nº 8 (3er Trimestre 2023)
ISSN: 2792-7962 – ISSNe: 2792-7970

Prácticas preventivas para fomentar la desconexión digital en la enseñanza universitaria

Preventive practices to promote digital disconnection in higher education

Carolina Serrano Falcón — *Profesora Titular de Universidad. Departamento de Derecho del Trabajo y de la Seguridad Social*
https://orcid.org/0000-0003-0502-7192

Rosa Moya Amador — *Profesora Titular de Universidad. Departamento de Derecho del Trabajo y de la Seguridad Social. Universidad de Granada*
https://orcid.org/0000-0001-5664-3433

María del Carmen García Garnica — *Catedrática de Universidad. Departamento de Derecho Civil*
https://orcid.org/0000-0003-3635-3601

Antonio Muñoz Ropa — *Informático Jefe de Servicio. CSIRC Seguridad informática*

Cita Sugerida: SERRANO FALCÓN, C., MOYA AMADOR, R. GARCÍA GARNICA, M.C. y MUÑOZ ROPA, A. «Prácticas preventivas para fomentar la desconexión digital en la enseñanza universitaria». *Revista Crítica de Relaciones de Trabajo, Laborum*. nº 8 (2023): 175-194.

Resumen

El uso de los dispositivos móviles y en particular el teléfono se ha generalizado en toda la sociedad y lógicamente también entre el alumnado universitario. Las universidades son conscientes de la necesidad de información y formación para garantizar un buen uso de los mismos. Esta es la razón que nos ha llevado a elaborar una guía de buenas prácticas sencilla, corta, atractiva, y de fácil lectura, que contiene en un único documento recomendaciones para un buen uso de las redes sociales y de la mensajería instantánea. La finalidad perseguida es concienciar de la importancia de aplicar medidas preventivas para preservar la salud digital y garantizar el derecho a la desconexión digital entre la comunidad universitaria. Esta guía contiene también información sobre cómo actuar y dónde dirigirse ante algún problema derivado de un mal uso de tales dispositivos.

Palabras clave

dispositivos móviles, universidades, desconexión digital, salud digital, ciberseguridad, protección de datos.

Abstract

The use of mobile devices and in particular the mobile phones has become widespread throughout society. Its use is increasing in the young population and logically also among university students. Universities are aware of the need for information and training to ensure a good use of them. This is the reason that has led us to develop a simple, short, attractive and easy to read guide of good practices, which contains in a single document, recommendations for a good use of social networks and instant messaging. The aim is to raise awareness of the importance of applying preventive measures to preserve digital health and guarantee the right to digital disconnection among the university community. This guide also contains information on how to act and where to turn to in the event of a problem arising from the misuse of such devices.

Keywords

mobile devices, universities, digital disconnection, digital health, cybersecurity, data protection.

Fecha Recepción: 02/03/2023 - Fecha Revisión: 02/03/2023 - Fecha Aceptación: 03/03/2023
Págs. 175-194

1. INTRODUCCIÓN. LA UNIVERSIDAD ANTE EL USO GENERALIZADO DE DISPOSITIVOS MÓVILES

Partimos de una realidad, que no hace falta justificar: hoy en día el teléfono móvil lo llevamos a todas partes, y está presente en el 99.5% de los hogares[1] según datos del INE. Cada vez utilizamos más los distintos dispositivos móviles, en especial el teléfono por la facilidad en su transporte, comodidad en su utilización. Ha pasado a ser un instrumento inseparable y cada vez más imprescindible de todos y cada uno de nosotros (disco duro que llevamos y del que ya no podemos prescindir de nuestra memoria externa…).

Si éste es un fenómeno global, lógicamente, el uso del teléfono móvil aumenta en la población joven, donde usan Internet con más frecuencia.[2] En el momento presente, como regla general, los estudiantes cuando acceden a la Universidad ya llevan tiempo utilizando dispositivos móviles y distintas redes sociales, haciéndolo a nivel personal, y en muchos casos habiéndose iniciado tempranamente con poca instrucción en los peligros que conlleva su mala utilización.

También es cada vez más frecuente en los últimos años que los jóvenes preuniversitarios hayan hecho uso de dispositivos móviles en la enseñanza secundaria e incluso primaria en sustitución de los manuales tradicionales (en especial la tablet), por lo que cuando llegan a las aulas universitarias tienen ya práctica en la utilización de Internet para el proceso de enseñanza-aprendizaje. Suelen estar en clase con sus dispositivos móviles y cuando en el aula se plantea cualquier pregunta o cuestión, rápidamente tienen la respuesta simplemente accediendo al teléfono móvil del que no se separan, o al ordenador con el que toman los apuntes. Incluso a veces, son los propios profesores los que les pedimos que lleven sus dispositivos para utilizar técnicas de gamificación en clase (entre otros, "Quiz" o "Kahoot") porque entendemos que aumenta la motivación y el compromiso e interés del alumno y su rendimiento.[3]

También es habitual que el alumnado escriba desde su dispositivo móvil mensajes al profesorado sin pararse a pensar cuándo es el momento adecuado para enviar este mensaje. Y al mismo tiempo socializan con el mismo, siendo habitual crear grupos de Whatsapp de clase.

En definitiva, a pesar de que el modelo de universidad que predomina en España es presencial, el uso de los dispositivos móviles está produciendo importantes cambios tanto dentro como fuera del aula, donde la brecha entre el ámbito digital y físico se está acortando.[4]

---

[1] INE: "Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares. Año 2021" Nota de prensa de 15 de noviembre de 2021, en https://www.ine.es/prensa/tich_2021.pdf consultado 28 de abril de 2022.

[2] Datos del INE sobre población que ha utilizado Internet de manera frecuente (al menos una vez por semana) en 2022 https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528559&p=%5C&pagename=ProductosYServicios%2FPYSLayout&param1=PYSDetalle&param3=1259924822888, consultado el 24 de abril de 2023.

[3] González, H.T.: "Recursos tecnológicos para la integración de la gamificación en el aula". *Tecnología, ciencia y educación,* núm. 13, 75-117, 2019.

[4] Es unánime esta apreciación. Por todas, véase Lastiri Santiago, M.: "El metaverso: origen, evolución y retos actuales", *La Ley mercantil*, núm. 99, 2023, pág. 2.: "en la segunda mitad del siglo XX, el mundo entero presenció y comenzó a disfrutar del profundo desarrollo tecnológico y empresarial del sector de las telecomunicaciones con la incorporación al mercado de nuevas herramientas, como los teléfonos móviles y la televisión (por antena, cable, satélite o fibra óptica), que revolucionaron tanto los principios históricos sobre los que se sustentaban las sociedades nacionales como a la humanidad en su conjunto".

La Universidad está inmersa en la nueva realidad histórico-social y tecnológica que caracteriza nuestro tiempo.[5] La referencia a los retos ante el avance de la tecnología está presente en el preámbulo de la nueva Ley *Orgánica* 2/2023, de 22 de marzo, del *Sistema Universitario* (LOSU).[6]

En la práctica ya hay actuaciones en las que se intenta dar respuesta a cuestiones relacionadas con el uso de dispositivos y en especial con los teléfonos móviles. Destacamos, entre otras, la formación en competencias digitales docentes por el profesorado[7] con el fin de enseñarle a utilizar metodologías activas utilizando los dispositivos móviles del alumnado (*Mobile Learning*).[8] También desde el ámbito universitario se es consciente de la necesidad de incidir en la seguridad informática al usar los dispositivos móviles y en la necesidad de la protección de datos. De hecho, algunas universidades están adheridas al "Pacto Digital para la Protección de las Personas" de la Agencia Española de Protección de Datos. Además, a las universidades les preocupa la salud digital del alumnado y de la comunidad universitaria y la sociedad en general, formando parte muchas de ellas de la Red Española de Universidades Promotoras de la salud (REUPS) que se constituyó con esta finalidad el 22 de septiembre de 2008,[9] poniendo de manifiesto que las universidades no están al margen de la necesidad de protección y actuaciones en este sentido.

Ahora bien, a pesar de que no es un tema ajeno al ámbito universitario, quienes realizamos tareas profesionales educativas, y estamos en el día a día cerca, hemos observado que al alumno no le llega esta información, ni tampoco todas las actuaciones en esta materia que se llevan a cabo en las universidades. Por este motivo, consideramos que su uso progresivo y generalizado merece algunas reflexiones y actuaciones a llevar a cabo.

Esta es la razón que nos ha llevado a elaborar —en el marco de un proyecto de innovación docente— una guía de buen uso de los dispositivos móviles dirigida a los alumnos. Está publicada en abierto,[10] con la pretensión de que sea útil para informar y dar a conocer al alumnado cómo se tiene que usar de forma adecuada un dispositivo móvil para preservar la seguridad, la protección de sus datos personales y para poder disfrutar de todos sus beneficios a la vez que mantener el control sobre él en pro del bienestar digital y así contribuir a garantizar el derecho a la desconexión digital entre la comunidad universitaria.

---

[5] Ibíd., así, las transformaciones digitales que han traído la tercera revolución industrial (en la segunda mitad del siglo XX con la informática y con ella a programarse las máquinas, ha desembocado en una progresiva automatización que más tarde vio la llegada de Internet); y la cuarta revolución industrial (siglo XXI, también llamada Industria 4.0 se caracteriza por los avances en robótica e inteligencia artificial.

[6] *BOE* 23 de marzo de 2023.

[7] Plan de Acción Digital 2021-2027 de la Unión Europea. Se puede consultar en https://education.ec.europa.eu/es/focus-topics/digital-education/action-plan

[8] Aznar-Diaz, I.; Hinojo-Lucena, F.J. Cáceres-Reche, M.P.; Romero Rodríguez, J.M.: "Analysis of the determingin factors of Good teaching practices of mobile learning at the Spanish University. An explanatory model. *Computers&Education,* 159-104007, 2020.
Se define el "Mobile learning" como "el aprendizaje que consiguen los estudiantes cuando son capaces de acceder a la información en cualquier momento y lugar, a través del uso de la tecnología móvil que permite la realización de unas actividades determinadas y concretas, enmarcadas en un contexto y las cuales proporcionan un aprendizaje". Martin y Ertberger, J.: "Here and now mobile learning: an experimental study on the use of the mobile technology. *Computer and Education,* 76-85, 2013.

[9] El Ministerio de Sanidad, Servicios Sociales e Igualdad (MSSSI), el Ministerio de Educación, Cultura y Deporte y la Conferencia de Rectores de las Universidades Españolas (CRUE) apoyan y favorecen el desarrollo de esta Red, e invitan al desarrollo de los proyectos de universidades saludables, invitando a unirse a esta Red a todas las universidades interesada.

[10] Esta guía ha sido financiada por la Universidad de Granada, en el marco del Proyecto de Innovación y buenas prácticas docentes de la UGR (2022-2023): "Buenas prácticas para un uso adecuado de los dispositivos móviles del alumnado en la UGR". Unidad de Calidad, Innovación Docente y Prospectiva. Puede consultarse en https://digibug.ugr.es/flexpaper/handle/10481/82379/guia%20interactiva.pdf?sequence=1&isAllowed=y

Dedicamos los siguientes apartados a explicar esta guía, su necesidad de implantación, así como el contenido de la misma, para terminar con unas conclusiones y propuestas para su implantación en el ámbito universitario.

2. UNA PROPUESTA INNOVADORA: "GUÍA PARA EL BUEN USO POR EL ALUMNADO UNIVERSITARIO DE SUS DISPOSTIVOS MÓVILES"

2.1. La necesidad de la guía. Objetivos

Como cuestión previa aclarar que esta guía va dirigida al alumnado universitario para que la tengan en cuenta no sólo al usar su dispositivo como una herramienta docente (es lo que se denomina BYOD o *Bring your own device*), [11] sino también cuando lo utilice como medio de socialización o como medio de comunicación entre compañeros/as de clase. Entendemos que es aquí sobre todo donde están expuestos a mayores conflictos (destacando los grupos de Whatsapp que ellos crean para comunicarse). No obstante, hay que aclarar que aunque estas recomendaciones pueden ser de utilidad en otros niveles educativos, esta propuesta está dirigida al alumnado universitario y a la Universidad como institución fundamental en la sociedad del conocimiento en la que vivimos, caracterizada por la revolución científica y tecnológica, particularmente en el ámbito de la información y la comunicación.

La idea de elaborar una guía para el buen uso por el alumnado universitario de sus dispositivos móviles ha tenido su origen en carencias que hemos detectado en nuestra actividad académica. Los alumnos son jóvenes y están muy habituados a usar con soltura sus dispositivos, aplicaciones y redes sociales. Ahora bien, esto no significa que conozcan cómo hacer un buen uso de su dispositivo móvil. No se debe a la falta de normativa, ni a la falta de organismos que se encargan de informarnos y prevenir sobre un mal uso de los dispositivos, como hemos indicado anteriormente. Pero quizás la dispersión normativa y la diversidad de instituciones que se encargan de estos temas (seguridad informática, protección de datos, salud digital…) y al mismo tiempo la creencia generalizada del alumnado que por ser nativos digitales conocen cómo utilizarlos y saben cómo evitar peligros existentes, hace que todas estas buenas acciones y prácticas que ya existen no las interioricen.

Percibimos que no están ni informados ni formados (y en muchos casos ni preocupados o concienciados) para hacer frente a un uso responsable de sus dispositivos en materia de seguridad informática, de protección de los datos personales y de su salud digital. En definitiva, la normativa y actuaciones existen, pero al alumnado hay que transmitírselo con facilidad. A ellos/as les parece lejana esta información, como si no fuera con ellos. Además, los alumnos/as tampoco tienen una percepción clara de dónde dirigirse si tienen algún problema derivado de su teléfono móvil (robo de teléfono móvil que ponga en peligro datos de la Universidad, insultos o acoso a través de un grupo de Whatsapp entre compañeros/as, difusión de sus datos entre los que están sus calificaciones...).

Estas carencias detectadas nos llevaron a poner en marcha esta propuesta innovadora. El objetivo principal es crear una guía sencilla, corta, atractiva, interactiva, de fácil lectura y pedagógica, para que el alumnado tenga una visión de conjunto de lo que hay que conocer para un buen uso de su teléfono móvil u otros dispositivos. Consideramos que, con la divulgación de esta guía, podemos contribuir a conseguir los siguientes objetivos:

[11] Se puede consultar la guía realizada por el INTEF (Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado), que, aunque no está dirigida al ámbito universitario, puede tener aquí utilidad. "Diseñando el aula del futuro. *Bring your own device* (BYOD): una guía para directores y docentes, enero de 2016. https://intef.es/wp-content/uploads/2016/02/Informe_resumen_BYOD_EUN_Enero_2016_INTEF.pdf

1) Protegerse de las amenazas digitales al formarles en seguridad informática para fomentar un uso responsable de los dispositivos y medios digitales.

2) Conocer la importancia de la protección de los datos personales (los suyos y los del resto de la comunidad universitaria) cuando utilizan redes sociales y mensajería instantánea.

3) Adquirir hábitos saludables y seguros con carácter preventivo cuando utilizan su dispositivo como herramienta docente y como herramienta de socialización.

4) Favorecer y estimular la convivencia activa en el seno de la comunidad universitaria, y que tengan claro dónde acudir ante un problema derivado de un mal uso de sus dispositivos móviles

2.2. La salud digital. Fomentando la desconexión digital

Está demostrado que el abuso de Internet y de las tecnologías, y por tanto, de los dispositivos móviles, pueden causar daños irreversibles en la salud,[12] entendiendo por esta, conforme a la Constitución de la Organización Mundial de la Salud (OMS) "un estado de completo bienestar físico, mental y social y no solamente la ausencia de afecciones o enfermedades", [13] estableciendo a continuación como principio que "el goce del grado máximo de salud que se pueda lograr es uno de los derechos fundamentales de todo ser humano sin distinción de raza, religión, ideología política o condición económica o social". El ideal de salud para todos los ciudadanos que persigue la OMS es el que les permita llevar una vida social y económicamente productiva.[14]

Los beneficios del uso de los dispositivos móviles son numerosos, pero también hay que estar alertas porque la conectividad permanente puede crear nuevos riesgos o agravar los existentes y que incidan en la salud física y mental del alumnado (riesgos psicosociales, ergonómicos, o el aislamiento provocado por la falta de interacción social). Hacer visible la necesidad de un buen uso de los dispositivos móviles como intervención preventiva ante problemas de salud que pueden derivar de su uso inadecuado va en la línea de la "Estrategia mundial sobre salud digital 2020-2025" donde uno de sus principios rectores es el de "promover el uso adecuado de las tecnologías digitales para la salud", recogiendo que el el uso adecuado de la salud digital abarca las siguientes dimensiones: la promoción de la salud y la prevención de las enfermedades, la seguridad del paciente, la ética, la interoperabilidad, la propiedad intelectual, la seguridad de los datos (confidencialidad, integridad y disponibilidad), la privacidad, la eficacia en función del costo, la implicación de los pacientes y la asequibilidad).

