INCORPORAR LA SALUD Y SEGURIDAD EN EL TRABAJO A LA EVALUACIÓN DE LOS RIESGOS DE CIBERSEGURIDAD

Resumen

En el presente informe se analiza una nueva perspectiva de investigación de la relación entre las ciberamenazas y la seguridad y salud de las población trabajadora. Para ello es preciso dejar a un lado la visión tradicional de la ciberseguridad, centrada únicamente en los aspectos técnicos, y ampliar el análisis a las consecuencias humanas y sociales de los ciberataques.

Ante la creciente adopción de la tecnología digital en todas las organizaciones y el incremento de los ataques contra sus sistemas y redes informáticos, es preciso tomar en consideración los nuevos riesgos emergentes relacionados con la seguridad y salud en el trabajo. En los próximos años habrá que hacer frente a nuevas necesidades y retos en esta materia.

La situación de la ciberseguridad

Durante los últimos años, la ciberseguridad se ha convertido en un tema candente para las empresas de todos los sectores. La ciberdelincuencia es cada vez más sofisticada y quienes la ejercen explotan todo tipo de vulnerabilidades para realizar sus ataques, ya sean físicas, técnicas o humanas.

Según el *Cambridge Dictionary*, un ciberataque es «un intento ilegal de dañar el sistema informático de una persona, o la información que este contiene, utilizando internet»[1]. Más específica es la definición del NIST (National Institute of Standards and Technology), según la cual un ciberataque es «un ataque a través del ciberespacio cuyo objetivo es el uso que hace una empresa del ciberespacio con el fin de alterar, inhabilitar, destruir o controlar de manera maliciosa un entorno o infraestructura informática, o destruir la integridad de los datos o robar información controlada»[2].

En un mundo cada vez más digitalizado, todas las empresas están en riesgo de ciberataque. En particular, 2020 fue un año crucial tanto en lo que respecta a la digitalización como a los problemas de ciberseguridad. Las empresas han adoptado más procedimientos organizativos basados en la flexibilidad y la tecnología de cara al teletrabajo, principalmente a causa de la pandemia de COVID-19, pero esto ha resultado ser terreno abonado para la ciberdelincuencia, hasta el punto de que el 78 % de las organizaciones han experimentado un mayor volumen de ciberataques debido a un cambio de tendencia hacia el teletrabajo[3].

El 87 % de las organizaciones de todo el mundo han sufrido algún intento de explotación de una vulnerabilidad ya existente, mientras que el 71 % de los profesionales de la seguridad han observado un incremento de las ciberamenazas (como el *phishing*, los programas maliciosos o los programas de chantaje) desde que comenzara la pandemia[4].

En conjunto, los ciberataques continúan aumentando, no solo en número de incidentes, sino también en cuanto a su impacto (ENISA, 2021a), mientras que los recursos y herramientas de los que se dispone para hacerles frente son diferentes según los países. Por ejemplo, en función de determinados factores como el compromiso con la ciberseguridad y la legislación, tres países europeos (Portugal, Lituania y Eslovaquia) aparecen clasificados como los mejores en el índice de ciberseguridad[5].

El incremento de las amenazas ha determinado la necesidad urgente de que la Comisión Europea ponga en marcha una estrategia eficaz de ciberseguridad de la UE para la década digital[6] a fin de

[1] https://dictionary.cambridge.org/dictionary/english/cyberattack
[2] https://csrc.nist.gov/glossary/term/cyber_attack
[3] https://atlasvpn.com/blog/cyberattack-volume-grew-in-78-of-businesses-globally
[4] https://www.checkpoint.com/pages/cyber-security-report-2021/
[5] https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/
[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

garantizar una digitalización segura, mejorando la resiliencia, desarrollando la capacidad de prevenir y responder a ciberincidentes y estableciendo una política sobre el ciberespacio coherente a escala internacional. Además, dicha estrategia pone de relieve la importancia de establecer un programa de concienciación sobre el ciberespacio para todas las instituciones, organismos y agencias de la UE con el fin de crear una cultura de ciberseguridad efectiva.

Amenazas actuales y futuras

Se estima que el coste de la ciberdelincuencia en todo el mundo alcanzará la cifra de 10,5 billones USD anuales para 2025[7]. De hecho, hay diversos agentes que utilizan el ciberespacio para fines maliciosos y con distintas motivaciones, desde ciberdelincuentes que buscan sobre todo el lucro económico hasta ciberterroristas animados por objetivos políticos e ideológicos. El panorama de la delincuencia en internet es muy amplio e incluye numerosas acciones ilegales —ya conocidas en el mundo físico— como la usurpación de identidad, el fraude, el espionaje o los delitos contra la propiedad intelectual, así como varias formas de ciberviolencia (como el acecho o el acoso). Estas acciones pueden servirse de los poderosos medios que proporciona el contexto digital y, debido a que el mundo está cada vez más interconectado, la ciberdelincuencia representa uno de los principales riesgos que se plantean para las dos próximas décadas[8].

Las ciberamenazas tienen gran prioridad para cualquier organización y país, debido a la variedad y gravedad de sus consecuencias: desde la pérdida de información valiosa hasta la parálisis de los sistemas informáticos y los servicios conexos, así como la gravedad de los riesgos que entrañan para la seguridad y la salud de las personas.

Pese a que se conocen desde hace años, algunos tipos frecuentes de ciberamenazas (cuadro 1), como el *phishing* y los programas de chantaje, continúan en aumento[9]. De hecho, son muy rentables para los ciberdelincuentes y el coste de su ejecución es muy bajo en comparación con el riesgo de que las personas atacantes sean detenidas (Hernández-Castro *et al.*, 2020). El *phishing* sigue siendo una de las principales tácticas de violación de la seguridad (Verizon, 2021), pero la diversidad de formas de los ciberataques demuestra la complejidad del panorama de ciberamenazas. Por ejemplo, los ataques a las cadenas de suministro van en aumento y representan una importante preocupación para las organizaciones de cara al futuro (ENISA, 2021b)[10].

Cuadro1: Algunas de las ciberamenazas más frecuentes[11]

Tipo	Descripción
Phishing y *phishing* personalizado	El *phishing* es la práctica de enviar comunicaciones fraudulentas que parecen provenir de una fuente legítima, habitualmente por correo electrónico. El objetivo es robar datos sensibles como la información de tarjetas de crédito o de inicio de sesión o instalar programas maliciosos en el dispositivo de la víctima. Hay diferentes formas de *phishing*, como el *phishing* personalizado, que es una variante más sofisticada de esta práctica que se dirige a una persona u organización concreta.

