Co-funded by the European Union

NIVEL 4-5 EQF

MÓDULOS DE FORMACIÓN PARA ESTUDIANTES DE FP

CYBER AGENT 01.2025

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

Financiado por la Unión Europea. No obstante, las opiniones y puntos de vista expresados son exclusivamente los de los autores y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva en el ámbito Educativo, Audiovisual y Cultural (EACEA). Ni la Unión Europea ni la EACEA se hacen responsables de ellos.

www.cyberagents.eu

Paquete de trabajo 3: Desarrollo de recursos de aprendizaje para agentes del cambio en ciberseguridad

Entrega 3.2: Módulos de formación para estudiantes de FP
Líder del 3.2: TIMTAL (TR)

CONTENIDO

LISTA DE TABLAS

INTRODUCCIÓN

Los rápidos cambios en la ciencia y la tecnología, las necesidades cambiantes de las personas y la sociedad, las innovaciones y los avances en las teorías y enfoques de aprendizaje y enseñanza han afectado directamente a las funciones que se esperan de las personas. Este cambio define a una persona que produce conocimiento, puede utilizarlo de manera funcional en la vida, puede resolver problemas, pensar de forma crítica, es emprendedora, decidida, tiene habilidades de comunicación, puede empatizar, contribuye a la sociedad y la cultura, etc.

La vertiginosa velocidad que ha traído consigo la era de la información conlleva necesidades en constante cambio por parte de las personas y las sociedades. Las innovaciones en las teorías de aprendizaje y enseñanza están cambiando radicalmente las funciones que se esperan de las personas. Ahora, no solo se trata de tener conocimientos, sino también de habilidades como ser capaz de utilizar esos conocimientos de manera funcional en la vida, ser capaz de producir soluciones a problemas complejos, ser capaz de pensar de manera crítica, ser capaz de actuar con espíritu emprendedor, ser capaz de comunicarse de manera eficaz, ser capaz de mostrar empatía y añadir valor a la sociedad. Esta transformación anima a las personas a aprender, adaptarse y mejorar constantemente.

En este contexto, la formación profesional también está experimentando una gran transformación. Las profesiones tradicionales están siendo sustituidas por otras nuevas, centradas en la tecnología y en constante desarrollo. La ciberseguridad es de vital importancia en este cambio. Porque en el mundo digitalizado, los riesgos de ciberseguridad están aumentando en todos los sectores y todas las profesiones. La ciberseguridad desempeña un papel fundamental en muchos ámbitos, desde los datos personales hasta la protección de los secretos empresariales, desde la seguridad de las infraestructuras críticas hasta la seguridad de las transacciones financieras.

La importancia de la formación en ciberseguridad en la educación profesional no se limita a las habilidades técnicas. También incluye la formación de personas con valores éticos, un alto sentido de la responsabilidad, familiarizadas con la normativa legal y abiertas al aprendizaje continuo. Porque la ciberseguridad no es solo un problema técnico, sino también una responsabilidad social. Por lo tanto, dar la importancia necesaria a la formación en ciberseguridad en la educación profesional es un paso fundamental para el futuro tanto de las personas como de la sociedad.

La formación profesional incluye la planificación, la investigación, el desarrollo, la organización y la gestión coordinada, la supervisión y las actividades docentes de todos los servicios de formación profesional y técnica, junto con los sectores de la agricultura, la industria y los servicios, dentro de la integridad del sistema educativo. El objetivo de estas actividades educativas es formar a personas expertas que garanticen la continuidad de la sociedad y el personal cualificado necesario en todas las etapas de la producción, y hacer hincapié en la formación profesional.

El programa de formación profesional Cyber Agent (EQF4-5) está diseñado para preparar a las personas para la vida en el ámbito de la ciberseguridad y se basa en las necesidades del mercado laboral y en el análisis de los puestos de trabajo. El plan de estudios de Cyber Agent tiene como objetivo proporcionar los conocimientos, las habilidades, las actitudes y los comportamientos que se deben poseer para realizar el trabajo y las transacciones pertinentes a través de lecciones y logros, mientras que, por otro lado, las actividades educativas se planifican de manera que preparen a las personas para la vida empresarial de acuerdo con este marco.

1. OBJETIVOS DEL PROGRAMA CYBERAGENT EQF NIVEL 4-5

La necesidad de ciberseguridad se ha vuelto muy importante, especialmente en los países de la UE, así como en todo el mundo, y ha aumentado rápidamente en los últimos años. Simultáneamente con los avances tecnológicos, los riesgos y amenazas cibernéticos también han cambiado a la misma velocidad y se han vuelto complejos. Los riesgos y amenazas cibernéticos han alcanzado un potencial que causará resultados mucho más amplios y negativos que los ataques físicos. Con sectores como las finanzas, las comunicaciones electrónicas, la energía, el transporte y la aviación prestando servicios en un entorno digital seguro, garantizar la ciberseguridad nacional se ha convertido en una de las principales prioridades de nuestro país. En este contexto, se pretende difundir la educación en materia de ciberseguridad en la educación formal e informal, y desarrollar y enriquecer los contenidos educativos.

2. EL MARCO EUROPEO DE CUALIFICACIONES

La UE ha desarrollado el Marco Europeo de Cualificaciones (EQF) como herramienta de traducción para que las cualificaciones nacionales sean más fáciles de entender y comparar. El EQF tiene por objeto apoyar la movilidad transfronteriza de los estudiantes y los trabajadores, promover el aprendizaje permanente y el desarrollo profesional en toda Europa.

El EQF es un marco de 8 niveles, basado en los resultados del aprendizaje, para todo tipo de cualificaciones que sirve como herramienta de traducción entre los diferentes marcos nacionales de cualificaciones. Este marco contribuye a mejorar la transparencia, la comparabilidad y la transferibilidad de las cualificaciones de las personas y permite comparar las cualificaciones de diferentes países e instituciones.

