011	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
44	Game based cybersecurity training for High School Students	Jin, G. 2018	SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education	ESTADOS UNIDOS
45	Gamification Techniques for Raising Cyber Security Awareness	Scholefield, S. 2019	Lecture Notes in Computer Science	ALEMANIA
46	Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer	Kumaraguru, P. 2007	ACM International Conference Proceeding Series	ESTADOS UNIDOS
47	Hacked time: Design and evaluation of a self-efficacy based cybersecurity game	Chen, T. 2020	DIS 2020 - Proceedings of the 2020 ACM Designing Interactive Systems Conference	PAISES BAJOS

48	HATCH: Hack and trick capricious humans – A serious game on social engineering	Beckers, K. 2016	Proceedings of the 30th International BCS Human Computer Interaction Conference	ESTADOS UNIDOS
49	How Do Children Interact with Phishing Attacks?	Alwanain, M. 2021	INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY	CHINA
50	How effective is anti-phishing training for children?	Lastdrager, E. 2019	Proceedings of the 13th Symposium on Usable Privacy and Security	ESTADOS UNIDOS
51	Human risk factors in cybersecurity	Cuchta, T. 2019	SIGITE 2019 - Proceedings of the 20th Annual Conference on Information Technology Education	ESTADOS UNIDOS
52	Impact of information security training on recognition of phishing attacks: A case study of vilnius gediminas technical university	Rastenis, J. 2020	Communications in Computer and Information Science	ALEMANIA
53	Informing, simulating experience, or both A field experiment on phishing risks	Baillon, A. 2019	PLoS ONE	ESTADOS UNIDOS
54	Integrated outreach: Increasing engagement in computer science and cybersecurity	Wolf, S. 2020	Education Sciences	SUIZA
55	It won't happen to me: Promoting secure behaviour among internet users	Davinson, N. 2010	Computers in Human Behavior	REINO UNIDO
56	Lessons from a real world evaluation of anti-phishing training	Kumaraguru, P. 2008	eCrime Researchers Summit	ESTADOS UNIDOS
57	NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks	Kunz, A. 2016	Lecture Notes in Informatics (LNI)	ALEMANIA
58	One phish, two phish, how to avoid the internet phish Analysis of training strategies to detect phishing emails	Zielinska, O.A. 2014	Proceedings of the human factors and ergonomics Society	ESTADOS UNIDOS
59	Online Cybersecurity Awareness Modules for College and High School Students	Peker, Y.K. 2018	2018 national cyber summit research track	ESTADOS UNIDOS
60	Phishing Academy: Evaluation of a Digital Educational Game on URLs and Phishing	Schoebel, S. 2021	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
61	Phishing Awareness and Elderly Users in Social Media	Alwanain, M. 2020	INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY	CHINA
62	Phishy - A serious game to train enterprise users on phishing awareness	Gokul, C.J. 2018	CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts	ESTADOS UNIDOS
63	Playing safe: A prototype game for raising awareness of social engineering	Newbould, M. 2009	Proceedings of the 7th Australian Information Security Management Conference	AUSTRALIA
64	POMEGA: Security game for building security awareness	Visoottiviseth, V. 2018	Proceeding of 2018 7th ICT International Student Project Conference	ESTADOS UNIDOS
65	Protecting people from phishing: The design and evaluation of an embedded training email system	Kumaraguru, P. 2007	Conference on Human Factors in Computing Systems - Proceedings	ESTADOS UNIDOS
66	Safe Internet: An Edutainment Tool for Teenagers	Neo, H.F. 2021	Lecture Notes in Electrical Engineering	ALEMANIA
67	Safe: Cryptographic Algorithms and Security Principles Gamification	Kaabi, L.A. 2022	IEEE Global Engineering Education Conference	ESTADOS UNIDOS
68	SAWIT—Security Awareness Improvement Tool in the Workplace	Kovačević, A. 2020	Applied Sciences	SUIZA
69	School of phish: A real-world evaluation of anti-phishing training	Kumaraguru, P. 2009	SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security	ESTADOS UNIDOS
70	Security education and awareness for K-6 going mobile	Giannakas, F. 2016	International Journal of Interactive Mobile Technologies	ESTADOS UNIDOS
70	SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education	Olano, M. 2014	2014 USENIX Summit on Gaming	ESTADOS UNIDOS
72	Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory	Ganesh, A. 2022	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
73	Smells Phishy?: An educational game about online phishing scams	Baslyman, M. 2016	eCrime Researchers Summit	ESTADOS UNIDOS

74	Snakes and ladders for digital natives: information security education for the youth	Reid, R. 2014	Information Management & Computer Security	REINO UNIDO
75	Spotlight on Phishing: A Longitudinal Study on Phishing Awareness Trainings	Quinkert, F. 2021	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
76	The role of instructional design in persuasion: A comics approach for improving cybersecurity	Zhang-Kennedy, L. 2016	International Journal of Human-Computer Interaction	ESTADOS UNIDOS
77	Training Users to Identify Phishing Emails	Weaver, B.W. 2021	Journal of Educational Computing Research	ESTADOS UNIDOS
78	Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance: JMIS	Silic, M. 2020	Journal of Management Information Systems	ESTADOS UNIDOS
79	What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game	Wen, Z.A. 2019	Conference on Human Factors in Computing Systems - Proceedings	ESTADOS UNIDOS

Tabla de clasificación de artículos y efectos conseguidos

	TÉCNICA	EFECTOS	TIPO EDUCACIÓN	POBLACIÓN DIANA/ INTERVALO DE EDAD	ÁREA DE ESTUDIO DE LOS AUTORES
1	GAMIFICACIÓN	2 (81% mejora)	CIBERSEGURIDAD	Niños (Estudiantes de Primaria 9-12)	TIC (Ingeniería de Sistemas)
2	MEDIOS AUDIOVISUALES	2	CIBERSEGURIDAD	Niños	TIC
3	GAMIFICACIÓN / SCAPE ROOM	1	CIBERSEGURIDAD	Jóvenes (Estudiantes preunivesitarios y Universitarios)	TIC
4	CAMPAMENTO DE CIBERSEGURIDAD	1 (44% mejora)	CIBERSEGURIDAD	Niños; Adolescentes (10-14)	TIC
5	PLATAFORMA ROBOTICA	1 (33% mejora)	CIBERSEGURIDAD	Adolescentes (Estudiantes de secundaria)	TIC (Ingeniería de Ciencias Computacionales)
6	MATERIALES AUDIOVISUALES	1 (98% mejora)	CIBERSEGURIDAD	Adultos (Empleados de organizaciones)	TIC (Ciencias Computacionales)
7	MATERIALES AUDIOVISUALES / PRÁCTICAS CON HERRAMIENTA WEB	1	CIBERSEGURIDAD	Niños; Adolescentes. (12- 18)	TIC (Ciencias de la Información y Computación)
8	SIMULADOR	1 (80%)	CIBERSEGURIDAD	Adultos (23-55)	TIC (Ciencias Computacionales)
9	EJERCICIOS PRÁCTICOS DE ENTRENAMIENTO (HERRAMIENTA VIRTUAL)	1 (49%)	CIBERSEGURIDAD	Adolescentes; Estudiantes de Secundaria (12-16)	TIC (Ciencias Computacionales)
10	SIMULACIÓN	5 (1%)	CIBERSEGURIDAD	Adultos; Empleados de organizaciones	TIC (Ciencias Computacionales)
11	MULTIMÉTODO: Sistema de gestión de aprendizaje (LMS): Materiales audiovisuales; Elearning	1	CIBERSEGURIDAD	Adultos (Profesores de Primaria)	Educación ; TIC (Ciencias Computacionales)
12	SIMULACIÓN	2: 54% Simulación frente a 30% Grupo Control (educación tradicional)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos	TIC (Ciencias Computacionales)
13	MATERIALES AUDIOVISUALES	1	CIBERSEGURIDAD	Adultos	TIC (Informática y Gestión de Tecnologías)

14	Multimétodo: material de texto 1,61; material audiovisual 1,8; Herramienta interactiva 1,73;	1	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adultos	TIC (Informática Aplicada)
15	CAMPAMENTO DE CIBERSEGURIDAD / APRENDIZAJE ENTRE PARES	1	CIBERSEGURIDAD	Adolescentes; Alumnos de Secundaria	TIC
16	GAMIFICACIÓN	2: 18% mejora pre-post test; Tasa de error del 0,34 a 0,17 sobre 5;	CIBERSEGURIDAD	Jóvenes (18-34)	TIC
17	Multimétodo: Clase expositiva; material audiovisual	2: Phishing en grupo experimental 108 frente a 174 grupo control	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos (Trabajadores de empresa)	TIC (Ciencias Computacionales)
18	Juego de Cartas	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños	TIC (Ciencias Computacionales e Ingeniería de la información ; Informática Aplicada y Multimedia)
19	Mixto: Clase expositiva; tallers grupales; laboratorio.	1	CIBERSEGURIDAD	Niños; Adolescentes (12-16)	TIC (Ciencias Computacionales) ; Ciencias de la Educación
20	Clases prácticas	6 Clases prácticas 30% a 87%; Grupo control (solo lectura) 30% a 91%	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adolescentes	TIC
21	GAMIFICACIÓN	1 70%	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adolescentes	TIC (Ciencias Computacionales; Ingeniería; Matemáticas)
22	GAMIFICACIÓN (Juego para el movil)	1 (15%+33% /2 =24%)	CIBERSEGURIDAD	Niños (9-11)	TIC (Ingeniería de Sistemas de Información y Comunicación)
23	GAMIFICACIÓN	5 (5%)	CIBERSEGURIDAD	Niños; Adolescentes; Jóvenes (9-22)	TIC (Ciencias Computacionales)
24	Taller de aprendizaje práctico (hands-on learning workshop)	1	CIBERSEGURIDAD	Adolescentes; Jóvenes	TIC (Gestión de Sistemas; Ingeniería Computacional)
25	GAMIFICACIÓN	2 Grupo tratamiento (Gamificación) frente a Grupo control	CIBERSEGURIDAD	Jóvenes (24-34)	TIC (Informática; Ciencias Computacionales;
26	GAMIFICACIÓN	1 (76%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes	TIC (Ciencias Computacionales)
27	GAMIFICACIÓN	1 (4/5 = 80%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos (18-65)	TIC (Ciencias Computacionales)
28	SIMULACIÓN	1 (clics en phishin 43% a 16% = mejora del 27%)	CIBERSEGURIDAD	Adultos (Empleados de organizaciones)	TIC (Ciencias Computacionales)
29	SIMULACIÓN	1 (mejora de entre un 12 y un 14%)	CIBERSEGURIDAD	Adultos	TIC (Ciencias Computacionales)
30	GAMIFICACIÓN	1 (70% - 80%)	CIBERSEGURIDAD	Niños (11 - 13 años)	TIC (Ciencias Computacionales)
31	GAMIFICACIÓN	1 (80%)	CIBERSEGURIDAD	Niños; Jóvenes; Adultos (7 a 35)	TIC (Ciencias Computacionales)
32	MEDIOS AUDIOVISUALES (VÍDEO EDUCATIVO)	1 (37%)	CIBERSEGURIDAD	Adultos (media de edad: 37 años)	TIC (Ciencias Computacionales)
33	GAMIFICACIÓN	2 (Grupo tratamiento 77% ; 55% Grupo control)	CIBERSEGURIDAD	Jóvenes; Adultos. (18-65)	TIC (Ciencias Computacionales)
34	GAMIFICACIÓN	1 (75%)	CIBERSEGURIDAD	Adolescentes; Jóvenes	TIC (Ciencias Computacionales)
35	Mixto: GAMIFICACIÓN; MATERIALES MULTIMEDIA; TEXTO	1 (8%)	CIBERSEGURIDAD	Jóvenes (18-23)	TIC (Información y Comunicación)
36	Mapas conceptuales	"2 grupo de control	CIBERSEGURIDAD	Niños; Adolescentes	Educación

37	Entrenamiento	2 (18% frente a grupo control)	CIBERSEGURIDAD	No se especifica	TIC (Ciencias Computacionales); Ciencias del comportamiento
38	GAMIFICACIÓN	1 (3,92/5 = 78%)	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adolescentes; Jóvenes (14-19)	TIC (Ingeniería Informática y Telecomunicaciones;
39	ESCAPE ROOM	1	CIBERSEGURIDAD	Niños; Adolescentes	TIC (Ciencias Computacionales)
40	ROBOT	2 (G intervención M=4.55 G.Control M=2.15)	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales; Informática)
41	Entrenamiento progresivo	1	CIBERSEGURIDAD	Jóvenes; Adultos (18-66)	Psicología; TIC (Informática)
42	Marcador de inicio de sesión +Imágenes	2 (Grupo tratamiento 82% ; G. Control 20%)	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Estudiantes	TIC (Ciencias Computacionales)
43	Campamento de ciberseguridad	1	CIBERSEGURIDAD	Adolescentes	TIC (Ciencias Computacionales; Informática; Tecnologías de Gráficos por Ordenador)
44	GAMIFICACIÓN	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adolescentes; Jóvenes	TIC (Informática)
45	FORMACIÓN INTEGRADA (Embedded training)	2 (G. intervención mejora 67% ; G. control 0%)	CIBERSEGURIDAD	Jóvenes; Adultos (media edad 25)	TIC (Ciencias Computacionales)
46	GAMIFICACIÓN	2	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales)
47	GAMIFICACIÓN	1 (50% - 100% ; Media 75%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Empleados (generales) de organizaciones	TIC (Informática) ; Económicas.
48	Entrenamiento	2 (Capacidad de identificar Phishing); 6 (concienciación)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños (7-13)	TIC (Ciencias Computacionales)
49	Entrenamiento	2 (14% frente a grupo control)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños (8-13)	TIC (Ciencias Computacionales)
50	GAMIFICACIÓN	2	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes	TIC (Ciencias Computacionales); Matemáticas
51	Entrenamiento	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos (empleados de organizaciones)	Económicas; TIC (Informática)
52	Educación tradicional (información) ; Simulación	Educación Tradicional: 6 (4 % de mejora frente a grupo control); Simulación: 2 (12% de mejora frente a grupo control)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes; Adultos	
53	CAMPAMENTO DE CIBERSEGURIDAD	1 (63%; 47%. Media 55%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños; Adolescentes (10-18)	TIC (Ciencias Computacionales); Educación
54	Entrenamiento	5	CIBERSEGURIDAD	jovenes; Adultos (18-43)	Psicología
55	Entrenamiento integrado	2 (28%)	CIBERSEGURIDAD	Empleados (generales) de organizaciones	TIC (Ciencias Computacionales)
56	GAMIFICACIÓN	1 (20%)	CIBERSEGURIDAD	Jóvenes; Adultos (18-56)	TIC (Ciencias Computacionales)
57	Entrenamiento	6	CIBERSEGURIDAD	Jóvenes; Adultos (19-67)	Psicología; Interación Humana-Computacional
58	E-Learning	1 (58%)	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adolescentes; Jóvenes; Adultos (13-63)	Psicología; Ciencias Computacionales
59	Gamificación	1 (12%)	CIBERSEGURIDAD	Niños; Adolescentes	TIC (Informática)
60	Entrenamiento	2 (50%)	CIBERSEGURIDAD	Tercera edad (65 - 75)	TIC (Ciencias Computacionales)
61	GAMIFICACIÓN	1 (29%)	CIBERSEGURIDAD	Jóvenes, Adultos	TIC (Ciencias Computacionales)
62	GAMIFICACIÓN	1	CIBERSEGURIDAD	Adolescentes; Jóvenes; Adultos	TIC (Ciencias Computacionales)

63	GAMIFICACIÓN	1	CIBERSEGURIDAD	Adolescentes; Jóvenes (15-23)	TIC (Tecnologías de la Información y Comunicación; Ingeniería Software)
64	Entrenamiento Integrado	2	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales)
65	GAMIFICACIÓN	1 (76%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Niños; Adolescentes. (11-22)	TIC (Ciencias Computacionales)
66	GAMIFICACIÓN	2 (20%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	NO CONSTA	TIC(Sistemas de Información y Seguridad)
67	Aprendizaje colaborativo (Collaborative learning)	1 (82%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Jóvenes; Adultos. (Empleados de empresas)	TIC (Ingeniería Software; Tecnologías de la Información en Finanzas)
68	GAMIFICACIÓN	2 (27% - 32%)	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales)
69	GAMIFICACION	1 (24%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Niños (9-11)	TIC (Ingeniería de Sistemas de Información y Comunicación) ; Matemáticas
70	GAMIFICACION	1	CIBERSEGURIDAD	Adolescentes; Jóvenes	TIC (Ciencias Computacionales)
70	GAMIFICACION	2 (72% grupo tratamiento; 14% G. control)	CIBERSEGURIDAD	no consta	TIC (Ciencias Computacionales)
72	GAMIFICACIÓN	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes (24-44)	TIC (Ciencias Computacionales)
73	GAMIFICACIÓN	1 (35%)	CIBERSEGURIDAD	Niños; Adolescentes (9-14)	TIC (Ciencias Computacionales)
74	SIMULACIÓN (entrenamiento)	1 (9%)	CIBERSEGURIDAD	Jóvenes; Adultos (empleados)	TIC (Ciencias Computacionales)
75	COMIC	1 (42%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Jóvenes (20-30)	TIC (Ciencias Computacionales)
76	Entrenamiento	2 (28%Grupo tratamiento; 12% g.control)	CIBERSEGURIDAD	Jóvenes (18-23)	Ciencias Sociales (Psicologia)
77	GAMIFICACIÓN	2	CIBERSEGURIDAD	Jóvenes; Adultos (empleados de organizaciones)	TIC (Tecnologías de la Información)
78	GAMIFICACIÓN; SIMULACIÓN ROLE-PLAYING	1 (37%)	CIBERSEGURIDAD	Jóvenes	TIC (Ciencias computacionales)
79	Lectura de Consejos y Relatos	2 (21% frente a grupo control)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Población general	Medios e información; Seguridad de la información

Estudio 4: Análisis de Expertos

Análisis de expertos sobre la educación en ciberseguridad dirigida a población no-técnica

Artículo publicado en Revista Electrónica de Criminología el 30/12/23
Beltrán, A. & Jiménez-Torres, M.G.(2023). Análisis de expertos sobre la educación en ciberseguridad dirigida a población no técnica. *Revista Electrónica de Criminología, 08-07*. 1-10.

RESUMEN

En este estudio se ha consultado a 10 expertos del ámbito de la educación en ciberseguridad para conocer sus opiniones y percepciones. Se les ha planteado 3 cuestiones de desarrollo y 6 de tipo likert, con un cuestionario final para calificar de validez de los expertos. Las cuestiones van referidas a la educación de la población no-técnica y la situación actual en torno a ella. Se ha encontrado consenso en torno a la falta de concienciación, conocimientos y preparación de la ciudadanía en materia de ciberseguridad y ciberdelincuencia. También la falta de más equipos interdisciplinares y personal de áreas no-técnicas a la hora de afrontar los retos de la ciberseguridad. Se ha identificado una falta de adaptación de la educación a las nuevas necesidades. También se detectó la necesidad de mejorar las campañas educativas y de actualizar de las medidas implantadas. Consecuencia de todo ello, se visibiliza la necesidad de reajustar las campañas de divulgación y la actualización constante de las estrategias educativas.

Palabras clave: Ciberseguridad; ciberdelito; educación; concienciación; interdisciplinariedad.

1. Introducción

En la última década, el impacto de la Cibercriminalidad va aumentando año tras año tal y como se demuestra con el aumento de hechos conocidos. La proporción dentro del conjunto de la criminalidad también está creciendo: se ha pasado del año 2016, de un 4,6%, al año 2020 con el 16,3%. En el mismo periodo, 2016-2020, se ha mantenido constante el aumento de los delitos informáticos, de hecho, solo en el 2020, se ha conocido un total de 287.963 hechos, lo que supone un 31,9% más con respecto al 2019 (ONTSI, 2022). Queda claro que la ciberdelincuencia es un problema en auge y, como se suele repetir en el ámbito, el factor humano es el eslabón más débil pero también el más importante. Es más necesario que nunca buscar un conocimiento amplio y

comprensión abierta sobre las distintas formas de cibedelincuencia a las que se enfrenta nuestra sociedad, especialmente aquellas nuevas y emergentes (DSN, 2019).

Estas nueva forma de delincuencia, la ciberdelincuencia, es un fenómeno complejo y global que requiere un enfoque interdisciplinar para abordar cualquier planteamiento de respuesta contra el mismo (López et al., 2021; Ghernaouti-Helie, 2009). Este punto es determinante y requiere de análisis, especialmente para responder a la pregunta de "¿Se está realmente abordando de forma interdisciplinar con presencia de ramas de las Ciencias Sociales? o por el contrario ¿Nos encontramos en un ámbito donde la mayor parte de profesionales son de áreas STEAM (Ciencia, Tecnología, Ingeniería, Artes y Matemáticas) con enfoques únicamente técnicos?". Dentro del enfoque interdisciplinar, tiene especial importancia la presencia de ciencias relacionadas con la conducta humana porque cuando hablamos de ciberdelincuencia y víctimas, hablamos de conductas. Tal y como se afirma en ONTSI (2022), "las costumbres online determinan en gran medida la exposición a los ataques". Existe un reconocimiento en la literatura de que los factores de comportamiento humano son la clave para combatir el ciberdelito (Hadlington & Chivers, 2018).

