Co-funded by the European Union

D3.1 MÓDULOS DE FORMACIÓN PARA ESTUDIANTES DE INSTITUCIONES DE EDUCACIÓN SUPERIOR

CYBER AGENT 09.2025

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.

Paquete de trabajo 3: Desarrollo de recursos de aprendizaje CyberAgent

Entrega 3.1: Módulos de formación para estudiantes de educación superior

Líder del WP3: TIMTAL. Líder del D3.1: VU.

CONTENIDO

INTRODUCCIÓN

Según el informe D2.2, las pymes se enfrentan a una importante escasez de especialistas cualificados en ciberseguridad, y los empleados actuales suelen carecer de los conocimientos sistémicos necesarios para responder adecuadamente a las amenazas cibernéticas cada vez más complejas. Por lo tanto, es especialmente importante que la educación superior prepare a especialistas que puedan aplicar sus conocimientos en el entorno de las pymes, tanto en el ámbito técnico como en el de la gestión. En vista de ello, en el documento D2.3 se creó una vía de aprendizaje basada en competencias, dividida en diferentes áreas temáticas y centrada en el desarrollo de habilidades prácticas.

Este documento presenta uno de los principales resultados del proyecto: los módulos de formación para estudiantes de educación superior (D3.1). El objetivo de esta actividad es crear programas de formación para instituciones de educación superior (IES) que cubran las áreas clave de conocimientos, habilidades y competencias en materia de ciberseguridad relevantes para las pequeñas y medianas empresas (pymes).

Estos módulos son el resultado de un trabajo constante basado en un análisis detallado de las necesidades (D2.2), durante el cual se encuestó a representantes de pymes, de la formación profesional (FP) y de instituciones de educación superior, así como en una estructura de itinerario formativo claramente definida (D2.3).

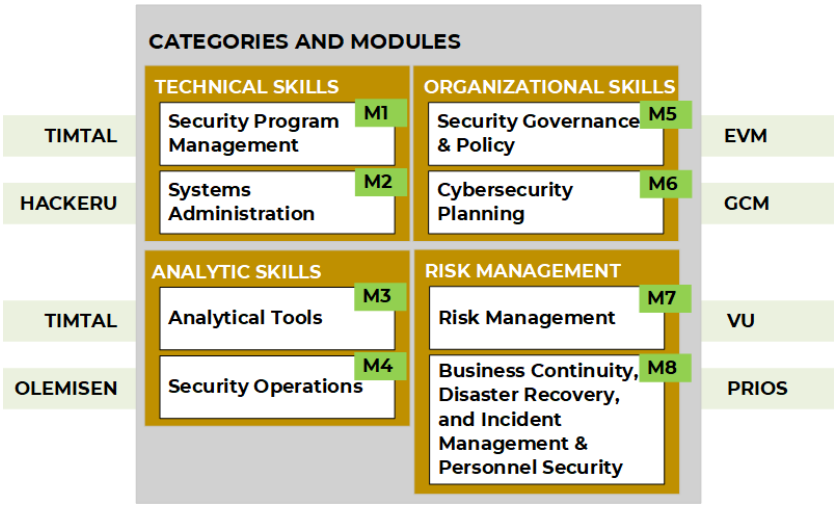
El programa de formación, que corresponde a los niveles 5-6 del Marco Europeo de Cualificaciones (MEC), está diseñado para estudiantes de educación superior y empleados avanzados de pymes. Consta de ocho módulos básicos y un módulo inspirador, que abarcan cuatro áreas de competencia esenciales:

- **Habilidades técnicas** (gestión de programas de seguridad, administración de sistemas).
- **Habilidades analíticas** (herramientas analíticas, operaciones de seguridad).
- **Habilidades organizativas** (gobernanza y políticas de seguridad, planificación de la ciberseguridad).
- **Gestión de riesgos** (gestión y mitigación de riesgos, continuidad del negocio, recuperación ante desastres y gestión de incidentes y seguridad del personal).

Cada módulo tiene un valor de 3 créditos ECTS (que corresponden a una carga de trabajo de 75 horas por parte del estudiante), se ajusta a los principios del Espacio Europeo de Educación Superior y sigue las recomendaciones metodológicas especificadas en D2.3: la educación se basa en métodos de aprendizaje activo (por ejemplo, estudios de casos, aprendizaje basado en proyectos) y aprendizaje autodirigido, con resultados de aprendizaje claramente diferenciados en los niveles de conocimientos, habilidades y competencias.

Cada módulo de 3 créditos ECTS ha sido desarrollado por diferentes socios del consorcio, aprovechando su experiencia específica en el campo y su experiencia profesional.

Los módulos desarrollados cubren las siguientes áreas clave, identificadas como de importancia crítica en el informe D2.2:



1. M1: GESTIÓN DE PROGRAMAS DE SEGURIDAD

Título del módulo	Código del módulo
GESTIÓN DE PROGRAMAS DE SEGURIDAD	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, híbrido	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
Ninguno

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75 horas	50 horas	25 horas

Objetivo y resultados del módulo		
Al finalizar este curso, los alumnos habrán adquirido las habilidades necesarias para gestionar de forma eficaz programas de seguridad en respuesta a las amenazas de ciberseguridad. Desarrollarán estrategias de defensa contra amenazas actuales, como el phishing, el ransomware y los ataques DDoS, dentro de los marcos de gestión de proyectos y recursos. Además, los estudiantes aprenderán a aplicar métricas de seguridad y métodos de garantía de calidad, adquiriendo la capacidad de optimizar los programas de seguridad, gestionar los recursos de manera eficiente y mejorar la seguridad de la organización mediante el uso de herramientas adecuadas contra las amenazas en constante evolución. Este curso también desarrollará su competencia en la evaluación, notificación y comunicación de amenazas, lo que les permitirá implementar estrategias de ciberseguridad de manera eficaz dentro de sus organizaciones.		
Resultados del aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**
Conocimientos: Los alumnos adquirirán conocimientos prácticos sobre las últimas amenazas a la ciberseguridad, como el phishing, el ransomware y los ataques DDoS, y aprenderán a gestionarlas mediante una gestión eficaz de proyectos y recursos y la implementación de medidas de control y	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, clases teóricas, ponentes invitados, cuestionarios, juegos, tareas prácticas/laboratorios, enseñanza y aprendizaje entre pares, aprendizaje autoguiado, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad de las pymes».	Pruebas de autoevaluación Prueba de evaluación de conocimientos

garantía de calidad.		
Habilidades: Los alumnos aprenderán a utilizar herramientas y software para protegerse contra las amenazas cibernéticas en constante evolución, y a aplicar prácticas de seguridad sólidas en la gestión de proyectos y recursos para mejorar las métricas generales de seguridad y el control de calidad dentro de sus organizaciones.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, tareas prácticas/laboratorios, actividades prácticas, entornos simulados, cuestionarios, juegos, estudios de casos, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Evaluaciones prácticas
Competencias: Los alumnos serán competentes en la evaluación y mitigación de posibles amenazas a la seguridad, la comunicación eficaz de cuestiones de ciberseguridad y la notificación precisa de amenazas e infracciones a través de los canales adecuados dentro de su organización.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, entornos simulados, competiciones de captura de la bandera, 5E, CBL, CL, POGIL, PBL, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Simulaciones Competiciones

Contenido del módulo: desglose de los temas	**Horas de trabajo presencial**					**Horas de trabajo individual y tareas**	
	Clases	Consultas	Prácticas (HEI)	Exámenes	**Todo el trabajo de contacto**	**Trabajo individual**	**Tareas**
Gestión de proyectos • Planificación de proyectos • Definición de los objetivos del proyecto • Definición del alcance y los requisitos del proyecto • Preparación del calendario del proyecto	8	0,5	3	0,5	**12**	**6**	• Planificar un proyecto de concienciación sobre ciberseguridad para los empleados de las pymes. • Defina objetivos claros para el proyecto de

• Herramientas de gestión de proyectos • Amenazas actuales para la ciberseguridad (DDoS, ransomware, malware, phishing, zero-day, ataques a IoT, etc.) • Modelización de amenazas y análisis de vulnerabilidades • Planes de respuesta ante emergencias e incidentes • Notificación de amenazas e incidentes de ciberseguridad							concienciación sobre ciberseguridad con el fin de mejorar la comprensión de los empleados de las pymes sobre las posibles amenazas a la seguridad. • Esbozar el alcance y los requisitos del proyecto de concienciación sobre ciberseguridad para los empleados de las pymes, incluidos los temas de formación y los recursos necesarios. • Preparar el calendario del proyecto de concienciación sobre ciberseguridad para empleados de pymes. • Utilizar herramientas de gestión de proyectos para supervisar el progreso y la utilización de los recursos del proyecto de concienciación sobre ciberseguridad dirigido a los empleados de las pymes. • Investigar las amenazas actuales de ciberseguridad y recopilar los resultados en un informe. • Crear un modelo de amenazas simplificado para ayudar a los empleados de las pymes a identificar posibles vulnerabilidades de seguridad en sus operaciones diarias. • Buscar y revisar ejemplos de planes de respuesta a emergencias e incidentes. • ¿Qué pasos deben tenerse en cuenta al preparar un informe sobre la notificación de amenazas e incidentes de ciberseguridad? Investigue y resuma.