El EQF abarca todos los tipos y niveles de cualificaciones, y el uso de los resultados del aprendizaje deja claro lo que una persona sabe, entiende y es capaz de hacer. El nivel aumenta según el grado de competencia, siendo el nivel 1 el más bajo y el 8 el más alto. Lo más importante es que el EQF está estrechamente vinculado a los marcos nacionales de cualificaciones, lo que le permite ofrecer un mapa completo de todos los tipos y niveles de cualificaciones en Europa, cada vez más accesibles a través de las bases de datos de cualificaciones.

El EQF se creó en 2008 y se revisó posteriormente en 2017. Su revisión ha mantenido los objetivos fundamentales de crear transparencia y confianza mutua en el panorama de las cualificaciones en Europa. Los Estados miembros se comprometieron a seguir desarrollando el EQF y a hacerlo más eficaz para facilitar la comprensión de las cualificaciones nacionales, internacionales y de terceros países por parte de los empleadores, los trabajadores y los estudiantes.

Cada uno de los ocho niveles del EQF se define mediante un conjunto de descriptores que indican los resultados del aprendizaje pertinentes para las cualificaciones de ese nivel en cualquier sistema de cualificaciones. Los resultados del aprendizaje se definen en términos de:

- Conocimientos: en el contexto del EQF, los conocimientos se describen como teóricos y/o fácticos.
- Competencias: en el contexto del EQF, las competencias se describen como cognitivas (que implican el uso del pensamiento lógico, intuitivo y creativo) y prácticas (que implican la destreza manual y el uso de métodos, materiales, herramientas e instrumentos).
- Responsabilidad y autonomía: en el contexto del EQF, la responsabilidad y la autonomía se describen como la capacidad del alumno para aplicar los conocimientos y las competencias de forma autónoma y responsable.

Tabla 1 (Conocimientos, habilidades y resultados del aprendizaje del EQF): Resultados del aprendizaje del nivel 4 del EQF

Conocimientos	**Capacidad**	**Responsabilidad y autonomía**
Conocimientos fácticos y teóricos en contextos amplios dentro de un campo de estudio o aprendizaje	Conjunto de habilidades cognitivas y prácticas necesarias para encontrar soluciones a problemas específicos en un campo de trabajo o educación	Aplicar la autogestión dentro de las directrices de contextos laborales o de aprendizaje que son generalmente predecibles pero sujetos a cambios; supervisar el trabajo rutinario de otros, asumir cierta responsabilidad en la evaluación y mejora de las actividades laborales o de aprendizaje

3. ESTUDIANTES DE FORMACIÓN PROFESIONAL EN CIBERSEGURIDAD (NIVEL 4-5 EQF)

El empleado de ciberseguridad (nivel 4-5) es un profesional cualificado que trabaja en el ámbito de los sistemas de información en el lugar de trabajo, participa en estudios de actividades preventivas de ciberseguridad en el ámbito del seguimiento de vulnerabilidades y los procesos de sensibilización sobre ciberseguridad, realiza un seguimiento de las acciones, supervisa el funcionamiento y la sostenibilidad de los sistemas utilizados en los análisis de ciberseguridad, determina los requisitos de las redes simples, configura redes físicas, realiza configuraciones de nivel simple relacionadas con el hardware de red, garantiza la seguridad, el mantenimiento y las mejoras de la red, proporciona asistencia técnica a los usuarios y lleva a cabo estudios de desarrollo profesional con el fin de proteger las infraestructuras informáticas del lugar de trabajo contra las amenazas cibernéticas en el marco de los requisitos de calidad, mediante la aplicación de medidas de salud y seguridad en el trabajo y de protección del medio ambiente.

3.1. PROGRAMA CYBERAGENT LEARNING PARA EQF-4-5

El plan de estudios de FP (EQF 4-5) se desarrolló adaptando estratégicamente el plan de estudios completo de la EHE (EQF 5-6). El proceso de adaptación consistió en concentrar el material para alinearlo con el alcance de 1 ECTS y centrarse en los resultados de aprendizaje más relevantes para el público de la EFP y las necesidades inmediatas de las pymes. Se dio prioridad a los temas que hacen hincapié en la aplicación práctica y las habilidades básicas de ciberseguridad, mientras que los conceptos teóricos más profundos se simplificaron para adaptarse a la trayectoria de aprendizaje de la EFP.

Tabla 2: Módulo 1

<table>
<tr><th>Unidades</th><th>Temas</th></tr>
<tr><td>Gestión de proyectos</td><td>Planificación de proyectos
Definición de los objetivos del proyecto
Amenazas actuales para la ciberseguridad (DDoS, ransomware, malware, phishing, zero-day, ataques a IoT, etc.)
Modelización de amenazas y análisis de vulnerabilidades
Notificación de amenazas e incidentes de ciberseguridad</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos serán capaces de definir las fases de la gestión de proyectos y crear un plan de proyecto básico. (Aplicación)
Los alumnos articularán objetivos de proyecto claros, medibles y alcanzables. (Análisis)
Los alumnos identificarán, clasificarán y evaluarán diversas amenazas de ciberseguridad. (Análisis)
Los alumnos desarrollarán modelos de amenazas y realizarán análisis de vulnerabilidad para escenarios específicos. (Aplicación)
Los alumnos prepararán informes de incidentes siguiendo los protocolos establecidos. (Aplicación)</td></tr>
<tr><td>Gestión de recursos</td><td>Herramientas y software de seguridad
Uso eficaz de los recursos tecnológicos</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos demostrarán un uso eficaz de las herramientas y el software de ciberseguridad para la detección y respuesta ante amenazas. (Aplicación)
Los alumnos optimizarán los recursos tecnológicos para mejorar la seguridad y la eficiencia. (Aplicación)</td></tr>
<tr><td>Métricas de seguridad</td><td>Métricas de seguridad y técnicas de medición
Recopilación de datos con SIEM
Análisis de métricas de seguridad
Supervisión de proyectos y evaluación del rendimiento
Informes de métricas de seguridad</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos identificarán y aplicarán métricas de seguridad y técnicas de medición relevantes. (Aplicación)</td></tr>
</table>