[7] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[8] https://www.weforum.org/agenda/2020/12/3-disruptive-frontier-risks-that-could-strike-by-2040/
[9] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[10] Una cadena de suministro es «la combinación del ecosistema de recursos necesarios para diseñar, fabricar y distribuir un producto». En el ámbito de la ciberseguridad, una cadena de suministro incluye equipos y programas informáticos, medios de almacenamiento local o en la nube y mecanismos de distribución https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[11] Son algunas de las ciberamenazas más frecuentes documentadas por la ENISA (2020, 2021). Véase también una descripción de las amenazas en el siguiente enlace: https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Tipo	Descripción
Programas maliciosos y programas de chantaje	El término general «programas maliciosos» se utiliza para describir distintos tipos de programas informáticos malintencionados como programas espía, programas de chantaje, virus y gusanos. Los programas de chantaje, por ejemplo, son un tipo de programa malicioso que encripta la información de la víctima y exige un pago a cambio de la clave para descifrarla. Es uno de los tipos de ciberataque más lucrativos.
Ingeniería social	La ingeniería social es una técnica que se utiliza para engañar y manipular a las personas con el fin de obtener información confidencial o acceder a sus ordenadores. El *phishing* es un ejemplo de ingeniería social.
Denegación de servicio (DoS)	Este tipo de ataque inunda sistemas, servidores o redes con tanto tráfico que el sistema es incapaz de procesar las peticiones legítimas. Los atacantes también pueden utilizar numerosos dispositivos comprometidos (ataque distribuido de denegación de servicio o DDos).
Violación de la seguridad de los datos	Una violación de la seguridad de los datos es un incidente de ciberseguridad en el que se roba información o se extrae de un sistema o se utiliza sin autorización.
Ciberespionaje	El objetivo de las actividades de ciberespionaje es robar datos sensibles o clasificados o propiedad intelectual con el fin de obtener una ventaja sobre una empresa rival o una entidad gubernamental.
Campañas de desinformación e información errónea	La desinformación consiste en crear y compartir información falsa de forma deliberada para causar daños. La información errónea es información falsa o inexacta que se propaga de forma accidental. Ambas cosas pueden ser preparativos para otros ataques (como la ingeniería social y el *phishing*) y utilizarse conjuntamente con otras ciberamenazas.

La paradoja es que, por un lado, pueden utilizarse tecnologías innovadoras para crear nuevas soluciones destinadas a mejorar la ciberseguridad mientras, por otro, esas mismas tecnologías ofrecen nuevas oportunidades a los propios ciberdelincuentes. De ahí que, al tiempo que se utiliza la inteligencia artificial (IA) de forma positiva para la detección de intrusiones y la identificación de programas maliciosos (Truong *et al.*, 2020), se desarrollan nuevas amenazas y se refuerzan las amenazas tradicionales (Brundage *et al.*, 2018). Por ejemplo, se pueden utilizar las tecnologías de IA para automatizar los ataques de ingeniería social, así como incrementar la eficacia de los programas maliciosos. Además, la proliferación de dispositivos de la internet de las cosas (IdC) implica nuevas vulnerabilidades que hay que tener en cuenta, ya que su capacidad de procesamiento y almacenamiento es más débil y ello limita las aplicaciones de seguridad para su protección[12].

Ciertas situaciones laborales han incrementado las oportunidades para quienes practican la ciberdelincuencia. El teletrabajo, por ejemplo, ampliamente adoptado en 2020 debido a la COVID-19, ha planteado nuevos retos para la seguridad de las empresas, como la creación de parámetros adicionales que pueden resultar vulnerables a violaciones de la seguridad o el uso de dispositivos personales en actividades relacionadas con el trabajo (práctica que en inglés se conoce como «Bring Your Own Device» o BYOD)[13]. De hecho, la comodidad de encontrar todo en un único dispositivo está

[12] https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/
[13] https://www.techrepublic.com/article/how-to-combat-the-security-challenges-of-a-remote-workforce/

asociada a importantes riesgos para la seguridad, por ejemplo cuando las conductas imprudentes relacionadas con el uso privado de los dispositivos digitales se extienden al uso empresarial (Disterer y Kleiner, 2013). Por no mencionar que la pérdida de un dispositivo digital implica poner en riesgo no solo la información personal, sino también la empresarial. Por consiguiente, el teletrabajo representa un reto para la seguridad de las empresas, a las que se insta a revisar sus políticas corporativas e invertir en formación adecuada para su personal (Borkovich y Skovira, 2020).

También es interesante observar que las propias personas trabajadoras que utilizan dispositivos ponibles (como auriculares inalámbricos o relojes inteligentes) pueden facilitar involuntariamente la actividad de los ciberdelincuentes. De hecho, las tecnologías ponibles presentan ciertos riesgos de ciberseguridad, como los dispositivos conectados a un ordenador portátil corporativo que podrían introducir virus en el sistema de la empresa, así como riesgos para la privacidad a causa de accesos no autorizados (Heembrock, 2015).

Otras ciberamenazas emergentes representan preocupaciones adicionales tanto para los particulares como para las empresas, debido al efecto amplificador de la redes sociales. Las ultrafalsificaciones o *deep fakes*, por ejemplo, consisten en la alteración por medios digitales de archivos de audio o vídeo de ciertas personas —a menudo personajes famosos o personalidades políticas— con fines maliciosos, como propagar información falsa y perjudicar su reputación. Sin embargo, la preocupación por estas amenazas va más allá de la propaganda y las elecciones políticas, ya que también pueden afectar a las empresas a través de la manipulación de los mercados, el sabotaje de marcas, el chantaje y la suplantación digital de un miembro de la dirección (Westerlund, 2019).

Por último, teniendo en cuenta los impresionantes avances de la innovación tecnológica, se estima que la informática cuántica, que puede procesar información de modo mucho más eficiente que los procedimientos tradicionales, podría ya estar disponible para 2025[14]. En teoría, estos ordenadores podrían desencriptar muchos de los sistemas de cifrado de seguridad actuales, pero se requieren importantes avances tecnológicos[15] para que esta tecnología sea de uso práctico.

En vista de la situación descrita, resulta evidente por qué los riesgos de ciberseguridad aparecen clasificados entre los riesgos mundiales más graves (Foro Económico Mundial, 2021).

El impacto de los ciberataques sobre la SST

Los ciberataques contra empresas e instituciones siempre se han analizado desde un punto de vista tecnológico, aunque el factor humano representa una parte igualmente importante del problema de la ciberseguridad (Corradini *et al.*, 2020). Del mismo modo, cuando se considera el impacto de los ciberataques, se pone el foco principalmente en los aspectos económicos (Cashell *et al.*, 2004; Anderson *et al.*, 2013) y raramente en la seguridad y salud de las población trabajadora. De hecho, el impacto se cuantifica principalmente en términos de costes tangibles, como la pérdida de datos y la interrupción de las operaciones empresariales, y de costes intangibles, como la pérdida de ventaja competitiva ocasionada por la pérdida de propiedad intelectual y el perjuicio para la reputación de la marca[16].

En realidad, los ciberataques pueden causar problemas psicológicos y daños físicos a las personas, incluso con pérdida de vidas: por consiguiente, está claro que la evaluación de los riesgos de ciberseguridad y la evaluación de los riesgos de SST en el lugar de trabajo no pueden considerarse actividades independientes, sino que deben llevarse a cabo conjuntamente (Izuakor, 2016). En consecuencia, las empresas deberían tomar en consideración los diversos impactos de las ciberamenazas y adoptar un enfoque más integral para optimizar la gestión de los riesgos de ciberseguridad (Couce-Vieira *et al.*, 2020), como se describe, por ejemplo, en el cuadro 2.

[14] https://builtin.com/founders-entrepreneurship/quantum-computing-revolution
[15] https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat
[16] https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/cyber-security-is-your-organisation-under-threat-of-a-cyber-attack.html

Cuadro 2: Diversidad de impactos objeto de la gestión de los riesgos de ciberseguridad

Categorías	Impacto
Organización	Daños económicos (como la reducción de la producción a causa de la indisponibilidad del servicio, la pérdida de cuota de mercado o la pérdida de ventajas de competitividad)
	Daños reputacionales (pérdida de confianza de las partes interesadas)
	Otros aspectos económicos (como los ciberseguros)
Personal	Daños físicos (como la pérdida de vidas a causa de un fallo en un sistema ciberfísico)
	Daños psicosociales (como ansiedad o frustración)
	Impacto sobre los derechos individuales (violación de la privacidad derivada de violaciones de la seguridad de los datos)
	Daños económicos personales
Otras organizaciones relacionadas	Perjuicios causados por la alteración de las interconexiones de la cadena de suministro global
Medio ambiente	Impacto sobre el medio ambiente natural (como la contaminación de la tierra a causa de un ciberincidente)

Adaptado de Couce-Vieira *et al.*, 2020

Estos impactos pueden ir asociados a costes cuantificables en términos económicos, como la pérdida de cuota de mercado, o no económicos, como los daños para la salud física o mental de las personas.

La siguiente sección trata de la importancia de los posibles impactos físicos y psicológicos para la seguridad y saludde las personas.

Aspectos de la ciberseguridad relacionados con la seguridad de las personas

La escasa consideración que merecen los aspectos de la ciberseguridad relacionados con la seguridad de las personas podría atribuirse a que los riesgos de ciberseguridad se perciben como amenazas externas, mientras que los problemas de seguridad y salud de la población trabajadora se atienden en el seno de las organizaciones[17]. Sin embargo, la evolución de las ciberamenazas y la creciente exposición de las organizaciones a ciberataques hace necesario adoptar un enfoque integral para hacerles frente de manera efectiva, incluida la protección de la seguridad y salud en el trabajo.

Los ciberataques no solo pueden poner en riesgo los activos de información de una organización, sino que también la seguridad física y mental del personal puede verse amenazada cuando los piratas informáticos o jáqueres atacan infraestructuras críticas[18] o toman el control de sus dispositivos tecnológicos. La manipulación de una máquina, por ejemplo, puede causar daños físicos a las personas y comprometer la información personal (Loukas, 2019).

Algunos ejemplos pueden aclarar esta cuestión. En 2014, una planta siderúrgica de Alemania fue jaqueada y los atacantes lograron apagar el horno[19]; el riesgo de que el ciberataque se transformase en un episodio crítico para la seguridad del personal fue muy alto, debido a la naturaleza de los materiales afectados.

[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/
[18] Las infraestructuras críticas son vitales para el funcionamiento de un país, dado que incluyen sectores como la energía, la salud pública, las telecomunicaciones, la banca y las finanzas.
[19] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

En 2017, la FDA (Food and Drug Administration de Estados Unidos) retiró aproximadamente 465 000 marcapasos por vulnerabilidades de seguridad. Los dispositivos eran susceptibles de pirateo informático, por lo que estaba en riesgo la vida de los pacientes[20].

Los ciberataques a los sistemas de control industrial (SCI) que incluyen elementos físicos y cibernéticos son una amenaza peligrosa para la vida humana. Cabe citar los ejemplos de Stuxnet[21], un gusano informático creado en 2010 para tomar el control de las centrifugadoras iraníes utilizadas para enriquecer uranio, o Triton Malware[22], que en 2017 infectó instalaciones petroquímicas de Oriente Medio y, por fortuna, fracasó. Estos tipos de ataques también pueden acarrear graves consecuencias para el medio ambiente.

El uso de equipos a distancia en situaciones peligrosas puede poner en riesgo la seguridad de la población trabajadoras, como en el caso de vehículos o máquinas que quedan fuera de control debido a la interrupción de señales inalámbricas o a los ataques de piratas informáticos (Steijn *et al.*, 2016).

En el sector de fabricación, cuando humanos y robots cooperan en las líneas de producción, los ciberataques podrían interrumpir procesos industriales físicos y causar heridas a las personas (Perales Gómez *et al.*, 2020).

Según Gartner, en el horizonte de 2025, los ciberatacantes podrían utilizar la tecnología operativa (TO) y otros sistemas ciberfísicos a modo de armas para herir o matar a seres humanos[23].

Si un pirata informático lanzase un ciberataque a un hospital, podría obtener acceso a información delicada de pacientes y plantilla, pero lo que puede correr un grave peligro es la capacidad para que los pacientes reciban la atención adecuada y las operaciones médicas necesarias (Argaw *et al.*, 2020)[24]. El análisis del ataque global realizado en mayo de 2017 con el programa de chantaje «WannaCry» revela importantes efectos negativos para el servicio nacional de salud británico (Ghafur *et al.*, 2019).

Durante la pandemia de COVID-19, los hospitales estadounidenses fueron objeto de una ola de ataques con programas de chantaje que interrumpieron la prestación de asistencia sanitaria en varios hospitales, con grave riesgo para la vida de los pacientes[25]. Los estudios sobre el uso de programas de chantaje contra organizaciones de atención sanitaria revelan que estas ciberamenazas pueden tener consecuencias de vida o muerte (Ponemon, 2021).

Impactos sociales y psicológicos

Los ciberataques pueden ir asociados a impactos sociales como la pérdida de confianza en la tecnología digital e impactos psicológicos como ansiedad, ira y depresión (Bada y Nurse, 2020). Las personas trabajadoras afectadas por ciberataques también pueden tener sentimientos de vergüenza, culpabilidad, confusión o frustración, especialmente en caso de fuga de información digital, y la importancia de estos impactos depende del entorno afectado por el ciberataque (Agrafiotis *et al.*, 2018). Por ejemplo, los daños psicológicos pueden ser mayores en una entidad financiera, donde las consecuencias de una violación de la seguridad de los datos pueden ser más graves que en otra entidad proveedora de servicios. En casos más extremos, la consecuencia de una fuga de datos puede a las personas afectadas al suicidio de—debido a la vergüenza que les causa la exposición pública de su información[26]— y la carga psicológica para el personal puede ser muy difícil de soportar.

---

[20] https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362

[21] https://spectrum.ieee.org/the-real-story-of-stuxnet

[22] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/

[23] https://www.thehindubusinessline.com/info-tech/cyber-attackers-could-weaponise-tech-to-kill-humans-by-2025-gartner/article35519872.ece

[24] En 2020, un hospital alemán fue víctima de un ataque informático que le impidió admitir pacientes. Una mujer que había llegado allí para recibir atención falleció de camino a otro hospital situado a más de 30 km de distancia. Tras la investigación, la fiscalía dictaminó que no había pruebas suficientes, pero es sabido que el departamento de urgencias del hospital tuvo que cerrar debido a un ataque con un programa de chantaje. https://www.wired.co.uk/article/ransomware-hospital-death-germany

25 https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/

[26] Un caso de consecuencias dramáticas fue el de Ashley Madison, una red social de citas jaqueada en julio de 2015. Los datos publicados por los piratas informáticos incluían nombres, contraseñas y direcciones, pero también información sobre las

De ahí que la privacidad y la seguridad estén cada vez más entrelazadas: mientras la privacidad se refiere a la recogida y utilización de datos personales, la seguridad tiene por objeto garantizar la protección de esos datos[27]. El Reglamento General de Protección de Datos (RGDP), que entró en vigor el 25 de mayo de 2018, exige que las organizaciones cumplan obligaciones de protección de datos y privacidad en la UE[28] y, en caso de violación de la seguridad de los datos que entrañe un riesgo para los derechos y libertades de los usuarios, las empresas tienen un plazo de 72 horas para notificarlo a las personas afectadas por dicha violación.

Es interesante observar cómo la violación de la privacidad puede tener efectos negativos para la salud mental de las personas. De hecho, la privacidad representa una necesidad psicológica estrictamente relacionada con el desarrollo de la identidad personal (Aboujaoude, 2019).

Los estudios sobre la victimización causada por la ciberdelincuencia ponen de relieve las experiencias negativas de empresas y particulares (por ejemplo, Augustina, 2015, y McGuire y Dowling, 2013). Especialmente cuando las organizaciones sufren ataques con programas de chantaje, los miembros de los departamentos de informática se ven afectados por el perjuicio que supone para su confianza profesional y para el aprecio que merece el personal cualificado[29]. Por otra parte, los ataques con programas de chantaje pueden tener un mayor efecto psicológico para las personas que otros incidentes de ciberseguridad, dado que, cuando las empresas pagan el chantaje, están «recompensando» a los atacantes en lugar de invertir dinero en su personal[30].

Cabe hacer consideraciones adicionales acerca del error humano, que se considera la causa principal del 90 % de las brechas de ciberseguridad[31]. Estos errores, como abrir correos electrónicos de *phishing* o descuidar la gestión de las contraseñas, pueden exponer a las organizaciones a graves consecuencias, como la instalación accidental de programas maliciosos en la red de la empresa. Es fácil imaginar la sensación de fracaso que experimentan las personas trabajadoras responsables de lo sucedido, una sensación que también puede suponer un freno a la hora de comunicar el error a su organización.

Con respecto a los errores humanos, es importante considerar los factores psicológicos que intervienen en los incidentes de ciberseguridad: el 52 % de las personas tienen más probabilidades de cometer errores cuando están estresadas, el 43 % cuando están cansadas y el 26 % cuando se sienten quemadas[32]. Por no mencionar que el personal profesional de la ciberseguridad sufre un alto grado de estrés o el síndrome de agotamiento profesional por trabajar en la prevención y mitigación de ciberataques[33]..

Por último, a modo de nota al margen, es importante observar cómo la dimensión ciberespacial afecta a los fenómenos de violencia. La ciberintimidación, por ejemplo, cuyo objetivo es humillar, perseguir y controlar a una persona utilizando medios digitales, es la forma más conocida de acoso en internet (Notar *et al.*, 2013). Aunque este fenómeno no se inscriba estrictamente en el campo de la ciberseguridad, los ataques con programas maliciosos y la suplantación de identidad pueden utilizarse para hacer daño a las personas. El acoso en internet puede producir efectos psicosomáticos, sociales y mentales graves (Dressing *et al.*, 2014; Betts, 2016). Por consiguiente, considerando que la ciberintimidación en el trabajo (Corradini, 2019; Farley *et al.*, 2021) puede poner en riesgo la seguridad y salud de la población trabajadora, este problema debería atenderse correctamente.

Objetivo de los ciberataques

Todos los sectores laborales cuentan con tecnología de innovación. Todas las organizaciones —microempresas y pequeñas y medianas empresas (pymes), así como las grandes empresas— pueden

preferencias sexuales de los clientes. Tras esta violación de la seguridad de los datos, se produjeron dimisiones, divorcios y suicidios. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/CYB-ET/Pres/8-4%20Waleed%20Hagag_PrivacyVSSecurity.pdf

[28] https://gdpr.eu/tag/gdpr/

[29] https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx

[30] https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

[31] https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

[32] https://www.tessian.com/research/the-psychology-of-human-error/

[33] https://news.vmware.com/security/hacking-burnout-for-cybersecurity-awareness-month-2021

ser objetivo de los ciberdelincuentes y, por tanto, corren el riesgo de sufrir ciberataques. Muchas microempresas y pequeñas empresas carecen de los recursos necesarios para defenderse, como demuestra el hecho de que el 43 % de las violaciones de seguridad de los datos afectan a este tipo de empresas (Verizon, 2019).

Está claro que, en un mundo crecientemente digitalizado, las empresas están cada vez más interconectadas, por lo que se amplía la superficie de ataque.

En cuanto a los sectores más vulnerables a los ciberataques, según el informe de IBM sobre la seguridad en 2021, las finanzas y los seguros fueron los que más ataques sufrieron en 2020 (23 %), seguidos de la fabricación (17,7 %), la energía (11,1 %), el comercio minorista (10,2 %), los servicios profesionales (8,7 %), las administraciones públicas (7,9 %), la asistencia sanitaria (6,6 %), los medios de comunicación (5,7 %), el transporte (5,1 %) y la educación (4,0 %).

Si observamos la evolución de los sectores afectados por ciberataques, hay estudios que ponen de relieve que el sector sanitario se está convirtiendo en un objetivo muy atractivo para los ciberdelincuentes[34], sobre todo debido a la información delicada que se conserva en las historias clínicas (Martin *et al.*, 2017). La pandemia de COVID-19 ha agravado la situación, de modo que quienes ejercen la ciberdelincuencia han dirigido su atención a la propiedad intelectual relativa al desarrollo de vacunas (Muthuppalaniappan y Stevenson, 2021) y han comenzado a utilizar correos electrónicos de *phishing* con la temática de la COVID-19[35]. Sin embargo, el sector sanitario ha sufrido grandes transformaciones a consecuencia de su lucha contra la pandemia y, según algunas perspectivas de futuro, deberá reducir su exposición en materia de seguridad[36].

Incluso las organizaciones docentes se están convirtiendo en un objetivo atractivo para los ciberdelincuentes, si se tiene en cuenta que el 44 % fueron atacadas con programas de chantaje en 2020 y el 35 % de estas pagaron el chantaje para recuperar sus datos[37]. Las causas se atribuyen esencialmente a las limitaciones de los presupuestos de ciberseguridad y a la ingente cantidad de usuarios, como el alumnado y el personal, que puede incrementar la exposición a los ataques. Por otra parte, la falta de cultura digital entre el personal docente y el alumnado obliga a adoptar programas de formación para un uso responsable de las tecnologías digitales (Corradini y Nardelli, 2020).

La situación actual en lo que respecta a los ciberataques está en constante evolución, por lo que es esencial llevar un control de actualizaciones año a año. Entre tanto, se presenta un panorama todavía más preocupante. De hecho, quienes se sirven de programas de chantaje están poniendo a prueba nuevos métodos de extorsión, que hacen que las organizaciones cooperen y compartan información para responder a las amenazas[38].

Factores de riesgo de victimización

Los ciberdelincuentes están más interesados en atacar a las empresas utilizando contraseñas robadas que en cometer ataques masivos para obtener información de consumidores[39]. Sin embargo, 330 millones de adultos de diez países sufrieron ciberdelincuencia en 2020[40], por no mencionar que una estrategia eficaz para obtener acceso a una organización es atacar a determinada población trabajadora, por ejemplo, mediante el *phishing* personalizado.

El riesgo de ser víctima de las diferentes formas de ciberdelincuencia depende de factores personales y ambientales (Jansen *et al.*, 2017) y los estudios de los perfiles de las víctimas pueden ayudar a comprender mejor la relación entre los ciberataques y el contexto de las víctimas.

[34] https://cybersecurityguide.org/industries/healthcare/
[35] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home
[36] https://www.protiviti.com/US-en/insights/whitepaper-top-risks-2021-and-2030-healthcare-industry-perspective
[37] https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/
[38] https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021
[39] https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/?utm_source=email&utm_medium=TMIEmail012821&utm_campaign=2020DBRReport
[40] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

Si se analiza a las víctimas de la ciberdelincuencia por generaciones, por ejemplo, parece que las personas adultas jóvenes (menores de 25 años) y las de mayor edad (más de 75 años) son más vulnerables a los ciberataques[41]. El género representa un importante factor que influye en el comportamiento relacionado con la ciberseguridad (Anwar *et al.*, 2017), aunque puede ser muy interesante continuar las investigaciones en este terreno —y según características demográficas— para plantear las actividades de prevención. Algunos estudios demuestran que las mujeres tienen más probabilidades de ser objeto de ataques de *phishing* (Darwish *et al.*, 2012), mientras otros revelan que ellas están más preocupadas por la privacidad en las redes sociales que los hombres (Tifferet, 2019).

Por último, teniendo en cuenta la necesidad de reforzar los entornos laborales contra las ciberamenazas, parece interesante analizar cómo afectan los factores organizativos, como las normas y las rutinas, a la susceptibilidad de las personas a los correos electrónicos de *phishing*, personalizado o no (Williams *et al.*, 2018). Un análisis tan amplio podría proporcionar información útil para mejorar el diseño de las interfaces y los programas de concienciación del personal.

Para un enfoque integral de la ciberseguridad: el papel de la concienciación

La relación entre las ciberamenazas y la SST representa un reto muy dinámico para las organizaciones, a las que se insta a integrar todas las medidas necesarias para adoptar un enfoque de ciberseguridad corporativa general[42].

Esta perspectiva requiere combinar los aspectos de seguridad y de protección, que normalmente se consideran conceptos separados, debido a diferentes límites legislativos, intereses y cuestiones prácticas (Boustras y Waring, 2020).

Para alcanzar este objetivo, la concienciación de las diferentes partes interesadas tiene un papel fundamental, que debe desarrollarse a partir de las perspectivas de la ciberseguridad y la SST, estrictamente interconectadas.

En lo que respecta a las cuestiones de ciberseguridad, hay estudios que ponen de relieve que el incorrecto cumplimiento de las políticas de protección y otros factores organizativos, como la insuficiencia de las medidas de respuesta, hacen que las organizaciones sean vulnerables a los ciberataques (Hart, 2019). Además, con independencia de la variedad de sectores laborales, la falta de concienciación de las personas en materia cibernética es responsable de numerosos incidentes de ciberseguridad[43]. De ahí que los programas de concienciación sobre el ciberespacio puedan desempeñar un papel importante para crear una cultura de ciberseguridad eficaz en las organizaciones (Corradini, 2020) y prevenir ciberataques (Aldawood y Skinner, 2018).

La concienciación sobre las posibles consecuencias de los ciberataques en el ámbito de la SST requiere ampliar el foco de atención a factores de riesgo que tradicionalmente no se toman en consideración en relación con la seguridad y salud en el trabajo. Las experiencias positivas derivadas de la gestión de riesgos de SST también podrían ser una gran fuente de inspiración, dado que las organizaciones cuentan con muchos más años de experiencia en este tema que en el ámbito de la ciberseguridad, y numerosos programas y aplicaciones destinados a incrementar la seguridad personal en el entorno de trabajo se siguen aplicando con éxito. Por otra parte, controlar el error humano se considera vital para prevenir accidentes en el ámbito de la SST.

Además, dado que los servicios, departamentos o expertos en materia de seguridad informática no suelen estar familiarizados con la SST y que, del mismo modo, la comunidad de SST no está familiarizada con las ciberamenazas, la cooperación entre estos dos ámbitos es esencial. Por ejemplo, la cooperación entre los departamentos de SST, Recursos Humanos y Seguridad Informática de una organización, en la medida de lo posible, puede facilitar que el problema de las ciberamenazas se considere desde distintas perspectivas y que se apliquen soluciones preventivas más eficientes e innovadoras.

[41] https://risk.lexisnexis.co.uk/about-us/press-room/press-release/20200223-biannual-cybercrime-report
[42] https://app.croneri.co.uk/feature-articles/health-safety-and-cyber-threats?topic=3682&product=154&section=3511
[43] https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

Concienciar a las partes interesadas

Teniendo en cuenta lo que se acaba de explicar, el primer paso es sensibilizar a las distintas partes interesadas acerca de los riesgos de SST asociados a las ciberamenazas, para que ello les lleve a actuar con responsabilidad.

Los programas de concienciación pueden ser sumamente útiles, pero para ser eficaces han de estar bien diseñados y adaptados a las situaciones concretas, de modo que sean adecuados para distintas partes interesadas. Deberían incluir un conjunto de herramientas y metodologías, como campañas, talleres, conferencias, materiales educativos y otras actividades de comunicación. Por otra parte, teniendo en cuenta las características de las microempresas y las pymes y sus limitados recursos, deberían introducirse iniciativas específicas para prestarles asistencia.

Los programas de concienciación deberían involucrar cuando menos a las siguientes partes interesadas internas y externas:

- El empresariado, que son legalmente responsables de la seguridad y salud de su personal, así como la **dirección** son agentes primordiales por su papel de liderazgo en las organizaciones. Conforme a la legislación de prevención de riesgos laborales, las personas empleadoras tienen amplias obligaciones de protección de sus personal frente a todos los riesgos relacionados con el trabajo y de gestión eficaz de dichos riesgos. Dado que las ciberamenazas pueden afectar a la seguridad y salud de las personas , estas deberían considerarse de forma expresa en las actividades de prevención y gestión de riesgos de laborales.
- Las personas **trabajadoras** deben ser informadas acerca de todos los riesgos para su seguridad y salud que puedan tener que afrontar durante su actividad laboral, y los riesgos de ciberseguridad deben estar incluidos entre ellos: por tanto, es evidente que proporcionar formación e información a las personas trabajadoras sobre esta cuestión en particular es una medida de prevención esencial.
- Las **profesionales de SST** deben participar en las iniciativas de concienciación, ya que en general carecen de conocimientos en materia de ciberseguridad. Podrían desempeñar un papel clave para prevenir los efectos de los ciberataques en la salud y seguridad del personaly se les debería mantener al día de la evolución de los contextos organizativos y de los riesgos relativos de ciberseguridad.
- **Inspección de trabajo**. Es probable que los nuevos retos planteados por las ciberamenazas en cuanto a SST requieran nuevos métodos y herramientas para que la inspección de trabajo desempeñe sus funciones. Por tanto, para que desarrolle su labor de inspección y prevención es fundamental que conozcan los riesgos de SST asociados a las ciberamenazas.
- **Dirección de seguridad informática**. A menudo no conocen bien los aspectos de la ciberseguridad relacionados con la seguridad de las personas debido a que, por la naturaleza de su trabajo, están esencialmente centrados en la seguridad de las redes y los datos y en la formulación y gestión de una política informática eficaz para su organización. Aumentar sus conocimientos sobre este tema podría contribuir a fomentar la cooperación con el servicio de prevención de riesgos laborales y a integrar una perspectiva adicional en la definición de normas y prácticas de seguridad defensiva en las organizaciones.

