FCT-P
2|06
2022

Laboratorio-Observatorio de Riesgos Psicosociales de Andalucía

LARPSICO | Universidad de Jaén

FICHA CIENTÍFICO-TÉCNICA PREVENTIVA
Colección #02/2022
Digitalización de las organizaciones de trabajo y gestión de riesgos psicosociales: nuevos factores, riesgos emergentes

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

Cristóbal Molina Navarrete
Estefanía González Cobaleda
María Rosa Vallecillo Gámez
Equipo Investigación LARPSICO

Junta de Andalucía
Consejería de Empleo, Formación y Trabajo Autónomo
INSTITUTO ANDALUZ DE PREVENCIÓN DE RIESGOS LABORALES

LABORATORIO OBSERVATORIO del IAPRL

Universidad de Jaén

FICHA CIENTÍFICO-TÉCNICA PREVENTIVA
Colección #02/2022
Digitalización de las organizaciones de trabajo y gestión de riesgos psicosociales: nuevos factores, riesgos emergentes

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

FCT-P
2|06
2022

SUMARIO

Palabras clave: ciberseguridad, riesgos psicosociales, estrés laboral, fuerza mayor
Keywords: cybersecurity, psychosocial risks, work stress, force majeure

1. Introducción: ciberseguridad, una necesidad para las empresas en la era digital

Lamentablemente, los ciberataques a los sistemas informáticos propios de entidades, organizaciones (públicas o privadas) o a empresas, de cualquier tamaño, no solo a las grandes, constituirían un "riesgo social de naturaleza tecnológica" y ámbito global cada vez más normalizado en la era digital. Una economía y una sociedad que hacen de la creación, obtención y distribución de datos un elemento clave para su funcionamiento dependen, en gran medida, de la eficacia para asegurar su información, a través de un determinado sistema de ciberseguridad lo suficientemente fiable como para prevenir, identificar y solucionar las amenazas, conocidas y probables, a la seguridad de los datos y las redes establecidas para el desarrollo de su actividad (o negocio). De este modo, la **"ciberseguridad"** (procesos y prácticas de protección de redes, dispositivos, sistemas y personas contra los ciberataques y para la garantía de privacidad de comunicaciones y datos) y la **"seguridad de la información"** (protección de los datos de las organizaciones frente al acceso no autorizado de terceras personas ajenas –incluye en la condición de terceros a personas empleadas–), se convierten en necesidades a abordar de manera inexorable por las empresas, también para las PYMES. Una necesidad que ha de verse sea como una fuente de **peligros** (amenazas) muy relevantes cuanto de **oportunidades significativas de desarrollo en un mundo cada vez más digitalizado (virtualizado)**.

La ciberseguridad y las políticas de gestión de los riesgos tecnológicos tienen mayor presencia en sectores **estratégicos** (ej. financiero –1 de cada 4 ciberataques–), en unas organizaciones más que en otras (ej. sistemas de inteligencia, servicios públicos, grandes empresas, etc.). Así lo entiende las autoridades de la Unión Europeo, que impulsan nueva regulación en ciberseguridad (**Directiva NIS2**). Una de sus principales novedades es la actualización e incremento de la lista de los sectores y de las actividades sujetas a las obligaciones en materia de ciberseguridad, destacando las consideradas esenciales, incluyendo las llamadas "cadenas de suministro" o "cadenas de valor global".

Sin entrar aquí ni en cuestiones muy técnicas ni tampoco en valoraciones de este tipo de regulaciones, que hallan algunas críticas en el sector privado, sobre todo porque es un nuevo cambio cuando apenas se ha implementado la Directiva anterior (**NIS1**), lo que más interesante resulta destacar es que, en realidad, los "ciber-riesgos" se dan en

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

todo el tejido económico-empresarial, incluso en el conjunto de la ciudadanía. Los estudios disponibles ponen de relieve que, en los dos últimos años, **más de uno de cada dos ordenadores habrían sufrido una infección por software malicioso** (*malware*). Las tecnologías digitales multiplican, pues, estos peligros, por lo que el grado de confianza en redes y dispositivos dependerá de normalizar igualmente su prevención.