• Los alumnos configurarán y utilizarán herramientas SIEM para la recopilación de datos y la supervisión de la seguridad. (Aplicación) • Los alumnos interpretarán y analizarán las métricas de seguridad para evaluar la postura de seguridad. (Análisis) • Los alumnos supervisarán y evaluarán el rendimiento del proyecto utilizando métricas de seguridad. (Evaluación) • Los alumnos compilarán y presentarán informes basados en el análisis de métricas de seguridad. (Aplicación)	
Garantía y control de calidad	Gestión de la calidad Estándares de calidad en ciberseguridad Técnicas de prueba y validación
Resultados del alumno: • Los alumnos implementarán prácticas de gestión de la calidad en proyectos de ciberseguridad. (Aplicación) • Los alumnos identificarán y aplicarán los estándares de calidad pertinentes en materia de ciberseguridad. (Aplicación) • Los alumnos desarrollarán y ejecutarán procedimientos de prueba y validación para soluciones de ciberseguridad. (Aplicación)	

Tabla 3: Módulo 2

Unidades	**Temas**
Administración de sistemas operativos	Sistemas operativos Relación entre hardware y software Binarios, conteo hexadecimal Bits y bytes Línea de comandos en el sistema operativo Comandos de Windows y Linux Cliente y servidor Windows Aplicaciones, procesos y servicios en Windows Extensiones y tipos de archivo Claves y valores del Registro Configuración del Panel de control Usuarios y grupos Estructura de dominio y administrador de servidores AD y GPO Interfaces y kernel de Linux Procesos en Linux Convenciones de nomenclatura de archivos y directorios Shells de Linux y sintaxis de comandos Manipulación de archivos y carpetas Trabajar con comandos de supervisión de tuberías y sistemas Gestión de procesos y control de tareas Gestión de servicios
Resultados del aprendizaje:	

<table>
<tr><td colspan="2">

- Los alumnos compararán y contrastarán diferentes sistemas operativos y sus arquitecturas.
- Los alumnos explicarán la interacción entre el hardware y el software en un entorno de sistema operativo.
- Los alumnos realizarán conversiones binarias y hexadecimales y comprenderán la representación de datos.
- Los alumnos ejecutarán comandos fundamentales en entornos Windows y Linux.
- Los alumnos gestionarán aplicaciones, servicios y procesos utilizando herramientas del sistema.
- Los alumnos configurarán y gestionarán Active Directory y GPO.
- Los alumnos interactuarán con interfaces Linux y realizarán operaciones a nivel del núcleo.
- Los alumnos gestionarán servicios y procesos del sistema utilizando comandos Linux.

</td></tr>
<tr><td>Administración de sistemas de bases de datos</td><td>Repositorios y listas de fuentes
Gestión de un servidor web
Registros del sistema y supervisión de registros
Programación de tareas en Linux
Solución de problemas del servidor y la red
Copias de seguridad y recuperación
Protección de GRUB
Cortafuegos
Objetos de Active Directory y gestión de GPO
DNS y DHCP
Fundamentos de PowerShell
Microsoft BitLocker, AppLocker y firewall
LDAP y Kerberos
NTLM
Políticas de contraseñas y bloqueos
Autenticación y control de acceso
Protocolo de mensajes de control de Internet (ICMP)
TCP frente a UDP
NetBIOS y SMB
SSL y TLS
Certificados
Protocolos Telnet y Secure Shell (SSH)
HTTP y HTTPS
Protocolos de sistemas de correo
Protocolo del sistema de nombres de dominio (DNS)
FTP y RDP
Encapsulación frente a descapsulación
Sniffers de red y Wireshark
TCP/UDP
DHCP, DNS</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos configurarán repositorios y gestionarán listas de fuentes.
- Los alumnos analizarán y supervisarán los registros para la resolución de problemas y la seguridad.

</td></tr>
</table>

<table>
<tr><td colspan="2">

- Los alumnos realizarán operaciones de copia de seguridad y recuperación para garantizar la integridad de los datos.
- Los alumnos implementarán medidas de seguridad, incluyendo cortafuegos, BitLocker y AppLocker.

</td></tr>
<tr><td>Administración de redes</td><td>Tipos de redes y redes inalámbricas
Redes y topologías
Identidad y acceso de dispositivos
Infraestructura y dispositivos de seguridad
Dispositivos especializados y arquitectura de red
Redes virtuales
Direcciones físicas y lógicas
Modelos OSI y de red
Encapsulación y descapsulación de datos
Protocolos de red y números de puerto
Medios y cables de red
Tecnologías inalámbricas
Herramientas de administración de redes
Cisco Packet Tracer
Clases de red y subredes
Protocolo de resolución de direcciones (ARP)
Direccionamiento IP estático frente a dinámico
Traducción de direcciones de red (NAT)
Conmutadores y Cisco IOS
Seguridad de puertos de conmutadores e interfaces de enrutadores
Configuración de VLAN y DTP
Enrutamiento entre VLAN
Introducción a las ACL
Solución de problemas de red</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos diseñarán y gestionarán redes, comprendiendo los protocolos y las topologías.
- Los alumnos configurarán VLAN, ACL y gestionarán esquemas de direccionamiento IP.
- Los alumnos utilizarán herramientas como Wireshark y Cisco Packet Tracer para la supervisión y la resolución de problemas.

</td></tr>
<tr><td>Administración de la nube</td><td>Hipervisores y máquinas virtuales
Contenedores
Protección de entornos virtuales
Copia de seguridad y recuperación
Computación en la nube y CSP
¿Qué son los modelos de servicios en la nube?
Tipos de implementación en la nube
Redes virtuales
Servicios informáticos de AWS
Amazon Elastic Compute Cloud (EC2)
Herramientas de supervisión en la nube
Herramientas de automatización y orquestación
Amenazas y vulnerabilidades de seguridad en la nube</td></tr>
</table>

	Gestión de identidades y accesos (IAM) Control de acceso basado en roles (RBAC) Autenticación multifactor (MFA) Cifrado de datos en la nube Nube privada virtual (VPC) Docker y Kubernetes
Resultados del aprendizaje: • Los alumnos gestionarán entornos virtuales utilizando AWS, Docker y Kubernetes. • Los alumnos implementarán controles de seguridad en la nube y gestión de identidades.	
Administración de sistemas ciberfísicos	Seguridad y controles de acceso Tipos de autenticación TACACS+ y RADIUS Configuración AAA Objetivos de gestión de riesgos Cifrado y descifrado Tablas hash y rainbow Suplantación de MAC y envenenamiento de ARP VLAN Hopping y DHCP no autorizado Inundación ICMP Inundación TCP y UDP Secuestro de sesión Spoofing de DNS Defensa en profundidad (DID) y confianza cero Zonas desmilitarizadas (DMZ) Honeypots y refuerzo de la red Mejores prácticas para una red segura VPN SSH y VNC Cortafuegos con estado frente a cortafuegos sin estado Basados en host frente a basados en red Cortafuegos de hardware frente a cortafuegos de software Cortafuegos de aplicaciones web (WAF) IA en cortafuegos IDS e IPS NIDS y HIDS Snort tcpdump
Resultados del aprendizaje: • Los alumnos aprenderán a proteger redes mediante cortafuegos, IDS/IPS y herramientas de detección de amenazas. • Los alumnos aplicarán técnicas de cifrado y gestionarán protocolos de seguridad.	
Fortalecimiento del sistema	Técnicas GenAI Generación de código Gestión de cuentas de usuario y control de acceso Detección de anomalías y resolución de problemas Resolución de errores del servicio Apache2 Gestión de parches y actualizaciones

	Copia de seguridad y recuperación automatizadas Recuperación de archivos eliminados con GenAI Procedimientos de ciberseguridad Detección y análisis de amenazas Respuesta y corrección de amenazas Aprovechamiento de la IA para la detección de amenazas en tiempo real Validación y prueba de modelos GenAI Configuración y seguridad de DNS Configuración y seguridad de DHCP Fundamentos de PowerShell Seguridad de puertos de conmutador Sistema básico de entrada/salida de red (NetBIOS) Protocolo de bloque de mensajes del servidor (SMB) Capa de sockets seguros (SSL) y seguridad de la capa de transporte (TLS) Certificados de seguridad Protocolos de sistemas de correo Protocolo del sistema de nombres de dominio (DNS) Protocolo de transferencia de archivos (FTP) Protocolo de escritorio remoto (RDP) Programación de tareas en Linux Solución de problemas del servidor Solución de problemas de red Copia de seguridad y recuperación Protección de GRUB Configuración y protección de cortafuegos
Resultados del aprendizaje: • Los alumnos aplicarán técnicas de refuerzo para mejorar la seguridad del sistema. • Los alumnos aprovecharán la IA para la detección de amenazas y la supervisión del sistema.	
Fortalecimiento del sistema	IR frente a SOC Eventos e incidentes Detección de alertas y clasificación de alertas Documentación y generación de informes ¿Qué son los ataques web? DoS y DDoS Inyección SQL y XSS Inyección de comandos e inclusión de archivos locales (LFI) Falsificación de solicitudes entre sitios (CSRF) Fuerza bruta y relleno de credenciales Pasar el hash y pasar el ticket Control de acceso defectuoso Ransomware Virus informáticos y gusanos Caballo de Troya y adware Keylogger y criptojacking Malware sin archivos

	Comprender la propagación del malware Gestión de IOC y políticas de contraseñas Políticas de uso aceptable (AUP) Políticas de «traiga su propio dispositivo» (BYOD) Políticas de acceso remoto

Resultados del aprendizaje:

- Distinguir las funciones clave y la colaboración entre R y SOC.
- Definir la diferencia entre incidentes de seguridad y violaciones de seguridad.
- Explicar las fuentes de las alertas de seguridad y los procesos de clasificación.
- Proporcionar documentación y informes eficaces sobre incidentes de seguridad.
- Describir los tipos comunes de ataques web (DoS/DDoS, inyección SQL, XSS, inyección de comandos, LFI, CSRF).
- Explicar los ataques de fuerza bruta y relleno de credenciales y describir sus contramedidas.
- Comprender los principios básicos de los ataques «pass the hash» y «pass the ticket».
- Explicar cómo se pueden explotar las vulnerabilidades del control de acceso.
- Explicar los diferentes tipos de malware (ransomware, virus, gusanos, troyanos, adware, keyloggers, criptojacking, malware sin archivos) y sus métodos de propagación.
- Explicar la importancia de gestionar los indicadores de inteligencia sobre amenazas (IOC).
- Describir los elementos clave de las políticas de contraseñas seguras y las políticas de uso aceptable (AUP).
- Evaluar el impacto en la seguridad de las políticas BYOD y de acceso remoto.

Tabla 4: Módulo 3

Unidades	**Temas**
Mediciones de rendimiento (métricas)	Métricas de rendimiento Supervisión del sistema y la red Supervisión de métricas de rendimiento Mapeo de redes Análisis de vulnerabilidades Análisis del tráfico de red

Resultados del aprendizaje:

- Los alumnos definirán las métricas de rendimiento y explicarán su importancia en la evaluación del rendimiento del sistema y la red.
- Los alumnos demostrarán la configuración y el uso de herramientas de supervisión para la evaluación continua del rendimiento del sistema y la red.
- Los alumnos analizarán e interpretarán las métricas de rendimiento para evaluar el estado del sistema e identificar oportunidades de optimización.
- Los alumnos crearán mapas de red para visualizar, supervisar y optimizar las estructuras de red.
- Los alumnos realizarán análisis de vulnerabilidades, identificarán riesgos de seguridad y recomendarán medidas correctivas.
- Los alumnos realizarán análisis del tráfico de red para detectar y responder a posibles amenazas.

Análisis de datos	Recopilación de datos Limpieza y preprocesamiento de datos Análisis de datos Visualización de datos Herramientas analíticas Aplicaciones del análisis de datos en la ciberseguridad
Resultados del aprendizaje: • Los alumnos recopilarán datos relevantes de sistemas, redes y registros de seguridad para su análisis. • Los alumnos limpiarán y preprocesarán los datos sin procesar para garantizar su precisión y coherencia. • Los alumnos aplicarán técnicas estadísticas y analíticas para extraer información significativa de los datos. • Los alumnos crearán visualizaciones de datos para comunicar de forma eficaz los resultados del análisis. • Los alumnos utilizarán herramientas como Python, R y Power BI para realizar análisis de datos exhaustivos. • Los alumnos aplicarán técnicas de análisis de datos para detectar, analizar y mitigar las amenazas a la ciberseguridad.	
Inteligencia de seguridad	Comprensión de la inteligencia de seguridad Fuentes de inteligencia de seguridad Métodos de recopilación de inteligencia sobre amenazas Estudios de casos sobre aplicaciones de inteligencia de seguridad
Resultados del aprendizaje: • Los alumnos explicarán la importancia de la inteligencia de seguridad en la gestión proactiva de amenazas. • Los alumnos evaluarán las fuentes de inteligencia de seguridad, incluyendo fuentes de amenazas, informes y herramientas de código abierto. • Los alumnos describirán métodos para recopilar y analizar inteligencia sobre amenazas. • Los alumnos examinarán casos reales para comprender la aplicación de la inteligencia de seguridad en la prevención de amenazas cibernéticas.	

Tabla 5: Módulo 4

Unidades	**Temas**
Fundamentos de las operaciones de seguridad	Comprensión de las operaciones de seguridad y el SOC (centro de operaciones de seguridad) Funciones y responsabilidades en las operaciones de seguridad Descripción general de las herramientas y tecnologías de operaciones de seguridad Ejemplos prácticos y casos de estudio
Resultados del aprendizaje:	

<table>
<tr><td colspan="2">

- Los alumnos explicarán el propósito y la estructura de un centro de operaciones de seguridad y su función en la ciberseguridad.
- Los alumnos describirán las funciones y responsabilidades del personal de operaciones de seguridad, incluyendo la respuesta a incidentes, la búsqueda de amenazas y la supervisión.
- Los alumnos identificarán y demostrarán el uso de herramientas y tecnologías comunes de operaciones de seguridad.
- Los alumnos analizarán ejemplos reales y casos prácticos para comprender las operaciones de seguridad en la práctica.

</td></tr>
<tr><td>Convergencia de la seguridad</td><td>Comprensión de la convergencia de la seguridad
Fundamentos de la seguridad física (principios de seguridad física, protección de activos físicos, políticas)
Amenazas comunes a las que se enfrentan las pymes
Estudios de casos que destacan cuestiones de convergencia</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos definirán la convergencia de la seguridad y explicarán su importancia en la integración de medidas de seguridad física y cibernética.
- Los alumnos aplicarán los principios de seguridad física para proteger los activos, las instalaciones y el personal.
- Los alumnos identificarán y evaluarán las amenazas de seguridad a las que se enfrentan habitualmente las pequeñas y medianas empresas (pymes).
- Los alumnos examinarán casos prácticos para comprender el impacto de los retos de la convergencia.
- Los alumnos revisarán los procesos de gestión de la información y los eventos de seguridad.

</td></tr>
<tr><td>Gestión de la información y los eventos de seguridad</td><td>Revisión de los principios de supervisión de la seguridad (basada en el módulo de otros socios)
Implementación de soluciones SIEM
Configuración de registros y alertas
Revisión de la inteligencia sobre amenazas y las metodologías de detección (basado en el módulo de otros socios)</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos explicarán los principios de supervisión de la seguridad y su aplicación en soluciones SIEM.
- Los alumnos configurarán y utilizarán soluciones SIEM para la detección y respuesta eficaz ante amenazas.
- Los alumnos configurarán mecanismos de registro y alerta en herramientas SIEM para supervisar eventos de seguridad.
- Los alumnos evaluarán la inteligencia sobre amenazas y las metodologías de detección para garantizar la eficacia de las operaciones de seguridad.

</td></tr>
<tr><td>Prácticas de operaciones de seguridad</td><td>Cumplimiento y normativa
Estrategias de mejora continua en las operaciones de seguridad
Automatización y coordinación
Métricas e informes</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos explicarán la importancia del cumplimiento normativo y la regulación en las operaciones de seguridad.

</td></tr>
</table>

• Los alumnos diseñarán e implementarán estrategias de mejora continua para las operaciones de seguridad. • Los alumnos aprovecharán la automatización y la coordinación para mejorar la eficiencia de las operaciones de seguridad. • Los alumnos desarrollarán y utilizarán métricas de seguridad y técnicas de generación de informes para comunicar la postura de seguridad.

Tabla 6: Módulo 5

Unidades	**Temas**
Contexto organizativo	Evolución de la ciberseguridad en las pymes Principales amenazas y vulnerabilidades actuales Impacto de la ciberseguridad en la estrategia empresarial Retos específicos de la ciberseguridad en las pymes frente a las grandes empresas Comprender las implicaciones normativas de las prácticas de ciberseguridad y cómo se alinean con las estructuras de gobernanza. Retos comunes de ciberseguridad específicos de las pymes, como presupuestos limitados, falta de personal dedicado a la seguridad y métodos prácticos para priorizar las inversiones en ciberseguridad.
Resultados del aprendizaje: • Los alumnos seguirán el desarrollo de las prácticas de ciberseguridad en las pequeñas y medianas empresas. • Los alumnos identificarán y evaluarán las amenazas y vulnerabilidades actuales más críticas que afectan a las pymes. • Los alumnos analizarán cómo la ciberseguridad influye en la estrategia empresarial y en la toma de decisiones operativas. • Los alumnos compararán los retos de ciberseguridad a los que se enfrentan las pymes con los que encuentran las organizaciones más grandes. • Los alumnos interpretarán los requisitos normativos en materia de ciberseguridad y evaluarán cómo se integran en la gobernanza de las organizaciones. • Los alumnos describirán soluciones prácticas para los retos comunes de ciberseguridad de las pymes, como las restricciones presupuestarias y la escasez de personal.	
Privacidad	Principios de privacidad en la ciberseguridad Protección de datos personales y RGPD Impacto de la privacidad en las operaciones de las pymes Herramientas y técnicas para la protección de la privacidad
Resultados del aprendizaje: • Los alumnos explicarán los principios básicos de la privacidad en el contexto de la ciberseguridad. • Los alumnos aplicarán los requisitos del RGPD y evaluarán su impacto en la protección de datos personales. • Los alumnos evaluarán cómo las normativas de privacidad afectan a las operaciones diarias y a los modelos de negocio de las pymes.	

<table>
<tr><td colspan="2">

- Los alumnos utilizarán herramientas y aplicarán técnicas para mantener la privacidad y proteger los datos sensibles.

</td></tr>
<tr><td>Leyes, ética y cumplimiento</td><td>Organizaciones, políticas y normas de ciberseguridad
Legislación nacional e internacional pertinente
Cumplimiento normativo en las pymes
Ética en la ciberseguridad
Consecuencias legales del incumplimiento en materia de ciberseguridad
Análisis de cómo se pueden utilizar las herramientas basadas en la inteligencia artificial para reforzar la gobernanza de la ciberseguridad y garantizar el cumplimiento mediante la supervisión continua y la respuesta automatizada a las amenazas.</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos identificarán las principales organizaciones de ciberseguridad y evaluarán los marcos normativos y estándares pertinentes.
- Los alumnos resumirán las leyes clave que afectan a la ciberseguridad a nivel nacional e internacional.
- Los alumnos diseñarán estrategias para lograr y mantener el cumplimiento normativo en el contexto de las pymes.
- Los alumnos examinarán las consideraciones éticas en la toma de decisiones y el comportamiento en materia de ciberseguridad.
- Los alumnos evaluarán las ramificaciones legales del incumplimiento de las leyes de ciberseguridad.
- Los alumnos explorarán cómo las herramientas de IA pueden mejorar la gobernanza, automatizar la supervisión y mejorar el cumplimiento.

</td></tr>
<tr><td>Gobernanza de la seguridad</td><td>Estructura de gobernanza de la ciberseguridad
Funciones y responsabilidades en la gestión de la seguridad
Modelos de madurez de la ciberseguridad
Mejorar las capacidades para realizar evaluaciones de riesgos y formular planes de respuesta estratégicos en condiciones de crisis simuladas (ransomware, ataques de phishing, etc.).
Comunicación a nivel ejecutivo y directivo
Estrategias de comunicación en materia de ciberseguridad
Informes de seguridad para la alta dirección
Gestión de crisis y comunicación en materia de ciberseguridad
Dominar las habilidades de gestión de crisis y toma de decisiones en situaciones de alto estrés que impliquen ataques impulsados por IA y ransomware.</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos diseñarán y evaluarán estructuras de gobernanza que respalden una gestión eficaz de la ciberseguridad.
- Los alumnos asignarán y aclararán las responsabilidades en los marcos de seguridad de la organización.
- Los alumnos evaluarán la madurez de la ciberseguridad utilizando modelos establecidos.

</td></tr>
</table>

• Los alumnos realizarán evaluaciones de riesgos y desarrollarán estrategias de respuesta para situaciones como el ransomware o el phishing. • Los alumnos desarrollarán planes de comunicación para transmitir conocimientos sobre ciberseguridad a los altos ejecutivos y miembros del consejo de administración. • Los alumnos formularán estrategias de comunicación eficaces para las partes interesadas internas y externas en materia de ciberseguridad. • Los alumnos generarán informes que informen a la alta dirección sobre el rendimiento y los riesgos de la ciberseguridad. • Los alumnos practicarán la gestión y la comunicación durante crisis de ciberseguridad, incluidas aquellas relacionadas con ataques impulsados por la inteligencia artificial.	
Política de gestión	Aplicación y supervisión de políticas
Resultados del aprendizaje: • Los alumnos implementarán políticas de ciberseguridad y establecerán procedimientos para su supervisión y aplicación continuas.	

Tabla 7: Módulo 6

Unidades	**Temas**
Introducción a la planificación de la ciberseguridad: seguridad de los datos, de las personas y de la sociedad	Seguridad de los datos: seguridad del almacenamiento de la información, proceso de investigación Seguridad de los datos: técnicas de ataque a contraseñas Seguridad humana: concienciación y comprensión Seguridad social: ¿qué son los delitos cibernéticos y la ética cibernética? Seguridad social: legislación cibernética, pruebas digitales, contratos digitales, convenios multinacionales (acuerdos)
Resultados del aprendizaje: • Los alumnos implementarán estrategias para proteger la información almacenada y apoyar los procesos de investigación. • Los alumnos identificarán y analizarán las técnicas comunes de ataque a contraseñas y desarrollarán las contramedidas adecuadas. • Los alumnos promoverán la concienciación sobre la ciberseguridad y fomentarán la comprensión entre los empleados y las partes interesadas. • Los alumnos explicarán las implicaciones sociales de los delitos cibernéticos y evaluarán las consideraciones éticas en los entornos digitales. • Los alumnos interpretarán conceptos clave del derecho cibernético, incluyendo las pruebas digitales, los contratos y los acuerdos internacionales.	
Gestión operativa y táctica	Implementación de controles de acceso Gestión de parches y actualizaciones de software Supervisión continua del sistema Formación en concienciación sobre seguridad para empleados
Resultados del aprendizaje: • Los alumnos diseñarán e implementarán mecanismos de control de acceso eficaces para proteger los sistemas y los datos.	

• Los alumnos establecerán procedimientos para la gestión oportuna de parches y actualizaciones de software con el fin de reducir las vulnerabilidades. • Los alumnos llevarán a cabo una supervisión continua de los sistemas para detectar y responder a incidentes de seguridad. • Los alumnos desarrollarán e impartirán programas de formación en materia de seguridad para mejorar el compromiso de los empleados y reducir el riesgo humano.

Tabla 8: Módulo 7

Unidades	**Temas**
Evaluación de riesgos	Marco y proceso generales de gestión de riesgos Principios de la gestión de riesgos Normas de gestión de riesgos Ejemplos prácticos y estudios de casos
Resultados del aprendizaje: • Los alumnos describirán y aplicarán el marco general y el proceso de gestión de riesgos en ciberseguridad. • Los alumnos explicarán los principios básicos que guían una gestión eficaz de los riesgos de ciberseguridad. • Los alumnos identificarán e interpretarán las normas de gestión de riesgos ampliamente aceptadas. • Los alumnos evaluarán escenarios de riesgo mediante ejemplos reales y estudios de casos.	
Identificación de riesgos	Fuentes tangibles e intangibles de riesgo Causas y eventos Amenazas y oportunidades Vulnerabilidades y capacidades Cambios en el contexto externo e interno Indicadores de riesgos emergentes La naturaleza y el valor de los activos y recursos Consecuencias y su impacto en los objetivos Limitaciones del conocimiento y fiabilidad de la información Sesgos, suposiciones y creencias de los implicados. Ejemplos prácticos y estudios de casos.
Resultados del aprendizaje: • Los alumnos distinguirán entre fuentes tangibles e intangibles de riesgo en entornos de ciberseguridad. • Los alumnos identificarán las causas del riesgo y los eventos desencadenantes. • Los alumnos analizarán las amenazas a la ciberseguridad y evaluarán las posibles oportunidades de mejora. • Los alumnos evaluarán las vulnerabilidades y las capacidades organizativas en la gestión de riesgos. • Los alumnos evaluarán cómo los cambios contextuales influyen en los riesgos de ciberseguridad. • Los alumnos identificarán los indicadores que señalan la aparición de nuevas amenazas a la ciberseguridad.	

<table>
<tr><td colspan="2">

- Los alumnos evaluarán el valor de los activos y la importancia de los recursos en relación con el riesgo.
- Los alumnos estimarán las posibles consecuencias y su impacto en los objetivos estratégicos.
- Los alumnos reconocerán las limitaciones de la información y el conocimiento en el proceso de identificación de riesgos.
- Los alumnos reflexionarán sobre cómo los factores humanos afectan a la percepción y la identificación de los riesgos.
- Los alumnos aplicarán técnicas de identificación a través de escenarios del mundo real.

</td></tr>
<tr><td>Amenazas internas</td><td>Definición y tipos de amenazas internas
Detección e identificación de amenazas internas
Ejemplos prácticos y estudios de casos</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos definirán las amenazas internas y clasificarán los distintos tipos.
- Los alumnos desarrollarán habilidades para detectar y responder a los indicadores de amenazas internas.
- Los alumnos analizarán estudios de casos de incidentes reales relacionados con amenazas internas.

</td></tr>
<tr><td>Modelos y metodologías de medición y evaluación de riesgos</td><td>Modelos y metodologías cuantitativos y cualitativos de evaluación de riesgos
Probabilidad de que se produzcan los eventos y consecuencias
La naturaleza y magnitud de las consecuencias
Niveles de sensibilidad y confianza.
Ejemplos prácticos y estudios de casos</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos compararán y aplicarán modelos cuantitativos y cualitativos en la evaluación de riesgos de ciberseguridad.
- Los alumnos evaluarán la probabilidad y los posibles resultados de los riesgos identificados.
- Los alumnos evaluarán la gravedad y el alcance de las consecuencias asociadas a los riesgos de ciberseguridad.
- Los alumnos determinarán los niveles de incertidumbre y confianza en las evaluaciones de riesgos.
- Los alumnos implementarán modelos de evaluación de riesgos en escenarios prácticos.

</td></tr>
<tr><td>Control de riesgos</td><td>Supervisión y revisión
Registro y presentación de informes
Ejemplos prácticos y estudios de casos</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:

- Los alumnos llevarán a cabo procesos regulares de supervisión y revisión de riesgos.
- Los alumnos documentarán y comunicarán las medidas de control de riesgos de forma eficaz.
- Los alumnos examinarán ejemplos del mundo real para comprender la implementación eficaz del control de riesgos.

</td></tr>
</table>

Tabla 9: Módulo 8

Unidades	Temas
Respuesta ante incidentes	Definición e importancia de la respuesta ante incidentes Componentes clave de un plan eficaz de recuperación ante incidentes Amenazas comunes a la ciberseguridad
Resultados del aprendizaje: • Los alumnos definirán la respuesta ante incidentes y explicarán su importancia en la gestión de la ciberseguridad. • Los alumnos identificarán e implementarán los elementos clave de un plan estructurado de recuperación de respuesta ante incidentes. • Los alumnos reconocerán y responderán a las amenazas comunes de ciberseguridad que se encuentran durante la gestión de incidentes.	
Recuperación ante desastres	Comprensión de la recuperación ante desastres Funciones y responsabilidades en la recuperación ante desastres Pasos de recuperación tras un desastre
Resultados del aprendizaje: • Los alumnos explicarán los principios y objetivos de la recuperación ante desastres en el contexto de la ciberseguridad. • Los alumnos describirán las funciones y responsabilidades de los miembros del equipo que participan en la recuperación ante desastres. • Los alumnos desarrollarán un plan paso a paso para restaurar los sistemas y las operaciones tras un desastre cibernético.	
Continuidad del negocio	Comprensión de la continuidad del negocio Funciones y responsabilidades en la continuidad del negocio Análisis del impacto en el negocio
Resultados del aprendizaje: • Los alumnos explicarán el concepto y la importancia de la planificación de la continuidad del negocio. • Los alumnos identificarán las funciones y responsabilidades relacionadas con garantizar la continuidad del negocio. • Los alumnos realizarán un análisis del impacto en el negocio para evaluar las funciones críticas y las dependencias.	
Concienciación, formación y educación en materia de seguridad	Comprensión de la concienciación sobre seguridad Responsabilidades de los empleados en materia de ciberseguridad
Resultados del aprendizaje: • Los alumnos explicarán el papel de la concienciación sobre seguridad en la reducción de los riesgos de ciberseguridad relacionados con el factor humano. • Los alumnos reconocerán las responsabilidades de los empleados en el cumplimiento de los protocolos y las mejores prácticas de ciberseguridad.	
Prácticas de contratación en materia de seguridad	Definición de los requisitos de los puestos de seguridad Realización de comprobaciones exhaustivas de antecedentes

<table>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos definirán las funciones de los puestos de trabajo relacionados con la ciberseguridad y formularán los requisitos adecuados.
Los alumnos aplicarán las mejores prácticas en la realización de verificaciones de antecedentes para funciones sensibles en materia de seguridad.</td></tr>
<tr><td>Prácticas de rescisión por motivos de seguridad</td><td>Revocación inmediata del acceso
Notificación a los equipos pertinentes
Consideraciones legales y de cumplimiento</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos implementarán procedimientos para revocar rápidamente el acceso tras la baja de un empleado.
Los alumnos coordinarán la comunicación con los departamentos pertinentes durante el proceso de salida.
Los alumnos examinarán los requisitos legales y de cumplimiento relacionados con la terminación del empleo en el ámbito de la ciberseguridad.</td></tr>
<tr><td>Seguridad de terceros</td><td>Evaluación del riesgo de terceros
Implementación de contrastes y requisitos de seguridad
Supervisión y auditoría continuas
Respuesta ante incidentes y comunicación</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos evaluarán los riesgos de seguridad asociados a los proveedores y socios externos.
Los alumnos diseñarán y aplicarán cláusulas contractuales para garantizar el cumplimiento de la seguridad de terceros.
Los alumnos establecerán prácticas de supervisión y auditoría continuas para la seguridad de terceros.
Los alumnos coordinarán con terceros durante las actividades de respuesta ante incidentes.</td></tr>
<tr><td>Seguridad en los procesos de revisión</td><td>Incorporación de la seguridad en las revisiones
Evaluación de vulnerabilidades y pruebas de penetración
Revisiones posteriores a incidentes</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos integrarán consideraciones de seguridad en los procesos de revisión de la organización.
Los alumnos realizarán evaluaciones de vulnerabilidad y pruebas de penetración como parte de las actividades de revisión.
Los alumnos realizarán revisiones posteriores a incidentes para evaluar la eficacia y mejorar las respuestas futuras.</td></tr>
<tr><td>Cuestión especial sobre la privacidad de la información personal de los empleados</td><td>Limitaciones en la recopilación de datos
Almacenamiento y control de acceso
Cumplimiento de las normativas de privacidad
Intercambio de datos y terceros
Consentimiento y derechos de los empleados</td></tr>
<tr><td colspan="2">Resultados del aprendizaje:
Los alumnos identificarán los límites adecuados para la recopilación de datos personales de los empleados.
Los alumnos aplicarán medidas de almacenamiento seguro y control de acceso para los datos confidenciales de los empleados.</td></tr>
</table>

- Los alumnos garantizarán el cumplimiento de las normativas de privacidad pertinentes, como el RGPD.
- Los alumnos evaluarán los riesgos y las normas relativas al intercambio de datos de los empleados con terceros.
- Los alumnos comprenderán los derechos de los empleados y la importancia de obtener su consentimiento informado.

CONCLUSIÓN

Este informe presenta el plan de estudios adecuado al nivel de formación profesional que debe tenerse en cuenta para la implementación exitosa de la formación de CyberAgent. Tras la investigación realizada desde el inicio del proyecto para identificar las necesidades de formación, este documento describe las necesidades de los estudiantes de formación profesional para su participación.

El plan de estudios elaborado para el proyecto CyberAgent de nivel 5-6 del EQF se tomó como referencia durante la preparación del programa. A partir de este plan de estudios de nivel, se seleccionaron los temas adecuados para el nivel 4-5 del EQF.

Por último, con el fin de garantizar que la formación sea de la máxima calidad en términos de contenido, organización y desarrollo de habilidades, se han planteado cuestiones relacionadas con temas no transferidos del nivel 5-6 del EQF.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau