Co-funded by the European Union

INFORME SOBRE LAS NECESIDADES DE FORMACIÓN DE LOS AGENTES DEL CAMBIO EN LA CIBERSEGURIDAD DE LAS PYME

CYBER AGENT .2023

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.

Paquete de trabajo 2: Enfoque y diseño de la estructura de CyberAgent

Entrega 2.2: Informe sobre las necesidades de formación de los y las agentes del cambio en la ciberseguridad de las PYMES

Líder del WP2 - Olemisen Balanssia ry
Responsable del paquete de trabajo 2.2 - Olemisen Balanssia ry

CONTENIDO

INTRODUCCIÓN

Este informe de proyecto tiene como objetivo analizar y mapear las necesidades de formación para identificar las competencias apropiadas requeridas para un/a Agente de Cambio de Ciberseguridad de PYME. A través de una revisión exhaustiva de la oferta formativa actual y de la comprensión de las preferencias de las PYMES en materia de ciberseguridad, este informe pretende salvar la brecha existente entre las competencias actuales y definir el conjunto ideal de habilidades requeridas.

A medida que aumenta la sofisticación de las ciberamenazas, es muy necesario que las PYMES se aseguren de contar con personal adecuadamente formado para combatirlas. Los agentes del cambio en el ámbito de la ciberseguridad desempeñan un papel crucial en este contexto. Este informe de proyecto analiza el panorama de la ciberseguridad a través de diferentes perspectivas: Educación y formación, inclusividad de género y el estado actual en las PYMES y la institución escolar.

1. METODOLOGÍA

Para este proceso de mapeo utilizamos un enfoque mixto que combinaba la investigación documental y de campo.

En la investigación documental se llevó a cabo una exhaustiva revisión bibliográfica para:

- Revisar las disposiciones educativas existentes y emergentes en los niveles de educación y formación profesional (EFP) e instituciones de educación superior (IES) en el ámbito de la ciberseguridad en cada país socio. Buscar y recopilar artículos, libros blancos, investigaciones e informes relacionados con el contenido y las necesidades de formación en ciberseguridad.
- Analizar los cursos de EFP e IES, sus planes de estudios y su relevancia para los retos de la ciberseguridad en el mundo real.

Los objetivos eran:

- Identificar los componentes curriculares actuales de los cursos de ciberseguridad ofrecidos en los niveles de EFP e IES en cada país.
- Evaluar la adecuación de estos planes de estudios a los retos de la ciberseguridad.
- Determinar si existen estrategias o programas específicos para implicar a más mujeres en los estudios de ciberseguridad.

Durante la fase de investigación de campo, realizamos 2 encuestas. Una diseñada para docentes y personas formadoras de EFP e IES de cada país para comprender los matices de las disposiciones actuales en materia de formación. La otra, adaptada a las PYMES para obtener una visión y una comprensión de la situación de las empresas en materia de ciberseguridad: cómo se implican y comprometen las personas empleadas en estos temas, los retos y las necesidades. El objetivo de esta investigación de campo era también determinar las características, las necesidades de formación y las preferencias de aprendizaje, haciendo especial hincapié en las necesidades de las mujeres en materia de ciberseguridad.

Se alcanzó un número significativo de respuestas para ambos cuestionarios. 190 docentes de EFP e IES y 176 personas empleadas de PYMES.

Encuesta 1: Determinación de las necesidades de formación de los y las agentes de cambio en materia de ciberseguridad de las PYMES - **Encuesta sobre EFP e IES.**

Tipo de institución	**Respuestas**	**Mujer**	**Hombre**	**Prefiero no decirlo**
IES (Instituciones de Educación Superior)	104	28	73	3
EFP (Educación y Formación Profesional)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Encuesta 2: Determinación de las necesidades de formación de los y las agentes del cambio en materia de ciberseguridad de las **PYMES.**

Número de respuestas	**Cuenta**
PYMES	176
Total	**176**

Los cuestionarios y los datos completos figuran en los apéndices C y D.

2. INVESTIGACIÓN (TODOS LOS SOCIOS)

2.1. DISPOSICIONES VIGENTES EN MATERIA DE EDUCACIÓN Y FORMACIÓN

En esta sección se presenta la investigación y se ofrece información derivada de la investigación documental y las encuestas, destacando los puntos fuertes y las lagunas de la actual infraestructura de educación y formación en los países socios.

2.1.1. PANORAMA DE LA FORMACIÓN EN CIBERSEGURIDAD EN EFP E IES

Realizamos un amplio análisis del panorama de la educación en ciberseguridad en todos los países socios para describir su estado actual y desencadenar los aspectos relevantes de la educación y la formación en ciberseguridad.

En Lituania, una búsqueda[1] en la base de datos AIKOS reveló un total de seis programas formales de educación en ciberseguridad ofrecidos por instituciones lituanas, que abarcan tanto los niveles de licenciatura como de máster:

Dirección del estudio	Programa	Institución	ECTS	Titulación
Ingeniería informática	Seguridad de la información y las tecnologías de la información[2]	Universidad Tecnológica de Kaunas	120	Máster en Informática
Gestión	Gestión de la ciberseguridad[3]	Universidad Mykolas Romeris	90	Máster en Dirección de Empresas
Ingeniería informática	Seguridad de la información y de las tecnologías de la información[4]	Universidad Técnica Vilnius Gediminas	120	Máster en Informática
Ingeniería informática	Sistemas de información y ciberseguridad[5]	Universidad de Vilna	210	Licenciado en Informática
Ingeniería informática	Tecnologías de Sistemas de Información y Ciberseguridad[6]	Colegio Marijampole	180	Profesional Licenciado en Informática
Ingeniería informática	Cibersistemas y seguridad[7]	Universidad de Kaunas	180	Profesional Licenciado en Informática

[1] Las palabras clave utilizadas en la búsqueda de programas fueron *ciberseguridad*, *seguridad* y sus variaciones. Fuente: www.aikos.smm.lt/Puslapiai/Pradinis.aspx
[2] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr= 8Gzz1EUgIeKfy0cWNVrrVdABKo0 %3d
[3] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[4] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0 %3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[7] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

Los programas de ciberseguridad a nivel de máster presentan enfoques distintos pero complementarios. La Universidad de Kaunas hace hincapié en la metodología de la investigación, los métodos de seguridad de la información y los aspectos jurídicos del espacio electrónico, centrándose en el desarrollo de capacidades de diseño e implantación de sistemas informáticos seguros. La Universidad Técnica Gediminas de Vilnius da prioridad a la formación de especialistas con un enfoque sistemático de las cuestiones de seguridad de la información, combinando conocimientos científicos con métodos y tecnologías para garantizar la seguridad de la información, además de fomentar el pensamiento crítico y el liderazgo. La Universidad Mykolas Romeris, sin embargo, se inclina claramente hacia la gestión en ciberseguridad, con el objetivo de formar especialistas expertos en la supervisión de entornos informáticos modernos y tareas complejas de ciberseguridad, con un fuerte énfasis en la gestión estratégica en contextos tecnológicos dinámicos.

Los programas de licenciatura en ciberseguridad se centran en el desarrollo de profesionales cualificados en informática y ciberseguridad, pero cada uno de ellos hace hincapié en aspectos distintos. El programa de la Universidad de Vilnius está orientado a proporcionar una base completa en ingeniería informática, centrándose en el análisis, diseño, desarrollo y mantenimiento de sistemas de información seguros. La Facultad de Marijampole, aunque también aspira a formar especialistas competentes en informática, hace más hincapié en aspectos prácticos como la creación, el mantenimiento y la administración de redes y sistemas informáticos. La Escuela Superior de Kaunas se diferencia por su objetivo de preparar especialistas con capacidades no sólo para diseñar e implantar cibersistemas, sino también para dirigir equipos, comprender las implicaciones éticas, jurídicas y sociales y trabajar eficazmente en entornos multiculturales. Aunque las tres instituciones aspiran a dotar a los estudiantes de competencias técnicas en ciberseguridad, sus objetivos varían desde la competencia técnica (Universidad de Vilnius), la aplicación práctica y el desarrollo de aptitudes interpersonales (Escuela Superior de Marijampole), hasta una combinación de consideraciones técnicas, de liderazgo y éticas (Escuela Superior de Kaunas).

La búsqueda también reveló cuatro programas registrados de educación no formal de adultos en ciberseguridad, cada uno de ellos centrado en las habilidades esenciales para reconocer, investigar y prevenir los ciberataques, especialmente mediante el uso de la criptografía. Aunque todos los programas comparten este objetivo básico, sus enfoques y alcances difieren. Algunos se centran en la ciberseguridad y las estrategias preventivas, mientras que otros ofrecen un plan de estudios más amplio que incluye la programación y abarca áreas como la ingeniería social, la gestión de identidades y la gestión de riesgos. En particular, varios programas comienzan con programación básica y avanzan hacia temas avanzados de ciberseguridad, adecuados para principiantes. Uno de los programas más destacados, en colaboración con Cybint, está dirigido a personas con conocimientos limitados de TI y ofrece conocimientos prácticos del mundo real tanto a tiempo completo como a tiempo parcial. En conjunto, estos programas pretenden desarrollar diversas competencias en ciberseguridad, desde la programación básica hasta el aprendizaje en profundidad centrado en las aplicaciones.

Varias políticas para reforzar la seguridad nacional y la defensa de Finlandia han influido en los programas educativos relacionados con la ciberseguridad. Ha habido un número creciente de iniciativas de investigación y desarrollo, programas educativos y de formación, y profesionales certificados en el campo de la ciberseguridad. La Estrategia Finlandesa de Ciberseguridad (2019) (https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/) y el Programa de Desarrollo de la Ciberseguridad (2021) hacen hincapié en la importancia de crear una competencia nacional en materia de ciberseguridad a través de la educación y la investigación. Para el sistema educativo, el objetivo es dotar a los estudiantes de habilidades y conocimientos para navegar por el mundo digital de forma segura y la conciencia de las amenazas cibernéticas y las medidas de protección **Lehto-IWS-018.pdf (jyu.fi).**

En la educación y formación profesional (EFP) finlandesa, la ciberseguridad no se destaca explícitamente como un enfoque separado o especializado en la mayoría de los materiales. Sin embargo, esto no significa necesariamente que la ciberseguridad esté totalmente ausente de los programas de EFP. Dada la creciente importancia de la alfabetización digital y la ciberseguridad en todos los sectores, estos temas se integran en programas más amplios de formación técnica y en TI. Es importante señalar que los proveedores de EFP en Finlandia tienen autonomía para organizar su oferta educativa según los requisitos regionales y específicos de cada campo. La formación profesional finlandesa ha experimentado recientemente la reforma más amplia en casi 20 años. El objetivo de la reforma de 2018 era crear un sistema de EFP más eficiente y flexible, basado en competencias y orientado al cliente, mejorar su eficiencia y adecuar mejor las cualificaciones a las necesidades del mercado laboral. Esto se hace principalmente reduciendo la regulación e introduciendo más autonomía y responsabilidad para los proveedores de EFP. (Fuente: **https://www.cedefop.europa.eu/files/8133_en.pdf)** Esto significa que algunas instituciones podrían ofrecer módulos más especializados en áreas como la ciberseguridad, en función de las demandas y asociaciones de la industria local. Según la investigación de Lehto, la ciberseguridad no es una asignatura independiente, sino que está integrada en diferentes materias, especialmente en el contexto de las Tecnologías de la Información y la Comunicación (TIC). La responsabilidad de la enseñanza recae en el profesorado para incorporar la educación en ciberseguridad dentro de sus asignaturas. Este planteamiento da lugar a una variación en la forma de aplicarlo en los distintos centros y cursos, y pone de relieve la necesidad de enfoques más estructurados y coherentes de la enseñanza de la ciberseguridad, incluida la posibilidad de convertirla en una asignatura independiente o en una parte más destacada de la enseñanza de las TIC.

A nivel de enseñanza superior, las universidades finlandesas ofrecen programas completos de titulación en ciberseguridad. Estos programas están diseñados para dotar a los y las estudiantes de conocimientos y habilidades avanzados en diversas áreas de la ciberseguridad. Muchas ofrecen un máster en seguridad de la información y tecnologías de la información, centrado en las implicaciones y aplicaciones de estos conceptos en el mundo real. Son accesibles in situ y a distancia.

El sector de la ciberseguridad en Bélgica está experimentando un aumento de la demanda de profesionales cualificados, con aproximadamente 4.000 vacantes de ciberseguridad abiertas (en noviembre de 2022). Reconociendo la urgencia y la necesidad de llenar este vacío, se han introducido varias iniciativas y programas educativos para desarrollar la experiencia en ciberseguridad del país. Numerosas instituciones belgas, como la Universidad Católica de Lovaina, la Escuela de Negocios Solvay, la Universidad de Ciencias Aplicadas de Howest y muchas otras, han desarrollado programas especializados en inglés, francés y holandés, capaces de llegar a un público amplio. Sin embargo, una investigación realizada por la organización belga Agoria, hizo hincapié en la necesidad de formación continua también entre los y las profesionales que ya no asisten a la universidad, con el fin de mantenerlos al día en el campo de la ciberseguridad y sus amenazas. La Estrategia Belga de Ciberseguridad para los años 2021-2025 reconoce el alto nivel de integración de la ciberseguridad en el entorno académico del país y subraya el papel fundamental que desempeñan las universidades y otras instituciones educativas en el impulso de los esfuerzos de investigación y desarrollo en este campo. Según la base de datos del CBB (Centro de Ciberseguridad de Bélgica), en Bélgica hay 33 cursos (licenciaturas, másteres y certificaciones) ofrecidos por instituciones de enseñanza superior, que se suman a una serie de programas de EFP ofrecidos tanto en el sector público como en el privado. La CBB es el organismo que supervisa, coordina y controla la aplicación de la estrategia belga de ciberseguridad, y actualmente está desarrollando una formación gratuita de concienciación sobre ciberseguridad para empleados belgas con el fin de difundir aún más los conocimientos sobre ciberseguridad entre la población. En general, la estrategia belga de ciberseguridad hace hincapié en la importancia de difundir los conocimientos y competencias en materia de ciberseguridad a través de la educación y se compromete a ampliar los cursos académicos, promover la investigación en este campo, fomentar la educación STEM y ofrecer oportunidades de formación práctica para hacer frente a la creciente demanda de profesionales en el panorama belga de la ciberseguridad.

En Noruega, la ciberseguridad no es una asignatura principal que se pueda estudiar en la FP. Sus elementos se incluyen en un programa de FP denominado "Informática y Electrónica". No existe un marco del Ministerio de Educación para la ciberseguridad, sólo se menciona en las competencias básicas digitales generales para toda la educación que los y las estudiantes deben ser capaces de utilizar y navegar por los recursos digitales dentro y fuera de las redes y salvaguardar la información y la seguridad de los datos.

La Estrategia Nacional de Competencia en Ciberseguridad señala el 14 de noviembre de 2023, la importancia de que los estudiantes de FP aprendan sobre ciberseguridad. Para muchas asignaturas de formación profesional, esto es muy relevante e importante. Hay una falta de materiales de aprendizaje de ciberseguridad en los cursos de formación profesional, y los profesores carecen de las habilidades para enseñar, particularmente en áreas como privacidad, tecnología doméstica inteligente e IoT. Los programas existentes para la educación en ciberseguridad, como GenCyber y CyberFirst, no abordan específicamente las necesidades de este programa vocacional (**fuente 1 - 2**).

A través de una colaboración entre la UiO, la NTNU y docentes de centros de FP seleccionados, el plan consiste en desarrollar material didáctico sobre ciberseguridad, que posteriormente se pondrá a disposición en la plataforma nacional de aprendizaje **NDLA (National Digital Learning Arena)**.

Dentro de la enseñanza superior, se encuentran tanto programas de un año en Cultura de seguridad digital como programas de licenciatura en ciberseguridad. El tema también se incluye en varios programas de máster en Ciencias de la Información e Informática. Existe una variedad de estudios específicos de ciberseguridad como informática aplicada y tecnología de la información, licenciatura en ciberseguridad, licenciatura en forense digital, infraestructura digital y ciberseguridad, cultura de la seguridad digital y máster basado en la experiencia en seguridad de la información. También hay estudios en los que se incluye la ciberseguridad como cultura y liderazgo en IES, cooperativas municipales de preparación para emergencias y trabajo de la junta en la práctica y estudio anual en gestión de crisis.

En Polonia, en los últimos años han aumentado los estudios cibernéticos. Cada vez se abren más cursos cibernéticos en las universidades y, al mismo tiempo, aumenta el número de cursos de FP.
La demanda de profesiones cibernéticas ha aumentado en Polonia en los últimos años y la concienciación sobre la cibernética también ha aumentado en la delegación polaca que promueve que las empresas contraten a expertos cibernéticos y protejan la información.
En Polonia, como en la mayoría de los países europeos, se considera obligatorio tener un título académico y, por tanto, los cursos cibernéticos suelen ser un estudio adicional después de la carrera. Porque la mayoría de los estudios de Akshmi son más largos pero de carácter teórico. Hay cursos cibernéticos que son cortos, pero la mayoría se centran en un aprendizaje práctico que prepara para el trabajo real.

El gran reto para un/una estudiante en el campo cibernético es que la mayoría de los centros de FP no tienen financiación propia, por lo que se requiere una solución financiera, y por tanto esta opción no siempre es adecuada para las personas interesadas.

Aunque la ciberseguridad debería ser una prioridad para todos los ámbitos de actividad, el sistema educativo de la EFP en Rumanía aún no está preparado para garantizar que los estudiantes sean competentes en este campo. En un análisis del plan de estudios para el ciclo inferior del bachillerato - ámbito tecnológico - en cualquier ámbito de la formación profesional, el plan de estudios de cultura técnica no proporciona unidades de resultados de aprendizaje sobre ciberseguridad. Algunas competencias específicas en este campo se pueden encontrar en el plan de estudios de conocimientos generales, en la disciplina de Tecnología de la Información y la Comunicación, en el plan de estudios de 9° curso. Éstas son:

1. Descripción y aplicación de medidas de seguridad en el uso de Internet:

- Uso inteligente de Internet
- La importancia del cifrado de la transmisión de datos
- Utilización de la firma digital
- Formas de defensa contra los virus

2. Utilizar el servicio de chat:

- Presentación de aplicaciones de colaboración para videoconferencias
- Presentación de las normas de la red IRC

Para el ciclo superior de bachillerato, grado 11th, sólo el campo de formación profesional Automatización Electrónica para las especialidades Técnico de Telecomunicaciones, Técnico Operador Informático, Técnico Operador Telemático, ofrece algunos contenidos sobre instalación de aplicaciones de seguridad. En el grado 12, sólo en la especialidad de Técnico en Informática, el módulo especializado incluye contenidos como:

- Principios básicos de la seguridad de los sistemas y redes informáticos
- Desarrollo de políticas de seguridad en la red
- Amenazas a la seguridad de las redes
- Protección de la navegación por Internet
- Virus y aplicaciones de seguridad

En lo que respecta a las IES la Universidad Transilvania de Brasov demuestra un fuerte compromiso con la educación en ciberseguridad, ofreciendo un completo programa de Máster en Ciberseguridad impartido íntegramente en inglés. La dedicación de la universidad para fomentar la experiencia en este campo crítico es evidente en el extenso plan de estudios previsto para el programa.

Este programa de Master en la Universidad de Transilvania es una excelente oportunidad para las personas que buscan una educación bien redondeada en la seguridad cibernética dentro de un entorno académico internacional. La combinación de un plan de estudios sólido y la instrucción en idioma Inglés posiciona las personas graduadas en la ruta para el éxito en el campo dinámico y desafiante de la seguridad cibernética.

La Universidad Babes-Bolyai de Cluj-Napoca, a través de la Facultad de Matemáticas e Informática, ha iniciado a partir del año académico 2023-2024 un programa de Master en Inglés en Seguridad Cibernética, destinado a preparar a los futuros y las futuras especialistas en este campo de vital importancia en el contexto de la transición a la sociedad de la información. Los cursos del nuevo programa comienzan en octubre de este año, junto con el año académico 2023-2024, la admisión de traer una competencia más allá de las expectativas. Más de 40 estudiantes, incluso del extranjero, admitidos en el programa se convertirán en especialistas en

el campo de la Ciberseguridad, las personas candidatas admitidas pueden incluso optar por estudiar un año académico en otras universidades de renombre en Europa.