En la finalidad que perseguimos, limitada al ámbito en el que desempeñamos nuestras tareas profesionales, el ámbito universitario, es imprescindible tener en cuenta que la desconexión digital hay que observarla desde la doble perspectiva del profesorado y del alumnado. Es decir, no sólo es

[12] Romero-Rodríguez, J.M.; Martínez-Heredia, N.; Campos Soto, M.N.; Ramos Navas-Parejo, M.: "Influencia de la adicción a Internet en el bienestar personal de los estudiantes universitarios", *Health and Addictions/Salud Y Drogas*, *21*(1), 2021. https://doi.org/10.21134/haaj.v21i1.559

[13] Preámbulo de la Constitución de la OMS adoptada por la conferencia sanitaria internacional, firmada en 1946 con entrada en vigor en 1948. Tenemos que diferenciarlo del término "cibersalud", término también, acuñado por la Organización Mundial de la Salud (OMS) y referido a "el uso de las tecnologías de información y comunicación para fomentar la salud, ya sea in situ o a distancia) https://www.cibersalud.es/organizacion-mundial-de-la-salud-cibersalud/

[14] Benavides, G. F., García A. M., Ruiz Frutos, C., "La salud y sus determinantes" en *Salud laboral. Conceptos y técnicas para la prevención de riesgos laborales*, VV. AA., Barcelona, 2007, p. 3.

importante que el alumnado se desconecte para evitar problemas con su salud física y mental, sino también hay que pensar que el profesorado tiene el derecho y la necesidad de desconectar. Aunque la LOSU hace mención especial al estudiantado, no podemos olvidar al profesorado, pues hay que evitar también su fatiga informática y promover su salud digital.

Los profesores/as, como trabajadores que son, tienen derecho a la protección de la seguridad y salud laboral[15] y a la desconexión digital regulada en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD).[16] En su apartado 1 señala que "los trabajadores y empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo… el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar". No es una regulación muy concreta, y poco se dice cómo se tiene que hacer efectivo por parte del empleador este derecho, remitiendo a la negociación colectiva o, si no se hace ahí, a la elaboración de una política interna "en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática" (artículo 88.3 LOPDGDD).[17]

Ante la falta de concreción en el citado artículo 88, nos podríamos preguntar cómo se hace efectivo este derecho en las universidades. Y ello porque es el empleador el que tiene que respetar el derecho a la desconexión y abstenerse de enviar mensajes al profesorado fuera del horario laboral. Pero también hay que proporcionarle instrucciones al alumnado de cómo tienen que utilizar el teléfono móvil para comunicarse con el profesorado para respetar su derecho a la desconexión. O se hace de esta forma, o difícilmente este derecho tendrá una efectividad plena.

Los alumnos/as llevan siempre encima su teléfono móvil, por lo que para ellos es muy fácil y cómodo contactar con el profesorado en cualquier momento del día y en cualquier parte. Y a veces se les olvida, que detrás de sus teléfonos móviles, hay personas trabajadoras con derechos legalmente reconocidos y por tanto exigibles como el derecho a los descansos, a la intimidad personal y familiar, a la conciliación y a una protección eficaz de la seguridad y salud de las personas trabajadoras, por lo que necesitan desconectar de su trabajo. Y precisamente esta guía puede contribuir en este sentido para advertir al alumno de la necesidad de hacer un buen uso de sus dispositivos por su bienestar digital, pero también para la toda la comunidad universitaria y que intenten evitar mensajes fuera del período y horario lectivo.

[15] No podemos olvidarnos de la obligación de seguridad y salud en el trabajo conforme al art. 14 de la Ley de Prevención de Riesgos Laborales y el artículo 16.2 de la misma ley que establece la obligación de la empresa de evaluar y gestionar todos los riesgos laborales, incluidos los psicosociales, a los que puede conducir el estar continuamente conectado al trabajo. A tener en cuenta también la reciente Estrategia Española de Seguridad y Salud en el Trabajo (EESST) 2023-2027 aprobada por el Consejo de Ministros el 14 de marzo de 2023. En la Estrategia se adquiere un compromiso firme con los ejes prioritarios del Marco Estratégico Europeo de Seguridad y Salud en el Trabajo 2021-2027 y, particularmente, con el objetivo de anticiparse a los riesgos derivados de las transiciones digital, ecológica y demográfica.

[16] También se hizo con anterioridad en otros países vecinos como Francia. Véase Tascón Lopez, R.: "El derecho de desconexión del trabajador (potencialidades en el ordenamiento español), *Trabajo y Derecho,* núm. 41, 2018.
También ya se ha dado algún paso en la Unión Europea con la Resolución del Parlamento Europeo, de 21 de enero de 2021, con recomendaciones destinadas a la Comisión sobre el derecho a la desconexión (2019/2181(INL) y la reciente Declaración Europea sobre los Derechos y principios digitales que ha proclamado el Parlamento Europeo, el Consejo y la Comisión (15 de diciembre de 2022). En esta declaración la Unión Europea se compromete a velar por la desconexión para que el uso de las herramientas digitales no suponga ningún tipo de riesgo "para la salud física y mental de los trabajadores en el entorno de trabajo".

[17] En este sentido avanza el informe de la comisión mundial de la Organización Internacional del Trabajo (OIT) sobre el futuro laboral *Trabajar para un futuro más prometedor*, planteando de cara a 2030, señalando que las tecnologías de la información y comunicación han de servir para conseguir que la realidad laboral se acerque a la definición de trabajo decente.

En relación al estudiantado universitario, es preciso destacar que en la nueva Ley Orgánica del Sistema Universitario (LOSU), encontramos hasta en tres ocasiones referencia expresa a la necesidad de velar por la salud de los estudiantes. Así: en el preámbulo (I) se habla de "la salud emocional del estudiantado" promoviendo asimismo su participación en el gobierno de la universidad en sus distintas unidades y en la propia gestión de servicios"; en el artículo 33 referido a los *derechos relativos a la formación académica*, el estudiantado tendrá los siguientes derechos, sin perjuicio de aquellos reconocidos por el estatuto del estudiante universitario aprobado por el Gobierno: e) las tutorías y al asesoramiento, a la orientación psicopedagógica y al cuidado de la salud mental y emocional, en los términos dispuestos por la normativa universitaria; y en el artículo 43.1 se establece que las universidades contarán con servicios de salud y acompañamiento psicológico y pedagógico y servicios de orientación profesional, dotados con recursos humanos y económicos, junto con el apartado quinto del mismo precepto legal que establece que las universidades, en colaboración con las Comunidades Autónomas en las que se encuentren ubicadas, ofrecerán servicios gratuitos dirigidos a la orientación psicopedagógica, de prevención y fomento del bienestar emocional de su comunidad universitaria y, en especial, del estudiantado, así como servicios de orientación profesional.

Por tanto, una forma de hacer efectivo este derecho es precisamente con esta herramienta que presentamos, como un instrumento más, añadido a los demás servicios gratuitos que se ofrezcan y que contribuiría sin duda al fomento del bienestar emocional. La guía puede ser una buena herramienta complementaria para contribuir a la desconexión digital, aunque se necesitan más medidas en este sentido.

3. EL CONTENIDO DE LA GUÍA

Como se puede apreciar del sumario de este trabajo, daremos a conocer el contenido de la guía -que a su vez coincide con los cuatro objetivos ya indicados- así como una explicación de cada uno de sus apartados. Para ello hemos enumerado las recomendaciones (las hemos entrecomillado para identificar el contenido de la guía) y a continuación hemos realizado una explicación a cada una de ellas.

3.1. Utiliza los dispositivos de forma segura

Primera recomendación:

"Es aconsejable que instales VPN cuando accedas desde fuera de la universidad a los recursos educativos. Utiliza la Wifi de tu universidad siempre que sea posible, ahorrarás datos y estarás más seguro/a. No olvides que las wifi's gratuitas en cafeterías suelen ser inseguras, no tienen clave o todo el mundo la sabe, por lo que se puede visualizar el tráfico de datos de tu teléfono, y por tanto averiguar tus claves y/o acceder al mismo".

Explicación:

Tenemos la costumbre de conectarnos a las redes wifis que vemos gratuitas para ahorrar datos en nuestros teléfonos. Esto es un peligro ya que no sabemos quién puede estar conectado. Puede ser alguien, con no buenas intenciones, que al estar en la misma red puede ver el tráfico que pasa por ella. Igualmente, si tenemos alguna vulnerabilidad, falta de actualizaciones por ejemplo o hemos caído en un phishing sin saberlo y tenemos el equipo comprometido, se podría tomar el control de forma remota del dispositivo con total transparencia para el usuario.

Ataque "*man in the middle*" es típico en los hoteles y en cafeterías. Se ofrece una wifi gratis donde el usuario se conecta, y no es más que alguien que ha ofrecido un punto de acceso a través de algún ordenador portátil simulando que es la red gratuita de la cafetería. De esta forma, nuestro teléfono móvil o dispositivo se conecta a un ordenador desde donde se puede ver el tráfico de red en texto plano, se pueden capturar claves, ver por dónde se navega, y se hace con el control, igualmente, del dispositivo a veces. Por este motivo, y para evitar que el tráfico de red lo pueda ver quien no debe, es mejor conectarse previamente a una VPN (*virtual private network* o red privada virtual), o lo que es lo mismo, establecer un canal cifrado entre nuestro dispositivo y otro ordenador de forma que no se puede ver con claridad lo que estamos transmitiendo, ya que se transmite y recibe todo de manera cifrada.

En todas las universidades españolas se suele ofrecer este servicio de VPN gratuito a todos los estudiantes y personal de las instituciones por lo que es recomendable utilizarlo.[18] Hay casos que si no conectas con VPN con la universidad no puedes acceder a según qué recursos o servicios que ofrece la institución como puede ser los datos que ofrece la biblioteca. Sobre todo, debemos utilizar la VPN si consideramos que es una medida exigida en el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022[19], de 3 de mayo, que es de obligado cumplimiento para las administraciones públicas.[20]

Es muy sencillo utilizar este tipo de conexión, tan solo hay que seguir los siguientes pasos:

— Descargar el programa compatible con la institución y que nos permita conectarnos a VPN e instalarlo.

— Configurarlo con los parámetros de la institución, para eso cada universidad tiene su servidor de conexión.

— Hay veces que para autenticarnos nos pedirán un segundo factor de autenticación para asegurarnos que somos nosotros.

— Por último, una vez configurado, solo hay que pinchar en el programa, e identificarnos hasta que nos diga que la conexión está establecida.

Hay que tener en cuenta que la velocidad de Internet es un poco más lenta, ya que el dispositivo cada vez que envía o recibe información tiene que cifrar y descifrar el contenido, pero no es tan costoso si consideramos los beneficios que nos aporta.

[18] Ahora bien, si la universidad no tiene este servicio, hay otras opciones que son gratuitas, por ejemplo "*risevpn"* u otros servicios que se ofrecen en la red. Pero no podemos olvidar que no hay nada gratuito, y "si algo es gratis el producto eres tú". Hay otras formas de conexión mediante VPN de pago, que son las aconsejables, pues en el caso de servicio VPN gratuitos miran los datos de navegación para sacar estadísticas y vender esa información a terceros. La OSI, Oficina de Seguridad del Internauta, dependiente del INCIBE, Instituto de Ciberseguridad, nos ofrece en su web algunas herramientas para poder establecer una VPN. Se pueden descargar de la siguiente dirección https://www.osi.es/es/herramientas-gratuitas/red-virtual-privada

[19] BOE núm. 106, de 4 de mayo de 2022.

[20] Por ejemplo, aparece es tema de las comunicaciones cifradas en la media op.acc.6 del anexo II, del citado Real Decreto 311/2022.

Segunda recomendación:

"Descarga tus apps de forma segura. Descarga las apps siempre en la tienda oficial (desde la App Store para Apple o desde Play store para Android). Y en caso de ordenadores, hay que descargarla desde el sitio web oficial".

Explicación:

Por ahorrar un dinero, y con lo típico de la picaresca, es frecuente bajarse de Internet programas de forma 'pirata' con claves válidas, y pensamos que hemos logrado ahorrarnos unos euros. Pues bien, este software pirata, en muchas ocasiones, tienen algún 'malware', o virus, que se suele instalar con la versión pirata de la aplicación y que permite desde robarnos información o dejar puertas falsas abiertas en los dispositivos. El programa pirateado funciona y hace su cometido, pero de forma no visible están funcionando estos programas que contienen *malware*.

Por ello es aconsejable descargar el software original. Hay ofertas en Internet para casi todos los tipos de *software* y versiones gratuitas de algunos otros. Este software en el caso de los teléfonos y en general los dispositivos móviles, es mejor descargarlos de las tiendas oficiales ya que hay un control de forma periódica en ellas para verificar si tienen algún malware/virus o no.

Ahora bien, en las tiendas oficiales no todo es una panacea, hay que tener cuidado con el software que nos pide más permisos de los necesarios. Por ejemplo, hace unos años salió un programa que activaba el flash del teléfono como si fuese una linterna y nos pedía acceso a los contactos. Ante ello, nos preguntamos: ¿para qué quiere una linterna acceso a mis contactos? En este caso está claro, para robarnos datos. En las tiendas oficiales se controlan ya todos estos temas, pero aun así se escapa alguno. Así que, aunque es seguro bajar de las tiendas oficiales, hay que tener cuidado a pesar de todo, y por supuesto evitar el software pirata, no merece la pena por las razones que ya hemos analizado.

Tercera recomendación:

"Cuando haya una videoconferencia para cursos de formación y reuniones en la Universidad, conéctate a través de tu cuenta institucional".

Explicación:

En todas las universidades ya hay sistemas de videoconferencia que se utilizan con mucha frecuencia durante el período de docencia online motivado por la pandemia. Ahora también se ofrece de forma gratuita al alumnado bien sea para clases, charlas, reuniones, etc.

Es aconsejable utilizar los sistemas que ofrecen las universidades para las actividades académicas, ya que verificarán que la identificación es correcta y así se evitará que acceda personal no deseado y que no está invitado a esa videoconferencia.

Las universidades han firmado convenios o contratos con los servicios ofrecidos por Google o Microsoft para ofrecer estos servicios a la comunidad universitaria. También se han contratado otros servicios de videoconferencia como Zoom, para que éstas sean lo más seguras posibles y cumplan con todas las normativas necesarias de privacidad y protección de datos.

Cuarta recomendación:

"Para poner una denuncia en caso de robo, es conveniente guardar la información de IMEI del teléfono. Este número identifica al teléfono de forma unívoca. Es conveniente guardarlo en lugar seguro por si acaso. También se pueden descargar utilidades antirrobo https://www.osi.es/es/herramientas-gratuitas/antirrobo. Y siempre es aconsejable hacer copias de seguridad para no perder todas las fotos y resto de nuestros documentos https://www.osi.es/es/herramientas-gratuitas/copias-de-seguridad".

Explicación:

En caso de robo del teléfono móvil, tablet o portátil, debemos poner una denuncia en la policía. Para poder identificarlo necesitamos en el caso del móvil el número IMEI, (*International Mobile Equipment Identity)*, y en cualquier otro caso casi siempre el número de serie. Estos datos los debemos guardar en lugar seguro.

El IMEI podemos consultarlo en el teléfono marcando *#06# y le damos a llamar. El número devuelto es el que debemos guardar. Este dato nos lo pedirá la policía si ponemos la denuncia.

Y si lo que queremos es o bien localizar el teléfono o borrar su contenido hay utilidades que nos ofrece la Oficina de Seguridad del Internauta (OSI).[21] Como medida adicional de seguridad para nuestros móviles/tablets/portátiles, es aconsejable hacer copias de seguridad, ya que se puede romper y es la única forma de recuperar su contenido. La OSI ofrece también aplicaciones gratuitas para poder hacer las copias de seguridad.[22]

Quinta recomendación:

"Utiliza contraseñas de acceso que sean robustas para evitar poner en riesgo el perfil de la universidad. No utilices para las contraseñas fechas de nacimiento o el "123456" clásico. Deben llevar números, letras y signos de control. No uses nunca en los dispositivos móviles la función de "recordar contraseña", pues si cae en manos inapropiadas pueden tener acceso a las apps donde esté activado el recuerdo de contraseña. No guardes contraseñas a la vista, ni física ni digitalmente. Utiliza lo que se llama un segundo factor de autentificación siempre que se pueda. No compartas contraseñas. Existen gestores de contraseñas que nos ayudan a recordarlas. Si tenemos muchas, aquí hay algunos gestores gratuitos https://www.osi.es/es/herramientas-gratuitas/gestores-de-contrasenas".

Explicación:

Si queremos conocer cómo de robusta es nuestra contraseña, es bueno verificarlo en herramientas que existen en Internet. Es conveniente seguir siempre las pautas que marque la institución en las normativas al efecto. Normalmente, se recomienda que sean de longitud mayor a 10 caracteres, que tenga mayúsculas y minúsculas, números, algún carácter de control (_*%&.).

Y siempre es también recomendable el segundo factor de autenticación (2FA) en todos los servicios de Internet que nos lo permita. Aunque hay estudios que ya adelantan que las contraseñas desaparecerán y utilizaran características biológicas para acceder a los dispositivos, aún tenemos que asegurarnos que nadie acceda a nuestros servicios de internet, y para ello el 2FA es ideal.

[21] https://www.osi.es/es/herramientas-gratuitas/antirrobo

[22] https://www.osi.es/es/herramientas-gratuitas/copias-de-seguridad

Sexta recomendación:

"Recuerda que si utilizas tu teléfono móvil, o cualquier otro dispositivo para para acceder a redes sociales, éstos deben contar con soluciones antimalware, (por Ej. antivirus y/o firewall) sistema operativo y otro software actualizado. En este enlace se puede encontrar de forma gratuita en https://www.osi.es/es/herramientas-gratuitas/antivirus-y-cleaners".

Explicación:

El tener un software antivirus es indispensable en cualquier dispositivo para evitar que un posible malware nos complique el uso de ese equipo, así como la pérdida de privacidad. Podemos pinchar en enlaces que, mediante técnicas de ingeniería social o engaño, nos lleven a perder el control del equipo y/o la privacidad de este. Hay antivirus gratuitos que podemos instalar en nuestros equipos, aunque, como ya hemos indicado "lo gratis no existe". Se aconseja comprar una licencia de alguna solución antimalware. Últimamente los sistemas Windows lo incorporan, pero no hay sistemas infalibles. Es bueno reforzarlo con algún otro sistema. Por otra parte, debemos tener activado el firewall. Es un sistema que impide conexiones de red a nuestro equipo de forma incontrolada aprovechando cualquier brecha. Los sistemas Windows traen un sistema de este tipo junto con el sistema. Se puede configurar, pero con solo activarlo ya hay una serie de medidas básicas que nos ayudarán en la securización de nuestro ordenador.

Séptima recomendación:

"Ante la menor duda con el enlace, evita acceder al sitio web, pues pueden redirigir a sitios fraudulentos de tipo phishing o a otros sitios Web".

Explicación:

Tenemos que ser precavidos y releer los mensajes que recibimos por email/sms/whatsApp/ etc. antes de pinchar en una URL que nos aparezca en el mensaje, sobre todo si nos piden datos identificativos. Hay que desconfiar de esos mensajes y pensar que lo que hacemos. Los bancos no piden claves por correo, ni vamos a tener tanta suerte como para haber ganado un premio sin haber participado conscientemente en un sorteo… Y por supuesto cuidado con las llamadas de los servicios técnicos de ordenadores que nos piden que instalemos un *software* para poder atendernos mejor, es un *malware*.[23]

Antes de finalizar este apartado de la guía en la que se han explicado las recomendaciones para utilizar los dispositivos de forma segura, queremos señalar que el Centro Criptológico Nacional (CNN), dependiente del Centro Nacional de Inteligencia (CNI), y del cual dependen todas las administraciones públicas, ha publicado una guía de buenas prácticas en mayo de 2021[24] para mejorar

[23] Toda esta información se puede completar consultando los siguientes sitios web donde se pueden encontrar más consejos y píldoras formativas en ciberseguridad: https://www.incibe.es/; https://www.osi.es/es; https://www.ccn-cert.cni.es/; https://www.is4k.es/; https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php; https://www.gdt.guardiacivil.es/webgdt/pinformar.php; https://www.pantallasamigas.net/; https://blogs.ugr.es/seguridadinformatica/

[24] Se puede consultar en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1757-ccn-cert-bp-03-dispositivos-moviles/file.html
Son también de interés las guías sobre configuración segura de dispositivos de Android https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/168-ciberconsejos-configuracion-segura-android/file o IOS https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/169-ciberconsejos-configuracion-segura-ios/file

el nivel de protección y seguridad de los dispositivos móviles. Este "ciberconsejo" consiste en un total de diez recomendaciones de seguridad a tener en cuenta. Muchas de ellas las hemos incluido en esta guía, junto con otras recomendaciones más específicas para el ámbito universitario.

3.2. Redes sociales y mensajería instantánea

Recomendación general:

"Ante todo, "respeto digital". Recuerda que la dignidad y respeto conforman los valores y compromisos éticos de nuestra Universidad. Actúa siempre con cortesía y prudencia y de forma cuidadosa con los demás y con nosotros mismos, para respetar la privacidad e intimidad, las opiniones, la propiedad intelectual e industrial, la información y también proteger nuestros datos personales sensibles".

Para ello, veamos algunas recomendaciones a tener en cuenta:

Primera recomendación:

"En la actividad académica y en las relaciones entre profesorado y alumnado y entre el alumnado de un mismo grupo o titulación, se recomienda utilizar las herramientas institucionales de comunicación: el correo electrónico institucional y la plataforma educativa de la universidad".

Explicación:

El uso de herramientas digitales de apoyo a la docencia y para la comunicación telemática entre los miembros de la comunidad académica está cada vez más extendido. Todas esas herramientas digitales requieren, en mayor o menor medida, el tratamiento de datos personales de sus usuarios. Por ello, conforme al principio de responsabilidad proactiva que establece el RGPD[25], con carácter previo a su empleo en la actividad académica, los centros deben llevar a cabo una evaluación de su seguridad, examinando su política de privacidad y sus condiciones de uso, optando por las que ofrezcan la debida transparencia y garantías al tratamiento de los datos personales del alumnado y procurando su adecuación a las exigencias también del Esquema Nacional de Seguridad. Asimismo, deberán elaborar protocolos y recomendaciones para procurar que el tratamiento de los datos personales del alumnado por el profesorado se limite al necesario y adecuado para la finalidad docente, sin comprometer su intimidad.

Cautelas, todas ellas, que podrán verse frustradas en caso de usarse en la actividad académica otras herramientas digitales de comunicación (así ocurrirá, por ejemplo, cuando en lugar de usarse el correo institucional o las plataformas institucionales de apoyo a la docencia, se usan aplicaciones de mensajería instantánea, puesto que supondrán un tratamiento indebido de datos personales del alumnado, como sus números personales de teléfono).

Segunda recomendación:

"Igualmente, se recomienda evitar el correo institucional para fines privados no académicos".

[25] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Explicación:

El cumplimiento del principio de adecuación a la finalidad en el tratamiento de datos personales y razones de seguridad aconsejan deslindar nítidamente la actividad en línea personal y la académica. De modo que no sólo se recomienda que en la actividad académica se usen las herramientas digitales institucionales aprobadas o diseñadas para tal fin; sino que, igualmente, se recomienda que dichas herramientas digitales no se usen para fines distintos a los que les son propios.

Son muchos los inconvenientes de usar las herramientas institucionales para fines privados. Entre ellos cabe destacar la posible pérdida de información personal o sensible, cuando se termine la vinculación con la institución de enseñanza; la sobreexposición de datos personales frente a la institución; y el incremento del riesgo de la seguridad de la información de la institución. Téngase en cuenta que en torno al 94% del *malware* se distribuye por correo electrónico, por lo que es fácil que los usuarios sean el "eslabón más débil" de la cadena, por el que puedan tener cabida más fácilmente los ataques informáticos a la institución. Este riesgo se minimizará sensiblemente si el uso del correo institucional se limita a la actividad académica que le es propia.

Tercera recomendación:

"No difundas por redes sociales (incluidos grupos de whatsapp) el listado de calificaciones que el profesor/a sube a Prado".

Explicación:

Los servicios de mensajería online constituyen la forma más utilizada para comunicarse, así consta en informes recientes. No sólo los utilizamos, sino que lo hacemos con muchísima frecuencia, incluso llegándose a afirmar que "los españoles están enganchados al móvil".[26] De todas las formas de mensajería instantánea, ahora mismo, por el momento, whatsapp se coloca como la tercera red social más utilizada en el mundo,[27] aunque Telegram -sobre todo- o Signal están adquiriendo fuerza en la actualidad. Probablemente, llegará un momento en que tratemos otras formas de mensajería instantánea, debido a los cambios tan rápidos que se están produciendo en el uso de la tecnología.[28] Pero hoy por hoy, nos hemos centrado en whatsapp[29] donde hemos comprobado que la mayor parte del alumnado se incorpora a un grupo de whatsapp de la clase que previamente ha creado el delegado/a de la misma. Pues bien, el alumnado no sólo debe adquirir competencias digitales en orden a procurar la autotutela de sus datos personales y sus derechos, sino también ser respetuoso con los datos personales y los derechos de los demás. Para ello, hay que hacerle partícipe del deber de no comprometer los datos personales del resto de estudiantes, ni difundir sus datos académicos o privados entre terceros.

[26] Según los datos del Panel de Hogares de la CNMC sobre Usos de Internet, audiovisual y servicios OTT del primer semestre de 2019.

[27] Después de Facebook y You Tube. "Digital Report 2022: el informe sobre las tendencias digitales, redes sociales y mobile".

[28] Hay un dato que nos puede hacer pensar que adquirirán fuerza otras formas de mensajería instantánea. Según Statista, quien usa más whatsapp son los usuarios de entre 41-55 años, seguido por los usuarios de 2540 años, y ya baja mucho entre el colectivo de 18-24 años (recordemos que es el que se está incorporando al mercado de trabajo), y baja aún más para el colectivo entre 12-17 años. Esto significa que utilizan otras formas distintas de comunicarse. https://es.statista.com/estadisticas/576109/porcentaje-de-los-usuarios-de-whatsapp-en-espana-en-por-edad/

[29] Según Statista, en 2020, más de un 95% de los españoles eran usuarios de whatsapp https://es.statista.com/estadisticas/934626/servicios-de-mensajeria-instantanea-mas-utilizados-por-los-usuarios-de-internet-en-espana/ .

Cuarta recomendación:

"Evita dar información confidencial o sujeta a propiedad intelectual. No difundas apuntes y material colgado por el profesor/a en la plataforma educativa. Respeta la propiedad intelectual".

Explicación:

El uso masivo de las herramientas digitales ha facilitado el desarrollo de prácticas ética y jurídicamente cuestionables, por ser lesivas de los derechos de propiedad intelectual y a la imagen de terceras personas. El ámbito académico es caldo de cultivo de esa realidad, alentada por plataformas y sitios webs, en ocasiones con la excusa de mal entendidas "prácticas colaborativas" entre el alumnado, que comparte en ellas materiales docentes de toda clase (desde libros completos, a pruebas de evaluación, presentaciones, etc.).

Quinta recomendación:

"No grabes imágenes ni conversaciones con el dispositivo móvil en clase. No tienes el consentimiento ni del docente ni del alumnado".

Explicación:

La voz y la imagen de las personas son bienes tutelados por sus derechos fundamentales a la propia imagen y a la protección de datos personales. Por tanto, su tratamiento sin su consentimiento es ilícito. Aparte de que, según su contenido o el uso que se haga de las mismas, puedan resultar lesionados otros derechos (p. ej. la intimidad, el honor, la propiedad intelectual).

Sexta recomendación:

"No olvides que detrás de las pantallas hay personas.

— No filtres conversaciones

— Si a través de redes sociales te llegan contenidos violentos o lesivos a la intimidad de terceros (ej. *porn-revenge* o *sexting*), "páralo", no seas cómplice del daño.

— No generes bulos o noticias falsas, o información descontextualizada o sesgada, y con escasa calidad informativa.

— No contribuyas con tus mensajes al discurso de odio y la discriminación. Y evita actuaciones que puedan dar lugar a un caso de *ciberbullying"*.

Explicación:

Las tecnologías de la información y la comunicación e Internet nos ofrecen un potencial de acceso a la información y al conocimiento sin precedentes en la historia de la humanidad. Pero, cuando lo que circula a través de ellas son contenidos ilícitos, también tienen un potencial lesivo sin precedentes.

Por ello, la capacitación digital debe pasar por concienciar a los usuarios, desde edades tempranas, a ser selectivos con los contenidos a los que acceden en ellas y responsables con su uso,

de modo que las personas no se pongan en riesgo a sí mismas, pero tampoco lesionen a los demás. Es responsabilidad de todos contribuir a hacer del espacio en línea un espacio seguro.

Séptima recomendación:

"Recuerda que en los grupos de whatsapp, el/la administrador del grupo puede incurrir en responsabilidades por los comentarios lesivos vertidos por terceros, si no los elimina o les pone freno con diligencia".

Explicación:

Al margen de otras posibles responsabilidades en que se pueda incurrir (por lesión a la intimidad, el honor, la imagen o la integridad moral de las personas), las obligaciones y responsabilidades previstas en el Reglamento General de Protección de Datos (RGPD) no son aplicables a las personas físicas que traten datos personales de terceros para fines estrictamente privados. Es lo que se conoce como "excepción doméstica". Ahora bien, esa excepción es de interpretación restrictiva, por lo que no ampara, y sí estará sujeta al RGPD, a la actividad en línea que trascienda de un círculo restringido y limitado de personas (generalmente, familiares y amigos). Además, la jurisprudencia viene asimilando al prestador de servicios de alojamiento al administrador de perfiles o grupos de redes sociales, haciéndole, en consecuencia, responsable por los contenidos lesivos o ilícitos para terceros que otras personas publiquen en ellos, si teniendo conocimiento de los mismos no los bloquea o elimina con diligencia.

3.3. El bienestar digital y la desconexión

Recomendación:

Tenemos que fomentar las relaciones saludables con la tecnología.

— Por el estudiantado —que es el protagonista en la Universidad— en aras a su "salud emocional"[30], que va a repercutir entre otros aspectos en un mejor rendimiento académico.

— Por el resto del personal de la Universidad —profesorado y PAS cada vez más inmersos en una situación de hiperconectividad que les dificulta desconectar de sus funciones y que invade cada vez más su esfera personal— evitando enviar mensajes fuera del horario de trabajo respetando el derecho a la desconexión digital.

Explicación:

El concepto de bienestar digital abarca tanto el "estado al que se aspira de equilibrio óptimo con el uso diario de las tecnologías móviles y los medios digitales", como el conjunto de herramientas destinadas a lograr dicho estado de bienestar y entre estas la salud digital[31]. En íntima conexión con el bienestar digital está la desconexión digital.

[30] En palabras de la nueva Ley Orgánica del Sistema Universitario (LOSU), hace referencia en el preámbulo (I) a la "la salud emocional del estudiantado promoviendo asimismo su participación en el gobierno de la universidad en sus distintas unidades y en la propia gestión de servicios".

[31] Matassi, M.: ¿Qué es el bienestar digital? disponible en https://www.youtube.com/watch?v=HLWZTkNz3oM y "Las redes sociales operan como un somnífero pero la gente no lo ve como algo negativo" disponible en https://www.perfil.com/noticias/agenda-academica/mora-matassi-las-redes-sociales-operan-como-un-somnifero-pero-las-personas-no-lo-ven-como-algo-negativo.phtml, consultado el 24 de abril de 2023.

Conforme a la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales y La Ley 10/2021, de Trabajo a Distancia[32], todas las empresas y organizaciones, tanto públicas como privadas, tienen la obligación de garantizar el derecho a la desconexión digital de todas las personas trabajadoras como ya hemos visto.

En relación al alumnado universitario, la institución universitaria, así como su profesorado, tenemos la obligación de informar y formar en el uso responsable de las tecnologías y de Internet, advirtiendo que el abuso de sobreexposición tecnológica y la conectividad permanente producen impactos negativos en la salud mental, cardiovascular y musculoesquelética, así como prevenir conductas adictivas evitando estar conectado a Internet muchas horas al día por medio de diferentes dispositivos tecnológicos, lo que se denomina como "Uso problemático de Internet" (UPI)[33].

Es importante advertir de la diferencia entre la utilización de la red social en el ámbito laboral o profesional, social o amistoso, familiar, comercial…etc., de la utilización en actividades relacionadas con la enseñanza-formación, y en nuestro caso con la enseñanza universitaria pues claramente la finalidad perseguida es distinta debiendo primar las herramientas específicas que para esta finalidad proporciona la propia Universidad, a las que todos hemos tenido que acudir con ocasión de la pandemia COVID-19 en cursos académicos ya superados.

Entre las acciones de formación, información y sensibilización para toda la plantilla —además de las recogidas en los dos apartados anteriores que también se comprenden en el concepto de bienestar digital— y más directamente dirigidas a concienciar sobre la necesidad de la desconexión digital, recomendamos:

— La conveniencia de que en las universidades se utilizaran cuentas de correo electrónico institucionales donde se puedan programar tales correos para que se envíen en un momento determinado. Por ejemplo, si un alumno envía un correo electrónico a las 2:00 de la mañana un sábado, que no le llegue a la cuenta del profesor hasta el lunes por la mañana.

— Igualmente, sería conveniente que en la medida de lo posible se limitara en las universidades el uso de las redes sociales para uso académico, sobre todo en horario no lectivo. Aunque no hay reglas establecidas sobre qué medios de comunicación son los más adecuados para comunicarse con el alumnado, sí hay estudios que valoran de forma positiva su uso para este fin por sus buenos resultados en la formación del alumnado.[34]

— No enviar (ni atender) ninguna red social o correo electrónico de carácter laboral fuera del horario laboral y en ningún caso los fines de semana, días festivos y vacaciones.

[32] También se reconoce el derecho a la desconexión digital de los trabajadores en la Carta de Derechos Digitales, adoptada por el Gobierno de España en julio de 2021 (aunque ésta no tiene carácter vinculante).

[33] Hinojo Lucena, F.J.; Aznar Díaz, I.; Trujillo Torres, J.M.; Romero Rodríguez, J.M.: "Uso problemático de Internet y variables psicológicas o físicas en estudiantes universitarios", *Revista Electrónica de investigación Educativa (REDIE),* núm. 23, 2021.

[34] López Zapico, M.A., Tascón Fernández, J.: "El uso de Twitter como herramienta para la enseñanza universitaria en el ámbito de las ciencias sociales. Un estudio de caso desde la Historia económica", *Education in the Knowledge society,* vol. 14, núm. 2, Ediciones Universidad de Salamanca, 2013; Muñoz Vazquez, M.: "Las redes sociales como recurso educativo en el ámbito universitario", *Aularia: revista Digital de Comunicación,* vol. 2, núm., Grupo Comunicar, 2013; Nieto Rojas, P.: "La utilización de Twitter como herramienta docente: su aplicación al Grado de Relaciones Laborales y Empleo", *Lan harremanak, revista de relaciones laborales,* núm. 37, 2017; Romero López, I.:"Redes sociales de refuerzo positivo: interacciones sociales online para medir, analizar y mejorar resultados académicos, Universidad Castilla-La Mancha, 2016 (en línea), citados en Pérez del Prado, D.: "El uso de Twitter como herramienta docente", en VV.AA.: *Técnicas de innovación docente en Derecho del Trabajo y de la Seguridad Social,* Cuadros Garrido, Mª.E.; Selma Penalva, A. (Dirs.),Aranzadi, 2021.

— El horario laboral debe coincidir con el horario de disponibilidad a través de la conexión digital que debe estar claramente establecido por la Universidad incidiendo en que este es el horario también para enviar o recibir información digital.

— Sería recomendable que los profesores, al igual que fijan sus horas de clase y de tutorías, fijen su horario de trabajo hasta cumplir la jornada laboral de forma que a los alumnos les sea más fácil su conocimiento como ocurre con el personal de administración y servicios.

— Se aconseja, tanto a profesores como a alumnos, silenciar los grupos de whatsapp, o aplicaciones similares relacionados con el centro, fuera del horario laboral establecido. También se puede utilizar alguna de las distintas aplicaciones que nos van a permitir desconectar y no estar tan atentos al dispositivo móvil, organizando nuestro descanso y el tiempo de inactividad que necesitamos. Estas apps controlan el teléfono y todo lo que desde él mismo se genera, para conseguir que evadirnos del terminal, pero todo ello sin apagarlo, por si acaso (Offtime, Digital Detox, Digital Detox Dragons, Phoneless, Opal, minimalist pone, OffScreen, One Sec…).

3.4. Ante problemas, dónde dirigirse

Recomendaciones:

— En caso de brechas o fugas de datos personales, tenemos en la Universidad (*indicar aquí el nombre de la Universidad correspondiente*) un protocolo para ello. Ante cualquier duda con tu dispositivo puedes preguntar al Centro de Atención al Usuario de la Universidad (*indicar aquí el número de teléfono*). Desde ahí te redigirán donde corresponda. También puedes enviar un mail a (*indicar aquí el mail correspondiente)* y ante cualquier robo o pérdida de los dispositivos móviles, debes poner una denuncia ante la Policía Nacional. https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#"

— Si se produce un conflicto de CONVIVENCIA por un uso inadecuado de los dispositivos y este conflicto te afecta, puedes acudir a la Comisión de Convivencia creada por la Universidad… donde canalizarán tales conflictos.

- Si estamos ante un conflicto de convivencia derivado de infracciones al derecho de protección de daos, lo resolverá el Delegado/a de Protección de Datos.

- Si son trámites, quejas y denuncias sobre situaciones de acoso sexual, se canalizarán a través de (*indicar aquí dónde hay que dirigirse en la correspondiente universidad donde se aplique la guía*).

— Si quieres ejercitar tus derechos en materia de protección de datos personales puedes consultar este enlace (*indicar aquí el enlace correspondiente de la universidad donde se aplique la guía)*.

Explicación:

Son numerosas las recomendaciones que hemos realizado para un buen uso del teléfono móvil, y las hemos agrupado en función de su contenido (seguridad informática, protección de datos en el uso de redes sociales y mensajería instantánea o bienestar digital y desconexión). Aunque esta guía tiene como finalidad principal preservar la salud digital del alumnado, consideramos necesario

proporcionarles una hoja de ruta en caso de que tengan que comunicar algún hecho que les afecte y que se ha producido por un mal uso del teléfono móvil. Como ejemplos podemos citar: qué hacer ante un robo, o qué hacer si se han subido a las redes sociales un listado de calificaciones colgado previamente por el profesor/a en una plataforma institucional, o cómo se tiene que actuar si se ha producido una situación de acoso sexual a través del uso de la mensajería instantánea…

Es posible que el alumno/a no sepa cómo dónde acudir para exponer su problema. Y ello porque hay numerosos servicios que podrían tener competencia para conocer de estos asuntos (por ejemplo, los centros de seguridad informática de las universidades, las unidades de igualdad, la oficina de protección de datos…). Por este motivo, si cuentan con la información previa para saber dónde dirigirse, el alumno/a tardará menos en solucionar su problema, y además se implicará a menos personas para la solución del conflicto. Actuar con rapidez es muy importante en estos casos.

