EUROPEAN UNION AGENCY FOR CYBERSECURITY

MANUAL DE USUARIO

MARCO EUROPEO DE COMPETENCIAS EN CIBERSEGURIDAD (ECSF)

SEPTIEMBRE 2022

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

aniversario 50 1973 - 2023

SOBRE ENISA

La Agencia de Ciberseguridad de la Unión Europea, ENISA, es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por la Ley de Ciberseguridad de la UE, la Agencia de Ciberseguridad de la Unión Europea contribuye a la ciberpolítica de la UE, mejora la fiabilidad de los productos, servicios y procesos de las TIC con sistemas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los retos cibernéticos del mañana. Mediante el intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, la Agencia colabora con sus principales interesados para reforzar la confianza en la economía conectada, aumentar la resiliencia de la infraestructura de la Unión y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos. Puede encontrar más información sobre ENISA y su trabajo aquí: www.enisa.europa.eu

CONTACTO

Para contactar con el editor, por favor use euskills@enisa.europa.eu

AGRADECIMIENTOS

Este marco es el resultado de la opinión y el acuerdo de los expertos del Grupo de trabajo ad hoc sobre el marco de competencias, compuesto por Agata BEKIER, Vladlena BENSON, Jutta BREYER, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE, Edmundas PIESARSKAS, Nineta POLEMI, Paresh RATHOD, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN y Jan HAJNY.

Fabio DI FRANCO y Athanasios GRAMMATOPOULOS dirigieron esta actividad para ENISA.

NOTA LEGAL

ENISA mantiene sus derechos de propiedad intelectual en relación con esta publicación.

NOTA SOBRE COPYRIGHT

ISBN: 978-92-9204-583-8 - DOI: 10.2824/95989

TRADUCCIÓN

Esta versión ha sido traducida del inglés al español por AMETIC.

TABLA DE CONTENIDOS

RESUMEN EJECUTIVO

La escasez de mano de obra en ciberseguridad y el déficit de cualificación es una preocupación importante tanto para la economía como para la sociedad y la para seguridad nacional. Al estudiar el problema, ENISA identificó la necesidad de Europa de un enfoque global para definir un conjunto de funciones y competencias de ciberseguridad que podrían ser para reducir la escasez y el déficit de cualificaciones. ENISA ha trabajado en el desarrollo de dicho marco y presenta el Marco Europeo de Competencias en Ciberseguridad (ECSF), que pretende reforzar la cultura europea de la ciberseguridad proporcionando una lengua europea entre las comunidades, dando un paso esencial hacia el futuro digital.

El ECSF proporciona una herramienta práctica de apoyo a la identificación y articulación de tareas, competencias, capacidades y conocimientos asociados a las funciones de la ciberseguridad europea profesionales. El objetivo principal del marco es crear un entendimiento común entre particulares, empresarios y proveedores de programas de aprendizaje en todos los Estados miembros de la UE. Estados, lo que la convierte en una valiosa herramienta para salvar la distancia entre el profesional de la ciberseguridad entornos de trabajo y aprendizaje.

El marco describe los requisitos más importantes de un profesional de la ciberseguridad lugar de trabajo mediante la definición de un conjunto de 12 perfiles de funciones típicas de los profesionales de la ciberseguridad. Los perfiles proporcionan una comprensión común de las principales misiones, tareas y competencias en materia de ciberseguridad necesarias en un contexto profesional de ciberseguridad, lo que la convierte en la referencia perfecta para perfilar las competencias y conocimientos necesarios para los profesionales de la ciberseguridad. El marco se diseñó para ser fácilmente comprensibles y lo suficientemente completos como para ofrecer una ciberseguridad adecuada en profundidad. así como lo suficientemente flexible como para permitir la personalización en función de las necesidades de cada usuario. Incorporando todas las perspectivas de las partes interesadas, el marco es aplicable a todos los tipos de y apoya el desarrollo de todas las profesiones relacionadas con la ciberseguridad.

El ECSF es el resultado del trabajo realizado por el Grupo de Trabajo ad hoc de la ENISA sobre la

Marco europeo de competencias en ciberseguridad[1] formado por expertos que representan diversos puntos de vista. Los resultados se basan en un análisis de los marcos existentes, los resultados y las conclusiones de la investigación sobre las necesidades del mercado y acuerdo entre expertos. Estudios de casos de usuarios y ejemplos, inspirados en diversos entornos laborales y de aprendizaje, demuestran la práctica aplicación de este marco y apoyar esta labor.

Se constató que las principales ventajas de utilizar el ECSF eran:

-garantizar una terminología común y un entendimiento compartido en materia de ciberseguridad por los profesionales de toda la UE;

- identificar el conjunto de competencias críticas necesarias desde la perspectiva de la ciberseguridad en mano de obra para apoyar su desarrollo y mejora;

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

- fomento de la armonización de la educación, la formación y la mano de obra en materia de ciberseguridad

Este Manual del usuario de la ECSF ofrece una visión general del ámbito de aplicación principal de la ECSF, principios marco y oportunidades de aplicación. El objetivo principal del manual es hacer que el ECSF sea fácilmente accesible, comprensible y utilizable por todas las partes interesadas con un papel activo o una necesidad de profesionales de la ciberseguridad debidamente cualificados.

El Marco Europeo de Competencias en Ciberseguridad (ECSF) pretende reforzar la ciberseguridad europea cultura por proporcionando un común Europea lenguaje a través de comunidades, tomar un paso esencial hacia adelante Europa digital futuro.

1. INTRODUCCIÓN

La escasez de competencias en ciberseguridad es uno de los principales retos que hay que afrontar para una Unión Europea cibersegura. Más concretamente, existe una falta de personal cualificado en el mercado laboral para asumir funciones en ciberseguridad y que puedan suficientemente hacer frente a la evolución de las ciberamenazas y a los nuevos retos en materia de ciberseguridad. La brecha en ciberseguridad tiene una serie de causas subyacentes. Entre ellos, un nivel insuficiente de comprensión de las competencias y aptitudes necesarias en la disciplina de la ciberseguridad entre diferentes actores en el mercado de las competencias de ciberseguridad. A lo largo de los años, esto se ha convertido en un problema bien documentado, que sigue afectando significativamente a los países a escala europea y mundial.

Con el fin de reducir la brecha y la escasez de cualificaciones actuales y futuras, es necesario aumentar la seguridad cibernética.

Se necesitan profesionales con las cualificaciones adecuadas. A tal fin, la Agenda Europea de Capacidades, el Plan de Acción sobre Educación Digital y el Pacto por las Capacidades siguen siendo vehículos importantes para movilizar a las partes interesadas para que colaboren en la consecución de los objetivos de la Década Digital creando más y mejores oportunidades de formación.

En este contexto, ENISA puso en marcha un Grupo de Trabajo ad hoc sobre la Ciberseguridad Europea un Marco de competencias en diciembre de 2020. Se reunió a un grupo multidisciplinar de expertos con el objetivo de promover la armonización de la educación, la formación y la mano de obra en materia de ciberseguridad conceptos de desarrollo. El marco desarrollado (ECSF) proporciona una herramienta europea abierta para construir una comprensión común de los perfiles de las funciones de los profesionales de la ciberseguridad y de las con las aptitudes y competencias necesarias. Este trabajo sienta las bases por aunar esfuerzos en un programa de capacitación de la mano de obra europea en ciberseguridad en en función de la demanda del mercado.

1.1. PÚBLICO DESTINATARIO

Aunque el ámbito último del contenido del marco ECSF es el núcleo de la ciberseguridad profesionales, también se hace hincapié en los grupos destinatarios del ECSF de expertos en no ciberseguridad que necesitan una visión global de la disciplina. Este enfoque hace que el marco fácil de entender para todas las partes interesadas.

Los destinatarios del ECSF son los equipos directivos de las organizaciones, los recursos humanos (RRHH) y funciones de ciberseguridad, profesionales de la ciberseguridad, recién llegados y aficionados a la ciberseguridad, como, así como proveedores de programas de aprendizaje de todo tipo en el contexto público y privado, sector asociaciones, investigadores de mercado y responsables políticos.

1.2. ESTRUCTURA DEL MANUAL

El manual del usuario está estructurado de la siguiente manera:

- El capítulo 1 presenta los principales retos que ponen de relieve la necesidad de crear un marco para las competencias en ciberseguridad, así como el público destinatario de este trabajo;

- El capítulo 2 presenta los principios de diseño del ECSF, así como las principales ventajas de su uso;

- El capítulo 3 explica las distintas aplicaciones del ECSF desde varios puntos de vista.

Además, el documento incluye dos (2) anexos que apoyan el manual del usuario del ECSF y su objetivos:

- El anexo A conecta el ECSF con otras normas y marcos de la UE.

- El Anexo B enumera los casos de uso del ECSF.

El objetivo de este anexo es conectar el ECSF con los sistemas europeos reconocidos existentes. normas y marcos pertinentes para este trabajo.

El ECSF proporciona una europeo abierto para construir una común comprensión de la ciberseguridad función profesional perfiles y común asignaciones con el apropiado habilidades y competencias necesario. Lo último alcance del Marco ECSF es la ciberseguridad núcleo profesionales, mientras que el énfasis también se coloca en no ciberseguridad expertos que necesita un completa vista de la disciplina.

2. COMPRENSIÓN DEL ECSF

El ECSF está compuesto por un conjunto representativo de 12 perfiles de funciones para la ciberseguridad profesionales (presentados en la figura 1) que suelen exigirse y aplicarse en organizaciones que despliegan profesionales de la ciberseguridad. Cada perfil está definido por una plantilla que incorpore los criterios clave establecidos (es decir, título, títulos alternativos, declaración resumida, misión, tareas principales, competencias clave, conocimientos clave, competencias electrónicas). El contenido de cada criterio se ajusta a cada función, pero puede adaptarse para permitir una aplicación flexible a responder a situaciones y necesidades específicas.

Los 12 perfiles de funciones de los profesionales de la ciberseguridad se ofrecen en un formato práctico, acordado por la UE y dedicado al ámbito profesional de la ciberseguridad. Los perfiles son fáciles de comprender y ofrecer puntos de entrada alternativos según el contexto, la perspectiva y la necesidad.

A través de estos perfiles, el ECSF puede utilizarse como herramienta común de referencia y comunicación que pueden aplicarse en diferentes organizaciones y países para una y la comprensión externa.

El ECSF introduce un representante juego de 12 rol perfiles para ciberseguridad profesionales (normalmente necesario y aplicado en organizaciones) en un acuerdo con la UE, orientado a la práctica formato dedicado a la ciberseguridad profesional dominio.

Título del perfil	Nombre del perfil de la función profesional
Título(s) alternativo(s)	Enumera los títulos alternativos típicos bajo el mismo perfil.
Resumen	Indica el objetivo principal del perfil.
Misión	Describe la razón de ser del perfil.
Entregable(s)	Una lista de resultados típicos del perfil, explicando también la relevancia del perfil desde un punto de vista no experto.
Tarea(s) principal(es)	Lista de tareas típicas realizadas por el rol perfilado.
Competencia(s) fundamental(es)	Lista de capacidades necesarias para desempeñar las funciones y obligaciones del puesto. La ética se hace explícita en algunos casos.
Conocimiento(s) fundamentales(es)	Una lista de los conocimientos esenciales necesarios para desempeñar las funciones y tareas del puesto de trabajo.
e-Competencias (EN16234-1 e-CF)	Conexión con EN16234-1 Marco de Competencia Electrónica (e-CF) - Un marco común europeo para los profesionales de las TIC de todos los sectores.

Tal como se presenta en el cuadro 1, el perfil de cada función está compuesto por un conjunto de elementos descriptivos diseñado para ofrecer una instantánea de la función en cuanto a su descripción, tareas y competencias.

Los títulos y los títulos alternativos típicos pueden utilizarse como referencia rápida para guiar a los usuarios de ECSF hacia los perfiles de funciones más adecuados para su aplicación.

Los componentes de los perfiles de funciones pueden modificarse para cubrir mejor las necesidades de las partes interesadas, y perfiles de funciones (del ECSF y de otros marcos) pueden mezclarse para la misma razón. Encontrará más información sobre la aplicación del ECSF en el capítulo 3.

Las competencias interpersonales (también llamadas transversales, transferibles o conductuales) son componentes necesarias en cualquier conjunto de competencias profesionales; por lo tanto, dichas competencias también son necesarias para los profesionales de la ciberseguridad. Una amplia gama de competencias entra dentro de las competencias interpersonales, como la capacidad de comunicarse, colaborar con los demás, informar, influir, pensar de forma crítica y gestionar el tiempo y los recursos. Las competencias interpersonales clave se incorporan al componente de competencias clave.

Por ejemplo, el perfil de la función de un Director de Seguridad de la Información (CISO) incluye como elementos clave habilidades la capacidad de influir, dirigir, comunicar, cooperar y colaborar. Todas ellas son habilidades esenciales para que un CISO cumpla sus misiones y tareas. Basándose en necesidades, podrían añadirse más habilidades blandas al perfil para un CISO o un mapeo con una habilidad blanda marco se puede hacer.

La ética es también un importante elemento transversal que afecta a todos los aspectos de la ciberseguridad y, por lo tanto, es un componente esencial de las competencias europeas en ciberseguridad. (ECSF). En el contexto de la ciberseguridad, la ética tiene que ver con qué decisiones se alinean con nuestros valores y lo que es moralmente aceptable tanto para el propietario de los datos como para la organización.

Los profesionales de la ciberseguridad podrían obtener acceso privilegiado a diversos tipos de información, incluso información sensible, la conciencia ética es un valor importante que deben tener. Aparte de eso, la toma de decisiones éticas es una habilidad importante que los profesionales de la ciberseguridad deben tener como sus decisiones afectan a otros individuos. Como en el caso de las competencias interpersonales, el ECSF analizó explícitamente si el aspecto ético del sector está en consonancia con los valores y la ética europeos.

El interesado podría realizar un análisis más detallado de las competencias blandas y éticas ya que el marco es flexible y adaptable.

2.1. LOS PRINCIPIOS DE DISEÑO DEL FSEEC

El Marco Europeo de Competencias en Ciberseguridad se basa en una serie de principios destinados a cubrir las necesidades de las partes interesadas. Esto facilita la comprensión, adopción y aplicación del manteniendo la pertinencia y el impacto a corto y largo plazo.

2.1.1. Sencillo pero completo

El marco está diseñado para ser lo suficientemente general como para garantizar su fácil comprensión y aplicada por un público más amplio. Al mismo tiempo, incluye detalles suficientes para ofrecer una visión en profundidad de la ciberseguridad. Estos atributos facilitan el uso del marco en un amplio abanico de sectores, actividades y entornos y por partes interesadas de diversos ámbitos (por ejemplo. organizaciones de distintos tamaños, conocimientos técnicos de diversa intensidad y sectores de actividad con diferentes actividades básicas).

Esto se ha logrado aplicando el nivel de detalle adecuado al contenido del ECSF que no sea ni demasiado específica ni demasiado abstracta. Al ofrecer 12 perfiles, el ECSF cubre un amplio espectro de diversas actividades laborales, pero mantiene un formato fácil de usar.

2.1.2. Flexible y ampliable

Al adoptar un enfoque modular y una estructura flexible, el marco permite a cada para que pueda ampliarse o utilizarse de forma independiente. Estas características permiten ampliación del ECSF y/o vinculación a otros marcos para ampliar sus aplicaciones.

Aplicando esta flexibilidad, los perfiles y sus componentes, definidos por el ECSF, pueden ser aplicados módulo a módulo, lo que permite adaptar cada uno de ellos a las necesidades específicas. Esta flexibilidad garantiza la pertinencia del marco a lo largo de los años y también permitirá actualizaciones del marco en el futuro.