En la Facultad de Matemáticas y Ciencias de la Computación, el Programa Máster de *Tecnologías de Internet* también ofrece, en el segundo semestre del primer año, un curso de *Criptografía y Seguridad de Sistemas*, que introduce a las personas estudiantes en el campo de la Ciberseguridad y los métodos específicos de cifrado de datos.

Además, el Programa Máster Tecnologías Modernas en Ingeniería de Sistemas de Software ofrece en el primer semestre del segundo año una asignatura optativa denominada Seguridad de los sistemas informáticos, centrada en los principales retos de la ciberseguridad.

Ambos cursos permiten a las personas estudiantes de máster de la Facultad de Matemáticas e Informática adquirir conocimientos y experiencia en esta materia, que en el contexto internacional actual es de vital importancia, y tomar conciencia de los retos que plantean el cifrado y la seguridad de los sistemas modernos.

La Facultad de Matemáticas e Informática de la Universidad de Bucarest ofrece un Programa de Máster en Seguridad y Lógica Aplicada, que ofrece una serie de cursos dedicados a la criptografía y la seguridad de los sistemas. Las personas estudiantes pueden adquirir conocimientos en los campos de la seguridad de sistemas operativos, criptografía, seguridad de redes y ciberseguridad, estando así preparadas para afrontar los retos de este campo.

En España la mayoría de los estudios en ciberseguridad son de Grado Superior, licenciaturas o másteres. Según los datos recuperados por el Instituto Nacional de Ciberseguridad de España, hay:

- Alrededor de 87 másteres en ciberseguridad ofrecidos por universidades públicas y privadas y otras instituciones de enseñanza superior.
- 4 especializaciones, en su mayoría especializaciones en informática forense.
- 3 títulos universitarios, todos ellos ofrecidos por el sector privado.

En cuanto a la formación a nivel de FP, existen alrededor de 60 cursos disponibles en los institutos de formación profesional españoles. Todos ellos están regulados por un mismo currículo, aprobado por el Ministerio de Educación en mayo de 2020 mediante el *Real Decreto 479/2020, de 7 de abril, por el que se establece el curso de especialización en ciberseguridad en entornos de tecnologías de la información*.

A pesar de los programas existentes, se reconoce la necesidad de realizar más esfuerzos. España ha puesto en marcha varios planes, como el Plan Nacional de Competencias Digitales, el Plan de Digitalización de las PYME 2021-2025 y el Plan España Digital 2025, con un enfoque clave en la creación de nuevos talentos para satisfacer la creciente demanda de competencias digitales, especialmente en ciberseguridad.

En Turquía, la necesidad de ciberseguridad ha aumentado rápidamente y se ha vuelto muy importante en este país, así como en todo el mundo, especialmente en los últimos años. Simultáneamente con los avances tecnológicos, los riesgos y amenazas cibernéticos también han cambiado al mismo ritmo y se han vuelto complejos. Los riesgos y amenazas cibernéticos han alcanzado el potencial de causar consecuencias mucho más amplias y negativas que los ataques físicos. Con sectores como las finanzas, las comunicaciones electrónicas, la energía, el transporte y la aviación prestando servicios en un entorno digital seguro, garantizar la ciberseguridad nacional se ha convertido en una de las principales prioridades del país. En este contexto, los estudios siguen difundiendo la formación en ciberseguridad en la formación profesional y la enseñanza superior en función de las necesidades del sector y desarrollando y enriqueciendo los contenidos formativos.

En el ámbito de estos estudios, en la formación profesional: Curso de fundamentos de ciberseguridad en la explotación de redes en el ámbito de las tecnologías de la información. En el ámbito de la ciberseguridad, fundamentos de programación, seguridad de sistemas, tecnologías de redes, desarrollo de software seguro, pruebas de penetración y respuesta a incidentes cibernéticos, informática forense, etc. Los logros del curso se entregan a los estudiantes.

En la enseñanza superior, se ofrece el programa de grado asociado "Analista y Operador de Ciberseguridad" en las escuelas de formación profesional de ciberseguridad, el programa de grado en ingeniería informática forense en las universidades y los programas de máster pertinentes en las universidades.

Además, los centros de educación continua de las universidades, los centros de educación pública de los municipios, las instituciones oficiales como TÜBİTAK, TSE y las instituciones educativas privadas también imparten formación sobre ciberseguridad.

2.1.2. RETOS DE LA CIBERSEGURIDAD Y NECESIDADES DEL SECTOR

Basándonos en una exhaustiva revisión bibliográfica, hemos enumerado los retos de ciberseguridad a los que se enfrentan las PYMES de los países del proyecto. En el cambiante panorama de la ciberseguridad, las pequeñas y medianas empresas (PYMES) de Lituania se enfrentan a múltiples retos de ciberseguridad. A medida que estas empresas dependen cada vez más de las tecnologías digitales para sus operaciones, se vuelven más vulnerables a un espectro de amenazas cibernéticas, lo que requiere una comprensión global y un enfoque estratégico para gestionar estos riesgos de manera eficaz.

En el estudio de 2022, Bukauskas et al.[8] distinguieron tipos de organizaciones en función de su madurez en materia de ciberseguridad y sus necesidades de competencias. Las organizaciones pequeñas, según el estudio, son comparables a las personas individuales en la sociedad, ya que el principal parámetro de la seguridad del espacio de trabajo digital es el nivel de ciberhigiene, en el que influye la comprensión general de las amenazas a la ciberseguridad. En este nivel, la ciberseguridad se coordina internamente dentro de la organización, lo que provoca posibles brechas de seguridad en los procesos empresariales. En las medianas empresas, la gestión y la regulación de la ciberseguridad también están poco coordinadas. Las respuestas a incidentes u otras actividades de ciberseguridad tampoco se enfatizan dentro de la organización. Teniendo en cuenta que las pequeñas empresas en Lituania constituyen el 97% de todas las empresas, Bukauskas et al. (2022) concluyeron que existe una necesidad significativa de especialistas en TI que proporcionen servicios de TI, consulten a los usuarios y cuyas funciones laborales incluyan garantizar los principios fundamentales de ciberseguridad. También destacaron, que se observa una carencia notable en inteligencia sobre amenazas e investigación científica, y una necesidad visible de especialistas en ciberseguridad en ingeniería de seguridad y ciclo de vida de los sistemas.

Pocos años antes, el programa "Crear para Lituania", en colaboración con el Ministerio de Defensa Nacional, organizó una consulta pública sobre la mejora de la concienciación en materia de ciberseguridad entre las pequeñas y medianas empresas[9] . La iniciativa también llegó a la conclusión de que es evidente que el nivel de concienciación sobre ciberseguridad entre las PYMES en Lituania no es alto y que las pequeñas empresas no han alcanzado un nivel adecuado de resistencia cibernética debido a la falta de comprensión de los riesgos digitales. Además, la iniciativa señaló que más de la mitad (57%) de las personas en puestos directivos de las empresas declararon que carecen de conocimientos suficientes para elegir soluciones de ciberseguridad, o no están seguros de tenerlos, y más de tres cuartas partes de las personas empleadas coincidieron en que carecen de información fácilmente comprensible.

Comparando las conclusiones de Bukauskas et al. (2022) y la anterior iniciativa Crear par Lituania (2019), es evidente que la situación de la ciberseguridad entre las PYMES en Lituania ha mostrado un progreso limitado. Ambos estudios subrayan una escasez persistente de conocimientos y preparación básicos en materia de ciberseguridad en estas empresas. A pesar de la creciente dependencia de las tecnologías digitales, las PYMES siguen mostrando vulnerabilidades debido a una resistencia cibernética inadecuada y a una falta general de comprensión de los riesgos digitales. Este reto permanente pone de manifiesto la urgente necesidad de mejorar la concienciación y la formación en ciberseguridad entre las PYMES, un sector crítico que constituye la mayor parte del panorama empresarial lituano.

[8] Bukauskas, L., Brilingaitė, A., Lepaitė, D., Juozapavičius, A., Ikamas, K., 2022. 'Projekto "Kibernetinio saugumo kompetencijų žemėlapio kūrimas" ataskaita', Vilniaus universitetas Informatikos institutas. Disponible en: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf [Consultado el 12 de enero de 2024]. DOI: https://doi.org/10.15388/CIBERSEK.2022.

[9] Crear para Lituania y Ministerio de Defensa Nacional, 2019. SVV Kibernetinio Saugumo Apklausos Apžvalga. [en línea] Disponible en: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

En Finlandia, un estudio de ETLA (Elinkeinoelämän tutkimuslaitos), Instituto de Investigación Económica de Finlandia destacó que el número de violaciones de datos en las empresas finlandesas, incluidas las pymes, se había duplicado en dos años. Las empresas finlandesas informaron de violaciones de datos tres veces más que la media europea en 2019, con la mayoría de los incidentes relacionados con estafas, ataques de phishing, violaciones de datos, malware y vulnerabilidades. Este estudio también destaca la escasez de profesionales cualificados en ciberseguridad como principal reto para las pymes finlandesas. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

El Centro Nacional de Ciberseguridad de Finlandia (NCSC-FI) (https://www.kyberturvallisuuskeskus.fi/en) es una iniciativa del Gobierno finlandés. Funciona como parte de la Agencia Finlandesa de Transportes y Comunicaciones (Traficom), organismo gubernamental responsable de la regulación de los sectores de las comunicaciones y el transporte en Finlandia. Proporcionan información sobre el estado actual de la ciberseguridad y ofrecen orientación y herramientas tanto a particulares como a organizaciones para mejorar sus prácticas de ciberseguridad. El centro también participa en iniciativas nacionales de ciberseguridad, como alertas de vulnerabilidad, y promueve la concienciación y la preparación contra las ciberamenazas.

Sus análisis semanales ofrecen una buena visión de los retos a los que se enfrentan las PYMES. Nos enteramos de que las PYMES finlandesas, como muchas otras, se han enfrentado a los mismos problemas de seguridad descritos por el instituto ETLA al ser blanco de muchos mensajes de phishing y estafa. Entre ellos figuran los intentos de hacerse pasar por servicios legítimos como Suomi.fi para suplantar credenciales u otra información sensible. Los recursos financieros de las PYMES pueden suponer una limitación a la hora de desplegar soluciones modernas de ciberseguridad para defenderse de las ciberamenazas. Por otro lado, las PYMES ya equipadas tienen problemas para mantenerse al día frente a las nuevas amenazas de ciberseguridad.

En nuestro esfuerzo por comprender la situación de la ciberseguridad a la que se enfrentan las PYMES en Bélgica, llevamos a cabo una investigación exhaustiva. Sin embargo, nos resultó difícil obtener datos exhaustivos o fuentes que aborden esta cuestión crítica. Esta falta de información dificulta la creación de estrategias y soluciones eficaces que puedan ayudar a las pymes a proteger sus activos digitales frente a las ciberamenazas.

Pudimos ponernos en contacto con profesionales que participan activamente en el ámbito de la ciberseguridad en Bélgica, gracias a la amplia red de la Fundación Women4Cyber. Estos expertos y expertas nos aportaron ideas y perspectivas vitales que nos ayudaron a comprender los diversos retos a los que se enfrentan las PYMES en materia de ciberseguridad. Recibimos información de Iva Tasheva, miembro destacado de Women4Cyber Belgium, que compartió su amplia experiencia y conocimientos sobre los retos a los que se enfrentan las PYMES cuando intentan proteger su infraestructura digital de las ciberamenazas.

Las PYMES se enfrentan a varios retos en materia de ciberseguridad, como dificultades para acceder a asistencia ad hoc, falta de formación en gestión de identidades y accesos para su personal y una comprensión limitada de las funciones y responsabilidades de los servicios en la nube. Además, las PYME tienen un acceso limitado a soluciones asequibles de análisis de vulnerabilidades y herramientas de supervisión, lo que las hace más vulnerables a las ciberamenazas. La hiperconectividad omnipresente en los entornos empresariales expone a las PYMES al robo de identidad y a actividades fraudulentas, mientras que el phishing y las estafas plantean riesgos continuos. Para hacer frente a estos retos, las PYMES deben tomar medidas proactivas, implantar protocolos de seguridad sólidos y ofrecer una formación completa a sus empleados para reforzar sus conocimientos y protegerlos contra posibles infracciones y pérdidas financieras.

La ciberseguridad se ha convertido en una de las principales prioridades para las empresas en España, incluidas las pequeñas y medianas empresas (pymes). El aumento del teletrabajo y de las clases online ha propiciado la generalización del uso de funciones de escritorio remoto, cloud computing y herramientas colaborativas, entre otras, incrementando los riesgos y ataques informáticos. El informe del Centro Criptológico Nacional (CCN-CERT) relaciona el aumento del teletrabajo y el uso de la tecnología con el incremento de estos riesgos. Los ataques más frecuentes que han sufrido las empresas son el ransomware y los ataques a sistemas de acceso remoto. El aumento de las ciberamenazas ha llevado a las empresas a incrementar el número de personas asignadas a los equipos de ciberseguridad, ya sea de forma interna o externa. Sin embargo, a pesar de ello, las empresas siguen subcontratando alrededor del 50% de estas funciones.

Además, todavía hay un 21% de empresas en España que no disponen de Centros de Operaciones de Seguridad (SOC) para procesar incidentes. En cuanto a la formación en ciberseguridad en el entorno empresarial, el análisis de Deloitte destaca que en 2022 las horas de formación online en ciberseguridad de los empleados de las organizaciones analizadas aumentaron casi un 30% respecto a los datos de 2021. Sin embargo, casi el 50% de las empresas en España no cuenta con ninguna certificación en ciberseguridad, lo que supone un claro reto de futuro.

Sin embargo, el mayor reto al que se enfrentan las empresas españolas sigue siendo la falta de talento en ciberseguridad. Según el informe "Análisis y Diagnóstico del Talento en Ciberseguridad en España" elaborado por ObservaCiber, en 2021 España tenía una brecha de talento estimada en 24.119. En 2024, se estima que España requerirá más de 83.000 personas expertas, elevando la brecha de talento hasta el 57,5%.

Parece que el eslabón más débil que hace que las PYME se enfrenten a retos de ciberseguridad es el factor "humano". El mayor reto para las PYMES es que el personal responsable de la ciberseguridad no puede dedicar tiempo suficiente al ámbito de la ciberseguridad porque tiene responsabilidades en más de un área. En relación con esto, la falta de un equipo separado de ciberseguridad ocupa el tercer lugar en la lista de dificultades experimentadas por las PYMES en la gestión de la ciberseguridad. Las PYMES tienen problemas para contratar y mantener personal empleado cualificado en ciberseguridad.

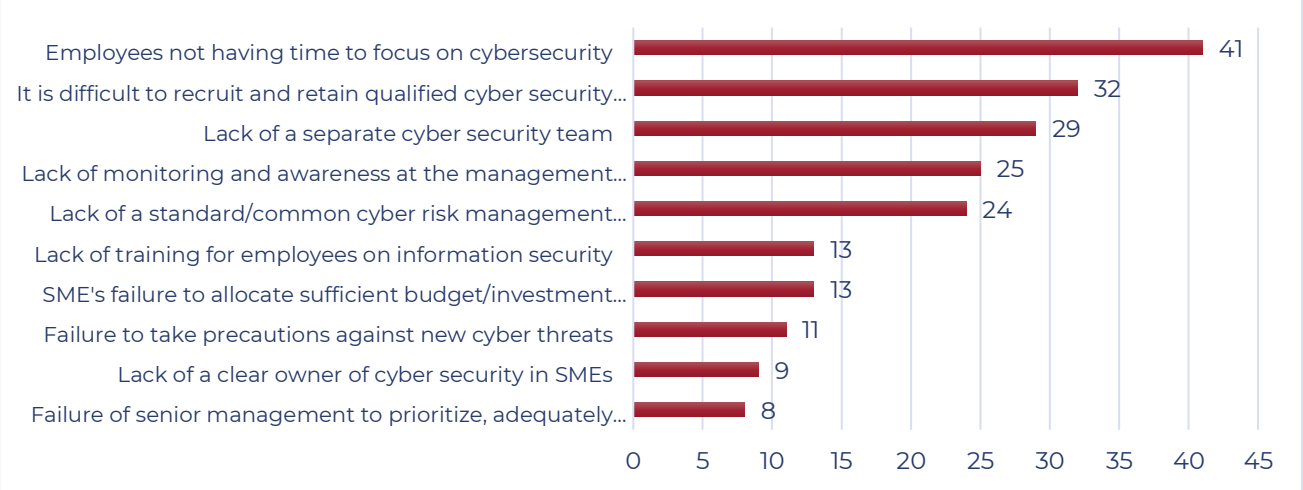


Figura 1 - Retos de las PYMES - Investigación en Türkiye.

En Rumanía, el entorno en línea brinda oportunidades de negocio y conexiones que pueden ayudar a las PYME a desarrollarse, pero también encierra muchos riesgos.

La ciberseguridad ya no es un cuento, también es una realidad en Rumanía, aunque hasta ahora no han sufrido ningún ciberataque importante.

La fuente de información utilizada es el INFORME VERIZON sobre ciberamenazas en 2023 - los principales puntos clave para las PYMES (DATA BREACH INVESTIGATIONS REPORT - DBIR), basado en 16.312 incidentes de seguridad de los cuales 5.199 se confirmaron como violaciones de la seguridad de los datos.

Puntos de interés para las PYMES:

- Las superficies de ataque para PYMES y corporaciones son similares, ya que utilizan software basado en la nube. La penetración no autorizada en el sistema, las técnicas de ingeniería social y los ataques básicos a aplicaciones web representan el 92% del total de tipos de ataques para las brechas registradas por las pymes (85% para las corporaciones).
- Ransomware 24% de los casos (los datos se roban antes de ser cifrados)

- Penetración no autorizada en el sistema: ataques complejos basados en malware y/o piratería informática para lograr sus objetivos.
- Los atacantes externos representan la mayor amenaza, causando el 83% de las brechas de seguridad actuales, alcanzando el 94% en el caso de los ataques a PYMES. El 94% de los actores implicados en la propagación de las amenazas son externos, frente al 89% en el caso de las grandes organizaciones, y el 98% de las violaciones tienen una motivación financiera, frente al 97% en el caso de las empresas.
- La motivación financiera ocupa el primer lugar en el 95% de los casos, porcentaje que aumenta hasta el 98% en el caso de los ataques a PYMES. Sólo el 1% está motivado por el espionaje.
- Las personas empleadas representan el eslabón débil de la cadena de seguridad - 74% de los casos (escaso conocimiento de las ciberamenazas). El principal método de intrusión puede deberse al uso de credenciales robadas - 49% y phishing - 12% u otros métodos, como la configuración incorrecta o el envío erróneo de datos sensibles.
- Correos electrónicos comerciales comprometidos: se engaña a la víctima para que transfiera grandes sumas de dinero a las cuentas de los atacantes.

En Noruega, las pequeñas y medianas empresas (PYMES) se enfrentan a importantes retos en materia de ciberseguridad. Muchas carecen de un conocimiento profundo de los riesgos que entraña, lo que da lugar a vulnerabilidades potenciales. Existe una laguna notable en la formación eficaz de las personas empleadas en materia de ciberseguridad, lo que convierte el error humano en un factor de riesgo habitual. Las PYMES, especialmente las que afirman disponer de recursos limitados, a menudo tienen dificultades para invertir en medidas avanzadas de ciberseguridad y en personal cualificado. También tienen que navegar por complejas leyes de protección de datos, lo que aumenta la complejidad de garantizar el cumplimiento de la normativa al tiempo que se salvaguarda la información sensible. El aumento de los ataques de phishing y de ingeniería social demuestra aún más su vulnerabilidad, al igual que la insuficiente seguridad de la red y el riesgo de amenazas internas. La gestión de estos riesgos es fundamental, pero a las PYMES les suele resultar difícil evaluar y gestionar eficazmente los riesgos. Además, la dependencia de proveedores externos introduce otra capa de complejidad, exponiendo potencialmente a las PYMES a amenazas adicionales de ciberseguridad.

2.2. LAS MUJERES EN LA CIBERSEGURIDAD

Analizamos las necesidades de formación y apoyo a las mujeres, las cualificaciones y competencias existentes de las mujeres en ciberseguridad y las recomendaciones para implicar a más empleadas en los retos de la ciberseguridad.