2. Ciberseguridad, nuevo yacimiento de empleo cualificado: capacitar a personas "ciber-vigilantes", prioridad de las políticas de formación profesional

Desde una perspectiva ocupacional y laboral, lo más llamativo es que el aumento **de las exigencias de ciberseguridad para organizaciones y empresas la ha convertido en un formidable yacimiento de empleo cualificado**. España alcanza una población laboral de ciberseguridad que supera las 150.000 personas trabajadoras ("ciber-vigilantes"), con una brecha de talento estimada en **más de 25.000**. Como se ha puesto de relieve en fechas recientes, la demanda de talento (profesionales competentes) en ciberseguridad doblará a la oferta en 2024, hasta alcanzar un nada despreciable número de 83.000 profesionales necesarios en el sector. Así se evidencia en **"Análisis y Diagnóstico del Talento en Ciberseguridad en España"**, un informe elaborado por **ObservaCiber**.

Por lo tanto, la capacitación (atracción, desarrollo, cualificación y retención) de personas en los diversos campos de la ciberseguridad constituye un reto preferente para las políticas de mercado de trabajo relativas a la educación-formación profesional para el empleo y para el crecimiento. Por ejemplo, INCIBE, dentro de su Plan Estratégico 2021-2025, sitúa la **promoción y detección de talento en ciberseguridad como una prioridad**. Debe destacarse que se trata de un empleo cualificado y bien remunerado.

Desde esta perspectiva, según las diversas estadísticas retributivas, existe una clara tendencia al alza en la remuneración de estos colectivos profesionales, que están entre las personas empleadas en el sector tecnológico mejor pagadas. Sobre todo, a medida que aumenta su especialización, su nivel de experiencia y, también, su responsabilidad. Si bien en Estados Unidos se alcanza la retribución más elevada (en torno a los 5.000 € al mes), con una notable diferencia respecto de los países europeos, también es estos, incluyendo a España, la profesión de ciber-vigilancia y seguridad informática constituye un sector realmente prometedor para los jóvenes profesionales, con salarios que están en torno a unos 3.000 € mes, pudiendo alcanzar cantidades superiores –hasta esos 5.000 euros/mes– conforme se progresa en experiencia y responsabilidad, como se decía. De ahí que esté entre las **profesiones tecnológicas mejor pagadas**.

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

3. Ciberseguridad en el trabajo: fuente de nuevas obligaciones y responsabilidades para las empresas y para las personas empleadas

3.1. ¿Qué es la ciberseguridad en el trabajo?

Ahora bien, toda moneda tiene dos caras. Si la cara de la profesión de ciberseguridad es la capacidad de creación de empleo bien remunerado, la cruz es la responsabilidad que genera. Aunque las obligaciones de ciberseguridad y/o seguridad de la información gestionada por las empresas no se forjan solo en las personas profesionales que deben vigilar para prevenir que tengan éxito los ciberataques y las fugas de seguridad, sino que recaen cada vez más sobre todas las personas empleadas en una empresa que cuente con sistemas informáticos para su actividad normalizada. Los **protocolos de seguridad o de ciber-vigilancia** existentes, dado que la gestión informativa de la empresa inicia desde el puesto de trabajo, como en la forma tradicional (papel, teléfono), más con los dispositivos tecnológicos, una clave de bóveda de las políticas de ciberseguridad en las empresas está en la concienciación, y en la capacitación, a las personas empleadas, en torno a la necesidad de cumplir con las normas para la seguridad en, y desde, su puesto.

Como ya se expresó en la **FCT-P 2/05-2021 (relativa a la nueva rama prevencionista de la ciber-psicología)**, tan significativa es esta dimensión laboral de la política de seguridad cibernética que ya cuenta con un sector especializado y que se denomina "**ciberseguridad en el trabajo**". ¿Qué se entiende por "ciberseguridad en el entorno de trabajo"? En sentido amplio pude entenderse como el:

> "conjunto de las medidas técnicas y de las organizativas que, establecidas por los departamentos de informática de las empresas, directamente, o a través de técnicas de contratación externa, como política de protección de la seguridad informativa en los puestos de trabajo, constituyen una responsabilidad de las personas empleadoras y crean nuevas obligaciones de cuidado por parte de las personas empleadas."

Como es lógico, la mayor importancia de esta nueva política de gestión cibersegura del trabajo en la empresa se producirá conforme se vaya consumando el actual tránsito desde modelos de organización del trabajo presenciales a otros totalmente virtuales o, como resulta más probable, híbridos o mixtos. No ya el trabajo a distancia, con especial transcendencia del teletrabajo (**Ley 10/2021, de 9 de julio**), sino también otro tipo de formas de trabajo flexibles, basadas en el uso intensivo de las nuevas tecnologías, como el denominado "*Smart work*", afectan de forma significativa al "perímetro de seguridad cibernética" de la empresa. Este se diluye, por la fragmentación de los lugares de trabajo (precisamente llamado remoto). De ahí que los sistemas de seguridad cibernética hayan de adecuarse a esa diversidad, exigiendo específicas obligaciones de capacitación para usos ciberseguros de los equipos de trabajo en los nuevos entornos digitalizados, con conexión permanente, pero múltiple y, por tanto, más vulnerable.

Las empresas son muy conscientes de ello ahora. Así, entre las condiciones básicas para implantar el "*Smart Work*" se incluye:

> "(...) 3. En relación con las herramientas a utilizar, será necesario que la persona trabajadora disponga de la tecnología, capacitación y cultura adecuadas para trabajar de manera colaborativa en remoto, i***mplantando la Compañía cuantas medidas de seguridad sean necesarias para proteger sus sistemas e***

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

información" (punto 4, ANEXO V –Las nuevas formas de trabajo en TDE, TME, TSOL– *de los acuerdos de modificación y prórroga del II Convenio colectivo de Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU*.)

A esta proliferación de formas de organización del trabajo externalizadas o dispersas, pero con permanente conexión digital, hay que sumar el incremento en las empresas de los usos extralaborales de los dispositivos digitales (en el centro de trabajo o teletrabajo) puestos a disposición por las empresas. Consecuentemente, se utilizan, con impacto en la empresa, aplicaciones externas y peligrosas desde el punto de vista de la seguridad de las redes, dispositivos tecnológicos e información de las empresas.

3.2. Enfoque disciplinario: tendencia a responsabilizar a la persona empleada por el fallo del sistema de seguridad de la información empresarial

Los fallos de seguridad en las empresas tienen graves consecuencias de todo tipo de, por lo que están obligadas a mantener una elevada diligencia de ciberseguridad a tales fines. Así se deriva del **art. 32 del Reglamento** 2016/679/UE, del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD). Esta norma comunitaria (que está reflejada también **en el art. 9.1 LOPDGDD**) establece que los sujetos responsables de tratamiento de datos deben adoptar las "*medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo…*".

Según su apartado 3, la adhesión a **códigos de conducta** (art. 40 RGPD) o mecanismo de **certificación de sistemas de ciberseguridad** (art. 42 RGPD; ej. **ISO 2701**) podrá servir como prueba eficaz para demostrar, por la empresa, el cumplimiento efectivo de la obligación de diligencia cualificada de ciber-vigilancia. Por supuesto, como acredita la doctrina judicial, un ataque cibernético puede tenerse como un riesgo imprevisible e, o, inevitable, esto es, **una situación jurídica típica de fuerza mayor** (SAN 37/2022, 14 de marzo). Por tanto, en el ámbito de la gestión del empleo, la empresa podrá acudir a un Expediente de Regulación Temporal de Empleo (ERTE-FM), conforme al **art. 47 ET**, o incluso Expediente de Regulación definitiva de Empleo (ERE), si el efecto derivado de la contaminación por el virus informático es permanente, acudiendo al art. 51 ET.

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

De este modo, se corrige el criterio de la autoridad laboral según el cual este tipo de ataques responderían a un riesgo previsible y, con la debida diligencia de ciberseguridad, evitable dentro de los procedimientos y protocolos establecidos a tal fin en la empresa. Para los Tribunales, la diligencia empresarial de ciberseguridad **no puede confundirse con una obligación de resultado, porque sigue siendo una obligación de medios**, esto es, basta con poner los medios adecuados, técnicos y organizativos, para evitar los daños derivados de los ciberataques informáticos. Lógicamente, corresponde a la empresa la prueba de haber desplegado ese deber de conducta diligente, pues en otro caso el riesgo actualizado en daño le será imputable. **La empresa no podrá eludir su responsabilidad imputando el fallo del sistema a un error humano, de una persona empleada** (*STS, 3ª –Sala contencioso-administrativa–, 188/2022, 15 de febrero*), como es frecuente hacer.

el hecho de que la actuación negligente de una persona empleada provoque la brecha de seguridad en la empresa no le exime de responsabilidad, en cuanto encargada de la correcta utilización de las medidas de seguridad que deberían haber garantizado la adecuada utilización del sistema de gestión cibersegura de datos diseñado.

Por supuesto, si la empresa constata que el fallo de seguridad de la información se ha debido a una negligencia de la persona empleada, que no respeta los protocolos que se han establecido al respecto, sí puede utilizar el poder disciplinario. Por tanto, aquellas personas empleadas no diligentes en términos de ciberseguridad en su puesto pueden ser sancionadas disciplinariamente por no afrontar debidamente su deber de actuar de conformidad con las instrucciones de ciberseguridad recibidas. Así empieza a fijarse de forma expresa también en los convenios colectivos (ej. **arts. 150 y ss. II convenio de las empresas vinculadas de Telefónica**).

4. La ciberseguridad como factor de riesgo psicosocial en los entornos de trabajo: del enfoque disciplinario al enfoque preventivo

4.1. Del enfoque sociotécnico y económico de la ciberseguridad a un enfoque más integral (holístico): el impacto en la salud laboral

Ahora bien, parece claro que antes de acudir a la potestad disciplinaria, en su caso, es obligado llevar a cabo una política de adecuada capacitación profesional por parte de la empres a la persona empleada en competencias de ciberseguridad en el trabajo (sea presencial, sea, más aún, teletrabajo o trabajo a distancia). Sin esa capacitación, no cabe afirmar que la empresa haya sido diligente a la hora de implantar el protocolo de gestión cibersegura del entorno de trabajo. Pero, además, conviene tener en cuenta que estas ***nuevas obligaciones de ciberseguridad generan un relevante factor de riesgo laboral de naturaleza psicosocial organizacional***.

Frente a la visión puramente técnica y económica de la ciberseguridad, hoy crece la visión más integral de la misma. El impacto de un ciberataque debe prestar la debida atención a los aspectos de la salud integral, física, pero, sobre todo, mental de las personas trabajadoras. Y ello debe hacerse tanto atendiendo a la **contribución de la ciberseguridad a la prevención de la violencia y el acoso cibernético** (la ciberseguridad como técnica de gestión de riesgos psicosociales derivados de la tecnología digital –como es el ciberacoso en el trabajo, por ejemplo–: ***FCT-P Colección 2, n. 5, año 2021***)

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

como, por lo que interesa aquí, **como factor de riesgo psicosocial para personas trabajadoras con obligaciones de ciberseguridad en el trabajo**. Y no solo en los profesionales que ejercen la función de ciber-vigilancia, sino en el conjunto de las personas trabajadoras, máxime en empresas donde la seguridad de la información tenga especial importancia.

4.2. Ciberseguridad (ciber-vigilancia), nueva profesión de alta tensión (psicosocial) en los entornos de trabajo digitalizados

Que la ciberseguridad de las organizaciones (la actividad que denominamos de ciber-vigilancia de la seguridad información) es una profesión de altísima tensión lo confirma un dato contundente: **El 50% de profesionales de ciberseguridad sufren ansiedad.**

Los principales **factores de riesgo** que estarían incidiendo en estas altas tasas de estrés laboral en las personas y equipos profesionales de ciberseguridad, así como del síndrome de burnout (considerado por la OMS, en el CIE-11, como **problema asociado exclusivamente a la salud en los entornos de trabajo**):

- **Complejidad de los entornos digitales y de sus amenazas (alta demanda)**: a la dificultad de protección derivada de la sofisticación del entorno digital, se suma los mayores recursos de las personas ciberdelincuencia para crear virus.
- **Escasez de personal**, por tratarse de una profesión en la que existe una brecha entre oferta y demanda muy notable (**sobrecarga laboral**), además de incidir en este déficit de personal las brechas digitales. *Las jefaturas de equipo estiman que cada persona empleada en ciberseguridad hace el trabajo de tres personas.*
- **Capacitación y recursos limitados (bajo control)**. El 67% de las personas de jefatura de equipos de ciberseguridad afirma que no tiene suficiente talento en su equipo.
- **Incomprensión por las empresas de las dificultades en el desempeño** de esta función, **responsabilizando a los profesionales de lo que ha ido mal**, sin reparar en la desatención frecuente de las mejoras presupuestarias pedidas **(falta de apoyo)**.

En este escenario de incremento del riesgo, **los efectos negativos en la seguridad y en la salud en el trabajo de la ciberseguridad** son evidentes:

- **casi un tercio (32%) ha sufrido un incidente de seguridad** importante en el último año, provocando desánimo en el equipo, mayor conflictividad y prolongación de las horas de trabajo
- **más de la mitad (51%) de los profesionales encuestados dicen experimentar emociones negativas** (ira, ansiedad, depresión) al sentirse desbordados por el trabajo. Aunque trabajan más horas para tratar de resolver los problemas, siguen sin poder cubrir su carga de trabajo.
- **dos de cada cinco (20%) han tenido que buscar ayuda profesional debido al impacto físico del estrés laboral** (migrañas, ataques de pánico o presión arterial alta). Y la mayoría (94%) de las personas responsables de seguridad han sentido una mayor presión para mantener la seguridad de su empresa en el último año.

En suma, los equipos de ciberseguridad y sus responsables necesitan más recursos, así como apoyo, para salir del ciclo constante de exceso de trabajo y ansiedad en el que estarían inmersos.

4.3. Obligaciones de ciberseguridad en el puesto, nuevo factor de carga psicosocial en el entorno laboral

Pero el problema no es solo de las personas que trabajan en ciberseguridad. Como vimos, la puesta en práctica efectiva de los protocolos de ciberseguridad en las empresas pasa por la creación de obligaciones de cuidado del conjunto de la plantilla. Por lo tanto, también esta nueva responsabilidad laboral debe tenerse en cuenta en el sistema de gestión preventiva de riesgos psicosociales de las empresas. En consecuencia cada una de las personas empleadas

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

en entornos laborales digitalizados (más para los entornos de teletrabajo) deben también afrontar competencias de ciberseguridad en su puesto de (tele)trabajo, para que sean entornos ciberseguros. Volviendo de nuevo sobre la evidencia científica, varios estudios recientes ponen de manifiesto que **una de cada 4 personas trabajadoras perdería su puesto debido a errores de ciberseguridad**.

A la incertidumbre por el auge de los ciberataques (basados en *ransomware* –como los que afectaron al SEPE y al Ministerio de Trabajo– o los que buscan el robo de las credenciales y datos bancarios), cuyas pérdidas son millonarias, se añadiría la propia de las nuevas cargas derivadas del deber de usar contraseñas efectivas, los buenos hábitos de navegación online o la detección de potenciales ataques de phishing, entre otros que deben ser tenidos en cuenta por cada persona trabajadora, tanto si desempeñan su función desde las oficinas de su empresa como si lo hacen de manera remota. Un mal uso o descuido de la persona empleada podría comprometer gravemente todo el sistema de seguridad de una empresa y ocasionar pérdidas millonarias. De ahí, como se dijo, que las empresas no solo estén obligadas a exigir un nivel formativo elevado en materia de seguridad digital, pudiendo sancionar disciplinariamente a quienes no se adecúen a estos estándares de ciberseguridad, sino que también debe incluir este tipo de cuestiones en la gestión de riesgos laborales, diferenciando, lógicamente, atendiendo a las capacitaciones y responsabilidades de cada persona empleada en ese ámbito (ex art. 29 LPRL).

El personal de las empresas se encontrará cada vez más sometidas a un nivel de exigencia de ciberseguridad análogo al exigido para el uso de sustancias químicas o de los más sofisticados instrumentos de seguridad física. Por lo tanto, también está sujeto a un régimen disciplinario severo si incumple con los protocolos de ciberseguridad ya establecidos, en línea con los de seguridad física o de higiene industrial. Como es natural, estos protocolos no solo deben ser objeto de comunicación a las personas empleadas, además de a su representación laboral, en línea con los protocolos de uso de todo tipo de dispositivos digitales ex art. 88 Ley Orgánica de Protección de Datos (y art. 18 de la Ley 10/2021, de trabajo a distancia), sino que deben formar parte de un sistema formativo eficiente. Solo si se cumple adecuadamente con este doble deber, formativo e informativo, cabe aplicar el régimen disciplinario por eventuales negligencias laborales.

5. Pautas para la gestión psicosocial de la ciberseguridad en el trabajo desde una perspectiva de bienestar de la persona "ciber-vigilante"

Como se establece en los convenios colectivos más recientes, las empresas que ya asuman los procesos de virtualización de sus entornos de (tele)trabajo "formarán a sus personas trabajadoras en las competencias y habilidades necesarias para afrontar la transformación digital" (ej. **art. 11 Convenio Colectivo** general de ámbito estatal para el sector de entidades de seguros, reaseguros y mutuas colaboradoras con la Seguridad Social; o el art. 80 del Convenio colectivo del sector de banca, entre otros muchos). No obstante, conviene insistir en que las pautas de ciberseguridad en el trabajo ha de ir más allá de esta gestión laboral, para **integrar un enfoque de gestión de la seguridad y la salud en la evaluación de los riesgos de ciberseguridad**. Así se ha sido reconocida, en el seno de la UE, por la ***Agencia Europea de Seguridad y Salud en el Trabajo (OSHA-EU)***.

En ambos casos será fundamental no solo concienciar y sensibilizar, sino formar debidamente, a todas las partes interesadas, desde los profesionales de la seguridad y salud en el trabajo hasta los profesionales de la ciberseguridad y de la seguridad informática, pasando por el conjunto del personal, para que la debida

La ciberseguridad en el trabajo como emergente factor de riesgo psicosocial: pautas para su eficaz gestión preventiva

Cybersecurity as an emerging psychosocial risk factor at work: guidelines for its effective preventive management

lucha eficaz contra la ciberdelincuencia no termine convirtiéndose en un factor de malestar psicosocial en los entornos de trabajo. Para alcanzar este objetivo se requiere adoptar una visión multidisciplinaria, integrando competencias técnicas y sociales para manejar las diferentes implicaciones de la ciberdelincuencia. La cooperación entre las funciones de seguridad informática y los sistemas de seguridad y salud en el trabajo será necesaria para definir un proceso innovador de evaluación de riesgos para que la protección de los activos tangibles e intangibles no se haga, de nuevo, sobre el malestar psicosocial de las personas empleadas que deben cooperar necesariamente en su optimización.

Una debida integración de la dimensión de gestión psicosocial en el sistema de ciberseguridad sea como fuente de protección frente a los riesgos digitales sea como fuente de riesgo para las personas empleadas (profesionales o no de la ciberseguridad, pero en cualquier caso con obligaciones en el sistema de seguridad) que debe también servir para las PYMES. Si bien estas no cuentan con los mismos medios que las grandes, sí que están expuestas a amenazas cibernéticas análogas, al igual que su personal. De ahí la necesidad de que cuenten con medios de apoyo por parte de las AAPP a tal fin, lo que puede canalizarse incluyendo estos enfoques de gestión de seguridad y salud en los entornos de (ciber)trabajo seguro en términos de garantía de la información en diversas líneas de financiación de la digitalización de las PYMES. En todo caso:

> Un mayor enfoque en el bienestar de las personas empleadas en ciberseguridad, una mayor inversión, una mejor formación y las herramientas adecuadas cambiarán la situación de creciente malestar psicosocial asociado a la carga de ciberseguridad.

6. Para saber más

Agencia Europea de Seguridad y Salud en el Trabajo (AESST; OSHA-EU, por sus siglas en inglés). (2022) *Incorporation occupational safety and health in the assessment of Cybersecurity Risks.* https://osha.europa.eu/es/publications/incorporating-occupational-safety-and-health-assessment-cybersecurity-risks

Bada, M. and Nurse, J. R. C. (2020). *The social and psychological impact of cyber-attacks, psychology*. In V. Benson and J. Mcalaney (Eds.), Emerging cyber threats and cognitive vulnerabilities (pp. 73–92). Academic Press.

González Cobaleda, Estefanía (2021). *La evaluación de los riesgos psicosociales en el mundo laboral actual, digital, ecológico e inclusivo*, Comares, Granada.

INCIBE (Instituto Nacional de Ciberseguridad). *La protección del puesto de trabajo. Políticas de seguridad para la PYME.* https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf

Molina Navarrete, C. (2021). *Datos y derechos digitales de las personas trabajadoras en tiempos de (pos)covid19*. Entre eficiencia de gestión y garantías. Editorial Bomarzo. Albacete.

Molina Navarrete, C. (2022). Los ciberataques en entornos de trabajo digitalizados: ¿Fuerza Mayor o riesgo previsible y evitable con la debida diligencia de ciberseguridad? https://www.transformaw.com/blog/los-ciberataques-en-entornos-de-trabajo-digitalizados-fuerza-mayor-o-riesgo-previsible-y-evitable-con-la-debida-diligencia-de-ciberseguridad/

Molina Navarrete, C. (2021) De la "Ciberdelicuencia" a la "Ciberseguridad": Nuevo "yacimiento de empleo de calidad", emergente "riesgo psicosocial" laboral. https://www.transformaw.com/blog/de-la-ciberdelicuencia-a-la-ciberseguridad-nuevo-yacimiento-de-empleo-de-calidad-emergente-riesgo-psicosocial-laboral/