2.1.3. Abierto e imparcial

El marco se ha desarrollado con las aportaciones de un amplio y diverso grupo de trabajo de expertos profesionales en ciberseguridad. Para desarrollar un marco imparcial, ENISA creó este grupo a partir de una serie de expertos de diversos ámbitos. El proceso de desarrollo del marco siguió un enfoque multiperspectivo que eliminaba cualquier sesgo hacia áreas de interés específicas. Además, como publicación de ENISA, el marco está disponible públicamente, es accesible y abierto.

Los perfiles y componentes del ECSF se han desarrollado sobre la base de un estudio en el que han participado múltiples partes interesadas perspectiva centrada no sólo en el punto de vista del empleo en ciberseguridad, sino también desde la perspectiva de los proveedores de programas de aprendizaje. Además, la veracidad del marco se ha mejorado con la participación y las revisiones de una serie de interesados.

2.1.4. Europa

Impulsado por la exigencia de minimizar las lagunas en las competencias de ciberseguridad y las carencias en la de la mano de obra en toda Europa, el ECSF tenía que ajustarse a las normas europeas específicas. Esta dirección se informados mediante el cumplimiento de las normas y marcos europeos existentes. El ECSF conecta bien con el actual panorama profesional europeo de las TIC para garantizar una fácil y un amplio reconocimiento. El ECSF aprovecha al máximo las experiencias existentes y proporciona vínculos coherentes con las normas profesionales pertinentes de la UE en materia de TIC. Los perfiles definidos por el marco están diseñados para ser conformes y complementarias de las leyes y reglamentos europeos y mejorar los enfoques ética identificados en el mercado europeo. El ECSF tiene en cuenta requisitos de protección de datos y privacidad establecidos por la normativa europea, trabajo común funciones solicitadas por el mercado europeo, y las normas y marcos europeos utilizados en los Sector de las TIC.

El ECSF es basado en principios diseñado para portada partes interesadas necesidades, ofreciendo fácil comprensión, adopción y aplicación mientras que mantener relevancia y impacto en la corto y a largo plazo.

2.2. PRINCIPALES VENTAJAS DEL ECSF

El ECSF es una herramienta completa y fácil de usar. Se basa en estudios de mercado recientes, la colaboración de expertos en ciberseguridad y un análisis de la situación general de la ciberseguridad y las TIC.

Expresa así las necesidades pertinentes del mercado europeo. Es compuesto por 12 funciones profesionales típicas en ciberseguridad, con una declaración resumida relacionada, misión, resultados observables (entregables), tareas, competencias, aptitudes, conocimientos y comprensión de los niveles de competencia exigidos y aplicados en el contexto del trabajo en Europa y se utiliza en toda Europa.

El ECSF proporciona una referencia inequívoca para identificar y reducir las emisiones actuales y futuras de gases de efecto invernadero. Es genérico, pero, al mismo tiempo, suficientemente detallado para dotar al mercado de la UE de una taxonomía clara de las cualificaciones, competencias y ocupaciones en la mano de obra de ciberseguridad. Además, puede conectarse fácilmente con otras estructuras existentes y marcos en ámbitos asociados.

Utilización del ECSF como lenguaje europeo común para las funciones y competencias profesionales en materia de ciberseguridad, conocimientos y competencias ofrece muchas ventajas, algunas de las cuales se enumeran a continuación.

1. El uso del ECSF garantiza una terminología común y un entendimiento compartido entre demanda (lugar de trabajo, contratación) y oferta (cualificación) de profesionales de la ciberseguridad, formación, evaluación y reconocimiento) en toda la UE.

2. El ECSF apoya la identificación de los requisitos de competencias críticas de la perspectiva de la mano de obra. Permite a los proveedores de programas de aprendizaje apoyar el desarrollo de competencias críticas y de responsables políticos que apoyen iniciativas específicas para mitigar las carencias de competencias detectadas.

3. El ECSF ayuda a comprender las funciones profesionales en materia de ciberseguridad y las competencias esenciales y la legislación pertinente. En particular, los no expertos y los departamentos de RRHH son capaces de comprender mejor los requisitos para la planificación de recursos de ciberseguridad, contratación y planificación profesional.

4. El ECSF promueve la armonización de la educación, la formación y la mano de obra en materia de ciberseguridad. desarrollo. Además, el uso de un lenguaje europeo común en ciberseguridad competencias y funciones se relaciona directamente con todo el ámbito profesional de las TIC.

5. El ECSF contribuye a lograr una mayor resistencia a los ciberataques y a garantizar sistemas TIC seguros en toda la sociedad. Proporciona una estructura estándar y ofrece

asesoramiento sobre cómo reforzar la capacitación de la mano de obra europea en ciberseguridad.

El ECSF proporciona un sin ambigüedades referencia a identificar y reducir la corriente y futuro ciberseguridad escasez de cualificaciones y lagunas.

Organizaciones:

-apoya el desarrollo de una estrategia de ciberseguridad y una estructura organizativa.

- apoya el desarrollo de la planificación de los recursos humanos de ciberseguridad

- proporciona apoyo en el proceso de contratación, en particular:

o la identificación de los requisitos de las funciones de ciberseguridad

o la evaluación de los candidatos a la ciberseguridad

- ofrece un análisis del papel de la ciberseguridad y de las carencias de competencias, con la consiguiente previsión de necesidades individuales, de equipo o de organización

- define planes de desarrollo y formación a nivel individual, de equipo o de organización

- apoya la evaluación de las funciones de ciberseguridad ayudando a crear plantillas para funciones de ciberseguridad

- proporciona un lenguaje común y de fácil comprensión para las licitaciones de ciberseguridad, contratación, vacantes y auditorías

Proveedores de programas de enseñanza:

- apoya el diseño de programas de aprendizaje y planes de estudios, el rediseño y el mantenimiento

- ofrece colaboración entre instituciones y movilidad en los programas de aprendizaje, por ejemplo, programas de aprendizaje transeuropeos de múltiples instituciones

- promueve la oferta de programas de aprendizaje y aumenta la concienciación

- posiciona los resultados del aprendizaje en un contexto laboral real

- apoya los procesos de evaluación y reconocimiento

- ofrece orientación profesional a los estudiantes

Individuos:

- Ayuda a los individuos a elegir y posicionarse en su carrera profesional.

- amplía las perspectivas de aprendizaje, abre nuevas vías de carrera y fomenta la profesionalidad.

- ayuda a comprender los requisitos prácticos del lugar de trabajo y las expectativas laborales en más detalle

- identifica vías de aprendizaje formales y no formales

- ofrece apoyo en la creación de trayectorias profesionales

Asociaciones profesionales:

- permite la consolidación de comunidades de partes interesadas para apoyar el intercambio de conocimientos, novedades, mejoras y aplicación en los Estados miembros de la UE

- presta apoyo en la realización de análisis de mercado y la presentación de los resultados en un lenguaje compartido

- ayuda a proporcionar una orientación profesional completa en el sector de la ciberseguridad

Responsables políticos y de gobierno / partes interesadas:

- apoya un entendimiento común en el ámbito de la ciberseguridad

- estimula la planificación de prioridades y la capacitación en ciberseguridad

- permite una cartografía de muchas iniciativas de ciberseguridad basada en los perfiles del ECSF

- apoya iniciativas políticas basadas en el análisis de datos

- ofrece un lenguaje común para todas las partes interesadas

- acelera la colaboración proporcionando un punto de partida de referencia común

- proporciona una referencia compartida para reunir y presentar información relacionada con los profesionales de la ciberseguridad información y necesidades a todos los niveles, nacional, europeo e internacional

3. APLICACIONES DE LA ECSF

Este capítulo demuestra cómo el Marco Europeo de Competencias en Ciberseguridad (ECSF) puede ser aplicarse de forma modular y flexible en función de las necesidades de las distintas partes interesadas.

El uso específico y la aplicación práctica dependen de muchos factores, como la perspectiva del mercado, tamaño de la organización, el contexto de una actuación concreta y el objetivo general.

Los 12 perfiles de funciones para profesionales de la ciberseguridad definidos por el ECSF son una herramienta flexible y una referencia europea estándar para un uso personalizado en un contexto particular.

1. Analizar la situación del entorno de destino.

Recopilar y procesar la información adecuada necesaria sobre la ciberseguridad relacionada con estado del entorno objetivo (por ejemplo, una organización) para crear una línea de base. Identificar las partes implicadas y el objetivo a alcanzar.

2. Determinar los objetivos específicos que deben alcanzarse.

Examinar el estado del entorno objetivo e identificar cualquier requisito específico relacionado con la ciberseguridad que deba cubrirse o cualquier objetivo que deba alcanzarse con el objetivo.

Dependiendo de la situación, puede ser posible utilizar el ECSF como una taxonomía para identificar los objetivos en cuestión.

3. Seleccione los componentes adecuados del ECSF.

Revise los perfiles ECSF y seleccione los que sean pertinentes para una situación concreta.

A continuación, seleccione los componentes que le ayuden a cubrir las necesidades o alcanzar los objetivos requeridos.

4. Adapte los componentes seleccionados en función de sus necesidades.

Realizar los cambios oportunos en los componentes seleccionados para adaptarlos mejor a una situación concreta. Mezclados, divididos o llevados a un contexto sectorial específico según las necesidades de cada situación.

5. Aplique los componentes personalizados al entorno de destino.

Adoptar medidas utilizando los componentes del ECSF adaptados para cubrir los objetivos relacionados con la seguridad necesarios para mejorar la situación del entorno objetivo y lograr el objetivo de la organización.

Los perfiles ECSF y/o sus componentes pueden ser Los 12 papeles perfiles definidos por el ECSF son una herramienta flexible y un estándar Europea referencia para uso personalizado en un determinado contexto.

Emplear profesionales de ciberseguridad en una organización:

1. Analizar el estado actual de la organización en materia de ciberseguridad.

2. Identificar la falta de personal para hacer frente al aumento de los problemas de ciberseguridad.

3. Seleccionar la tarea apropiada de un perfil ECSF que articule una

escasez o carencia de competencias específicas.

4. Adaptar Combinar los perfiles ECSF con tareas de interés para la organización y

estructurar nuevas funciones con las tareas, competencias y conocimientos actualizados para satisfacer las

necesidades cambiantes de las organizaciones y crear funciones de ciberseguridad modificadas.

5. Aplicar Utilice el perfil recién generado para crear ofertas de empleo orientadas a la

necesidades específicas de la organización.

Profesionales de ciberseguridad

1. Analizar Comprender los objetivos empresariales y la estrategia de la organización.

2. Identifique cualquier falta de experiencia y personal en áreas relacionadas con la ciberseguridad.

3. Seleccione Utilice el/los perfiles(es) ECSF para identificar las habilidades y conocimientos asociados que le falta a la organización.

4. Adaptar Analizar las competencias y conocimientos seleccionados del ECSF para identificar la formación necesidades de un profesional de la ciberseguridad para satisfacer las necesidades de la organización.

5. Aplicar Identificar las intervenciones de formación para mejorar la competencia de la plantilla de la organización.

Elaboración propia / opciones profesionales

1. Analizar Elige una carrera que te interese.

2. Identifique sus carencias y los conocimientos necesarios para pasar al sector de la ciberseguridad.

3. Seleccione Identifique el/los perfiles(es) ECSF que considere útil(s) desde el punto de vista de la carrera profesional desarrollo, y utilizar las habilidades, conocimientos y competencias relacionadas como directrices para el reciclaje y la mejora de las cualificaciones.

4. Adaptar Mejorar los perfiles ECSF seleccionados incluyendo competencias adicionales y conocimientos en función de las necesidades individuales.

5. Aplicar Identificar un programa de formación que incorpore la mayoría de las competencias y

desarrollo de los conocimientos necesarios para reorientar o mejorar las competencias para el perfil.

3.1. EMPLEAR A PROFESIONALES DE LA CIBERSEGURIDAD- APLICAR LA ECSF COMO ORGANIZACIÓN

El ECSF proporciona un conjunto de referencia estándar de 12 funciones típicas ejecutadas por la ciberseguridad profesionales desde una perspectiva organizativa, cubriendo las necesidades de ciberseguridad de las organizaciones y los procesos de ciberseguridad que deben seguirse para asegurar sus empresas, productos, servicios y sus cadenas de suministro. El marco ofrece así una valiosa guía y hoja de ruta no sólo para crear, ampliar y gestionar sistemas de ciberseguridad de una organización, sino también para garantizar su ciberseguridad. misión, visión y objetivos. Así pues, una organización puede utilizar el ECSF como punto de partida. punto o guía para acceder rápida y fácilmente a las funciones principales necesarias para gestionar sus riesgos de ciberseguridad y desarrollar su enfoque de ciberseguridad.

Al mismo tiempo, el ECSF perfiles proporcionan un entendimiento común entre las partes implicadas en relación con unas funciones de ciberseguridad de la organización.

Tres ejemplos indicativos, que se presentan más adelante en este capítulo, pretenden mostrar la aplicación práctica del marco en la:

I. mejora de las prácticas de ciberseguridad de una pequeña empresa;

II. proceso de contratación de una gran empresa con requisitos de cumplimiento cada vez más estrictos;

III. planificación de los recursos de ciberseguridad en una gran organización.

Ejemplo I: La mejora de las prácticas de ciberseguridad de una pequeña empresa presenta la aplicación de la ECSF para responder a las necesidades de una pequeña empresa que quiere mejorar su ciberseguridad. estructura y práctica.

Muestra cómo una empresa podría utilizar el ECSF para apoyar el desarrollo de una estrategia de ciberseguridad, incluida la planificación de los recursos humanos para ciberseguridad y la planificación de la adquisición de ciberseguridad.

Al utilizar el ECSF como punto de partida o como guía, la empresa no necesita inventar o investigar los roles básicos necesarios para mejorar su postura de ciberseguridad. Los roles pueden concederse a diferentes personas o pueden fusionarse para ser asumidas por una sola o pocas personas. en función de la estrategia, los requisitos, las necesidades y el presupuesto.

El ejemplo también muestra cómo el ECSF puede ayudar a la organización en el proceso de contratación.

identificando las funciones y responsabilidades de ciberseguridad que se necesitan dentro de una pequeña empresa. En este ejemplo, un análisis de las carencias de funciones y competencias en materia de ciberseguridad y la consiguiente previsión de las necesidades a nivel organizativo. Además de apoyar los procesos de recursos humanos en la contratación, el ECSF también proporciona un lenguaje común para contratación de servicios de ciberseguridad.

Ejemplo I: Mejora de las prácticas de ciberseguridad de una pequeña empresa

Una pequeña empresa de servicios en la nube alcanzó el éxito en apenas unos meses gracias a sus fundadores, hermanos Alicia y Max, pusieron en práctica su idea de una solución innovadora. Alicia era la experta y Max era un genio del marketing. Por desgracia, ninguno de los dos tenía experiencia en dirigir o crear una empresa. Al cabo de un año, la empresa empezó a despegar y así que se trasladaron a su propia oficina y contrataron personal para hacer crecer el negocio.

El ECSF puede ser utilizado como guía y hoja de ruta proporcionando un común comprender entre las partes implicadas en relación con un de la organización ciberseguridad papeles.

Fase de expansión, nadie se planteó organizar la empresa. Muchas funciones y deberes se y los retos se afrontaban de forma ad hoc. Afortunadamente, no se produjeron incidente ocurrido durante esta fase de transición.