Si nos vamos a los datos de 2020 sobre hábitos y conductas de la ciudadanía, España ya se encuentra en el puesto número 7 de viviendas con acceso a internet de toda la UE (López et al., 2021). Algunas de las conductas más destacables según la ONTSI (2022) son: el acceso a contenidos digitales gratuitos desde webs no oficiales, la descarga e instalación de software, el comercio online y las transacciones no verificables. También, de las personas consultadas en dicho estudio, el 41,1% declara realizar alguna conducta de riesgo a sabiendas; un 59,7% afirma haber sufrido un incidente de seguridad en el último semestre de 2021; el 14,2% manifiesta haber sufrido el ataque de virus o malware y alrededor del 14% reconocen haberse quedado sin acceso a servicios debido a ciberataques. De lo anterior se desprende que, a nivel de conductas, existe un problema extendido en la ciudadanía, pero cuando nos vamos al por qué y, concretamente, a la preparación de la ciudadanía, nos encontramos los siguientes datos: Tan solo el 6,6% de internautas se considera totalmente preparado o preparada para afrontar los desafíos de seguridad. El 27,3% manifiesta estar bastante preparado o preparada mientras que el 37,8% declara que lo está suficientemente. El 21,3% se consideran algo preparados y el 6,8% nada preparado (ONTSI, 2022).

A consecuencia de lo anterior ha surgido una mayor conciencia sobre la necesidad de educación en ciberseguridad dirigida a la ciudadanía y población-no técnica. Junto con esta educación en ciberseguridad, y muy ligada a ella, se encuentra la educación en ciberdelincuencia. Consiste en aquella educación dirigida a dar a conocer los peligros

de la red, las ciberamenazas y las distintas formas de los ciberdelitos. Por lo tanto, educar y concienciar se hacen más necesarios que nunca y es por todo ello que las instituciones públicas han promovido la cultura de prevención de la cibercriminalidad entre la ciudadanía y empresas. El Ministerio del Interior ha elaborado y puesto en marcha un Plan Estratégico contra la Cibercriminalidad que se articula en torno a seis ejes estratégicos, entre los que están la cultura de prevención de la cibercriminalidad y la potenciación de capacidades (ANDS, 2021).

La educación se muestra una herramienta eficaz a la hora de prevenir y proporcionar herramientas a la ciudadanía, pero también implica una serie de cualidades intrínsecas. Tal y como plantea Ghernaouti-Helie (2009), los programas educativos específicos deben ser eficaces y estar disponibles para cada tipo de población objetivo, por un lado a responsables políticos, profesionales de la justicia y la policía, gestores, profesionales de las TIC, y por otra parte, a los usuarios finales (incluidos niños y ancianos). Al igual que otros autores, defienden la introducción de conocimientos relacionados con la seguridad informática en los planes de estudio de todos los niveles educativos (Árpád, I., 2013). Cabe preguntarse si las estrategias educativas están siendo adaptadas al siglo XXI, qué tipo de perfiles profesionales están implicados y cómo mejorar dichas estrategias. La finalidad de esta investigación es responder a estas cuestiones, estableciendo los siguientes objetivos de investigación:

O1 – Conocer la situación en materia de educación en ciberseguridad dirigida a la población general.
O2 – Analizar los perfiles profesionales y académicos de los agentes implicados en materia de ciberseguridad.
O3 – Analizar posibles puntos de mejora en las actuales políticas y proyectos implementados.

En cuanto a las preguntas de investigación, se han planteado las siguientes:

1. Pregunta de investigación: ¿Qué aspectos o qué puntos se podrían mejorar en la educación en ciberseguridad orientada a la población general?.
2. Pregunta de investigación: En la organización a la que pertenecen los expertos, ¿trabajan personas provenientes de titulaciones técnicas como informática, telecomunicaciones, TIC, ingenierías, etc.? ¿Y de áreas de ciencias sociales como psicología, sociología, criminología, ciencias de la educación, etc.?.
3. Pregunta de investigación: ¿Hay una representación proporcional entre perfiles de titulaciones técnicas y de las ciencias sociales en el ámbito de la educación en ciberseguridad?.

4. Pregunta de investigación: ¿Tiene la población general unos conocimientos, preparación y capacidades mínimas en ciberseguridad? ¿Y concienciación sobre la ciberdelincuencia?.
5. Pregunta de investigación: ¿Cree que los esfuerzos que se están realizando para educar a la población son proporcionales al avance del ciberdelito y sus técnicas?.
6. Pregunta de investigación: ¿La educación en ciberseguridad se está orientando demasiado hacia personal técnico y menos a la población general?.
7. Pregunta de investigación: ¿Los proyectos educativos que se están poniendo en marcha, están siendo adaptados y actualizados en las novedades educativas y las técnicas didácticas?.

Para alcanzar los objetivos, se ha realizado una consulta a expertos en la materia para que puedan transmitir su opinión de un modo sistemático y estructurado. En la sección de metodología, se describe de forma detallada el procedimiento que se ha puesto en marcha, la justificación del método, el diseño, instrumento y participantes . En resultados, se han detallado de un modo organizado y en profundidad las respuestas de forma separada. En la sección discusión, se debate la cuestión de la educación en ciberseguridad, sus retos, puntos débiles y posibilidades de mejora. Finalmente, en las conclusiones, se han detallado las ideas finales, depuradas y sintetizadas, las limitaciones y algunas propuestas para futuras investigaciones.

2. Metodología

2.1. Diseño

La metodología de juicio de expertos es una técnica que se usa con diversas finalidades "una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados, y que pueden dar información, evidencia, juicios y valoraciones" (Escobar & Cuervo, 2008). Es relevante que los jueces sean conocedores del área de conocimiento del que van a dar su opinión. Los jueces expertos son personas que emiten su juicio sobre determinada cuestión y no personal jurisdiccional. El conocimiento puede venir dado, tanto por su experiencia laboral, como por su formación académica. Por lo tanto, para la selección, se debe tener en consideración su educación, ocupación y experiencia y, una vez cerrada la lista, establecer la comunicación para poder realizar la tarea de valoración.

"*La evaluación mediante el juicio de experto consiste en solicitar a una serie de personas la demanda de un juicio hacia un objeto, un instrumento, un material de enseñanza, o su opinión respecto a un aspecto concreto*." (Cabero-Almenara & Llorente, 2013)

Entre las ventajas que presenta esta metodología, se encuentran: la calidad de las respuestas que conseguimos sobre el área de estudio en cuestión, el nivel de profundización sobre la temática, facilidad y rapidez para obtener la información, la facilidad a nivel técnico para llevar a cabo la investigación, la diversidad de medios para poder hacer la recogida de información y también la posibilidad de obtener información y datos actualizados sobre el objeto de estudio. Para la aplicación del método y poder garantizar los mejores resultados, lo hemos dividido en cuatro etapas:

1. Cálculo del número de expertos.

2. Confección de la lista de posibles candidatos y envío de los cuestionarios.

3. Selección de los expertos.

4. Recepción de las respuestas y procesamiento de los resultados.

En lo que se refiere al número de expertos finales que deben ser utilizados, cabe señalar que no hay un acuerdo unánime para su determinación, aunque en líneas generales, suelen oscilar entre 15 y 30 (Escobar-Pérez & Cuervo-Martínez, 2008) “Al escoger un número de expertos menor que nueve, el error medio grupal comienza a aumentar considerablemente. Para un número de expertos mayor de 25 el error medio grupal es prácticamente nulo, lo que significa que escoger un número de expertos mayor complica el trabajo y no mejora significativamente los resultados. De igual forma, se puede determinar que la cantidad óptima de expertos a consultar para la aplicación del método, oscila entre 15 y 25” (García & Fernández, 2008). Es un criterio avalado por la experiencia de diferentes autores en la actividad docente investigativa y por la aplicación de este método en investigaciones por más de 25 años.

Las formas de poner en acción la estrategia del juicio de experto son diversas, como las presenciales, las entrevistas o el método Delphi, donde se desarrollan las propuestas de conjunto buscando un acuerdo (Robles & Rojas, 2015). En este estudio, se ha seleccionado la “Agregación individual de los expertos”, que consiste en obtener la información de manera individual de cada uno de ellos, sin que estos se encuentren en contacto.

En referencia a la selección de expertos, inicialmente se elaboró una lista de posibles candidatos a encuestar. Se realizó un análisis de la información disponible respecto a la competencia de cada uno de ellos, teniendo en consideración sus condiciones de trabajo y las posibilidades reales de participación. Una vez realizada la lista, se les les hizo llegar anticipadamente el cuestionario junto con los instrumentos para evaluar su capacitación en el tema. Por lo tanto, el procedimiento empleado para esta selección de

los expertos ha sido estructurados (frente a otros que procedimientos que carecen de estructura o filtros) Para ello, se emplearon 2 criterios de selección: el biograma y el de competencia experta. La decisión de emplear una combinación de 2 técnicas se tomó para dar una mayor fiabilidad a la hora de hacer la selección.

a) Biograma: Se basa en realizar una biografía del experto en la que se pueden incorporar diferentes aspectos: lugar donde trabaja, años de experiencia, actividades desarrolladas, acciones formativas llevadas a cabo, experiencia en investigación, experiencia en la producción de TIC, años de trabajo, lugares dónde ha trabajado, entre otros. A partir de este biograma, se justifica la selección del experto por parte del investigador. En este caso, se estableció como mecanismo de adecuación del experto que conformen alguno de los siguientes perfiles: haber realizado estudios teóricos o empíricos sobre ciberseguridad/ciberdelincuencia ; haber realizado estudios teóricos o empíricos sobre educación vinculada a ciberseguridad/ciberdelincuencia; ser profesional relacionado con la ciberseguridad/ciberdelincuencia; ser docente de acciones formativas relacionado con el objeto de estudio; participar o haber participado en políticas públicas relacionadas con educación en ciberseguridad/ciberdelincuencia.

b) Una vez elaborada la lista de posibles expertos y confirmada la voluntariedad de estos a participar, se procedió a la calificación con la finalidad de determinar el grado de competencia en el tema que se quiere investigar. El método consiste en usar la autovaloración que la persona realiza en diferentes aspectos e indicadores. En base a ello, se establece un valor que es empleado para seleccionar a los expertos. Entre estos procedimientos, el de mayor significación es el denominado “competencia del experto en el tema (C)” (García & Fernández, 2008). Se obtiene mediante la opinión de los propios expertos hacen sobre su conocimiento y las fuentes a partir de las cuales argumentan y justifican su conocimiento.

Para determinar esta competencia (C); se hizo un cálculo a partir de la opinión del experto sobre su nivel de conocimiento acerca del problema planteado y de las fuentes que le permitan argumentar sus criterios. El cálculo se estableció en la expresión C =1/ 2 (Cc +Ca) donde:

Cc.: Coeficiente de conocimiento o información que tiene el experto acerca del tema. Calculado a partir de la valoración del propio experto en la escala del 0 al 10 y multiplicado por 0,1.

Ca : Coeficiente de argumentación o fundamentación de los criterios de los expertos

Tabla 8

Calificación por argumentación del criterio

Argumentación del criterio		
N°	Aspecto a calificar	valor
1	Análisis teóricos realizados por el experto	0.3
2	Experiencia obtenida	0.5
3	Trabajos de autores nacionales	0.05
4	Trabajos de autores extranjeros	0.05
5	Conocimiento propio del estado del problema en el extranjero	0.05
6	Intuición del experto	0.05

Para evaluar el coeficiente de competencia, se empleó el siguiente criterio:

• Sí C está entre 0,8 y 1, el coeficiente de competencia es alto.

• Sí C está entre 0,5 y 0,8 el coeficiente de competencia es medio.

• Sí C está entre 0,25 y 0,5 el coeficiente de competencia es bajo.

En la consulta se incluye la autovaloración y la fuente de argumentación. Posteriormente, en el procesamiento de las encuestas de selección, se obtuvo el coeficiente de competencia del experto, garantizando así una selección estructurada y justificada. Por último, en la fase final del proceso de consulta a los expertos, se elaboran las conclusiones del juicio. Se debe estimar la presencia de variables individuales como la personalidad o las habilidades sociales de los jueces, que pueden generar sesgos a favor de uno o varios aspectos del mismo (Robles & Rojas, 2015).

2.2. Instrumento

En cuanto a los instrumentos de recogida de información en el juicio de experto, de todo el amplio abanico de herramientas que permiten recoger la información de una manera cuantitativa, hemos seleccionado los cuestionarios. El motivo es que permiten dar una información más detallada y extendida. Se han incluido 3 preguntas de desarrollo, una tabla de valoración de 6 preguntas para poder cruzar los datos de una forma numérica, la tabla de argumentación del criterio y una valoración numérica de autocalificación del experto.

2.3. Participantes

El número total de expertos consultados asciende a un total de 42, de los cuales han remitido el cuestionario cumplimentado un total de 10. La identidad se ha anonimizado empleando códigos del E1 al E10 y asignándolos de forma aleatoria. Entre los expertos se encuentran personas de dilatada experiencia y en sectores clave, tanto hombres

como mujeres. Muchos de ellos pertenecen a un ámbito principalmente académico, mientras que una parte pequeña son de áreas más prácticas y de intervención directa en el área de estudio.

3. Resultados

En la Tabla 2 se pueden observar los coeficientes de competencia, a través de los cuales se puede determinar la calidad de la argumentación y medir de un modo cuantitativo el nivel de las personas consultadas. Los resultados se obtienen a partir de la autocalificación y la calificación de argumentación que, según el tipo de argumentación, recibirá una puntuación u otra (Tabla1). De los 10 jueces expertos, 3 tienen una puntuación de (C) Alto, ya que son mayores de 0.8, mientras que los otros 7 se encuentran en un nivel medio (entre 0.5 y 0.8). En cuanto a la media total es de 0.7475, por lo que es un nivel medio y cercano al alto pero sin alcanzarlo (0.8). Por todo ello, se puede afirmar que los distintos jueces expertos tienen una competencia válida para poder respaldar las respuestas aportadas a las preguntas planteadas.

Tabla 2

Coeficiente de competencia de los jueces expertos

	Autocalificación	**Calificación de argumentación**	**Coeficiente de competencia C =1/ 2 (Cc +Ca)**	**Coeficiente (C)**
E1	9	0.5	0.5*(9*0.1+0.5)= 0.7	(C) Medio
E2	9	0.55	0.5*(9*0.1+0.55)=0.725	(C) Medio
E3	9	0.55	0.5*(9*0.1+0.55)=0.7258	(C) Medio
E4	9	0.95	0.5*(9*0.1+0.95)=0.925	(C) Alto
E5	10	0.6	0.5*(10*0.1+0.6)=0.8	(C) Alto
E6	7	0.55	0.5*(7*0.1+0.55)=0.625	(C) Medio
E7	8	0.9	0.5*(8*0.1+0.9)=0.85	(C) Alto
E8	9	0.55	0.5*(9*0.1+0.55)=0.725	(C) Medio
E9	8	0.55	0.5*(8*0.1+0.55)=0.675	(C) Medio
E10	9	0.55	0.5*(9*0.1+0.55)=0.725	(C) Medio
Total	Media: 8,7	6.65	Media 0.7475	(C) Medio

A continuación, se exponen los resultados encontrados a las preguntas planteadas a los jueces expertos:

Pregunta 1 ¿Qué aspectos o qué puntos cree que se podrían mejorar en la educación en ciberseguridad orientada a la población general?.

E1 señala los conocimientos, la concienciación y las fakes news como elementos claves a tratar. También la importancia de la huella digital, las estafas y las prisas sumadas al desconocimiento.

E2 señala la sencillez (adaptar los conceptos a la ciudadanía, hacerla entendible). También usa el concepto “democratizar” los conceptos para que sean accesibles a todo el mundo. Fomentar el interés en la ciudadanía que, tal y como indica, las personas atribuyen la responsabilidad a los otros.

E3 señala que se debe ayudar a detectar estafas como elemento central de la ciberdelincuencia. También afirma que se necesita más información de acceso seguro a Internet, navegación segura, protección de datos, cookies, rastros, etc. Se centra, por lo tanto, en medidas concretas de protección.

E4 señala que se debe hacer comprender (concienciar) sobre las amenazas que existen y el impacto que puedan tener en sus vidas. Para este experto, la ciudadanía también debería estar en constante actualización, aprendiendo siempre las nuevas medidas de protección, tener una actitud proactiva y también concienciar en la autoprotección.

E5 señala los riesgos asociados a las TIC: vulneración de privacidad y uso fraudulento. También apunta a que la ciudadanía debe conocer las instituciones a las que acudir en caso de sufrir un riesgo asociado a la ciberseguridad.

E6 señala en primer lugar la importancia de la huella digital, la falta de concienciación en la población a la hora de publicar información de sus propias vidas en RRSS sin pararse a pensar en las consecuencias. Además, el problema no parece ser solamente que suban su propia información privada, sino que también suben información de sus propios hijos/as.

E7 señala la necesidad de difusión y accesibilidad de acciones formativas, con una especial atención a los/as jóvenes.

E8 señala un aspecto clave, el de una especial atención a los perfiles vulnerables “susceptibles de sufrir ataques”. También señala, al igual que otros expertos, la necesidad de más campañas por parte de las instituciones públicas. El tercer elemento que resalta, es el de la necesidad de actuar sobre la brecha digital existente.

E9 señala que un elemento de gran peso en relación a la educación. Indica que los proyectos de formación implementados deben ser impartidos por personas que tengan experiencias prácticas. Se destaca la importancia de tener conocimientos prácticos sobre la materia y no solamente académicos para una mayor conexión con la realidad de la ciberseguridad. Estos conocimientos prácticos pueden ser así transmitidos a las personas a las que se dirige la educación.

E10 señala a la necesidad de mejorar en la divulgación de cara a la ciudadanía, sobre todo en lo que se refiere a la autoprotección y las medidas de seguridad que ponen en

marcha las personas. Por último, indica que un punto a mejorar es la falta de recursos y medios.

Pregunta 2: en su organización ¿Trabajan personas provenientes de titulaciones técnicas como informática, telecomunicaciones, TIC, ingenierías, etc.? ¿Y de áreas de ciencias sociales como psicología, sociología, criminología, ciencias de la educación, etc.?

- E1 “Provienen de ambos sectores, tanto técnicos como no técnicos.”
- E2 “Sí, hay profesionales de diversas áreas, tanto técnicas como sociales.”
- E3 “En mi organización son todos informáticos.”
- E4 “Sí, trabajo en una universidad. Sí, por el mismo motivo.”
- E5 “Sí, de todo tipo. Asimismo, existen perfiles no técnicos dedicados a la ciberseguridad como economistas, periodistas, abogados, entre otros.”
- E6 “Sí”
- E7 “Sí, de ambas áreas. Es una Universidad.”
- E8 “En mi entorno suelo ser el único con titulación en informática. El resto de mis compañeros son distintas disciplinas educativas, trabajo social, sociosanitario, etc.”
- E9 “Trabajo con gente que viene de titulaciones técnicas y también de ciencias sociales ya que estoy en un ámbito educativo.”
- E10 “Trabajamos mayoritariamente de las primeras.”

Pregunta 3: ¿Considera que en el ámbito de la educación en ciberseguridad hay una representación proporcional entre perfiles de titulaciones técnicas y de las ciencias sociales?

- E1: Este experto responde negativamente y reafirma la idea de que la mayoría de los perfiles son de tipo técnicos. “No, actualmente la educación en ciberseguridad, y la conciencia que tiene la mayoría de la sociedad, abarca perfiles técnicos.”
- E2: De nuevo, va en la misma dirección de la dominancia de las áreas técnicas. También apunta a un cambio en el futuro, con una disminución progresiva. “No, domina las áreas técnicas, aunque creo que esta diferencia tenderá a disminuir con el paso del tiempo. Regulaciones como el RGPD va generando interés en la ciberseguridad a perfiles como abogados y los sistemas de gestión como las ISO 27001, ISO 22301 y el Esquema Nacional de Seguridad permiten a profesionales de otras titulaciones de ciencias acercarse a la ciberseguridad de manera gradual.”

- E3: “Creo que no, creo que la ciberseguridad se imparte en titulaciones muy concretas y relacionadas con la materia y que no es una enseñanza de ámbito general ni que se imparta en todas las titulaciones. Podría impartirse más en titulaciones de ciencias sociales.”
- E4: “No, de momento suelen tener más peso los perfiles técnicos.”
- E5: “Aún no las hay, se entiende la ciberseguridad como una disciplina técnica y no es exclusiva de este ámbito.”
- E6: Este experto señala un punto interesante y es que, según el tipo de organización, la situación será una u otra. En el caso de este experto, al pertenecer a una ONG dirigida a la educación, los perfiles prioritarios son de tipo social, pero también afirma que en las anteriores organizaciones eran mayoritarios los perfiles técnicos. “No, los profesionales técnicos son menos numerosos que los de ciencias sociales, pero también es debido al tipo de empresa, es una ONG que se dedica a la educación. Cuando he trabajado en otras empresas, los perfiles técnicos siempre han sido menores a los perfiles humanistas.”
- E7: “Hay demasiados técnicos y menos perfiles de sociales.”
- E8: En este caso, la percepción del experto es contraria a casi la totalidad de los expertos. Según señala, hay pocos perfiles técnicos y en general desconocen aspectos clave. “Para nada, cada vez que hablo con mis compañeros del tema me doy cuenta que no saben casi nada de ello...”
- E9: “No, en temas de ciberseguridad la exigencia son carreras técnicas, no obstante conozco algún perfil que viene de otras ramas y se ha redirigido al mundo de la ciberseguridad, bien con un master de ello, o con certificaciones de ciberseguridad.”
- E10: “No, sobre todo de técnicas.”

En la Tabla 3 se pueden ver los resultados totales de las respuestas a las 6 preguntas tipo likert. En general, las respuestas de los expertos es bastante homogénea y en la misma dirección. Las puntuaciones mínimas en cifras absolutas es de 10 y la máxima de 50. En las puntuaciones medias la mínima es de 1 y la máxima de 5. En la primera pregunta, la media es de 1.7, por lo que se puede afirmar que, según los expertos, la sociedad carece de capacidades mínimas en ciberseguridad. En la segunda tenemos un 1,5, así que está en la misma línea de la primera pregunta. Entienden que la población no está preparada debidamente para enfrentarse a los riesgos del ciberespacio y a los ciberdelitos. En la tercera tenemos una puntación de 1.6, afirmando

así que los esfuerzos por educar a la población en ciberseguridad son insuficientes frente al ciberdelito.