Gestión de recursos • Gestión de recursos humanos (equipos de proyecto) • Concienciación sobre seguridad y formación del equipo • Gestión del inventario de hardware y software • Herramientas y software de seguridad • Uso eficaz de los recursos tecnológicos • Asignación de presupuesto y recursos	8	0,5	3	0,5	**12**	**6**	• Planifica una estrategia de gestión de recursos para garantizar el uso eficaz de los recursos de una pyme ficticia. • Crear un plan temático de muestra para la formación en materia de ciberseguridad. • Preparar un inventario de hardware y software para una PYME ficticia. • Investigar las herramientas y el software de seguridad más utilizados. • Crear un presupuesto de muestra y un plan de asignación de recursos para una PYME hipotética.
Métricas de seguridad • Métricas de seguridad y técnicas de medición • Recopilación de datos con SIEM • Análisis de métricas de seguridad • Supervisión del proyecto y evaluación del rendimiento • Revisión de acciones y adaptación del proyecto • Informes sobre métricas de seguridad	8	0,5	4	0,5	**13**	**6**	• Investigar las métricas de seguridad utilizadas para evaluar la postura de ciberseguridad en las pymes. • Investiga las fuentes de las que el software SIEM recopila registros. • Configure y examine un software SIEM de código abierto. • Analizar las métricas de seguridad mediante la recopilación de registros con el software SIEM. • Informar de los resultados del análisis de las métricas de seguridad con gráficos y elementos visuales.
Control de calidad y control de calidad • Gestión de la calidad • Normas de calidad en ciberseguridad • Auditorías de cumplimiento y calidad • Técnicas de prueba y validación • Recomendaciones de evaluación y mejora	8	0,5	4	0,5	**13**	**7**	• ¿Cómo deben planificarse los procesos de garantía y control de calidad para mejorar la eficacia de las aplicaciones de ciberseguridad en las pymes? Investigue y resuma. • Investigue los elementos de control del anexo

							A de la norma ISO/IEC 27001:2022. • Investigue e informe sobre qué son las técnicas de prueba y validación. • ¿Qué beneficios aportan a las pymes la revisión y la mejora continuas de los procesos de calidad?
Total	**32**	**2**	**14**	**2**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Prueba de autoevaluación I	10%	10 puntos: 95-100 % de respuestas correctas. 9 puntos: 85-94 % de respuestas correctas. 8 puntos: 75-84 % de respuestas correctas. 7 puntos: 65-74 % de respuestas correctas. 6 puntos: 55-64 % de respuestas correctas. 5 puntos: 45-54 % de respuestas correctas. 4 puntos: 35-44 % de respuestas correctas. 3 puntos: 25-34 % de respuestas correctas. 2 puntos: 15-24 % de respuestas correctas. 1 punto: 0-14 % de respuestas correctas.
Prueba de autoevaluación II	10%	
Prueba de autoevaluación III	10%	
Prueba de autoevaluación IV	10%	
Prueba de evaluación de conocimientos	60%	

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*
Lecturas obligatorias
Lecturas recomendadas
https://sansorg.egnyte.com/dl/RFrVIbX2oc https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2: ADMINISTRACIÓN DE SISTEMAS

Título del módulo	**Código del módulo**
ADMINISTRACIÓN DE SISTEMAS	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, mixto	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
Ninguno

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75	50	25

Objetivo y resultados del módulo		
Al finalizar este curso, los alumnos serán capaces de gestionar de forma continua (identificar, analizar, evaluar, estimar y mitigar) los riesgos relacionados con la ciberseguridad de las infraestructuras, los sistemas y los servicios de las TIC mediante la planificación, la aplicación, la notificación y la comunicación del análisis, la evaluación y el tratamiento de riesgos. Los estudiantes conocerán los fundamentos de las redes para gestionar adecuadamente los dispositivos de red, operar en servidores Linux y Windows, gestionándolos y protegiéndolos. Además, los conocimientos sobre la nube y la inteligencia artificial en el contexto de la ciberseguridad les resultarán muy útiles para acelerar adecuadamente las tareas y realizar automatizaciones y escalados. Los estudiantes también aprenderán a reforzar los sistemas, realizar la búsqueda de amenazas y garantizar la disponibilidad de los servidores (acrónimo de la tríada CIA).		
Resultados del aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**

Conocimientos: Los alumnos adquirirán conocimientos sobre administración de redes, sistemas operativos, fundamentos de redes, herramientas de administración de redes, seguridad de dispositivos de red, administración de sistemas Linux, administración de sistemas Windows, virtualización, computación en la nube utilizando IA para procedimientos de redes y ciberseguridad, procedimientos de ciberseguridad, detección de amenazas, análisis de amenazas, respuesta a amenazas, remediación de amenazas, fundamentos de ciberseguridad, defensa de la organización contra ataques, seguridad de infraestructuras y redes, supervisión y análisis de redes, gestión de incidentes. Serán capaces de establecer y describir procedimientos eficaces de administración de sistemas y rutinas operativas adaptadas a las necesidades específicas de los lugares de trabajo de las pymes en materia de normas de cumplimiento.	A elección del profesor: clases presenciales, grabaciones de vídeo, presentaciones, dispositivos virtuales (si procede), análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre iguales, tutorías.	Pruebas de autoevaluación y pruebas de evaluación de conocimientos.
Habilidades: Los alumnos aprenderán a utilizar metodologías y herramientas para diseñar e implementar arquitecturas de sistemas seguras, incluidos sistemas operativos, bases de datos, redes e infraestructuras en la nube para lugares de trabajo de pymes.	A elección del profesor: clases en directo, grabaciones de vídeo, presentaciones, dispositivos virtuales (si procede), análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre iguales, tutorías.	Pruebas de autoevaluación y pruebas de evaluación de conocimientos
Competencias: Los alumnos serán competentes para desarrollar e implementar marcos estratégicos de ciberseguridad para la administración de sistemas, liderar proyectos y equipos para mejorar el fortalecimiento y la disponibilidad de los sistemas, y tomar decisiones éticas para mantener prácticas sólidas de ciberseguridad en diversos ámbitos administrativos para los lugares de trabajo de las pymes.	A elección del profesor: clases en directo, grabaciones de vídeo, presentaciones, dispositivos virtuales (si procede), análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre iguales, tutorías.	Pruebas de autoevaluación y pruebas de evaluación de conocimientos.

Contenido del módulo: desglose de los temas	Horas de trabajo presencial					Horas de trabajo individual y tareas	
	Clases	Consultas	Prácticas (HEI)	Exámenes	**Todo el trabajo**	**Trabajo individual**	**Tareas**
Administración de sistemas operativos • Sistemas operativos • Relación entre hardware y soft-ware • 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 adminis-trador 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 co-mandos • Manipulación de archivos y carpe-tas • Trabajo con tuberías y comandos de supervisión del sistema • Gestión de procesos y control de tareas • Gestión de servicios	4	0,5	2	0,5	**7**	**3,5**	Recuento hexadecimal Practicar comandos de Windows Práctica con comandos de Linux Práctica con el Administrador de tareas Creación y gestión de archivos Modificación y visualización de claves y valores del Registro Modificación de la configuración del Panel de control Gestión de usuarios y grupos Gestión de la estructura del dominio Creación y eliminación de objetos de Active Directory Gestión de procesos en Linux Manipulación de archivos y carpetas Trabajar con tuberías Comandos de supervisión del sistema Gestión de servicios Linux
Administración del sistema de bases de datos • Repositorios y listas de fuentes • Gestión de un servidor web	4	0,5	2	0,5	**7**	**3,5**	Gestión de 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							Verificación y gestión de registros del sistema y supervisión de registros Programación de tareas en Linux Solución de problemas del servidor Restauración de copias de seguridad Protección de GRUB Gestión de servicios de bases de datos Configuración de políticas de contraseñas Configuración de políticas de bloqueo de cuentas Configuración de la autenticación y el control de acceso
Administración de redes • Tipos de redes y redes inalámbricas • Redes y topologías • Identidad y acceso de dispositivos • Dispositivos de infraestructura y seguridad • Dispositivos especializados y arquitectura de red • Redes virtuales • Direcciones físicas y lógicas • Modelos OSI y de red • Encapsulación y descapsulación de datos	4	0,5	2	0,5	**7**	**3,5**	Creación de topologías de red Gestión de dispositivos de red Construcción de la red Protección de dispositivos de red Creación de redes virtuales Configuración de protocolos de red y números de puerto Trabajar con Cisco Packet Tracer

• 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 direc-ciones (ARP) • Direccionamiento IP estático frente a dinámico • Traducción de direcciones de red (NAT) • Conmutadores y Cisco IOS • Seguridad de puertos de conmu-tadores e interfaces de enrutado-res • Configuración de VLAN y DTP • Enrutamiento entre VLAN • Introducción a las ACL • Solución de problemas de red							Trabajar con el protocolo de resolución de direcciones (ARP) Planificación de una red Configuración de direcciones IP estáticas y dinámicas Configuración de DHCP y NAT Trabajar con Cisco IOS Configuración de VLAN Solución de problemas de red
Administración de la nube • 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 • 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	4	0,5	2	0,5	**7**	**3,5**	Creación de máquinas virtuales Configuración de contenedores Protección de entornos virtuales Trabajar con copias de seguridad Gestión de redes en la nube Configuración de redes virtuales Trabajar con herramientas de supervisión de la nube Implementación de la automatización y la orquestación Detección de amenazas y vulnerabilidades de seguridad en la nube Configuración de la gestión de identidades y accesos (IAM) Implementación del cifrado de datos en la nube Trabajar con Docker y Kubernetes