Con el tiempo, la empresa adquirió cierta notoriedad mediática que se hizo viral, lo que se tradujo en un aumento de los ingresos interés de nuevos inversores y clientes por las pequeñas empresas de nueva creación. Sin embargo, los grandes clientes y los inversores exigían garantías y pruebas de medidas de seguridad adecuadas y una organización estructura antes de implicarse en la empresa. Los fundadores se dieron cuenta de que tendrían para dar forma realmente a las cosas dentro de su organización. Eran conscientes de que la clave del éxito de la organización eran los empleados y, para que la organización floreciera y ofreciera servicios resistentes, era esencial definir sus funciones y responsabilidades en materia de ciberseguridad.

Sin embargo, la pregunta que había que responder era qué organización era necesaria y qué

¿Qué funciones y qué tipo de competencias necesita la organización?

Los financiadores utilizaron el ECSF e identificaron que su organización necesitaba cinco funciones clave para

apoyar su línea de base de ciberseguridad:

- un responsable estratégico de ciberseguridad (CISO)
- un responsable jurídico de ciberseguridad
- arquitecto de ciberseguridad
- algunos ejecutores de ciberseguridad
- de respuesta a incidentes cibernéticos.

Al examinar internamente si sus empleados eran capaces de cubrir estas funciones, comprobaron lo siguiente que su responsable jurídico ya gestionaba el cumplimiento de la normativa legal y reglamentaria. y que tenía interés en enriquecer sus competencias en materia de privacidad y asuntos jurídicos de ciberseguridad. Los Recursos Humanos podrían apoyar la mejora de las cualificaciones utilizandouna lista de conocimientos y competencias clave obtenidos del ECSF.

El arquitecto TIC de la organización tenía experiencia previa en diseño de redes seguras y por lo que con una formación adicional para actualizar y enriquecer su competencia también podría cubrir los requisitos arquitectónicos de ciberseguridad de la organización.

Los administradores del sistema seguían muchas buenas prácticas de ciberseguridad, pero trabajaban sobre todo de forma ad hoc, sin estrategia ni estructura. En consecuencia, los fundadores identificaron una necesidad para contratar a un Responsable de Ciberseguridad Estratégica. El responsable de contratación se encargó de redactar una descripción del puesto basada en el perfil del CISO de la ECSF y publicar la vacante en su sitio web.

Por último, se estableció que las funciones de respuesta a incidentes de la empresa debían operar 24/7 para garantizar el funcionamiento continuo de los servicios.

El ejemplo I mostró lo útil que puede ser el ECSF por las siguientes ventajas:

- comprender las funciones de ciberseguridad
- determinar las necesidades de mano de obra
- evaluar los procesos y la estructura
- reciclaje y/o mejora de las cualificaciones de los empleados
- apoyar el proceso de contratación
- creación de capacidad en ciberseguridad
- crear una organización cibersegura y de confianza
- aumentar la resistencia frente a los ciberataques.

Ejemplo II: Elaboración de la descripción de un puesto de trabajo demuestra la aplicación del ECSF al crear una descripción del puesto de trabajo. Muestra cómo el ECSF puede ser beneficioso desde el punto de vista de los recursos humanos. recursos sin necesidad de conocer a fondo la profesión de la ciberseguridad. Este ejemplo muestra cómo puede crearse una oferta de empleo y cómo evitar la creación de ofertas engañosas. o expectativas confusas y cómo atraer al personal debidamente cualificado. También demuestra cómo combinar los componentes de un perfil de funciones ECSF y cómo adaptarlos en función de las necesidades laborales de una organización.

Este ejemplo muestra cómo una organización puede utilizar el ECSF para crear una descripción de un proyecto. función. Incluso sin una formación en RRHH, es posible definir las tareas, habilidades y conocimientos que se exige a un candidato a la contratación conociendo la misión del puesto. Además de proporcionar apoyo al proceso de contratación, el ECSF también puede ayudar a la empresa a definir la formación planes para el personal recién contratado. Cabe destacar que el ECSF no sólo proporciona un de ciberseguridad, sino también para fines de auditoría, especialmente cuando él Se está aplicando el principio de rendición de cuentas, y se está llevando a cabo una segregación esencial y clara de funciones.

Ejemplo II: Elaboración de la descripción de un puesto

Una gran aseguradora está ampliando su cartera a los seguros de ciberseguridad, ya que muchos clientes buscan este servicio. Tras una ligera reestructuración interna y la actualización del inventario de personal, la empresa decide añadir la ciberseguridad al departamento de cumplimiento.

En consecuencia, la dirección del departamento de cumplimiento llega a la conclusión de que necesitan contratar a un Oficial de Cumplimiento Cibernético para apoyar la nueva misión.

El departamento de RR.HH. de la empresa se encarga de encontrar y contratar a las personas más adecuadas. candidato. Dado que la ciberseguridad es un área nueva para la organización, RRHH también debe crear un papel descripción. Para definir este nuevo papel, RRHH entrevista a directivos y personal con conocimientos para identificar las necesidades y las tareas clave para este puesto. Se identifican las necesidades y las

Las tareas seleccionadas son las siguientes:

- Garantizar el cumplimiento de la normativa y ofrecer asesoramiento jurídico y orientación en materia de protección de datos. normas, leyes y reglamentos sobre protección de datos;

- identificar y documentar las lagunas en el cumplimiento;

- elaborar un plan de auditoría que describa los marcos, las normas, los procedimientos y la auditoría pruebas;

- ejecutar el plan de auditoría y recopilar pruebas y mediciones;

- elaborar y comunicar los resultados de las auditorías (informes).

El responsable de RRHH reconoce que se trata de una función compleja y que ninguna contratación plantillas que se ajusten a esta función. Por lo tanto, es necesario crear una nueva descripción de función y una nueva plantilla ser creados y aprobados por la dirección.

El responsable de RRHH, que ahora utiliza el ECSF, analiza las diferentes funciones dentro del marco. En Las funciones especificadas se incluyen en las tareas clave identificadas en las funciones de Ciberjurídico, Política & Responsable de Cumplimiento y Auditor de Ciberseguridad.

Para realizar estas tareas, las competencias identificadas y los conocimientos necesarios son los siguientes:

- Competencias

  o comprender las implicaciones de las modificaciones del marco jurídico para la

  la estrategia y las políticas de ciberseguridad y protección de datos de la organización;

  o Seguir y practicar marcos, normas y metodologías de auditoría;

  o Aplicar herramientas y técnicas de auditoría;

  Trabajar en equipo y colaborar con los compañeros.

- Conocimientos

  o conocimientos avanzados sobre ciberseguridad nacional, comunitaria e internacional y

  normas, legislación, políticas y reglamentos relacionados con la privacidad;

  o Conocimiento del cumplimiento de la seguridad de la información y de los requisitos normativos en

internacional, nacional y de la UE;

o Conocimientos básicos sobre almacenamiento, tratamiento y protección de datos.

Ahora se puede crear una nueva descripción de funciones adaptada a las necesidades de la empresa mediante la asignación y combinando partes del perfil para el puesto de Responsable Cibernético Jurídico, de Políticas y Cumplimiento y partes del perfil para la función de Auditor de Ciberseguridad. Cabe destacar que, al corresponderse con el perfil de

Esta nueva función única se basa en el contenido básico del ECSF. Esto proporciona un papel uniforme y estructurado que puede remontarse a su origen.

Tras esta correspondencia con el ECSF, la descripción de la función requerida está disponible y se puede utilizar redactar la descripción de la función y el puesto subsiguiente que RRHH necesita para obtener la aprobación interna y publicar en el sitio web de contratación de la empresa. Otros elementos, como la misión del perfil, pueden se utilizará como texto introductorio para la publicación de esta vacante.

El ejemplo II demostró lo útil que puede ser el ECSF por las siguientes ventajas:

- comprender las funciones de ciberseguridad
- determinar las necesidades de mano de obra
- identificar los requisitos de las funciones
- apoyar el proceso de contratación
- apoyar la creación de un modelo de vacante personalizado
- utilizar un lenguaje común para las vacantes.

Ejemplo III: Una gran empresa cuya actividad principal se desarrolla fuera de las TIC necesita crear un departamento de ciberseguridad demuestra la aplicación del ECSF al crear un nuevo departamento de ciberseguridad y preparar una estrategia de ciberseguridad para la empresa. También propone una categorización de los 12 perfiles en cuatro (4) macroáreas de alto nivel comprensión y comunicación. Muestra cómo una gran organización puede utilizar el ECSF para apoyar el desarrollo de una estrategia de ciberseguridad, incluida la planificación de recursos humanos y desarrollo del talento en ciberseguridad.

Ejemplo III: Una gran empresa cuya actividad principal se desarrolla fuera de las TIC necesita crear un departamento de ciberseguridad. Una gran empresa con una actividad principal no relacionada con las TIC o los servicios de ciberseguridad realizó la necesidad de proteger sus valiosos activos de las amenazas a la ciberseguridad. De hecho, la empresa adoptada estrategia incorporaba un plan masivo de digitalización de los procesos empresariales y la La dependencia de las TIC era cada vez mayor para las operaciones críticas de las empresas. Como la empresa no disponía de conocimientos internos para gestionar los riesgos de ciberseguridad, el consejo de administración decidió contratar a un Chief Security Information Officer (CISO) para definir la ciberseguridad global.en consonancia con los objetivos de la empresa. Esto también requeriría establecer un departamento para hacer frente a los riesgos de ciberseguridad.

El CISO, recién nombrado, utilizó el ECSF como directriz y como referencia sólida para la funciones de ciberseguridad necesarias para gestionar sus riesgos de ciberseguridad. Lo utilizó

como una herramienta flexible para ayudar a estructurar un departamento de ciberseguridad. También reconoció que, para proporcionar una clara

esquemático, sería útil situar las funciones del ECSF en el contexto de un círculo de gestión, bajo cuatro (4) macroáreas: a) Planificar, b) Implementar, c) Operar y d) Mejorar.

En la macrozona del Plan se fijaron prioridades y objetivos, estrategias, políticas y planes de acción desarrolladas, arquitecturas definidas, recursos asignados. En esta macroárea, el CISO, la Política y Cumplimiento, el Gestor de Riesgos y los perfiles de Arquitecto se situaron de forma natural.

Aplicación de medidas de ciberseguridad (ejecutor) y formación y sensibilización (Educador) se asignaron a la macroárea Implementar. Las Operaciones diarias fueron el área más "tangible". Respuesta a incidentes (incluidos SOC), las actividades forenses son actividades cotidianas de los especialistas en ciberseguridad. La amenaza perfil de inteligencia también se consideró un área operativa, ya que estos profesionales trabajan en datos operativos utilizando múltiples fuentes.

Probador de penetración (pruebas de amenazas actuales y emergentes), Investigador (que aporta nuevas tecnologías y soluciones) y Auditor (identificación de carencias) apoyan la fase de Mejora.Sin embargo, dado que el ECSF es una herramienta flexible para un uso personalizado en un contexto particular, el CISO aplicó la guía de 5 pasos para adaptar los perfiles de funciones a sus necesidades y objetivos específicos. El análisis de los perfiles ECSF le ayudó a definir los planes de recursos necesarios para lograr el objetivo corporativo.

En la macrozona del Plan ha decidido:

- encargarse de las tareas políticas y de cumplimiento para racionalizar la estructura de la organización;

- contratar a un arquitecto de ciberseguridad que ayude a definir la estrategia global de arquitectura Para hacer frente a los riesgos de ciberseguridad y garantizar soluciones seguras desde el diseño para apoyar la transformación digital;

- contratar a un gestor de riesgos de ciberseguridad que ayudaría a evaluar la ciberseguridad corporativa de riesgo y ayudar a definir planes de acción para gestionar los riesgos identificados.

En el macroámbito de la aplicación, aprovechó las competencias y los conocimientos del ECSF componentes para comprender qué capacitación se necesitaría para aprovechar los recursos disponibles o, alternativamente, decidir contratar externamente. La multinacional tenía un equipo existente de instructores en un campo diferente. Sin embargo, no había ningún equipo especializado para diseñar e impartir cursos de concienciación o formación en ciberseguridad. El CISO investigó si algunos de los formadores contaban con las competencias y los conocimientos enumerados en el ECSF y el interés por unirse a su nuevo equipo.

En la macroárea Operar, el CISO estudió cómo gestionar la ciberseguridad día a día. y decidieron crear centros de operaciones de seguridad mundiales con capacidad para hacer frente a incidentes. que trabajan en distintos continentes para prestar asistencia las 24 horas del día, los 7 días de la semana. Además, una amenaza Se contrató a un especialista en inteligencia para que proporcionara información operativa que guiara la caza de amenazas y la mitigación de riesgos. El CISO llegó a la conclusión de que no era necesario contratar a un experto digital. forense, sino más bien contratar a una empresa de consultoría especializada para cualquier necesidades.

En la macroárea Mejorar, el CISO decidió contratar a un proveedor de servicios externo para pruebas de penetración con el objetivo de comprobar la resistencia de la infraestructura corporativa y aplicaciones. El CISO también evaluó la capacidad del equipo de auditoría interna y decidió contratar a un auditor de ciberseguridad para auditar las políticas relacionadas con la seguridad. El CISO no consideró que la necesidad de contratar a un investigador en ciberseguridad, ya que la investigación en ciberseguridad quedaba fuera del ámbito de la su organización.

En resumen, el Ejemplo III puso de manifiesto la utilidad del ECSF por las siguientes ventajas:

- comprender las funciones de ciberseguridad
- ayudar a crear una estructura organizativa
- identificar los requisitos de las funciones de ciberseguridad
- ayudar en la planificación de los recursos humanos
- mejorar la cualificación de los empleados
- apoyar la evaluación de los candidatos
- utilizar una terminología común para la colaboración.

3.2. CAPACITAR A LOS PROFESIONALES DE LA CIBERSEGURIDAD- APLICAR EL FCEB COMO PROVEEDOR DE FORMACIÓN

El ECSF ofrece un lenguaje y un vocabulario comunes para el desarrollo de las competencias profesionales. ciberseguridad a los proveedores de programas e instituciones de aprendizaje de todo tipo, como la Educación Superior (ES), la Educación y Formación Profesionales (EFP), o cualquier otra programa educativo o formación relacionados con la ciberseguridad. Los perfiles de funciones definidos proporcionan una ciberseguridad impulsada por los centros de trabajo e integrado en Europa para vincular los requisitos actuales de práctica profesional con planes de estudios y programas de aprendizaje relacionados con la ciberseguridad.

El ECSF define los requisitos típicos de un perfil desde dos puntos de vista fundamentales.

- ¿Qué hace esta función en la organización?

  Aborda la perspectiva del lugar de trabajo (secciones de perfil sobre misión, resultados y tareas)

- ¿Qué debe saber y saber hacer esta persona?

  Abordar la perspectiva del aprendizaje (secciones del perfil sobre competencias, conocimientos y e-CF competencias)

El ECSF sitúa los resultados del aprendizaje en un contexto laboral real. En particular, las descripciones en Los perfiles de funciones del ECSF permiten a los proveedores de programas de aprendizaje revisar sus planes de estudios de forma manera estructurada y sistemática, incluso desde el punto de vista de los profesionales. Como se ilustra en el anexo B.2, la ECSF podría contribuir a varias actividades emprendidas en instituciones académicas.

- El ECSF podría servir para desarrollar o actualizar los resultados de aprendizaje de los cursos y alinear a las necesidades del mercado laboral. Las aptitudes, conocimientos y competencias de una función perfil puede utilizarse para orientar la fase de diseño de los planes de estudios y apoyar el establecimiento de los resultados de aprendizaje deseados. Por ejemplo, al analizar las necesidades educativas de un puesto específico de ciberseguridad, un perfil ECSF alineado proporciona un punto de partida sólido para comprender los requisitos educativos asociados.

- El ECSF podría servir como herramienta de colaboración para crear programas académicos conjuntos y por permitir la movilidad de los estudiantes.

- El ECSF podría servir de base para la definición de un marco para una ciberseguridad plan de estudios que ayudaría a las universidades a trazar el enfoque principal de su ciberseguridad programa y comunicarlo a los alumnos.

Como se ilustra en el anexo B.1, el ECSF aborda algunos de los retos identificados en la

Panorama europeo de las cualificaciones profesionales en ciberseguridad. En particular:

- el ECSF apoya una terminología acordada en todos los ámbitos y sectores relacionados con

competencias en ciberseguridad;

- la ECSF podría apoyar el desarrollo de una plataforma integrada de competencias para proporcionar información actualizada sobre el mercado laboral, las competencias y los cursos de formación, sistemas de certificación y una hoja de ruta profesional.

La ECSF ofrece común idioma y vocabulario para el desarrollo de profesionales ciberseguridad habilidades a los proveedores de aprender programas y aprender instituciones de todos tipos.

En el contexto del desarrollo de las cualificaciones de ciberseguridad y el diseño de planes de estudios, Los perfiles de funciones ECSF sirven como herramienta de comunicación entre empresarios y educadores para mejorar el proceso de consulta y los resultados de la colaboración. El empresario puede definir rápidamente actividades o tareas requeridas y trabajar hacia atrás para identificar las competencias, habilidades y conocimientos que los educadores deben incluir en los planes de estudios. Este enfoque acelera significativamente el diseño de planes de estudios acordados entre empresarios, gobiernos y educadores.

Los conocimientos y las competencias pueden utilizarse para definir los resultados del aprendizaje, determinar los niveles adecuados de programas de aprendizaje, y crear planes de estudios para las profesiones relacionadas con la ciberseguridad. Dado que los conocimientos y

Las competencias, al igual que todo el contenido de las descripciones de funciones, se ofrecen como ejemplos orientativos para un uso flexible de las mismas. adaptación al contexto, también pueden utilizarse otras fuentes.

Conexión de los niveles de aprendizaje (MEC) y los niveles de competencia en el lugar de trabajo (e-CF)

El Marco Europeo de Cualificaciones (MEC) es un marco común europeo de referencia

para las cualificaciones. El objetivo del MEC es comparar las cualificaciones y los resultados del aprendizaje que surgen en los distintos países y sistemas educativos nacionales. El MEC se basa en el

El ECSF puede ser utilizado como comunicación herramienta entre empresarios y educadores.

Recomendación sobre el Marco Europeo de Cualificaciones para el aprendizaje permanente adoptada por el Parlamento Europeo y el Consejo el 23 de abril de 2008.

El MEC define ocho (8) niveles de logro educativo con descriptores que diferencian cada nivel. El criterio para cada nivel se basa en la evaluación de Conocimientos, Habilidades, Responsabilidad y Autonomía.El Marco Europeo de Competencia Electrónica (e-CF), norma EN 16234-1, utilizado por el ECSF, es el siguiente un marco europeo común para las competencias, conocimientos y aptitudes profesionales en el ámbito de las TIC. se refiere a las competencias necesarias y aplicadas en el lugar de trabajo. Dimensión 3 del e-CF define los niveles de competencia que tienen su origen en el dominio del puesto de trabajo. Hay cinco (5) niveles de eCompetence definidos e-1 a e-5 relacionados con los niveles de aprendizaje EQF 3 a 8 (los niveles EQF 1 y 2 son no es pertinente en este contexto).

A continuación, se ilustra la relación entre los niveles e-1 a e-5 del e-CF con los niveles 3 - 8 del MEC:

Gracias a esta relación sistemáticamente desarrollada, es posible relacionar la competencia en e-CF con los niveles de aprendizaje del MEC. La relación, debido a la diferente naturaleza de cada marco, no es de plena equivalencia. Sin embargo, puede aplicarse para aumentar la transparencia y proporcionar un lenguaje compartido entre los requisitos de las competencias profesionales en el lugar de trabajo y las cualificaciones relacionadas de las instituciones educativas11. Así, el e-CF

Por lo tanto, los niveles de competencia incorporados en los perfiles de funciones del ECSF pueden utilizarse como un guía general de niveles educativos exigidos.

3.3. TOMAR SUS PROPIAS DECISIONES PROFESIONALES- APLICAR EL FCEP COMO UNA PROFESIONAL INDIVIDUAL

El lenguaje común definido por el ECSF puede utilizarse para aclarar cualquier confusión entre

funciones profesionales en ciberseguridad y programas educativos en ciberseguridad. Al ofrecer un lenguaje común y una descripción clara de las funciones profesionales en ciberseguridad, las tareas que se espera que lleven a cabo, así como las aptitudes, las competencias y los conocimientos necesarios, el ECSF puede construir un entendimiento compartido y proporcionarla claridad necesaria para atraer a nuevas personas al campo de la ciberseguridad o ayudarles a planificar sus trayectorias profesionales.

Los profesionales que ya trabajan en puestos relacionados con la ciberseguridad pueden utilizar el ECSF como guía para progresar en su campo. Mediante la correspondencia de sus competencias y conocimientos con los perfiles de funciones del ECSF de interés, los individuos pueden identificar cualquier habilidad o conocimiento que les falte y que necesiten desarrollar,

dominar o aprender para estar preparados para cubrir futuros requisitos laborales o posibles transiciones entre funciones de ciberseguridad mientras progresan en su carrera profesional. Esto ayuda al diálogo entre trabajadores y empresarios a la hora de planificar la formación continua en el ámbito de la ciberseguridad. Como el ECSF indica vías de aprendizaje formales y no formales, también ayuda a nuevos participantes que no saben por dónde empezar. Sumándose a los conocimientos previos y competencias suele ser un camino más fácil que empezar de cero. El anexo B.6 trata de este tema, y proporciona ideas y ejemplos más profundos en la "toma de decisiones individuales sobre la carrera profesional".

Utilizando el ECSF como punto de partida, un individuo puede identificar las competencias y habilidades necesarias para pasar de una función a otra o identificar las necesidades de formación actuales.

El lenguaje común definido por el ECSF puede ser útil para las personas que buscan empleos en ciberseguridad. El ECSF puede ayudar a filtrar las ofertas de empleo y a entender el trabajo descripción, al tiempo que puede facilitar la movilidad general del puesto dentro de la ciberseguridad al relacionar las aptitudes, conocimientos y competencias del individuo con el ECSF.

El ECSF puede construir una comprender y proporcionar la claridad necesaria para atraer a nuevos individuos en la ciberseguridad campo o asistir en la planificación su carrera caminos.

La ciberseguridad es una buena oportunidad profesional incluso para personas especializadas en otros campos. de la ciberseguridad, por lo que reciclar a las personas y trasladarlas al ámbito de la ciberseguridad es una buena manera de satisfacer las necesidades de mano de obra del mercado y reducir las carencias de mano de obra en este campo. Desde La ciberseguridad es una materia multidisciplinar, por lo que un cambio de carrera de este tipo podría ser más rápido para las personas con antecedentes cercanos a uno de los principales aspectos del campo12:

- técnica

- relacionada con la tecnología, enfoques y soluciones tecnológicas concretas

que pueden utilizarse para luchar contra la ciberdelincuencia y el ciberterrorismo;

- humanos

- relacionados con factores humanos, aspectos de comportamiento, cuestiones de privacidad, así como

sensibilizar y concienciar a la sociedad sobre la ciberdelincuencia y el terrorismo amenazas;

- organizativa: relacionada con los procesos, procedimientos y políticas de las organizaciones, así como la cooperación (público-privada, público-pública) entre organizaciones;

- normativa

- relacionada con las disposiciones de la ley, la normalización y la medicina forense.

Al tener una comprensión clara de los principales perfiles para los roles de ciberseguridad en el campo y un lenguaje común de ciberseguridad en un abanico más amplio de sectores, como el que ofrece el ECSF,

Las personas que deseen orientar su carrera hacia la ciberseguridad pueden utilizar el ECSF como punto de partida. punto para identificar las competencias y conocimientos específicos que necesitan adquirir para la transición.

Si la persona ya trabaja en ciberseguridad (y desea ampliar sus conocimientos), trabaja actualmente en otro campo (desea cambiar de profesión) o busca un puesto académico ciberseguridad en el futuro), el ECSF puede ayudar a comprender mejor los principales perfiles de las funciones de ciberseguridad (proporcionando una descripción y analizándolos en tareas, habilidades, conocimientos y competencias), así como ayudar en el análisis y la comparación de programas de aprendizaje disponibles (correspondencia entre los resultados del aprendizaje y las capacidades y conocimiento de los perfiles de ciberseguridad de preferencia).

3.4. CONSTRUIR COMUNIDADES DE CIBERSEGURIDAD- APLICAR EL FCEB COMO UNA ASOCIACIÓN PROFESIONAL

El ECSF crea una terminología común y una comprensión compartida de los perfiles de las funciones de profesionales de la ciberseguridad. Así, puede ser utilizado por las asociaciones profesionales como norma para garantizar que su trabajo pueda utilizarse y aplicarse en toda la UE, eliminando la confusión en terminología y cualquier falta de comprensión.

Las organizaciones profesionales pueden utilizar el marco para realizar análisis de mercado utilizando el ECSF y presentar los resultados en un lenguaje común. Por ejemplo, se espera que el ECSF ser útil para poner de relieve los perfiles que faltan en el mercado, los empleos de ciberseguridad que

El ECSF crea una común terminología y compartida comprensión de los perfiles de las funciones de ciberseguridad profesionales, y así puede eliminar confusión en terminología y cualquier falta de comprender

Utilizando el ECSF, se puede garantizar que y los aspectos legislativos de algunos perfiles profesionales. Además, utilizando el ECSF como terminología común, las asociaciones profesionales pueden trabajar para orientación profesional en el sector de la ciberseguridad, tal y como se presenta en el Anexo B.5.

El uso del ECSF también permite consolidar una comunidad de partes interesadas para apoyar nuevos desarrollos, mejoras y posterior aplicación en los Estados miembros de la UE. Tal de colaboración permite la interacción humana, lo que se traduce en ventajas como intercambio de conocimientos, identificación de tendencias a escala de la UE, actividades de aprendizaje entre iguales, aplicación de enfoques multidisciplinares y capacitación para adaptar y personalizar el ECSF a las necesidades específicas de cada país. requisitos.

En general, las asociaciones profesionales de ciberseguridad pueden utilizar el ECSF como herramienta para fundamentar sus actividades en garantizar su aplicabilidad en toda la UE, con el objetivo de lograr un mayor endurecimiento contra los ciberataques en toda la UE como sociedad.

3.5. CAPACITAR ESTRATÉGICAMENTE AL SECTOR- APLICAR EL FCEEC COMO RESPONSABLE POLÍTICO

Con el ECSF, una comunidad profesional crucial se asegura una visibilidad clara al utilizar el marco crea una comprensión compartida de lo que hacen los especialistas en ciberseguridad. Por lo tanto, el ECSF proporciona una herramienta para analizar y compartir recopilaciones de datos críticos relacionados con el personal de ciberseguridad y estadísticas en una terminología común y comprensible en toda la UE. Estos datos son importantes para a los responsables políticos para que conozcan mejor el estado de la mano de obra en ciberseguridad en todo el mundo.

UE, permitiéndoles así comprender y estimar las futuras necesidades de especialistas en ciberseguridad. en cantidad y calidad. Estas aportaciones estratégicas contribuyen a actualizar y mantener el propio ECSF, por lo que su pertinencia en el futuro siga siendo válida. Además, mediante la definición de una terminología común, el ECSF permite la colaboración transfronteriza entre responsables políticos a través de datos y intercambio de información.

Con un enfoque estructurado para un entorno de mercado muy diverso, los perfiles del papel de ECSF proporcionan una valiosa herramienta de apoyo a los responsables políticos, los encuestadores de mercado y otros partes interesadas con la influencia y el papel necesarios para potenciar estratégicamente el sector. Perfiles del ECSF puede ser útil para los estudios de datos sobre la oferta y la demanda realizados a escala nacional, europea e internacional. Los perfiles proporcionan una definición compartida y consensuada para facilitar la recopilación de datos fiables y comparables en el mercado laboral de la ciberseguridad, incluida la oferta y la demanda para los distintos tipos de profesionales de la ciberseguridad y los requisitos correspondientes para determinadas competencias.

Los procesos de elaboración de políticas en materia de ciberseguridad pueden beneficiarse de la recopilación de datos en el momento de la toma de decisiones, por ejemplo, disposiciones de financiación, prioridades de inversión y periodos de intervención.

Además de las actividades principales de cada perfil, las actividades que realizan pueden contribuir a generar y recopilar conjuntos de datos pertinentes que puedan respaldar las decisiones políticas. El anexo B.3 muestra cómo la fragmentación de la información constituye un reto a la hora de tomar decisiones y las acciones INCIBE está abordando este reto con el apoyo de la ECSF. Mediante la incorporación de la ECSF como marco homogéneo para la definición de perfiles de ciberseguridad, miembro de la UE los Estados obtienen un valioso apoyo para lograr sus objetivos de aumentar los talentos en ciberseguridad y alinearse con el resto de los países a nivel europeo.

Dada un estructurado enfoque de una muy diverso mercado entorno, el Función del ECSF perfiles proporcionan una herramienta valiosa por el apoyo de los responsables políticos, mercado peritos y otras partes interesadas con la influencia y papel para potenciar el sector estratégicamente.

4. TÉRMINOS Y DEFINICIONES

CIberseguridad Cualquier actividad necesaria para proteger la red y la información sistemas, los usuarios de dichos sistemas y otras personas afectados por ciberamenazas.

Mandato de ENISA

(Reglamento (UE) 2019/881)

ciberamenaza Cualquier circunstancia, evento o acción potencial que podría

dañar, interrumpir o perjudicar de cualquier otro modo la red y las

sistemas de información, los usuarios de dichos sistemas y otros

personas.

Mandato de ENISA

(Reglamento (UE) 2019/881)

Información y

Comunicación

Tecnología

TIC significa Tecnología de la Información y la Comunicación. En

se utiliza en muchos contextos diferentes y desde un punto de vista técnico

vista Las TIC se refieren a los ordenadores digitales e Internet

sistemas (de comunicación), incluidos programas informáticos, equipos y

redes. Desde un punto de vista económico y político, las TIC

se refiere a un sector transversal de empresas, entre ellas

fabricantes, proveedores de productos o proveedores de servicios relacionados

al ámbito de las TIC.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

competencia Capacidad demostrada de aplicar conocimientos, aptitudes y

actitudes para lograr resultados observables. Algunos ejemplos son B.1.

Desarrollo de aplicaciones y E.3. Gestión de riesgos.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

Competencia Capacidad para llevar a cabo actividades de gestión o técnicas y

tareas a nivel cognitivo o práctico; saber cómo hacerlo.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

aptitudes interpersonales Aptitudes interactivas que se utilizan para afrontar con éxito situaciones en

el lugar de trabajo; puede referirse a la calidad del trabajo, la interacción social o

emoción.

(también denominadas competencias transversales, transferibles o conductuales)

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

conocimiento Conjunto de hechos que deben aplicarse en un campo de trabajo o estudio; saber

qué hacer.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

actitud Representación del elemento humano de una competencia electrónica; es

reflexiona sobre el modo en que una persona integra conocimientos y habilidades y

los aplica adecuadamente en su contexto.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

resultado del aprendizaje Declaración de lo que una persona sabe, comprende y puede

realizar al finalizar un proceso de aprendizaje

Cualificaciones europeas

Marco Europeo de Cualificaciones (MEC)

perfil de la función Un esquema o documento general que demuestre la

relación entre las actividades o tareas específicas de una función y

las aptitudes, competencias y conocimientos individuales necesarios para

desempeñarlas. A diferencia de un puesto de trabajo concreto, una función se deriva de un

Liderazgo creativo -

Gestión del talento

Perfiles TIC de CWA

necesidad organizativa de hacer algo. Empleados asignados

puede cumplir los requisitos de la organización realizando todas o

parte de las tareas necesarias para garantizar su función.

perfil del puesto Descripción detallada y adaptada al contexto de lo que un

empleado hace para asegurarse de que el titular del puesto no tiene dudas

sobre sus tareas, deberes, responsabilidades y, a menudo, las de

a los que informan. Suele contener información precisa sobre

las competencias, aptitudes y conocimientos necesarios y prácticos

información sobre salud y seguridad y remuneración.

Perfiles TIC CWAnivel de competencia Indicación clara del grado de dominio que permite a un

profesional para cumplir los requisitos en el desempeño de una

competencia. EN 16234-1 (e-CF) incorpora la competencia

niveles de e-1 a e-5. El e-CF caracteriza la competencia

niveles combinando los niveles de influencia dentro de una comunidad,

complejidad del contexto y autonomía.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

nivel de aprendizaje Indica una graduación y puede estar representado por un

cualificación. Por lo general, los niveles de aprendizaje se derivan de un

sistema educativo o indicar una clasificación en una taxonomía de

comportamientos intelectuales o de aprendizaje (como memorizar,

aplicar, interpretar) y tienen relación con la competencia

niveles, sino que deben distinguirse de éstos.

EN16234-1:2019

Marco de competencias electrónicas

(e-CF)

5. REFERENCIAS

ENISA Mandate, Regulation (EU) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

European ICT Professional Role Profiles, CWA 16458 https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=17991 76DA0D15C74D91B71423CAD4A9A3

EN 16234-1:2019 e-Competence Framework (e-CF), A common European Framework for ICT Professionals in all sectors

CEN/TS 17699:2022 Guidelines for developing ICT Professional Curricula as scoped by EN 16234-1 (e-CF)

CEN/TS 17834:2022 European Professional Ethics Framework for the ICT Profession (EU ICT Ethics)

European Qualifications Framework (EQF)

ESCO The European multilingual classification of Skills, Competences and Occupations, http://www.ec.europa.eu/esco

IFIP Code of Ethics

NIST Incident Response Lifecycle

The National Initiative for Cybersecurity Education (NICE) by the National Institute of Standards and Technology in the US

National Cybersecurity Strategies (NCSSs), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

The Cybersecurity Body of Knowledge (CyBOK) by the UK National Cyber Security Programme and the University of Bristol, https://www.cybok.org

JRC, Taxonomy and glossary for Cybersecurity by European Commission, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

The European Skills Agenda, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196

Digital Education Action Plan, https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education-action-plan

Pact for Skills, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

Leading the Digital Decade, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

ENISA, Forensic Analysis, Webserver analysis, Handbook, Document for teachers, 2016, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016- resources/exe3_forensic_analysis_iii-handbook USER MANUAL SEPTEMBER 2022

33

Council of Europe, Electronic Evidence in Civil and Administrative Proceedings, Guidelines and explanatory memorandum, 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

A ANEXO:

CONEXIÓN DE LA ECSF A OTRAS NORMAS DE LA UE Y MARCOS

El ECSF es un marco de apoyo al ámbito profesional de la ciberseguridad en la UE. Conectar las estructuras europeas reconocidas existentes de interés para los profesionales de la UE. ciberseguridad era un principio vital del diseño del ECSF (véase la sección 2.1)

En los párrafos siguientes se ofrece un breve resumen de las principales normas y marcos para

a la que se conecta el ECSF.

A.1 EN16234-1 E-CF UNA REFERENCIA COMÚN EUROPEA

MARCO PARA LOS PROFESIONALES DE LAS TIC DE TODOS LOS SECTORES

La Norma Europea (EN) 16234-1 Marco Europeo de Competencia Electrónica (e-CF) proporciona un

referencia de 41 competencias aplicadas a las tecnologías de la información y la comunicación (TIC)

lugar de trabajo utilizando una lengua europea estándar para las competencias, aptitudes, conocimientos y

niveles de competencia comprensibles en toda Europa. El objetivo principal de esta norma es

proporcionar un lenguaje europeo común para las competencias y aptitudes relacionadas con las TIC en el lugar de trabajo,

los niveles de conocimiento y competencia requeridos y aplicados por las organizaciones y los profesionales. En

De este modo, todas las partes interesadas del sector, incluidos los sectores público y privado y los particulares, tienen

acceso a una referencia compartida.

La norma se estableció como herramienta para apoyar el entendimiento mutuo y proporcionar

transparencia del lenguaje mediante la articulación de las competencias requeridas y desplegadas por

Profesionales de las TIC. Esta norma está estructurada en múltiples dimensiones. Las dimensiones

reflejan áreas de planificación empresarial y de recursos humanos e incorporan el puesto y el trabajo

directrices de competencia. Además, esta norma añade un componente transversal que proporciona

descriptores TIC genéricos básicos para aplicar con éxito las competencias de e-CF en el contexto de una

lugar de trabajo.

Cuadro 4: Visión general de la norma EN16234-1 (e-CF). Fuente: CEN 2019

Dimensión 1

5 áreas e-CF

Dimensión 2

41 e-Competencias identificadas

Dimensión 3

5 niveles de competencia electrónica

e-1 e-2 e-3 e-4 e-5

A. Plan

A.1. Sistemas de información y estrategia empresarial

Alineación

A.2. Gestión del nivel de servicio

A.3. Desarrollo del plan de negocio

A.4. Planificación de productos/servicios

A.5. Diseño arquitectónico

A.6. Diseño de la aplicación

A.7. Vigilancia de las tendencias tecnológicas

A.8. Gestión de la sostenibilidad

MANUAL DEL USUARIO

SEPTIEMBRE 2022

35

A.9. Innovar

A.10. Experiencia del usuario

B. Construir

B.1. Desarrollo de aplicaciones

B.2. Integración de componentes

B.3. Pruebas

B.4. Despliegue de la solución

B.5. Producción de documentación

B.6. Ingeniería de sistemas TIC

C. Ejecutar

C.1. Apoyo al usuario

C.2. Apoyo al cambio

C.3. Prestación de servicios

C.4. Gestión de problemas

C.5. Gestión de sistemas

E. Activar

D.1. Desarrollo de la estrategia de seguridad de la información

D.2. Desarrollo de la estrategia de calidad de las TIC

D.3. Educación y formación

D.4. Compras

D.5. Desarrollo de las ventas

D.6. Marketing digital

D.7. Ciencia y análisis de datos

D.8. Gestión de contratos

D.9. Desarrollo del personal

D.10. Gestión de la información y el conocimiento

D.11. Identificación de necesidades

E. Gestione

E.1. Evolución de las previsiones

E.2. Gestión de proyectos y carteras

E.3. E.3. Gestión de riesgos

E.4. Gestión de las relaciones

E.5. Mejora de los procesos

E.6. Gestión de la calidad de las TIC

E.7. Gestión del cambio empresarial

E.8. Gestión de la seguridad de la información

E.9. Gobernanza de los sistemas de información

El e-CF proporciona vínculos coherentes en el contexto de las cualificaciones en TIC y otros marcos de

relevancia para el sector (en particular, MEC, DigComp, Perfiles europeos de funciones profesionales de las TIC,

competencias conductuales, ESCO, EQANIE, SFIA, Conocimientos Fundamentales para las TIC

profesión, ISO y otras normas del sector de las TIC).

Para cada función de ciberseguridad, se seleccionó un conjunto de competencias e-CF aplicables en el

nivel de aplicación como elemento incorporado a la descripción del perfil para la función de

profesional de la ciberseguridad.

A.2 PERFILES PROFESIONALES DE LAS TIC EN EUROPA

El CWA 16458 European ICT Professional Role Profiles ofrece un conjunto genérico de funciones típicas

que realizan los profesionales de las TIC en cualquier organización y que abarcan todo el proceso empresarial de las TIC.

Treinta perfiles en total ofrecen un buen punto de partida e inspiración para la creación de más

perfiles flexibles y específicos para cada contexto, basados en las funciones de la organización y en las descripciones de los puestos de trabajo individuales

o especializaciones en subdominios de diversos contextos. Aplicando las competencias de e-CF al

construcción de perfiles de TIC, los perfiles europeos de funciones profesionales de TIC también proporcionan una herramienta y

punto de entrada para la aplicación del e-CF a particulares y organizaciones que deseen trabajar con el e-CF.

MANUAL DEL USUARIO

SEPTIEMBRE 2022

36

Los perfiles profesionales europeos de las TIC se describen utilizando un formato coherente

que incorpore los siguientes elementos: una declaración de síntesis, una declaración de misión, entregables,

principales tareas, e-Competencias y áreas de Indicadores Clave de Rendimiento (KPI)13

.

Adoptando los elementos más adecuados del perfil europeo de las TIC acordado e impulsado por la práctica.

de descripción, los perfiles ECSF son comparables y proporcionan una información única y sencilla.

visión accesible y completa de los requisitos de la ciberseguridad europea

profesionales.

Estos perfiles detallados de alto contenido tienen vínculos poco precisos con las funciones genéricas incorporadas en el

conjunto de perfiles profesionales europeos de las TIC. Desde la perspectiva del usuario de ECSF, la confianza puede

en la sostenibilidad de la estructura a través de su asociación con las TIC europeas

Perfiles, pero con una aplicación centrada en la comunidad de la ciberseguridad.

A.3 MARCO EUROPEO DE CUALIFICACIONES

La UE desarrolló el Marco Europeo de Cualificaciones (MEC) como herramienta de traducción para

facilitar la comprensión y la comparabilidad de las cualificaciones nacionales. El MEC pretende

Apoyar la movilidad transfronteriza de estudiantes y trabajadores, y fomentar el aprendizaje permanente y la movilidad.

desarrollo profesional en toda Europa.

El MEC es un marco de 8 niveles basado en los resultados del aprendizaje14 para todo tipo de cualificaciones. Se puede consultar en

sirve de herramienta de traducción entre los distintos marcos de cualificaciones nacionales. Este

el marco contribuye a mejorar la transparencia, comparabilidad y transferibilidad de las cualificaciones de las personas

y permite comparar cualificaciones de distintos países e instituciones.

El MEC abarca todos los tipos y niveles de cualificaciones y el uso de los resultados del aprendizaje

deja claro lo que una persona sabe, comprende y es capaz de hacer. El nivel aumenta

según el nivel de aprendizaje, siendo el nivel 1 el más bajo y el 8 el más alto. La mayoría

Y lo que es más importante, el MEC está estrechamente vinculado a los marcos nacionales de cualificación15 , por lo que proporciona una

mapa exhaustivo de todos los tipos y niveles de cualificaciones en Europa, que son cada vez más

accesible a través de bases de datos de cualificaciones. El MEC se creó en 2008 y posteriormente se revisó en

201716

.

Los perfiles ECSF contienen competencias y asignaciones de nivel de e-CF, que proporcionan un

relación coherente con los niveles del MEC (véase la sección 3.2). Esta relación orientativa proporciona un puente en

comprensión entre la oferta de programas de aprendizaje y las necesidades del lugar de trabajo.

A.4 ESCO - CLASIFICACIÓN EUROPEA DE CAPACIDADES Y COMPETENCIAS

Y OCUPACIONES

ESCO es la clasificación multilingüe de capacidades, competencias, cualificaciones y competencias europeas.

ocupaciones. El objetivo clave de ESCO es proporcionar un diccionario que describa, identifique y

clasificar las ocupaciones y competencias profesionales pertinentes para el mercado laboral de la UE, la educación y la

formación y mostrando sistemáticamente las relaciones entre dichas ocupaciones y competencias. ESCO

está gestionada por la Comisión Europea, que se encarga de actualizar la clasificación.

El recurso ESCO apoya dos de las estrategias clave de la UE en este ámbito, Europa 2020 y Skills

Agenda para Europa17

.

13 CWA 16458 Perfiles profesionales europeos de las TIC

14 https://europa.eu/europass/en/description-eight-eqf-levels

15 https://europa.eu/europass/en/national-qualifications-frameworks-nqfs

16 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=ES

17 https://ec.europa.eu/social/main.jsp?catId=1326&langId=en

El objetivo de ESCO es describir todas las ocupaciones del mercado laboral europeo, incluyendo por tanto

ciberseguridad. Por lo tanto, es útil establecer una correspondencia orientativa entre el papel del ECSF

y algunos de los perfiles de las ESE.

En el Cuadro 5 se enumeran varias ocupaciones de las ESE relacionadas con la ciberseguridad, junto con una lista indicativa de las mismas.

a los perfiles de funciones ECSF. Dado que la relación entre ellos no siempre es uno a uno,

se definieron las siguientes relaciones para explicar las conexiones correspondientes:

- es - Esta Ocupación ESCO puede asignarse al perfil de función ECSF correspondiente como ambos describen la misma función de ciberseguridad.

- puede incluir - Esta ESE Ocupación puede incluir, en función del contexto, la ECSF perfil de funciones indicado. (Se trata de una asignación indicativa).

- Algunos aspectos de esta Ocupación de la ESE pueden describir partes de el perfil de función ECSF indicado. (Se trata de una asignación indicativa).

Cuadro 5: Relación entre los perfiles de las ESE y los perfiles de las ECSF

Código de la ESE Ocupación de la ESE Relación Perfil de la función de la ESE

2149.2.8 Ingeniero de investigación podría incluir Investigador de ciberseguridad

2310.1 Profesor de enseñanza superior podría incluir Educador en ciberseguridad

2356 Tecnología de la información formador podría incluir Educador en Ciberseguridad

2511.18 Auditor de TI podría incluir Auditor de Ciberseguridad

2519.2 El responsable de auditoría TIC podría incluir al Auditor de Ciberseguridad

2529.1 El responsable de seguridad TIC es el Director de Seguridad de la Información (CISO)

2529.2 Experto forense digital es Investigador forense digital

2529.3 Seguridad de los sistemas integrados ingeniero podría incluirse Implementador de ciberseguridad

2529.4 Hacker ético es Probador de Penetración

2529.6 Podría incluirse al administrador de seguridad de las TIC Implementador de ciberseguridad

2529.7 Ingeniero de seguridad TIC podría incluirse Arquitecto de ciberseguridad

2529.7 Ingeniero de seguridad TIC podría incluirse Implementador de ciberseguridad

2619.4 El responsable de la protección de datos es el responsable cibernético jurídico, de políticas y de conformidad

Nota importante: La relación entre la ocupación de la ESE y el perfil de funciones de la ECSF no no representa una equivalencia, sino que ofrece una aproximación que el lector puede considerar adecuada.

investigar.

B ANEXO:

CASOS DE USO

Un caso de uso muestra por qué y cómo una organización utiliza el ECSF, haciendo hincapié en la variedad de

enfoques y beneficios. Este anexo es una recopilación de casos que se hicieron públicos el 20 de

Julio de 2022.

Los siguientes casos de uso son meros ejemplos ilustrativos. La información y los contenidos incluidos

en estos casos no debe considerarse como una declaración de aprobación o validación por parte de

ENISA. El uso de estos ejemplos debe considerarse como casos de inspiración más que como

condicionar las líneas de base o las referencias de evaluación comparativa.

B.1 CASO PRÁCTICO DEL PROYECTO CONCORDIA H2020

Esta sección incluye partes del caso práctico redactado por el proyecto CONCORDIA H202018

.

Hacia una plataforma integrada de cibercapacidades basada en la Ciberseguridad Europea

Marco de competencias

Dificultad para comprender el conjunto de la formación

Las necesidades de protegerse contra las amenazas a la información y las operaciones, de mantener la

ciberseguridad de una organización y aumentar la resistencia frente a dichas amenazas, son

que todas las partes interesadas siguen sintiendo con urgencia. Un componente esencial para satisfacer estas necesidades es la

existencia de profesionales cibercompetentes. Y la competencia en materia de ciberseguridad no es

(externos o internos a una organización), sino también para los profesionales que se dedican a la formación.

todos los miembros del personal de una organización, aunque no estén directamente implicados en la ciberseguridad

procesos y actividades.

En lo que respecta a los profesionales de la ciberseguridad, diversas publicaciones siguen informando de un

ciberseguridad, señalando que las 3 principales competencias que faltan o no están suficientemente cubiertas por

los profesionales existentes varía de un año a otro19. Por otra parte, una considerable

de cursos y formaciones relacionados con la ciberseguridad.

organizaciones internacionales. Una simple búsqueda en Internet revelará muchos cursos que se relacionan

al ámbito de la ciberseguridad, sin ofrecer una imagen clara sobre las competencias ofrecidas o

cómo podrían relacionarse con una función específica. Para aumentar esta confusión, hay cursos de formación que

parecen dirigirse a una función específica (por ejemplo, CISO), tienen títulos similares pero un plan de estudios diferente.

De ahí que, en varios casos, la información facilitada confunda al aprendiz sobre qué y cómo deben

deben percibir los conceptos de ciberseguridad, así como la forma de utilizarlos para cubrir sus

necesidades. Además, los cursos para profesionales se promocionan en diversas plataformas y se

son difíciles de comparar en cuanto a las competencias cubiertas y el perfil de las funciones

abordado. Esto dificulta que una persona construya una trayectoria profesional clara e identifique

oportunidades de desarrollo.

18 https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-europeancybersecurity-skills-framework/

19 https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-newisaca-research-shows-retention-difficulties-in-years

El mapa CONCORDIA de cursos para profesionales de la ciberseguridad

En un intento de abordar estos retos, hemos construido el mapa CONCORDIA de cursos y

formaciones para profesionales de la ciberseguridad20. El mapa muestra información estructurada sobre

oferta europea existente de cursos de corta duración/formación y proporciona diferentes filtros para ayudar a emparejar

más fácil la necesidad específica de desarrollo de competencias con la oferta. [...]

Se puede optar por clasificar los cursos en función del nivel de ciberseguridad abordado (Device-
,

centrada en la red, en el software/sistema, en los datos/aplicación, en el usuario), o en la relevancia para una

sector industrial (por ejemplo, telecomunicaciones, finanzas, transporte, e-movilidad, e-salud o defensa), sino también sobre

el formato (presencial, en línea, combinado) y el calendario del curso/formación.

Falta un ingrediente clave - Solución facilitada por ECSF

Aunque ofrecemos en el mapa CONCORDIA una gran cantidad de filtros para ayudar a los usuarios

identificar más fácilmente el curso o cursos de interés, la base de datos carece de un ingrediente clave: los enlaces a la función

perfiles que cada uno de los cursos aborda a través de los conocimientos y competencias tratados. El sitio

e-CF Marco Europeo de Competencias para los profesionales de las TIC disponible en el momento de la construcción

el mapa define 30 perfiles de funciones y 40 competencias asociadas, pero son difíciles de

asociados a las especificidades del ámbito de la ciberseguridad.

Este era un reto del ecosistema educativo de ciberseguridad que ya señalamos hace dos años

y recogido en la Hoja de ruta CONCORDIA para la educación21 bajo el epígrafe C5:

Heterogeneidad de la terminología relacionada con las competencias. Esta falta de una terminología

terminología consensuada en todos los sectores en relación con las competencias de ciberseguridad necesarias para un puesto específico

dificulta a las empresas cubrir los puestos vacantes. Les resulta difícil hacer coincidir la contratación

criterios con los estudios y las cualificaciones que figuran en los CV de los candidatos debido a la

uso de terminología no estándar. A su vez, las personas no pueden identificar fácilmente las competencias que necesitan

poseer o desarrollar para responder a la demanda del mercado. Y, por último, los proveedores de cursos tienen dificultades

en el diseño de planes de estudios que respondan a las necesidades del mercado.

Como parte de la hoja de ruta de CONCORDIA, nos comprometimos a crear una plataforma única que albergara todos los servicios existentes.

Programas relacionados con la ciberseguridad (programas de nivel universitario y de doctorado, cursos cortos y

formación para profesionales). [...]

La plataforma debería considerar la posibilidad de recopilar los contenidos utilizando categorías basadas en una norma

terminología (marco de competencias específicas incluido). Las categorías se utilizarían además como filtros

para diferentes consultas de la base de datos de cursos. Los 12 perfiles de funciones definidos en la versión actual

del Marco Europeo de Competencias en Ciberseguridad (ECSF) parecen ser una solución natural.

Ventajas para las partes interesadas

La adopción de un léxico estándar como el propuesto por la ESCF, que incluya

Los perfiles de las funciones de ciberseguridad ayudarán a las empresas a identificar el talento adecuado para los puestos de trabajo, así como a

a los proveedores de educación para que adapten mejor sus planes de estudios a las necesidades de la mano de obra cibernética. En

aplicar la misma terminología y utilizar un marco de competencias a escala de la UE en las descripciones de los puestos de trabajo,

la descripción del curso y el perfil de la función ayudarían a las personas a seleccionar los módulos de formación adecuados

apoyar su trayectoria profesional y filtrar mejor las ofertas de empleo en función de su competencia

y nivel de conocimientos. Por último, los responsables políticos podrían recopilar datos más estructurados en

a nivel nacional/regional en apoyo de la futura elaboración de políticas y disponer de una base sólida a la hora de

coordinarse con países externos para hacer frente a los retos de ciberseguridad a escala mundial.

20 https://www.concordia-h2020.eu/map-courses-cyber-professionals/

21 https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

MANUAL DEL USUARIO

SEPTIEMBRE 2022

40

Hacia una plataforma integrada de competencias

A partir de la base de datos CONCORDIA de cursos y formación para profesionales de la ciberseguridad,

el proyecto REWIRE22 intenta dar nuevos pasos hacia la integración de las

contenidos relacionados con las competencias en ciberseguridad. La plataforma REWIRE CyberABILITY - actualmente en diseño

fase - proporcionará información actualizada sobre el mercado laboral, las competencias, la formación

cursos, sistemas de certificación y una hoja de ruta profesional.

B.2 CASO PRÁCTICO DEL PROYECTO SPARTA H2020

Esta sección incluye partes del caso de uso redactado por el proyecto SPARTA H202023

.

Mejora de la enseñanza superior mediante ECSF y SPARTA Curricula Designer

Introducción

Este caso práctico ofrece recomendaciones sobre cómo utilizar el ECSF para configurar la educación

programas relacionados con la ciberseguridad. Como ECSF manifiesta la estructura de alto nivel

perfiles desde el punto de vista de los profesionales, incluidas las tareas principales, los conocimientos y competencias pertinentes, este

puede proporcionar un enfoque más centrado para elaborar un estudio especializado y exhaustivo

programas, adaptados a perfiles específicos, en lugar de cubrir la ciberseguridad en general.

Desafío

Las instituciones educativas elaboran sus planes de estudios teniendo en cuenta el itinerario completo, empezando por la

cursos fundamentales que el alumno debe aprender como base para el siguiente conjunto de

cursos de seguimiento, que a menudo son específicos de ciberseguridad. Sin embargo, la selección de cursos a

incluirse en los planes de estudios de ciberseguridad depende de la institución.

Cada centro educativo tiene su propio entorno específico (determinado, por ejemplo, por la infraestructura,

equipamiento, experiencia de los profesores, composición de los programas existentes, etc.) y no hay

manera universal cómo debe construirse el currículo.

Los proveedores de educación difieren en cuanto al subdominio concreto de la ciberseguridad en el que les gustaría centrarse

on. Algunos proveedores son muy técnicos y se centran, por ejemplo, en la informática, mientras que otros tienen una orientación más social y se centran en aspectos jurídicos y sociales. Por tanto, la interoperabilidad entre los

programas de estudio resultantes y una lengua común es actualmente un reto importante.

Algunos programas académicos no desarrollan aptitudes y competencias que preparen a los estudiantes para

funciones laborales específicas disponibles en el mercado de trabajo. Esto supone un reto para los estudiantes que no

comprender cuáles son las posibilidades profesionales al término de sus estudios.

Solución habilitada por ECSF

El ECSF puede contribuir a las siguientes actividades que abordan los retos mencionados:

- Evaluación: La descripción de los perfiles permite a las instituciones revisar sus planes de estudios de forma

manera estructurada y sistemática, comprendiendo el punto de vista de los profesionales. Este

permite comprender para qué perfil la institución destina principalmente a sus titulados.

22 https://rewireproject.eu/

23

https://sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula

%20Diseñador.pdf

MANUAL DEL USUARIO

SEPTIEMBRE 2022

41

- Mejora: Puede realizarse a partir del ejercicio de evaluación. Esto es especialmente

importante teniendo en cuenta el conjunto de conocimientos / competencias atribuidas a un perfil específico.

- Enfoque: La educación que imparten las universidades puede diferir en la forma de abordar las materias básicas.

competencias. Algunas podrían estar más centradas en cursos tecnológicos específicos, otras

en derecho, otros en medicina forense, etc. Al disponer de un ECSF con el que trabajar, pueden mapear su núcleo

competencias en diversas áreas de cursos, importantes para perfiles definidos. Esto permite

a la institución a desarrollar programas internos más eficaces en torno a las principales

competencias.

- Colaboración: ECSF proporciona a los proveedores de educación un lenguaje común y

vocabulario para describir sus cursos, crear programas conjuntos y permitir

movilidad de los estudiantes.

Al aplicar el ECSF a la educación en ciberseguridad, se recomienda el siguiente enfoque:

- Los cursos de los planes de estudios pueden clasificarse en fundamentales o cibernéticos.

Categorías de seguridad. Los cursos fundamentales son aquellos que pueden no estar directamente relacionados con

la ECSF, sino que sirven de requisito previo para estudios posteriores. Por ejemplo,

Criptología fundamental es el requisito previo para Criptoanálisis o Criptología avanzada;

La Teoría de Números es necesaria para la mayoría de los cursos intermedios y avanzados de informática.

cursos.

- Una vez identificados los cursos Fundamentales, los cursos de Ciberseguridad pueden ser

propuestas para abordar los requisitos de las funciones laborales a las que aspiran los estudiantes. La vinculación es

en función del contenido de los cursos individuales, que pueden vincularse a los perfiles

y, por último, a los roles laborales. Los pasos concretos, [...], son:

a. Para un rol de trabajo específico 1, los proveedores de educación encuentran los perfiles pertinentes

(Perfil 1 y Perfil 12 en nuestro ejemplo). Esta correspondencia, marcada en marrón

deben ser especificadas por los anunciantes/empleadores.

b. Los proveedores de formación identifican los conocimientos y competencias necesarios para los

perfiles. Estos requisitos están definidos por el ECSF, marcados en azul

flechas.

c. Los proveedores de educación diseñan nuevos cursos o reutilizan los existentes (en nuestro ejemplo

cursos 1, 2, 3, 4) que aborden los conocimientos y competencias identificados en el paso

arriba. Esta correspondencia entre los cursos y su contenido debe realizarse mediante

administradores de cursos.

d. Disponer de todos los cursos necesarios (y todos los requisitos previos para ellos, cursos generales no relacionados con la ciberseguridad, otros cursos para ampliar el ámbito de los estudiantes,

etc.), el núcleo del plan de estudios está listo.

- Por supuesto, el ECSF puede aplicarse también de forma exactamente opuesta: componiendo primero

el plan de estudios de los distintos cursos, analizando los conocimientos y competencias que se imparten,

utilizar el ECSF para identificar perfiles y, por último, encontrar las funciones laborales que se apoyan

por el plan de estudios. Este mapeo revela qué conocimientos y destrezas exactos están ya

presente en los planes de estudios o, por otro lado, qué falta y debería destacarse o

añadidos a los cursos. De este modo, el ECSF ayuda a estructurar los planes de estudios para una mejor

se ajustan a los perfiles y funciones laborales previstos.

Resultado / Valor añadido de SPARTA

El proyecto SPARTA utilizó un marco de competencias en ciberseguridad para crear una herramienta gratuita llamada Cybersecurity

Diseñador de planes de estudios. Se trata de una sencilla aplicación web que ayuda a los proveedores de educación a crear nuevos

programas de estudio sobre ciberseguridad y/o analizar los programas de estudio existentes en función de su

contenido y su reflejo de los requisitos de los empleos de ciberseguridad.

La herramienta [...] permite a los administradores de programas de estudios componer su programa de estudios arrastrando

y soltando cursos de la sección izquierda a la sección central. Cursos de los que

MANUAL DEL USUARIO

SEPTIEMBRE 2022

42

Los administradores elaboran los programas de estudio, que pueden ser predefinidos o personalizados. Mientras que

componer el programa de estudio, los datos estadísticos sobre su contenido se muestran en la parte derecha

sección. Además de otros datos, la información sobre qué competencias y funciones laborales se

soportados por el programa. Utilizando la herramienta, es fácil averiguar qué contenidos son

que faltan en el programa de estudios y qué funciones laborales específicas son las más adecuadas para los titulados de

el programa. En este caso, el marco de competencias de ciberseguridad es el núcleo de las aplicaciones que

permite vincular las competencias y los conocimientos con las funciones del puesto de trabajo. [...]

B.3 CASO DE USO DE INCIBE

Esta sección incluye partes del caso práctico redactado por INCIBE24

.

Caso práctico de INCIBE

Introducción

La eficacia en la protección de un país depende en gran medida de las capacidades de su población, y

Las estimaciones en este sentido son que en 2022 España podría alcanzar una plantilla de ciberseguridad cercana al

a 122.284 trabajadores, con un déficit de talentos estimado en 24.119. En consecuencia, una de las principales prioridades

para la administración hoy en día es afrontar el reto de identificar, atraer, desarrollar y

retener el talento en los distintos ámbitos de la ciberseguridad.

Prueba de este compromiso es la elaboración por parte del Gobierno español del Plan Nacional 2019 de

Estrategia de Ciberseguridad25, que hace hincapié en la necesidad no sólo de contar con una defensa y protección

para empresas y ciudadanos, sino también para apoyar el impulso de la ciberindustria,

reconocer el papel clave que desempeña la ciberseguridad en el actual entorno de transformación

e incertidumbre y la oportunidad que ofrece para aumentar la competitividad de España. En consonancia con

objetivo 4 de la Estrategia, la línea de actuación 5 destaca la importancia de impulsar el

industria de la ciberseguridad, además de la generación y retención de talento para el fortalecimiento

de la autonomía digital.

Por otro lado, el Plan España Digital 202526 busca reforzar las palancas que faciliten

volver a la senda del crecimiento económico, y uno de sus ejes estratégicos es fortalecer la

capacidad de ciberseguridad para mitigar los riesgos y aumentar la confianza en el camino hacia un mundo digital y

economía sostenible.

En su eje estratégico 4, dedicado monográficamente a la ciberseguridad, incorpora las medidas

que conforman las tres principales líneas de actuación de INCIBE para los próximos años: aumentar la

capacidades de ciberseguridad de ciudadanos y empresas; impulsar la ciberseguridad española

ecosistema en torno a su industria, su I+D+i y su talento en ciberseguridad; y consolidar a España como un

nodo internacional del sector. España Digital 2025 ya reconoce el papel clave de

talento en ciberseguridad como motor del sector.

Estas iniciativas nacionales generan un escenario adecuado que favorece la investigación, la innovación y la

involucra a los agentes más relevantes de la cadena de valor, como instituciones educativas y

organizaciones, para que vean el beneficio de gestionar los conocimientos, capacidades y

experiencias tecnológicas que respondan a los grandes retos que tiene el país en materia de

ciberseguridad.

24 http://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills

25 https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

26 https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

MANUAL DEL USUARIO

SEPTIEMBRE 2022

43

Por su parte, el Instituto Nacional de Ciberseguridad de España (INCIBE), empresa dependiente del

Ministerio de Economía y Transformación Digital, a través de la Secretaría de Estado de

Digitalización e Inteligencia Artificial; y la entidad de referencia para el desarrollo de

ciberseguridad y confianza digital de ciudadanos y empresas, y de la comunidad académica y

de investigación (RedIRIS), tiene como misión mejorar la ciberseguridad y la confianza digital de los

ciudadanos, menores y empresas privadas en España.

Además, su misión incluye la protección y defensa de estos grupos, la promoción de

industria española y la I+D+i en ciberseguridad, así como la identificación, generación y

atracción de talentos al sector de la ciberseguridad.

El talento en ciberseguridad es, por tanto, una piedra angular de las actuaciones de INCIBE. Sin talento es

imposible desarrollar una industria fuerte o las soluciones de alto valor añadido necesarias para participar

en un mercado tan competitivo como el de la ciberseguridad.

Sin embargo, la información disponible hasta ahora sobre el estado del talento en el sector de la ciberseguridad en

España era variada y fragmentada, procedente de distintas fuentes, lo que dificultaba la profunda

comprensión del entorno necesaria para canalizar las acciones. [...]

Por ello, con el objetivo de ofrecer una visión clara del talento en ciberseguridad en España, INCIBE

publica en marzo de 2022, los resultados de un análisis y diagnóstico del talento en ciberseguridad en

nacional, cuyo proceso se ha llevado a cabo mediante premisas analíticas rigurosas, globales

de trabajo y procesos participativos e inclusivos que han tenido en cuenta las principales

actores del ecosistema de la ciberseguridad. [...]

Desafío

Las recomendaciones derivadas de este proyecto de análisis son el punto de partida para garantizar una

industria de la ciberseguridad robusta y rentable que se caracteriza por poner el talento de las personas en el

núcleo de iniciativas. En este sentido, toda la cadena de valor de la ciberseguridad puede ver este estudio como un

oportunidad de seguir conectando con el talento de la ciberseguridad en España y conocerlo mejor.

Por lo tanto, es necesario estructurar y aplicar prácticas eficaces que incidan en la

gestión de este tipo específico de talento en las organizaciones. La importancia de la ciberseguridad para

la supervivencia de las organizaciones requiere la necesidad de abordar el problema de la identificación de este tipo de

talento específico en ciberseguridad, la evolución del proceso de contratación y embarque, así

como la adopción de acciones que contribuyan a mejorar la gestión y mitigar la fuga de talentos.

Por ello, el impulso de políticas nacionales, coordinadas desde la administración que

se centran en reforzar y promover iniciativas para hacer de la ciberseguridad una prioridad estratégica en

organizaciones, así como estructurar y elaborar un itinerario de formación para la realización de

ciberseguridad como actividad profesional son prioridades en las que tanto organizaciones como

empresas de selección establecerán en sus actuaciones para la identificación, captación, contratación

y gestión del talento en ciberseguridad.

De esta forma, se establecen una serie de recomendaciones que este tipo de agentes (Público

Administración, empresas de contratación y otras organizaciones) podrían aplicar para aumentar

talento en ciberseguridad en España y que marcan el punto de partida para resolver los retos que tenemos por delante

a este respecto. [...]

Solución habilitada por ECSF

MANUAL DEL USUARIO

SEPTIEMBRE 2022

44

Existen diversos factores (políticos, económicos, sociales, tecnológicos, jurídicos, etc.) que pueden influir en

la industria de la ciberseguridad y, en consecuencia, la escasez de talento, las lagunas y, en general, una

desajuste entre la oferta y la demanda.

Uno de estos factores relevantes en la Unión Europea, es la falta de normalización del

definición de las funciones de ciberseguridad y de las competencias asociadas a dichas funciones.

Proporcionar una base para la comunicación continua entre las distintas partes interesadas (Gobierno,

la industria, el mundo académico, los responsables políticos y los ciudadanos).

Este tipo de herramienta sirve de base para una mano de obra más competente y completa que

entiende el mismo idioma que los demás profesionales del Europeo. [...]

Resultado / Valor añadido

Por ello, en el contexto presentado, se han puesto en marcha dos iniciativas a escala nacional,

que dará valor al ECSF desarrollado por ENISA y que será de gran utilidad. [...]

Ambas iniciativas, coordinadas entre sí, incorporarán el ECSF como un homogéneo

marco para la definición de perfiles de ciberseguridad, que permitirá a España alcanzar su talento

objetivos y alinearse con el resto de países a nivel europeo. [...]

B.4 CASO PRÁCTICO DE CIBERSEGURIDAD EUROPEA

ORGANIZACIÓN EUROPEA DE NORMALIZACIÓN (ECSO)

Esta sección incluye partes del caso práctico redactado por la Comisión Europea de Ciberseguridad.

(ECSO)27

.

Hacia un enfoque educativo armonizado con las competencias europeas en ciberseguridad

(ECSF)

Tras haber trabajado en educación, formación y competencias en su GT5 desde 2016, la ECSO ha visto de primera mano los retos que plantean la fragmentación y los enfoques dispersos que existen dentro de

ciberseguridad en la actualidad. En esta entrada de blog, ECSO reflexiona sobre los enfoques europeos existentes en materia de

y se centra en el Marco Europeo de Competencias en Ciberseguridad de la ENISA.

(ECSF).

La educación no es sólo una prerrogativa nacional. También está intrínsecamente ligada a la colaboración

entre las entidades nacionales, la comunidad de la ciberseguridad en general y los organismos europeos. Con esto en

mente, la colaboración es clave a la hora de idear planteamientos paneuropeos para armonizar

ciberseguridad y abordar el déficit de competencias o, más concretamente, de mano de obra.

Hay muchas oportunidades para aprovechar el espíritu de colaboración de la ciberseguridad europea.

comunidad para ofrecer soluciones prácticas e iniciativas que puedan tener un impacto "sobre el terreno",

y el Marco Europeo de Competencias en Ciberseguridad (ECSF) de ENISA puede desempeñar un papel importante en este sentido.

respeto.

Educación en ciberseguridad: la perspectiva de la ECSO

Desde la perspectiva de la Organización Europea de Ciberseguridad (ECSO), como representante

del ecosistema y la comunidad público-privada de la ciberseguridad europea), el potencial

27 https://www.ecs-org.eu/newsroom/consolidated-educational-and-recruiting-scheme-the-glue-to-fix-todays-scatteredapproach

El valor del ECSF no es desdeñable cuando se trata de vincular los esfuerzos existentes, proporcionar

elementos fundamentales para una mano de obra europea de ciberseguridad y

marco y taxonomía para la aplicación de perfiles y competencias. Profesionales de la ciberseguridad,

tanto los proveedores de educación y formación como los responsables políticos y los profesionales de la contratación saldrán ganando

de la aplicación más amplia del ECSF.

El desafío

Es evidente que existe una necesidad creciente de mano de obra cualificada en ciberseguridad. Diversos estudios

de la industria y el mundo académico de todo el mundo confirman que la demanda de mano de obra en ciberseguridad

es muy elevado y que resulta difícil contratar a profesionales competentes. La edición de 2021 del

Cybersecurity Workforce Study publicado por ECSO Member (ISC)²28 afirma que la escasez de

profesionales de la ciberseguridad es de 2,72 millones en todo el mundo, cifra que, aunque ha disminuido desde los 3,12

millones de euros el año anterior, sigue siendo una cifra significativa. Aunque estos estudios ofrecen una base sobre la que

para evaluar la situación global, la realidad es que es muy difícil cuantificar el alcance de la

escasez de talentos en ciberseguridad en Europa. Sabemos que la demanda de expertos aumentará inevitablemente

debido al crecimiento del mercado de la ciberseguridad y al panorama normativo, dejando un vacío urgente

llenar con más (y diferentes tipos de) expertos. [...]

Pero no es sólo una cuestión de cifras. A través de un reciente estudio de la ECSO sobre la contratación de RRHH

prácticas y tendencias, la ECSO también ha observado un aumento del tiempo que tarda, por término medio, en

organizaciones para cubrir sus puestos de ciberseguridad. Muchas organizaciones indican que puede llevar

a seis meses para el proceso de contratación, que es más lento que en los dominios de conocimiento del orden,

mientras que otros afirman que tienen dificultades para cubrir todos sus puestos de ciberseguridad.

Esto indica claramente que existe un desajuste entre la oferta y la demanda (es decir, una brecha

entre los requisitos académicos y los de la industria) y los factores de empuje y atracción (es decir, la idoneidad de los candidatos

y evaluación, atracción hacia el empleo y prestaciones). Sin embargo, el principal problema para los empresarios

sigue siendo la falta generalizada, en todo el mundo, de especialistas en ciberseguridad, mientras que la demanda es constante

creciente. Varias organizaciones destacan también la complejidad de contratar expertos para un ámbito que

que no dominan. La encuesta de la ECSO también indicaba que, como tendencia creciente, varios candidatos,

a pesar de carecer de competencias importantes en ciberseguridad, enriquecen su currículum con conceptos de ciberseguridad

y palabras clave.

Estos retos ponen claramente de manifiesto la necesidad de un lenguaje común para apoyar la contratación.

y la importancia de tener en cuenta el carácter multidisciplinar de la ciberseguridad, tan

únicas de este campo frente a las profesiones más tradicionales de las TI/TIC. Aunque los marcos existentes, como

NICE, CyBoK y eCF ofrecen directrices útiles para el desarrollo de competencias, un marco europeo

que ofrece una taxonomía general de perfiles y trayectorias profesionales inherentes a la ciberseguridad,

ha estado ausente. La publicación del ECSF es, por tanto, muy oportuna y fundamental para

apoyo a la comunidad europea de la ciberseguridad para atraer, capacitar y reciclar a expertos.

Existe una solución

La ECSO aplicará el ECSF de diversas maneras para impulsar su adopción y aprovechar su potencial para

armonizar la educación y las competencias en materia de ciberseguridad en toda Europa.

ECSO lo hará:

- Trazar su plan de estudios mínimo de referencia para el ECSF, dando a los diseñadores de cursos y

a los profesionales una mirada de primera mano sobre la mejor manera de definir sus planes de estudios hacia la dedicación

itinerarios profesionales. Esto contribuirá a garantizar que los cursos universitarios reflejen adecuadamente las

de las necesidades del mercado laboral de la ciberseguridad, al tiempo que se

actualización del plan de estudios.

28 https://www.isc2.org/Research/Workforce-Study

MANUAL DEL USUARIO

SEPTIEMBRE 2022

46

- Utilizar el ECSF y el manual de uso asociado para apoyar a RRHH/contratación en la redacción de

anuncios de empleo y organización de la evaluación de las competencias prácticas

procedimientos. También llevaremos a cabo una encuesta de seguimiento de los recursos humanos utilizando los perfiles de los puestos de trabajo del ECSF para

comprender qué funciones son las más necesarias para las organizaciones y crear progresivamente un

comprensión cuantitativa del mercado laboral europeo de la ciberseguridad.

- Utilizar el ECSF como taxonomía de base para dos plataformas específicas previstas por la

Fundación Women4Cyber y ECSO [...]

Resultado y valor añadido

El valor añadido del ECSF para la comunidad europea de la ciberseguridad es, en primer lugar, tener un

marco y taxonomía comunes sobre los que trabajar. Esto permitirá comprender mejor

de las necesidades de cualificación y las realidades prácticas de los distintos perfiles laborales, lo que mejorará la

ciberseguridad, no sólo mediante medidas más eficaces de contratación y retención, sino también

también facilitando la incorporación o reincorporación de más mujeres y otros grupos infrarrepresentados

(es decir, los neurodiversos) en este campo. La ECSF, al destacar los aspectos técnicos y no técnicos

aspectos de los diferentes perfiles, contribuirá a eliminar la idea errónea de que la ciberseguridad es

sólo un tema técnico, cuando se trata tanto de personas como de procesos. En este sentido,

hacer hincapié en la importancia de las competencias interpersonales (transferibles) en este ámbito contribuirá de forma significativa

para atraer a más mujeres a la profesión de la ciberseguridad. El ECSF también reducirá la

fragmentación de los enfoques mediante la introducción de directrices descendentes sobre cómo categorizar las

naturaleza polifacética de la profesión de ciberseguridad. Los perfiles propuestos por la ECSF son

suficientemente amplia para poder sustentar las numerosas funciones que ofrece la profesión, al tiempo que

segmentarse de forma que resulte comprensible y aplicable para los profesionales,

expertos del sector, responsables políticos, especialistas en contratación y demandantes de empleo.

En la ECSO estamos convencidos de que el ECSF aportará un valor significativo a

nuestro trabajo y apoyar a la comunidad en general con una herramienta concreta para

armonizar los esfuerzos y colmar la brecha entre la oferta y la demanda

de expertos.

B.5 CASO PRÁCTICO DE ISC2

Esta sección incluye partes del caso de uso redactado por (ISC)²29

.

Utilización del CBK CISSP de (ISC)² para apoyar el Marco Europeo de Competencias en Ciberseguridad /

Comunidades profesionales de ciberseguridad

Introducción

El (ISC)² CISSP CBK - a veces llamado simplemente el "Body of Knowledge" - se refiere a un compendio desarrollado por pares de lo que un profesional competente en ciberseguridad debe identificar y

poseer, incluidos los conocimientos, destrezas, habilidades, técnicas y prácticas para tener éxito. El sitio

(ISC)² CBK es una colección de temas relevantes para los profesionales de la ciberseguridad de todo el mundo. En

establece un marco común de términos y principios de seguridad de la información que permite

profesionales de la ciberseguridad y las TI/TIC de todo el mundo para discutir, debatir y resolver asuntos

pertenecientes a la profesión con un entendimiento, una taxonomía y un léxico comunes. (ISC)² fue

creado, en parte, para agregar, normalizar y mantener el CBK (ISC)² para la ciberseguridad

profesionales de todo el mundo. El CBK de (ISC)2 presenta un recurso listo para usar para los profesionales actuales y futuros.

que los aspirantes a profesionales de la ciberseguridad adopten en el marco del ECSF.

29 https://www.isc2.org/-/media/9644E0ED44954F7CAF895D45620213EA.ashx

MANUAL DEL USUARIO

SEPTIEMBRE 2022

47

Desafío

Como describe ENISA en su informe recientemente publicado "Addressing The EU Cybersecurity Skills

Shortage And Gap Through Higher Education", la escasez mundial de competencias en ciberseguridad y la falta

de una mano de obra suficiente y cualificada son preocupaciones que tienen un impacto significativo en los países miembros de la UE.

la capacidad de los Estados para proteger a los ciudadanos de las amenazas cada vez mayores que emanan de la

uso de la tecnología en la sociedad. A pesar del trabajo realizado, los ciberataques y la

La amenaza de ciberataques sigue siendo un riesgo importante para la seguridad pública. Las organizaciones europeas

tienen dificultades para dotar de personal adecuado a sus equipos de ciberseguridad. Las consecuencias evitables -

sistemas mal configurados, despliegues precipitados, respuesta incompleta a incidentes, retraso en la aplicación de parches,

Una gestión inadecuada de los riesgos hace que muchas organizaciones europeas sean objetivos apetecibles para las amenazas.

actores de todo el mundo.

Solución facilitada por el ECSF (cómo se afrontaron los retos)

Para hacer frente a los retos que plantean el déficit de cualificaciones y la escasez de mano de obra, (ISC)² propone una

solución centrada en ayudar a los profesionales de la ciberseguridad a identificar y asignar los conocimientos necesarios,

habilidades, destrezas, técnicas y prácticas a los perfiles identificados en la Ciberseguridad Europea

(ECSF). El (ISC)2 CISSP CBK se corresponde con varias áreas de habilidades y conocimientos

en los siguientes perfiles ECSF:

- 2.1 Director de Seguridad de la Información (CISO)

- 2.2 Respuesta a ciberincidentes

- 2.3 Responsable de ciberlegislación, política y conformidad

- 2.4 Especialista en inteligencia sobre ciberamenazas

- 2.5 Arquitecto de ciberseguridad

- 2.6 Auditor de ciberseguridad

A partir de los conceptos tratados en el CBK, los profesionales que trabajan actualmente en las

perfiles enumerados o los que aspiran a trabajar en estos perfiles pueden utilizar las competencias clave y los

áreas de conocimiento de los perfiles ECSF combinados con los CBK de (ISC)2 para determinar cómo los

CBK cumple con los conocimientos y habilidades requeridos para el puesto y en los que pueden necesitar

complementar su educación/formación con otras fuentes. De este modo, los candidatos podrán

vía de educación/formación para alcanzar sus objetivos.

La siguiente tabla proporciona un ejemplo de cómo el (ISC)2 CISSP CBK puede ser utilizado por un

CISO actual o aspirante a CISO para identificar las habilidades clave y áreas de conocimiento del Perfil CISO ECSF.

que tienen o necesitan construir. [...]

Resultado / Valor añadido

El beneficio previsto de la correspondencia entre el CBK del CISSP de (ISC)² y el ECSF es que creará una carrera profesional.

orientación y vías educativas profesionales para ayudar a los actuales y aspirantes a la ciberseguridad.

que los profesionales identifiquen y obtengan los conocimientos, competencias y habilidades profesionales necesarios para

obtener y cubrir más rápidamente los perfiles abiertos, tal y como se identifican en el ECSF, mitigando así la

ciberseguridad y reducir el déficit de mano de obra cualificada.

B.6 CASO PRÁCTICO DE ISACA

Esta sección incluye partes del caso de uso escrito por ISACA30

.

30 https://www.isaca.org/training-and-events/careers-home/career-pathway/european-cybersecurity-skills-framework-andisaca-credentials

Toma de decisiones individuales sobre la carrera profesional: Credenciales profesionales Ciberseguridad europea

Marco de competencias

Introducción

Sabine trabajaba como analista SOC unos años después de obtener su título universitario, y

estaba interesada en saber cuál era la mejor manera de avanzar en su carrera. Habló con su mentor, que

le comunicó que ISACA había sido una gran plataforma de lanzamiento para su carrera y la animó a

estudiar la afiliación y la posible certificación. Hay que tener en cuenta que entrar en el sector de la ciberseguridad

da la posibilidad de trabajar con todo, desde las personas y la psicología hasta los aspectos jurídicos, políticos y

gobernante, hasta el nivel técnico más bajo (o más alto). El reto consiste en encontrar un

punto de partida y, a continuación, determinar qué competencias específicas se pueden aprender y luego dominar para

ampliar o incluso pasar de un rol de ciberseguridad a otro. La ESCF especifica varias funciones con

sus competencias necesarias para trabajar en esa función específica. Observe que estas competencias son

no todo lo necesario para una función concreta, sino lo mínimo indispensable. De este modo, Sabine puede identificar

la brecha de competencias si uno quiere cambiar de función o pasar a otra área dentro de

Ciberseguridad.

Desafío

Como nueva profesional en un campo de gran demanda y como mujer en el ámbito de la ciberseguridad, Sabine se encontraba en

buscando ayuda en diferentes áreas:

- Orientación profesional y recursos -incluidas credenciales- para ayudarla a progresar en su carrera.

- Una red de colegas y líderes del sector para ayudarla a superar los retos profesionales.

- Asistencia en el desarrollo de aptitudes interpersonales que la ayuden a convertirse en una futura líder polifacética.

- Cómo superar los retos y aprovechar las oportunidades como mujer en el mundo laboral

ciberseguridad

- Información que le ayude a hacer bien su trabajo actual y a prepararse para el futuro.

retos en funciones de nivel superior

Cualquier persona puede utilizar la ESCF para ver qué funciones se necesitan para gestionar casi cualquier tipo de

desafío o tarea en el ámbito de la ciberseguridad. Además, al utilizar la ESCF como base de referencia, un

A continuación, el individuo puede identificar qué competencias son necesarias para pasar de un papel a otro.

Ello favorecerá el diálogo entre trabajadores y empresarios a la hora de planificar la formación continua.

formación en el ámbito de la ciberseguridad. Esto también beneficiará a una persona que quiera entrar en

en Ciberseguridad, pero no saben por dónde empezar. Para la mayoría de las personas que se suman a

conocimientos y competencias es más fácil que aprender algo completamente nuevo.

Con la misión de convertirse en un profesional de la ciberseguridad C-suite en este desafiante campo

Sabine investigó el esquema de responsabilidades del CISO:

Perfil 1

CISO

Misión

Define, mantiene y comunica la visión y la estrategia de ciberseguridad,

políticas y procedimientos y gestiona su aplicación en toda la

organización. Dirige las actividades relacionadas con la ciberseguridad en toda la organización.

Gestiona los vínculos/enlaces con autoridades externas y organismos profesionales.

La ambición de Sabine es identificar las lagunas de sus competencias para progresar en su carrera con un

credenciales debidamente alineadas al siguiente nivel.

Solución ECSF

MANUAL DEL USUARIO

SEPTIEMBRE 2022

49

Sabine investigó el PERFIL ECSF 1 e identificó lagunas en sus conocimientos:

Clave

conocimiento

✓ Conocimiento de normas, marcos y políticas de ciberseguridad y privacidad,

normativas, legislaciones, certificaciones y buenas prácticas

Comprensión de los requisitos éticos de las organizaciones de ciberseguridad

✓ Conocimiento de los controles de seguridad

Conocimiento de los modelos de madurez de ciberseguridad

✓ Conocimiento de tácticas, técnicas y procedimientos de ciberseguridad.

Conocimientos de gestión de recursos

Conocimiento de las prácticas de gestión

Conocimiento de los marcos de gestión de riesgos

Sabine decidió seguir el consejo de su mentor y asistir a una reunión del capítulo local de ISACA para ver si

era lo que buscaba. Quedó inmediatamente impresionada por las oportunidades que ofrecía. El capítulo

le dio una calurosa bienvenida y le presentó a varias personas clave de la sección, personas que trabajaban para la organización.

en el tipo exacto de funciones que buscaba Sabine y serían excelentes mentores o patrocinadores.

El presidente de certificación del capítulo informó a Sabine de que el Certified Information Security Manager

(CISM) sería una gran opción para ella, ya que demuestra un conocimiento completo de

seguridad de la información, así como sólidas capacidades de gestión. La certificación es para aquellos con cinco o

más años de experiencia, así que Sabine decidió hacer un plan de 18 meses para estudiar y obtener el

certificación.

Se afilió a ISACA como miembro esa misma noche y aprovechó al máximo los recursos que la

que la asociación ofrece tanto a escala mundial como local. Se incorporó a la asociación en línea

comunidades, empezaron a asistir a seminarios web y reuniones de las secciones locales ofrecidos a través de

SheLeadsTech, un programa ofrecido por la Fundación One in Tech de ISACA. Y asistió a

casi todas las reuniones que ofrecía la sección local.

A los seis meses de afiliarse, un compañero de la sección le propuso trabajar como

analista de seguridad de la información en su organización.

Resultado

Sabine es miembro de ISACA desde hace siete años. Obtuvo su certificación CISM

y pronto fue ascendida a directora de seguridad de la información. Ahora es directora de información

seguridad, con un camino claro hacia el puesto de CISO.

Además de encontrar credenciales y empleos a través de ISACA, Sabine también encontró varios recursos

que la ayudaron a añadir valor a su organización. Antes de la entrada en vigor del GDPR, Sabine pudo

aprovechar el Centro de Recursos GDPR ofrecido por ISACA para ayudarla a comprender la situación

a fondo y conocer cuáles eran los pasos más críticos que debía dar en su puesto actual.

El interés y la experiencia que adquirió en privacidad gracias a ese proyecto le permitieron

obtener la credencial de Ingeniero Certificado en Soluciones de Privacidad de Datos (CDPSE) de ISACA a través de su

programa de adopción anticipada.

Ha sido ponente en conferencias de ISACA a nivel nacional y de capítulo, perfeccionando su

de comunicación, y el año pasado asumió un puesto en la junta directiva de la sección. Como directora

MANUAL DEL USUARIO

SEPTIEMBRE 2022

50

ha tenido la oportunidad de contratar para algunos puestos, y la mayoría de sus contrataciones han procedido de la

ISACA, al igual que encontró su primer ascenso hace seis años. Habiendo visto el valor de

la certificación CISM en su propia carrera, ha empezado a ofrecer preparación para la certificación CISM a sus

equipo a través de la oferta de formación empresarial de ISACA.

El área de interés más reciente de Sabine, mientras se prepara para su puesto de CISO, es la seguridad de las empresas emergentes.

tecnologías. Dada la creciente atención que la normativa presta a la IA en Europa, ha dirigido sus esfuerzos a

en esa área en primer lugar, obteniendo recientemente un Certificado de Fundamentos de Inteligencia Artificial de

ISACA.

Siete años después de atravesar las puertas de su primera reunión del capítulo de ISACA, Sabine ha

ha ampliado su red con cientos de profesionales a escala local y miles a escala mundial. Es una

y oradora, y ahora es mentora de otras personas que en su día estuvieron en su misma situación.

posición. Entre los consejos que da a sus alumnos está el de estar siempre aprendiendo, y que ISACA, como

comunidad de aprendizaje global, es un gran recurso.

Sabine ha esbozado los pasos que hay que dar para llegar a la C-suite y planea ocupar un puesto de CISO dentro de cinco

años. Confía en que su red y credenciales ISACA serán una ventaja significativa

mientras persigue sus objetivos.

Trayectoria profesional:

- Analista SOC

- Analista de seguridad de la información

- Responsable de seguridad de la información

- Director de Seguridad de la Información.

B.7 CASO PRÁCTICO DE SANS/GIAC

Esta sección incluye partes del caso de uso escrito por SANS institute y GIAC (Global

Certificación de seguridad de la información)31

.

Por qué son importantes los marcos de trabajo y las certificaciones en ciberseguridad

La Directiva sobre redes e información (NIS) II es una actualización del mandato existente para la

Unión Europea. Ello contribuirá a fomentar un lenguaje común de ciberseguridad en toda una

sectores de la economía y requerirá el intercambio de información entre

de los Estados miembros e intersectorial. Directivas como ésta tienen cada vez más importancia en

establecer barreras de seguridad para las actividades cibernéticas. Para proteger el valor de los accionistas, la

La Comisión del Mercado de Valores (SEC) está estudiando un informe cibernético para las empresas que cotizan en bolsa.

exigir informes sobre cómo sus equipos de seguridad gestionarán el riesgo, los incidentes y la ciberseguridad.

experiencia del consejo de administración. El informe sobre la mitigación de los riesgos de seguridad se vinculará a las funciones de cada puesto

habilidades.

Los marcos están ayudando a articular estas funciones laborales. Hasta hace poco, la mayoría de las ofertas de empleo eran

listados genéricos que buscan profesionales de la ciberseguridad sin tareas bien definidas, habilidades o la

conocimiento de lo que se necesita para proteger los activos de la organización. Marcos de trabajo como

como el Marco Europeo de Competencias en Ciberseguridad (ECSF) están empezando a normalizar la

el talento necesario para puestos como respondedor a incidentes cibernéticos, investigador forense digital e investigador forense digital.

Director de Seguridad de la Información. La normalización permite a las organizaciones identificar

31 https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

talento para hacer frente a futuras amenazas. Esto está en consonancia con otras profesiones. Por ejemplo, los médicos tienen

áreas especializadas como radiólogos, pediatras y neurocirujanos que tienen la

experiencia necesaria en su área para proporcionar un tratamiento adecuado.

La certificación desempeña un papel importante en la preparación de las personas para determinadas funciones laborales. Certificación

valida al individuo utilizando las mejores prácticas y directrices para la educación y la

pruebas psicológicas, como las normas internacionales ISO/IEC 17024. Un ejemplo de

La certificación considerada la norma mundial es la de contable público certificado (CPA). Trabaje en

La experiencia puede convertir a alguien en experto, pero el CPA es la base respetada de un

profesional certificado e incluso puede ser un requisito para el cumplimiento en proyectos específicos o

auditorías.

Algunos ejemplos en los que los marcos de personal han contribuido al avance del sector de la ciberseguridad

incluyen:

- Las grandes empresas tecnológicas y financieras suelen tener varios equipos de seguridad que están normalizando

sus funciones y requisitos laborales a través del marco para recolocar y rotar

trabajadores rápidamente en función de la misión.

- Las organizaciones pueden trazar un mapa de la experiencia y certificación de su plantilla para emparejar rápidamente

competencias del personal con los requisitos del proyecto. Esto es especialmente importante para las consultoras,

empresas tecnológicas y contratistas.

- Los marcos proporcionan un lenguaje común en la mano de obra de distintos sectores como

tecnología, financiera, sanitaria, minorista y de servicios públicos, lo que permite a los equipos trabajar juntos para

proteger las amenazas a la seguridad cibernética y física.

- Los marcos ofrecen a las instituciones académicas un modelo para salvar la distancia entre

sus ofertas educativas y las competencias actuales en ciberseguridad necesarias en todo el

industrias, preparando a sus estudiantes para el empleo.

SANS y GIAC comprenden la importancia de los marcos de trabajo y han alineado cursos y

certificaciones a estos marcos. Los marcos son una plantilla para que las organizaciones estandaricen

requisitos del puesto, aunque cada organización y misión necesitará cierta personalización vinculada

a su misión específica. Hemos ayudado a diseñar e implantar programas de desarrollo de la mano de obra

programas que utilizan marcos como plantilla para empresas de Fortune 500, organismos gubernamentales,

y organizaciones de todos los tamaños.

TP-09-22-509-ES-N

SOBRE ENISA

La Agencia de Ciberseguridad de la Unión Europea, ENISA, es la agencia de la Unión dedicada a

alcanzar un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y

reforzada por la Ley de Ciberseguridad de la UE, la Agencia de Ciberseguridad de la Unión Europea

contribuye a la ciberpolítica de la UE, aumenta la fiabilidad de los productos, servicios y

procesos con sistemas de certificación de ciberseguridad, coopera con los Estados miembros y la UE

y ayuda a Europa a prepararse para los retos cibernéticos del mañana. A través del conocimiento

y sensibilización, la Agencia trabaja en colaboración con sus principales socios.

partes interesadas para reforzar la confianza en la economía conectada, impulsar la resiliencia de la

y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos. Más información en

Para más información sobre ENISA y su labor, visite: www.enisa.europa.eu.