cyVETsecurity

Co-funded by the Erasmus+ Programme of the European Union

# O1. Currículo para FP en materia de ciberseguridad

*Una herramienta para identificar competencias en ciberseguridad para diferentes perfiles profesionales*

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

Esta obra está licenciada bajo la Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visite http://creativecommons.org/licenses/by-nc-sa/4.0/ o envíe una carta a Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

CC_Attribution-Non Commercial-ShareAl

# TABLA DE CONTENIDOS

# 1. Introducción

De acuerdo a un reciente informe realizado por Intel Security, denominado "Hacking the Skills Shortage" (https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf) en 2019 (este mismo año) habrá entre uno y dos millones de puestos de trabajo relacionados con la ciberseguridad que quedarán sin cubrir. El informe incluye los resultados de un estudio realizado entre 775 poderes de decisión relacionados con el mundo IT y la seguridad de la información, respondiendo el 82% de ellos que existe una falta de competencias relacionadas con la ciberseguridad en su sector.

En la misma línea, un estudio de ESG de 2017 (Enterprise Strategy Group) mostraba que un 45% de organizaciones reconocen una problemática escasez de competencias en ciberseguridad (https://www.esg-global.com/blog/esg-research-suggests-cybersecurity-skills-shortage-is-getting-worse). Por supuesto, esto se aplica a todas las áreas relacionadas con la ciberseguridad, pero el informe de ESG menciona expresamente el impacto de esta escasez de competencias en la seguridad analítica y en las operaciones realizadas por las organizaciones.

En vista de un panorama que se muestra amenazante y cambiante a gran velocidad y de la revisión de la estrategia en ciberseguridad de la UE de 2013, enfrentar de forma conjunta los peligros relacionados con la ciberseguridad fue uno de los retos identificados durante la revisión a medio plazo del Mercado Único Digital. Por ello, el 13 de septiembre de 2017 la Comisión adoptó un paquete de medidas en materia de ciberseguridad.

Este paquete se lanzó en base a instrumentos ya existentes y presentó nuevas iniciativas para mejorar la resistencia y la respuesta de la UE a ciber ataques. Está en el interés estratégico de la UE que las herramientas tecnológicas en materia de ciberseguridad se desarrollen de forma que permitan florecer a economía digital al tiempo que se protege nuestra seguridad, nuestra sociedad y nuestra democracia. Esto incluye la

protección de hardware y software críticos. Para reforzar la capacidad en ciberseguridad de la UE, la Comisión y la Alta Representante han propuesto, entre otras prioridades y acciones, abordar el gap existente entre competencias y ciber defensa. Con este objetivo, la UE creó en 2018 una plataforma de formación en ciber defensa (ETEE), aunque no está disponible, al menos de momento, para el público en general.

Todos estos datos e iniciativas comentados representan la realidad del mundo de la información respecto a lo que concierne a la ciberseguridad y el proyecto CyVETsecurity se nutre de este protagonismo que la ciberseguridad está teniendo en las agendas europeas e internacional produciendo dos resultados que pretenden contribuir a reducir el gap entre competencias (y concienciación) en ciberseguridad y las necesidades reales, no sólo desde el punto de vista de las empresas sino de la sociedad en general.

El primero de estos dos resultados es este "currículo para formación profesional en materia de ciberseguridad", que es una selección del principal conocimiento, habilidades y competencias relacionadas con ciberseguridad desde una investigación exhaustiva realizada por el equipo del proyecto, que ha incluido las siguientes fuentes:

- El instituto SANS (**Escal Institute of Advanced Technologies),** una organización americana especializada en formación y certificación en seguridad y ciberseguridad.
- El National Institute of Standards and Technology (NIST), una agencia no reguladora de los Estados Unidos que ha desarrollado la certificación NIST 800-53 para un marco en ciberseguridad, aplicado por las principales organizaciones del mundo IT y tomado como referencia para la descripción de las distintas profesiones/funciones relacionadas con la ciberseguridad.
- La **International Organization for Standardization** (ISO), que proporciona una familia de estándares respecto a la seguridad de la información bajo la ISO/IEC 27000 .
- El marco DigiCom (**Marco Europeo para la Competencia Digital de la Ciudadanía**), que ofrece una descripción comprehensiva de conocimiento, habilidades y actitudes que toda persona necesita en el ámbito digital en 5 áreas clave, siendo la seguridad una de ellas.

Durante este proceso de investigación, encontramos que el conocimiento, habilidades y competencias relacionadas con la ciberseguridad se pueden agrupar de la siguiente manera (de acuerdo al SANS Institute), en estas áreas:

- **Detección de intrusos.** Incluye descubrir actividad potencialmente dañina que pueda comprometer la confidencialidad, integridad o disponibilidad de la información. Hay varios tipos de detección de intrusos. La detección basada en la red pretende detectar comportamiento no autorizado basado en el tráfico de una determinada red. La detección basada en el hosting busca encontrar actividad ilícita en un aparato específico. La detección física se centra en la identificación de amenazas en sistemas físicos.
- **Desarrollo de software seguro.** La mayor parte de filtraciones de datos se deben a vulnerabilidades o debilidades en el código del software y el software comercial necesita ser parcheado de forma regular.
- **Prevención o reducción de riesgos.** Incluye el seguimiento de riesgos identificados, el descubrimiento de nuevos riesgos y el seguimiento de riesgos a lo largo de un proyecto. Primero es necesario entender qué datos se necesitan proteger y porqué. Las organizaciones deben identificar sus activos más valiosos y las posibles amenazas que pueden ponerlos en peligro. Saber cómo se almacena la información, quién tiene acceso a ella y cómo se protegen los datos son tres cuestiones críticas para una protección de datos óptimo.
- **Seguridad en la nube.** Existen varias amenazas específicas de la seguridad en la nube. Algunos de los principales peligros incluyen la filtración de datos, la explotación de vulnerabilidades de los sistemas, el hackeo de cuentas, un uso inadecuado o negligente y el malware.
- **Supervisión de la red y gestión de accesos.** Las organizaciones necesitan profesionales que sepan qué buscar y puedan tomar decisiones rápidas cuando se detectan comportamientos sospechosos.
- **Análisis de seguridad.** Para construir soluciones innovadoras para prevenir que los hackers entren a redes corporativas y roben datos sensibles.
- **Seguridad de datos**. Especialmente importante para organizaciones en campos vulnerables, como la salud o los servicios financieros.

**¿Qué encontrarás en este documento?**

Tomando las áreas mencionadas como base, hemos definido diferentes unidades de competencia, resultados de aprendizaje y criterios de evaluación asociados, y lo hemos hecho teniendo en cuenta distintos perfiles profesionales.

En el siguiente capítulo explicaremos qué metodología hemos usado para hacerlo y construir nuestro curriculum para FP en materia de ciberseguridad, pero primero nos gustaría explicarte cómo puedes usar este documento.

- Si eres un profesor o profesora de FP, puedes usar el currículum completo o partes de él. Dependiendo de tu alumnado (alumnado en ciclos de FP reglada, empleados/desempleados que desean mejorar su formación…) y de los objetivos de la formación, tal vez sólo necesites algunas unidades, la mayor parte o incluso todas. Sin importar el número de unidades que utilices, puedes introducir "píldoras" y prácticas relacionadas con la ciberseguridad y la seguridad de la información en cualquier programa de FP existente y/o diseñar nuevos programas de formación cogiendo total o parcialmente nuestro currículo tal como es o adaptándolo y completándolo con cualquier otro contenido que encuentres relevante. Respecto a la impartición, también hemos producido materiales formativos que cubren las distintas unidades de competencia que hemos definido (podrás encontrarlos en nuestro resultado número 2 "Retos sobre ciberseguridad". Puedes usar ambos documentos juntos o de forma separada pero ten en cuenta que el resultado número 2 se ha basado en el resultado 1 (este documento que estás leyendo).
- Si eres una empresa, puedes usar ambos resultados para la formación interna de tus trabajadores y trabajadoras o incluso sólo este resultado número 1 para solicitar a un proveedor de formación el diseño de una acción que cubra las unidades que son importantes para tu organización. También puedes usar este documento como apoyo para definir el perfil de un futuro trabajador o trabajadora durante un proceso de selección y contratación.
- Si eres una autoridad educativa a cargo del diseño de un currículo, puedes encontrar este resultado interesante para conocer qué unidades podrían ser interesantes de cara a su implantación en una variedad de programas de FP (o en otros niveles educativos) o

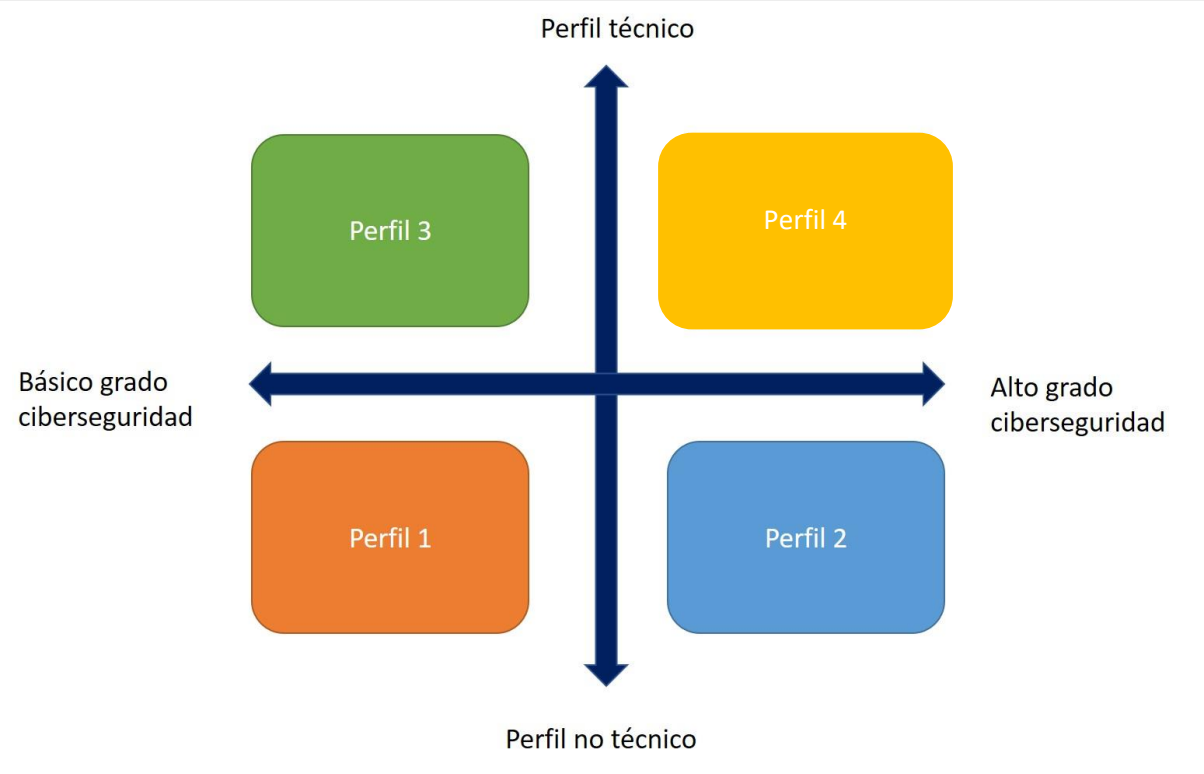
incluso para definir una formación especializada en ciberseguridad. La bibliografía utilizada y referenciada en el último capítulo también puede resultarte de utilidad.

El currículo que proponemos ha sido construido siguiendo una estructura modular, (resultados de aprendizaje, RAs, agrupados en unidades para ser impartidos de forma conjunta o independiente) en la forma de una matriz, siendo las filas las unidades de competencia y los resultados de aprendizaje y criterios de evaluación asociados, las columnas.

## 2. Metodología

Tomando como base las áreas de conocimiento descritas en el capítulo anterior, nuestro paso siguiente fue caracterizar distintos perfiles profesionales y su relación con la ciberseguridad.

Definimos 4 tipos de perfiles:



- **Perfil 1** se refiere a profesionales con un perfil no técnico y que no necesitan un alto grado de conocimiento y habilidades en materia de ciberseguridad dada la naturaleza de su trabajo, sólo aquéllos necesarios para prácticamente cualquier persona. Podríamos hablar de alguien que trabaja o estudia cocina, mecánica de vehículos, fontanería, cuidados a dependientes… Las unidades de competencia definidas se centran sobre todo en la concienciación (higiene en ciberseguridad) y en tipos de amenazas, buenas prácticas en el uso de redes sociales, protección frente a las amenazas más habituales.

- **Perfil 2** incluye profesionales con un perfil no técnico pero que necesitan un grado de conocimiento y habilidades en ciberseguridad mayor debido a la naturaleza de su trabajo, principalmente porque gestionan información sensible (por ejemplo, alguien que trabaja en un banco, en contabilidad, en una compañía de seguros, en la administración de un hospital…). Las unidades de competencia definidas se centran principalmente en la protección de datos (regulación y leyes…) y en el almacenamiento, manejo e intercambio seguro de datos.

- **Perfil 3** reúne a profesionales con perfiles técnicos pero que necesitan sólo conocimiento y habilidades relacionadas con la ciberseguridad limitadas a aquéllas directamente relacionadas con su trabajo. Pensamos fundamentalmente en perfiles industriales en el contexto de una fábrica interconectada y digital (por ejemplo, un programador/a CNC, trabajo con robots conectados…). Las unidades de competencia para este perfil se centran en la ciberseguridad relacionada con la conexión entre el mundo OT (tecnologías de la operación) y el mundo IT (tecnologías de la comunicación).

- **Perfil 4** se refiere a profesionales con un perfil técnico (origen en IT) y con conocimiento y habilidades especializadas en ciberseguridad, teniendo en mente profesiones relacionadas fundamentalmente con el mundo IT (analistas, gestores de redes, desarrolladores de software…) dentro de la formación profesional. Las unidades de competencia se centran en el análisis de vulnerabilidades, gestión de seguridad, seguridad perimetral y análisis forense.

Estos 4 perfiles fueron definidos y descritos durante la primera reunión del proyecto en Tallinn. Antes de proseguir, debemos realizar una aclaración. Los perfiles no se refieren a ningún nivel EQF[1] en particular. Será la definición de los resultados de aprendizaje (RAs) junto con los criterios de evaluación asociados los que proporcionarán "las pistas" para decidir si es factible impartir las unidades de competencia definidas a los distintos públicos objetivo (junto a los perfiles profesionales definidos anteriormente). No obstante, cuando diseñamos el curriculum sí que tuvimos en cuenta lo siguiente:

- Las unidades relacionadas con el perfil 1 se definieron tomando en consideración cualquier nivel o cualquier programa de FP, ya que cubren aspectos básicos de la ciberseguridad que pueden (y deberían) ser aplicados tanto a nivel profesional como personal. Digamos que se centran en la ciber higiene y concienciación que es escasamente enseñada en programas de FP y cubren competencias digitales básicas de las que, no obstante, carece la mayoría de la población (ver https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework y http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf)
- Las unidades identificadas para el perfil 2 se definieron teniendo en mente un nivel EQF entre 3 y 5 (aunque no es excluyente su aplicación en otros niveles si el/la docente lo considera oportuno). Pensamos en ciclos de grado medio y superior relacionados con la administración, finanzas, sanidad o comercio.
- Las unidades del perfil 3 se definieron teniendo en cuenta un nivel EQF entre 3 y 5 (aunque no se excluye su aplicación en otros niveles si el/la docente lo considera oportuno) y perfiles industriales tales como programación de la producción, robótica y automatización, electricidad, energía o electrónica.

[1] EQF, *European Qualifications Framework*, es el marco común de referencia europeo que relaciona entre sí los sistemas de cualificación de los distintos países y sirve de mecanismo de conversión para mejorar la interpretación y comprensión de las cualificaciones de diferentes países y sistemas de Europa. Establece 8 niveles que abarcan toda la gama de cualificaciones, desde el nivel básico (nivel 1, como pueden ser los títulos de educación básica) hasta los más avanzados (nivel 8, por ejemplo, el doctorado)

- Por último, las unidades pensadas para el perfil 4 encajarían más adecuadamente con un nivel EQF 4-6 y teniendo en cuenta perfiles con conocimientos previos en IT, tales como desarrolladores/as de apps, programación o gestión de redes y sistemas de comunicación.

La definición de RAs y criterios de evaluación identificados para cada unidad fue una de las partes más difíciles de este documento. La información disponible es realmente extensa de modo que seleccionar y definir unidades específicas fue también difícil. La forma de superar este reto fue tener en mente en todo momento los perfiles definidos así como las áreas de conocimiento en materia de ciberseguridad definidas por el SANS Institute. Simplificar la cantidad de información en la definición de resultados de aprendizaje también fue un proceso complejo que pasó por distintas fases, comenzando por unos 12-20 RAs por unidad (¡y aún más criterios de evaluación!) hasta agrupar RAs de forma que las unidades fueran más gestionables, uniendo y simplificando algunos RAs. A continuación se presenta un ejemplo, donde pasamos de esto:

| UNIDADES DE COMPETENCIA | RESULTADOS DE APRENDIZAJE |
|---|---|
| **Unidad 1. Test de penetración** | U1LO1. El alumno/a es capza de determinar el nivel de seguridad de capacidades desarrolladas basadas en resultados del test. |
| | U1LO2. El alumno/a es capza de testar planes para tratar con especificaciones y requerimientos. |
| | U1LO3. El alumno/a es capza de instalar y mantener la infraestructura de red de un sistema operativo de un dispositivo (por ejemplo, IOs, firmware…) |
| | U1LO4. El alumno/a es capaz de realizar recomendaciones basadas en los resultados del test. |
| | U1LO5. El alumno/a es capaz de determinar el alcance, infraestructura, recursos y tamaño de la muestra de datos para asegurar que los requisitos del sistema son adecuados. |
| | U1LO6. El alumno/a es capaz de validar especificaciones y requerimientos para su testeo. |
| | U1LO7. El alumno/a es capaz de analizar los resultados del testeo de software, hardware e interoperabilidad. |
| | U1LO8. El alumno/a es capaz de realizar tests en sistemas bajo desarrollo. |
| | U1LO9. El alumno/a es capza de realizar test de interoperabilidad en sistemas que intercambian información electrónica con otros sistemas. |
| | U1LO10. El alumno/a es capza de realizar testeo operacional. |
| | U1LO11. TEl alumno/a es capza de testear, evaluar y verificar hardware y software para determinar si cumplen con las especificaciones requeridas. |
| | U1LO12. El alumno/a es capza de registrar y gestionar los datos de testeo. |
| | U1LO13. El alumno/a es capza de desarrollar y dirigir sistemas de testeo y procedimientos de validación y documentación. |
| | U1LO14. El alumno/a es capza de identificar y dirigir la solución de problemas técnicos encontrados durante el testeo o la implantación de nuevos sistemas. |
| | U1LO15. El alumno/a es capza de identificar, valorar y recomenadr ciberseguridad o productos que facilitan la ciberseguridad para sus uso en un sistema y asegurar que los productos recomendados cumplen los requisitos de evaluación y validación de la empresa. |
| | U1LO16. El alumno/a es capza de realizar análisis de riesgos (por ejemplo, de amenazas, vulnerabilidades y probabilidad de suceso) cuando una aplicación o sistema sufre un cambio importante. |
| | U1LO17. El alumno/a es capza de utilizar modelos o simulaciones para analizar o predecir el funcionamiento de un sistema bajo distintas condiciones de operatividad. |
| | U1LO18. El alumno/a es capza de testear y evaluar interfaces seguras entre sistemas de información, sistemas físicos y/o tecnologías integradas. |
| | U1LO19. El alumno/a es capza de realizar una evaluación de riesgos en la seguridad de la información. |
| | U1LO20. El alumno/a es capza de realizar revisiones de seguridad e identificar gaps de seguridad en la arquitectura. |

A esto:

| UNIDADES DE COMPETENCIA | RESULTADOS DE APRENDIZAJE |
|---|---|
| **Unidad 1. Test de penetración** | U1LO1. El alumno/a es capaz de identifcar las fases de un proceso de auditoría |
| | U1LO2. El alumno/a es capaz de recopilar evidencias |
| | U1LO3. El alumno/a es capaz de buscar y explotar vulnerabilidades |
| | U1LO4. El alumno/a es capaz de hacer un informe de vulnerabilidades |

En algunos casos, realizamos esta simplificación por nuestra cuenta, pero en el caso de los perfiles 3 y 4 (más complicados en términos de contenido) contamos con la ayuda de empresas asociadas de España y Holanda.

Una última cuestión a tener en cuenta es que los perfiles no son necesariamente excluyentes, es decir, aunque hemos definido unidades para distintos perfiles profesionales, es posible intercambiarlas a tu conveniencia e impartir una unidad de competencia dirigida en principio al perfil 2 al 3 (y viceversa). Esto dependerá de tu grupo objetivo y de tus intenciones. En el diseño de retos hemos tenido esto en cuenta y para cada uno hemos definido qué conocimiento previo se necesita para llevar a cabo el reto. Incluso podrías mezclar los perfiles, para que trabajaran juntos en la resolución de retos, obteniendo un enfoque más multidisciplinar.

# 3. El currículo CyVETsecurity

| | UNIDADES | RESULTADOS DE APRENDIZAJE | CRITERIOS DE EVALUACIÓN |
|---|---|---|---|
| Perfil 1 | Unidad 1. Protección de dispositivos y contenido digital | **U1LO1**. El alumno/a es capaz de identificar riesgos físicos y virtuales asociados a la tecnología | El alumno/a identifica tres tipos de riesgos físicos y tres virtuales. |
| | | **U1LO2**. El alumno/a es capaz de implementar las estrategias para prevenir riesgos y se auto actualiza en esta materia | El alumno/a describe una estrategia para prevenir ciberataques. |
| | | **U1LO3**. El alumno/a es capaz de instalar y actualizar software anti malware | El alumno/a instala/actualiza software anti malware en un dispositivo dado. |
| | | **U1LO4**. El alumno/a es capaz de protegerse frente al fraude a través del uso de contraseñas seguras | El alumno/a genera y testea una contraseña segura. |
| | | **U1LO5**. El alumno/a es capaz de proteger distintos dispositivos vulnerables a distintas amenazas digitales (malware, phishing, etc.) | El alumno/a identifica dispositivos potencialmente vulnerables y posibles mecanismos para su protección. |
| | | **U1LO6**. El alumno/a es capaz de identificar información sensible/valiosa así como ataques a distintos tipos de datos | El alumno/a identifica datos sensibles y posibles ataques dependiendo de la naturaleza de los datos. |
| | Unidad 2. Protección de datos personales e identidad digital | **U2LO1**. El alumno/a es capaz de adecuar su comportamiento en el mundo digital y gestionar su huella digital adecuadamente. | El alumno/a conoce la LOPD.<br>El alumno/a describe cómo funciona Google analytics.<br>El alumno/a entiende y explica el concepto de huella digital. |
| | | **U2LO2**. El alumno/a es capaz de identificar los peligros de que su identidad sea robada o utilizada indebidamente por otros. | El alumno/a identifica escenarios donde puede haber un uso indebido de sus datos.<br>El alumno/a describe el término "robo de identidad" y valora el riesgo de que suceda. |
| | | **U2LO3**. El alumno/a es capaz de proteger información relevante para otra persona de su entorno (como un compañero de trabajo, una amiga...) | El alumno/a identifica técnicas asociadas a la protección de identidad e información. |
| | | **U2LO4**. El alumno/a es capaz de encontrar, borrar y/o modificar información on-line sobre sí mismo/a. | El alumno/a explica cómo borrar/modificar información personalmente identificable (PII) contenida en una organización.<br>El alumno/a recopila su huella digital. |
| | | **U2LO5.** El alumno/a es capaz de gestionar su propio rastro digital. | El alumno/a gestiona su huella digital. |
| | | **U2LO6**. El alumno/a es capaz de actuar de forma crítica cuando comparte información on-line sobre sí mimo/a. | El alumno/a demuestra técnias apropiadas cuando comparte información personalmente identificable (PII) on-line. |
| | | **U2LO7**.El alumno/a es capaz de hacer uso de múltiples identidades digitales, dirigidas a diferentes objetivos. | El alumno/a crea múltiples cuentas en redes sociales y diferencia entre contenido profesional y personal entre ellas. |

| | | | |
|---|---|---|---|
| Perfil 2 | **Unidad 3. Gestión de la seguridad de la información y regulación** | **U3LO1**. El alumno/a es capaz de entender la importancia de la seguridad de la información y su significado para la organizacón. | El alumno/a explica claramente cuáles son las indicaciones de la organización respecto a la seguridad de la información.<br>El alumno/a sugiere mejoras las indicaciones proporcionadas. |
| | | **U3LO2**. El alumno/a es capaz de identificar leyes básicas, regulaciones y principios éticos de ciberseguridad y seguridad de la información (por ejemplo la LOPD o la ISO 27.000). | El alumno/a identifica conceptos clave, regulaciones y procedimientos de seguridad de la información y ciberseguridad.<br>El alumno/a aplica regulaciones relacionadas con la seguridad de la información. |
| | | **U3LO3**. El alumno/a es capaz de planificar su propio trabajo basado en las instrucciones sobre seguridad de la información en su puesto. | El alumno/a trabaja aplicando instrucciones sobre seguridad de la información. |
| | | **U3LO4**. El alumno/a es capaz de trabajar aplicando seguridad en las comunicaciones de datos: confidencialidad, integridad y disponibilidad. | El alumno/a es capaz de explicar el significado de confidencialidad, integridad y disponibilidad.<br>El alumno/a explica las posibles consecuencias de romper la confidencialidad en la información. |
| | | **U3LO5**. El alumno/a es capaz de impartir formación en seguridad al personal con quien trabaja: indicaciones en seguridad, control y supervisión. | El alumno/a prepara un breve conjunto de instrucciones relacionadas con la seguridad de la información para una organización o personal de una organización. |
| | **Unit 4. Seguridad de la información como parte de la seguridad de una organización** | **U4LO1.** El alumno/a es capaz de observar, evaluar, prevenir e informar sobre riesgos de información en el puesto de trabajo | El alumno/a nombra las amenazas a la seguridad de datos y los riesgos que existen en su trabajo diario.<br>El alumno/a aplica medidas para la protección de datos. |
| | | **U4LO2**. El alumno/a es capaz de utilizar los sistemas de seguridad de la organización en relación con la seguridad de la información. | El alumno/a usa los sistemas de seguridad de la organización en relación con la seguridad de la información. |
| | | **U4LO3.** El alumno/a es capza de gestionar la seguridad física en las instalaciones | El alumno/a identifica diferentes situaciones de seguridad física en la organización. |
| | | **U4LO4**. El alumno/a es capaz de trabajar de forma segura con su móvil y los servicios en la nube. | El alumno/a aplica medidas para trabajar de forma segura en un ambiente |
| | | **U4LO5.** El alumno/a es capaz de asegurar el almacenamiento material y de datos y su protección. | El alumno/a almacena y protege material y datos. |
| | | **U4LO6.** El alumno/a es capaz de aplicar principios básicos de seguridad del software: sistemas operativos, aplicaciones… | El alumno/a usa las aplicaciones y dispositvos personales de forma segura |
| | **Unit 5. Introducción a la ciber defensa** | **U5LO1**. El alumno/a es capaz de identificar información crítica de distintos medios. | El alumno/a analiza críticamente información adquirida de distintos medios, identificando la más vulnerable |
| | | **U5LO2**. El alumno/a es capaz de evaluar la vulnerabilidad de infraestructura crítica para la sociedad. | El alumno/a identifica vulnerabilidades de la infraestructura crítica de la sociedad. |
| | | **U5LO3**. El alumno/a es capaz de identificar ciber ataques y ciber amenazas | El alumno/a enumera ciber ataques y amenazas comunes y probables teniendo en cuenta la información que gestiona en su trabajo. |

| | | | |
|---|---|---|---|
| Perfil 3 | **Unidad 6. Conocimiento básico IT para OT** | **U6LO1.** El alumno/a es capaz de aplicar conocimiento básico sobre networking (cisco, hp…) | El alumno/a define qué es una red básica, qué es routing/switching o portfordwarding básicos. |
| | | **U6LO2**. El alumno/a es capaz de identificar los principios básicos de la ciberseguridad | El alumno/a define los principios básicos de la ciberseguridad y entiende qué significan. |
| | | **U6LO3**. El alumno/a es capaz de identificar los principios básicos de la GDPR en cuanto a usos de datos personales. | El alumno/a explica lo que significa GDPR en cuanto al uso de datos personales. |
| | | **U6LO4.** El alumno/a es capaz de identificar una contraseña compleja. | El alumno/a explica cómo funciona una contraseña compleja, por qué es conveniente usar contraseñas distintas en cada plataforma y cómo funcionan las contraseñas a nivel de bits. |
| | | **U6LO5**. El alumno/a es capaz de usar Windows/linux/macos de forma básica. | El alumno/a usa adecuadamente 2 de esos sistemas operativos. |
| | | **U6LO6**. El alumno/a es capaz de describir los viruses o amenazas más comunes en distintos sistemas operativos. | El alumno/a hace un pequeño resumen de los viruses más comunes en linux/Windows/Macos |
| | **Unidad 7. Procedimientos en la empresa y máquinas** | **U7LO1**. El alumno/a es capaz de aplicar los procedimientos de la empresa, detectando posibles problemas relacionados con la seguridad e informando a un/a especialista sobre ellos. | El alumno/a aplica el procedimiento cuando se detecta una brecha en la seguridad de la empresa<br>El alumno/a se comunica con el/a especialista en IT de forma clara y entendible. |
| | | **U7LO2**. El alumno/a es capaz de detectar mal funcionamiento en una máquina o brechas en su seguridad. | El alumno/a explica 3 ejemplos de brechas posibles en la seguridad de la máquina y cómo actuar. |
| | | **U7LO3**. El alumno/a es capaz de identificar los riesgos de conectar un USB aleatorio en la red de la empresa, en una máquina o un ordenador. | El alumno/a explica por qué no se debe conectar un USB aleatorio en la red de la empresa, los riesgos que conlleva y cómo prevenirlos. |
| | | **U7LO4.** El alumno/a es capaz de interpretar una herramienta de monitorización y detectar tráfico inusual. | El alumno/a usa una herramienta de monitorización (como wireshark) para leer una lista de tráfico en la red, evaluando si existen anomalías.<br>El alumno/a comunica posibles amenazas a un/a especialista en seguridad de forma clara y aplicando el protocolo de la empresa. |
| | | **U7LO5.** El alumno/a es capaz de aplicar protocolos de redes (routing/VPN/PF/, etc…) | El alumno/a explica las bases del establecimiento de redes, no desde un punto de vista IT pero a nivel básico de usuario. |
| | **Unidad 8. GDPR/LOPD y protección de datos** | **U8LO1**. El alumno/a es capaz de identificar la regulación sobre protección aplicable en su país y a nivel europeo. | El alumno/a hace un resumen de la LOPD/GDPR en su país.<br>El alumno/a busca información relevante respecto a la protección de datos aplicable a su actividad, usando la fuente adecuada. |
| | | **U8LO2**. El alumno/a es capaz de trabajar de forma segura con datos conectados a distintos tipos de máquinas usadas en el trabajo. | El alumno/a identifica información sensible que puede ser susceptible de ser afectada por regulaciones sobre protección de datos. |

| | | | |
|---|---|---|---|
| Perfil 4 | **Unidad 9. Test de penetración** | **U9LO1**. El alumno/a es capaz de identificar y aplicar las fases de un proceso de auditoría. | Las fases del proceso de auditoría están claramente identificadas.<br>El test se realiza siguiendo las fases del proceso de auditoría, evaluando y verificando el hardware y/o software para determinar el cumplimiento con las especificaciones definidas. |
| | | **U9LO2**. El alumno/a es capaz de recopilar evidencias. | El alcance, infraestructura, recursos y muestra de datos para asegurar los requisitos del sistema se demuestran de forma correcta.<br>Los datos para el test están adecuadamente registrados y gestionados. |
| | | **U9LO3**. El alumno es capaz de buscar y explotar vulnerabilidades. | Se utilizan modelos y simulaciones para analizar o predecir la actuación de los sistemas.<br>Los resultados del software, hardware o test de interoperabilidad se analizan correctamente.<br>La evaluación de interfaces seguras entre sistemas de información, físicos y/o tecnologías integradas se realiza para buscar vulnerabilidades. |
| | | **U9LO4**. El alumno/a es capaz de hacer un informe de vulnerabilidades | Las vulnerabilidades y gaps de seguridad en la arquitectura se identifican correctamente.<br>Las recomendaciones basadas en el test se dan de forma concreta y clara. |
| | **Unidad 10. Gestión y gobernanza de seguridad** | **U10LO1**. El alumno/a conoce y entiende los estándares y regulaciones de seguridad (ISO, ISACA, NIST). | Las mejores prácticas en gestión IT por el uso de marcos bien conocidos (como ITL) está correctamente explicado.<br>Los estándares de seguridad en la gestión de la información (como ISO/IEC 27001/27002) se aplican. |
| | | **U10LO2**. El alumno/a es capaz de implantar un sistema de gobierno de la seguridad de la información. | Se explica el rol de la información desde un punto de vista estratégico.<br>Los roles y stakeholders en la tecnología de la información están identificados.<br>La estrategia de negocio e IT están alineadas.<br>Se dan recomenaciones sobre cómo deben gestionarse los datos en la organización. |
| | | **U10LO3**. El alumno/a es capaz de realizar un análisis de riesgos. | La evaluación de amenazas y vulnerabilidades como parte del impacto del negocio es analizada.<br>Se actualiza la documentación de seguridad basándose en los resultados de la supervisión. |
| | | **U10LO4**. El alumno/a es capaz de trabajar aplicando regulaciones sobre información personal (LOPD) | Se toman en cuenta las regulaciones nacionales e internacionales sobre la protección de datos. |
| | **Unidad 11. Desarrollo de seguridad** | **U11LO1.** El alumno/a es capaz de identificar técnicas de programación seguras. | Se desarrollan o integran diseños de ciberseguridad para sistemas y redes.<br>Se emplean procesos de gestión de configuración seguros.<br>La programación se realiza teniendo en cuenta medios de protección para minimizar la intrusión. |
| | | **U11LO2**. El alumno/a es capaz de desarrollar apps con posesión de información (certificados, protocolos, firmas…) | Las apps se desarrollan aplicando permisos basados en firmas digitales.<br>El acceso a proveedores de contenidos de las apps está deshabilitados.<br>Las apps se desarrollan añadiendo una configuración de seguridad de red. |
| | | **U11LO3**. El alumno/a es capaz de desarrollar apps sin filtraciones de datos (autorización, acceso) | Las apps se desarrollan almacenando los datos privados de forma interna.<br>Se comprueba la validez de los datos. |
| | | **U11LO4**. El alumno/a es capaz de trabajar de acuerdo a regulaciones (ASVS) | El diseño, desarrollo y testeo de aplicaciones web se realiza observando los Estándares de Verificación de Seguridad de Aplicaciones (ASVS) |

| | | |
|---|---|---|
| **Unit 12. Análisis forense** | **U12L01**. El alumno/a es capaz de identificar y aplicar fases del análisis forense. | Se identifican y siguen las fases cuando se aplica un análisis forense.<br>Los hallazgos se proporcionan de acuerdo a los procedimientos de informe establecidos. |
| | **U12L02**. El alumno/a es capaz de clonar dispositivos. | Se realizan buenos duplicados de discos duros, floppy diskettes, CDS, teléfonos móviles o GPS. |
| | **U12L03**. El alumno/a es capaz de realizar diversos análisis. | Se conduce el análisis de archivos de acceso, evidencias y otra información para determinar los mejores métodos para identificar a los intrusos a una red.<br>Se identifica la información a la que ha accedido un intruso.<br>Se captura y analiza el tráfico de una red asociado con actividades maliciosas. |
| | **U12L04**. El alumno/a es capaz de recuperar información | Los datos recuperados se examinan para determinar la relevancia de la intrusión.<br>Los datos se extraen usando técnicas de data carving (Toolkit forense, Foremost...)<br>Los datos registrados se desencriptan. |
| **Unidad 13. Seguridad perimetral** | **U13L01**. El alumno/a es capaz de implementar técnicas de seguridad en la comunicación | Los servidores Web y de e-mail se han asegurado:<br>Se ha configurado un firewall para la seguridad del servidor.<br>Se asegura la protección de los servidores DNS y DHCP.<br>Se comunican los requisitos de seguridad a otros departamentos de la organización. |
| | **U13L02**. El alumno/a es capaz de diseñar e implementar una red de acuerdo al modelo de seguridad | Se identifican fallos potencialmente críticos.<br>Se realizan acciones para mitigar los efectos de posibles fallos.<br>Se encriptan las conexiones de red.<br>Las redes inalámbricas se protegen con sistemas de encriptado y contraseña.<br>El almacenamiento de backups es automático en una red local o global y protegidda de uso no autorizado. |
| | **U13L03**. El alumno/a es capaz de identificar sistemas de gestión de autentificación e identidad (SSO). | Se implementa el modelo AAA (autentificación, autorización y justificación).<br>Se gestiona la política VPN.<br>Los sistemas single sign-on están integrados en las apps Web y móviles. |
| | **U13L04**. El alumno/a es capaz de identificar soluciones de gestión de eventos | Los principales proveedores de sistemas SIEM se han identificado.<br>Se selecciona la mejor solución que combina las necesidades de la organización y la eficiencia presupuestaria. |

## 4. Bibliografía


- International Organization of Standardization. *ISO/IEC 27000:2018*
  https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
- European Digital Competence Framework for Citizens. *DigComp into Action. A user guide to the European Digital Competence Framework.* http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110624/dc_guide_may18.pdf
- National Institute of Standards and Technology. National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework. 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). *Marco Común de Competencia Digital Docente*. 2017. https://aprende.intef.es/sites/default/files/2018-05/2017_1020_Marco-Com%C3%BAn-de-Competencia-Digital-Docente.pdf