Dada la futura extensión de los riesgos relacionados con la ciberseguridad a la seguridad personal en el lugar de trabajo, sería preciso que otros tipos de partes interesadas se concienciasen sobre las implicaciones de la ciberseguridad para la SST y contribuyesen a las estrategias de prevención. Entre ellas, por ejemplo, están las personas expertas en interacción persona-ordenador (IPO) y las desarrolladoras de programas informáticos.

La **IPO** es un campo de estudio multidisciplinario, centrado en principio en la interacción entre los usuarios y los ordenadores, que ahora comprende muchas formas de diseño de tecnologías de la información[44]. Teniendo en cuenta que los equipos utilizados para el trabajo estarán cada vez más conectados en red, será crucial que las interfaces IPO sean adecuadamente diseñadas por personas

[44] https://www.interaction-design.org/literature/topics/human-computer-interaction

expertas en este campo con el fin de reducir al mínimo los impactos en materia de ciberseguridad y SST (Korfmacher, 2019).

Del mismo modo, las **desarrolladoras de programas informáticos** pueden desempeñar un importante papel, teniendo en cuenta que una parte cada vez mayor de la población trabajadora, tanto si trabaja de forma presencial como a distancia, lleva a cabo su actividad por medio de sistemas informáticos. Por consiguiente, es importante concienciar a las desarrolladoras de programas informáticos sobre los efectos que tienen los ciberataques para la seguridad y salud del personal, para que se aseguren de diseñar y ejecutar estos sistemas cuidadosamente en cuanto a su capacidad de protección contra los riesgos de ciberseguridad, que va a tener un efecto positivo para el bienestar de la plantilla, ayudándola a sentirse protegida contra ataques.

En conclusión, una recomendación clave es involucrar a personas **expertas en comportamiento humano** para diseñar y ejecutar programas de concienciación en materia cibernética. De hecho, el éxito de estas iniciativas depende de la motivación de quienes participan en ellas, así como de los métodos y herramientas utilizados para llevarlas a cabo. Por consiguiente, hacen falta competencias y conocimientos adecuados sobre el comportamiento humano.

Por último, la ciberseguridad es, por encima de todo, un problema humano. De ahí que, para su gestión efectiva, vaya a ser cada vez más necesario contar con equipos multidisciplinarios, que combinen capacidades técnicas con aptitudes humanas y sociales.

Siguientes pasos

En el futuro, los estudios deberían centrarse en las interconexiones entre los dos ámbitos comentados: la ciberseguridad y la SST. Determinar necesidades y carencias ayudará a establecer los posibles riesgos de los ciberataques para las personas trabajadoras, así como a definir estrategias de prevención y políticas adecuadas en el seno de las organizaciones. En la bibliografía ya se han analizado conexiones interesantes entre la seguridad y la protección, como la positiva relación entre una cultura de seguridad defensiva, la satisfacción en el empleo y los comportamientos adecuados para la protección de las organizaciones (Green y D'Arcy, 2010).

Los estudios existentes sobre la relación entre la ciberseguridad y los riesgos para la seguridad de las personas están centrados fundamentalmente en el sector sanitario (por ejemplo, Martin *et al.*, 2017) y en los vehículos autónomos (por ejemplo, Taeihagh y Lim, 2019), mientras que hacen falta estudios adicionales para aclarar los posibles efectos de los ciberataques para la seguridad y la salud de las personas en todos los sectores laborales.

Por otra parte, teniendo en cuenta que los sistemas empotrados serán cada vez más dominantes en el futuro, será necesario garantizar una integración adecuada entre la seguridad defensiva y la seguridad personal. De hecho, estos sistemas podrían diseñarse con el fin de responder a objetivos de seguridad defensiva (como los ataques de los piratas informáticos) y garantizar funciones de seguridad personal que eviten perjuicios para los usuarios (trabajadores). La integración entre la seguridad y la protección es un tema candente en el desarrollo de sistemas esenciales[45] y las normas internacionales pueden ser útiles como apoyo para las organizaciones[46].

Por último, es posible suponer que las formas híbridas de trabajo —que combinen el trabajo en casa con el trabajo presencial en la oficina— estarán todavía más extendidas en el futuro, así como los entornos de trabajo inteligentes basados en las tecnologías de la internet de las cosas y los sistemas ciberfísicos (Podgórski *et al.*, 2017). Por lo tanto, las organizaciones tendrán que actualizar su evaluación de riesgos para detectar posibles peligros para su personal, al objeto de adoptar medidas adecuadas. Con este fin, será necesario implementar nuevos métodos y herramientas.

[45] https://insights.sei.cmu.edu/blog/integrating-safety-and-security-engineering-for-mission-critical-systems/
[46] Véase, por ejemplo, ISO/TR 22100-4, Seguridad de las máquinas. Relación con la norma ISO 12100. Parte 4: Orientación a los fabricantes de maquinaria para considerar aspectos relacionados con la protección informática (ciberseguridad); IEC TR 63074:2019 *Safety of machinery – Security aspects related to functional safety of safety-related control systems* [Seguridad de las máquinas. Aspectos de protección relacionados con la seguridad funcional de los sistemas de control relacionados con la seguridad].

Conclusiones

La transformación digital es un proceso imparable, que va acompañado de varios retos a los que todos los países deben hacer frente. En la actualidad, la ciberseguridad representa una gran preocupación para empresas e instituciones de todos los tamaños y sectores, y en el futuro irá en aumento.

Sin embargo, la gestión de la ciberseguridad no puede reducirse a la mera protección tecnológica de los sistemas y de la información. Dado que los ciberataques también pueden afectar a la salud y seguridad de la población trabajadora, las organizaciones deberán aplicar un enfoque holístico en relación con la ciberseguridad. Para conseguir este objetivo, será necesario **adoptar una visión multidisciplinaria, que integre competencias técnicas y sociales** para hacer frente a las distintas implicaciones de las ciberamenazas.

En cuanto a las grandes organizaciones, es altamente recomendable que los departamentos de Seguridad Informática y SST cooperen para definir un proceso innovador de evaluación de riesgos, con el fin de proteger los activos tangibles e intangibles y, sobre todo, a los seres humanos. Otro tema candente es cómo aplicar estrategias eficaces para las microempresas y las pymes, que a menudo carecen de recursos específicos internos[47], pero que están igualmente expuestas a las consecuencias de las ciberamenazas.

Se presenta un reto muy difícil de cara al futuro. Si se quiere comenzar con buen pie, en primer lugar será necesario contar con un amplio y sólido programa de concienciación sobre estos temas a fin de preparar a las empresas, a la población trabajadora y a la comunidad de SST, así como a quienes dirigen la seguridad informática y otros agentes pertinentes —como las personas expertas en IPO, las desarrolladoras de programas informáticos y las expertas en comportamiento humano— para un entorno cada vez más digitalizado y para la evolución de las ciberamenazas.

Autores: Isabella Corradini, directora científica del Centro de Estudios Themis (Italia),

Gestión del proyecto: Emmanuelle Brun y Annick Starren, con la colaboración de Ana Cayuela, de la Agencia Europea para la Seguridad y la Salud en el Trabajo (EU-OSHA).

El presente documento de reflexión se ha elaborado por encargo de la Agencia Europea para la Seguridad y la Salud en el Trabajo (EU-OSHA). Su contenido, incluidas las opiniones o conclusiones expresadas, es responsabilidad exclusiva de los autores y no refleja necesariamente las opiniones de la EU-OSHA.

[47] https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

Bibliografía

Aboujaoude, E. (2019). «Protecting privacy to protect mental health: The new ethical imperative» [Proteger la privacidad para proteger la salud mental: el nuevo imperativo ético]. *Journal of Medical Ethics*. *45*(9), 604–607.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. y Upton, D. (2018). «A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate» [Una taxonomía de ciberdaños: definir los impactos de los ciberataques y entender cómo se propagan]. *Journal of Cybersecurity*, *4*(1).

Aldawood, H. y Skinner, G. (2018). «Educating and raising awareness on cyber security social engineering: A literature review» [Educar y concienciar sobre ingeniería social en el ámbito de la ciberseguridad: revisión bibliográfica]. Publicado en la Conferencia Internacional del IEEE sobre Enseñanza, Evaluación y Aprendizaje para la Ingeniería (TALE). IEEE, 62–68.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. y Savage, S. (2013). «Measuring the cost of cybercrime» [Cuantificar el coste de la ciberdelincuencia]. Publicado en R. Böhme (ed.) *The economics of information security and privacy* (265–300). Springer-Verlag.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. y Xu, L. (2017). «Gender difference and employees' cybersecurity behaviors» [La diferencia de género y las conductas de ciberseguridad de los empleados]. *Computers in Human Behavior*, 69, 437–443.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. y Flahault, A. (2020). «Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks» [La ciberseguridad en los hospitales: análisis de los retos y trabajo para mitigar los riesgos]. *BMC Medical Informatics and Decision Making, 20*(146).

Augustina, J. R. (2015). «Understanding cyber victimization: Digital architectures and the disinhibition effect» [Entender la cibervictimización: las arquitecturas digitales y el efecto desinhibidor]. *International Journal of Cyber Criminology*. *9*(1), 35–54.

Bada, M. y Nurse, J. R. C. (2020). «The social and psychological impact of cyber-attacks, psychology» [Impactos sociales y psicológicos de los ciberataques, psicología]. Publicado en V. Benson y J. Mcalaney (ed.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press.

Betts, L. R. (2016). «Cyberbullying: Approaches, consequences, and interventions» [Ciberintimidación: enfoques, consecuencias e intervenciones]. Publicado en J. Binder (ed.), *Palgrave studies in Cyberpsychology*. Palgrave Macmillan.

Borkovich, D. J. y Skovira, R. J. (2020). «Working from home: Cybersecurity in the age of covid-19» [El teletrabajo: la ciberseguridad en la era de la COVID-19]. *Issues in Information Systems*. *21*(4), 234–236.

Boustras, G. y Waring, A. (2020). «Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context» [Hacia una reconceptualización de la seguridad y la protección, sus interacciones y requisitos políticos en el contexto del siglo XXI]. *Safety Science*, 132.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. *et al*. (2018). «The malicious use of artificial intelligence: Forecasting, prevention, and mitigation» [El uso malicioso de la inteligencia artificial: previsión, prevención y mitigación]. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Cashell, B., Jackson, W. D., Jickling, M. y Webel, B. (2004). «The Economic Impact of Cyber-Attacks» [El impacto económico de los ciberataques]. *CRS Report for Congress*.

Corradini, I. (2020). Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology [Crear una cultura de ciberseguridad en las organizaciones: cómo salvar la brecha entre las personas y la tecnología digital]. Springer.

Corradini, I. (2019). *Crimini relazionali nell'era digitale. Conoscere per prevenire. Cyber-bullismo-mobbing-stalking.* Themis.

Corradini, I., Nardelli, E. y Ahram, T. (ed.) (2020). «Advances in human factors in cybersecurity» [Avances en los factores humanos de la ciberseguridad]. AHFE 2020. *Advances in Intelligent Systems and Computing.* Vol. 1219, Springer.

Corradini, I. y Nardelli, E. (2020). «Developing digital awareness at school: A fundamental step for cybersecurity education» [Desarrollar la conciencia digital en la escuela: un paso fundamental para la educación en ciberseguridad]. Publicado en I. Corradini, E. Nardelli y T. Ahram (ed.) «Advances in human factors in cybersecurity» [Avances en los factores humanos de la ciberseguridad]. AHFE 2020. *Advances in Intelligent Systems and Computing.* Vol. 1219, Springer.

Couce-Vieira, A., Insua, D. R. y Kosgodagan, A. (2020). «Assessing and forecasting cybersecurity impacts» [Evaluación y previsión de impactos de ciberseguridad]. *Decision Analysis. 17*(4), 356–374.

Darwish, A., El Zarka, A. y Aloul, F. (2012). «Towards understanding phishing victims' profile» [Hacia el entendimiento del perfil de las víctimas de *phishing*]. *International Conference on Computer Systems and Industrial Informatics*. 1–5.

Disterer, G. y Kleiner, C. (2013). «BYOD - Bring Your Own Device». *HMD*. 50, 92–100.

Dressing, H., Bailer, J., Anders, A., Wagner, A. y Gallas, C. (2014). «Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims» [El ciberacoso en una gran muestra de usuarios de redes sociales: prevalencia, características y efectos para las víctimas]. *Cyberpsychology, Behavior, and Social Networking,* 17: 61–67.

ENISA. (2020). «Threat Landscape 2020» [Panorama de las ciberamenazas en 2020]. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2021a). «Threat Landscape 2021» [Panorama de las ciberamenazas en 2020], 27 de octubre de 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021b). «Threat Landscape for Supply Chain Attacks» [Panorama de las amenazas de ataque a las cadenas de suministro], 29 de julio de 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Farley, S., Coyne, I. y D'Cruz, P. (2021). «Cyberbullying at Work: Understanding the influence of technology» [La ciberintimidación en el trabajo: entender la influencia de la tecnología]. Publicado en P. D'Cruz, E. Noronha, G. Notelaers y C. Rayner (ed.), *Handbooks of workplace bullying, emotional abuse and harassment*. Vol. 1, Springer.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. y Aylin, P. (2019). «A retrospective impact analysis of the WannaCry cyberattack on the NHS» [Análisis retrospectivo de impactos del ciberataque con WannaCry contra el sistema nacional de salud británico]. *NPJ Digital Medicine*. *2*(98).