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 tablas rainbow • Spoofing MAC y envenenamiento ARP • VLAN Hopping y DHCP malicioso • 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	4	0,5	2	0,5	**7**	**3,5**	Configuración de la infraestructura Componentes principales Implementación de controles de seguridad Trabajar con TACACS+ y RADIUS Configuración de AAA Experimentar con el cifrado y descifrado Análisis de ataques comunes y técnicas de defensa Configuración de zonas desmilitarizadas (DMZ) Investigación de honeypots Fortalecimiento mediante las mejores prácticas para una red segura Instalación de VPN Trabajar con Secure Shell (SSH) Trabajo con Virtual Network Computing (VNC) Técnicas de trabajo con cortafuegos Implementación de IA en cortafuegos Uso de Snort y tcpdump para la protección y la detección
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 • Gestión de activos de TI e inventario	4	0,5	2	0,5	**7**	**3,5**	Trabajar con técnicas de GenAI Gestión de cuentas de usuario y control de acceso Detección de anomalías y resolución de problemas Resolución de errores del servicio Apache2 con GenAI Configuración de la gestión de parches y actualizaciones Configuración de copias 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 • Gobernanza y marcos normativos • Configuración y seguridad del 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							Gestión de activos de TI Recuperación de archivos eliminados con GenAI Implementación de la seguridad DNS y DHCP Trabajar con Microsoft BitLocker y Microsoft AppLocker Configuración del firewall de Microsoft Configuración de la seguridad de puertos de conmutador Protección del protocolo de transferencia de archivos (FTP) Protección del protocolo de escritorio remoto (RDP) Programación de tareas de seguridad en Linux Protección de GRUB Configuración y seguridad de cortafuegos (iptables)
Disponibilidad • IR frente a SOC • Eventos e incidentes • Detección 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)	4	0,5	3	0,5	**8**	4	Detección de eventos e incidentes Realización de la clasificación de alertas Elaboración de documentación e informes adecuados Implementación de actividades posteriores al incidente Realizar y proteger contra DoS y DDoS

• Falsificación de solicitudes entre sitios (CSRF) • Fuerza bruta y relleno de credenciales • Pasar el hash y pasar el ticket • Reconocimiento LDAP • 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 • Análisis estático y dinámico del malware • Análisis seguro del malware • Análisis híbrido Investigación de malware • Realización de análisis estático y dinámico 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							Detección de ataques web y propagación de malware Realizar análisis seguros de malware estático y dinámico Gestión de IOC Configuración de políticas de contraseñas Configuración de políticas de «traiga su propio dispositivo» (BYOD) Configuración de políticas de acceso remoto
Total	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Prueba de autoevaluación (1)	5 %	10 puntos: 95-100 % de respuestas correctas. 9 puntos: 85-94 % de respuestas correctas. 8 puntos: 75-84 % de respuestas correctas. 7 puntos: 65-74 % de respuestas correctas. 6 puntos: 55-64 % de respuestas correctas. 5 puntos: 45-54 % de respuestas correctas. 4 puntos: 35-44 % de respuestas correctas. 3 puntos: 25-34 % de respuestas correctas. 2 puntos: 15-24 % de respuestas correctas. 1 punto: 0-14 % de respuestas correctas.
Prueba de autoevaluación (2)	5 %	
Prueba de autoevaluación (3)	5 %	
Prueba de autoevaluación (4)	5 %	
Prueba de autoevaluación (5)	5 %	
Prueba de autoevaluación (6)	5 %	
Prueba de autoevaluación (7)	5 %	
Prueba de evaluación de conocimientos	65 %	

3. M3: HERRAMIENTAS ANALÍTICAS

Título del módulo	Código del módulo
HERRAMIENTAS ANALÍTICAS	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, híbrido	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
Ninguno

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75	50	25

Objetivo y resultados del módulo		
Al finalizar este curso, los alumnos habrán adquirido las habilidades necesarias para proteger los activos de la organización mediante métricas de rendimiento, análisis de datos e inteligencia de seguridad. Aprenderán a aplicar eficazmente herramientas analíticas para identificar posibles riesgos y vulnerabilidades de ciberseguridad, a aprovechar la información basada en datos para mejorar las medidas de seguridad y a utilizar métricas de rendimiento relacionadas con contraseñas, uso del navegador, correo electrónico y aplicaciones de procesamiento de datos. Al finalizar el módulo, los participantes serán capaces de evaluar y mitigar las posibles amenazas de seguridad utilizando las herramientas adecuadas e informar de cualquier amenaza o interrupción a los canales reglamentarios correspondientes.		
Resultados del aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**
Conocimientos: Los alumnos adquirirán conocimientos prácticos sobre cómo aplicar mediciones de rendimiento, análisis de datos e inteligencia de seguridad para proteger los activos de la organización.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, clases teóricas, ponentes invitados, cuestionarios, juegos, tareas prácticas/laboratorios, enseñanza y aprendizaje entre pares, aprendizaje autoguiado, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad de las pymes».	Pruebas de autoevaluación Prueba de evaluación de conocimientos

Habilidades: Los alumnos aprenderán a utilizar herramientas analíticas para identificar posibles riesgos y vulnerabilidades de ciberseguridad, aplicar conocimientos basados en datos para reforzar las prácticas de ciberseguridad y utilizar métricas de rendimiento para evaluar y mejorar la seguridad de las contraseñas, la navegación, el correo electrónico y el manejo de datos.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, tareas prácticas/laboratorios, actividades prácticas, entornos simulados, cuestionarios, juegos, estudios de casos, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Evaluaciones prácticas
Competencias: Los alumnos serán competentes en la evaluación y mitigación de posibles amenazas de seguridad utilizando herramientas analíticas, informando con precisión de las amenazas y violaciones a los canales adecuados dentro de su organización.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, entornos simulados, competiciones de captura de la bandera, 5E, CBL, CL, POGIL, PBL, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Simulaciones Competiciones

Contenido del módulo: desglose de los temas	**Horas de trabajo presencial**					**Horas de trabajo individual y tareas**	
	Clases magistrales	Consultas	Prácticas (HEI)	Exámenes	**Todo el trabajo de contacto**	**Trabajo individual**	**Tareas**
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	10	0,5	5	0,5	**16**	**8,5**	• Investigar sobre métricas y herramientas de rendimiento. Comparar herramientas de supervisión del rendimiento e identificar sus diferencias. • Completar la instalación de Zabbix y realizar la configuración básica. • Crear una aplicación para supervisar métricas de rendimiento con Zabbix.

							• Identifique las vulnerabilidades del sistema objetivo utilizando software de mapeo de redes (como nmap, rustscan, etc.). • Realizar un análisis de vulnerabilidades en el sistema objetivo utilizando el software Nessus. Preparar un informe de pruebas de vulnerabilidad. • Realizar un análisis del tráfico de red utilizando Wireshark.
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	10	0,5	5	0,5	**16**	**8,5**	• Realizar pasos de limpieza y preprocesamiento de datos en un conjunto de datos relacionado con cuestiones de ciberseguridad preparado para una PYME hipotética. • Analizar el conjunto de datos limpiado y preprocesado de la PYME hipotética y visualizar los resultados. • ¿Cuáles son algunos ejemplos de aplicaciones del análisis de datos en la ciberseguridad? Investigue.
Inteligencia de seguridad • Comprender la inteligencia de seguridad • Fuentes de inteligencia de seguridad • Métodos de recopilación de inteligencia sobre amenazas • Marcos de inteligencia sobre amenazas • Plataformas de inteligencia de seguridad basadas en IA • Casos prácticos sobre aplicaciones de inteligencia de seguridad	10	0,5	7	0,5	**18**	**8**	• Investigue cómo la inteligencia de seguridad contribuye a las estrategias de seguridad proactivas de las pymes. • ¿Cuáles son las fuentes más comunes para obtener inteligencia de seguridad? ¿Cómo se evalúa la fiabilidad de estas fuentes? • Defina las ventajas y limitaciones de cada método de recopilación de inteligencia sobre amenazas. • Explique las características principales de los marcos de inteligencia sobre amenazas, como

							MITRE ATT&CK y Cyber Kill Chain. • Examine un caso práctico real en el que se utilizó la inteligencia de seguridad. Describa los métodos de recopilación de inteligencia utilizados en ese caso práctico.
Total	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Estrategia de evaluación	Porcentaje de ponderación comparativa	Criterios de evaluación
Prueba de autoevaluación I	15%	10 puntos: 95-100 % de respuestas correctas. 9 puntos: 85-94 % de respuestas correctas. 8 puntos: 75-84 % de respuestas correctas. 7 puntos: 65-74 % de respuestas correctas. 6 puntos: 55-64 % de respuestas correctas. 5 puntos: 45-54 % de respuestas correctas. 4 puntos: 35-44 % de respuestas correctas. 3 puntos: 25-34 % de respuestas correctas. 2 puntos: 15-24 % de respuestas correctas. 1 punto: 0-14 % de respuestas correctas.
Prueba de autoevaluación II	15%	
Prueba de autoevaluación III	15%	
Prueba de evaluación de conocimientos	55%	

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*
Lecturas obligatorias
...
Lecturas recomendadas
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4: OPERACIONES DE SEGURIDAD

Título del módulo	Código del módulo
OPERACIONES DE SEGURIDAD	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, mixta, consultas	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
Ninguno

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75	50	25

Objetivo y resultados del módulo		
Al finalizar este curso, los estudiantes serán capaces de gestionar eficazmente las operaciones de seguridad dentro de las infraestructuras, los sistemas y los servicios de las TIC. Adquirirán las habilidades necesarias para supervisar, detectar, responder y recuperarse de incidentes de ciberseguridad mediante la aplicación de las mejores prácticas, herramientas y marcos relevantes para las operaciones de seguridad.		
Resultados del aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**
Conocimientos: Los alumnos adquirirán conocimientos avanzados sobre operaciones de seguridad, incluyendo supervisión, detección, respuesta a incidentes y recuperación. Serán capaces de establecer y describir rutinas operativas de ciberseguridad eficaces adaptadas a las necesidades específicas de los lugares de trabajo de las pymes en cumplimiento de las normas de ciberseguridad.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza, por ejemplo, clases teóricas, análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre pares, tutorías, etc.] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Pruebas de autoevaluación Prueba de evaluación de conocimientos

Habilidades: Los alumnos serán capaces de aplicar metodologías y herramientas avanzadas para realizar tareas de operaciones de seguridad, diseñar e implementar estrategias de supervisión eficaces, llevar a cabo respuestas a incidentes y desarrollar rutinas operativas sólidas específicamente adaptadas a los lugares de trabajo de las pymes.	A seleccionar por el profesor, de la parte 1.3. [*Métodos de enseñanza, por ejemplo, clases teóricas, análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre pares, tutorías, etc.]* de D2.3 *«Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes»*.	Pruebas de autoevaluación. Prueba de evaluación de conocimientos
Competencias: Los alumnos serán competentes en el desarrollo y la implementación de políticas y procedimientos estratégicos de operaciones de seguridad para los lugares de trabajo de las pymes.	A seleccionar por el profesor, de la parte 1.3. [*Métodos de enseñanza, por ejemplo, clases teóricas, análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre iguales, tutorías, etc.]* de D2.3 *«Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes»*.	Pruebas de autoevaluación Prueba de evaluación de conocimientos

Contenido del módulo: desglose de los temas	**Horas de trabajo presencial**					**Horas de trabajo individual y tareas**	
	Clases magistrales	Consultas (pymes)	Prácticas (IES)	Pruebas	Todo el trabajo presencial	Trabajo individual	Tareas

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	6	0,5	2	0,5	**9**	6	Identificar y comprender la estructura y la función de un SOC, analizar diversas funciones dentro de las operaciones de seguridad, investigar las herramientas utilizadas en las operaciones de seguridad y analizar un caso práctico.
Convergencia de la seguridad - Comprensión de la convergencia de la seguridad - Fundamentos de la seguridad física (principios de seguridad física, protección de activos físicos, políticas) - Estudio de caso que destaca los principios de convergencia en materia de seguridad	8	0,5	4	0,5	**13**	6	Revisar la definición y los principios de la convergencia de la seguridad, reconocer la importancia de integrar las operaciones de seguridad física y digital, identificar y evaluar los riesgos en los ámbitos cibernético y físico.

Gestión de la información y los eventos de seguridad - Revisión de los principios de supervisión de la seguridad. - Implementación de soluciones SIEM	8	0,5	4	0,5	**13**	6	Introducción a la supervisión de la seguridad y la implementación de SIEM. Principios básicos, como tipos de registros, métodos de detección y ciclo de vida de la supervisión. Aspectos prácticos de la implementación de un SIEM, incluyendo arquitectura, recopilación de datos, creación de reglas y gestión de alertas.
Prácticas de operaciones de seguridad - Identificar fuentes de datos y optimizar la recopilación de registros - Centralizar las alertas con el SIEM - Prueba de su SIEM	4	0,5	10	0,5	**15**	7	Programa de formación completo y orientado a la práctica con conocimientos esenciales y habilidades prácticas en gestión de registros, configuración de SIEM y detección de amenazas en diversos entornos de TI.
Total	**26**	**2**	**20**	**2**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Prueba de autoevaluación (1)	10 %	10 puntos: 95-100 % de respuestas correctas. 9 puntos: 85-94 % de respuestas correctas. 8 puntos: 75-84 % de respuestas correctas. 7 puntos: 65-74 % de respuestas correctas. 6 puntos: 55-64 % de respuestas correctas.
Prueba de autoevaluación (2)	10 %	

Prueba de autoevaluación (3)	10 %
Prueba de autoevaluación (4)	10 %
Prueba de evaluación de conocimientos	60 %

5 puntos: 45-54 % de respuestas correctas.
4 puntos: 35-44 % de respuestas correctas.
3 puntos: 25-34 % de respuestas correctas.
2 puntos: 15-24 % de respuestas correctas.
1 punto: 0-14 % de respuestas correctas.

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*
Lectura obligatoria
Cybellium (2024). *Guía de estudio sobre los centros de operaciones de seguridad (SOC): una guía completa para aprender sobre los centros de operaciones de seguridad (SOC)* Muniz, J. (2021). *El centro de operaciones de seguridad moderno*. Pearson Education. ENISA (2017). *Estrategias para la respuesta a incidentes y la cooperación en caso de crisis cibernéticas*. **Estrategias para la respuesta a incidentes y la cooperación en caso de crisis cibernéticas — ENISA (europa.eu)**
Lecturas recomendadas
Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Centro de operaciones de seguridad de código abierto (SOC): guía completa para establecer, gestionar y mantener un SOC moderno. Cybellium (2023). Gestión de un centro de operaciones de seguridad (SOC).

5. M5: GOBERNANZA Y POLÍTICA DE SEGURIDAD

Título del módulo	Código del módulo
GOBERNANZA Y POLÍTICA DE SEGURIDAD	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial / Online / Híbrido	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
Ninguno

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75	50	25

Objetivo y resultados del módulo
La asignatura «Gobernanza y políticas de seguridad» tiene como objetivo preparar a los estudiantes para afrontar los retos de la ciberseguridad en las pymes, integrando la gobernanza de la seguridad en la estrategia empresarial y garantizando el cumplimiento de la normativa legal, como el RGPD. El módulo abarca aspectos como la identificación de amenazas y vulnerabilidades, el diseño de políticas de seguridad sólidas y adaptables y la gestión eficaz de incidentes. Además, se centra en el desarrollo de estructuras de gobernanza que asignen funciones claras en la organización, alineando la ciberseguridad con los objetivos estratégicos. Los estudiantes adquirirán competencias técnicas en la evaluación y mitigación de riesgos cibernéticos, y desarrollarán habilidades de análisis para proponer mejoras en la madurez de la seguridad. También aprenderán a comunicar eficazmente las necesidades de ciberseguridad a los ejecutivos, apoyando la toma de decisiones informadas y garantizando el cumplimiento normativo y la ética en materia de ciberseguridad. El módulo «Gobernanza y políticas de seguridad» también incorpora un examen específico de la prevención del phishing, los ciberataques impulsados por la inteligencia artificial y la gestión del ransomware, analizando cómo estas amenazas específicas requieren un enfoque integrado de la gobernanza y el cumplimiento normativo. La eficacia de las políticas de seguridad no solo se medirá por su capacidad para prevenir incidentes, sino también por su adaptabilidad a las amenazas emergentes y el cumplimiento de la normativa legal vigente.

Resultados del aprendizaje del módulo	Métodos de enseñanza y aprendizaje	Métodos de evaluación
Conocimientos: Los alumnos adquirirán conocimientos avanzados sobre cómo implementar nuevas rutinas y flujos de trabajo de ciberseguridad en los lugares de trabajo de las pymes, incorporando los principios y tendencias actuales de ciberseguridad y el cumplimiento de la legislación nacional e internacional relevante para su sector. Adquirir conocimientos avanzados sobre cómo integrar la prevención del phishing, gestionar las amenazas impulsadas por la IA y responder al ransomware en entornos de pymes.	**Clases magistrales (lecturas dirigidas):** Las clases magistrales proporcionarán una base conceptual sólida en materia de ciberseguridad, gobernanza, privacidad y cumplimiento normativo, fomentando la participación activa de los alumnos. Incluye clases interactivas que incorporan sesiones regulares de preguntas y respuestas, encuestas y ejercicios de resolución de problemas en directo. Utilizando herramientas como Mentimeter y Poll Everywhere, **Participación en debates y foros:** La participación en debates y foros permitirá a los alumnos debatir y analizar críticamente cuestiones de ciberseguridad, fomentando sus habilidades argumentativas. Se aplicará a cuestiones relacionadas con la ética, las políticas y la toma de decisiones en materia de ciberseguridad. **Estudios de** casos**:** Los estudios de casos permitirán a los estudiantes analizar situaciones de ciberseguridad en pymes, aplicando los conocimientos teóricos para resolver problemas reales. Se centrarán en temas como la gestión de violaciones de datos, el ransomware, el phishing, los ataques impulsados por la inteligencia artificial, la implementación de políticas de seguridad y la gobernanza.	**Pruebas de autoevaluación:** Las autoevaluaciones permiten a los alumnos evaluar su comprensión de cada subtema a través de una serie de preguntas, proporcionando información continua para identificar áreas de mejora. No afectan a la nota final, pero son fundamentales para el aprendizaje autodirigido. **Examen final (opcional):** El examen final es opcional y permite a los estudiantes obtener un certificado de finalización mediante la evaluación de su comprensión general del curso a través de preguntas de desarrollo, análisis de casos y preguntas de opción múltiple. Es necesario aprobarlo para obtener el certificado de finalización, mientras que aquellos que no lo realicen recibirán un certificado de asistencia.
Habilidades: Los alumnos adquirirán habilidades en el uso de metodologías avanzadas para realizar evaluaciones de riesgos, diseñar e implementar nuevas rutinas de	**Talleres prácticos:** Los talleres prácticos permitirán a los alumnos aplicar los conceptos de ciberseguridad a través de ejercicios como el desarrollo de políticas y simulaciones de incidentes, con comentarios en tiempo real del	**Evaluaciones prácticas:** Las evaluaciones prácticas a lo largo del curso permitirán a los alumnos aplicar los conocimientos teóricos a situaciones

ciberseguridad y preparar estrategias de respuesta, garantizando una gobernanza y un cumplimiento eficaces en los lugares de trabajo de las pymes. Desarrollar habilidades en el diseño y la implementación de rutinas integrales de ciberseguridad que aborden amenazas avanzadas y garanticen el cumplimiento normativo de la organización.	instructor. Están diseñados para reforzar las habilidades prácticas y preparar a los alumnos para aplicar lo que han aprendido en situaciones reales. **Trabajos prácticos y proyectos individuales:** Los trabajos prácticos y los proyectos individuales permitirán a los alumnos aplicar los conceptos de ciberseguridad a través de tareas como la redacción de políticas y el análisis de riesgos, desarrollando habilidades de trabajo autónomo y la aplicación práctica de los conocimientos teóricos. **Proyectos colaborativos:** Los proyectos colaborativos permitirán a los alumnos trabajar en equipo para desarrollar soluciones de ciberseguridad para pymes, incluyendo políticas de seguridad y modelos de gobernanza. Fomentarán el trabajo en equipo, la gestión de proyectos y la aplicación práctica de los conocimientos adquiridos, con comentarios de profesores y compañeros.	simuladas, como el desarrollo de políticas de ciberseguridad y simulaciones de incidentes, con el objetivo de evaluar su capacidad para resolver problemas reales en el contexto de las pymes. **Proyectos en grupo:** Los proyectos en grupo permitirán a los alumnos desarrollar un proyecto integral de ciberseguridad, desde la identificación de riesgos hasta la propuesta de modelos de gobernanza y planes de respuesta a incidentes, evaluando tanto la calidad del contenido como la capacidad de colaboración. Este proyecto es clave para la evaluación final e integra todo el aprendizaje del curso.
Competencias: Los alumnos serán competentes en el desarrollo y la implementación de políticas estratégicas de ciberseguridad, liderando iniciativas para establecer nuevas rutinas y flujos de trabajo en los lugares de trabajo de las pymes, y tomando decisiones éticas que se ajusten a los objetivos de la organización y a los requisitos de cumplimiento. Adquirirán competencia en la formulación y ejecución de políticas de ciberseguridad que prevengan amenazas cibernéticas sofisticadas y	**Simulaciones de escenarios:** Las simulaciones de escenarios permitirán a los alumnos gestionar incidentes de ciberseguridad en entornos virtuales que reproducen ataques reales, tomando decisiones estratégicas bajo presión. Este método mejora las habilidades en la gestión de crisis y la respuesta a incidentes, y es clave para enseñar la evaluación de políticas de seguridad y la toma de decisiones en situaciones críticas. Los estudiantes deberán demostrar cómo aplicarían las políticas de gobernanza para prevenir o responder a incidentes específicos, como ataques de phishing, ransomware y ataques impulsados por IA, evaluando su	**Simulaciones y gestión de incidentes:** Se evaluará la capacidad de los alumnos para gestionar incidentes de ciberseguridad en simulaciones que reproducen crisis reales en una pyme. El objetivo es medir su capacidad para manejar la presión, tomar decisiones estratégicas y ejecutar planes de respuesta en tiempo real, evaluando su aplicación práctica en situaciones dinámicas.

garanticen el cumplimiento de las normativas internacionales de ciberseguridad.	comprensión del marco normativo pertinente.	

Contenido del módulo: desglose de los temas	Horas de trabajo presencial					Horas de trabajo individual y tareas	
	Clases	Consultas	Prácticas (IES)	Pruebas	**Todo el trabajo**	**Trabajo**	**Tareas**
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 - Comprensión de 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.	5	0,5	3	0,5	**9**	**4**	Lectura, investigación, preparación de casos prácticos
Privacidad -Principios de privacidad en 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	4	0,5	3	0,5	**8**	**4**	Análisis de políticas, tarea individual
Leyes, ética y cumplimiento -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.	5	0,5	3	0,5	**9**	**5**	Estudio de caso, análisis legislativo

Gobernanza de la seguridad -Estructura de gobernanza de la ciberseguridad -Funciones y responsabilidades en la gestión de la seguridad -Modelos de madurez de la ciberseguridad -Integración de la ciberseguridad en la gobernanza corporativa -Mejorar las capacidades para realizar evaluaciones de riesgos y formular planes de respuesta estratégicos en condiciones de crisis simuladas (ransomware, ataques de phishing, etc.)	4	0,5	3	0,5	**8**	**4**	Análisis de escenarios de gestión de riesgos
Comunicación a nivel ejecutivo y directivo -Estrategias de comunicación sobre ciberseguridad -Informes de seguridad para la alta dirección -Toma de decisiones basada en datos de seguridad -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.	4	0,5	3	0,5	**8**	**4**	Preparación de presentaciones, comunicación con las partes interesadas
Política de gestión -Desarrollo de la política de seguridad -Implementación y supervisión de políticas -Evaluación y mejora continua de las políticas -Adaptación de las políticas de seguridad a los cambios tecnológicos y normativos -Exploración de cómo unas políticas eficaces de formación y sensibilización pueden ser un componente crucial del cumplimiento normativo y la mitigación de riesgos.	4	0,5	3	0,5	**8**	**4**	Redacción y revisión de un documento normativo
Total	**26**	**3**	**18**	**3**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Autoevaluación I	10%	Evaluación de conceptos fundamentales sobre el contexto organizativo.
Autoevaluación II	10%	Evaluación de conceptos fundamentales sobre privacidad.
Autoevaluación III	10%	Evaluación de leyes, ética y políticas de cumplimiento.
Autoevaluación IV	10%	Evaluación de políticas de ciberseguridad.
Autoevaluación V	10%	Evaluación de la comunicación a nivel ejecutivo.

Autoevaluación VI	10%	Evaluación de las políticas de gestión y la creación de políticas en materia de seguridad.
Prueba de evaluación de conocimientos	40%	Examen final que abarca preguntas integradoras sobre todos los temas del curso.

10 puntos: 95-100 % de respuestas correctas.
9 puntos: 85-94 % de respuestas correctas.
8 puntos: 75-84 % de respuestas correctas.
7 puntos: 65-74 % de respuestas correctas.
6 puntos: 55-64 % de respuestas correctas.
5 puntos: 45-54 % de respuestas correctas.
4 puntos: 35-44 % de respuestas correctas.
3 puntos: 25-34 % de respuestas correctas.
2 puntos: 15-24 % de respuestas correctas.
1 punto: 0-14 % de respuestas correctas.

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL).*

Lectura obligatoria

...

«EU Cybersecurity Law: Governing Resilience and Coherence in the Digital Age» (Ley de ciberseguridad de la UE: gobernanza de la resiliencia y la coherencia en la era digital), de Luisa Marin

- Este libro ofrece un análisis en profundidad de las leyes y políticas de ciberseguridad de la UE, fundamentales para comprender cómo se estructura y se aplica la gobernanza de la ciberseguridad en el contexto de la UE.

«La ciberseguridad en la Unión Europea: resiliencia y adaptabilidad en la política de gobernanza», de George Christou

- Este libro explora los marcos de gobernanza y los procesos de elaboración de políticas para la ciberseguridad dentro de la UE, lo que ayuda a los estudiantes a comprender la interacción dinámica entre los diferentes niveles de gobernanza.

«Phishing y contramedidas: comprender el creciente problema del robo de identidad electrónica», de Markus Jakobsson y Steven Myers

- Aunque no es específico de la UE, el análisis detallado de las técnicas de phishing y las contramedidas que ofrece este libro puede contextualizarse en el marco de la UE centrándose en el cumplimiento del RGPD y los principios de protección de datos.

«Legislación y normativa europea en materia de ciberseguridad», editado por Nadya Purtova y Bert-Jaap Koops

- Este volumen editado abarca las medidas legales y reglamentarias específicas de la ciberseguridad en la Unión Europea, incluidos los retos de cumplimiento y marcos como la Directiva NIS y el RGPD.

«Ransomware: Understanding Digital Extortion and its Threat to Your Organization» (Ransomware: comprender la extorsión digital y su amenaza para su organización), de Allan Liska y Timothy Gallo

- Este texto, complementado con estudios de casos y ejemplos específicos de la UE, ayudará a los estudiantes a comprender las implicaciones de los ataques de ransomware en el marco de la normativa de la UE.

Lecturas recomendadas
«El Reglamento General de Protección de Datos (RGPD) de la UE: un comentario», de Lukas Feiler y Nikolaus Forgó • Este comentario ofrece información detallada sobre el RGPD, esencial para comprender el panorama normativo de la UE y su impacto en las prácticas de ciberseguridad. **«Protección de datos y ciberseguridad en Europa: marcos jurídicos y consideraciones prácticas»,** de Paul Lambert • Este libro ofrece información práctica sobre la armonización de las estrategias de protección de datos y ciberseguridad en la UE, incluido el cumplimiento de la normativa y las mejores prácticas en materia de medidas de seguridad. **«Seguridad de las redes y la información: perspectivas europeas e internacionales»,** editado por Jeanne Pia Mifsud Bonnici y Joe Cannataci • Esta recopilación examina el panorama de la seguridad de las redes y la información desde perspectivas tanto europeas como internacionales, proporcionando un contexto más amplio para los esfuerzos de la UE en materia de ciberseguridad. **«Inteligencia artificial en la ciberseguridad: prácticas, retos y ética»,** de Elena Fersman y Martin Fredriksson • Una visión general completa de la integración de las tecnologías de IA en la ciberseguridad, que aborda los retos éticos, operativos y normativos, especialmente pertinentes en el contexto de la UE. **«La ciberseguridad en la era digital: herramientas, técnicas y aplicaciones»,** de Gregory B. White, Eric A. Fisher y James L. Antonakos • Aunque no se centra exclusivamente en la UE, este libro también abarca una amplia gama de temas relacionados con la ciberseguridad moderna.

Material de estudio *(materiales originales de HackerU y Cybint)*
Lecturas obligatorias
• Administración de redes TCP/IP: Ayuda para administradores de sistemas Unix, 3.ª edición, de Craig Hunt (O'Reilly). • Referencia de bolsillo esencial para la administración de sistemas: comandos y formatos de archivo (Pocket Administrator), de Eleen Frisch (O'Reilly). • Redes informáticas: guía para principiantes para dominar las redes informáticas, Internet y el modelo OSI, de Ramon Nastase
Lecturas recomendadas
• Certificación CompTIA A+ All-in-One For Dummies (Informática/Tecnología), 5.ª edición, de Glen E. Clarke, Edward Tetz y Timothy L. Warner • Coding All-in-One For Dummies, 1.ª edición, de Nikhil Abraham • Fundamentos de la tecnología de la información, volumen 1: Introducción a los sistemas de información, de Eric Frick • Arquitectura de TI para principiantes, 1.ª edición, de Kalani Kirk Hausman y Susan L. Cook

- Ciberseguridad para Dummies (Informática/Tecnología), 1.ª edición, de Steinberg
- Linux para Dummies, 10.ª edición, 10.ª edición, de Richard Blum
- Windows 10 para Dummies, 3.ª edición (Informática/Tecnología), 3.ª edición, de Rathbone
- Redes para principiantes, 12.ª edición, de Doug Lowe

6. M6: PLANIFICACIÓN DE LA CIBERSEGURIDAD

Título del módulo	Código del módulo
PLANIFICACIÓN DE LA CIBERSEGURIDAD	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, mixta, consultas	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
-

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75	50	25

Objetivo y resultados del módulo

Al finalizar este curso, los estudiantes serán capaces de comprender y aplicar los principios básicos de la planificación y la gestión de la ciberseguridad. Adquirirán la capacidad de implementar normas y marcos internacionales, desarrollar estrategias de seguridad a largo plazo, gestionar medidas operativas y tácticas de ciberseguridad y planificar arquitecturas de red seguras, como la nube y el modelo «zero trust». Además, los estudiantes estarán preparados para diseñar planes eficaces de respuesta a incidentes e implementar estrategias de continuidad del negocio, garantizando la resiliencia de la organización y la eficacia de las medidas de ciberseguridad ante las amenazas en constante evolución.

Resultados del aprendizaje del módulo	Métodos de enseñanza y aprendizaje	Métodos de evaluación
Conocimientos: Los alumnos adquirirán conocimientos avanzados sobre cómo integrar los principios avanzados de ciberseguridad y las tendencias actuales en la planificación estratégica y la gestión operativa.	Clases magistrales, estudios de casos, debates en grupo, aprendizaje autodirigido.	Pruebas de autoevaluación, pruebas de evaluación de conocimientos.
Habilidades: Los alumnos adquirirán habilidades en planificación estratégica y gestión operativa, lo que les permitirá diseñar e implementar de manera eficaz estrategias de ciberseguridad que aborden los riesgos emergentes y garanticen respuestas tácticas sólidas.	Ejercicios prácticos, talleres, estudios de casos.	Evaluaciones basadas en proyectos, evaluaciones prácticas.

Competencias: Los alumnos serán competentes en el desarrollo y la implementación de marcos estratégicos de ciberseguridad, así como en la dirección y gestión de iniciativas de ciberseguridad.	Talleres, seminarios, ejercicios de juego de roles	Evaluación continua, pruebas basadas en escenarios.

Contenido del módulo: desglose de los temas	**Horas de trabajo presencial**					**Horas de trabajo individual y tareas**	
	Clases	Consultas	Prácticas (HEI)	Exámenes	**Todo el trabajo de contacto**	**Trabajo individual**	**Tareas**
1. Introducción a la planificación de la ciberseguridad: seguridad de los datos, las personas y 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)	8	0,5	6	0,5	**15**	**8**	Definir los aspectos legales de la seguridad de los datos, las personas y la sociedad, así como las leyes y políticas que rigen los datos en las pymes. Clasificar los tipos de ciberataques relevantes para las pymes. Identificar herramientas útiles para prevenir ciberataques.
2. Planificación estratégica -Definición de metas y objetivos de ciberseguridad. -Análisis DAFO (fortalezas, debilidades, oportunidades y amenazas). -Desarrollar estrategias de seguridad a largo plazo -Establecimiento de indicadores clave de rendimiento (KPI) -Revisión y actualización de la estrategia de seguridad	8	2	6	2	**18**	**8**	Definir los objetivos de ciberseguridad relevantes para las pymes mediante un análisis DAFO, desarrollar estrategias a largo plazo para abordar los riesgos, asignar los recursos y el presupuesto correspondientes, establecer indicadores clave de rendimiento (KPI) para medir el progreso y actualizar periódicamente la estrategia en función de las nuevas amenazas.

3. 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 los empleados	8	1	6	2	**17**	**9**	Implemente medidas de control de acceso para restringir el acceso no autorizado, mantenga los sistemas mediante la gestión de parches, establezca un sistema de supervisión para detectar actividades inusuales y proporcione a los empleados formación sobre ciberseguridad.
Total	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Prueba de autoevaluación (1)	10%	10 puntos: 96-100 % de respuestas correctas. 9 puntos: 91-95 % de respuestas correctas. 8 puntos: 86-90 % de respuestas correctas. 7 puntos: 80-85 % de respuestas correctas. 6 puntos: 70-79 % de respuestas correctas. 5 puntos: 60-69 % de respuestas correctas. 4 puntos: 50-59 % de respuestas correctas. 3 puntos: 40-49 % de respuestas correctas. 2 puntos: 30-39 % de respuestas correctas. 1 punto: 0-29 % de respuestas correctas.
Prueba de autoevaluación (2)	10%	
Prueba de autoevaluación (3)	10%	
Prueba de evaluación de conocimientos	70%	

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*

Lectura obligatoria

1. Nair, A. y Greeshma, M. R. (2023). Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing Limited.
2. Falco, G. J. y Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press.
3. Marco de ciberseguridad (CSF) 2.0 del NIST, Instituto Nacional de Estándares y Tecnología, 26 de febrero de 2024

Lecturas recomendadas

1. Mehta, S. (2023). *Guía para el examen de certificación CRISC® (Certificado en Control de Riesgos y Sistemas de Información) de ISACA*. Packt Publishing Limited.
2. Gregory, P. H. (2021). *Guía completa para el examen CISM Certified Information Security Manager*. McGraw-Hill.
3. ISACA. (2021). *Manual de revisión CRISC, 7.ª edición*. ISACA.
4. Parlamento Europeo y Consejo. (14 de diciembre de 2022). *Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero*.
5. Guía del Reglamento General de Protección de Datos (RGPD), Oficina del Comisionado de Información.

7. M7: GESTIÓN Y MITIGACIÓN DE RIESGOS

Título del módulo	Código del módulo
GESTIÓN Y MITIGACIÓN DE RIESGOS	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, mixta, consultas	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos			
Ninguno			
Número de créditos ECTS asignados	**Carga de trabajo del estudiante**	**Horas de trabajo presencial**	**Horas de trabajo individual**
3	75	50	25

Objetivo y resultados del módulo		
Al finalizar este curso, los alumnos serán capaces de gestionar de forma continua (identificar, analizar, evaluar, estimar y mitigar) los riesgos relacionados con la ciberseguridad de las infraestructuras, los sistemas y los servicios de las TIC mediante la planificación, la aplicación, la notificación y la comunicación del análisis, la evaluación y el tratamiento de riesgos.		
Resultados del aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**
Conocimientos: Los alumnos adquirirán conocimientos avanzados sobre los procesos de gestión de riesgos, incluyendo la identificación, evaluación y control de riesgos, lo que les permitirá establecer y describir rutinas de ciberseguridad eficaces adaptadas a las necesidades específicas de los lugares de trabajo de las pymes, de conformidad con las normas nacionales e internacionales.	A seleccionar por el profesor, de la parte 1.3. [*Métodos de enseñanza, por ejemplo, clases teóricas, análisis de bibliografía, ponentes invitados, enseñanza y aprendizaje entre iguales, tutorías, etc.]* de D2.3 «*Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes*».	Pruebas de autoevaluación Prueba de evaluación de conocimientos

Habilidades: Los alumnos adquirirán las habilidades necesarias para aplicar metodologías y herramientas avanzadas para realizar evaluaciones de riesgos exhaustivas, diseñar y aplicar estrategias eficaces de gestión de riesgos y desarrollar rutinas sólidas de ciberseguridad específicamente adaptadas a los lugares de trabajo de las pymes.	A seleccionar por el profesor, de la parte 1.3. [*Métodos de enseñanza, por ejemplo, tareas prácticas/laboratorios, cuestionarios, juegos, análisis de vídeos técnicos, estudios de casos, actividades prácticas, etc.]* de D2.3 «*Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes*».	Pruebas de autoevaluación Prueba de evaluación de conocimientos
Competencias: Los alumnos serán competentes en el desarrollo y la implementación de políticas estratégicas de ciberseguridad para los lugares de trabajo de las pymes.	A seleccionar por el profesor, de la parte 1.3. [*Métodos de enseñanza, por ejemplo, concursos, CTF, entornos simulados, 5E, CBL, CL, PBL, etc.]* de D2.3 «*Estructura de la ruta de aprendizaje de los agentes del cambio en ciberseguridad para pymes*».	Pruebas de autoevaluación Prueba de evaluación de conocimientos

Contenido del módulo: desglose de los temas	Horas de trabajo presencial					Horas de trabajo individual y tareas	
	Clases magistrales (HEI)	Consultas	Prácticas (HEI)	Exámenes	Todo el trabajo de contacto	Trabajo individual	Tareas
Evaluación de riesgos Proceso general de gestión de riesgos Marco general de gestión de riesgos Principios de la gestión de riesgos Normas de gestión de riesgos Ejemplos prácticos	2	0	2	0	**4**	5	Describa brevemente los pasos clave del proceso de gestión de riesgos, incluyendo la identificación, evaluación y control de riesgos. Defina los contextos internos y externos de la gestión de riesgos para una PYME. Especifique el alcance de la evaluación de riesgos e identifique los factores de riesgo clave. Desarrolle criterios de riesgo específicos para la PYME elegida.
Identificación de riesgos Liderazgo y compromiso en la gestión de riesgos Definición del alcance de las actividades de gestión de riesgos Contexto externo e interno de la gestión de riesgos Fuentes tangibles e intangibles de riesgo Causas y acontecimientos 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	4	0	4	0	**8**	5	Identificar las fuentes de riesgo tangibles e intangibles para las pymes. Clasificar los riesgos en función de las causas, los acontecimientos, las amenazas y las oportunidades. Analizar las vulnerabilidades y capacidades internas de la PYME y evaluar cómo los cambios en los contextos externos e internos podrían afectar al negocio. Identificar los posibles riesgos emergentes para la PYME y proponer indicadores para supervisarlos. Considerar cómo la naturaleza y el

fiabilidad de la información Sesgos, suposiciones y creencias de los implicados Ejemplos prácticos y estudios de casos							valor de los activos y recursos influyen en este análisis.
Amenazas internas Definición y tipos de amenazas internas. Los costes de las amenazas internas Creación de un programa de mitigación de amenazas internas Detección e identificación de amenazas internas Evaluación de las amenazas internas Gestión de las amenazas internas Ejemplos prácticos y casos de estudio	6	0	6	0	**12**	5	Definir y clasificar los diferentes tipos de amenazas internas relevantes para las pymes. Analizar los posibles costes que estas amenazas podrían suponer para la empresa. Desarrollar un programa básico de mitigación de amenazas internas para una PYME. Destacar componentes clave como las estrategias de detección, identificación y gestión. Proponer un método para evaluar las amenazas internas y esbozar los pasos para gestionar estas amenazas de manera eficaz en el contexto de una PYME.
Modelos y metodologías de medición y evaluación de riesgos Modelos y metodologías cuantitativos y cualitativos de evaluación de riesgos Probabilidad de que se produzcan los acontecimientos y consecuencias La naturaleza y magnitud de las consecuencias Complejidad y conectividad; Factores relacionados con el tiempo y volatilidad Evaluación de la eficacia de los controles existentes Niveles de sensibilidad y confianza	6	0	6	0	**12**	5	Compare y contraste un modelo cuantitativo y otro cualitativo de evaluación de riesgos. Evalúe la probabilidad de que se produzca un evento de riesgo y la naturaleza y magnitud de sus consecuencias para una PYME. Considere cómo la complejidad, los factores relacionados con el tiempo y la volatilidad influyen en esta evaluación. Evalúe la eficacia de los controles actuales en la gestión de los riesgos identificados. Incluya

Ejemplos prácticos y estudios de casos							un análisis de los niveles de sensibilidad y confianza en las medidas de control.
Control de riesgos Formulación y selección de opciones de tratamiento de riesgos Planificación e implementación del tratamiento de riesgos Evaluación de la eficacia de ese tratamiento. Decidir si el riesgo restante es aceptable. Supervisión y revisión Registro y presentación de informes Ejemplos prácticos y estudios de casos	6	0	6	0	**12**	5	Identifique y seleccione las opciones adecuadas para el tratamiento de riesgos en las pymes. Justifique su selección basándose en la naturaleza de los riesgos implicados. Elabore un breve plan de tratamiento de riesgos en el que se describa cómo se aplicarán las opciones de tratamiento seleccionadas en el entorno de una PYME. Proponer un método para evaluar la eficacia del tratamiento de riesgos y determinar si el riesgo restante es aceptable.
Total	**24**	**2**	**24**	**0**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Prueba de autoevaluación (1)	5%	10 puntos: 95-100 % de respuestas correctas. 9 puntos: 85-94 % de respuestas correctas. 8 puntos: 75-84 % de respuestas correctas. 7 puntos: 65-74 % de respuestas correctas. 6 puntos: 55-64 % de respuestas correctas. 5 puntos: 45-54 % de respuestas correctas. 4 puntos: 35-44 % de respuestas correctas. 3 puntos: 25-34 % de respuestas correctas. 2 puntos: 15-24 % de respuestas correctas. 1 punto: 0-14 % de respuestas correctas.
Prueba de autoevaluación (2)	5%	
Prueba de autoevaluación (3)	5%	
Prueba de autoevaluación (4)	5%	
Prueba de autoevaluación (5)	5%	
Prueba de evaluación de conocimientos	75%	

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*
Lectura obligatoria

1. Adarsh Nair y Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management**
2. Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press, libro electrónico
3. Kristina Narvaez, Betty Simkins, John Fraser (2014) Implementación de la gestión de riesgos empresariales: estudios de casos y mejores prácticas. John Wiley & Sons
- ENISA (2022) Normas de gestión de riesgos
4. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre medidas para un alto nivel común de ciberseguridad en toda la Unión, por la que se modifica el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972, y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2)
5. ISO 31000 Gestión del riesgo — Directrices

Lecturas recomendadas

- Shobhit Mehta (2023) Guía para el examen de certificación CRISC® (Certified in Risk and Information Systems Control) de ISACA. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
- Peter H. Gregory (2021) Guía de examen todo en uno para la certificación CISM en gestión de la seguridad de la información. McGraw-Hill
- ISACA (2021) Manual de revisión CRISC, 7.ª edición. ISACA
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011

8. M8: CONTINUIDAD DEL NEGOCIO, RECUPERACIÓN ANTE DESASTRES Y GESTIÓN DE INCIDENTES Y SEGURIDAD DEL PERSONAL

Título del módulo	Código del módulo
CONTINUIDAD DEL NEGOCIO, RECUPERACIÓN ANTE DESASTRES, GESTIÓN DE INCIDENTES Y SEGURIDAD DEL PERSONAL	

Profesor(es)	Institución o departamento donde se imparte el módulo

Modalidad de impartición	Idioma
Presencial, en línea, mixta, consultas	*Inglés, finés, turco, noruego, lituano, rumano, francés, polaco, español*

Requisitos previos
Ninguno

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	75	50	25

Objetivo y resultados del módulo

Al finalizar este curso, los alumnos serán capaces de formular y administrar planes integrales de continuidad del negocio y recuperación ante desastres (BC/DR), desarrollar un programa funcional de gestión de incidentes y establecer una política de seguridad del personal sólida y eficaz. Los alumnos aprenderán a proteger los activos, garantizar la prevención de pérdidas excesivas, evitar el tiempo de inactividad y evitar o limitar las situaciones de crisis y los entornos de gestión de crisis.
Al finalizar este curso, los alumnos serán capaces de redactar y supervisar la aplicación sostenida de un manual exhaustivo de ciberseguridad para pymes utilizando principios y tecnologías avanzadas de ciberseguridad integrados de conformidad con todas las leyes nacionales e internacionales. Los alumnos también realizarán un seguimiento de su aplicación.

Resultados del aprendizaje del módulo	Métodos de enseñanza y aprendizaje	Métodos de evaluación
Conocimientos: Los alumnos adquirirán conocimientos avanzados sobre cómo crear y aplicar un manual completo de ciberseguridad en el lugar de trabajo para pymes, incorporando principios avanzados de ciberseguridad, los últimos mecanismos de defensa y el cumplimiento de la legislación y las normas nacionales e internacionales en materia de gestión de incidentes, continuidad del negocio y seguridad del personal.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Pruebas de autoevaluación, prueba de evaluación de conocimientos.

Habilidades: Los alumnos adquirirán las habilidades necesarias para crear y mantener un manual de ciberseguridad en el lugar de trabajo para pymes, utilizando metodologías avanzadas para evaluar los riesgos, diseñar estrategias eficaces de gestión de riesgos y respuesta a incidentes, y desarrollar planes integrales de continuidad del negocio adaptados a las necesidades de su organización.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Pruebas de autoevaluación, prueba de evaluación de conocimientos
Competencias: Los alumnos serán competentes en el desarrollo y la implementación de un manual de ciberseguridad para pymes, liderando proyectos y equipos de seguridad de manera eficaz, garantizando la alineación con los objetivos de la organización y las obligaciones de cumplimiento.	A seleccionar por el profesor, de la parte 1.3. [Métodos de enseñanza] de D2.3 «Estructura de la ruta de aprendizaje de los agentes de cambio en ciberseguridad para pymes».	Pruebas de autoevaluación, prueba de evaluación de conocimientos

Contenido del módulo: desglose de los temas	**Horas de trabajo presencial**					**Horas de trabajo individual y tareas**	
	Clases	Consultas	Prácticas (HEI)	Exámenes	**Todo el trabajo presencial**	**Trabajo individual**	**Tareas**
Respuesta ante incidentes - Definición e importancia de la respuesta ante incidentes en la ciberseguridad - Componentes clave de una recuperación eficaz tras una respuesta ante incidentes - Descripción general de las amenazas comunes a la ciberseguridad (phishing, amenazas internas, etc.) - Desarrollo de un plan de respuesta ante incidentes (IRP) - Funciones y responsabilidades del equipo de respuesta ante incidentes - Simulación del incidente: realización de un plan simulado.	5	0,5	3	0,5	**9**	**5**	Desarrolle un plan detallado de respuesta ante incidentes para su pyme, que incluya las funciones, responsabilidades y medidas que se deben tomar durante un incidente de ciberseguridad. Simule un incidente y realice un simulacro para comprobar la eficacia de su plan.

Recuperación ante desastres - Comprender la recuperación ante desastres - Desarrollo de un plan de recuperación ante desastres - Funciones y responsabilidades en la recuperación ante desastres - Pasos para la recuperación tras un desastre	5	0,5	3	0,5	**9**	**5**	Cree un plan de recuperación ante desastres que describa los procedimientos para restaurar la infraestructura de TI y los datos después de un evento catastrófico. Incluya un cronograma para la recuperación y asigne responsabilidades a los miembros del equipo para cada fase del proceso.
Continuidad del negocio - Comprender la continuidad del negocio - Desarrollo del plan de continuidad del negocio (BCP) - Funciones y responsabilidades en la continuidad del negocio - Análisis del impacto en el negocio - Prueba y mejora del BCP	5	0,5	3	0,5	**9**	**5**	Diseñar un plan de continuidad del negocio que garantice que las funciones críticas del negocio sigan operativas durante y después de una interrupción. Identificar los servicios y recursos esenciales y esbozar estrategias de contingencia para mantenerlos en diversos escenarios.
Concienciación, formación y educación en materia de seguridad - Comprensión de la concienciación sobre seguridad - Desarrollo de un programa de formación en seguridad - Responsabilidades de los empleados en materia de ciberseguridad - Medición de la eficacia de la concienciación sobre seguridad -	1	0,5	2	0,5	**4**	**1**	Desarrolle un programa de formación en materia de seguridad para su pyme, centrándose en las políticas y mejores prácticas clave en materia de ciberseguridad. Imparta una sesión de formación a los empleados y evalúe sus conocimientos mediante cuestionarios o actividades interactivas.

Prácticas de contratación en materia de seguridad - Definición de los requisitos de los puestos de seguridad - Realización de comprobaciones de antecedentes - Realizar entrevistas para los componentes de seguridad - Evaluación y desarrollo continuos	1	0,5	2	0,5	**4**	**1**	Establecer prácticas de contratación centradas en la seguridad, incluyendo verificaciones de antecedentes y preguntas en las entrevistas diseñadas para evaluar la concienciación de los candidatos en materia de ciberseguridad. Crear una lista de verificación de las cualificaciones y características esenciales en materia de seguridad para los posibles empleados.
Prácticas de rescisión por motivos de seguridad - Revocar el acceso de inmediato - Recuperación de datos y dispositivos - Entrevista de salida para obtener información sobre seguridad - Notificación a los equipos pertinentes - Consideraciones legales y de cumplimiento	1	0,5	2	0,5	**4**	**2**	Elabore un procedimiento de despido seguro que incluya pasos para revocar el acceso, recuperar los activos de la empresa y realizar entrevistas de salida. Implemente un simulacro de despido para evaluar la eficacia de su procedimiento.
Seguridad de terceros - Evaluación del riesgo de terceros - Diligencia debida en la selección de proveedores - Implementación de contrastes y requisitos de seguridad - Supervisión y auditoría continuas - Respuesta ante incidentes y comunicación	2	0,5	2	0,5	**5**	**2**	Identifique los riesgos potenciales asociados a los proveedores externos y cree una lista de verificación de seguridad para evaluar su cumplimiento de las normas de ciberseguridad de su pyme. Redacte un modelo de contrato que incluya los requisitos de seguridad y las sanciones por incumplimiento.

Seguridad en los procesos de revisión - Incorporación de la seguridad en las revisiones - Realización de auditorías de seguridad periódicas - Evaluación de vulnerabilidades y pruebas de penetración - Revisiones posteriores a incidentes	1	0,5	1,5	0,5	**3,5**	**2**	Desarrolle un proceso para revisar y actualizar periódicamente las políticas y procedimientos de ciberseguridad de su pyme. Programe y realice una auditoría simulada para garantizar que todas las medidas de seguridad estén actualizadas y cumplan con las normas pertinentes.
Cuestión especial en materia de privacidad de la información personal de los empleados - Limitaciones en la recopilación de datos - Almacenamiento y control de acceso - Cumplimiento de la normativa de privacidad - Intercambio de datos y terceros - Consentimiento y derechos de los empleados	2	0,5	2	0,5	**5**	**2**	Redactar una política de privacidad para el tratamiento de la información personal de los empleados, garantizando el cumplimiento de las leyes de protección de datos y las mejores prácticas. Realizar una evaluación de riesgos para identificar posibles vulnerabilidades en el almacenamiento y el tratamiento de los datos de los empleados.
Total	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Prueba de autoevaluación (1)	5%	10 puntos: 95-100 % de respuestas correctas. 9 puntos: 85-94 % de respuestas correctas. 8 puntos: 75-84 % de respuestas correctas. 7 puntos: 65-74 % de respuestas correctas. 6 puntos: 55-64 % de respuestas correctas. 5 puntos: 45-54 % de respuestas correctas. 4 puntos: 35-44 % de respuestas correctas. 3 puntos: 25-34 % de respuestas correctas. 2 puntos: 15-24 % de respuestas correctas. 1 punto: 0-14 % de respuestas correctas.
Prueba de autoevaluación (2)	5%	
Prueba de autoevaluación (3)	5%	
Prueba de autoevaluación (4)	5%	
Prueba de autoevaluación (5)	5%	
Prueba de evaluación de conocimientos	75%	

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*
Lectura obligatoria
- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, libro electrónico. - Michael Wallace, Lawrence Webber (2017). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets.* AMACOM. - Instituto Nacional de Estándares y Tecnología (NIST). *Guía de planificación de contingencias para sistemas de tecnología de la información*. NIST SP 800-34 Rev. 1. - Cochran, K.A. (2024). Respuesta a incidentes, continuidad del negocio y recuperación ante desastres. En: Cybersecurity Essentials. Apress, Berkeley, CA. **https://doi.org/10.1007/979-8-8688-0432-8_14**
Lecturas recomendadas
- ISACA (2023). *Manual de revisión CISM, 15.ª edición*. ISACA. - Peter H. Gregory (2021). *Guía completa para el examen CISM (Gestor certificado en seguridad de la información)*. McGraw-Hill. - IT Governance (2022). *ISO 22301:2019 – Sistemas de gestión de la continuidad del negocio. Requisitos.* - M. Souppaya, L. Feldman, G. Witte [2024], Guía para la recuperación de incidentes de ciberseguridad, División de Seguridad Informática, Laboratorio de Tecnología de la Información, Instituto Nacional de Estándares y Tecnología, Departamento de Comercio de los Estados Unidos. - Ihab Hanna Sawalha [2021]. Opiniones sobre la continuidad del negocio y la recuperación ante desastres. Revista Internacional de Servicios de Emergencia

ANEXOS

PLANTILLA PARA EL PROGRAMA

DESCRIPCIÓN DEL MÓDULO

Título del módulo	Código del módulo
...	

Profesor(es)	Institución o departamento donde se imparte el módulo
...	...

Modalidad de impartición	Idioma
Presencial, en línea, mixta, consultas	*Inglés, ...*

Requisitos previos
...

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo presencial	Horas de trabajo individual
3	...	...	...

Objetivo y resultados del módulo		
...		
Resultados del aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**

Facilitar recursos (equipos, software, tecnología)
...

Contenido del módulo: desglose de los temas	Horas de trabajo presencial					Horas de trabajo individual y tareas	
	Clases magistrales	Consultas	Prácticas (HEI)	Exámenes	**Todo el trabajo presencial**	**Trabajo individual**	**Tareas**
1							
...							
n							
Total							

Estrategia de evaluación	**Porcentaje de ponderación comparativa**	**Criterios de evaluación**
Autoevaluación I		...
...		...
Autoevaluación n		...
Prueba de evaluación de conocimientos		...

Material de estudio *(Apellido, inicial del nombre. (Año, mes, día). Título del artículo. Título de la revista/periódico, número de volumen (número de edición), números de página de todo el artículo, editor, URL)*
Lecturas obligatorias
...
Lecturas recomendadas
...

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