A partir de las puntuaciones a la pregunta 4 (1,5), se puede afirmar que valoran una falta de concienciación sobre los peligros de la ciberdelincuencia por parte de la población. En la pregunta 5 tenemos la puntuación más alta (3.1), siendo aun así un punto medio de la escala (entre 1 y 5). Se podría decir que no existe acuerdo sobre la cuestión de si se está orientando excesivamente hacia personal técnico frente a la población general. Por último, están en desacuerdo sobre la cuestión de si los proyectos educativos están siendo adaptados y actualizados a las novedades educativas y técnicas didácticas (2,1).

Tabla 3

Valoración de los expertos sobre las preguntas planteadas

Valoración de los expertos tipo Likert (del 1 al 5), siendo: 1 En total desacuerdo/ 2 En desacuerdo / 3 Indiferente / 4 De acuerdo /5 Totalmente de acuerdo			
Pregunta planteada	**Suma**	**Media**	**Desv.**
1. ¿Cree que actualmente la población general tiene unos conocimientos y capacidades mínimas en ciberseguridad?	17	1,7	,948
2. ¿Cree que se está preparando a la población general lo suficiente para enfrentarse a los riesgos del ciberespacio y a los ciberdelitos?	15	1,5	,527
3. ¿Cree que los esfuerzos que se están realizando para educar a la población son proporcionales al avance del ciberdelito y sus técnicas?	16	1,6	1,264
4. ¿Cree que la población general está suficientemente concienciada de los peligros de la ciberdelincuencia?	15	1,5	,500
5. ¿Cree que la educación en ciberseguridad se está orientando demasiado hacia personal técnico y menos a la población general (es decir, a un ámbito académico y profesional y no tanto a la ciudadanía)?	31	3,1	1,286
6. ¿Cree que los proyectos educativos que se están poniendo en marcha, están siendo adaptados y actualizados en las novedades educativas y las técnicas didácticas?	21	2,1	,875
Valores mínimos y máximos	10-50	1-5	

4. Discusión

Tras el análisis de los resultados nos encontramos con varios puntos que son a destacar. En primer lugar, que existe una visión general sobre la falta de concienciación, de conocimientos y de preparación de la población general frente a la ciberdelincuencia (pregunta 1, 2, 3 y 4 tipo likert). Es un punto de especial relevancia ya que, tal y como se ha expuesto en el informe de la ONSTI (2022) y de López et al. (2021), se afirma que el crecimiento de la ciberdelincuencia se va acelerando, cada día es mayor y con una mayor incidencia en la población general. El consenso de los expertos también va de acorde a dichos informes cuando se informa de la autopercepción de la población y su propia falta de capacitación para protegerse. En cuanto a las altas tasas de conductas

de riesgo (ONSTI, 2022), van en línea con los resultados encontrados en este estudio, donde los jueces expertos afirman en la pregunta 4 (Likert) que la ciudadanía no está concienciada sobre la problemática.

Actualmente, se han puesto en marcha diversas campañas de concienciación, sin embargo, tenemos también los resultados encontrados en el informe anual elaborado por la ONTSI (2022). Dicho informe señala que las campañas no llegan bien a la ciudadanía ya que el 48,8% de las personas consultadas declara no conocer ninguna en concreto. Precisamente uno de los expertos (E5), en la pregunta de desarrollo 1, va en esta misma línea cuando defiende que "*La ciudadanía debe conocer las instituciones a las que acudir en caso de sufrir un riesgo asociado a la ciberseguridad*". Las campañas deben arrojar luz a la ciudadanía para conocer los medios públicos a su disposición para prevenir y actuar ante un ciberataque. Sobre las formas en que se podría mejorar en la educación en ciberseguridad (pregunta 1 de desarrollo), las opiniones son variadas, aunque con algunos patrones en común. Es habitual incluir la mejora y aumento de campañas y divulgación. Esta afirmación es coherente con lo dicho anteriormente, ya que las campañas no están llegando correctamente a la ciudadanía. Por todo ello, sería necesario aumentarlas y mejorarlas.

Es común a prácticamente a todos los expertos la importancia de la concienciación sobre las ciberamenazas y no solamente la adquisición de medidas de autoprotección. La relevancia de este dato reside en que la concienciación está directamente relacionada con el conocimiento y el comportamiento online (Zwilling et al., 2022) . En este punto, la educación puede suponer un punto de partida desde el cual mejorar la conciencia. La educación aporta conocimientos para protegernos, pero también una mayor comprensión sobre la amenaza, cómo detectarla y cuál puede ser el origen de la victimización. En relación a las amenazas, los expertos señalaron las estafas como un elemento de especial preocupación y en incluirlo como elemento clave a la hora de educar a la población.

En cuanto a colectivos y población diana, fueron 2 los expertos que señalaran a grupos específicos. En el primer caso, se señala a la población joven como de especial importancia para recibir la educación. En el segundo caso, se habla de perfiles más vulnerables, precisamente aquellos a los que se ha redirigido la ciberdelincuencia tras los años del COVID-19, tal y como señala Miró (2021). Existirían colectivos con una mayor necesidad de educación y para los que sería necesario personalizar la educación. Es en este punto donde entrarían las ciencias de la educación para poder adaptarse a los distintos perfiles según sus características (niños, jóvenes, adultos, personas mayores, diversidad intelectual y funcional, población migrante, etc.). En cuanto a

quiénes tienen que educar, uno de los expertos (E9) en la pregunta de desarrollo 1, señala la importancia de que tengan conocimientos prácticos y no solamente teóricos o académicos. Esta indicación reafirma la importancia de la cercanía entre profesionales y ciudadanía, en la misma línea que el experto E2 en la pregunta de desarrollo 1, donde habla de "democratizar" la educación en ciberseguridad.

Abordando la cuestión de los perfiles técnicos o relacionados con las ciencias sociales (pregunta 2 de desarrollo), podemos observar que mayoritariamente los perfiles en las organizaciones de los expertos son variados o mixtos. Solamente 2 afirman que son predominantemente informáticos/técnicos. Estos últimos irían en la línea de Sánchez et al., (2022), quienes señalan que los equipos y expertos encargados de la ciberseguridad tienen un perfil técnico, con una alta preparación en informática pero no sobre el comportamiento humano, la incidencia de la cultura y la formación. También se debe resaltar que, la afirmación de los expertos sobre perfiles multidisciplinares en su entorno de trabajo (8 de 10), puede ser debido a que muchos/as pertenecen a instituciones universitarias y académicas, donde es habitual que haya todo tipo de perfiles.

La pregunta 3 de desarrollo reafirma lo anteriormente dicho, ya que, aunque casi todos/as afirman que en su institución están presentes distintos tipos de perfiles, cuando se les pregunta *"¿Considera que en el ámbito de la educación en ciberseguridad hay una representación proporcional entre perfiles de titulaciones técnicas y de las ciencias sociales?",* la respuesta mayoritaria es negativa, que son mayoritariamente técnicos. De hecho, uno de los expertos argumenta su respuesta en la línea de lo anteriormente expuesto que, los perfiles técnicos o mixtos, se agrupan según las organizaciones: por una parte ONGs, Universidades, etc. con perfiles variados y con representación de CCSS, mientras que en otras serían predominantes las técnicas.

El análisis de estas 2 cuestiones tiene su importancia en que cuando hablamos de educación en ciberseguridad, cibercrimen, víctimas, concienciación, etc. hablamos de criminología, psicología, educación, ciencias políticas, derecho, etc. Sin embargo, en muchas ocasiones nos encontramos que los autores provienen exclusivamente de ciencias de la computación o informática (Sánchez et al., 2022). Es en este punto donde hay que resaltar el hecho de que la ciberdelincuencia es un fenómeno complejo que requiere un enfoque interdisciplinar (López et al., 2021; Ghernaouti-Helie, 2009). Las respuestas de los expertos apuntan en la misma dirección de forma general, a pesar de que afirman trabajar en entornos con una presencia de profesionales variada.

Finalmente, otro punto de especial interés es el encontrado a raíz de los resultados de la pregunta 6 (Likert). Se señala la falta de adaptación de las técnicas empleadas para

educar. Aunque existen novedades e innovaciones, no se están poniendo en marcha a un nivel práctico. Desde las ciencias de la educación y ramas relacionadas, se investiga y se prueban nuevas formas enseñanza, con una fuerte implementación de las TIC, la gamificación y la simulación (Zhang-Kennedy & Chiasson, 2021; Coenraad et al., 2020). Dichas innovaciones deben ser puestas a disposición de la educación en ciberseguridad en el terreno práctico. También en relación a esto nos encontramos las respuestas a la pregunta 3 (likert) donde los expertos están en desacuerdo con que los esfuerzos que se están realizando para educar a la población son proporcionales al avance del ciberdelito y sus técnicas. Se desprende de estas ideas la necesidad de readaptar las estrategias educativas a las novedades de la ciberdelincuencia. Del mismo modo que si fuese una carrera tecnológica, la autoprotección debe tener siempre puesta la mirada en las nuevas formas de ciberataques.

5. Conclusiones

En esta investigación se ha consultado a expertos en el ámbito de la educación en ciberseguridad para conocer sus opiniones y percepciones basadas en amplia experiencia y formación. Se les ha planteado 3 cuestiones de desarrollo y 6 de tipo likert, con un cuestionario final para calificación de validez como expertos. De las respuestas obtenidas se muestra una realidad que no se corresponde con las necesidades a las que se enfrenta la sociedad. En primer lugar, aunque son necesarios perfiles procedentes de distintas áreas, incluidas las Ciencias Sociales, la realidad es que por lo general predominan los perfiles técnicos. La falta de equipos interdisciplinares con personas procedentes de derecho, criminología, psicología, sociología o ciencias de la educación pueden provocar una carencia de otras perspectivas o conocimientos de gran importancia a la hora de abordar la ciberdelincuencia.

También se puede afirmar que la percepción de los expertos sobre la ciudadanía es clara: existe una gran falta de concienciación, conocimientos y preparación por parte de las personas no-técnicas para protegerse a sí mismas y a sus familias. Esta carencia se refleja en las estadísticas de ciberdelincuencia, que van en aumento cada año y con previsiones de que a la larga los delitos online puedan superar a los tradicionales (offline). A esto se añade la falta de adaptar las técnicas y estrategias educativas al ámbito y aumentar la educación dirigida a la población general, no solo la dirigida a personal técnico o avanzado. En cuanto a las propuestas de mejora, hay consenso sobre que se deben mejorar y aumentar las campañas de divulgación dirigidas a la población, incluyendo información sobre ciberamenazas y ciberdelitos (con especial

atención a las estafas), medidas de autoprotección y una atención a determinados perfiles.

Por último, analizando todos los resultados de forma conjunta, existe una idea general compartida por los expertos: hay una falta de más y mejores estrategias de educación, más divulgación y visibilización de la problemática, una mejor adaptación de los medios educativos y más énfasis en concienciar sobre las ciberamenazas. Las políticas y estrategias que se implementan por parte de las instituciones son las responsables directas a la hora de mejorar esta autoprotección. Por lo tanto, es de especial relevancia que la administración pública esté actualizada y pueda reajustar su respuesta de acorde con la realidad vigente, por ejemplo, reformulando las campañas de divulgación o mejorando las técnicas educativas. En caso contrario, esa necesidad detectada se convertirá en victimización con el paso del tiempo.

Las limitaciones del estudio fueron la escasa participación de los expertos consultados y posibles sesgos en las preguntas. De los 42 expertos a los que se les envió el cuestionario, tan solo 10 respondieron. La redacción de las preguntas de investigación pueden siempre pueden incluir sesgos al dirigir la investigación (y en este caso las respuestas de los expertos) a unas determinadas posiciones u opiniones. Con todo, las implicaciones de este estudio son relevantes de cara a la mejora de las posibles mejoras en la educación en ciberseguridad y la concienciación ante la ciberdelincuencia. Se debe destacar la problemática de la excesiva orientación de la educación hacia personal técnico y a un nivel avanzado frente a la educación básica a la ciudadanía general. Para futuras investigaciones, sería interesante profundizar en formas concretas de mejorar las campañas de educación en ciberseguridad y en cómo redefinir las estrategias actuales. También ampliar la información sobre metodologías concretas que perfeccionen la enseñanza y el aprendizaje de ciberseguridad en la población general.

6. Referencias

ANDS (Asociación Nacional de Directores de Seguridad). (2021). Plan Estratégico contra la Cibercriminalidad. *Asociación Nacional de Directores de Seguridad.* Recuperado de https://directoresdeseguridad.es/2021/03/16/plan-estrategico-contra-la-cibercriminalidad/

Árpád, I. (2013). A Greater Involvement of Education in Fight Against Cybercrime. *Procedia - Social and Behavioral Sciences*, 83, 371–377. Doi: https://doi.org/10.1016/J.SBSPRO.2013.06.073

Cabero-Almenara, J., & Llorente, M. (2013). La aplicación del juicio de experto como técnica de evaluación de las tecnologías de la información y comunicación (TIC). *Eduweb*, 7(2), 11–22. Recuperado de http://tecnologiaedu.us.es/tecnoedu/images/stories/jca107.pdf

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation and Gaming*, *51*(5), 586–611. https://doi.org/10.1177/1046878120933312

DSN. (2019). Estrategia Nacional de Ciberseguridad 2019. *Departamento de Seguridad Nacional, España*. Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez de contenido y Juicio de Expertos: Una Aproximación a Su Utilización. *Avances En Medición*, 6, 27–36 . Recuperado de https://www.researchgate.net/publication/302438451_Validez_de_contenido_y_juicio_de_expertos_Una_aproximacion_a_su_utilizacion

García, L., & Fernández, S. J. (2008). Procedimiento de aplicación del trabajo creativo en grupo de expertos. *Ingeniería Energética, XXIX* (2),46-50. Consultado el 16 de Abril de 2022. Recuperado de https://www.redalyc.org/articulo.oa?id=329127758006

Ghernaouti-Helie, S. (2009). An Inclusive Information Society Needs a Global Approach of Information Security. *2009 International Conference on Availability, Reliability and Security*, 658-662. DOI: 10.1109/ARES.2009.127

Hadlington, L., & Chivers, S. (2020). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness

and Personality Factors. *Policing: A Journal of Policy and Practice*, 14, 479-492. DOI:10.1093/police/pay027

López, J., Sánchez, F., Herrera, D., Martínez, F., Rubio, M., Gil, V., Santiago, A.M., & Gómez, M.A . (2021). Informe sobre la Cibercriminalidad en España. Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad . Ministerio del Interior, España. Recuperado de https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

Miró, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC. http://dx.doi.org/10.7238/idp.v0i32.373815

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2022). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. *Observaciber*. Recuperado de https://www.observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

Robles, P. & Rojas, M. (2015). La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada. *Revista Nebrija de Lingüística Aplicada* (2015) 18. Recuperado de: https://www.nebrija.com/revista-linguistica/files/articulosPDF/articulo_55002aca89c37.pdf

Sánchez, F., Martínez, J.E., & Téllez, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *Methaodos Revista De Ciencias Sociales*, *10*(2), 243–258. https://doi.org/10.17502/mrcs.v10i2.577

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, *54*(1), 1–39. https://doi.org/10.1145/3427920

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Estudio 5: Estudio observacional

Educar y proteger: Análisis de la eudcación en ciberseguridad para combatir la ciberdelincuencia

Resumen

La ciberdelincuencia es un problema en aumento que afecta a toda la ciudadanía. Actualmente, se están poniendo en marcha planes educativos para educar a la población y poder disminuir esas tasas de victimización. El objetivo de este estudio es analizar las relaciones entre los conocimientos en ciberseguridad y ciberamenazas, la vulnerabilidad y la victimización. Al mismo tiempo, también se ha estudiado la influencia de la educación y variables sociodemográficas sobre las anteriores variables. Para ello, se ha administrado un cuestionario a una muestra de 229 personas de distintos puntos del territorio español. Los resultados muestran que la educación mejora los conocimientos y consigue disminuir la vulnerabilidad y victimización ante la ciberdelincuencia. Además el sexo, la edad y la procedencia también tienen una relación directa con las variables. Este estudio demuestra la importancia de los programas educativos en ciberseguridad y su influencia para poder mejorar la protección de la ciudadanía.

Palabras clave: ciberseguridad; ciberdelito; vulnerabilidad; educación.

1. Introducción

La ciberdelincuencia y la vulnerabilidad en el ciberespacio son problemas que van en aumento en nuestra sociedad, afectan a un gran número de personas y tiene un gran impacto en la ciudadanía. Según el Departamento de Seguridad Nacional (DSN, 2019) la vulnerabilidad en el ciberespacio llega a ser calificada como uno de los principales riesgos para nuestro desarrollo como nación. Supone un gran riesgo para la seguridad de nuestros datos personales, de las actividades comerciales y un perjuicio económico para quienes lo sufren. Además, en el Estudio sobre percepción y nivel de confianza en España (ONTSI, 2022), se encontró que en el último semestre de 2021, el 60% de las personas afirma haber sufrido un incidente de seguridad, un aumento de 4,4% respecto al primer semestre de 2021. En cuanto al fraude en la red, el porcentaje de quienes aseguran haberlo sufrido aumentó al 71%, lo que supone una subida de 6,3% sobre el semestre anterior. También va en aumento el “phishing”, que consiste en usar el engaño para manipular a las víctimas y conseguir infectarles el dispositivo o robar información.

Existe un reconocimiento en la literatura de que los factores de comportamiento humano son la clave para combatir el ciberdelito (Hadlington & Chivers, 2018; García-Guilabert, 2016). Aunque la tecnología de la información es usada masivamente por toda la sociedad a nivel mundial, es necesario enseñar los temas de seguridad de la información para evitar que se conviertan en víctimas de la ciberdelincuencia (Ismailova & Muharnetjanova, 2016). Los resultados encontrados por Fernández-Montalvo et al. (2015) también suponen una señal de alarma e indican la necesidad de establecer programas preventivos para el uso seguro de Internet. Se trata de conseguir que el uso de Internet encuentre un espacio natural en las actividades del sujeto, evitando los riesgos y peligros derivados de una utilización indiscriminada y sin criterios específicos. La baja capacidad para conseguir encontrar y enjuiciar a los ciberdelincuentes, hace necesario mejorar la protección de las potenciales víctimas.

Los hábitos de ciberseguridad, también denominado ciberhigiene, suele desempeñar un papel importante en victimización. Algunos ejemplos de estos hábitos son emplear cortafuegos y aplicaciones antivirus. Los individuos con buena ciberhigiene siguen las mejores prácticas de seguridad y protegen su información personal (Cain et al., 2018). En su investigación, estudiaron los conocimientos de ciberseguridad, sobre las ciberamenazas y sus comportamientos relacionados con la ciberhigiene. Además, incluyeron variables como formación y experiencia previas, el impacto de la edad, el sexo y la victimización. En sus resultados, destacan la importancia de la educación y los conocimientos y de tener en cuenta las variables demográficas implicadas. Dentro de los conocimientos, existen algunos básicos como: detectar el phishing, recursos a los que acudir en caso de ser víctimas, las ciberamenazas existentes, las ciberestafas más habituales o la creación de contraseñas seguras.

En el estudio de Zwilling et al. (2020), analizaron las relaciones entre la concienciación, los conocimientos y el comportamiento en materia de ciberseguridad con las herramientas de protección. Encontraron que los internautas poseen una concienciación adecuada sobre las ciberamenazas, pero sólo aplican medidas de protección mínimas, por lo general relativamente comunes y sencillas. Los resultados del estudio también muestran que un mayor conocimiento cibernético está relacionado con el nivel de ciberconciencia. Además, la concienciación también está relacionada con las herramientas de protección. Así pues, los encuestados con más conocimientos de ciberseguridad toman más medidas para prevenir los ataques, especialmente cuando las herramientas de defensa son sencillas. También descubrieron que el conocimiento de la ciberseguridad y el uso de Internet estaban relacionados con las actividades de protección a través de la mediación de la concienciación sobre la ciberseguridad. Estos

resultados ponen de relieve el importante papel de la educación de ciberseguridad para motivar a los usuarios a adoptar conductas proactivas.

En Drew (2020), se ha estudiado la educación para la prevención de la delincuencia centrada en aumentar los conocimientos y su eficacia en reducir la victimización. Encontraron la necesidad de incluir elementos clave que puedan tener un impacto significativo y real en el uso de la autoprotección. Estos tienen un impacto significativo y real en el uso de comportamientos y estrategias de autoprotección. Educar a los individuos resulta ser un método útil para fomentar la autoprotección y un mayor uso de los métodos de prevención, reduciendo así la probabilidad de victimización. Por lo tanto, existe una relación entre educación, conocimientos y vulnerabilidad que es de interés estudiar para poder prevenir la ciberdelincuencia.

Existen evidencias de diferencias entre los distintos colectivos de la sociedad en su capacidad para defenderse. Un ejemplo claro es la edad, factor generador de la denominada “brecha digital”, en este caso, de forma intergeneracional. Se ha encontrado que las personas mayores presentan menores conocimientos y capacidades para defenderse en el ámbito digital frente a las más jóvenes (Ramadhani et al., 2020). En Gudiño (2018) hablan de la desprotección de los mayores ante los riesgos a los que se ven expuestos en uso diario de las nuevas tecnología. Entre los factores de vulnerabilidad encontraron: el aislamiento social, los problemas de salud cognitivos, físicos y mentales; el nivel de riqueza, las habilidades o conocimientos limitados en ciberseguridad. En cuanto a la prevención, la intervención directa con las personas mayores reduce los riesgos de ciberdelincuencia, la mejora de la concienciación y las habilidades (Burton et al, 2022). Se han desarrollado programas exitosos donde se aprenden las técnicas de seguridad y las medidas de protección desde un nivel inicial, explicando a personas de la tercera edad sobre cómo y por qué un ciberdelincuente envía estafas de phishing por correo electrónico (Cook et al., 2011).