Hamlyn-Harris, J. H. (2017). «Three reasons why pacemakers are vulnerable to hacking» [Tres razones por las que los marcapasos son vulnerables al jaqueo]. The Conversation. http://theconversation.com/three-reasons-why-pacemakers-are- vulnerable-to-hacking-83362

Hart, D. V. (2019). «Factors influencing the adoption of cybersecurity situational awareness programs» [Factores que influyen en la adopción de programas de concienciación situacional sobre la ciberseguridad]. *Isaca Journal*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs

Heembrock, M. (2015). «The risks of wearable tech in the workplace» [Los riesgos de la tecnología ponible en el lugar de trabajo]. *Risk Management Magazine.* https://www.rmmagazine.com/articles/article/2015/02/02/-The-Risks-of-Wearable-Tech-in-the-Workplace-

Hernandez-Castro, J., Cartwright, A. y Cartwright, E. (2020). «An economic analysis of ransomware and its welfare consequences» [Un análisis económico de los programas de chantaje y sus

consecuencias para el bienestar de las personas]. *Royal Society Open Science*. 7(3), 190023.

Wang, C. (2016). «Understanding the impact of cyber security risks on safety» [Entender el impacto de los riesgos de ciberseguridad sobre la seguridad de las personas]. ICISSP 2016 - 2.ª Conferencia Internacional sobre Seguridad y Privacidad de los Sistemas de Información.

Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. y van der Zee, S. (2017). «Victims» [Víctimas]. Publicado en R. Leukfeldt (Ed.), *Research agenda. The human factor in cybercrime and cybersecurity*, Eleven International Publishing.

Kavallieratos, G., Katsikas, S. y Gkioulos, V. (2020). «Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey» [La ciberseguridad y la coingeniería para la seguridad personal en los sistemas ciberfísicos: un estudio exhaustivo]. *Future Internet*. *12*(4), 65.

Korfmacher, S. (2019). «The relevance of cybersecurity for functional safety and HCI» [La pertinencia de la ciberseguridad para la seguridad funcional y la IPO]. Publicado en V. Duffy (ed.), *Digital human modeling and applications in health, safety, ergonomics and risk management human body and motion HCII 2019 lecture notes in computer science*. 11581. Springer.

Loukas, G. (noviembre de 2019). «Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0» [Amenazas de seguridad ciberfísicas para la salud y seguridad en el trabajo (SST) en la Industria 4.0]. https://www.safe-machines-at-work.org/fileadmin/user_upload/pdf/LOUKAS.pdf

Martin, G., Martin, P., Hankin, C., Darzi, A. y Kinross, J. (2017). «Cybersecurity and healthcare: How safe are we?» [Ciberseguridad y asistencia sanitaria: ¿hasta qué punto estamos seguros?]. *British Medical Journal (Clinical research ed.),* 358, j3179.

McGuire, M. y Dowling, S. (2013). «Cybercrime: A review of the evidence. Summary of key findings and implications (Home Office Research Report, 75) [Ciberdelincuencia: análisis de datos fehacientes. Resumen de los principales hallazgos e implicaciones (Informe de investigación del Ministerio del Interior, 75)]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Muthuppalaniappan, M., y Stevenson, K. (2021). «Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health» [Los ciberataques contra los sistemas sanitarios y la pandemia de COVID-19: una amenaza urgente para la salud mundial]. *International Journal for Quality in Health Care*, *33*(1).

Notar, C. E., Padgett, S. y Roden, J. (2013). «Cyberbullying: A review of the literature» [Ciberintimidación: revisión bibliográfica]. *Universal Journal of Educational Research, 1*(1), 1–9.

Perales Gómez, Á.L., Fernández Maimó, L., Huertas Celdrán, A., García Clemente, F.J., Gil Pérez, M. y Martínez Pérez, G. (2020). «SafeMan: A unified framework to manage cybersecurity and safety in manufacturing industry» [SafeMan: un marco unificado para gestionar la ciberseguridad y la seguridad de las personas en la industria manufacturera]. *Software: Practice and Experience 51(3),* 607–627.

Podgórski, D., Majchrzycka, K., Dąbrowska, A., Gralewicz, G. y Okrasa, M. (2017). «Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies» [Hacia un marco conceptual de la gestión de riesgos de SST en los entornos de trabajo inteligentes basado en los EPP inteligentes, la inteligencia ambiental y las tecnologías de la internet de las cosas]. *International Journal of Occupational Safety and Ergonomics*, *23*(1), 1–20.

Ponemon. (2021). «The impact of ransomware on healthcare during covid-19 and beyond» [Efectos del *ransomware* sobre los sistemas sanitarios durante la COVID-19 y posteriormente]. https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

Stacey, N., Ellwood, P., Bradbrook, S., Reynolds, J., Williams, H. y David, L. (2018). «Key trends and drivers of change in information and communication technologies and work location. Foresight on new and emerging risks in OSH» [Tendencias y factores clave que impulsan el cambio en las tecnologías de la información y la comunicación y en la ubicación del trabajo. previsión de riesgos nuevos y emergentes en materia de SST]. Agencia Europea para la Seguridad y la Salud en el Trabajo. https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

Steijn, W., van der Vorm, J., Luiijf, E., Gallis, R. y van der Beek, D. (6 de septiembre de 2016). «Emergent risks to workplace safety as a result of IT connections of and between work equipment» [Riesgos emergentes para la seguridad en el lugar de trabajo a consecuencia de las conexiones TI de los equipos de trabajo y entre ellos]. *TNO report*.

Taeihagh, A. y Lim, H. S. M. (2019). «Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks» [Control de los vehículos autónomos: respuestas emergentes a los riesgos para la seguridad, la responsabilidad civil, la privacidad, la ciberseguridad y la industria]. *Transport Reviews*, 39, 103–128.

Tifferet, S. (2019). «Gender differences in privacy tendencies on social network sites: A meta-analysis» [Diferencias de género en las tendencias relacionadas con la privacidad en la redes sociales: un metaanálisis]. *Computers in Human Behavior*, 93: 1–12.

Truong, T. C., Diep, Q. B. y Zelinka, I. (2020). «Artificial Intelligence in the Cyber Domain: Offense and Defense» [La inteligencia artificial en el dominio del ciberespacio: ofensa y defensa]. *Symmetry, 12*(3), 410.

Verizon. (2019). «2019 Data breach investigations report» [Informe de investigación sobre violaciones de la seguridad de los datos en 2019]. https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

Verizon. (2021). «2021 Data breach investigations report» [Informe de investigación sobre violaciones de la seguridad de los datos en 2021]. https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

Foro Económico Mundial. (2021). «These are the top cybersecurity challenges of 2021» [Estos son los principales retos de ciberseguridad de 2021]. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

Westerlund, M. (2019). «The emergence of deepfake technology: A review» [La aparición de la tecnología *deepfake*: una revisión]. *Technology Innovation Management Review, 9*(11), 40–53.

Williams, E. J., Hinds, J., y Joinson, A. N. (2018). «Exploring susceptibility to phishing in the workplace» [Exploración de la susceptibilidad al *phishing* en el lugar de trabajo]. *International Journal of Human-Computer Studies*, 120, 1–13.