Microsoft hizo una encuesta: en 35 países europeos, menos de 1 de cada 5 licenciados en informática eran mujeres. El interés por la ciencia, la tecnología, la ingeniería y las matemáticas disminuye demasiado pronto. De hecho, el Programa para la Evaluación Internacional de Alumnos (PISA) de la OCDE revela que los niños tienen muchas más probabilidades que las niñas de imaginarse a sí mismos como profesionales de las TIC, científicos o ingenieros. (Microsoft, 2017).

Si nos fijamos en la proporción de mujeres entre las personas especialistas en TIC con empleo, en la UE-27 en 2020 sólo el 18,5% de todas las personas especialistas en TIC eran mujeres. Los mayores porcentajes de mujeres se registraron en Bulgaria (28,2%), Grecia (26,6%) y Rumanía (26,2%) (véase el gráfico 5 (Women go tech, 2021)). Los países de la región nórdica-báltica también se situaron en su mayoría cerca de los primeros puestos de la lista, con la excepción de Noruega, que se situó más bien en la parte media de la clasificación por países. (Women go tech, 2021).

Según el Departamento de Estadística de la República de Lituania, el número de personas empleadas en la categoría de información y comunicación en el cuarto trimestre de 2022 era de 29,4 mil hombres y 21,5 mil mujeres. En el primer trimestre de 2023, era de 34,6 mil hombres y 20,7 mil mujeres. En el segundo trimestre de 2023, había 36,8 mil hombres y 14,8 mil mujeres, y en el tercer trimestre de 2023, las cifras eran de 34,5 mil hombres y 18,0 mil mujeres. Se observa un descenso notable del número de mujeres empleadas entre el primer y el segundo trimestre de 2023, seguido de un aumento en el tercer trimestre de 2023 (Rodiklių Duomenų Bazė - Oficialiosios Statistikos Portalas, s.f.).

Con hasta un 11% de mujeres trabajando en ciberseguridad, se llevó a cabo una encuesta para conocer la opinión del público sobre las perspectivas de las mujeres en este campo. El 44,4% de las personas encuestadas respondió que el número de mujeres en el ámbito de la ciberseguridad debería situarse entre el 30 y el 60%. La mayor parte de las personas encuestadas respondió que las mujeres deberían representar entre el 30 y el 60% de profesionales (35,2%). Si se analizan las respuestas por sexo y grupo de edad, se observa que las mujeres, especialmente las más jóvenes (menores de 25 años y de 25 a 45 años), piensan con mayor frecuencia que el número de mujeres debería rondar la mitad. Los hombres jóvenes (menores de 25 años) piensan que debería haber hasta un 30% de mujeres. Se puede observar que las propias mujeres tienden a ver un número mucho mayor de mujeres en el campo de la Ciberseguridad que el que existe actualmente en el mercado. Esto es una buena noticia, ya que atraer a las mujeres a este campo no sólo ayudaría a solucionar la escasez de profesionales, sino que también aumentaría la seguridad de las propias organizaciones. (Bukauskas et al., 2022).

En Finlandia, como en muchos países europeos, existe un entendimiento común sobre el desequilibrio de género en la ciberseguridad y en el campo de las TI en general. Han aumentado las iniciativas y los esfuerzos para apoyar a las mujeres en el campo de la ciberseguridad y promover su participación para hacer frente a los retos de la ciberseguridad. La mayoría de ellas cuentan con el apoyo de organizaciones sin ánimo de lucro.

En el campo de la ciberseguridad se han puesto en marcha varias iniciativas para desarrollar itinerarios educativos y profesionales, programas de formación y eventos de creación de redes. La estrategia también se basa en la promoción de modelos de conducta, destacando las trayectorias profesionales de mujeres de éxito en ciberseguridad y compartiendo sus historias para inspirar a más mujeres a seguir carreras en este campo. Women4Cyber y las iniciativas enumeradas subrayan la importancia de la diversidad y la inclusión no sólo para hacer frente al desequilibrio en la desigualdad de género, sino también para contribuir a la fortaleza y resistencia generales del sector de la ciberseguridad. Las instituciones públicas y privadas también están apoyando esta estrategia al incluir esta dimensión de igualdad de género como prioridad absoluta en todas sus iniciativas.

Women4Cyber Finlandia (W4CFI)

Creada en agosto de 2021, W4CFI es una organización sin ánimo de lucro cuyo objetivo es aumentar el número de mujeres empleadas en el sector finlandés de la ciberseguridad. Forma parte de la iniciativa más amplia Women4Cyber de la UE y se centra en apoyar una industria más diversa e inclusiva en Finlandia. W4CFI participa en varias actividades, como la orientación, el intercambio de conocimientos y la sensibilización para aumentar y apoyar la participación de las mujeres en la ciberseguridad **Women4Cyber Finlandia.**

Proyecto del Ministerio finlandés de Transportes y Comunicaciones y la Universidad Aalto

El Ministerio de Transportes y Comunicaciones finlandés, en colaboración con la Universidad Aalto, está elaborando un paquete educativo para hacer de la ciberseguridad una competencia cívica en toda la Unión Europea. Esta iniciativa pone de relieve la creciente importancia de la ciberseguridad en la vida cotidiana y la necesidad de concienciar y capacitar a todos los ciudadanos, incluidas las mujeres. Subraya el papel de las instituciones educativas a la hora de proporcionar una educación y formación accesibles en materia de ciberseguridad, lo que resulta crucial para capacitar a las mujeres en este campo. Finlandia impulsa la educación en ciberseguridad en la UE. **Plataforma de Competencias y Empleos Digitales** (europa.eu).

Movimiento "Mimmit koodaa" (Código de la Mujer)

Esta iniciativa ofrece talleres, formación, oportunidades de establecer contactos, seminarios web y apoyo profesional. Se centra en desafiar los estereotipos y animar a más mujeres a explorar carreras en tecnología, incluida la ciberseguridad. Esta organización pretende crear vías para que las mujeres entren y destaquen en el campo de la ciberseguridad. **Mimmit** koodaa

En el panorama belga de la ciberseguridad, las mujeres representan el 19% de la mano de obra, según el primer estudio socioeconómico sobre el sector de la ciberseguridad en Bélgica publicado por Agoria en 2022. Con la coordinación del Ministerio de Economía belga (FPS Bélgica), los actores políticos competentes en Bélgica han elaborado un plan quinquenal para las mujeres en el ámbito digital denominado "Mujeres en el ámbito digital - Estrategia nacional e intersectorial 2021-2026". El plan quinquenal incluye una estrategia común e intersectorial basada en cinco objetivos estratégicos útiles para combatir los prejuicios y hacer frente a los obstáculos estructurales que impiden a las mujeres participar en la economía digital. Los cinco objetivos son los siguientes:

1. Garantizar que más mujeres se gradúen en el sector digital;

2. Estimular a todas las mujeres a participar en el mercado laboral digital y/o en el sector digital;
3. Mejorar la retención de las mujeres en el sector digital;

4. Crear nuevas imágenes para promover el papel de la mujer en este campo (dentro y fuera de la pantalla);

5. Cerrar la brecha de género entre grupos objetivo específicos (**enlace a la Estrategia**).

La Fundación Women4Cyber, con sede en Bruselas, organiza y apoya una amplia gama de actividades dirigidas a mujeres que trabajan o inician su carrera profesional en el ámbito de la ciberseguridad en Bélgica y en Europa. En Bélgica, la Fundación apoya y coopera con la sección nacional belga (**Women4Cyber Belgium**) en estas actividades. La sección nacional belga cuenta con unos 20 miembros activos que trabajan en las iniciativas. Las actividades, eventos y programas organizados por el sección son, por ejemplo reuniones y eventos de networking (virtuales y presenciales) como el "café virtual" en el que la Sección Belga de W4C invita a expertos en diversos campos relacionados con la ciberseguridad y la seguridad de la información a hablar; seminarios web y sesiones informativas; programas de tutoría destinados a ayudar a las mujeres a mejorar sus habilidades y avanzar en sus carreras de ciberseguridad a todos los niveles; proyectos y eventos en colaboración con la Coalición Belga de Ciberseguridad (como la organización del **Día Internacional de la Mujer 2023**); promoción de becas para programas educativos relacionados con la ciberseguridad como los organizados por Solvay Brussels School of Economics & Management.

En Noruega, abordar la brecha de género en ciberseguridad es crucial para crear una mano de obra resistente y diversa. La proporción de mujeres en TI es sólo del 29%. La baja cifra está muy relacionada con el número de mujeres que eligen asignaturas matemáticas y técnicas en secundaria.

Necesidades de formación y apoyo y recomendaciones para implicar a las mujeres

Hacen falta programas de ciberseguridad diseñados específicamente para fomentar la participación de las mujeres. Estos programas deberían equilibrar los aspectos técnicos con las cuestiones de ciberseguridad centradas en la organización y el ser humano. Existen varias ofertas de formación técnica superior en este campo, mientras que las ofertas de formación superior en las ocupaciones más típicas de las mujeres (pedagogía - ocupaciones sanitarias) no tienen ofertas de este tipo y el desarrollo de ofertas de formación más cortas en ciberseguridad relacionadas con esas ocupaciones podría llegar a más mujeres. Esto también lo apoya el propio sector, que afirma que la diversidad puede aportar perspectivas únicas a los retos de la ciberseguridad. Aumentar la concienciación sobre las carreras internas de ciberseguridad entre las mujeres podría ocurrir a través de talleres, seminarios y programas de divulgación específicos en escuelas y universidades puede inspirar a más mujeres a entrar en este campo.

Otro enfoque, sugerido por muchas de las 50 mujeres tecnológicas noruegas nominadas en 2022, es el establecimiento de programas de tutoría y oportunidades de creación de redes para mujeres en el ámbito de la ciberseguridad, con el fin de proporcionarles orientación y apoyo esenciales, ayudándolas a navegar y avanzar en este campo.

El propio sector de la ciberseguridad sugiere que las organizaciones apliquen prácticas y políticas de contratación inclusivas que fomenten activamente la contratación y retención de mujeres en puestos de ciberseguridad. El 32 % de las mujeres que desempeñan funciones técnicas suelen ser "la única mujer de la sala" en el trabajo, según el informe de McKinsey "Women in the Workplace 2022".

Por último, la promoción de mujeres a puestos de liderazgo en ciberseguridad puede proporcionar modelos de conducta e inspirar a otras mujeres a seguir caminos similares, como por ejemplo **Mia Landsem**.

En Rumanía, la ciberseguridad sigue siendo uno de los sectores tecnológicos más dinámicos y apasionantes. Sin embargo, este sector necesita un cambio sistémico en la representación y remuneración de las mujeres. A pesar del creciente interés por el campo de la ciberseguridad, la disparidad de género persiste. Las mujeres siguen estando muy infrarrepresentadas, mientras que la mayoría de los puestos de trabajo son predominantemente masculinos. El futuro de la ciberseguridad depende de la capacidad de atraer, retener y promocionar a más ciberprofesionales, incluidas más mujeres.

Se han realizado muchos estudios para mostrar lo infravaloradas que están las mujeres en todo el mundo, pero también para que todo el mundo comprenda la importancia de las mujeres en todos los ámbitos, y en particular en la ciberseguridad. La extrema diferencia de género entre la base de empleados de ciberseguridad indica que otras fuerzas en el trabajo no son iguales en absoluto. Las mujeres representan el 39% de la mano de obra total. Representan el 38% los empleos STEM, pero sólo alrededor del 25% de la mano de obra de ciberseguridad, según Cybersecurity Ventures.

Hay varias barreras que mantienen a las mujeres alejadas de la ciberseguridad. Según una investigación de (ISC)2, organización sin ánimo de lucro dedicada a la formación y certificación en ciberseguridad, la mayoría de las mujeres que han trabajado en este campo denuncian discriminación por motivos de género. Casi todas las mujeres (87%) declararon haber sufrido discriminación inconsciente, mientras que el 19% dijo haber sido objeto de discriminación abierta. Las mujeres también citaron retrasos inexplicables en la promoción profesional (53%) y respuestas exageradas a los errores (29%).

La discriminación también se manifiesta en una brecha salarial. La investigación de (ISC)2 muestra que el 32% de los hombres que trabajan en ciberseguridad ganan una media de 50.000 a 100.000 dólares anuales, mientras que sólo el 18% de las mujeres en ciberseguridad ocupan el mismo tramo de ingresos. Y el 25% de los hombres frente al 20% de las mujeres ganan entre 100.000 y 500.000 dólares anuales.

Hay argumentos de peso para aumentar el número de mujeres en ciberseguridad, como los beneficios de la diversidad, la innovación, la empatía emocional y una perspectiva imparcial, todas ellas aptitudes valiosas para el lugar de trabajo en ciberseguridad.

Jay Koehler, miembro de la junta directiva de Women in Cybersecurity, aportó otra idea: "Las mujeres abandonan porque es un 'club de chicos' y hay un escaso sentido de pertenencia". Este problema puede abordarse mediante el compromiso y la responsabilidad de proporcionar seguridad psicológica y un lugar de trabajo respetuoso con el género, así como creando redes de mujeres.

Existe la esperanza de que la ciberseguridad deje de ser una "profesión dominada por los hombres" y se llene de personas con talento de todos los géneros y procedencias.

La literatura sobre la participación de las mujeres en la ciberseguridad en España es escasa. La mayor parte de la literatura existente muestra un pronunciado desequilibrio de género en la comunidad científica en general, incluyendo las disciplinas STEM, con una notable disminución en la progresión de las mujeres a etapas superiores de la carrera, comúnmente considerado como un "fenómeno pipeline". En lo que respecta a la educación superior, la brecha de género sigue siendo pronunciada, ya que sólo el 18% de los que finalizan estudios en estas materias son mujeres. La contratación de mujeres en las PYMES para puestos relacionados con la I+D sigue siendo muy baja, no llegando al 30% según los datos del Instituto Nacional de Estadística. En cuanto a las investigadoras en ciberseguridad de los IES en España, son muy pocos los que presentan una plantilla equilibrada en cuanto a género. De los 31 IES revisados por *la Fundación Alternativas*, 11 de ellos no tienen ninguna mujer participando en sus equipos de investigación y sólo 5 de ellos demuestran una plantilla más igualitaria. En respuesta a estos retos, el análisis de las necesidades de formación y apoyo identifica áreas clave de mejora. Deben desarrollarse iniciativas para animar a más mujeres a cursar estudios de doctorado y garantizar una representación equilibrada a lo largo de todo el proceso educativo. Es crucial abordar los prejuicios en los procesos de promoción profesional, y los programas de tutoría pueden desempeñar un papel fundamental a la hora de guiar a las mujeres a través de las

complejidades del campo de la ciberseguridad. Además, se recomienda la colaboración con organizaciones de la industria privada para investigar las trayectorias profesionales y estimular la participación de las mujeres en funciones de ciberseguridad en industrias privadas. La evaluación de las cualificaciones y competencias subraya la importancia de los programas de formación personalizados, que hacen hincapié en habilidades y competencias específicas de ciberseguridad.

2.3. ANÁLISIS DE LAS OCUPACIONES EN LA ESCO

Interpretamos la actual clasificación ESCO (Clasificación europea multilingüe de capacidades, competencias y ocupaciones) en relación con los resultados de aprendizaje identificados, incluidos los conocimientos, las capacidades y las competencias. El objetivo es:

- Analizar las ocupaciones existentes en la ESCO relacionadas con la ciberseguridad.
- Asignar los resultados de aprendizaje identificados a las ocupaciones en la ESCO en términos de conocimientos, aptitudes, competencias, etc.

Para cada ocupación existe un conjunto de competencias, destrezas y conocimientos. A continuación figuran definiciones y ejemplos de competencia, aptitudes, conocimientos y valor.

La competencia se refiere a la capacidad de un individuo para realizar una tarea o un trabajo específico de forma eficaz. Abarca una combinación de conocimientos, habilidades y comportamientos aplicados para mejorar el rendimiento. Ejemplo: Ser competente en la gestión de proyectos implica una combinación de habilidades organizativas, conocimiento de los procesos de gestión de proyectos y capacidad para comunicarse eficazmente con los miembros del equipo.

Las destrezas son habilidades o capacidades específicas adquiridas mediante la práctica, la formación o la experiencia que permiten a una persona realizar tareas. Por ejemplo: Conocimientos de pruebas de penetración, capacidad para utilizar herramientas y programas informáticos de ciberseguridad, conocimientos de programación y capacidad para analizar y responder a las amenazas en tiempo real.

El conocimiento se refiere a los hechos, la información y la comprensión aprendidos a través de la educación o la experiencia. Abarca la comprensión teórica de hechos y principios relacionados con un campo concreto. Ejemplo: Comprensión de cómo se llevan a cabo diferentes tipos de ciberataques (por ejemplo, phishing, ransomware, ataques DDoS) o conocimiento de varios métodos de cifrado y familiaridad con las últimas tendencias y desarrollos en ciberseguridad.

Este análisis se divide en 2 fases:

Fase 1: Examen y selección de las ocupaciones en la ESCO

Consulta en el portal ESCO para filtrar las ocupaciones relacionadas con la ciberseguridad y documentando en el siguiente apartado cada ocupación, prestando especial atención a las habilidades, competencias, conocimientos listados.

ESCO Ocupación Título	Conocimientos	Habilidades	Competencias
3512.3 - Técnico de seguridad TIC	• redes TIC • vectores de ataque al hardware • contramedidas de	• abordar los problemas de forma crítica • analizar el sistema	• integrar los componentes del sistema • proporcionar

	ciberataques • sistemas operativos adquisición de TIC • equipos de red • aplicación web • amenazas a la seguridad	TIC • garantizar una gestión adecuada de los documentos • ejecutar pruebas de software identificar los puntos débiles del sistema TIC	documentación técnica • resolver problemas de sistemas TIC • utilizar software de control de acceso
2529.1 - jefe de seguridad TIC - Incluye a las personas que desempeñan funciones de seguridad corporativa.	• riesgos para la seguridad de las redes TIC • legislación sobre seguridad de las TIC • normas de seguridad de las TIC • vectores de ataque • técnicas de auditoría • contramedidas de ciberataques • ciberseguridad • protección de datos • sistemas de apoyo a la toma de decisiones • confidencialidad de la información • estrategia de seguridad de la información • política interna de gestión de riesgos • resiliencia organizativa	• educar en la confidencialidad de los datos • garantizar el cumplimiento de las normas organizativas en materia de TIC • garantizar el cumplimiento de los requisitos legales • garantizar la cooperación entre departamentos • garantizar la privacidad de la información • identificar los riesgos para la seguridad de las TIC • aplicar la gestión de riesgos de las TIC • aplicar políticas de seguridad de las TIC • aplicar la gobernanza empresarial	• dirigir ejercicios de recuperación en caso de catástrofe • mantener un plan de continuidad de las operaciones • gestionar el cumplimiento de las normas de seguridad informática • gestionar los planes de recuperación en caso de catástrofe • seguir la evolución en su campo de especialización • seguir las tendencias tecnológicas • utilizar el sistema de apoyo a la toma de decisiones
2529.2 - experto forense digital - recupera y analiza información de ordenadores y otros tipos de dispositivos de almacenamiento de datos; examina de forma forense soportes digitales que pueden haber sido ocultados, encriptados o dañados, con el fin de identificar, preservar, recuperar, analizar y presentar hechos y opiniones sobre la información digital.	• riesgos para la seguridad de las redes TIC • normas de seguridad de las TIC • informática forense • contramedidas de ciberataques • confidencialidad de la información • herramienta de pruebas de penetración • lenguajes de consulta • lenguaje de consulta del marco de descripción de recursos	• aplicar la ingeniería inversa • desarrollar una estrategia de seguridad de la información • educar en la confidencialidad de los datos • recopilar datos con fines forenses • identificar los riesgos para la seguridad de las TIC • identificar los puntos débiles del sistema TIC • aplicar herramientas	• gestionar el cumplimiento de las normas de seguridad informática • gestionar datos para asuntos jurídicos • realizar conservaciones forenses de dispositivos digitales