Dentro de los distintos colectivos, también encontramos a los nativos digitales, que son aquellos que han crecido con las nuevas tecnologías. Aunque la usan a diario, algunos estudios sobre población escolar, encontraron que casi el 30% del alumnado no había recibido ningún tipo de formación o información previa a la actuación formativa de ciberseguridad (Gamito et al., 2020). A pesar de ello, la formación general en el ámbito digital y la agilidad en el uso de TICs debería ser un factor positivo en relación a los conocimientos y una menor vulnerabilidad. También se han encontrado diferencias según el sexo, siendo los hombres los que obtienen mejores resultados en conocimientos y menor vulnerabilidad (Cain et al., 2018). En cuanto a la procedencia, no hay estudios que investiguen la incidencia sobre la población migrante en España y

su capacitación para defenderse. La población migrante, solicitante de asilo, refugiada y apátrida, en muchos casos, proviene de países donde no hay alfabetización digital, por lo tanto, también sería una población de mayor riesgo en el ciberespacio.

En este estudio, se busca dar respuesta a si la educación en ciberseguridad y los conocimientos reducen la vulnerabilidad, victimización y factores sociodemográficos. Concretamente, nos planteamos la siguiente pregunta de investigación ¿Puede la educación en ciberseguridad y los conocimientos sobre este tema reducir la vulnerabilidad y la victimización? Para ello, se han planteado un total de 4 objetivos de investigación:

- Objetivo 1: Comprobar los niveles de vulnerabilidad, victimización, educación, sensación de seguridad y conocimientos en ciberseguridad/ciberdelincuencia.
- Objetivo 2: Averiguar la relación existente entre el nivel de conocimientos, vulnerabilidad, victimización y educación.
- Objetivo 3: Estudiar la influencia de las variables sociodemográficas (sexo, edad y procedencia) en los conocimientos, vulnerabilidad y victimización.
- Objetivo 4: Estudiar la influencia que tiene la educación en ciberseguridad en los conocimientos, vulnerabilidad y victimización.

2. Metodología

La metodología implementada ha sido el estudio observacional por método de encuesta. Se ha empleado un cuestionario dividido en 4 secciones. La primera sección incluyen las variables sociodemográficas (4 preguntas); la segunda preguntas para evaluar los conocimientos (8 preguntas); la tercera contiene preguntas para evaluar la vulnerabilidad (10 preguntas); la última sección contiene preguntas referidas a la educación, la victimización y la autopercepción de seguridad (4). Para la validez del cuestionario se ha hecho una consulta a jueces expertos e incluido conceptos clave del ámbito. Posteriormente, se administró a una muestra piloto para obtener un primer feedback. Para el análisis de fiabilidad se han realizado pruebas de Alfa de Cronbach, obteniendo una puntuación de 0,725. Este indicador muestra la consistencia interna de la herramienta empleada. Teniendo en cuenta que el mínimo aceptable para la fiabilidad es de 0,7, encontramos que el instrumento es apto para la evaluación de interés.

La plataforma empleada para el cuestionario es GoogleForms, que permite un diseño fácil con múltiples opciones, recibir las respuestas automaticamente y enviar por distintas vías el enlace de acceso. Se ha tratado de una muestra incidental mediante el envío masivo por distintos medios y tomando datos de residencia para controlar la variable territorial. La muestra obtenida es de un total de N=229. En la Tabla 2.1 se muestran los porcentajes según sexo (48,9% hombres y 48,5% mujeres) y de edad,

divididos en tres rangos según sean nativos digitales (48%) y no nativos digitales (51.9%). Este último grupo, se ha subdividido entre población adulta (43,2%) y tercera edad (8,7%). Finalmente, en la variable “colectivo por procedencia”, se muestra el porcentaje de personas nacionales (81,7%) y extranjeras (migrantes, solicitantes de asilo, refugiados y apátridas) con un 18,3%.

TABLA 2.1 Datos sociodemográficos

Sexo

	N	%
Hombres	112	48,9%
Mujeres	111	48,5%
Sin especificar	6	2,6%

Edad

	N	%
Menores de 35	110	48,0%
Entre 35 y 65	99	43,2%
Mayores de 65	20	8,7%

Colectivo por procedencia

	N	%
Nacionales	187	81,7%
Extranjeros	42	18,3%

En cuanto a las variables planteadas, son las siguientes:

VI Sexo: Variable Nominal- Dicotómica. Hombres; Mujeres.

VI Edad: Variable nominal

- Colectivo 1 Nativos digitales (Menores de 35)
- Colectivo 2 No-Nativos digitales (Mayores de 35 y menores de 65)
- Colectivo 3 No-Nativos digitales (Mayores de 65)

VI Procedencia Variable Nominal

- Colectivo 1 Nacionales.
- Colectivo 2 Población extranjera: migrantes, solicitantes de asilo, refugiados y apátridas.

VI Educación en ciberseguridad/ciberdelincuencia: Si ha recibido formación/cursos en ciberseguridad y/o ciberamenazas. Variable Ordinal.

VI Nivel de conocimientos: conocimiento sobre las amenazas y formas de ciberdelincuencia, así como las medidas de ciberseguridad necesarias para protegerse. Variable Cuantitativa Discreta.

VD Vulnerabilidad: Se entiende por vulnerable cuando el individuo no pone en marcha medidas de protección. No basta solo con tener conocimiento (el cómo defenderse), sino también emprender acciones para evitar ser víctima. Por lo tanto, la vulnerabilidad tiene un componente de concienciación y esfuerzo sumado a la educación. La puntuación 0 corresponde con una alta vulnerabilidad y 10 una escasa vulnerabilidad. Variable Dicotómica

VD Victimización: Si en algún momento ha sufrido algún tipo de ciberdelito y una o varias veces. La idea de víctima de ciberdelito es amplia, y puede incluir, por ejemplo, el sufrir malware en cualquier dispositivo, una ciberestafa o el robo de información. Ordinal

VD Autopercepción de seguridad: Si el individuo se considera seguro para afrontar posibles ciberdelitos. Ordinal

3. Resultados

3.1 Niveles de vulnerabilidad, victimización, educación, sensación de seguridad y conocimientos en ciberseguridad/ciberdelincuencia.

En la Tabla 3.1 se muestran los datos descriptivos. Se debe tener en cuenta que la vulnerabilidad se ha tratado de forma invertida, siendo la puntuación 0 la correspondiente a una persona vulnerable y 10 una persona con alta capacidad para defenderse. Se puede observar que la media en conocimientos apenas alcanza el 4,89, siendo la puntuación máxima de 16 y una desviación del 3.66. Solo el 12,3% supera la puntuación de 10, estando la mayor parte de los individuos por debajo de ese valor. En vulnerabilidad la media es 5.51, siendo la puntuación máxima 10, por lo tanto, se encuentra en unos valores medios de protección. La mayor parte de los individuos se encuentran entre 3 puntos y 8 puntos en vulnerabilidad (84,3%). En cuanto a la desviación, presenta un valor de 2.11.

Analizando los datos de victimización, el 60.7% afirman no haber sido nunca víctima de ningún tipo de ciberdelito, mientras que el resto afirma haber sido víctima al menos en una ocasión. De los que afirman haber sido víctimas, la mayor parte lo fueron en una sola ocasión con un 31% del total. Por otra parte, analizando los datos en educación, el 60,7% de las personas consultadas afirman no haber recibido nunca ningún tipo de formación, frente al 39,3% que sí la ha recibido. En cuanto a la sensación de inseguridad, es mayoritaria, encontrando que el 57% de las personas se sienten poco o muy poco seguras, frente al 24,5% que sí se sienten seguras. También existe un porcentaje muy bajo que afirman sentirse muy seguras, tan solo el 4,4%. El restante de los consultados (18,5%) no sabrían decirlo. La puntuación media es de 1,66 sobre 4.

TABLA 3.1 Estadísticos Descriptivos

Estadísticos Descriptivos

		Conocimientos de ciberseguridad básica	Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Víctima de ciberdelito	Educación en ciberseguridad	Sensación de seguridad
N	Válido	229	229	229	229	229
Media		4,89	5,51	1,49	1,66	1,66
Desviación		3,669	2,112	,698	,927	1,119
Mínimo		0	0	1	1	0
Máximo		15	10	4	4	4

Nivel de conocimientos de ciberseguridad básica

	N	%
0	21	9,2%
1	18	7,9%
2	28	12,2%
3	32	14,0%
4	26	11,4%
5	22	9,6%
6	15	6,6%
7	17	7,4%
8	10	4,4%
9	12	5,2%
10	7	3,1%
11	7	3,1%
12	2	0,9%
13	5	2,2%
14	3	1,3%
15	4	1,7%

Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)

	N	%
0	1	0,4%
1	8	3,5%
2	14	6,1%
3	20	8,7%
4	24	10,5%
5	41	17,9%
6	37	16,2%
7	47	20,5%
8	24	10,5%
9	8	3,5%
10	5	2,2%

Víctima de ciberdelito

	N	%
Nunca	139	60,7%
1 vez	71	31,0%
2 o 3 veces	15	6,6%
Más de 3 veces	4	1,7%

Educación en ciberseguridad

	N	%
No	139	60,7%
Poca formación	42	18,3%
Algo de formación	36	15,7%
Mucha formación	12	5,2%

Sensación de seguridad

	N	%
No sabe	41	17,9%
Muy poco seguro	63	27,5%
Poco seguro	69	30,1%
Algo seguro	46	20,1%
Muy seguro	10	4,4%

De las cuestiones relacionados con conocimientos (Tabla 3.2), la mayor parte de la ciudadanía (80,7%) afirma no conocer instituciones específicas en caso de ser víctimas de ciberdelitos. Tras ser preguntadas específicamente por el INCIBE, el OSI y el IS4K, el 72,1% de las personas consultadas no conocen ninguna de ellas. De las que conocen, encabezan la lista el Incibe (23,6%), seguido por el OSI (8,7%) y el IS4K (3,1%).La mayor parte afirman conocer el Phishing (76,5%), pero cuando se hace una pregunta de evaluación sobre en qué consiste este ciberdelito, tan solo el 44,8% acierta. El porcentaje es aún menor cuando se pregunta sobre cómo detectarlo (37,1%). En cuanto a la estafa relacionada con el Bizum, el 37,1% caería en la estafa, mientras que el 62,9% sería capaz de evitarla.

En las cuestiones relacionadas con vulnerabilidad, tan solo el 27,9% afirma de disponer antivirus en el móvil, frente al 72,1% que carecen de él. En cuanto al uso de las VPN (Virtual Private Network), el porcentaje es similar, 69% no dispone de él. Más de la mitad de las personas (55,9%) afirman hacer copias de seguridad periódicas de su información. Sobre las contraseñas, el 79% es capaz de reconocer una contraseña segura (8 caracteres, con números, letras, mayúsculas, minúsculas y símbolos), sin embargo, el 31,9% afirma no usarlas. Además, el 80,3% de los encuestados afirma repetir contraseñas en distintos sitios. Por último, el 45,4% se conectan a conexiones wifi que no requieran contraseñas.

TABLA 3.2 Principales resultados de cuestionario

Cuestiones destacadas	Resultados
En caso de sufrir un ciberataque o sufrir un ciberdelito ¿sabrías con qué institución específica (además de la policía) ponerte en contacto?	19,3% si 80,7% no
Ante la pregunta de ¿Qué tipos de ciberdelitos que conoces?	76,5% Phishing
¿Qué es el phishing?	44,8% acierta
¿Cómo detectar el phishing?	37,1% acierta
¿Cuál de estas instituciones públicas de ciberseguridad conoces?	72,1% no conoce ninguna 23,6% Incibe 8,7% OSI 3,1% IS4K
Te envían una solicitud de Bizum ¿recibes o te cobran el cargo?	62,9% acierta 37,1% caería en la estafa
¿Tienes antivirus en el móvil?	27,9% sí tiene 72,1% no tiene
¿Haces copias de seguridad de forma periódica?	55,9% sí

¿Usas VPN (virtual private network) en el ordenador?	69% no usa
¿Cual de las siguientes contraseñas es más segura?	79% acierta
Usas contraseñas seguras: 8 caracteres, con números, letras, mayúsculas, minúsculas y símbolos.	31,9% no las usa
¿Repites contraseñas en distintos sitios?	80,3% las repite
¿Alguna vez te conectas a wifi pública que no requiere contraseña?	45,4% se conectan

3.2 Relación existente entre el nivel de conocimientos, vulnerabilidad, victimización y educación.

Una vez realizado el análisis estadístico (Spearman) para las variables conocimientos, vulnerabilidad, victimización y educación, se encontró una alta correlación entre dichas variables (Tabla 3.3). La variable conocimientos obtiene un coeficiente de correlación significativo de 0,438 con la variable vulnerabilidad (Sig. <0,001); con la variable victimización obtiene una relación significativa negativa de -0,172 (Sig. 0,009); con la variable educación tiene la correlación más fuerte de las tres, con 0,537 de coeficiente (Sig. <0,001). La vulnerabilidad tiene una correlación significativa con la variable educación del 0,330 (Sig. <0,001), sin embargo, su relación con la victimización no es significativa (Sig. 0,127). La victimización tiene una relación negativa y significativa con la variable educación, obteniendo un coeficiente de -0,177 (Sig. 0,007).

TABLA 3.3 Correlaciones entre conocimientos, vulnerabilidad, victimización y educación en ciberseguridad

Correlaciones

			Conocimientos de ciberseguridad básica	Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Víctima de ciberdelito	Educación
Rho de Spearman	Nivel de conocimientos de ciberseguridad básica	Coeficiente de correlación		,438**	-,172**	,537**
		Sig. (bilateral)		<,001	,009	<,001
	Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Coeficiente de correlación	,438**		-,101	,330**
		Sig. (bilateral)	<,001		,127	<,001
	Víctima de ciberdelito	Coeficiente de correlación	-,172**	-,101		-,177**
		Sig. (bilateral)	,009	,127		,007
		Coeficiente de correlación	,537**	,330**	-,177**	

Educación en ciberseguridad	Sig. (bilateral)	<,001	<,001	,007	.

**. La correlación es significativa en el nivel 0,01 (bilateral).

3.3 Influencia de las variables sociodemográficas sobre los conocimientos, vulnerabilidad y victimización.

Se han obtenido los siguientes resultados en relación a la variable sexo (Tabla 3.4) . En primer lugar, existen diferencias significativas entre los conocimientos según el sexo, con una t de 4,904 (Sig. <0,001). La media de conocimientos en hombres es mayor que el de las mujeres. Los hombres obtienen una media de 5,97 frente al 3,69 de las mujeres. El resto de variables, vulnerabilidad y victimización, no obtienen diferencias significativas (Sig. 0,255 y 0,384 respectivamente). Por lo tanto, los datos muestran que no existe una influencia de la variable sexo sobre vulnerabilidad y victimización, pero sí sobre los conocimientos en ciberseguridad básica.

TABLA 3.4 Estadísticos variable Sexo

	Sexo	N	Media	Desviación estándar
Nivel de conocimientos de ciberseguridad básica	Hombres	112	5,97	3,976
	Mujeres	111	3,69	2,872
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Hombres	112	5,53	2,009
	Mujeres	111	5,45	2,206
Víctima de ciberdelito	Hombres	112	1,46	,684
	Mujeres	111	1,53	,724

Prueba t de muestras independientes

	Prueba de Levene de igualdad de varianzas		Prueba t para la igualdad de medias				
					Significación		
	F	Sig.	t	gl	P de un factor	P de dos factores	Diferencia de medias
Conocimientos de ciberseguridad básica	12,422	<,001	4,904	221	<,001	<,001	2,280
Nivel de vulnerabilidad	1,303	,255	,270	221	,394	,787	,076
Víctima de ciberdelito	,761	,384	-,713	221	,238	,476	-,067

La tabla 3.5 muestra los resultados en relación a la procedencia de los participantes y la prueba t de muestras independientes. Se han dividido en nacionales y extranjeros. En la variable conocimientos, se han hallado diferencias significativas entre los grupos, con una t de 3,341 y una significación de <0,001. Los nacionales obtienen mejores resultados que los extranjeros, con una puntuación media de 5,26 de los nacionales frente al 3,21 de los extranjeros. También se han encontrado diferencias significativas en la variable vulnerabilidad, con una t de 4,871 y una significación de <0,001. Al igual que en el anterior caso, los nacionales obtienen una mejor puntuación de vulnerabilidad. Los nacionales tienen una media de 5,82 frente al 4,14 de los extranjeros. Finalmente, la procedencia resultó no ser significativa en la victimización.

TABLA 3.5 Estadísticos variable Procedencia

	Procedencia	N	Media	Desviación estándar
Nivel de conocimientos de ciberseguridad básica	Nacionales	187	5,26	3,685
	Extranjeros	42	3,21	3,120
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Nacionales	187	5,82	1,860
	Extranjeros	42	4,14	2,600
Víctima de ciberdelito	Nacionales	187	1,50	,721
	Extranjeros	42	1,45	,593

Prueba t de muestras independientes

	Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias				
					Significación		
	F	Sig.	t	gl	P de un factor	P de dos factores	Diferencia de medias
Conocimientos de ciberseguridad básica	5,281	,022	3,341	227	<,001	<,001	2,048
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	13,735	<,001	4,871	227	<,001	<,001	1,675
Víctima de ciberdelito	1,497	,222	,421	227	,337	,674	,050

La tabla 3.6 muestra los resultados de la variable edad y del análisis Anova. En la variable conocimientos se ha encontrado diferencias significativas entre los 3 grupos en los que se ha dividido la muestra según su edad. Se ha obtenido una puntuación F de 16,268 y una significación de <0,001. El grupo que ha obtenido mejores resultados es el de menores de 35, con una puntuación media de 5,97, el siguiente es el del rango 35-65, que obtiene una media de 4,36. Por último, los mayores de 65, tienen una media de 1,5. También la variable vulnerabilidad muestra resultados significativos. Tiene un F de 13,306 y una significación de <0,001. La media de los menores de 35 y del rango de 35-65 muestran medias muy similares con 5,74 y 5,71 respectivamente. El grupo mayor de 65 tiene una media de 3,30, la menor de los 3 grupos. Finalmente, la variable victimización no tiene resultados significativos en relación a la edad. Obtiene una F de 3.93 y una significación de 0,021.

TABLA 3.6 Estadísticos variable Edad

		N	Media
Nivel de conocimientos de ciberseguridad básica	Menores de 35	110	5,97
	Entre 35 y 65	99	4,36
	Mayores de 65	20	1,50
	Total	229	4,89
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Menores de 35	110	5,74
	Entre 35 y 65	99	5,71
	Mayores de 65	20	3,30
	Total	229	5,51
Víctima de ciberdelito	Menores de 35	110	1,36
	Entre 35 y 65	99	1,60
	Mayores de 65	20	1,70
	Total	229	1,49

ANOVA

		gl	F	Sig.
Nivel de conocimientos de ciberseguridad básica	Entre grupos	2	16,268	<,001
	Total	228		
	Entre grupos	2	13,306	<,001

Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Total	228		
Víctima de ciberdelito	Entre grupos	2	3,939	,021
	Total	228		

3.4 Influencia de la educación en ciberseguridad sobre los conocimientos, vulnerabilidad y victimización.

En relación a la tabla 3.7, se muestra el efecto de la educación en ciberseguridad sobre las variables objeto de estudio. En la variable conocimientos, se encontró una F 34,765 y una significación de <0,001. Las personas que recibieron educación en ciberseguridad tienen una media de conocimientos mayor que aquellas que no. La media de las que no recibieron educación es de 3,28 frente a las que recibieron mucha 8,75. Las que recibieron algo tienen 7,86 y las que tuvieron poca 6.55. En cuanto al nivel de vulnerabilidad, también resultó ser significativa con una F de 10,833 y una significación de <0,001. Las personas que no recibieron educación tienen una media de vulnerabilidad de 4,91. De las que sí recibieron, obtienen medias muy similares de vulnerabilidad en los distintos niveles de educación (Poca=6,38; Algo=6.36; Mucha=6,83). En relación a la variable victimización, se encontró que existen diferencias débiles (F de 3,516) pero significativas (Sig. 0,016). Los individuos que no han recibido nunca educación en ciberseguridad tienen una media mayor en victimización que el resto (1,58). Aquellas que tienen mucha formación obtienen una media de 1,08, las que han recibido algo 1,53 y las que tuvieron poca 1,29.

TABLA 3.7 Estadísticos variable educación

		N	Media	Desviación estándar
Nivel de conocimientos de ciberseguridad básica	No	139	3,28	2,551
	Poca formación	42	6,55	3,270
	Algo de formación	36	7,86	3,796
	Mucha formación	12	8,75	4,827
	Total	229	4,89	3,669
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	No	139	4,91	2,198
	Poca formación	42	6,38	1,413

	Algo de formación	36	6,36	1,775
	Mucha formación	12	6,83	1,642
	Total	229	5,51	2,112
Víctima de ciberdelito	No	139	1,58	,711
	Poca formación	42	1,29	,596
	Algo de formación	36	1,53	,774
	Mucha formación	12	1,08	,289
	Total	229	1,49	,698

ANOVA

		gl	Media cuadrática	F	Sig.
Nivel de conocimientos de ciberseguridad básica	Entre grupos	3	324,010	34,765	<,001
	Total	228			
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Entre grupos	3	42,794	10,833	<,001
	Total	228			
Víctima de ciberdelito	Entre grupos	3	1,660	3,516	,016
	Total	228			

4. Discusión final y conclusiones

Tras analizar los resultados obtenidos, se ha encontrado un nivel bajo de conocimientos en la población consultada. Dichos conocimientos aportan una capacitación que permite a los individuos defenderse, sin embargo, esa carencia encontrada les deja en una situación de mayor vulnerabilidad. Además, los niveles de educación son bajos, ya que el 60% nunca la recibió ningún tipo de formación. El 39,3% que sí la recibió también es bajo si lo comparamos con el 81% de Cain et al., (2018), pero más aproximado al 30% de Gamito et al., (2020). El porcentaje de victimización es elevado (60,7%) en comparación a otros estudios, 24% y 30% (Buelga *et al.*, 2010; Estévez, *et al.*, 2010). Sin embargo, es una cifra moderada si tenemos en cuenta que existen formas leves de ser víctima de ciberdelitos. Un ejemplo sería la victimización por Malware, que en otros estudios alcanza el 72% (García-Guilabert, 2016). En cuanto a la sensación de seguridad, apenas el 24,5% afirma sentirse segura. Este sentimiento generalizado puede deberse a que, al plantearse las cuestiones sobre ciberamenazas, los individuos han sido más conscientes del desconocimiento que tienen sobre el tema.

Son preocupantes algunos resultados de hábitos en ciberseguridad, por ejemplo, el escaso uso de antivirus en el teléfono móvil (72,1% no tiene). Contrasta con el uso de antivirus en el ordenador, ya que en Cain et al. (2018) encontraron que entre el 47% y el 78% disponen de él y lo actualizan con regularidad. También destaca el desconocimiento de instituciones como el Incibe, la OSI y el IS4K. Estas instituciones son las encargadas de brindar información, materiales didácticos y educación a la población general, sin embargo, no están consiguiendo llegar a la ciudadanía. Cabría cuestionarse si las campañas implementadas por estas instituciones son efectivas cuando la mayor parte de la población afirma no conocerlas. Por último, el 37,1% de la población consultada caería en la estafa del Bizum, lo que indica que desconocen aspectos básicos de esta plataforma de pagos y que puede llevarles a ser víctimas de este tipo de delitos.

Para el segundo objetivo de estudio, se confirmó que existe relación directa entre conocimientos y vulnerabilidad. Aquellos individuos con un mayor de nivel de vulnerabilidad presentan menores conocimientos. Lo mismo sucede al contrario, aquellas personas con más conocimientos tienen una menor vulnerabilidad. Estos datos señalan la importancia de mejorar los conocimientos en ciberseguridad para disminuir la vulnerabilidad ante las ciberamenazas Sobre la cuestión de si existe una relación inversa entre conocimiento y victimización por ciberdelito, también se han encontrado diferencias significativas. Cuanto mayor es el conocimiento que presentan los individuos, menor es la tasa de victimización, reforzando así la importancia de los conocimientos para evitar ser víctima de la ciberdelincuencia.

También se han encontrado diferencias significativas entre conocimientos y educación, hallando que a mayor nivel de educación, mejores conocimientos. Por el contrario, aquellos individuos que no han recibido educación en ciberseguridad, presentan las menores tasas de conocimientos. En el análisis de correlaciones entre vulnerabilidad y educación, también se han obtenido resultados significativos, encontrando que a una mayor educación, existe una menor vulnerabilidad. Los resultados coinciden con Zwilling et al. (2020) y Drew (2020) sobre la mejora de la protección mediante la educación y los conocimientos en ciberseguridad. Las importancia de estos resultados reside en el peso que tiene la educación como forma de prevención de la ciberdelincuencia en la población general.

Finalmente, se encontró una relación significativa entre victimización y educación. A un mayor nivel de educación, se reduce la victimización y viceversa. Sorprendentemente, los niveles de victimización no se correlacionan con los de vulnerabilidad. En estudios anteriores, se examinó si el hecho de haber sido víctima en el pasado afectaba a la

ciberhigiene (Cain et al., 2018). Presumiblemente, después de haber sido atacados, los usuarios se comportarían de forma más segura en el futuro y sabrían cómo evitar los ataques (menos vulnerables), pero esta postura no recibió apoyo empírico. El hecho de que un usuario haya sufrido ataques en el pasado no influían en su vulnerabilidad actual. Por lo tanto, esos resultados estarían en la misma línea que los obtenidos en este estudio, ausencia de relación significativa entre vulnerabilidad y victimización.

En relación al objetivo 3, se analizó la influencia de las variables sociodemográficas (sexo, edad y procedencia) con las variables objeto de estudio: vulnerabilidad, conocimientos y victimización. Los resultados hallados apuntan a que existen diferencias significativas en la variable sexo, encontrando mayores conocimientos en hombres que en mujeres. En relación a la procedencia, estas diferencias consisten en que las personas nacionales tienen mejores resultados que las extranjeras. Las extranjeras obtienen peores tasas de conocimientos y son más vulnerables, por lo que demuestra una situación de desventaja frente a los nacionales. Por su parte, en la variable edad, los nativos digitales muestran mejores resultados de educación, conocimientos y vulnerabilidad que los no-nativos digitales. Este hecho se explica en que los jóvenes son los que más saben de tecnología y están más preparados. Los resultados encontrados contrastan con el estudio de Cain et al., (2018), en el que los usuarios de más edad tendían a comportarse de forma más segura que los más jóvenes.

Para responder al cuarto objetivo de investigación encontramos que existe una influencia positiva de la educación sobre los conocimientos, e inversa sobre la vulnerabilidad y la victimización. Las que recibieron educación en ciberseguridad tienen más conocimientos que las que no la recibieron, son menos vulnerables y tienen menores tasas de victimización. Sobre el tipo de educación, también es llamativo que apenas el 17% incluía formación sobre ciberseguridad y ciberamenazas. El resto de individuos recibieron educación sobre alguno de los 2 aspectos en solitario. Como limitaciones, señalar que las cuestiones relacionadas con la educación, la victimización y la sensación de seguridad se hicieron de forma genérica sin especificar formas concretas. De cara a futuras investigaciones, sería interesante profundizar en las diferencias según tipos de victimización, analizar mejor los niveles de educación y consultar de una forma más extensa sobre la sensación de seguridad.

Como conclusiones, se puede afirmar que se confirmó así la hipótesis de que recibir educación mejora los conocimientos y reduce la vulnerabilidad y la victimización. Actualmente, se defiende la idea de que la mayor parte de la población debe tener estos conocimientos mínimos en ciberseguridad, sin embargo, los resultados demuestran que una parte importante de individuos consultados carecen de ellos. También se muestra

fundamental la atención a las personas mayores de 65 y las personas extranjeras, que son la población más vulnerable ante las ciberamenazas. Además, otra consecuencia de no recibir educación en ciberseguridad es que puede generar una sensación de insegurad , tal y como se ha detectado. Por lo tanto, para reducir la victimización, la vulnerablidad y la sensación de inseguridad, se deben aumentar los esfuerzos de las instituciones en fomentar y mejorar la educación en ciberseguridad, concienciar sobre las ciberamenazas y prestar una mayor atención a los colectivos menos protegidos.

5. Referencias

Buelga, S., Cava, M.J., & Musitu, G. (2010). Cyberbullying: victimización entre adolescentes a través del teléfono móvil y de internet. Psicothema*, 22,* 784-789

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: a realist review. Exp. Gerontol. 159, 111678 https://doi.org/10.1016/j.exger.2021.111678

Cain, A., Edwards, M., & Still, J. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Old Dominion University, Department of Psychology, Norfolk, VA 23529, USA

Cook, D., Szewczyk, P., & Sansurooah, K. (2011). Seniors Language Paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens. Paper presented at the 9th Australian Information Security and Management Conference, Citigate Hotel, Perth, Western Australia

Drew, J.M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research, Policy and Practice. Retreived from: http://hdl.handle.net/10072/393427

DSN. (2019). Estrategia Nacional de Ciberseguridad 2019. Departamento de Seguridad Nacional, España. Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Estévez, A., Villardón, L., Calvete, E., Padilla, P., & Orue, I. (2010). Adolescentes víctimas de cyberbullying: prevalencia, y características. Behavioral Psychology/Psicologia Conductual. 1. 73-89. Recuperado de https://www.researchgate.net/publication/261362739_Adolescentes_victimas_de_cyberbullying_prevalencia_y_caracteristicas

Fernández-Montalvo, J., Peñalva, A., & Irazabal, I. (2015). Hábitos de uso y conductas de riesgo en Internet en la preadolescencia. Comunicar, XXII(44),113-120.[fecha de Consulta 9 de Marzo de 2022]. ISSN: 1134-3478. Disponible en: https://www.redalyc.org/articulo.oa?id=15832806012

García-Guilabert, N. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. IDP. Revista de Internet, Derecho y Política. N.º 22, págs. 59-72. UOC. http://dx.doi.org/10.7238/idp.v0i22.2969.

Gamito, R., Aristizabal, P., Vizcarra, M., & León, I. (2020) Seguridad y protección digital de la infancia: retos de la escuela del siglo XXI. Educar , vol. 56(1) 219-237

Gudiño, D. (2018). Los riesgos de las redes sociales y su prevención en los mayores. Servicio de Publicaciones de la Universidad de Extremadura, 855-866

Hadlington, L. & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. Policing: A Journal of Policy and Practice, April, 1-14

Ismailova, R., & Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2015.1132800

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2022). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. Observaciber. https://www.observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1712269

IV. DISCUSIÓN GENERAL Y CONCLUSIONES

1. Discusión general

En esta investigación se ha planteado la cuestión de si se está consiguiendo prevenir a la población general ante la ciberdelincuencia mediante la educación en ciberseguridad. También el cómo se está poniendo en marcha la estrategia educativa en la materia, las relaciones entre la educación y la victimización y cuáles serían las mejoras que se podrían hacer. Se realizó una revisión de la literatura científica, una revisión sistemática sobre las técnicas, un análisis bibliométrico, una consulta a expertos y se administró un cuestionario a 229 participantes. Tras el análisis de los resultados obtenidos, se realizará la discusión de los mismos, relacionándolos con las preguntas, objetivos e hipótesis de partida. Por último, se expondrán cuáles son las conclusiones más relevantes, las limitaciones encontradas y algunas propuestas para futuras investigaciones.

1.1. ¿Cuál es la situación de la educación en ciberseguridad orientada a la población en general?

Esta pregunta planteada se corresponde con 3 objetivos, en primer lugar, explorar los distintos proyectos implementados y los resultados obtenidos, atendiendo a la diferencia entre educación a nivel básico y avanzado. En segundo lugar, realizar un análisis descriptivo mediante la recopilación de bibliografía , analizar la evolución de la cuestión objeto de estudio, los principales autores, teorías y estudios realizados. Por último, el objetivo de recopilación y análisis de la literatura reciente sobre la educación en ciberseguridad y el análisis bibliométrico de los mismos.

Cuando hablamos de la situación de la educación en ciberseguridad, tenemos que plantearnos lo siguiente: ¿Por qué poner el foco en la ciudadanía para prevenir el ciberdelito y no en el ciberdelincuente?. Dentro de la delincuencia tenemos los delitos tradicionales cometidos en el espacio físico donde estaría toda aquella criminalidad habitual. En el caso de España, el mayor volumen lo ocupan los delitos patrimoniales (robos, hurtos, etc.). Es una delincuencia sobre la que se puede intervenir sobre el delincuente con planes de reinserción social, previniendo la comisión del delito, mejorando los espacios, instalando medidas de seguridad, presencia de FCSE, etc. Sin embargo, cuando hablamos de ciberdelincuencia, nos debemos mover de marco teórico y adaptar todo lo que se conoce hasta el momento para poder adaptar las estrategias y medidas encaminadas a prevenirla. El espacio, que ya no es físico, sino virtual, el

tiempo, que deja pasa a ser asíncrono, y la distancia entre el delincuente y la víctima, suponen cambios a los que hay que enfrentarse y readaptar la respuesta por parte de las instituciones y la sociedad en general.

Un dato de especial relevancia en referencia a esto es que tan solo en España la impunidad de los ciberdelitos conocidos es del 99,5% ya que las 1671 sentencias condenatorias solo representan el 0,5% de los casos (López et al., 2021). La dificultad y complejidad de averguación de la identidad de delincuente, el carácter transnacional de gran parte de estos hechos en el que la víctima está aquí, pero el cibercriminal muchas veces está en Rusia, Europa del Este o China (con las barreras que ello supone), hacen que ese modo tradicional de operar de la justicia quede obsoleto. Ya no podemos detectar, investigar, identificar, enjuiciar y condenar de un modo sencillo, para posteriormente reeducar y reinsertar al delincuente como medida de prevención de la reincidencia. Deben tener mayor peso las otras estrategias de cara a prevenir la delincuencia, orientarse de cara al Control Social, por ejemplo, implementando estrategias con personal técnico especializado para proteger infraestructuras críticas, redes públicas, etc. Pero existe otra vía complementaria que permitiría reducir el porcentaje de incidencia, la intervención sobre las potenciales víctimas para protegerlas.

Esta estrategia es en muchas ocasiones cuestionadas, sin embargo, no se puede defender o criticar una estrategia sin tener en cuenta el tipo de delito. No es igual hablar de prevención en violencia de género, que en el radicalismo violento, los delitos contra el patrimonio, el narcotráfico o los homicidios. Según el tipo de fenómeno criminológico, el perfil del delincuente, víctima, factores causales de la criminalidad, etc. la capacidad que se tenga para prevenir, según qué estrategia se tome, será distinta. En el caso de la ciberdelincuencia, es clara la dificultad que supone enjuiciar a los criminales y poder intervenir para su reinserción. Viendo los datos del aumento exponencial de la victimización por ciberdelitos (29.000 en 2011 a 240.000 en 2021), también queda más que claro que lo que se está haciendo es insuficiente para combatir la ciberdelincuencia. Por lo tanto, se debe aprovechar todas las medidas y estrategias posibles, siendo medidas complementarias y no excluyentes.

La medida de proteger a las víctimas es una de las 3 estrategias posibles que existe. Comparte su espacio junto con la prevención sobre los medios de control y sobre los delincuentes, pero que en el caso de la ciberdelincuencia tiene una cualidad particular. Esta capacidad de protección a la víctima va asociada a un mayor conocimiento y concienciación de los peligros. Si nos vamos a la delincuencia tradicional, el tener una doble cátedra en criminología y derecho penal, influirá poco en ser víctima de un atraco retirando dinero de un cajero. Por el contrario, cuando hablamos de cibervictimización,

si tenemos en cuenta que una persona ha podido recibir un curso básico de horas sobre autoprotección, con creación de contraseñas seguras, se ha concienciado de la importancia de no repetir passwords, ha aprendido a identificar el phishing y es conocedora de las ciberamenazas, sí es probable que la vulnerabilidad y la potencialidad que tiene como víctima disminuya frente a alguien que desconoce y vive despreocupado de todo lo anterior.

Es por todo ello, que el peso que puede tener esta estrategia de prevención sobre la víctima es mayor. Al igual que nos formamos en educación vial para poder conducir, debemos formarnos en educación en ciberseguridad para navegar en internet. Además, al igual que nos concienciamos en los peligros al volante, debemos concienciarnos en la ciberdelincuencia en internet. Si miramos a nuestro alrededor podemos ver claramente esta falta de educación y concienciación, en los que se piensa “yo no hago cosas importantes en internet, yo no puedo ser víctima de ningún ciberdelito”. Otro símil sería en la pandemia del COVID-19, cuando los expertos afirmaban que no es más eficaz que el 10% ciento de la población use las mejores mascarillas del mercado, sino que el 90% de la gente use mascarillas, aunque sean de baja calidad. En la cuestión de la ciberseguridad, ciertamente es necesario que exista ese 10% de la población que tenga una formación avanzada en ciberseguridad para poder protegernos a todos. Pero también es necesario que el 90% de la población restante (la población general), tenga unos conocimientos básicos de autoprotección.

Los resultados obtenidos en el análisis bibliométrico y de contenido mostraron grandes diferencias en el volumen de producción entre la educación orientada a personal especializado (con funciones en ciberseguridad) frente a la educación orientada a la población no-técnica, confirmando así la H2 planteada. También se confirmó la preponderancia de EEUU y el rápido crecimiento de la producción científica en la última década. Se encontró un aumento del interés en aspectos técnicos frente a educativos y sociales en los últimos años. En cuanto a las diferencias de producción desde CCSS y ciencias se halló una gran asimetría, siendo las ciencias las que más investigaciones generaron. Adicionalmente, se encontraron diferencias entre la educación en ciberseguridad y la educación en ciberdelincuencia, siendo la primera más abundante y dirigido a un perfil más avanzado que la segunda.

A raíz de la revisión de la literatura científica se ha encontrado que existen aportaciones multidisciplinares sobre el área de estudio. En gran medida, se han orientado a estudiar el peso de distintas variables y factores sobre el riesgo de victimización. Por lo general, se defiende que los conocimientos y la capacitación son elementos fundamentales para la protección de la ciudadanía. La educación, como forma de transmisión y preparación

de dichos conocimientos, se muestra una herramienta clave en poder empoderar a la población no-técnica y prevenir la victimización. Por todo ello, según la literatura científica, se confirma la H1. La oferta educativa reglada principalmente se enfoca a un nivel avanzado, con estudios dirigidos al alumnado de titulaciones técnicas, másteres y cursos de especialización. Por otra parte, las insitituciones y, secundariamente, el sector privado, han puesto en marcha iniciativas y campañas dirigidas a educar a la población no-técnica. Aunque efectivamente se están haciendo cada vez más esfuerzos, a día de hoy parece insuficiente, teniendo en consideración las altas tasas de victimización y ciberdelincuencia que muestran las estadísticas.

La literatura defiende el crucial papel que juega la educación. En primer lugar, aportando conocimientos, y en segundo lugar, mejorando la concienciación. Por ejemplo, McQuade (2006) afirma que una gran oportunidad para minimizar los delitos informáticos a través de la "*conciencia pública, educación formal y capacitación profesional*", reafirmando así su apuesta por el papel de la educación en ciberseguridad, concienciación y capacitación para minimizar delitos informáticos. En la misma línea, Choi & Lee (2017) lanzan la siguiente recomendación "*La esperanza es que la educación sobre los peligros potenciales de Internet y la violencia cibernética interpersonal induzca una actividad online y un compromiso más responsable*". Por lo tanto, también señalan a la educación como una variable determinante de cara a incidir en las condutas de riesgo y la autodefensa de los usuarios.

La literatura científica encontrada y los resultados del análisis bibliométrico encajan con las respuestas aportadas por los expertos. En el apartado de consulta, dichos expertos, se recogieron sus opiniones y percepciones basadas en amplia experiencia y formación. De las respuestas obtenidas se muestra una realidad que no se corresponde con las necesidades a las que se enfrenta la sociedad. Aunque son necesarios perfiles procedentes de distintas áreas, incluidas las Ciencias Sociales, la realidad es que por lo general predominan los perfiles técnicos. La falta de equipos interdisciplinares con personas procedentes de derecho, criminología, psicología, sociología o ciencias de la educación pueden provocar una carencia de otras perspectivas o conocimientos de gran importancia a la hora de abordar la ciberdelincuencia. Este hecho va en la línea de lo que afirman algunos autores (Sánchez et al., 2022; López et al., 2021; Ghernaouti-Helie, 2009) cuando dicen que se requieren enfoques interdisciplinares.

La percepción de los expertos sobre la ciudadanía es clara: existe una gran falta de concienciación, conocimientos y preparación por parte de las personas no-técnicas para protegerse a sí mismas y a sus familias. Esta carencia se refleja en las estadísticas de ciberdelincuencia, que van en aumento cada año y con previsiones de que a la larga los

delitos online puedan superar a los tradicionales (offline). Adicionalmente, se añade la falta de adaptar las técnicas y estrategias educativas al ámbito y aumentar la educación dirigida a la población general, no solo la dirigida a personal técnico o avanzado. Este punto expuesto por los expertos también corroboran nuestra H2. Parece necesario emplear métodos distintos y adaptar los contenidos a un lenguaje sencillo para que pueda ser comprensible a la ciudadanía.

En la Revisión sistemática también se identificaron los perfiles científicos o áreas de estudio de los autores en dichas investigaciones. Los resultados mostraron la supremacía de los perfiles procedentes de ciencias STEAM, especialmente de ciencias computacionales e informática. Los perfiles procedentes de CC.SS. son escasos, como sería el caso de psicología, criminología, sociología o ciencias de la educación. Es contradictorio con la idea de que deben estar presentes perfiles con conocimientos en pedagogía, aprendizaje y del el comportamiento humano en general. Además, cuando se habla de víctimas, delincuentes, heurísticos, factor del miedo, vulnerabilidad, capacitación, ciberresiliencia, error humano, etc. estamos dentro del área de estudio de estas ciencias. La riqueza de poder tener distintas visiones, metodologías, enfoques y conocimientos, permitirá abordar la cuestión de la educación en ciberseguridad orientada a población no-técnica de un modo completo y más adaptado a la realidad.

Finalmente, en esta revisión de la literatura, se halló que son más abundantes las técnicas educativas que se orientan únicamente a la ciberseguridad frente a las que incluyen también aspectos sobre ciberdelincuencia. La relevancia de este hecho es que, la ciberseguridad, como elemento único, puede no ser suficiente a la hora de prevenir la ciberdelincuencia en la población. Si solamente se da formación en medios y herramientas para poder protegerse, pero no se informa lo suficiente de cuáles son las amenazas reales en el ciberespacio, no estaremos completando totalmente la prevención de los individuos. La clave de esta cuestión es la concienciación. Cuando se informa a la población sobre cuáles son las amenazas existentes, también estamos apelando a una cierta preocupación o miedo moderado, que motivará al individuo y conseguirá que ponga en marcha esos conocimientos de ciberseguridad.

1.2. ¿Cómo se está educando en ciberseguridad, qué técnicas didácticas y proyectos educativos se están poniendo en marcha?

Esta cuestión se corresponde con el objetivo 4, identificar las estrategias y técnicas didácticas para la educación en ciberseguridad. En la revisión de la literatura y la búsqueda de proyectos puestos en marcha se ha hallado un amplio abanico de estrategias educativas, desarrollo de innovaciones en las técnicas didácticas, campañas públicas y proyectos socioeducativos. Actualmente, hay diversas instituciones implicadas, algunas más específicas, como es el caso del INCIBE o la OSI, que tienen una función clave en la educación a la población no-técnica. También las FCSE y otras instituciones, que aunque tienen otras funciones principales, están añadiendo actividades dirigidas a concienciar y educar en materia de seguridad a la ciudadanía. Se han desarrollado planes públicos como la AgendaDigital y también programas de alfabetización digital que incluyen ciberseguridad desde las comunidades autónomas y la Unión Europea.

Tras los resultados hallados en la revisión sistemática, se puede afirmar que las principales técnicas que se están empleando en el ámbito de la educación en ciberseguridad son: la gamificación, el entrenamiento, las técnicas multimétodo, la simulación y los medios audiovisuales. Este conjunto de técnicas van más allá de la educación expositiva tradicional y enfocan la educación como un proceso interactivo en el que la persona participante debe implicarse activamente. La gamificación aplica los conocimientos de la teoría del juego y la teoría del flujo (Deterding et al., 2011; Silic, 2020) a contextos ajenos al juego, con la finalidad de modificar los comportamientos y resultados. Son numerosos los beneficios que presenta en el proceso educativo (mejorar la capacidad de protección, la motivación intrínseca, el aprendizaje, las habilidades de afrontamiento y el cumplimiento de las normas de seguridad).

El entrenamiento es una estrategia para mejorar la capacidad de discriminación, adecuada para aumentar sensibilidad a las señales visuales de engaño y para producir una mejora de las capacidades discriminativas. También es una buena técnica para combinar con otras dentro del multimétodo. Las tareas multimétodo se refieren al uso mixto de varias técnicas de forma conjunta, aunque casi siempre suelen ser la combinación de las técnicas más habituales. El uso mixto de técnicas muestra buenos resultados y permite beneficiarse de los beneficios que aporta cada una de ellas. El hecho de que en la mayoría de ocasiones que se emplea el multimétodo se incluya la gamificación, es otra muestra de la versatilidad y efectividad que tiene la misma. De los

resultados obtenidos se desprende que esta opción resulta de las mejores a la hora de educar en ciberseguridad.

Por último, los campamentos de ciberseguridad o Cybercamp también muestran buenos resultados por ser una actividad inmersiva, con alta socialización y trabajo en equipo. Existen otras técnicas, como el empleo de Robot o Robot Social, las clases prácticas, el Escape Room, las técnicas de E-Learning, los juego de cartas, talleres grupales/ colaborativos, los mapas conceptuales, uso de cómic y la lectura de consejos/ relatos. Para concluir, existen diversas técnicas y metodologías que presentas ventajas y desventajas. Según el perfil al que se dirija, según edad y población deben utilizarse unos u otros, y también encontramos que lo óptimo es el uso mixto de más de una técnica.

1.3. ¿Las víctimas tienen conocimientos sobre la ciberdelincuencia y nociones de ciberseguridad?

Para responder a esta pregunta, se han planteado 2 objetivos. En primer lugar, determinar las diferencias de conocimientos en ciberseguridad entre personas que han sido víctimas de ciberdelitos y personas que no. En segundo lugar, obtener información sobre la capacidad y conocimientos de la población general en ciberseguridad. Para ello, se hizo una revisión de la literatura científica, con especial atención a los informes de entidades públicas. También se realizó un estudio en el que se analizó, mediante un cuestionario, dichas variables y la relación entre las mismas.

Existen distintas teorías para la prevención de la ciberdelincuencia. Entre todas ellas, nos encontramos algunas donde una variable a tener en cuenta es la propia víctima. En el caso de la ciberdelincuencia, por su particularidad, se diferencia de otras formas de delincuencia en múltiples aspectos. Concretamente, muchos de los tipos de ciberdelitos se basan en el error o imprudencia de la víctima, por ejemplo en el caso del phishing, donde al confundir una página ilegítima con una legítima, o al abrir un enlace de un emisor desconocido, se termina siendo víctima de una estafa o robo. La actividad de la víctima tiene un mayor peso a diferencia de otros tipos de delitos como la delincuencia contra las personas, contra la libertad, contra las personas, o formas tradicionales de delitos contra el patrimonio (hurtos o robos en vía pública). No tiene especial relevancia la educación previa de una persona víctima de un robo mediante la “técnica del tirón” o una persona que sufre un hurto de la cartera en el metro. Sin embargo, el saber crear

una contraseña segura sí puede ser importante a la hora de prevenir un robo de nuestras cuentas.

Tras la revisión de la literatura y las teorías en torno a la victimización en línea, se debe destacar la CyberTAR, que es la integración de los conceptos de la Teoría de las Actividades Rutinarias (TAR) a los delitos informáticos y al ciberespacio. Según esta teoría, los ciberdelitos se basan en las redes informáticas para conectar a los delincuentes motivados con objetivos potenciales de victimización en ausencia de una tutela capaz. Considera las oportunidades delictivas como la causa última de los hechos delictivos. La CyberTAR sostiene que la separación de los delincuentes motivados y los objetivos adecuados en el tiempo puede conciliarse, considerando su interacción como "retrasada en el tiempo" (Reyns, 2017).

El encaje de la educación en ciberseguridad y ciberdelincuencia dentro de este marco teórico viene a ser que, si se refuerzan los conocimientos en ciberseguridad y las distintas formas de ciberdelincuencia, la probabilidad de victimización disminuirá. Las conductas imprudentes aumentan la probabilidad de victimización. Por el contrario, disponer de un guardián digital disminuye tal probabilidad (Choi, 2008). Estas variables tienen una especial relación con la educación en ciberseguridad porque incide directamente con los modos en como interactuamos con las TIC y, sobre todo, en cómo nos protegemos externamente adquiriendo software de seguridad.

El elemento central que resultaría de mayor interés de esta teoría explicativa es la idoneidad del objetivo. Este elemento se relacionaría directamente con la educación, ya que está encaminado a proveer a la persona de conocimientos para evitar ser víctima de ciberdelitos. Esas capacidades serán las que harán disminuir la idoneidad y, por lo tanto, reducir la probabilidad de ser víctima. Se suele decir que en ciberseguridad, el eslabón más débil es el factor humano y, en consecuencia, es ahí donde reside la fuerza de la CyberTAR como corriente explicativa y el valor de la educación en relación con el objetivo idóneo.

En el estudio realizado en esta investigación, se ha encontrado un nivel bajo de conocimientos en la población consultada. Dichos conocimientos aportan una capacitación que permite a los individuos defenderse, sin embargo, esa carencia encontrada les deja en una situación de mayor vulnerabilidad. Además, los niveles de educación son bajos, ya que el 60% nunca la recibió ningún tipo de formación. El porcentaje de victimización es elevado (60,7%) en comparación a otros estudios, 24% y 30% (Buelga *et al.*, 2010; Estévez, *et al.*, 2010). Sin embargo, es una cifra moderada si tenemos en cuenta que existen formas leves de ser víctima de ciberdelitos. En cuanto

a la sensación de seguridad, apenas el 24,5% afirma sentirse segura. Este sentimiento generalizado puede deberse a que, al plantearse las cuestiones sobre ciberamenazas, los individuos han sido más conscientes del desconocimiento que tienen sobre el tema.

Son preocupantes algunos resultados de hábitos en ciberseguridad, por ejemplo, el escaso uso de antivirus en el teléfono móvil. También destaca el desconocimiento de instituciones como el Incibe, la OSI y el IS4K. Estas instituciones son las encargadas de brindar información, materiales didácticos y educación a la población general, sin embargo, no están consiguiendo llegar a la ciudadanía. Cabría cuestionarse si las campañas implementadas por estas instituciones son efectivas cuando la mayor parte de la población afirma no conocerlas. Finalmente, el 37,1% de la población consultada caería en la estafa del Bizum, lo que indica que desconocen aspectos básicos de esta plataforma de pagos y que puede llevarles a ser víctimas de este tipo de delitos.

También se confirmó que existe relación directa entre conocimientos y vulnerabilidad. Aquellos individuos con un mayor de nivel de vulnerabilidad presentan menores conocimientos. Lo mismo sucede al contrario, aquellas personas con más conocimientos tienen una menor vulnerabilidad. Estos datos señalan la importancia de mejorar los conocimientos en ciberseguridad para disminuir la vulnerabilidad ante las ciberamenazas. Sobre la cuestión de si existe una relación inversa entre conocimiento y victimización por ciberdelito, también se han encontrado diferencias significativas. Cuanto mayor es el conocimiento que presentan los individuos, menor es la tasa de victimización, reforzando así la importancia de los conocimientos para evitar ser víctima de la ciberdelincuencia.

Por otra parte, se han encontrado diferencias significativas entre conocimientos y educación, hallando que a mayor nivel de educación, mejores conocimientos. Por el contrario, aquellos individuos que no han recibido educación en ciberseguridad, presentan las menores tasas de conocimientos. En el análisis de correlaciones entre vulnerabilidad y educación, también se han obtenido resultados significativos, encontrando que a una mayor educación, existe una menor vulnerabilidad. Se confirma, por lo tanto, las H1 y H3 en la que se plantea la importancia de la educación y también la relación entre todas estas variables. Las relevancia de estos resultados reside en el peso que tiene la educación como forma de prevención de la ciberdelincuencia en la población general.

Se encontró una relación significativa entre victimización y educación. A un mayor nivel de educación, se reduce la victimización y viceversa. Sorprendentemente, los niveles de victimización no se correlacionan con los de vulnerabilidad. En estudios anteriores,

se examinó si el hecho de haber sido víctima en el pasado afectaba a la ciberhigiene (Cain et al., 2018). Presumiblemente, después de haber sido atacados, los usuarios se comportarían de forma más segura en el futuro y sabrían cómo evitar los ataques (menos vulnerables), pero esta postura no recibió apoyo empírico. El hecho de que un usuario haya sufrido ataques en el pasado no influían en su vulnerabilidad actual. Por lo tanto, esos resultados estarían en la misma línea que los obtenidos en este estudio, ausencia de relación significativa entre vulnerabilidad y victimización.

Cuando se analizó la influencia de las variables sociodemográficas (sexo, edad y procedencia) con las variables objeto de estudio: vulnerabilidad, conocimientos y victimización, se encontró que existen diferencias significativas. En la variable sexo, presentan mayores conocimientos los hombres que las mujeres. En relación con la procedencia, estas diferencias consisten en que las personas nacionales tienen mejores resultados que las extranjeras. Las extranjeras obtienen peores tasas de conocimientos y son más vulnerables, por lo que demuestra una situación de desventaja frente a los nacionales. Por su parte, en la variable edad, los nativos digitales muestran mejores resultados de educación, conocimientos y vulnerabilidad que los no-nativos digitales.

En esta investigación también encontramos que existe una influencia positiva de la educación sobre los conocimientos, e inversa sobre la vulnerabilidad y la victimización. Las que recibieron educación en ciberseguridad tienen más conocimientos que las que no la recibieron, son menos vulnerables y tienen menores tasas de victimización. Sobre el tipo de educación, también es llamativo que apenas el 17% incluía formación sobre ciberseguridad y ciberamenazas. El resto de individuos recibieron educación sobre alguno de los 2 aspectos en solitario.

A través de la consulta a expertos se muestra una realidad que no se corresponde con las necesidades a las que se enfrenta la sociedad. En primer lugar, aunque son necesarios perfiles procedentes de distintas áreas, incluidas las Ciencias Sociales, la realidad es que por lo general predominan los perfiles técnicos. La falta de equipos interdisciplinares con personas procedentes de derecho, criminología, psicología, sociología o ciencias de la educación pueden provocar una carencia de otras perspectivas o conocimientos de gran importancia a la hora de abordar la ciberdelincuencia. También se puede afirmar que la percepción de los expertos sobre la ciudadanía es clara: existe una gran falta de concienciación, conocimientos y preparación por parte de las personas no-técnicas para protegerse a sí mismas y a sus familias. Esta afirmación coincide con la percepción existente en la literatura encontrada (ONSTI, 2022; López et al.,2021; Zwilling et al., 2022).

A esto se añade la falta de adaptar las técnicas y estrategias educativas al ámbito y aumentar la educación dirigida a la población general, no solo la dirigida a personal técnico o avanzado. Por último, analizando todos los resultados de forma conjunta, existe una idea general compartida por los expertos: hay una falta de más y mejores estrategias de educación, más divulgación y visibilización de la problemática, una mejor adaptación de los medios educativos y más énfasis en concienciar sobre las ciberamenazas. Las políticas y estrategias que se implementan por parte de las instituciones son las responsables directas a la hora de mejorar esta autoprotección. Por lo tanto, es de especial relevancia que la administración pública esté actualizada y pueda reajustar su respuesta de acorde con la realidad vigente. En caso contrario, esa necesidad detectada se convertirá en victimización con el paso del tiempo.

1.4. ¿Cómo se podría mejorar la estrategia de educación en ciberseguridad?

En el caso de la estrategia para prevenir la ciberdelincuencia se debería seguir el ejemplo de la seguridad vial. Si seleccionásemos una muestra representativa de la sociedad que no tuviese carnet de conducir ni conocimientos en educación vial y, por otro lado, seleccionásemos una muestra de personas con carnet de conducir, está claro que habría diferencias en las cifras de accidentes entre el primer grupo y el segundo. Independientemente de la situación de las carreteras, la buena señalización u otras variables ajenas a la persona, la educación vial será un elemento relevante para explicar esa diferencia. Del mismo modo, aquellas personas que hayan tenido una educación en ciberseguridad, que hayan sido concienciadas en los peligros existentes en la red, conozcan la ciberdelincuencia y sus distintas formas, en qué consisten, cómo funcionan y cómo detectarla, tendrán una menor tasa de victimización.

A día de hoy existen unos conocimientos estandarizados y muy bien establecidos sobre qué debe saber una persona para poder obtener el carnet de conducir, sin embargo, no ocurre lo mismo en ciberseguridad. No existe nada parecido a un “carnet para navegar en internet” ni existen escuelas con unos contenidos establecidos por ley para poder tener una navegación segura y proteger nuestros dispositivos. Deberían implementarse programas de clases prácticas en las que poder realizar simulacros, con situaciones controladas en las que podamos hacer frente a ciberamenazas en un ambiente controlado y supervisado.

Si bien es cierto que ya se están impartiendo talleres, seminarios y cursos formativos, en general, se efectúa de un modo fragmentado en distintas instituciones y organismos. Tampoco existe un estándar de contenidos orientado a la población general o un catálogo de contenidos mínimos, al igual que existen por ley en otros ámbitos. Al ser un área reciente, no se debe crear solamente un modelo de educación para las nuevas generaciones en las escuelas y centros de secundaria para educar a los nuevos usuarios de internet, también es necesario un plan de choque inicial orientado a las personas adultas que no han recibido esa educación en ningún momento.

Siguiendo el ejemplo de la alfabetización, según la UNESCO en España la tasa de alfabetización es del 98,44%. ¿A quién se alfabetiza entonces? A los niños en los centros escolares, que son los que parten de 0. Sin embargo, no es necesario hacerlo en adultos porque ya tuvieron una educación primaria en su momento. En el caso de la ciberseguridad, nos encontramos que la mayor parte de la sociedad no ha recibido una educación formal y regulada. Por lo tanto, es necesario incluir los contenidos en el currículum educativo, o al menos establecer unos contenidos mínimos de modo informal (por ejemplo, con charlas de entes externos a los centros). No puede limitarse únicamente a expertos en ciberseguridad, ciencias computacionales, informática e ingenierías, sino que debe ser una tarea multidisciplinar, en donde se incluyan ramas que puedan aportar distintos conocimientos y experiencias: Ciencias de la educación, psicología de la educación, sociología, criminología etc.

En la escuela y el instituto se están impartiendo charlas del Cuerpo Nacional de Policía y Guardia Civil, pero sería necesario añadir en el propio currículum escolar una asignatura de ciberseguridad. Eso pensando en el futuro, pero también existe mucha gente que no tiene o no ha tenido contacto con las instituciones, que no ha tenido esa formación en su escolarización, y que no está en empresas en donde se imparte esa formación a sus trabajadores. También existen perfiles de especial vulnerabilidad como la tercera edad, personas con discapacidad intelectual o personas extranjeras. Al igual que como señalan algunos autores (Miró, 2021), es en esa población en la que es necesario aumentar la actuación, y es ahí donde puede tener un especial valor y relevancia el tercer sector.

El tercer sector, que es el tejido asociativo conformado por entidades sociales, Ongs, asociaciones y entidades públicas que trabajan directamente con la ciudadanía en cuestiones sociales, son las que pueden tener un rol destacado en esa transmisión. Están en contacto con las instituciones y a su vez en contacto directo con la ciudadanía. Es de especial relevancia, que muchas de estas entidades tienen contacto directo con personas que no están involucradas en otras organizaciones, como puedan ser:

instituciones educativas públicas, privadas, empresas, etc. El tercer sector llega a personas extranjeras en situación regular, en situación irregular, de bajos recursos, solicitantes de asilo y refugiados, personas en situación de calle, con situaciones de vulnerabilidad, desempleadas, etc. y que pueden tener una mayor vulnerabilidad ante la ciberdelincuencia.

Actualmente, algunas entidades como los ADL y las oficinas de empleo de las comunidades autónomas, están impartiendo cursos de alfabetización digital en donde se incluyen contenidos de ciberseguridad. También desde los ayuntamientos y comunidades autónomas se han hecho iniciativas formativas para poder abarcar la educación en ciberseguridad y alfabetización digital. Sin embargo, existe un enorme potencial en todo el tejido asociativo que tiene larga y extensa experiencia en realizar cursos y talleres de todo tipo, y que podrían también absorber estas funciones de educación en ciberseguridad. Sobre todo, en colectivos que sean más difíciles de acceder por los canales más habituales.

En cuanto a las propuestas de mejora por parte de los expertos consultados, hay consenso sobre que se deben mejorar y aumentar las campañas de divulgación dirigidas a la población, incluyendo información sobre ciberamenazas y ciberdelitos (con especial atención a las estafas), medidas de autoprotección y una atención a determinados perfiles. Señalan que existe una falta de más y mejores estrategias de educación, más divulgación y visibilización de la problemática, una mejor adaptación de los medios educativos y más énfasis en concienciar sobre las ciberamenazas. Las políticas y estrategias que se implementan por parte de las instituciones son las responsables directas a la hora de mejorar esta autoprotección. Por lo tanto, es de especial relevancia que la administración pública esté actualizada y pueda reajustar su respuesta de acorde con la realidad vigente, por ejemplo, reformulando las campañas de divulgación o mejorando las técnicas educativas. En caso contrario, esa necesidad detectada se convertirá en victimización con el paso del tiempo.

Es de destacar la importancia que tiene la adaptación de la educación a las poblaciones específicas a las que se dirige. En cuanto a niños y adolescentes, las técnicas empleadas más habituales son las técnicas de gamificación, en algunos casos adaptadas de modo específico para esos colectivos. El empleo de juegos tiene un componente motivador muy grande en estos colectivos y, sobre todo, consigue un equilibrio necesario entre aprendizaje y entretenimiento. También son especialmente útiles los materiales audiovisuales y los cybercamps. Los materiales audiovisuales fomentan la activación de distintos sentidos y crean estímulos visuales y auditivos. Estas cualidades permiten mejorar la motivación y la atención en la infancia frente a la

exposición oral o los textos. En el caso de los cybercamps, estos permiten crear un entorno educativo completo con inmersión educativa prolongada y compartida.

Las limitaciones actuales en la educación, en general, apuntan a una falta de concienciación. En muchos casos, no es tanto la falta de conocimientos, como que es la ausencia de motivación para poner en marcha dichos conocimientos. En consecuencia, es necesario tener en cuenta las limitaciones e incluir en los planes de educación la concienciación de cara a las ciberamenazas. Debe abarcar todos los niveles formativos, desde el preescolar hasta el universitario (dirigiéndose a la ciudadanía general, además de a personal especializado), que cuente con participación pública y privada, que sepa absorber la experiencia y conocimiento de otros países y que involucre a los ministerios clave: de educación, cultura, industria, etc. Finalmente, señalan el aspecto crucial que debe regir la educación en ciberseguridad: implicar el factor educativo a todos los niveles sociales. Son los gobernantes los que deben tomar las decisiones sobre las políticas públicas de ciberseguridad, sin embargo, el peso de la educación no debe caer sobre un único actor. La educación debe ser transversal, la cuestión a decidir sería entonces cuál es el peso que debe jugar cada uno de ellos.

Otras recomendaciones son: que los esfuerzos en educación deben centrarse en gran medida en el riesgo de descargar archivos, ya que descarga de archivos está asociada tanto a la victimización por spam como por estafa; que la educación sea lo más personalizada posible; hacer hincapié en los riesgos existentes; impartir la formación de manera práctica disponiendo cada alumno de dispositivos para practicar las técnicas y, finalmente, incluir casos reales contados por el formador y otros testimonios de víctimas. La formación deberá estar apoyada por un documento sencillo y práctico, con recursos e información de interés, así como remarcando las ideas clave que se trasladará a los menores, tanto en formato electrónico como en papel.

En lo que respecta a los jóvenes y adultos, gran parte de las técnicas que se han implementado han seguido la línea de la gamificación, ya que es garante de buenos resultados. También nos encontramos el entrenamiento y la simulación como las grandes apuestas para poder educar y proteger a estos colectivos. El entrenamiento y la simulación van muy unidos, suelen incluir ejemplos de ciberataques ante los que el participante debe protegerse. Mediante ensayo y error y con mensajes de feedback, se van mejorando los conocimientos y la capacidad de defensa. También permiten al usuario/a habituarse al lenguaje del ámbito, al modus operandi de los ciberdelincuentes, identificar y detectar contenidos sospechosos o fraudulentos y aprender a reaccionar ante ellos.

Finalmente, debe haber una presencia interdisciplinar en todo el proceso. Las ciencias relacionadas con la computación, las nuevas tecnologías, la comunicación, ingenierías o la informática tienen un papel principal y determinante en la ciberseguridad. Sin embargo, cuando hablamos de educación en ciberseguridad orientado a la población general, tienen un rol principalmente de contenidos, diseñando y seleccionando cuáles deben ser aquellos elementos necesarios para una correcta protección. En cuanto a los métodos, son las ciencias de la educación, la pedagogía, la didáctica o la psicología de la educación las que tienen un mayor peso, ya que establecen el cómo hacer llegar a la población ese contenido. Es el deber de estas ciencias el poder adaptar de un modo óptimo el contenido a la población objetivo según edad, educación previa, particularidades del aprendizaje, etc.

Como limitaciones, señalar que las cuestiones relacionadas con la educación, la victimización y la sensación de seguridad del cuestionario se hicieron de forma genérica sin especificar formas concretas. En el análisis de expertos, las limitaciones del estudio fueron la escasa participación de los expertos consultados. De los 42 expertos a los que se les envió el cuestionario, tan solo 10 respondieron. Además, la redacción de las preguntas de investigación siempre pueden incluir sesgos al dirigir la investigación (y en este caso las respuestas de los expertos). Otra limitación es la capacidad de generalizar los resultados del cuestionario a la población general, ya que se trató de una muestra de 229 participantes. También añadir que es un tema que evoluciona con gran rapidez y requiere de actualización constante, con muchos cambios en poco tiempo. Se publican numerosos artículos y se ponen en marcha nuevas políticas y campañas dirigidas a este ámbito.

Para futuras investigaciones, sería interesante profundizar en formas concretas de mejorar las campañas de educación en ciberseguridad y en cómo redefinir las estrategias actuales. Se debe estudiar mejor los efectos de las distintas técnicas para optimizar dichas campañas según los perfiles, contenidos y formas que deben incluir. Se debería estudiar la implementación de programas pilotos encaminados a la concienciación e incluir entidades del tercer sector para facilitar que llegue a la ciudadanía. También ampliar la información sobre metodologías concretas que perfeccionen la enseñanza y el aprendizaje de ciberseguridad en la población general. Finalmente, sería interesante profundizar en las diferencias según tipos de victimización, analizar mejor los niveles de educación y consultar de una forma más extensa sobre la sensación de seguridad.

2. Conclusiones generales

Los resultados en su conjunto van en la misma línea, encontrando que la educación en ciberseguridad/ciberdelincuencia es un elemento clave para prevenir la victimización y mejorar los conocimientos de los usuarios. Las medidas puestas en marcha son insuficientes viendo las altas tasas de victimización por ciberdelincuencia. Existe también una necesidad de más perfiles procedentes del ámbito de las ciencias sociales, ya que la educación mejoraría con una mayor interdisciplinariedad y aportaciones desde distintas ramas del conocimiento. Además, los resultados plantear ciertas cuestiones sobre si la producción científica está actuando de un modo acorde a las recomendaciones de muchas estrategias nacionales de seguridad. Estas estrategias defienden la creación de una cultura de ciberseguridad, en donde la población general tenga conocimientos para autoprotegerse de la ciberdelincuencia. Sin embargo, gran parte de la educación se dirige a personal técnico y no tanto a la ciudadanía no-técnica.

En cuanto a la forma de educar, se ha encontrado que la gamificación, el entrenamiento, la simulación, el multimétodo y los medios audiovisuales son las técnicas más habituales. De ellas, las que obtienen mejores resultados de eficacia son la gamificación y el multimétodo. En líneas generales, los beneficios de emplear estas técnicas son: la mejora de la motivación intrínseca, asentar los conocimientos, conseguir valoraciones muy positivas de los participantes y mejorar la atención frente a la educación tradicional (expositiva). También se destaca la importancia de adaptar las técnicas a la población objetivo en función de variables sociodemográficas (edad, sexo, procedencia y colectivo vulnerable).

A raíz del estudio mediante cuestionario, se confirmó la hipótesis de que recibir educación mejora los conocimientos y reduce la vulnerabilidad y la victimización, planteamiento respaldado en la revisión de la literatura científica. Actualmente, se defiende la idea de que la mayor parte de la población debe tener estos conocimientos mínimos en ciberseguridad, sin embargo, los resultados demuestran que una parte importante de individuos consultados carecen de ellos. Otra consecuencia de no recibir educación en ciberseguridad es que puede generar una sensación de inseguridad, tal y como se ha detectado. Por lo tanto, para reducir la victimización, la vulnerablidad y la sensación de inseguridad, se deben aumentar los esfuerzos de las instituciones en fomentar y mejorar la educación en ciberseguridad, concienciar sobre las ciberamenazas y prestar una mayor atención a los colectivos menos protegidos.

Referencias

Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. Journal of Medical Internet Research, 22(5). https://doi.org/10.2196/18394

Aggarwaly, A., Rajadesingan, A., & Kumaraguru, P. (2012). PhishAri: Automatic realtime phishing detection on twitter. In Seventh IEEE APWG eCrime researchers summit (eCRS). Las Croabas, Puerto Rico, 22–25 October 2012. http://precog.iiitd.edu.in/Publications_files/AA_AR_PK_eCRS_2012.pdf

Alalwan, J.A. (2018). Fear of cybercrime and the compliance with information security policies: a theoretical study. *Proceedings of the 9th International Conference on E-Education, E-Business, E-Management and E-Learning*. 85–87. https://doi.org/10.1145/3183586.3183590

Alarcón, V. (2017). ¿Qué leyes regulan la ciberseguridad en la Unión Europea y en España?. Signaturit. Recuperado de: https://blog.signaturit.com/es/que-leyes-regulan-la-ciberseguridad-en-la-union-europea-y-en-espana

Alessi S.M. & Trollip, S.R. (2001). Multimedia for Learning: Methods and Development. , Boston, MA:Allyn & Bacon, Inc.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). Information, 11(2), 121. MDPI AG. Retrieved from http://dx.doi.org/10.3390/info11020121

Al-Nemrat A., Jahankhani H., & Preston D.S. (2010) Cybercrime Victimisations/Criminalisation and Punishment. In: Tenreiro de Magalhães S., Jahankhani H., Hessami A.G. (eds) Global Security, Safety, and Sustainability. ICGS3 2010. Communications in Computer and Information Science, vol 92. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-15717-2_7

Alshalan, A. (2009). Cyber-Crime Fear and Victimization: An Analysis of a National Survey.

Amador, A. (2017). Acceso y uso de las TIC en los hogares costarricenses. En A. Salas y M. Guzmán (Coords.), *Programa sociedad de la información y el conocimiento. Universidad de Costa Rica* (pp. 173-210). San José, Costa Rica: Prosic, UCR. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_2017.pdf

Andreatos, A. (2020). Movies as an Aid to Teach Principles of Cybersecurity and Cybercrime in Higher Education. *International Journal of Education and Information Technologies*. 14. 76-82. DOI:10.46300/9109.2020.14.10

Arab, L. E. & Díaz, A. (2015). Impacto de las redes sociales e internet en la adolescencia: Aspectos positivos y negativos. *Revista Médica Clínica Las Condes*, *26*(1), 7-13. doi: 10.1016/j.rmclc.2014.12.001

Árpád, I. (2013). A Greater Involvement of Education in Fight Against Cybercrime. *Procedia - Social and Behavioral Sciences*, 83, 371–377. https://doi.org/10.1016/J.SBSPRO.2013.06.073

Astorga-Aguilar, C. & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare*, vol. 23, núm. 3. Universidad Nacional. CIDE Disponible en: http://www.redalyc.org/articulo.oa?id=194161290017 DOI: 10.15359/ree.23-3.17

Avila Silva, J. (2018). Los menores víctimas de la ciberdelincuencia, medidas preventivas en el ámbito internacional. Advocatus, 15(31), 79-90. https://doi.org/10.18041/0124-0102/a.31.5223

Bacigalupo, S., Bajo, M., Basso, G. J., Cancio, M., Díaz-Maroto, J., Fakhouri, Y., Lascuraín, J. A., Maraver, M., Mendoza, B., Molina, F., Peñaranda, E., Pérez, M., Pozuelo, L., & Rodríguez, D. (2019). Manual de Introdución al Derecho Penal. In *Manual de Introducción al Derecho Penal*. https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DP-2019-110

Bashir, M., Lambert, A., Wee JMC., & Guo B. (20015). An examination of the vocational and psychological characteristics of cybersecurity competition participants. 2015 *USENIX Summit on Gaming, Games, and Gamification in Security Education* (3GSE 15)

Benenson, Z., Dewald, A., Eßer, H., Freiling, F., Müller, T., Moch, C., Voemel, S., Schinzel, S., Spreitzenbarth, M., Stock, B., & Stüttgen, J. (2011). Exploring the Landscape of Cybercrime. Proceedings - 1st SysSec Workshop, SysSec 2011. 10.1109/SysSec.2011.23.

Beuran R., Chinen KI., Tan Y., & Shinoda Y. (2016). Towards effective cybersecurity education and training. *Japan Advanced Institute of Science and Technology.* Recuperado de https://www.jaist.ac.jp/~razvan/publications/effective_cybersecurity.pdf

Bidgoli, M., Knijnenburg, B.P., & Grossklags, J. (2016). When cybercrimes strike undergraduates. *ECrime Researchers Summit, ECrime*, *2016-June*, 42–51. https://doi.org/10.1109/ECRIME.2016.7487948

Bodeau, D. & Graubart, R. (2016). *Cyber Resilience Metrics: Key Observations.* Consultado el 08/02/2020. Recuperado de https://n9.cl/nf8kl

Bossler, A.M., & Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. Journal of Criminal Justice, 38(3), 227–236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Journal of Academy of Accounting and Financial Studies*, 11, 43–56.

Buja, A.G., Wahid, S.D., Rahman, T.F.A., Deraman, N.A., Jono, M.N. & Aziz, A.A. (2021). Development of organization, social and individual cyber security awareness model (OSICSAM) for the elderly. *International Journal of Advanced Technology and Engineering Exploration*, 8(76), 511-519. Advanced Technologies & Aerospace Collection; ProQuest One Academic. https://doi.org/10.19101/IJATEE.2020.762185

Burton, A., Cooper, C., Dar, A., Mathews, L., Tripathi, K.: Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: a realist review. Exp. Gerontol. 159, 111678 (2022). https://doi.org/10.1016/j.exger.2021.111678

Cain, A., Edwards, M., & Still, J. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Old Dominion University, Department of Psychology, Norfolk, VA 23529, USA

Campos, N. (2007). Las ciencias de la educación ¿Cuáles son?. Filosofía de la educación. Recuperado de: http://filo-edu.blogspot.com/2007/12/las-ciencias-de-la-educacion-cuales-son.html

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies* 10, 229–42.

Cárceles, M.M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista Criminalidad*, 57(1), 121-135.

Caro, P., & Moreno, M. (2022). Análisis y ejecución de Malware y Códigos Maliciosos en un entorno controlado. Escola Tècnica Superior d'Enginyeria Industrial de Barcelona. Recuperado de https://upcommons.upc.edu/handle/2117/372262

Cerceda, J., Sánchez, F., Herrera, D., Martínez, F., Rubio, M., Gil, V., Santiago, A.M., & Gómez, M.A . (2019). Estudio sobre la Cibercriminalidad en España. Gabinete de Coordinación y Estudios. Ministerio del Interior, España.

Chadee, D., & Ng Ying, N.K. (2013). Predictors of fear of crime: general fear verses perceived risk. *Journal of Applied Psychology*, 43(1), 1896-1904.

Check Point. (2015). *Security Report*. Consultado el 08/02/2020. Recuperado de https://blog.checkpoint.com/2015/06/16/check-point-2015-security-report-paints-a-picture-of-the-threat-landscape-and-its-not-pretty/

Choi, K. (2010). *Risk Factors in Computer-Crime Victimization*. LFB Scholarly Publishing LLC. Retrieved from https://www.perlego.com/book/2028086/risk-factors-in-computercrime-victimization-pdf

Choi, K. (2008). "Computer Crime Victimization and Integrated Theory: An Empirical Assessment". *International Journal of Cyber Criminology* 2 (1): 308–333. Disponible en: https://www.researchgate.net/publication/238621672_Computer_Crime_Victimization_and_Integrated_Theory_An_Empirical_Assessment

Choi,K., & Lee,J.R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory, *Computers in Human Behavior*. DOI: 10.1016/j.chb.2017.03.061

Chou, Y. (2015). Gamificación procesable: más allá de los puntos, las insignias y las tablas de clasificación . Medios de Octalysis. ISBN 978-1-5117-4404-1.

Cibervoluntarios. (2023). ¿Qué hacemos?. Consultado el 23/05/23. Recuperado de: https://www.cibervoluntarios.org/es/que-hacemos

Clough, J. (2011). Cybercrime. Commonwealth Law Bulletin. 37:4, 671-680 http://dx.doi.org/10.1080/03050718.2011.621277

Clough, J. (2015). Principles of cybercrime. New York City, New York: Cambridge University Press.

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44: 588-608.

Colom, A., & Rodríguez, M. (1996). Teoría de la educación y ciencias de la educación: carácter y ubicación. *Ediciones Universidad de Salamanca*. (8), pp. 43-54

Comisión Europea. (2013). Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. *EUR-Lex.* Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ES:PDF

Comisión Europea. (2023). La Ley de Ciberseguridad de la UE. *Comisión Europea* Recuperado de: https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-act

Congreso. (2021). Respuesta del Gobierno 128926. Secretaría de Estado de Relaciones con las Cortes y Asuntos Constitucionales, Gobierno de España. Recuperado de https://www.congreso.es/entradap/l14p/e12/e_0128926_n_000.pdf

Connolly, C., Maurushat, A., Vaile, D. & Van Dijk, P. (2011). An overview of international cyber-security awareness raising and educational initiatives. Galexia. Consultado el 09/02/2022. Recuperado de https://n9.cl/sqs92

Consejo Europeo. (2023). Ciberseguridad: cómo combate la UE las amenazas cibernéticas. *Web oficial del Consejo de la UE y del Consejo Europeo*. Recuperado de: https://www.consilium.europa.eu/es/policies/cybersecurity/

Cook, D., Szewczyk, P., & Sansurooah, K. (2011). Seniors Language Paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens. Paper presented at the *9th Australian Information Security and Management Conference*, Citigate Hotel, Perth, Western Australia.

Coughlin, T.M. (2017) Cybersecurity Education for Adolescents and Non-Technical Adults. Master's Thesis.

Coz, J. R. (2015). Panorama Internacional en el establecimiento de Estrategias Nacionales de Ciberseguridad. December. Recuperado de: https://www.researchgate.net/publication/258795133_FojonPanorama_Internacional_en_el_establecimiento_de_Estrategias_Nacionales_de_Ciberseguridad

Crescenzi-Lanna, L., Valente, R., & Suárez-Gómez, R. (2019). Aplicaciones educativas, seguras e inclusivas: La protección digital desde una perspectiva ética y crítica *Comunicar*; Huelva Tomo 27, N.º 61, : 93-102. DOI:10.3916/C61-2019-08

Cressato, G. (2017). Ciberbulling y Sexting: Actualidad. Badajoz: Universidad de Extremadura. Tesis doctoral. Recuperado de http://dehesa.unex.es/handle/10662/6476

CSIRT-CV (2023). ¿Qué es el CSIRT-CV?. Consultado el 23/05/2023. Recuperado de https://www.csirtcv.gva.es/

Davara-Fernández, L. (2019). Formación TIC (redes sociales, internet, ciberseguridad, big data, etc.) en casa, en el colegio, en la universidad y en la empresa: características, razón de ser y contenido. Revista Tecnología, Ciencia Y Educación, (12), 89–110. https://doi.org/10.51302/tce.2019.243

DeCusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., ... & Mah, B. (2022). A Cybersecurity Awareness Escape Room using Gamification Design Principles. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference* (CCWC) (pp. 0765-0770)

De Bona, M., & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3407023.3409179

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L. & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics & Informatics*, 35, 1277-1287.

Del Fresno, M., Daly, A. J., & Sánchez-Cabezudo, S.S. (2016). Identificando a los nuevos influyentes en tiempos de Internet: medios sociales y análisis de redes sociales. *Revista Española de Investigaciones Sociológicas* (REIS), 153(1), 23-40

DSN. (2019). Estrategia Nacional de Ciberseguridad 2019. Departamento de Seguridad Nacional, España. Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, 68, 359–367. https://doi.org/10.1016/J.CHB.2016.11.044

Dodel, M., & Mesch G. (2018): Inequality in digital skills and the adoption of online safety behaviors, Information, Communication & Society. DOI: 10.1080/1369118X.2018.1428652

Dondlinger, M.J. (2007). Educational video game design: A review of the literature. *Journal of Applied Educational Technology*, vol. 4, no. 1, pp. 21-31.

Donoso, T., Vilà, R., Rubio, M., & Prado, M. (2016). Perfil de cibervictimización ante las violencias de género 2.0. FEMERIS Vol.1, Núm. 1/2 (2016). Recuperado de: https://e-revistas.uc3m.es/index.php/FEMERIS/article/view/3226

-Dorner, R., Gobel, S., Effelsberg, W., & Wiemeyer, J. (2016). Serious Games. Springer, Cham. https://doi.org/10.1007/978-3-319-40612-1

Drew, J.M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*. Retreived from: http://hdl.handle.net/10072/393427

Drew, J.M., & Farrell, L. (2018). Online victimisation risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Journal of Police Practice and Research: An International Journal*, 19, 537-549.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity theory approach. Theory and Practice in Situational Crime Prevention. *Crime Prevention Studies*, 16, 7e39.

Echeburúa, E., & De Corral, P. (2010). Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: Un nuevo reto. Adicciones, 22(2), 91-96. doi: 10.20882/adicciones.196

EdWeek Research Center. (2020). The State of Cybersecurity in Education in K-12 Schools. Recuperado de https://n9.cl/1uado

Enisa. (2012). Involving Intermediaries in Cyber-security Awareness Raising. Consultado el 09/02/2022. Recuperado de: https://www.enisa.europa.eu/publications/involving-intermediaries-in-cyber-security-awareness-raising

Escuela de Altos Estudios de la Defensa. (2013). Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario». Monografías 137. Consultado el 08/02/2020.

Eur-Lex. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019. *Official Journal of the European Union*. Recuperado de https://eur-lex.europa.eu/eli/reg/2019/881/oj

Ewen, R. B. (2010). An introduction to theories of personality. New York: Psychology Press

Eynde, V. (2021). Derecho Penal europeo y delitos informáticos. Consultado el 14 de septiembre de 2022. Recuperado de https://eynde.es/derecho-penal-europeo-y-delitos-informaticos-2/?lang=es

Fernández-Montalvo, J., Peñalva, A., & Irazabal, I. (2015). Hábitos de uso y conductas de riesgo en Internet en la preadolescencia. Comunicar, *XXII*(44),113-120. ISSN: 1134-3478. Disponible en: https://www.redalyc.org/articulo.oa?id=15832806012

Fernandez-Montalvo, J., Peñalva, A., Irazabla, I. & Lopez-Goni, J. (2017). Effectiveness of a digital literacy programme for primary education students. Culture and Education, 29(1), 1-30. http://doi.org/10.1080/11356405.2016.1269501

Finkelhor, D. (2008). *Childhood Victimization. Violence, Crime, and Abuse in the Lives of Young People.* [artículo en línea]. Oxford, USA: Oxford University Press, pág. 26. http://dx.doi.org/10.1093/acprof :oso/9780195342857.001.0001

Fundación Telefónica. (2016). Ciberseguridad, la protección de la información en un mundo digital. ISBN: 978-84-08-16304-6. Disponible en http://www.fundaciontelefonica.com/publicaciones

Galov, D. (2020). Remote spring: the rise of RDP bruteforce attacks. Kaspersky Retrieved from https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

Gamito, R., Aristizabal, P., Vizcarra, M., & León, I. (2020) Seguridad y protección digital de la infancia: retos de la escuela del siglo XXI. *Educar* , vol. 56(1) 219-237. DOI:10.5565/rev/educar.1113

García-Maldonado, G., Joffre-Velázquez, V. M., Martínez-Salazar, G. J. & Llanes-Castillo, A. (2011). Ciberbullying: Forma virtual de intimidación escolar. *Revista Colombiana de Psiquiatría*, 40(1), 115-130. DOI:10.1016/S0034-7450(14)60108-6

Garcia-Guilabert, N. (2014). Victimizacion de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio. Escuela Internacional de Posgrado. Tesis doctoral. Recuperado de: https://dialnet.unirioja.es/servlet/tesis?codigo=50240&orden=1&info=link

García-Guilabert, N. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. IDP. *Revista de Internet, Derecho y Política*, (22),48-61. ISSN: Disponible en: https://www.redalyc.org/articulo.oa?id=78846481005

García-Fuentes, O., Raposo-Rivas, M., & Martínez-Figueira, M. E. (2023). El enfoque educativo STEAM: una revisión de la literatura. *Revista Complutense de Educación*, 34(1), 191-202. DOI:10.5209/rced.77261

Garcia-Valcarcel, A., Basilotta, V., & Lopez, C. (2014). ICT in Collaborative Learning in the Classrooms of Primary and Secondary Education. *Comunicar*, 42(21), 65-74. https://doi.org/10.3916/C42-2014-06

Gatti, F.M., Brivio, E., & Galimbertim C. (2017). “The future is ours too”: a training process to enable the learning perception and increase self-efficacy in the use of tablets in the elderly. *Educational Gerontology*. 43(4):209-24. DOI:10.1080/03601277.2017.1279952

Generalitat Valenciana. (2022). Proyecto Pilotem CV. Vicepresidencia segunda y conselleria de Servicios Sociales, Igualdad y Vivienda – Generalitat Valenciana. Recuperado de https://inclusio.gva.es/es/web/integracion-inclusionsocial-cooperacion/publicador-de-contenidos/-/asset_publisher/8kjNzmUvx8hO/content/proyecto-pilotem

Ghernaouti-Helie, S. (2009). An Inclusive Information Society Needs a Global Approach of Information Security. 2009 *International Conference on Availability, Reliability and Security*, 658-662. DOI:10.1109/ARES.2009.127

Glenny, M. (2011) Dark market: How hackers became the new mafia. New York: *Ed. Vintage*. ISBN: 9780307476449

Gobierno de España. (2013). Agenda digital para españa. Consultado el 08/02/2020. Recuperado de https://avancedigital.mineco.gob.es/programas-avance-digital/agenda-digital/Paginas/planes-especificos.aspx

Gottfredson, M. & Hirschi, T. (1990). A general theory of crime. Stanford, CA: *Stanford University Press.*

Grupo Atico34. (2020). Oficina de Seguridad del Internauta (OSI). Consultado el 23/05/2023. Recuperado de https://protecciondatos-lopd.com/empresas/oficina-seguridad-internauta-osi/

Gudiño, D. (2018). Los riesgos de las redes sociales y su prevención en los mayores. *Servicio de Publicaciones de la Universidad de Extremadura,* 855-866 ISBN 978-84-09-07198-2. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6765386

H50DigitalPolicial. (2023). Aprobado el plan estratégico contra la cibercriminalidad, estadísticas y nuevas tendencias criminales observadas. *H50 Digital Policial*. Recuperado de https://www.h50.es/aprobado-el-plan-estrategico-contra-la-cibercriminalidad-estadisticas-y-nuevas-tendencias-criminales-observadas/

Hadlington, L. & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. Policing: *A Journal of Policy and Practice*, April, 1-14. DOI: 10.1093/police/pay027

Hairston, J.R., Smith, D., Williams, T., Sabados, W., & Forney, S. (2020). Teaching Cybersecurity to Students with Visual Impairments and Blindness. *Journal of Science Education for Students with Disabilities* 23, 1. Iss. 1, Article 7. DOI: 10.14448/jsesd.12.0007 Recuperado de: https://scholarworks.rit.edu/jsesd/vol23/iss1/7

Hammond, T.C. & Lee, J.K. (2010). Editorial: Digital Video and Social Studies. *Contemporary Issues in Technology and Teacher Education, 10*(1), 124-132. Waynesville, NC USA: Society for Information Technology & Teacher Education. Retrieved September 10, 2023 from https://www.learntechlib.org/primary/p/34125/.

Hellems, F., & Bhatia, S. (2022). Removing the Veil: Shining Light on the Lack of Inclusivity in Cybersecurity Education for Students with Disabilities. SIGCSE 2022 - Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V.2, 1108. https://doi.org/10.1145/3478432.3499114

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime : an empirical foundation for a theory of personal victimization.* Cambridge (Mass.): Ballinger. Recuperado de https://lib.ugent.be/en/catalog/rug01:000508194

Hornetsecurity. (2020). Malware - Definición, tipos y cómo funciona una protección segura. *Hornetsecurity*. Recuperado de https://www.hornetsecurity.com/es/knowledge-base/malware/?_adin=11551547647

Howard, S.K., Yang, J., Ma, J., Maton, K., & Rennie, E. (2018). App clusters: Exploring patterns of multiple app use in primary learning contexts. *Computers & Education*, 127, 154-164. https://doi.org/10.1016/j.compedu.2018.08.021

Huntley, S. (2020). Findings on Covid-19 and online security threats. *Google Threats Analysis Group*. Retrieved from https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats

IBM Security. (2020). 2020 Consumer Small Business Covid-19 Awareness Study. Recuperado de https://www.ibm.com/downloads/cas/ZVNNJNQJ

Im, C.I., & Yeon, Y.K. (2009). Formation Research about Case-based Design Principles for Simulation. *Institute for Educational Technology*, vol. 25, pp. 117-149.

INCIBE (Instituto Nacional de Ciberseguridad de España). (2020). Kit de concienciación. Consultado el 08/02/2020. Recuperado de https://www.incibe.es/protege-tu-empresa/kit-concienciacion

INCIBE (Instituto Nacional de Ciberseguridad de España). (2023). ¿Qué es el Incibe?. Consultado el 24/04/2023. Recuperado de https://www.incibe.es/que-es-incibe

INE (Instituto Nacional de Estadistica). (2018). Encuesta sobre equipamiento y uso de las tecnologías de la información y comunicación en los hogares: Resultados año 2018. Recuperado de https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735576692

Ismailova, R., & Muhametjanova, G. (2016): Cyber crime risk awareness in Kyrgyz Republic, *Information Security Journal: A Global Perspective*. DOI:10.1080/19393555.2015.1132800

Jansen, J. & Van-Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*. Vol. 123, pp. 40-55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Kang, M.H., Kim, H.S., & Lee, J.M. (2011). The Effects of Flow and Cognitive Presence on Learning Outcomes in a Middle School Class using Web-based Simulation. *Korean Association for Educational Information and Media*, vol. 17, pp. 39-61. DOI:10.1016/j.iheduc.2016.04.002

Kim, S.R., Yang, J.H., & Kim, S.B. (2016). A Cybercrime Prevention Program based on Simulation and Quiz Game: Applying Item Response Theory for Effective Information Security Learning. International Journal of Security and Its Applications. 10. 165-180. DOI: 10.14257/ijsia.2016.10.5.16

Kim, Sangkyun. (2014). Star question: Gamification of a reviewing process using self-setting question and game mechanism in undergraduate education. *Social Sciences* (Pakistan). 9. 437-441. DOI:10.3923/sscience.2014.437.441

Kokkinos, C.M., & Saripanidis, I. (2017). A lifestyle exposure perspective of victimisation through Facebook among university students. Do individual differences matter? *Computers in Human Behavior*, 74, 235-245. DOI https://doi.org/10.1016/j.chb.2017.04.036

Letslaw. (2021). Ciberdelincuencia en el código penal. *Letslaw*. Consultado el 13 de septiembre de 2022. Recuperado de https://letslaw.es/ciberdelincuencia/

Leukfeldt, E.R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behaviour*, 37(3), 263-280.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (1995). BOE núm. 281, de 24/11/1995.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.

Lievens, E. (2015). Children, protection of. In Robin, M., & Peng, H. (Eds.), The International Encyclopedia of Digital. *Communication and Society* (pp. 1-5). https://doi.org/10.1002/9781118767771.wbiedcs018

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). Developing a framework for researching children's online risks and opportunities in Europe. Recuperado de http://bit.ly/30ghWuG

López,J., Sánchez, F., Herrera, D., Martínez, F., Rubio, M., Gil, V., Santiago, A.M., & Gómez, M.A . (2021). Estudio sobre la Cibercriminalidad en España. Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad . Ministerio del Interior, España. Recuperado de https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/Informe-Cibercriminalidad-2021.pdf

Marcum, C.D., Ricketts, M.L., & Higgins, G.E. (2010). Assessing sex experiences of online victimisation: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review*, 35(4), 412-437. DOI:10.1177/0734016809360331

Martens, M., DeWolf, R., & DeMarez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, 92, 139-150. DOI:10.1016/j.chb.2018.11.002

Martínez-López, N.M., & Martínez-López, R. (2018). Los jóvenes y la ciberseguridad en zonas rurales del Estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165. *RECAI Revista de Estudios en Contaduría, Administración e Informática*, 7, 14-35. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6881871

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, 9(1), 151-184. https://dx.doi.org/10.5354/0719-2584.2020.53447

McQuade, S.C. (2006). Understanding and managing cyber crime. Boston:Pearson/Allyn and Bacon. Vol.1 No.3.

McLeod, S.A. (2016, Febuary *05).* Bandura - social learning theory. Simply Psychology. www.simplypsychology.org/bandura.html

MDSA2030 (Minsterio de Derechos Sociales y Agenda 2030) . (2021). Estrategia de desarrollo sostenible 2030. Recuperado de 2030 https://www.mdsocialesa2030.gob.es/agenda2030/index.htm

Mendez, A., Perez, E., Hernandez, I., Romero, R., & García, P. (2022). Informe de migración y denuncia segura. Platform for International Cooperation on Undocumented Migrants. Recuperado de file:///C:/Users/Utente/Desktop/url.htm

Miguez, M.I., & Dafonte, A. (2018). La aplicación de cuestionarios de autoevaluación en el aula a través de dispositivos móviles. *Servicio de Publicaciones de la Universidad de Extremadura*, 245-254.

Miró-Llinares, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminología*, núm. 13-07.

Miró-Llinares, F. (2012). El cibercrimen. Fenomenología y criminología de la delinciuencia en el ciberespacio. [artículo en línea]. Madrid: *Marcial Pons,* págs. 91, 122-125. http://dx.doi.org/10.1049/el.2012.2349

Miró-Llinares, F., Drew, J., & Townsley, M. (2020). Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. *International Journal of Cyber Criminology*, 14(1), 139-155. Retrieved from

https://www.proquest.com/scholarly-journals/understanding-target-suitability-cyberspace/docview/2404395082/se-2

Moitra, S. (2005) Developing policies for cyber crime. *European Journal of Crime, Criminal Law and Criminal Justice*, 13(3), 435-464

Montiel, I. (2016). Cibercriminalidad social juvenil: la cifra negra. IDP. *Revista de Internet, Derecho y Política,* 22(22), 119–131. https://doi.org/10.7238/idp.v0i22.2972

Nalin A., Gamagedara, A., & Love, S. (2013) A game design framework for avoiding phishing attacks. *Computers in Human Behavior* 29, n.o 3 706-14. https://doi.org/10.1016/j.chb.2012.12.018

NCIRSC - National center of Incident readiness and Strategy for Cybersecurity. (2013). Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace. Recuperado de: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. Int. J. Cyber Criminol., vol. 5, no. 1, p. 773

NICCS (National Initiative for Cybersecurity Careers and Studies). (2019). Official website of the Department of Homeland Security. Glossary. Consultado el 15/01/2023. Recuperado de https://niccs.us-cert.gov/about-niccs/glossary#C

Nieva, E. (2020). Es clave que la sociedad tenga unas nociones básicas en ciberseguridad. El Correo Gallego 14 sep 2020. Recuperado de https://www.elcorreogallego.es/tendencias/es-clave-que-la-sociedad-tenga-unas-nociones-basicas-en-ciberseguridad-MX4572583

Oksanen, A., & Keipi, T. (2013) Young people as victims of crime on the internet: A population-based study in Finland, Vulnerable Children and Youth Studies, 8:4, 298-309, DOI: 10.1080/17450128.2012.752119

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2022). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. Observaciber. https://www.observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

OSIC (Observatorio Nacional para la Seguridad de la Información y la Ciberseguridad). (2019) Ciberpedia. Consultado el 31/12/2019. Recuperado de https://observatoriociber.org/recursos/ciberpedia/#letra-c

Pérez, A. (1978). Las fronteras de la educación, Edit. Zero, ZYX, Madrid.

Pérez , J., & Merino, M. (30 de junio de 2008). Concepto de pedagogía - Definición, Significado y Qué es. Definicion.de. Última actualización el 21 de mayo de 2021. Recuperado el 21 de febrero de 2023 de https://definicion.de/pedagogia/

Pérez, R. (2016). Adolescencia, socialización y TIC. En R. Pérez y M. Guzmán (Coords.), Programa sociedad de la información y el conocimiento Universidad de Costa Rica (pp. 103-122). San José, Costa Rica: Prosic, UCR . Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/rec ursos/informe_2016.pdf

Power, A., & Kirwan, G. (2014) Cyberpsychology and new media; a thematic reader. *The Free Library*. Recuperado de https://www.thefreelibrary.com/Cyberpsychology

Pulido, G. M., & Rosell, R. R. (2017). Cooperación Público-Privada en el fomento de la cultura de ciberseguridad. Cuaderno de Estrategia IEEE 185, 217-246 http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2017/Cuaderno_185.html

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. Information Management & Computer Security, 20(5), 382–420. http://dx.doi.org/10.1108/09685221211286548

Rader, E., Wash, R., & Brooks, B. (2012). Stories As Informal Lessons About Security. Proceedings of the Eighth Symposium on Usable Privacy and Security July 2012 Article No.: 6 Pages 1–17 https://doi.org/10.1145/2335356.2335364

Ramadhani, A., Bramantoro, T., Khotimah, F.K., Santosa, L.M., Sudiartha, N.C., & Mudara, I.K. (2020). SEIMUT PERSIA: promoting dental and oral health care and physical performance in elderly. Indonesian Journal of Dental Medicine. 3(1):10-12

Redecker, C. (2017). European framework for the digital competence of educators. DigCompEdu. JCR Science for Policy Report. http://bit.ly/2JhGb6l

Resnick, M y Rosenbaum, E. (2013). Designing for tinkerability. En Honey, M., y

Kanter, D.E. (ed.) *Design, make, play: Growing the next generation of STEM innovators*. London: Routledge.

Robila, S. A., Ragucci, J. W. (2006). Do not be a phish: steps in user education. In 11th annual SIGCSE conference on innovation and technology in computer science education, Bologna, Italy, June 2006, 26–28. doi: 10.1145/1140124.1140187

Rocheleau, J., Chalghoumi, H., Jutai, J., Farrell, S., Lachapelle, Y., & Cobigo, V. (2021). Caregivers' Role in Cybersecurity for Aging Information Technology Users with

Intellectual Disability. *Cyberpsychology, Behavior, and Social Networking*. DOI: 10.1089/cyber.2020.0572

Rodríguez, J.A., Oduber, J., & Mora, E. (2017). Actividades rutinarias y cibervictimización en Venezuela. *URVIO, Revista Latinoamericana de Estudios de Seguridad,* (20),63-79.[fecha de Consulta 10 de Febrero de 2021]. ISSN: 1390-3691. Disponible en: https://www.redalyc.org/articulo.oa?id=5526/552656641006

Romero, H., & Rojas, E. (2013). La Gamificación como participante en el desarrollo del B-learning. *Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology*. Consultado el 09/02/2022. Recuperado de: https://n9.cl/mn81u

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs*, 2(4), 328-335.

Rifon. (2005). Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *The Journal of Consumer Affairs*., 39(2), 339–362. https://doi.org/info:doi/

Rincón, H., & Prieto, J. A. (2020). Portal Web con sistema clasificador de noticias para apoyo al fomento de la ciberseguridad . 8, 120–127.

Ritterfeld, U., Cody, M., & Vorderer, P. (2009). Serious Games: Mechanisms and Effects. Routledge, New York

Sánchez, F., Martínez, J. E., & Téllez, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *Methaodos Revista De Ciencias Sociales*, 10(2), 243–258. https://doi.org/10.17502/mrcs.v10i2.577

SANS Institute. (2016). Security Awareness: A Tale of Two Challenges. Consultado el 09/02/2022. Recuperado de: https://www.netcal.com/blog/security-awareness-tale-two-challenges/

Santillán, J.P., Cadena, V., & Cadena, M. (2019). Educación Steam: entrada a la sociedad del conocimiento. Ciencia Digital, 3(3.4.), 212-227. https://doi.org/10.33262/cienciadigital.v3i3.4.847

Sarre, R., Yui-Chung, L. & Chang, L.Y.C. (2018). Responding to cybercrime: Current trends. *Journal of Police Practice and Research: An International Journal*, 19, 515-518.

Seas, J. (2016). Didáctica general I .San José, Costa Rica: EUNED. Recuperado de: https://repositorio.so.ucr.ac.cr/programas_educacion/educacion/2018/II%20ciclo/ED-0012%20Did%C3%A1ctica%20General.pdf

Seebruck, R. (2015) A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation,* 14, 36-45.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems - Proceedings*, 1, 373–382. DOI https://doi.org/10.1145/1753326.1753383

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. *ACM*, pp. 88-99 DOI:10.1145/1280680.1280692

Shpigelman, C.N. (2017). Leveraging social capital of users with intellectual disabilities through Facebook participation: the perspectives of family members and direct support staff. *Intellectual and Developmental Disabilities*. 55: 407-418. DOI:10.1352/1934-9556-55.6.407

Skinner, T., Taylor, J., Dale, J., & McAlaney, D. J. (2018). The development of intervention E-learning materials and implementation techniques for cyber-security behaviour change. *Proceedings of AISB Annual Convention 2018*, 29-33. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056807649&partnerID=40&md5=609b2145ef510ebd0b4524a32922f747

Snyder, F. (2001). Sites of criminality and sites of governance. *Social & Legal Studies* 10, 251–6. DOI: 10.1177/a017406

Sommestad, T., Karzen, H. & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security*, 9(1), 26-46. DOI:10.4018/IJISP.2015010102

Sotelo, V. (2016). Fundamentos de la Psicología. *Universidad Continental*. ISBN 978-612-4196. Recuperado de http://repositorio.continental.edu.pe/

Soto, P. (2021). ¿Qué es el malware? Tipos y maneras de evitar ataques de este tipo. *Redseguridad*. Recuperado 12 de septiembre de 2022, de https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html

Steptoe, A., & Wardle, J. (2001). Locus of control and health behaviour revisited: a multivariate analysis of young adults from 18 countries. *British journal of psychology* (London, England : 1953), 92(Pt 4), 659–672. DOI: https://doi.org/10.1348/000712601162400

Svabensky, V., Vykopal, J., & Celeda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. SIGCSE 2020 - *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2–8. DOI: https://doi.org/10.1145/3328778.3366816

Tejedor-Calvo, S., & Pulido-Rodríguez, C. (2012). Retos y riesgos del uso de Internet por parte de los menores. ¿Cómo empoderarlos?. *Comunicar,* 39, 65-72. DOI: https://doi.org/10.3916/C39-2012-02-06

Taylor, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education : a pedagogical approach. *Financial Cryptography And Data Security: Fc 2020 International Workshops*. Revised Selected Papers, 207-217. DOI: https://doi.org/10.1007/978-3-030-54455-3_15

Taylor, J., McAlaney, J., James, S., Dale, J., Hodge, S., Thackray, H., & Richardson, C. (2017) Teaching psychological principles to cybersecurity students. *Conference: 2017 IEEE Global Engineering Education Conference (EDUCON*). DOI: 10.1109/EDUCON.2017.7943091

Thackray, H., McAlaney, J., Dogan, H., Taylor, J., & Richardson, C. (2016). Social psychology: An under-used tool in cybersecurity. *Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016*. DOI: https://doi.org/10.14236/ewic/HCI2016.64

Thompson, N., Mcgill, T.J. & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behaviour. Computers & Security, 70, 376-391.

Teets, C., & Grimes, K. (2019). Assessment of learning styles and learning retention among the elderly population in Frankfort, Kentucky. *Kentucky State University*. Recuperado de https://digitalcommons.murraystate.edu/postersatthecapitol/2019/KSU/9/

Torreblanca, J. (2006). La ciencia política empírica (II): enfoques de investigación. México: Mc Graw Hill. P. 57 Recuperado de https://www.redalyc.org/pdf/729/72917905015.pdf

Turanovic, J.J. & Pratt, T.C. (2014). Can't stop, won't stop: Self-control, risky lifestyles, and repeat victimisation. *Journal of Quantitative Criminology*, 30(1), 29-56. DOI: https://doi.org/10.1007/s10940-012-9188-4

UNICEF. (2012). La seguridad de los niños en línea: retos y estrategias mundiales. Innocenti Insights. Consultado el 09/02/2022. Recuperado de https://www.unicef-irc.org/publications/pdf/ict_spa.pdf

Unión Europea. (2010). Agenda digital europea. Consultado el 08/02/2020. Recuperado de https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:52010DC0245

Unión Europea. (2020). The EU's Cybersecurity Strategy for the Digital Decade. Recuperado de https://ec.europa.eu/newsroom/dae/redirection/document/72164

Vakhitova, Z.I., Reynald D.M. & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, 32(2), 169-188. DOI:10.1177/1043986215621379

Valencia-Arias, A. (2020). Tendencias investigativas en educación en ciberseguridad: un estudio bibliométrico. *Revista Ibérica de Sistemas y Tecnologías de Información*. Pp: 225–239. ISSN 16469895 Recuperado de https://www.proquest.com/docview/2394537804

Valls-Prieto, J. (2016). Nuevas formas de combatir el crimen en internet y sus riesgos. *Revista Electrónica de Ciencia Penal y Criminología*. 2016, núm. 18-22, pp. 1-36. Recuperado de: http://criminet.ugr.es/recpc/18/recpc18-22.pdf ISSN 1695-0194

Vanderhoven, E., Schellens, T. & Valcke, M. (2014). Enseñar a los adolescentes los riesgos de las redes sociales: Una propuesta de intervención en secundaria. *Comunicar*, 22(43), 123-132. DOI: https://doi.org/10.3916/C43-2014-12

Vasconcelos, J.P., & Muller, C. (2022) ¿Qué es la brecha digital?. I*nternetsociety*. Recuperado de https://www.internetsociety.org/es/blog/2022/03/que-es-la-brecha-digital/

Vázquez-Cano, E., & Sevillano-García, M. L. (2017). Lugares y espacios para el uso educativo y ubicuo de los dispositivos digitales móviles en la educación superior. *Edutec. Revista Electrónica de Tecnología Educativa*, (62), 48-61 DOI: https://doi.org/10.21556/edutec.2017.62.1007

Wall, D.S. (2008). Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology*, vol. 22, nos. 1-2, pp. 45–63 (ISSN 0965-528X).

Wang, M. (2007). Designing online courses that effectively engage learners from diverse cultural backgrounds. *British Journal of Educational Technology, 38*(2), 294–311. DOI: https://doi.org/10.1111/j.1467-8535.2006.00626.x

Wash, R., & Rader, R. (2015). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, pp. 309–325.

Wilsem, J. (2013). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice,* 29(4), 437–453. https://doi.org/10.1177/1043986213507402

Yar, M. (2005). «The Novelty of “Cybercrime” An Assessment in Light of Routine Activity Theory». *European Journal of Criminology*, Vol. 4, núm. 2, págs. 407-427. http://dx.doi.org/10.1177/147737080556056

Zhanna, M. S., & Lostri, E. (2020). The Hidden Costs of Cybercrime. *Center for Strategic & International Studies*. Recuperado de https://www.csis.org/analysis/hidden-costs-cybercrime

Zen Protocol. (2017). An introduction to the Zen protocol. Recuperado de https://www.zenprotocol.com/files/zenprotocolwhitepaper.pdf