Estas recomendaciones que hemos incluido en la guía las tendrá que adaptar cada Universidad en función de cómo tenga estructurados sus organismos y sus competencias. Pero pueden servir de modelo para redactar este apartado que consideramos imprescindible. Las universidades cuentan con unidades o servicios específicos sobre seguridad informática, donde además de atender al usuario, llevan a cabo campañas de concienciación en materia de ciberseguridad, o informan sobre el Instituto Nacional de Ciberseguridad (INCIBE), la Oficina de Seguridad del Internauta (OSI), el Centro Criptológico Nacional (CCN), o la Agencia Española de Protección de Datos (AEPD). Incluir en esta guía una referencia a qué hacer en caso de fuga o brecha de datos personales es dar a conocer estos servicios que tiene la Universidad para que se pueda hacer un uso de los mismos.

Ahora bien, los problemas de seguridad informática no son los únicos existentes al usar el teléfono móvil. También peligra la intimidad del alumnado, o se pueden producir situaciones discriminatorias, o puede ocurrir que se insulte o se acose, o que se difundan datos personales sin consentimiento, provocando situaciones de conflicto en la comunidad universitaria.

Precisamente esta guía tiene una vocación preventiva, porque aplicando sus recomendaciones se evitan conflictos y se fomenta la convivencia en consonancia con lo establecido en la reciente Ley 3/2022, de 24 de febrero, de convivencia universitaria (LCU). [35] Precisamente es la finalidad de esta ley, establecer medidas "favorezcan y estimulen la convivencia activa y corresponsabilidad entre todos los miembros de la comunidad universitaria". Serán las universidades las que establezcan sus propias normas de convivencia y estas disposiciones "incluirán medidas de prevención primaria como la sensibilización, la concienciación y la formación, para fomentar el reconocimiento y el respeto a la diversidad y la equidad en el ámbito universitario, medidas de prevención secundaria para actuar sobre contextos, circunstancias y factores de riesgo, y evitar que se produzcan las situaciones de violencia, discriminación o acoso… y procedimientos específicos para dar cauce a las quejas o denuncias por situaciones de violencia, discriminación o acoso que pudieran haberse producido…" (artículo 4.2. LCU).

Sin duda esta guía puede cumplir con la función encomendada a las universidades de concienciar y sensibilizar y formar al alumnado para lograr una adecuada convivencia. Por este motivo, en esta recomendación que incluimos en la guía se ha hecho referencia a la comisión de convivencia, para que el alumno/a sepa dónde acudir ante este tipo de conflicto, haciendo una especial referencia a casos de conflictos producidos por acoso o por vulneración de datos personales.

Aunque no mencionamos el régimen disciplinario del estudiantado, pues la guía que aquí presentamos está destinada a prevenir, sería también conveniente explicarle al alumnado las

[35] BOE núm. 48, de 25 de febrero de 2022.

consecuencias que determinadas conductas pueden tener. Además, debido a la utilización cada vez mayor de los teléfonos móviles, es muy probable que las conductas sancionables se produzcan en su mundo digital a través de sus dispositivos móviles. De momento no contamos con datos de las actuaciones de la comisión de convivencia en las universidades, pues su creación es muy reciente, pero esperemos que con este tipo de propuestas como la que aquí presentamos se contribuya a evitar situaciones de conflicto.

4. CONCLUSIONES

La aplicación de la guía que hemos elaborado y que en este trabajo presentamos aportará sin duda, numerosos beneficios en la comunidad universitaria y en la sociedad en general, para prevenir e informar sobre los inconvenientes que se pueden presentar en cuanto o a la seguridad, privacidad, salud digital de alumnado y profesorado. También hay que destacar las grandes ventajas pedagógicas que supone su correcta utilización para la realización de actividades asíncronas y la creación de contenidos colaborativos con la participación de los estudiantes que de forma fácil y cómoda pueden acceder en cualquier momento y desde cualquier lugar, permitiendo la conexión de grupos de estudiantes y también con los profesores[36]. Un buen uso supone que el dispositivo móvil se convierta en una herramienta más para compartir conocimiento en igualdad y socializar en valores de compañerismo, solidaridad, que inspiran a la Universidad en el siglo XXI y en la conocida como "sociedad de la información".

Tenemos la convicción de que esta propuesta es de gran utilidad práctica y beneficiosa para la comunidad universitaria, donde al igual que en otros ámbitos de la vida se avanza en la utilización de internet y las redes sociales como una herramienta básica para la comunicación y transmisión de información, contribuyendo a la promoción de una relación saludable y equilibrada con la tecnología. Convencidos de que la información y la formación son aspectos totalmente necesarios para que los alumnos y los profesores adquieran la capacitación en la utilización y prevención de conductas no deseables.

5. BIBLIOGRAFÍA

Aznar-Diaz, I.; Hinojo-Lucena, F.J. Cáceres-Reche, M.P.; Romero Rodríguez, J.M.: "Analysis of the determingin factors of Good teaching practices of mobile learning at the Spanish University. An explanatory model, en *Computers&Education,* 2020.

González, H.T.: "Recursos tecnológicos para la integración de la gamificación en el aula", en *Tecnología, ciencia y educación,* núm. 13, 2019.

Hinojo Lucena, F.J.; Aznar Díaz, I.; Trujillo Torres, J.M.; Romero Rodríguez, J.M.: "Uso problemático de Internet y variables psicológicas o físicas en estudiantes universitarios", en *Revista Electrónica de investigación Educativa (REDIE),* núm. 23, 2021.

Lastiri Santiago, M.: "El metaverso: origen, evolución y retos actuales", en *La Ley mercantil*, núm. 99, 2023.

López Zapico, M.A., Tascón Fernández, J.: "El uso de Twitter como herramienta para la enseñanza universitaria en el ámbito de las ciencias sociales. Un estudio de caso desde la Historia económica", en *Education in the Knowledge society,* vol. 14, núm. 2, 2013.

Martin Y Ertberger, J (2013): "Here and now mobile learning: an experimental study on the use of the mobile technology. *Computer and Education,* 76-85.

[36] Se puede consultar más detenidamente en el Mooc "Mobile Learing. Claves para la aplicación de los dispositivos móviles en el aula". (Universidad de Granada, Coordinadora académica Inmaculada Aznar).

Matassi, M.: ¿Qué es el bienestar digital? disponible en https://www.youtube.com/watch?v=HLWZTkNz3oM y "Las redes sociales operan como un somnífero pero la gente no lo ve como algo negativo" disponible en https://www.perfil.com/noticias/agenda-academica/mora-matassi-las-redes-sociales-operan-como-un-somnifero-pero-las-personas-no-lo-ven-como-algo-negativo.phtml,, 2023.

Muñoz Vazquez, M.: "Las redes sociales como recurso educativo en el ámbito universitario", en *Aularia: revista Digital de Comunicación,* vol. 2, núm. 1, 2013.

Nieto Rojas, P.: "La utilización de Twitter como herramienta docente: su aplicación al Grado de Relaciones Laborales y Empleo", en *Lan harremanak, revista de relaciones laborales,* núm. 37, 2017.

Pérez del Prado, D.: "El uso de Twitter como herramienta docente", en VV.AA. *Técnicas de innovación docente en Derecho del Trabajo y de la Seguridad Social,* Cuadros Garrido, Mª.E. y Selma Penalva, A. (Dirs.), Aranzadi, 2021.

Romero López, I.: "Redes sociales de refuerzo positivo: interacciones sociales online para medir, analizar y mejorar resultados académicos", Universidad Castilla-La Mancha, 2016.

Romero-Rodríguez, J.M.; Martínez-Heredia, N.; Campos Soto, M.N.; Ramos Navas-Parejo, M.: "Influencia de la adicción a Internet en el bienestar personal de los estudiantes universitarios", en *Health and Addictions/Salud y Drogas*, núm. *21*, 2021.

Tascón Lopez, R.: "El derecho de desconexión del trabajador (potencialidades en el ordenamiento español)", *Trabajo y Derecho,* núm. 41, 2018.