		de diagnóstico de redes TIC • prestar asesoramiento en materia de TIC • proteger la información confidencial de los clientes • utilizar programación de secuencias de comandos • utilizar programas informáticos para la conservación de datos • realizar pruebas de seguridad de las TIC	
2529.3 - Ingeniero de seguridad de sistemas empotrados: los ingenieros de seguridad de sistemas empotrados se centran en los productos conectados y sus redes de apoyo, y no tanto en la seguridad organizativa como el ingeniero de seguridad de TIC.	• riesgos para la seguridad de las redes TIC • normas de seguridad de las TIC • internet de los objetos • programación informática • contramedidas de ciberataques • sistemas integrados • estrategia de seguridad de la información • anomalías de software	• analizar el sistema TIC • crear diagrama de flujo • definir políticas de seguridad • desarrollar un controlador de dispositivo TIC • desarrollar un prototipo de software • ejecutar pruebas de software • identificar los riesgos para la seguridad de las TIC • identificar los puntos débiles del sistema TIC • interpretar textos técnicos • prestar asesoramiento en materia de TIC • realizar pruebas de seguridad de las TIC • proporcionar documentación técnica	• estar al día de las últimas soluciones en sistemas de información • gestionar el cumplimiento de las normas de seguridad informática • supervisar el rendimiento del sistema • realizar un análisis de riesgos • comunicar los resultados de las pruebas utilizar patrones de diseño de software • utilizar bibliotecas de software • utilizar herramientas de ingeniería de software asistida por ordenador • definir los requisitos técnicos
2529.4 - hacker ético - realiza evaluaciones de vulnerabilidad de seguridad y pruebas de penetración de acuerdo con métodos y protocolos	• vectores de ataque • informática forense • contramedidas de ciberataques • ética	• realizar pruebas de seguridad de las TIC • proporcionar documentación técnica	• abordar los problemas de forma crítica • analizar el contexto de una organización • supervisar el

aceptados por la industria; analiza sistemas para vulnerabilidades potenciales que pueden resultar de una configuración inadecuada del sistema, defectos de hardware o software, o debilidades operacionales.	• requisitos legales de los productos TIC • herramienta de pruebas de penetración • anomalías de software • herramientas para la automatización de pruebas TIC • amenazas para la seguridad de las aplicaciones web	• desarrollar exploits de código • realizar auditorías de las TIC • ejecutar pruebas de software • identificar los riesgos para la seguridad de las TIC • identificar los puntos débiles del sistema TIC	rendimiento del sistema
2529.5 - Gestor de la resiliencia de las TIC: investiga, planifica y desarrolla modelos, políticas, métodos, técnicas y herramientas que mejoran la ciberseguridad, la resiliencia y la recuperación en caso de catástrofe de una organización.	• técnicas de recuperación de las TIC • ciberseguridad interna • política de gestión de riesgos • resiliencia organizativa • mejores prácticas de copia de seguridad del sistema	• elaborar planes de emergencia • desarrollar una estrategia de seguridad de la información • realizar auditorías de las TIC • identificar los riesgos para la seguridad de las TIC • implantar un sistema de recuperación de las TIC • aplicar la gestión de riesgos de las TIC	• analizar los procesos empresariales • analizar el contexto de una organización • cumplir la normativa legal • dirigir ejercicios de recuperación en caso de catástrofe • gestionar el cumplimiento de las normas de seguridad informática • gestionar los planes de recuperación en caso de catástrofe • gestionar la seguridad del sistema • realizar pruebas de seguridad de las TIC
2529.6 - Administrador de seguridad TIC - planifica y ejecuta medidas de seguridad para proteger la información y los datos de accesos no autorizados, ataques deliberados, robo y corrupción.	• riesgos para la seguridad de las redes TIC • Internet de los objetos • contramedidas de ciberataques • herramientas de desarrollo de bases de datos • gobernanza de internet • gestión de dispositivos móviles • sistemas operativos • resiliencia organizativa • metodologías de garantía de calidad • mejores prácticas de copia de seguridad del sistema	• identificar los puntos débiles del sistema TIC • interpretar textos técnicos • mantener la gestión de identidades TIC • mantener la seguridad de la base de datos	• aplicar las políticas de la empresa • atender a la calidad de los sistemas TIC • garantizar una gestión adecuada de los documentos • gestionar la arquitectura de datos de las TIC • gestionar el cumplimiento de las normas de seguridad informática • solucionar problemas relacionados con las TIC • resolver problemas de sistemas TIC
2529.7 - Ingeniero de seguridad de las TIC - asesora y aplica	• legislación sobre	• desarrollar una	• definir los criterios de

soluciones para controlar el acceso a datos y programas y garantiza la protección de la misión y los procesos empresariales de la organización.	seguridad de las TIC • normas de seguridad de las TIC • vectores de ataque • análisis empresarial • contramedidas de ciberataques • ciberseguridad • tecnologías emergentes • arquitectura de la información • estrategia de seguridad de la información • sistemas operativos • resiliencia organizativa • gestión de riesgos • datos no estructurados	estrategia de seguridad de la información • educar en la confidencialidad de los datos • garantizar la seguridad de la información • realizar auditorías de las TIC • ejecutar pruebas de software • identificar los riesgos para la seguridad de las TIC • identificar los puntos débiles del sistema TIC • aplicar la gestión de riesgos de las TIC • prestar asesoramiento en materia de TIC • analizar el sistema TIC • definir políticas de seguridad	calidad de los datos • definir los requisitos técnicos • mantener registros de tareas • estar al día de las últimas soluciones en sistemas de información • gestionar el cumplimiento de las normas de seguridad informática • gestionar los planes de recuperación en caso de catástrofe • supervisar el rendimiento del sistema • realizar análisis de datos • realizar un análisis de riesgos • informar de los resultados de las pruebas solucionar problemas • verificar las especificaciones formales de las TIC
2529.8 - Gestor de seguridad de las TIC - propone e implementa las actualizaciones de seguridad necesarias; asesora, apoya, informa y proporciona formación y concienciación en materia de seguridad y toma medidas directas sobre la totalidad o parte de una red o sistema.	• técnicas TIC de gestión de problemas • gestión de proyectos TIC • política de calidad de las TIC • normas de seguridad de las TIC • requisitos de los usuarios de sistemas TIC • internet de los objetos • vectores de ataque • informática forense • estrategia de seguridad de la información • política interna de gestión de riesgos • gobernanza de internet • requisitos legales de los productos TIC	• definir políticas de seguridad • desarrollar una estrategia de seguridad de la información • establecer un plan de prevención de la seguridad de las TIC • aplicar la gestión de riesgos de las TIC	• dirigir ejercicios de recuperación en caso de catástrofe • mantener la gestión de identidades TIC • gestionar el cumplimiento de las normas de seguridad informática • gestionar los planes de recuperación en caso de catástrofe • resolver problemas de sistemas TIC
2529.9 - ingeniero del conocimiento - integra conocimientos estructurados en sistemas informáticos (bases de conocimientos) para resolver	• inteligencia empresarial • modelización de procesos empresariales • herramientas de	• utilizar una interfaz específica de la aplicación • utilizar bases de datos	• analizar los requisitos de la empresa • aplicar la teoría de los sistemas TIC

problemas complejos que normalmente requieren un alto nivel de experiencia humana o métodos de inteligencia artificial.	desarrollo de bases de datos • extracción de información • estructura de la información tratamiento del lenguaje natural • principios de inteligencia artificial • lenguaje de consulta del marco de descripción de recursos • ciclo de vida del desarrollo de sistemas • teoría de sistemas • algoritmización de tareas • programación web	• utilizar lenguajes de marcado	• evaluar el conocimiento de las TIC • crear árboles semánticos • definir los requisitos técnicos • gestionar la integración semántica de las TIC • gestionar los conocimientos empresariales • gestionar la base de datos

Fase 2: Cartografía de la ocupación en la ESCO y resultados del aprendizaje

Con la tabla anterior, analizamos las ocupaciones documentadas e identificamos los resultados del aprendizaje asociados a cada función. Utilizamos el marco ESCO para categorizar estos resultados en conocimientos, habilidades y competencias.

Un resultado de aprendizaje es un enunciado claro y específico que describe lo que se espera que los estudiantes aprendan y sean capaces de hacer al término de un periodo de instrucción. El enunciado incluye conocimientos, destrezas y actitudes.

En la sección del clasificador de ocupaciones ESCO, los profesionales de las tecnologías de la información y la comunicación se dividen en dos subsecciones: Desarrolladores y análisis de software y aplicaciones y Profesionales de bases de datos y redes. Esta última consta de cuatro grupos: Profesionales de bases de datos y redes, Administradores de sistemas, Profesionales de redes informáticas y Profesionales de bases de datos y redes no clasificados bajo otros epígrafes. Todas las ocupaciones de ciberseguridad presentadas en la tabla se encuentran en este grupo unitario. Por ejemplo, el grupo incluye a las personas especialistas en seguridad de las tecnologías de la información y la comunicación.

En estos casos, las tareas incluirían

(a) desarrollar planes para salvaguardar los archivos informáticos contra modificaciones, destrucción o divulgación accidentales o no autorizadas y para satisfacer las necesidades urgentes de tratamiento de datos.

(b) formar a las personas usuarias y fomentar la concienciación en materia de seguridad para garantizar la seguridad del sistema y mejorar la eficiencia del servidor y de la red.

(c) mantener conversaciones con las personas usuarias para tratar cuestiones como las necesidades de acceso a los datos informáticos, las infracciones de seguridad y los cambios de programación.

(d) seguimiento de los informes actuales sobre virus informáticos para determinar cuándo actualizar los sistemas de protección antivirus.

(e) modificar los ficheros de seguridad informática para incorporar nuevos programas, corregir errores o cambiar el estado de acceso individual.

(f) controlar el uso de los ficheros de datos y regular el acceso para salvaguardar la información de los ficheros informáticos.

(g) realizar evaluaciones de riesgos y ejecutar pruebas del sistema de tratamiento de datos para garantizar el funcionamiento de las actividades de tratamiento de datos y las medidas de seguridad.

(h) cifrar las transmisiones de datos y erigir cortafuegos para ocultar la información confidencial mientras se transmite y mantener alejadas las transferencias digitales contaminadas.

Descripción de los resultados del aprendizaje para cada ocupación:

Ocupación	**Resultados del aprendizaje**
Técnico de seguridad TIC (3512.3)	• Demostrar un conocimiento exhaustivo de las redes TIC, los vectores de ataque de hardware, las contramedidas contra ciberataques y los sistemas operativos. • Analizar críticamente y diagnosticar las vulnerabilidades de los sistemas TIC para mejorar su seguridad. • Aplicar y gestionar estrategias sólidas de gestión de documentos que respeten los protocolos de seguridad de las TIC. • Desarrollar y ejecutar planes detallados de pruebas de software para identificar y rectificar las vulnerabilidades del software. • Integrar los componentes del sistema y emplear software de control de acceso para crear sistemas TIC seguros y eficaces**.**
Jefe de Seguridad de las TIC (2529.1)	• Comprender y analizar los riesgos, la legislación y las normas de seguridad de las redes TIC para salvaguardar la información de la organización. • Desarrollar y aplicar estrategias de seguridad de la información y políticas internas de gestión de riesgos. • Dirigir ejercicios de recuperación en caso de catástrofe y mantener planes de continuidad operativa.

	• Educar al personal sobre la confidencialidad de los datos y garantizar la cooperación entre departamentos para mejorar las prácticas de seguridad.
Experto forense digital (2529.2)	• Analizar y probar la seguridad de los sistemas empotrados, especialmente en el entorno de la Internet de las Cosas (IoT). • Desarrollar y ejecutar prototipos y pruebas de software y utilizar herramientas de ingeniería de software asistida por ordenador. • Gestionar el cumplimiento de las normas de seguridad informática y realizar análisis de riesgos y seguimiento del rendimiento del sistema. • Definir y aplicar políticas de seguridad y requisitos técnicos para sistemas empotrados.
Ingeniero de seguridad de sistemas integrados (2529.3)	• Analizar y probar la seguridad de los sistemas empotrados, especialmente en el entorno de la Internet de las Cosas (IoT). • Desarrollar y ejecutar prototipos y pruebas de software y utilizar herramientas de ingeniería de software asistida por ordenador. • Gestionar el cumplimiento de las normas de seguridad informática y realizar análisis de riesgos y seguimiento del rendimiento del sistema. • Definir y aplicar políticas de seguridad y requisitos técnicos para sistemas empotrados.
Hacker ético (2529.4)	• Realizar evaluaciones de vulnerabilidad de la seguridad y pruebas de penetración utilizando métodos aceptados por la industria. • Identificar y explotar las posibles vulnerabilidades de los sistemas para mejorar las medidas de seguridad. • Desarrollar exploits de código y ejecutar auditorías TIC para garantizar la integridad del sistema. • Analizar el contexto de una organización para adaptar eficazmente las estrategias de

	seguridad.
Gestor de la capacidad de recuperación de las TIC (2529.5)	• Desarrollar y aplicar planes de contingencia y estrategias de seguridad de la información para situaciones de emergencia. • Implantar y gestionar sistemas de recuperación de TIC y procesos de gestión de riesgos. • Dirigir ejercicios de recuperación en caso de catástrofe y gestionar la seguridad del sistema durante las crisis. • Analizar los procesos empresariales para mejorar la resistencia de la organización y el cumplimiento de la normativa legal.
Administrador de seguridad TIC (2529.6)	• Planificar y aplicar medidas de seguridad para proteger los datos y gestionar los sistemas de identidad de las TIC. • Mantener la seguridad de la base de datos y garantizar la integridad y resistencia del sistema. • Resolver problemas de sistemas TIC y llevar a cabo metodologías de resolución de problemas y garantía de calidad. • Gestionar la arquitectura de datos y cumplir las políticas organizativas de protección de datos.
Ingeniero de seguridad TIC (2529.7)	• Asesorar y aplicar soluciones para controlar el acceso a los datos y proteger los procesos empresariales. • Analizar los sistemas TIC y definir las políticas de seguridad y los criterios de calidad de los datos. • Realizar análisis de datos y análisis de riesgos y gestionar el cumplimiento de las normas de seguridad informática y los planes de recuperación en caso de catástrofe. • Mantenerse al día de las nuevas tecnologías y soluciones de sistemas de información
Responsable de seguridad TIC (2529.8)	• Proponer y aplicar actualizaciones de seguridad y gestionar la seguridad de las TIC en diversos proyectos. • Dirigir ejercicios de recuperación en caso

	de catástrofe y establecer planes de prevención de la seguridad de las TIC. • Mantener y gestionar los sistemas de gestión de identidades de las TIC y resolver problemas complejos del sistema. • Desarrollar y aplicar estrategias de seguridad de la información y gestionar planes de recuperación en caso de catástrofe.
Ingeniero del conocimiento (2529.9)	• Integrar el conocimiento estructurado en sistemas informáticos utilizando herramientas avanzadas como el lenguaje de consulta RDF y la programación web. • Gestionar la integración semántica y los sistemas de bases de datos para mejorar la gestión del conocimiento empresarial. • Analizar los requisitos empresariales y aplicar la teoría de los sistemas TIC para desarrollar bases de conocimiento eficaces. • Cree árboles semánticos y evalúe el conocimiento de las TIC para resolver problemas complejos mediante métodos de IA.

ANÁLISIS Y CONCLUSIONES

2.4. ANÁLISIS DE LA INVESTIGACIÓN DE CAMPO

Análisis de la encuesta sobre el terreno de EFP e IES

Los datos de la encuesta " Identificación de las necesidades de formación de los y las agentes del cambio en ciberseguridad de las PYMES" contienen una serie de preguntas centradas en la formación en ciberseguridad en el contexto de la Educación y Formación Profesionales (EFP) y de las Instituciones de Educación Superior (IES). Recopilamos datos sobre los temas incluidos en la formación en ciberseguridad, los métodos de enseñanza, la inclusión de la perspectiva de género y los datos demográficos de los encuestados.

El objetivo de este estudio es analizar las respuestas para comprender el estado actual de la formación en ciberseguridad, las metodologías empleadas y las percepciones en torno a la inclusión y la eficacia en este campo.

El análisis de las respuestas se basará en la siguiente estructura clave:

- Demografía
- Plan de estudios, necesidades de formación y preferencias de aprendizaje
- Requisitos de competencia y aptitudes futuras
- Perspectivas específicas de género

Demografía:

La distribución por sexos de las personas encuestadas entre los centros de formación profesional y los centros de enseñanza superior es la siguiente:

Total de encuestados por tipo de institución

Tipo de institución	Respuestas	Mujer	Hombre	Prefiero no decirlo
IES (Instituciones de Educación Superior)	104	28	73	3
EFP (Educación y Formación Profesionales)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Aunque existe un desequilibrio de género tanto en las instituciones de enseñanza superior como en las de formación profesional, la diferencia es menor en las de formación profesional. Para ofrecer una imagen más clara de la representación de género en relación con el número total de respuestas de cada institución y ajustar los resultados relativos al número de respuestas sesgadas, hemos calculado el porcentaje de cada género dentro de ambos tipos de institución.

Distribución de las personas encuestadas por tipo de institución

Tipo de institución	Femenino	Hombres	Prefiero no decirlo %.	Total
IES (Instituciones de Educación Superior)	27	70	3	**100%**
EFP (Educación y Formación Profesionales)	42	56	2	**100%**

El análisis ajustado al sesgo de respuesta confirma que, si bien ambos tipos de instituciones tienen una mayor proporción de personas encuestadas varones, la brecha entre la representación masculina y femenina sigue siendo menor en las instituciones de EFP. La razón podría ser diversa (por ejemplo, factores culturales, estructurales o políticos que influyen en la diversidad de género en la educación en ciberseguridad en estos tipos de instituciones). El mayor porcentaje de mujeres encuestadas en la EFP sugiere áreas potenciales para una mayor investigación sobre las prácticas que apoyan un entorno más inclusivo de género en la formación profesional en comparación con la educación superior.

Plan de estudios, necesidades de formación y preferencias de aprendizaje

Temas incluidos en las formaciones sobre ciberseguridad existentes en las IES y EFP

Tema	Respuestas	IES	EFP
Fundamentos de ciberseguridad	151	90	61
Seguridad de la red	123	72	51
Análisis y gestión de amenazas	99	65	34
Criptografía	92	57	35
Respuesta a incidentes	82	49	33
Gestión de riesgos	77	43	34
Leyes y políticas de ciberseguridad	73	42	31
Técnicas avanzadas de mitigación de amenazas	54	33	21

Parece que los conocimientos y habilidades fundamentales y la seguridad de la red son prioritarios. El análisis y la gestión de amenazas, la criptografía y la respuesta a incidentes sugieren una cobertura exhaustiva de las amenazas a la ciberseguridad en las formaciones. Gestión de Riesgos y Leyes y Políticas de Ciberseguridad a pesar de apuntar a una concienciación de la necesidad de un enfoque holístico que incluya la comprensión del contexto legal y la gestión eficaz de los riesgos no siempre se selecciona. Es interesante observar que las técnicas avanzadas de mitigación de amenazas se incluyen menos en las formaciones.

Para proporcionar los resultados sin el sesgo introducido por el número de encuestados de cada tipo de institución (HEI y EFP), los datos se normalizaron por el número total de respuestas para cada tipo de institución. Este enfoque nos permite ver la proporción de instituciones que incluyen cada tema en sus programas de formación en ciberseguridad.

Temas	**Proporción IES**	**Proporción de EFP**
Fundamentos de ciberseguridad	15.76%	15.48%
Seguridad de la red	12.61%	12.94%
Análisis y gestión de amenazas	11.38%	8.63%
Criptografía	9.98%	8.88%
Respuesta a incidentes	8.58%	8.38%
Gestión de riesgos	7.53%	8.63%
Leyes y políticas de ciberseguridad	7.36%	7.87%
Técnicas avanzadas de mitigación de amenazas	5.78%	5.33%

Curiosamente, existen prioridades similares con ligeras variaciones. Tanto las IES como los centros de FP hacen especial hincapié en los "Fundamentos de la ciberseguridad" y la "Seguridad de las redes". Esto indica que estos temas se reconocen como componentes críticos de la educación en ciberseguridad. Las proporciones están muy igualadas, con los "Fundamentos de la ciberseguridad" ligeramente más enfatizados en las IES en comparación con los centros de FP y la "Seguridad de la red" mostrando un patrón similar pero con una brecha más estrecha.

Hay una variación notable en el énfasis en temas más especializados como "Análisis y gestión de amenazas", "Criptografía" y "Técnicas avanzadas de mitigación de amenazas". Las IES tienden a asignar una proporción ligeramente mayor de sus programas de formación a estos temas en comparación con las EFP. Esto puede explicarse por el hecho de que las IES se centran en proporcionar una comprensión más completa y teórica de la ciberseguridad, que a menudo incluye una gama más amplia de temas especializados. Por otro lado, los centros de FP, aunque siguen cubriendo un amplio espectro de temas, pueden dar prioridad a las aplicaciones prácticas y a la preparación inmediata para el empleo.

Métodos de enseñanza

Métodos de enseñanza	**Proporción IES**	**Proporción de EFP**
Casos prácticos	60.91%	39.09%
Proyectos de grupo	58.95%	41.05%
Laboratorios prácticos	59.02%	40.98%
Conferencias	56.97%	43.03%
Aula invertidas	34.78%	65.22%
Simulaciones en línea	51.35%	48.65%

Los métodos de estudio de casos, proyectos en grupo, laboratorios prácticos y conferencias se utilizan ampliamente en ambos tipos de instituciones, con mayor preferencia en las IES que en la FP. En cuanto al método de aula invertida, es más frecuente en FP (65,22%) que en IES (34,78%), lo que indica una inclinación hacia el modelo de aprendizaje interactivo en la formación profesional. Las aulas invertidas dan prioridad al aprendizaje activo y a la participación de los y las estudiantes, que se ajustan bien al enfoque práctico y basado en competencias característico de la EFP.

Eficacia de los métodos de enseñanza

Método de enseñanza	Cuenta
Sesiones prácticas	141
Talleres presenciales	134
Simulaciones interactivas	104
Cursos en línea	100
Tutoriales en vídeo	73
Seminarios en línea	68

Esta visión general pone de relieve la diversidad de métodos de enseñanza preferidos, pero con un claro énfasis en las experiencias de aprendizaje prácticas, interactivas y flexibles. Las sesiones prácticas y los talleres presenciales son muy valorados, ya que proporcionan una experiencia de aprendizaje interactiva y práctica. Las simulaciones interactivas y los cursos en línea también recibieron menciones significativas, lo que demuestra la importancia de las modalidades de aprendizaje accesibles.

Retos a los que se enfrentan las instituciones escolares.

Preguntados por los principales retos a los que se enfrentan las instituciones escolares, he aquí un resumen de los temas más recurrentes:

- **Diversidad de conocimientos y experiencia de las personas participantes**: El personal docente se enfrentan a dificultades debido a la variedad de orígenes y niveles de experiencia de las personas participantes. Adaptar la formación a todo el grupo y garantizar que tanto las personas con nivel técnico como las que no tienen nivel técnico puedan beneficiarse de las sesiones es todo un reto.
- **Mantener actualizado el material didáctico**: La rápida evolución de las amenazas a la ciberseguridad exige actualizar continuamente el material didáctico y los métodos de enseñanza para garantizar su pertinencia.
- **Limitaciones de la formación práctica**: Existe un reto significativo a la hora de proporcionar experiencia práctica. Entre las limitaciones cabe citar la insuficiencia de instalaciones de laboratorio, la falta de capacidades de simulación en el mundo real y la dificultad de crear escenarios realistas de ciberataques para la práctica.
- **Limitaciones de recursos**: El personal docente a menudo tienen que hacer frente a recursos financieros limitados, falta de personal cualificado, materiales de estudio anticuados e insuficientes herramientas de hardware y software necesarias para una formación eficaz.
- **Compromiso y motivación de las personas estudiantes**: Mantener la atención del alumnado y motivarles para que participen activamente en su aprendizaje es difícil, sobre todo cuando hay que cubrir contenidos técnicos complejos y a veces áridos.

- **Plan de estudios y estructura educativa**: Se necesitan planes de estudios completos y multidisciplinares que abarquen todos los aspectos de la ciberseguridad. Además, la incorporación de la ciberseguridad a los planes de estudio, sobre todo en la enseñanza secundaria, sigue siendo un reto importante.
- **Acceso a herramientas y tecnologías actualizadas**: Proporcionar a las personas estudiantes acceso a las últimas herramientas y tecnologías de ciberseguridad para el aprendizaje práctico suele ser un reto, lo cual es crucial para la comprensión práctica.
- **Cuestiones lingüísticas y de localización**: Es posible que los recursos de ciberseguridad no siempre estén disponibles en la lengua materna del alumnado, lo que añade un nivel de complejidad a la formación en regiones de habla no inglesa.
- **Alineación de la industria y la educación**: Equilibrar la necesidad de enseñar los fundamentos teóricos con las habilidades prácticas que se ajustan a las necesidades de la industria es un reto. También es necesario preparar a las personas estudiantes para el mercado laboral con competencias pertinentes.
- **Capacidad y desarrollo del profesorado**: Garantizar que el personal docente tenga conocimientos actualizados y sean capaces de transmitir eficazmente conceptos complejos es crucial, pero también un reto.

Adaptación a las necesidades específicas de las PYMES

Opción de respuesta	Cuenta
Neutro	82
Alineado	67
Ligeramente desalineado	19
Altamente alineados	17
No alineado	5

La mayoría de las respuestas indican una alineación neutra, lo que sugiere que hay margen de mejora en este punto. Un número significativo de personas encuestadas calificó sus programas como alineados, mientras que muy pocos docentes creen que sus programas están muy alineados o no alineados con las necesidades de la industria. Las respuestas en el extremo inferior de la escala (No alineado y ligeramente no alineado) reflejan preocupaciones o retos a la hora de alinear completamente el contenido educativo con la naturaleza evolutiva de la ciberseguridad en la industria. Esta distribución de las respuestas muestra que el reto de garantizar una educación en ciberseguridad adaptada a las tendencias y requisitos de la industria sigue siendo relevante. Pone de relieve la relevancia del proyecto CyberAgent, cuyo objetivo es proporcionar actualizaciones continuas de los planes de estudios, asociaciones con la industria y oportunidades de formación práctica para mejorar la alineación de los programas de formación en ciberseguridad con las necesidades de la industria de la ciberseguridad.

Temas específicos para las PYMES

Tema/Habilidad	Cuenta
Ciberseguridad básica para PYMES	91
Protección de datos y privacidad para las PYMES	75
El programa no incluye temas ni competencias específicas de las PYMES	**64**
Respuesta a incidentes para PYMES	58

Evaluación y gestión de riesgos en el contexto de las PYMES	53
Elaboración de políticas de ciberseguridad para las PYMES	46

Se hace mucho hincapié en los principios básicos de la ciberseguridad y la protección de datos. Los temas mencionados con más frecuencia, Ciberseguridad básica para PYMES y Protección de datos y privacidad para PYMES, indican que los educadores dan prioridad a dotar a las PYMES de los conocimientos necesarios para proteger sus datos y comprender conceptos básicos de ciberseguridad. El número "No se incluyen en el programa temas o habilidades específicos para PYMES" es indicativo de una laguna en algunos programas de formación en ciberseguridad en lo que respecta a contenidos adaptados a las pequeñas y medianas empresas (PYMES). Destaca un área crítica de mejora en la formación en ciberseguridad, especialmente teniendo en cuenta los retos y amenazas a los que se enfrentan las PYMES.

Las PYMES suelen operar con recursos limitados y pueden no tener acceso a conocimientos especializados en ciberseguridad, lo que las hace especialmente vulnerables a las ciberamenazas. La ausencia de contenidos específicos para las PYME en los programas de formación en ciberseguridad sugiere que estos programas pueden no abordar plenamente las necesidades específicas de las PYMES, dejando potencialmente una laguna en su preparación y resistencia frente a los ciberataques. Para colmar esta laguna es necesario integrar temas y conocimientos específicamente diseñados para satisfacer las necesidades de ciberseguridad de las PYMES, como la evaluación de riesgos adaptada a las operaciones de las empresas más pequeñas, prácticas de ciberseguridad rentables y estrategias para desarrollar una política de ciberseguridad eficaz con recursos limitados.

Déficit de cualificación de los empleados de las PYMES

Habilidad/Tema	**Cuenta**
Detección de amenazas y respuesta	103
Experiencia en seguridad en la nube	87
Respuesta a incidentes y recuperación	69
Protección de datos	67
Gestión y análisis de riesgos	63
Tecnologías emergentes	58
Seguridad de la red	41
Conocimientos sobre cumplimiento y normativa	36

El análisis revela que el personal empleado carece de competencias en áreas clave, siendo la detección de amenazas y la respuesta a las mismas las más mencionadas. Esto subraya la importancia de preparar a las personas estudiantes para identificar y responder a las amenazas de ciberseguridad como una capacidad esencial en este campo. Los conocimientos sobre seguridad en la nube ocupan el segundo lugar, lo que demuestra la dependencia de las tecnologías en la nube y la necesidad de conocimientos especializados para proteger los entornos en la nube por parte del personal empleado. También se valoran la respuesta y recuperación ante incidentes, la privacidad y protección de datos y la gestión y análisis de

riesgos. En cuanto a las tecnologías emergentes, se considera que la necesidad de estar al día de los últimos avances en este campo no es un área deficitaria. Lo mismo ocurre con la seguridad de la red, que es un área fundamental que forma parte de la mayoría de los programas de formación en ciberseguridad. Esto demuestra la eficacia de la formación en este punto.

Amenazas

Amenazas	Cuenta
Ciberataques impulsados por la IA	117
Ataques de ransomware	96
Phishing e ingeniería social	87
Fallos de seguridad en la nube	82
Vulnerabilidades de IoT	75
Amenazas de Deepfake	51
Amenazas internas	25

El análisis revela un enfoque significativo en los ciberataques impulsados por IA como la amenaza de ciberseguridad emergente mencionada con más frecuencia, lo que indica una preocupación por la sofisticación y complejidad de las ciberamenazas impulsadas por inteligencia artificial. Los ataques de ransomware y el phishing y la ingeniería social también ocuparon los primeros puestos, lo que demuestra la presencia de estos vectores de ataque para las PYMES. Las brechas de seguridad en la nube y las vulnerabilidades de IoT ponen de relieve las preocupaciones relacionadas con la seguridad de los servicios en la nube y la expansión de Internet de las Cosas, lo que refleja los desafíos en la protección de ecosistemas tecnológicos diversos y distribuidos para las PYME. Las amenazas Deepfake y las amenazas Insider no se consideran grandes vectores de amenaza. Unos programas de formación que cubran los 5 temas principales pueden equipar mejor a los estudiantes y a los empleados de las pymes para hacer frente a las amenazas a las que se enfrentan.

Nuevas tendencias

Zona	Cuenta
IA y aprendizaje automático en ciberseguridad	160
Identidad digital y privacidad	96
Hacking ético y habilidades defensivas	82
Amenazas de la informática cuántica	67
Sistemas de seguridad descentralizados (por ejemplo, Blockchain)	52
Habilidades interpersonales y formación interdisciplinar	47

Hay un fuerte énfasis en la IA y el aprendizaje automático en ciberseguridad como el área mencionada con más frecuencia, lo que refleja la importancia de estas tecnologías para mejorar las medidas de ciberseguridad y la necesidad de profesionales cualificados en estas áreas. La Identidad Digital y la Privacidad es otro enfoque significativo que destaca la importancia de proteger las identidades digitales y garantizar la privacidad. La puntuación en Hacking Ético y Habilidades Defensivas indica una demanda de habilidades prácticas que permitan a los profesionales identificar vulnerabilidades y defenderse de los ataques de forma eficaz. Las Amenazas de la Computación Cuántica, los sistemas de seguridad descentralizados, como la tecnología blockchain y las Habilidades blandas y la Formación interdisciplinar no se consideraron tendencias emergentes. La distribución de las respuestas pone de manifiesto la diversidad del campo de la ciberseguridad y la importancia de preparar a profesionales con un conjunto diverso de habilidades y conocimientos para hacer frente a los retos actuales y futuros. Sin embargo, el tema de la IA ocupa el primer puesto de la lista.

Igualdad entre hombres y mujeres

Porcentaje de mujeres	Número de respuestas
Menos del 10	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
Más del 75	3

El porcentaje de mujeres en los programas de formación en ciberseguridad revela una disparidad en la diversidad de género, ya que la mayoría de las respuestas muestran una baja participación femenina. En concreto, 79 respuestas sitúan la participación femenina entre el 10% y el 25%, y 57 respuestas indican que es inferior al 10%. Se sugiere un nivel moderado de diversidad de género en algunos programas, con 43 respuestas que estiman que la tasa de participación de las mujeres se sitúa entre el 26% y el 50%. Sin embargo, los programas con un alto porcentaje de participantes femeninas son notablemente escasos, como lo demuestran sólo 8 respuestas que indican un rango del 51% al 75%, y un número mínimo de 3 respuestas que estiman más del 75%. Estos datos subrayan el reto de lograr la diversidad de género en los programas de formación en ciberseguridad, destacando una brecha sustancial en la participación femenina en la mayoría de los programas reportados.

Iniciativas de género

Respuesta	Número de respuestas
Sí	30
No	160

Los datos indican que una mayoría significativa de los encuestados, 160 en total, no emplean iniciativas o estrategias específicas para fomentar la participación de las mujeres en la formación en ciberseguridad. Sólo 30 encuestados confirmaron la aplicación de tales medidas. Esto sugiere que, si bien existe cierta concienciación y esfuerzo para aumentar la participación femenina en la formación en ciberseguridad a través de iniciativas específicas, es posible que la mayoría de los programas aún no prioricen o apliquen estrategias específicas para abordar la diversidad de género. Esta falta de iniciativas específicas podría contribuir a los bajos porcentajes de participación femenina señalados en las respuestas a la pregunta anterior.

Formación con perspectiva de género

Respuesta	Número de respuestas
Sí	47
No	44
Inseguro	72
No es relevante para mí	27

Los resultados sugieren una opinión dividida entre los encuestados sobre la disponibilidad de módulos de formación en ciberseguridad que incluyan la perspectiva de género. El grupo más numeroso, formado por 72 personas encuestadas, expresó incertidumbre ("No estoy seguro/a"), lo que indica una falta de consenso o conocimiento claros sobre la presencia de materiales que incluyan la perspectiva de género. Existe una división casi equitativa entre los que creen que hay suficientes módulos de inclusión de género (47 respuestas) y los que no (44 respuestas). Además, 27 encuestados consideraron que la pregunta no era relevante para su experiencia o contexto.

Esta división refleja el debate en curso y las diversas percepciones sobre la inclusividad de los contenidos de formación en ciberseguridad. El elevado número de respuestas inseguras pone de manifiesto una posible laguna en el conocimiento o la accesibilidad de los recursos de formación inclusiva en materia de género dentro del ecosistema de educación y formación en ciberseguridad.

Barreras contra la inclusión de género

Barrera	Cuenta
Estereotipos o normas culturales	107
Falta de concienciación sobre las oportunidades en ciberseguridad	86
Falta de tutoría o de modelos de conducta	74
Retos para la conciliación de la vida laboral y familiar	60
Percepción de prejuicios sexistas en el sector	58

Los obstáculos más importantes para la participación de las mujeres en la ciberseguridad, según la percepción de las encuestadas, son los estereotipos o las normas culturales (107 menciones) y la falta de conocimiento sobre las oportunidades en ciberseguridad (86 menciones). Estas dos barreras sugieren que las percepciones sociales y la información insuficiente sobre las trayectorias profesionales obstaculizan significativamente la entrada de las mujeres en el campo de la ciberseguridad. La falta de tutoría o de modelos de conducta y los problemas de conciliación de la vida laboral y familiar son también obstáculos importantes, que ponen de relieve la importancia de las redes de apoyo y de los entornos de trabajo flexibles para fomentar la participación de las mujeres. Además, los prejuicios de género percibidos en la industria apuntan a la necesidad de cambios culturales y sistémicos en el sector para hacerlo más acogedor y equitativo para las mujeres.

Programa específico de fomento de la diversidad y la inclusión

Respuesta	Número de respuestas
Sí	44
No	85
No estoy seguro	61

Los datos revelan que una parte significativa de las instituciones encuestadas, con 85 respuestas, no cuentan con políticas o programas específicos para promover la diversidad y la inclusión de las mujeres en la formación en ciberseguridad. Mientras tanto, 44 personas encuestadas indicaron que sus instituciones sí implementan tales iniciativas, destacando un enfoque hacia el tratamiento de la diversidad de género en el campo. Sin embargo, un número notable de personas encuestadas, 61, no están seguros de si sus instituciones cuentan con tales políticas o programas, lo que apunta a una posible falta de comunicación o sensibilización con respecto a los esfuerzos existentes en materia de diversidad e inclusión. Además, esta respuesta mixta sugiere que, aunque algunas instituciones están dando pasos hacia la inclusión en la formación en ciberseguridad, sigue existiendo una brecha sustancial, tanto en la implementación de programas de diversidad como en la concienciación de tales iniciativas entre el profesorado, el personal y las personas estudiantes.

Sugerencias de mejora

Sugerencia	Cuenta
Mayor visibilidad de las mujeres profesionales de éxito en ciberseguridad	95
Más mujeres instructoras o formadoras en ciberseguridad	89
Ofrecer becas o incentivos	81
Oportunidades de tutoría	49
Contenidos de formación que eviten los prejuicios sexistas	33
Actualizar periódicamente las políticas en favor de la inclusión	31
Casos prácticos y escenarios con perspectiva de género	24
Programas de formación a medida	21
Más sesiones de formación sólo para mujeres	18

El análisis de las respuestas, relativas a las sugerencias para hacer que la formación en ciberseguridad incluya más a las mujeres, revela un fuerte consenso sobre la importancia de varias estrategias clave. La sugerencia más respaldada, con 95 menciones, es el aumento de la visibilidad de las mujeres profesionales de éxito en ciberseguridad. Esto subraya el papel fundamental de los modelos de conducta y las figuras con aspiraciones para inspirar a las mujeres a seguir carreras en ciberseguridad. Le sigue de cerca, con 89 menciones, la petición de más instructoras o personal de formación en ciberseguridad, lo que subraya la necesidad de representación dentro de la mano de obra educativa. La oferta de becas o incentivos, con 81 menciones, se considera crucial para hacer que este campo sea más accesible económicamente y atractivo para las mujeres. Las oportunidades de tutoría, señaladas por 49 encuestados, subrayan la importancia de la orientación y el apoyo de profesionales experimentados en este campo. La necesidad de contenidos de formación que eviten los prejuicios sexistas y de políticas actualizadas periódicamente para apoyar la inclusión apuntan a la necesidad de ajustes en los planes de estudio y las políticas que reflejen y promuevan la diversidad.

Análisis de la encuesta sobre el terreno a las PYMES

Demografía:

La encuesta recibió respuestas de los países socios. Rumanía es el país con mayor número de respuestas (28), seguido de Noruega (23) y Lituania, España y Bélgica, con 21 respuestas cada uno. Finlandia y Turquía también tienen un número significativo de respuestas, con 20 cada una, y Polonia les sigue de cerca con 19 respuestas.

Sector de actividad

Sector de la empresa	Cuenta
TI	18
Educación	6
Construcción	4
Consultoría	4
Ciberseguridad	4

Los datos indican una fuerte representación del sector de TI, con 18 personas encuestadas que identifican a su empresa como perteneciente a este sector. Los sectores de la educación, la construcción, la consultoría y la ciberseguridad también cuentan con una representación notable, con un número de personas encuestadas que oscila entre 4 y 6. Más allá de los cinco primeros, hay una larga cola de sectores con menos recuentos, lo que ilustra el amplio enfoque de la encuesta en varias industrias.

Perfil de los encuestados

Cargo en la empresa	Cuenta
Director	48
Ejecutivo/Propietario	35
Técnico (Ingeniero/Desarrollador/Analista)	27
Otros	25
Coordinador/Administrador	8
Ventas/Marketing	8
Especialista/Experto	8
Empleado	8
Consultor	3
Educación/enseñanza	2
Finanzas/Contabilidad	1
Gestión de proyectos	1
RRHH	1
Total	**175**

Hay una gran variedad de títulos de trabajo con un público profesional diverso y un gran panel de puestos como "Empleado/a" y "Director/a" que indica un amplio espectro de personas encuestadas, que abarcan varios niveles dentro de las jerarquías organizativas. La ciberseguridad es una cuestión transversal que afecta a personas de diferentes funciones y responsabilidades dentro de las empresas.

Género

La distribución por sexos entre las personas encuestadas revela una mayor representación de hombres (102) en comparación con las mujeres (69), con una pequeña parte de las personas encuestadas (4) que prefieren no revelar su sexo. Esta distribución sugiere una brecha de género en el campo representado por la encuesta, lo que refleja tendencias más amplias dentro de los sectores de la ciberseguridad y la tecnología, donde a menudo se informa del predominio masculino. Sin embargo, el número significativo de mujeres encuestadas indica una participación significativa de las mujeres en el campo, lo que apunta a cambios en curso en la diversidad de género del sector. Aunque la brecha de género es evidente, la diversidad en las respuestas también apunta a un panorama de ciberseguridad que cambia gradualmente.

Distribución por sexo y país

País	Mujer	Hombre	Prefiero no decirlo
Bélgica	10	10	1
Finlandia	9	11	0
Lituania	9	12	0
Noruega	8	15	0
Polonia	8	9	2

País	Mujer	Hombre	Prefiero no decirlo
Rumanía	12	16	0
España	6	14	1
Türkiye	7	13	0

La tabla muestra la distribución por sexos en los distintos países. El número de hombres encuestados supera al de mujeres en todos los países, lo que concuerda con la distribución general por sexos comentada anteriormente. Sin embargo, la diferencia varía de un país a otro: en algunos, como Bélgica, el número de hombres y mujeres encuestados es el mismo (10 en cada caso), mientras que en Polonia la distribución entre hombres (9) y mujeres (8) es más equilibrada, con un pequeño número de personas encuestadas que prefieren no indicar su sexo (2). Países como Rumanía y Noruega tienen un mayor número de encuestados en total y mantienen una mayor proporción entre hombres y mujeres. Este desglose por sexo y país proporciona una comprensión matizada de la composición demográfica de los encuestados, destacando tanto las disparidades de género como la diversidad geográfica dentro del campo de la ciberseguridad.

Tamaño de la empresa

Tamaño de la empresa	Cuenta
Hasta 10 empleados	64
11-50	60
51-250	51

Las respuestas a la encuesta indican que entre las personas participantes hay un número significativo de pequeñas y medianas empresas. El grupo más numeroso es el de las empresas de hasta 10 personas empleadas (64 personas encuestadas), seguido de cerca por las que tienen entre 11 y 50 personas empleadas (60 personas encuestadas) y, a continuación, por las que tienen entre 51 y 250 personas empleadas (51 personas encuestadas).

El predominio de empresas pequeñas entre las personas encuestadas pone de relieve la importancia de soluciones de ciberseguridad a medida que aborden las necesidades y limitaciones específicas de las PYMES.

Nivel de conocimientos

Nivel de conocimientos sobre ciberseguridad	Cuenta
Intermedio	85
Principiante	64
Avanzado	26

Las respuestas a la encuesta indican que la mayoría de las personas encuestadas consideran que el nivel actual de conocimientos de ciberseguridad de su plantilla es "Intermedio" (85), seguidos de las que lo consideran en un nivel "Principiante" (64), y una parte más pequeña considera que su personal empleado tiene conocimiento de ciberseguridad "Avanzado" (26).

Esta distribución sugiere un importante potencial de crecimiento y desarrollo de los conocimientos de ciberseguridad en las organizaciones representadas. La mayoría de los niveles "Intermedio" y "Principiante" apunta a la necesidad de iniciativas de formación y educación continuas para elevar la base de conocimientos de ciberseguridad de estas personas empleadas. Destaca la oportunidad de programas de formación en ciberseguridad dirigidos a diferentes niveles de conocimiento, garantizando que los principiantes comprendan bien los principios básicos de la ciberseguridad.

La presencia de personal con conocimientos avanzados, aunque menos numerosos, es alentadora, ya que indica una capa fundacional de experiencia en ciberseguridad dentro de algunas organizaciones.

Nivel de conocimientos en función del tamaño de la empresa.

Tamaño de la empresa	Avanzado	Principiante	Intermedio
Hasta 10 personas empleadas	6	25	33
11-50	10	20	30
51-250	10	19	22

La tabla indica cómo se distribuyen los niveles de conocimiento en ciberseguridad (Avanzado, Principiante, Intermedio) entre los diferentes tamaños de empresa. Las pequeñas empresas (hasta 10 personas empleadas) muestran una inclinación hacia el nivel "Intermedio" de conocimientos de ciberseguridad, seguidas del "Principiante". Esto sugiere que, aunque las pequeñas empresas pueden tener algunos conocimientos de ciberseguridad, todavía hay una parte significativa en el nivel principiante, lo que indica que hay margen de mejora y la necesidad de una formación más básica. Las medianas empresas (11-50 personas empleadas) tienen una distribución equilibrada entre los niveles de conocimiento, con una ligera preferencia por el conocimiento "Intermedio". Esto podría reflejar un enfoque más estructurado de la formación en ciberseguridad en organizaciones ligeramente más grandes, pero indica igualmente la presencia tanto de necesidades de conocimientos avanzados como de formación básica. Las PYMES más grandes (51-250 personas empleadas) siguen un patrón similar al de las medianas empresas, con igual número de niveles avanzados y principiantes y un recuento ligeramente inferior de conocimientos intermedios.

En todos los tamaños de empresa, el nivel "Intermedio" de conocimientos de ciberseguridad es el más común.

Personas empleadas que se ocupan de tareas de Ciberseguridad

Número	Cuenta
1-5	88
0	22
6-10	17
21+	12
11-20	5

Rango de las personas empleadas en ciberseguridad	Cuenta
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Las tablas muestran la distribución del número de personas empleadas que realizan trabajos relacionados con la ciberseguridad en diferentes organizaciones. Ofrece una visión más clara de cómo se distribuyen las responsabilidades de ciberseguridad en los distintos rangos de número de personas empleadas. La gran mayoría de las respuestas se sitúan entre 0 y 4, lo que indica un gran número de organizaciones con equipos de ciberseguridad muy pequeños o incluso ninguno dedicado específicamente a la ciberseguridad. Hay un descenso significativo en la frecuencia a medida que nos movemos a rangos más altos, con un cierto resurgimiento en las organizaciones que tienen más de 100 personas empleadas dedicados a la ciberseguridad. Esto se explica por el hecho de que esas empresas trabajan en el ámbito de la ciberseguridad como ocupación principal.

En detalle, los datos sugieren una amplia gama en el tamaño de los equipos de ciberseguridad, siendo el tamaño más común el de una sola persona empleada, seguido de ningúna persona dedicada a la ciberseguridad, lo que indica que muchas organizaciones confían mínimamente o no confían en absoluto en personal dedicado a la ciberseguridad. La frecuencia disminuye notablemente a medida que aumenta el tamaño del equipo.

La distribución pone de manifiesto una posible brecha en la asignación de personal de ciberseguridad, en la que un número significativo de pequeñas y medianas empresas (PYMES) puede no contar con los recursos adecuados dedicados a la ciberseguridad, lo que las expone a mayores riesgos. La presencia de equipos más grandes en algunas organizaciones sugiere un reconocimiento de la importancia de la ciberseguridad en determinados sectores o empresas más grandes.

Las mujeres en la ciberseguridad

Rango de mujeres en ciberseguridad	Cuenta
0	78
1-5	57
6-10	8
11-15	4
16-20	1

Los resultados de la pregunta "¿Cuántos de estas personas empleadas son mujeres?" ponen de manifiesto una importante brecha de género en la plantilla de ciberseguridad de las PYMES. La observación más sorprendente es que la mayoría de las empresas, 78 en total, declararon no tener ninguna mujer en sus puestos de ciberseguridad. Esto indica un problema prevalente de infrarrepresentación de las mujeres en esta área crítica en todas las PYMES encuestadas. Se observa una disminución gradual del recuento a medida que aumenta el número de mujeres en puestos de ciberseguridad, con 31 empresas que tienen una mujer en dicho puesto. La presencia de unas pocas empresas con 10 o más mujeres en puestos de ciberseguridad, aunque positiva, sigue siendo una excepción y no la norma. Estos casos podrían representar organizaciones con equipos de ciberseguridad más grandes o aquellas que se han centrado específicamente en la diversidad de género dentro de su plantilla de ciberseguridad. Esto subraya la necesidad de iniciativas dirigidas a animar y apoyar a las mujeres a seguir carreras en ciberseguridad. El número significativo de empresas que no cuentan con ninguna mujer en puestos de ciberseguridad pone de relieve un área crítica de intervención para promover la diversidad de género y la inclusión dentro del sector. Superar esta brecha de género podría contribuir a una mayor diversidad de perspectivas a la hora de abordar los retos de la ciberseguridad.

Utilización de servicios externos

Respuesta	Cuenta
No	115
Sí	60

Las respuestas revelan un aspecto significativo de la forma en que las PYMES abordan la ciberseguridad. La mayoría de las empresas encuestadas, 115 de 175, indican que no contratan servicios externos para trabajos de ciberseguridad. Esto sugiere una preferencia o necesidad de gestionar internamente los esfuerzos de ciberseguridad en un amplio segmento de la población de PYMES. Varios factores podrían impulsar esta tendencia, como las limitaciones presupuestarias, la percepción de control sobre las prácticas de ciberseguridad o la creencia de que sus recursos internos existentes son suficientes para satisfacer sus necesidades de ciberseguridad. Esta situación hace que el proyecto CyberAgent sea muy pertinente para dotar al personal empleado de habilidades y conocimientos básicos.

60 empresas declararon haber contratado servicios externos para tareas de ciberseguridad. Es probable que este grupo reconozca las ventajas de la subcontratación, como acceder a conocimientos especializados, mantenerse al día de las últimas amenazas y contramedidas de ciberseguridad o complementar sus capacidades internas. La decisión de contratar servicios externos también podría reflejar la comprensión de la complejidad de las amenazas a la ciberseguridad, que pueden ser difíciles de gestionar de forma totalmente interna, especialmente para las PYMES con recursos limitados.

Esta división pone de manifiesto una divergencia en la estrategia de ciberseguridad entre las PYMES, que se equilibra entre la gestión interna y la externalización de las funciones de ciberseguridad. Subraya la importancia de un enfoque adaptado a la ciberseguridad, reconociendo que las diferentes organizaciones pueden tener necesidades, capacidades y recursos variados que influyen en sus decisiones sobre si buscar apoyo externo para los esfuerzos de ciberseguridad.

Eficacia de los programas de formación

Respuesta	Cuenta
1 (Ineficaz)	8
2	38
3	79
4	39
5 (Muy eficaz)	11

Las respuestas proporcionan información sobre las percepciones relativas a la eficacia de los programas de formación actuales a la hora de preparar a las personas estudiantes para los retos de ciberseguridad del mundo real en las PYMES. La mayoría de las personas encuestadas, con 79 recuentos, calificaron la eficacia de los programas de formación actuales con un "3", lo que indica una percepción neutra o moderada de su eficacia. Esto sugiere que, si bien existe cierto nivel de confianza en estos programas, también hay un margen de mejora significativo. Las respuestas también muestran una tendencia hacia el extremo inferior de la escala, con 38 respuestas "2", lo que indica escepticismo sobre la eficacia de estos programas de formación. En los extremos, "1" (ineficaz) recibe el menor número de respuestas (8), y "5" (muy eficaz), un poco más (11). Esto indica que muy pocas personas encuestadas consideran que los programas de formación actuales son completamente ineficaces o muy eficaces a la hora de preparar a las personas estudiantes para los retos de la ciberseguridad en las PYMES. El número equilibrado de respuestas para "4" (39 recuentos) sugiere que un segmento notable de participantes ve los programas de formación como relativamente eficaces, aunque no sin limitaciones significativas. Aunque los programas de formación actuales proporcionan cierta preparación para los retos de ciberseguridad del mundo real en las PYMES, existe una brecha entre la formación proporcionada y las necesidades de la industria. Este desfase podría deberse a varios factores, como el ritmo de evolución de las amenazas a la ciberseguridad, la aplicación práctica de las competencias o la especificidad de los retos a los que se enfrentan las PYMES.

Las 3 principales áreas de formación en ciberseguridad

Categoría	Cuenta
Detección de amenazas y respuesta	102
Gestión y análisis de riesgos	81
Respuesta a incidentes y recuperación	72
Protección de datos	68
Experiencia en seguridad en la nube	51

Seguridad de la red	46
Conocimientos sobre cumplimiento y normativa	31
Tecnologías emergentes	24

El análisis de las respuestas revela que "Detección y respuesta a amenazas" se considera el área más crucial en la formación en ciberseguridad, con 102 recuentos, lo que indica una fuerte creencia en su importancia para abordar los retos de ciberseguridad del mundo real en las PYMES. Esta área es seguida de cerca por "Gestión y análisis de riesgos" y "Respuesta a incidentes y recuperación", con 81 y 72 recuentos respectivamente, lo que subraya el valor otorgado a la comprensión de los riesgos y a la capacidad de responder a incidentes de forma eficaz. La "privacidad y protección de datos" también recibe un énfasis significativo, lo que refleja la creciente importancia de las leyes de protección de datos y la necesidad de salvaguardar la información personal y sensible en la era digital. La "experiencia en seguridad en la nube" es identificada como un área clave por 51 personas encuestadas, probablemente debido a la creciente adopción de servicios en la nube y a los retos de seguridad únicos que presentan. La seguridad de la red, con 46 recuentos, sigue siendo una preocupación fundamental, lo que subraya la necesidad de contar con defensas sólidas contra las amenazas basadas en la red. "Cumplimiento y conocimiento de la normativa" y "Tecnologías emergentes" se consideran menos importantes.

Competencias y conocimientos

Área de competencia y conocimiento	Esencial (%)	Alta necesidad (%)	Necesidad moderada (%)	Baja necesidad (%)	No es necesario (%)
Protección de datos	38.29	38.29	13.14	10.29	0.00*
Evaluación y gestión de riesgos	34.86	36.00	24.00	4.57	0.57
Respuesta a incidentes y recuperación	33.14	38.86	19.43	8.00	0.57
Habilidades de comunicación	32.57	35.43	22.29	8.00	1.71
Conocimientos técnicos	30.29	32.00	26.29	8.57	2.86
Inteligencia y vigilancia de amenazas	29.71	37.14	24.00	8.57	0.57
Elaboración y aplicación de políticas	24.00	37.14	24.00	12.57	2.29

*: El porcentaje "No es necesario" para "Privacidad y protección de datos" no está disponible (NaN), lo que podría deberse a que todos los encuestados consideran esta área al menos de cierta necesidad, por lo que puede considerarse como 0%.

La tabla presenta las puntuaciones medias de cada competencia y área de conocimiento, derivadas de las respuestas a la encuesta que califican su importancia en una escala de 1 (no necesario) a 5 (esencial). Estas puntuaciones proporcionan una visión cuantitativa de la forma en que las personas encuestadas priorizan las distintas áreas dentro del campo.

Esta tabla ofrece un desglose claro de cómo valoran la personas encuestadas cada competencia y área de conocimiento. Áreas como "Privacidad y protección de datos" y "Evaluación y gestión de riesgos" tienen el mayor porcentaje de valoraciones "Esencial", lo que refleja su importancia crítica en este campo. En cambio, "Elaboración y aplicación de políticas" muestra una distribución más amplia de respuestas, lo que indica una percepción más variada de su importancia. Los resultados ponen de relieve un fuerte énfasis en los conocimientos técnicos, la concienciación sobre las amenazas y la capacidad de responder a los incidentes, junto con la necesidad crucial de una comunicación eficaz y de prácticas de protección de datos.

Nuevas amenazas a la ciberseguridad

Amenaza emergente para la ciberseguridad	**Frecuencia**
Phishing e ingeniería social	105
Ciberataques impulsados por la IA	95
Ataques de ransomware	90
Fallos de seguridad en la nube	60
Amenazas de Deepfake	57
Vulnerabilidades de IoT	44
Amenazas internas	31

El phishing y la ingeniería social se consideran las amenazas más acuciantes, mientras que los ciberataques impulsados por la inteligencia artificial y los ataques de ransomware también reciben una atención significativa. Esto indica que las PYMES son muy conscientes de la necesidad de protegerse frente a las ciberamenazas tradicionales y emergentes. También se destacan las brechas de seguridad en la nube y las amenazas de deepfake, lo que refleja la preocupación por la seguridad de los servicios en la nube y el posible uso indebido de la inteligencia artificial. Las vulnerabilidades de IoT y las amenazas internas también se identifican, aunque se consideran menos inminentes que las otras categorías. Cabe destacar que hay respuestas que indican que algunas personas encuestadas no están seguros sobre amenazas específicas o no tienen ideas a nivel de su empresa, lo que sugiere una posible laguna en la concienciación o preocupación sobre amenazas emergentes específicas entre algunas PYMES.

Déficit de conocimientos o competencias en ciberseguridad

Déficit de conocimientos o competencias en ciberseguridad	Frecuencia
Bajo nivel de concienciación sobre amenazas	105
Bajo nivel de formación periódica sobre ciberseguridad	88
Bajo nivel de evaluación de la vulnerabilidad	80
Bajo nivel de conocimientos técnicos	71
Escasa comprensión de la política y la normativa	50
Bajo nivel de Soft Skills	37

Las lagunas más significativas en cuanto a conocimientos o habilidades de ciberseguridad entre las personas empleadas se encuentran en la concienciación sobre amenazas, la formación periódica en ciberseguridad, la evaluación de vulnerabilidades, las habilidades técnicas y la comprensión de políticas y normativas. La frecuencia de estas respuestas pone de manifiesto la necesidad crucial de una educación y formación exhaustivas en ciberseguridad que aborden estas áreas específicas. El conocimiento de las amenazas destaca como la carencia más significativa, lo que indica que las personas empleadas pueden no ser plenamente conscientes de las amenazas a la ciberseguridad que podrían afectar a su organización. Esta carencia subraya la importancia de mejorar los programas de concienciación y formación para ayudar a las personas empleadas a reconocer las amenazas potenciales con mayor eficacia. La formación periódica en ciberseguridad también se considera una carencia, lo que apunta a la necesidad de formación continua y actualizaciones sobre las últimas prácticas y amenazas de ciberseguridad, en lugar de sesiones de formación puntuales.

Nuevas tendencias

Nuevas tendencias en formación sobre ciberseguridad	Frecuencia
IA y aprendizaje automático en ciberseguridad	134
Identidad digital y privacidad	108
Hacking ético y habilidades defensivas	86
Habilidades interpersonales y formación interdisciplinar	54
Amenazas de la informática cuántica	39
Sistemas de seguridad descentralizados (por ejemplo, Blockchain)	28

El análisis revela un claro énfasis en la IA y el aprendizaje automático en ciberseguridad como la tendencia más prevista para los próximos cinco años. Esto indica un creciente reconocimiento del papel de las tecnologías avanzadas en la mejora de las defensas de ciberseguridad y el desarrollo de nuevas soluciones de seguridad. La alta frecuencia de respuestas en esta categoría sugiere que los programas de formación necesitarán incorporar cada vez más componentes de IA y aprendizaje automático para preparar a los profesionales de la ciberseguridad para el futuro. La identidad digital y la privacidad emergen como la segunda tendencia más anticipada, destacando las preocupaciones en torno a la protección de datos personales y la gestión de identidades digitales en un mundo cada vez más en línea. Esta tendencia sugiere una demanda de formación que cubra las complejidades de las leyes de privacidad, las técnicas de protección de datos y las soluciones de gestión de identidades. El hacking ético y las habilidades defensivas se identifican como la tercera tendencia clave, lo que refleja la importancia de las estrategias de defensa proactivas en ciberseguridad. El énfasis en el hacking ético muestra un cambio hacia una formación que permita a los profesionales de la ciberseguridad pensar como atacantes para defender mejor a sus organizaciones.

Adecuación de los programas de formación

Respuesta	Frecuencia
Sí	81
No estoy seguro	65
No	29

El análisis de la pregunta que exploraba las opiniones de las personas encuestadas sobre la adecuación de los actuales programas de formación en ciberseguridad, revela una perspectiva mixta entre las personas participantes. Una parte significativa, que representa la mayoría de las personas encuestadas, cree que los programas actuales de formación en ciberseguridad son adecuados, como indican las respuestas "Sí". Esto sugiere que un cierto número de personas considera que la formación disponible en la actualidad satisface las necesidades de sus organizaciones o se ajusta a sus expectativas sobre lo que debería implicar la formación en ciberseguridad. Sin embargo, un número considerable de personas encuestadas no está seguras de la idoneidad de los programas de formación actuales, lo que pone de manifiesto un grado de incertidumbre o falta de información sobre las opciones de formación disponibles o su eficacia para abordar los retos actuales de la ciberseguridad. Esta incertidumbre podría atribuirse a la naturaleza evolutiva de las ciberamenazas y a la dificultad de mantener actualizados los programas de formación con los últimos avances en este campo. Las respuestas "No", aunque representan el grupo más pequeño, indican una clara preocupación por que los programas de formación existentes no sean suficientes para satisfacer las necesidades actuales en materia de ciberseguridad. Este grupo podría percibir lagunas en la cobertura formativa de las amenazas, tecnologías o metodologías emergentes.

Inclusividad de los programas de formación

Respuesta	Frecuencia
Sí	81
No estoy seguro	65
No	29

El análisis de las respuestas indica una perspectiva diversa sobre la inclusividad de los actuales programas de formación en ciberseguridad en relación con el género. Una pluralidad de personas encuestadas considera que la formación actual es inclusiva y aborda eficazmente las necesidades de todos los géneros, como indican las respuestas "Sí". Esto sugiere que una parte significativa de la comunidad de ciberseguridad cree que los actuales esfuerzos de formación están dando pasos hacia la inclusión y la igualdad de género. Sin embargo, un gran número de personas encuestadas respondió "No estoy seguro/a" sobre la inclusividad de estos programas, lo que indica una considerable incertidumbre o falta de concienciación sobre la inclusividad de género en la formación en ciberseguridad. Esta respuesta podría poner de relieve una brecha de comunicación entre los proveedores de formación y las personas participantes o sugerir que los esfuerzos de inclusión pueden no ser tan visibles o impactantes como se pretendía. Las respuestas "No", que representan el grupo más pequeño entre las personas encuestadas, ponen

de relieve, no obstante, una preocupación fundamental por el hecho de que la formación actual en ciberseguridad no aborde suficientemente las necesidades de todos los géneros. Esta respuesta apunta a una laguna en los esfuerzos de inclusión dentro de los programas de formación en ciberseguridad, lo que sugiere que se necesita más trabajo para garantizar que estos programas sean acogedores y se adapten a las necesidades de las personas de todas las identidades de género.

2.5. PREFERENCIAS Y NECESIDADES DE FORMACIÓN

Sobre la base de los resultados de la investigación de campo, a continuación se describen las características y necesidades de formación, las preferencias de aprendizaje, la formación y el apoyo identificados de las mujeres que trabajan en el ámbito de la ciberseguridad

Identificación de las necesidades de formación:

Área 1 - Conocimientos y habilidades fundamentales

Una prioridad en la enseñanza de la ciberseguridad. Especialmente temas como los fundamentos de la ciberseguridad y la seguridad de las redes. Existen lagunas significativas en áreas como la detección y respuesta ante amenazas, conocimientos de seguridad en la nube, respuesta y recuperación ante incidentes, privacidad y protección de datos, y gestión y análisis de riesgos. Los programas de formación deben abordar estas carencias. Además, existe una gran necesidad de contenidos orientados a la ciberseguridad para las PYMES.

Área 2 - Temas especializados

Es necesaria una formación que cubra un amplio espectro de amenazas y contramedidas de ciberseguridad. Se destacaron algunos temas especializados como el análisis y la gestión de amenazas, la criptografía y las técnicas avanzadas de mitigación de amenazas. La formación debe incorporar contenidos sobre las amenazas emergentes mencionadas con más frecuencia, incluidos los ciberataques impulsados por IA, los ataques de ransomware, el phishing y la ingeniería social, las brechas de seguridad en la nube y las vulnerabilidades de IoT.

Área 3 - Aplicación práctica

La preferencia por métodos de enseñanza como laboratorios prácticos, estudios de casos y proyectos en grupo pone de relieve la importancia de la aplicación práctica, interactiva y real en la formación en ciberseguridad.

Prácticas actuales:

En cuanto al método de enseñanza, podemos observar el uso de diversas prácticas como estudios de casos, proyectos en grupo, laboratorios prácticos y conferencias. Existe una mezcla de enfoques teóricos y prácticos en los programas de formación actuales.

Los programas de formación actuales abarcan una serie de temas de ciberseguridad, dando prioridad a las materias básicas. Sin embargo, se observa una ausencia de contenidos específicos para PYMES en algunos programas.

En cuanto a la inclusión y el equilibrio de género, algunos programas han puesto en marcha iniciativas para aumentar la participación femenina y crear entornos de formación que tengan en cuenta las cuestiones de género, aunque estos esfuerzos parecen ser minoritarios.

Desafíos:

Los principales retos a los que se enfrenta la educación en ciberseguridad son:

- Adaptar la formación a las distintas formaciones y niveles de experiencia es un reto, ya que existe una gran diversidad de competencias y experiencias.
- Mantener actualizado el material del curso para hacer frente a la rápida evolución de las amenazas a la ciberseguridad. Requiere actualizaciones continuas de los materiales de formación.
- Restricciones prácticas de la formación debidas a las limitaciones de las instalaciones de laboratorio, las capacidades de simulación en el mundo real y la creación de escenarios realistas de ciberataques para la práctica.
- Mantener a las personas estudiantes comprometidas y motivadas, especialmente con contenidos técnicos complejos, es difícil.
- La alineación de la industria y la educación con el equilibrio de los fundamentos teóricos con las habilidades prácticas que se ajustan a las necesidades de la industria plantea un reto.

Sugerencia para el desarrollo de la formación:

- Adaptar la formación a las necesidades de las PYMES: integrar temas y competencias específicamente diseñados para satisfacer las necesidades de ciberseguridad de las PYMES.
- Mejorar la aplicación práctica ampliando el uso de métodos de enseñanza prácticos e interactivos para mejorar las habilidades prácticas y la preparación para el mundo real.
- Incorporar tendencias emergentes como la IA y el aprendizaje automático, la identidad digital y la privacidad, y el hacking ético. Ahora se consideran áreas clave para el futuro enfoque de los programas de formación.
- Abordar los déficits de competencias centrándose en las áreas en las que las personas empleadas tienen carencias, como la detección y respuesta ante amenazas, la seguridad en la nube y la respuesta ante incidentes, a fin de prepararlos mejor para afrontar los retos y convertirse en ciberagentes eficaces y resilientes.
- Desarrollar iniciativas de diversidad de género para aumentar la participación femenina mediante iniciativas específicas, tutoría y modelos de conducta.

3. PERFIL DE CUALIFICACIÓN DE UN AGENTE DE CAMBIO DE CIBERSEGURIDAD PARA PYMES

Sobre la base de los resultados de la investigación documental y sobre el terreno, he aquí un ejemplo del conjunto de conocimientos, habilidades y competencias esperados del Ciberagente. Estos resultados articulan los logros esperados de las personas participantes al final de sus respectivos programas de formación en ciberseguridad, garantizando un desarrollo desde conocimientos y habilidades fundacionales en el nivel 4/5 del MEC hasta unas habilidades más avanzadas y orientadas al liderazgo en el nivel 6 del MEC.

Perfil de cualificación del ciberagente	Conocimientos	Habilidades	Competencias
En el nivel 4/5 del MEC	**Fundamentos de ciberseguridad** - Conceptos básicos de ciberseguridad - Tipos de ciberamenazas (phishing, ransomware, ataques ddos), vectores de ataque - Importancia de la ciberseguridad para proteger los activos de las organizaciones. **Marco jurídico y de datos sobre ciberseguridad** - Legislación, normas y requisitos de cumplimiento en materia de ciberseguridad - Estrategias y políticas de seguridad de la información - Protección de datos - Políticas de gestión de riesgos	**Seguridad** - Identificar posibles riesgos y vulnerabilidades de ciberseguridad - Utilizar herramientas y programas informáticos de ciberseguridad para protegerse de las ciberamenazas - Promover la aplicación práctica de prácticas básicas de ciberseguridad, creación de contraseñas seguras, navegación segura, seguridad del correo electrónico y manejo seguro de datos sensibles.	**Gestión y mitigación de riesgos** - Evaluar y mitigar las posibles amenazas a la seguridad **Comunicación eficaz sobre cuestiones de ciberseguridad** - Capacidad para comunicar eficazmente sobre cuestiones de ciberseguridad, - Informar de las amenazas e infracciones a los canales apropiados dentro de la organización.

En el nivel 6 del MEC	**Conceptos avanzados de ciberseguridad** - Comprender los principios avanzados de la ciberseguridad, incluidas las ciberamenazas sofisticadas y los vectores de ataque, - Conocimiento de las últimas tendencias en amenazas a la ciberseguridad y mecanismos de defensa. **Legislación y cumplimiento en materia de ciberseguridad** - Conocimiento de la legislación, las normas y los requisitos de cumplimiento en materia de ciberseguridad nacionales e internacionales, y otros pertinentes para su sector específico.	**Evaluación y gestión avanzadas de riesgos** - Capacidad para realizar evaluaciones de riesgos exhaustivas - Utilización de metodologías y herramientas avanzadas - Diseñar y aplicar estrategias eficaces de gestión de riesgos para mitigar los riesgos identificados. **Experiencia en arquitectura de seguridad y defensa de redes** - Diseñar, implantar y evaluar arquitecturas de red seguras, incluido el uso de cortafuegos, sistemas de detección de intrusiones (id) y sistemas de prevención de intrusiones (ips). **Respuesta a incidentes y recuperación** - Capacidad de preparación, respuesta y recuperación ante incidentes de ciberseguridad, - Desarrollar planes de recuperación y continuidad de la actividad.	**Planificación y elaboración de políticas** - Capacidad para desarrollar y aplicar políticas y marcos estratégicos de ciberseguridad alineados con los objetivos de la organización y las obligaciones de cumplimiento. **Liderazgo en iniciativas de ciberseguridad** - Dirigir y gestionar proyectos y equipos de ciberseguridad, incluida la capacidad de inspirar y guiar a los empleados en la aplicación de estrategias de ciberseguridad. **Toma de decisiones** - Tomar decisiones éticas en relación con las prácticas de ciberseguridad

En el nivel 4/5 del MEC, los posibles resultados del aprendizaje podrían ser:

- El alumnado aprenderá los conceptos fundamentales de la ciberseguridad, incluida la terminología básica, los tipos de ciberamenazas como el phishing, el ransomware y los ataques DDoS, y sus respectivos vectores de ataque.
- El alumnado será capaz de identificar los posibles riesgos y vulnerabilidades en materia de ciberseguridad, utilizar las herramientas y el software pertinentes para mitigar estos riesgos y aplicar prácticas básicas de ciberseguridad, como la creación de contraseñas seguras y la navegación segura.
- El alumnado adquirirá conocimientos sobre legislación, normas y requisitos de cumplimiento en materia de ciberseguridad, junto con estrategias y políticas para la seguridad de la información y la gestión de riesgos dentro de una organización.
- El alumnado desarrollará la competencia necesaria para evaluar y mitigar eficazmente las posibles amenazas a la seguridad y comunicar los problemas de ciberseguridad de forma clara y eficaz dentro de la organización, incluida la notificación de amenazas y violaciones a los canales adecuados.

En el nivel 6 del MEC, los posibles resultados del aprendizaje podrían ser:

- El alumnado desarrollará una comprensión avanzada de los principios de ciberseguridad, incluida la capacidad de identificar ciberamenazas y vectores de ataque sofisticados y mantenerse informados sobre las últimas tendencias en defensas de ciberseguridad.
- El alumnado adquirirá un conocimiento exhaustivo de la legislación nacional e internacional sobre ciberseguridad, las normas y los requisitos de cumplimiento, adaptando este conocimiento a las necesidades específicas de su sector.
- El alumnado será capaz de llevar a cabo evaluaciones detalladas de riesgos utilizando metodologías y herramientas avanzadas, y de elaborar estrategias eficaces de gestión de riesgos para mitigarlos.
- El alumnado diseñará, implementar y evaluarán arquitecturas de red seguras, incluido el dominio del uso de tecnologías de seguridad críticas como cortafuegos, IDS e IPS.
- El alumnado será competente en la planificación y ejecución de estrategias de respuesta y recuperación ante incidentes, garantizando la resistencia de la organización mediante planes eficaces de recuperación y continuidad de la actividad.
- El alumnado demostrará su liderazgo en ciberseguridad desarrollando políticas estratégicas, gestionando proyectos y equipos de ciberseguridad y tomando decisiones informadas y éticas bajo presión.

4. APÉNDICES

4.1. APÉNDICE A: LISTA DE LA BIBLIOGRAFÍA REVISADA

Panorama de la formación en ciberseguridad en EFP e IES

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=fin
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4gNukWMvDPXICf62FqF
14. Análisis y Diagnóstico del Talento en Ciberseguridad en España, Marzo 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competencias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Retos de la ciberseguridad y necesidades del sector

1. El estado de la ciberseguridad en España, Deloitte, 2022 https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html
2. Ferreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://digital.csic.es/handle/10261/310469
3. El reto de la ciberseguridad en España: un país vulnerable, Telefónica https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 de Marzo de 2023 https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209
6. Análisis y Diagnóstico del Talento en Ciberseguridad en España, Marzo 2022, **Observaciber**, https://www.observaciber.es/
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
8. Panorama actual de la Ciberseguridad en España https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
9. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
10. **Plan de Digitalización de PYMES 2021-2025** https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
11. **https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf**

12. http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28
13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Las mujeres en la ciberseguridad

1. Microsoft (2017, marzo). Por qué las niñas europeas no estudian STEM. Microsoft News. Recuperado el 20 de enero de 2024, de https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Las mujeres se pasan a la tecnología. (2021, septiembre). La mano de obra de las TIC en Europa y su reto de género después de Covid-19. Women Go Tech. Obtenido el 20 de enero de 2024, del sitio Web: https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf.
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (s.f.) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius y Lepaite. (2022, 5 de agosto). Ataskaita Lietuvos kibernetinio saugumo kompetenciju¸ žemelapis. Universidad de Vilna. Obtenido el 20 de enero de 2024, del sitio Web: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf.
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres empleadas en ciencia y tecnología (reparto por sectores). España, UE-27 y UE-28. Serie 2019-2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. Análisis y Diagnóstico del Talento en Ciberseguridad en España, Marzo 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

4.2. APÉNDICE B: CUESTIONARIO DE LA ENCUESTA

Cuestionario sobre EFP e IES

Esta encuesta está diseñada para recopilar información sobre el estado actual y las necesidades futuras de formación en ciberseguridad y ayudar a dar forma a un programa de formación en ciberseguridad eficaz y adaptado a los retos de ciberseguridad de las pequeñas y medianas empresas (PYME).

La encuesta se divide en 4 secciones:

- Demografía
- Plan de estudios, necesidades de formación y preferencias de aprendizaje
- Requisitos de competencia y aptitudes futuras
- Perspectivas específicas de género

La encuesta dura aproximadamente 8 minutos.

DEMOGRAFÍA

¿Cuál es su país?
▫ Lituania
▫ Bélgica
▫ Noruega
▫ Türkiye
▫ Finlandia
Rumanía
▫ España
Polonia
¿En qué centro escolar enseña actualmente?
▫ EFP (Educación y Formación Profesionales)
▫ IES (institución de enseñanza superior)
¿Cuál es su sexo?
Hombre
▫ Mujer
▫ Prefiero no decirlo
¿Cuántos años lleva dedicado a la formación en ciberseguridad?
▫Menos de 1 año
1-5 años
▫ 6-10 años
▫ Más de 10 años

PLAN DE ESTUDIOS, NECESIDADES DE FORMACIÓN Y PREFERENCIAS DE APRENDIZAJE
¿Cuáles de los siguientes temas se incluyen en su programa de formación en ciberseguridad? (Seleccione todos los que procedan)
▫ Fundamentos de la ciberseguridad

▫ Análisis y gestión de amenazas
▫ Técnicas avanzadas de mitigación de amenazas
Criptografía
▫ Seguridad de la red
▫ Leyes y políticas de ciberseguridad
▫ Gestión de riesgos
▫ Respuesta a incidentes
▫ Otros: _____

¿Qué métodos de enseñanza utiliza principalmente en su formación sobre ciberseguridad? (Seleccione todos los que procedan)

▫ Conferencias
Laboratorios prácticos
▫ Estudios de casos
▫ Proyectos en grupo
▫ Simulaciones en línea
▫ Aula invertida
Otros: _____

¿Qué formatos de aprendizaje serían los más eficaces para la formación en ciberseguridad? (Seleccione todos los que procedan)

Talleres presenciales
▫ Cursos en línea
Seminarios web
▫ Simulaciones interactivas
▫ Tutoriales en vídeo
Sesiones prácticas
▫ Otros: _____

¿Cuáles son los mayores retos a los que se enfrenta a la hora de impartir una formación eficaz en ciberseguridad?

Pregunta abierta

En una escala de 1 a 5, ¿con qué eficacia cree que los programas de formación actuales preparan a las personas estudiantes para los retos reales de ciberseguridad de las PYMES?

▫ Muy ineficaz
▫ Algo ineficaz
▫ Neutral
▫ Algo eficaz
▫ Muy eficaz

¿En qué medida cree que la formación actual en ciberseguridad se ajusta a las necesidades específicas de las PYME?

1 (No alineado)
2 (Ligeramente alineado)
3 (Alineado)
4 (Bien alineado)

5 (Altamente alineado)

¿Existen temas o conocimientos específicos que incluya en su formación para abordar las necesidades específicas de las PYMES en materia de ciberseguridad? (Seleccione todo lo que corresponda)

▫ Ciberseguridad básica para PYMES
▫ Evaluación y gestión de riesgos en el contexto de las PYMES
▫ Respuesta a incidentes para PYMES
▫ Protección de datos y privacidad para las PYMES
▫ Desarrollo de políticas de ciberseguridad para PYMES
▫ Otros: _____

¿Con qué frecuencia personaliza o adapta su formación en ciberseguridad para atender mejor a las PYMES?

▫ Siempre
▫ A menudo
▫ A veces
▫ Rara vez
▫ Nunca

¿Recibe comentarios o está en contacto con representantes o profesionales de las PYMES para garantizar la pertinencia del contenido de su formación con respecto a sus necesidades?

▫ Sí, regularmente
▫ Ocasionalmente
▫ Rara vez
▫ Nunca

Según su experiencia, ¿qué grado de eficacia cree que tiene la formación actual en ciberseguridad a la hora de equipar a profesionales de las PYMES para hacer frente a los retos de la ciberseguridad?

▫ Muy ineficaz
▫ Algo ineficaz
▫ Neutral
▫ Algo eficaz
▫ Muy eficaz

¿Qué sugerencias tiene para mejorar la pertinencia y eficacia de la formación en ciberseguridad para las PYMES?

Pregunta abierta

REQUISITOS DE COMPETENCIA Y APTITUDES FUTURAS

En su opinión, ¿cuáles son los principales déficits de competencias en la mano de obra actual de las PYMES en materia de ciberseguridad? (Elija hasta tres)

▫ Detección y respuesta a las amenazas
▫ Experiencia en seguridad en la nube

▫ Conocimientos en materia de cumplimiento y normativa
▫ Respuesta a incidentes y recuperación
▫ Gestión y análisis de riesgos
▫ Privacidad y protección de datos
▫ Tecnologías emergentes
▫ Seguridad de la red

Califique, en una escala de 1 (no necesario) a 5 (muy necesario), las competencias y conocimientos necesarios:

	Clasificación				
Evaluación y gestión de riesgos Comprender los tipos de riesgos y su impacto.					
Conocimientos técnicos Aspectos técnicos de la ciberseguridad y conocimientos de sistemas operativos, redes y gestión de bases de datos.					
Respuesta a incidentes y recuperación Identificar, responder y recuperarse de brechas e incidentes de seguridad.					
Elaboración y aplicación de políticas Desarrollar y aplicar políticas y prácticas de seguridad eficaces.					
Inteligencia y vigilancia de amenazas Mantenerse al día de las últimas tendencias en ciberseguridad, amenazas y metodologías de ataque.					
Habilidades de comunicación Comunicación eficaz con el personal, la dirección y, posiblemente, los clientes sobre cuestiones de ciberseguridad.					
Protección de datos Principios de privacidad de los datos y cómo proteger la información sensible.					

¿Considera que hay algún conjunto de competencias y conocimientos relevantes que no se hayan enumerado en la pregunta anterior y que puedan ser muy necesarios para las PYMES?
Pregunta abierta
¿Para qué amenazas emergentes de ciberseguridad cree que deben estar preparadas las PYMES en los próximos 5 años? (Elija hasta tres)
▫ Ataques de ransomware
▫ Vulnerabilidades de IoT
▫ Fallos de seguridad en la nube
▫ Ciberataques impulsados por la IA
Amenazas internas
▫ Otros: _____

¿Cuáles cree que serán las 3 principales tendencias emergentes en la formación en ciberseguridad en los próximos 5 años? (Elija hasta 3 opciones)

▫ IA y aprendizaje automático en ciberseguridad
▫ Centrarse en las competencias interpersonales y la formación interdisciplinar
▫ Amenazas de la computación cuántica
▫ Hacking ético y habilidades defensivas
▫ Identidad digital y privacidad
▫ Sistemas de seguridad descentralizados (por ejemplo, Blockchain).
▫ Otros: _____

¿Hay algún método, herramienta o plataforma de formación en particular que considere excepcionalmente eficaz para la educación en ciberseguridad?

Abrir texto

¿Algún comentario o sugerencia adicional para mejorar la formación en ciberseguridad de las PYMES?

Abrir texto

PERSPECTIVAS ESPECÍFICAS DE GÉNERO

¿Cuál es el porcentaje estimado de mujeres entre las personas participantes en sus programas de formación en ciberseguridad?

Menos del 10%.
▫ 10% - 25%
▫ 26% - 50%
▫ 51% - 75%
▫ Más del 75%

¿Existen iniciativas o estrategias específicas que empleen para fomentar la participación de las mujeres en la formación sobre ciberseguridad?

▫ Sí
▫ No

En caso afirmativo, especifique: _____

¿Cree que hay suficientes módulos de formación en ciberseguridad que tengan en cuenta la perspectiva de género?

▫ Sí
▫ No
▫ No estoy seguro
▫ No es relevante para mí

Según su experiencia, ¿cuáles son los principales obstáculos que impiden a las mujeres participar o progresar en la formación y las carreras de ciberseguridad? (Seleccione todas las que procedan)

▫ Falta de concienciación sobre las oportunidades en ciberseguridad
Estereotipos o normas culturales
▫ Falta de tutoría o de modelos de conducta.

▫ Retos para la conciliación de la vida laboral y familiar
▫ Percepción de prejuicios sexistas en la industria.
▫ Otros: _____

¿Dispone su institución de políticas o programas específicos para promover la diversidad y la inclusión, en particular de las mujeres, en la formación sobre ciberseguridad?

▫ Sí
▫ No
▫ No estoy seguro

¿Qué podría hacer que la formación en ciberseguridad tuviera más en cuenta la perspectiva de género? (Elija hasta tres)

▫ Más mujeres instructoras o formadoras en ciberseguridad
▫ Ofrecer becas o incentivos.
▫ Contenidos de formación que eviten los prejuicios sexistas
▫ Mayor visibilidad de las mujeres profesionales de éxito en ciberseguridad
▫ Más sesiones de formación sólo para mujeres
▫ Casos prácticos y escenarios con perspectiva de género
▫ Programas de formación a medida
▫ Oportunidades de tutoría
▫ Otros: _____

CUESTIONARIO PYMES

El objetivo de esta encuesta es determinar las necesidades de formación de los y las agentes de cambio en ciberseguridad de las PYMES. Sus respuestas ayudarán a comprender el panorama actual de los conocimientos y competencias en materia de ciberseguridad en diversas PYMES, a identificar las lagunas en la formación sobre ciberseguridad y a mejorar la eficacia de los futuros programas de formación.

La encuesta se divide en 3 secciones:

- Demografía
- Necesidades de formación
- Inclusividad y necesidad de las mujeres en ciberseguridad.

La encuesta dura aproximadamente 5 minutos.

DEMOGRAFÍA

¿Cuál es su país?

▫ Lituania
▫ Bélgica
▫ Noruega
▫ Türkiye
▫ Finlandia
Rumanía
▫ España
Polonia

¿Cuál es su cargo y departamento actuales en la empresa?

Posición: _____
Departamento: _____

¿Cuál es su sexo?

Hombre
▫ Mujer
▫ Prefiero no decirlo

¿Cuántos personas empleadas trabajan en la empresa?

▫ hasta 10 personas empleadas
▫ 11-50
▫ 51-250

¿Cómo calificaría el nivel actual de conocimientos y competencias en ciberseguridad del personal?

▫ Principiante
▫ Intermedio
▫ Avanzado

¿Cuántas personas empleadas realizan trabajos relacionados con la ciberseguridad?

Insertar número: _____

¿Contrata servicios externos para trabajos de ciberseguridad?

▫ Sí
▫ No

NECESIDADES DE FORMACIÓN

En una escala de 1 (ineficaz) a 5 (muy eficaz), ¿con qué eficacia cree que los programas de formación actuales preparan a las personas estudiantes para los retos reales de ciberseguridad de las PYMES?

1- Ineficaz
5- Muy eficaz

En su opinión, ¿cuáles son los principales déficits de competencias en la mano de obra actual de las PYMES en materia de ciberseguridad? (Elija hasta tres)

▫ Detección y respuesta a las amenazas
▫ Experiencia en seguridad en la nube
▫ Conocimientos en materia de cumplimiento y normativa
▫ Respuesta a incidentes y recuperación
▫ Gestión y análisis de riesgos
▫ Privacidad y protección de datos
▫ Tecnologías emergentes
▫ Seguridad de la red
▫ Otros: _____

Califique, en una escala de 1 (no necesario) a 5 (esencial), las competencias y conocimientos necesarios:

	Clasificación				
Evaluación y gestión de riesgos Comprender los tipos de riesgos y su impacto.					
Conocimientos técnicos Aspectos técnicos de la ciberseguridad y conocimientos de sistemas operativos, redes y gestión de bases de datos.					
Respuesta a incidentes y recuperación Identificar, responder y recuperarse de brechas e incidentes de seguridad.					
Elaboración y aplicación de políticas Desarrollar y aplicar políticas y prácticas de seguridad eficaces.					

Inteligencia y vigilancia de amenazas Mantenerse al día de las últimas tendencias en ciberseguridad, amenazas y metodologías de ataque.					
Habilidades de comunicación Comunicación eficaz con el personal, la dirección y, posiblemente, los clientes sobre cuestiones de ciberseguridad.					
Protección de datos Principios de privacidad de los datos y cómo proteger la información sensible.					

¿Considera que hay algún conjunto de competencias y conocimientos relevantes que no se hayan enumerado en la pregunta anterior y que puedan ser muy necesarios para las PYMES?

Pregunta abierta

¿Para qué amenazas emergentes de ciberseguridad cree que deben estar preparadas las PYMES en los próximos 5 años? (Elija hasta tres)

▫ Ataques de ransomware
▫ Vulnerabilidades de IoT
▫ Fallos de seguridad en la nube
▫ Ciberataques impulsados por la IA

Amenazas internas

▫ Otros: _____

¿Qué lagunas específicas, si las hay, cree que existen en el estado actual de conocimientos o aptitudes de las personas empleadas en materia de ciberseguridad?

▫ Bajo nivel de conocimientos técnicos
▫ Bajo nivel de Soft skills
▫ Bajo nivel de evaluación de la vulnerabilidad
▫ Bajo nivel de comprensión de la política y la normativa
▫ Bajo nivel de conocimiento de las amenazas.
▫ Bajo nivel de formación periódica sobre ciberseguridad
▫ Otros: _____

¿Cuáles cree que serán las 3 principales tendencias emergentes en la formación en ciberseguridad en los próximos 5 años? (Elija hasta 3 opciones)

▫ IA y aprendizaje automático en ciberseguridad
▫ Centrarse en las competencias interpersonales y la formación interdisciplinar
▫ Amenazas de la computación cuántica
▫ Hacking ético y habilidades defensivas
▫ Identidad digital y privacidad
▫ Sistemas de seguridad descentralizados (por ejemplo, Blockchain).
▫ Otros: _____

INCLUSIÓN Y NECESIDADES DE LAS MUJERES EN CIBERSEGURIDAD

¿Considera que la formación actual en ciberseguridad es integradora y aborda eficazmente las necesidades de todos los géneros?

▫ Sí
▫ No
▫ No estoy seguro

Si se identifica como mujer, ¿se ha enfrentado a algún obstáculo o dificultad para acceder o participar en formación/estudios sobre ciberseguridad?

▫ Sí

▫ No
▫ Prefiero no decirlo
▫ En caso afirmativo, especifique: _____

¿Conoce alguna iniciativa o programa dentro de su organización que apoye o promueva específicamente la participación de las mujeres en la ciberseguridad?

▫ Sí
▫ No
▫ No estoy seguro

¿Qué tipos de apoyo o recursos animarían a más mujeres de su organización a participar en la formación sobre ciberseguridad? (preguntas abiertas)

Pregunta abierta

¿Qué mejoras o innovaciones sugeriría para aumentar la eficacia de la formación en ciberseguridad?

Pregunta abierta

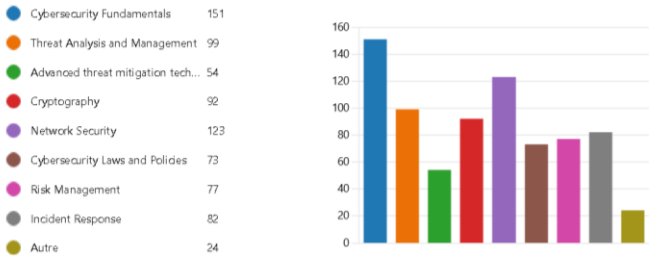
4.3. APÉNDICE C: RESULTADOS DE LA ENCUESTA

EFP E IES

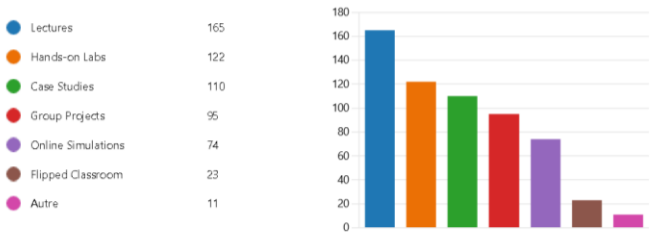
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

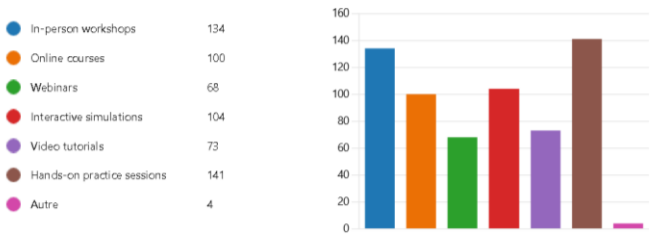
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

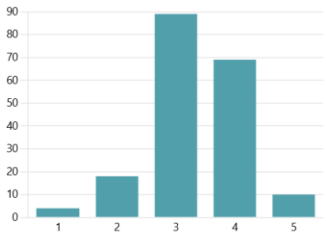
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

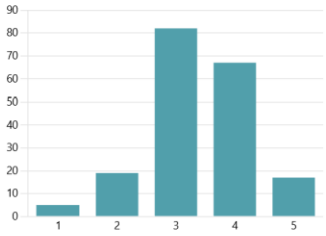
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



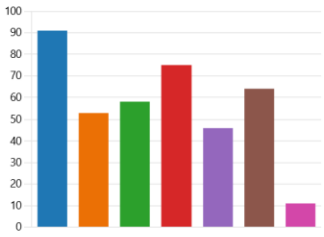
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

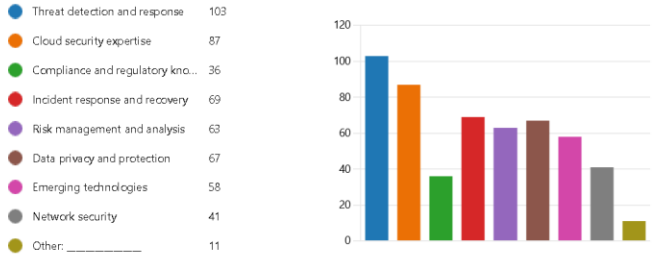
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

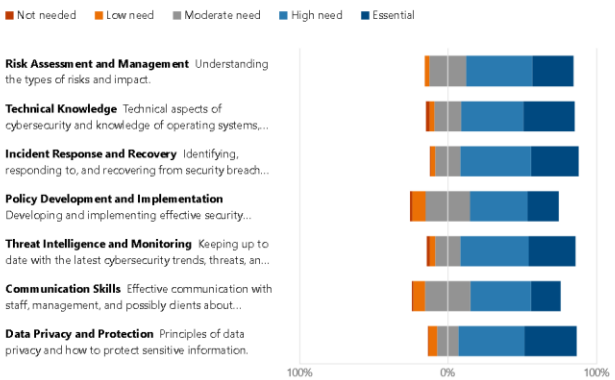
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

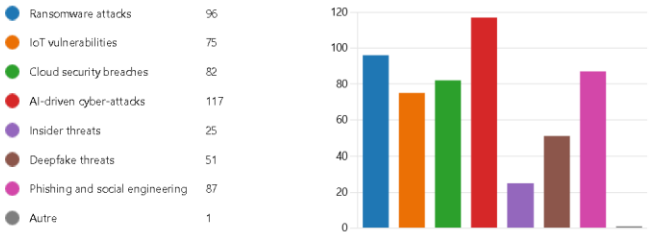
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

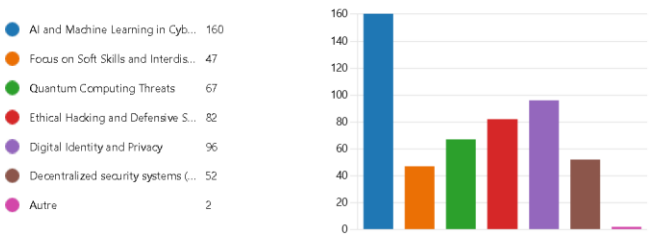
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

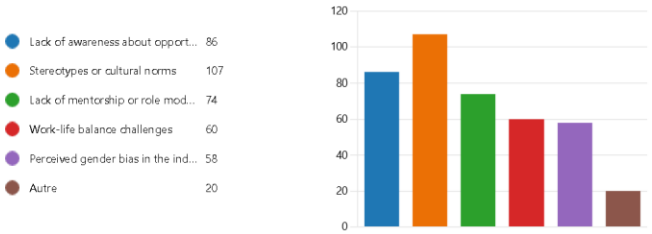
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

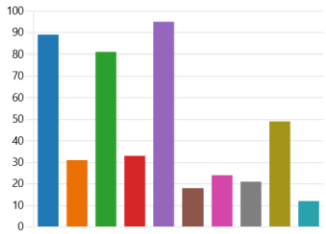
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

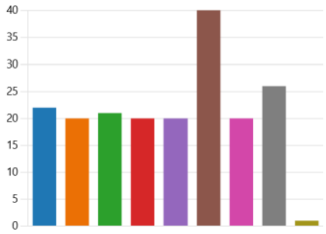
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

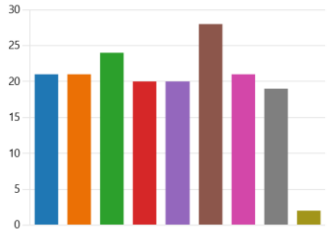
PYME

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**

Lithuania	21
Belgium	21
Norway	24
Türkiye	20
Finland	20
Romania	28
Spain	21
Poland	19
Azerbaijan	2



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

5. **How many employees are working in the company?**

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

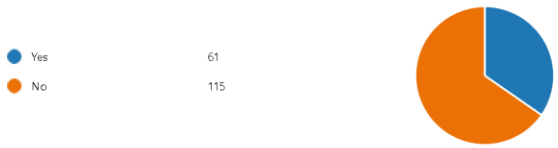
176
Réponses

Dernières réponses
"1"
"1"
"0"

Mettre à jour

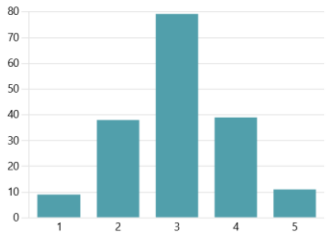
31 répondants (**18**%) répondu **1** pour cette question.

9. **Do you hire external services for cybersecurity work?**

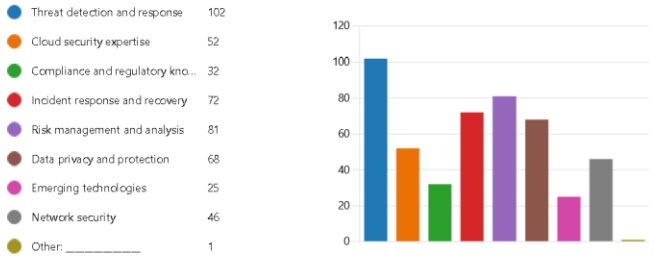


10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

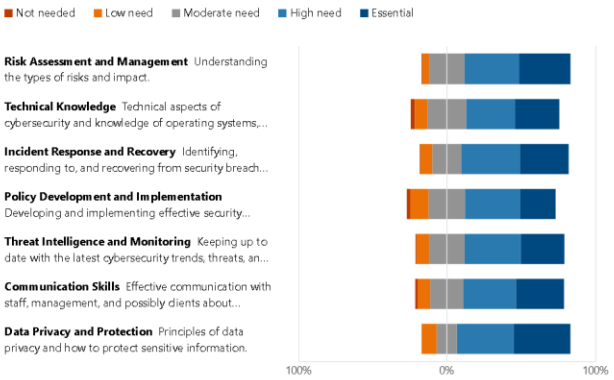
3.03
Évaluation moyenne



11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



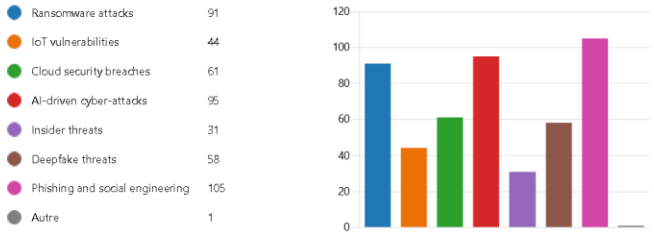
13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

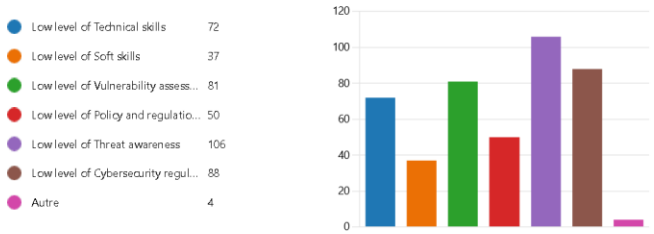
Dernières réponses
"My assumption is that Subject matter experts (SME's) in a big company are ...
"Cyber Security on all these topics arround Generative AI - which is complete...
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

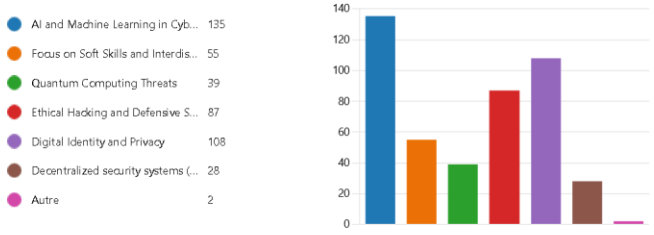
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**

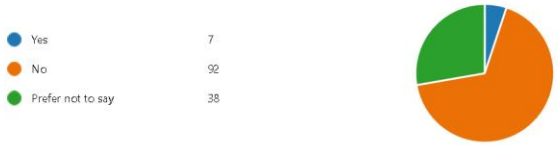


16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

4.4. APÉNDICE D: LISTA DE PROFESIONES DE ESCO EXAMINADAS

Referencias:

2529.1 **https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf**
2529.2 **https://esco.ec.europa.eu/sites/default/files/digital%2**0forensics%20expert.pdf
2529.3
https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529.5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529.6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529.7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529.9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

HackerU by ThriveDX

Olemisen Balanssia ry

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau