Octubre de 2023

Ciberseguridad para FP y PYMEs

PLAN DE ESTUDIOS EUROPEO DE CIBERSEGURIDAD

DESARROLLADO POR Meta4 Innovations E.U.

PAQUETE DE TRABAJO 3 - CURRÍCULO EUROPEO DE CIBERSEGURIDAD

Funded by the European Union

Financiado por la Unión Europea. No obstante, los puntos de vista y opiniones expresados son exclusivamente los del autor o autores y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva en el Ámbito Educativo y Cultural Europeo (EACEA). Ni la Unión Europea ni la EACEA pueden ser consideradas responsables de las mismas. KA220-VET-C9588303

CONTENIDO

Sobre el proyecto **2**

Sinopsis **3**

1. CURRICULUM **4**

Unidad 1: Introducción a la ciberdefensa 5

Unidad 2: Protección de datos y privacidad 6

Unidad 3: Gestión de riesgos y cumplimiento 7

Unidad 4: Ingeniería social y suplantación de identidad (phishing) 8

Unidad 5: Seguridad en la nube para PYME 9

Unidad 6: Fundamentos de la seguridad de las redes 10

Unidad 7: Desarrollo seguro de software 11

Unidad 8: Protección segura de puntos finales 12

Unidad 9: Gestión y respuesta ante incidentes 13

Unidad 10: Continuidad de la actividad y recuperación en caso de catástrofe 14

2. Observaciones finales **15**

SOBRE EL PROYECTO

SecureFuture - Ciberseguridad para FP y PYMEs - es un proyecto Erasmus+ ejecutado entre diciembre de 2022 y diciembre de 2024. El proyecto lo lleva a cabo un consorcio de seis socios de cinco países, todos ellos con experiencia relevante en educación y formación profesional (FP) y ciberseguridad.

PAÍS	ORGANIZACIÓN
Türkiye	Istanbul Ticaret Universitesi (coordinador)
Türkiye	Estambul Valiligi
Portugal	Mindshift Talent
España	Media Creativa 2020
Italia	Pragma Ingeniería
Austria	Innovaciones Meta4

El consorcio SecureFuture detectó que la formación que se imparte actualmente en los centros de FP de la Unión Europea (UE) no está a la altura de las necesidades del mercado laboral o que hay países que carecen de formación sobre ciberseguridad a este nivel. Además, muchas pequeñas y medianas empresas (PYME) no cuentan entre su personal con empleados cualificados para proteger sus empresas contra las ciberamenazas, y encontrar ayuda externa en materia de ciberseguridad resulta muy costoso.

Teniendo en cuenta estos aspectos, el proyecto está desarrollando un marco europeo, un plan de estudios y contenidos formativos sobre ciberseguridad para orientar a los sistemas de FP y a las PYME que deseen dotar a sus estudiantes y empleados de competencias en ciberseguridad. Este documento hace referencia al plan de estudios europeo sobre ciberseguridad.

SINOPSIS

El currículo europeo de ciberseguridad propuesto es el resultado final del paquete de trabajo 3 del proyecto: WP3 - Currículo europeo de ciberseguridad.

El líder del WP3 - Meta4 Innovations E. U. - preparó un plan de trabajo, directrices y plantillas para todos los socios con el fin de facilitar el diseño y desarrollo de una propuesta de Curriculum Europeo de Ciberseguridad. Como proceso de desarrollo interconectado, este Currículo Europeo de Ciberseguridad está conformado por el Marco a través de la comparación de las competencias nacionales actuales sobre ciberseguridad, que fue desarrollado colectivamente por todos los socios.

Durante el mes de julio de 2023 se llevó a cabo una encuesta en toda Europa en todos los países socios - Austria, Italia, Portugal, España y Turquía - en la que un grupo de 66 expertos proporcionaron sus aportaciones, para proporcionar una visión general de las respectivas necesidades nacionales en relación con el plan de estudios para el proyecto. Estas aportaciones fueron resumidas por Meta4 y compartidas con los socios para concurr las Unidades de Aprendizaje de este Currículo Europeo de Ciberseguridad.

1. CURRICULUM

VISIÓN GENERAL

Teniendo en cuenta el uso heterogéneo del ECVET en los países socios, la media de puntos ECVET por hora de formación, la asociación del proyecto SecureFuture acordó lo siguiente:

20 horas de formación = 1 punto ECVET

El plan de estudios europeo de ciberseguridad contiene 10 módulos con una duración de 120 horas, lo que corresponde a 6 puntos ECVET.

Unidad 1: Introducción a la ciberdefensa

Introducción

El módulo “Introducción a la ciberdefensa" es una exploración fundamental de la ciberseguridad para las PYME. Proporciona una comprensión exhaustiva de los conceptos y principios básicos cruciales para salvaguardar los sistemas y datos digitales frente a las amenazas en constante cambio. Este módulo dota al alumnado de los conocimientos y habilidades esenciales necesarios para defenderse de las amenazas a la ciberseguridad y proteger los activos de información críticos en el dinámico panorama actual.

Objetivo

El objetivo es dotar al alumnado de una sólida comprensión de los conceptos y principios básicos de la ciberseguridad para identificar, mitigar y responder eficazmente a las ciberamenazas.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Comprender los principios básicos de la ciberseguridad y la protección de datos. K2. Identificar las ciberamenazas y vulnerabilidades más comunes. K3. Comprender los aspectos jurídicos y éticos de la ciberseguridad.	**Habilidades**	S1. Demostrar la capacidad de analizar el tráfico de red para detectar actividades sospechosas. S2. Capacidad para configurar cortafuegos contra amenazas y vulnerabilidades. S3. Competencia en la realización de pruebas y evaluaciones de seguridad.	**Responsabilidad y autonomía**	RA1. Evaluar y priorizar los riesgos de seguridad para desarrollar un plan de acción a medida para la ciberseguridad. RA2. Responder eficazmente a ciberamenazas comunes como el malware o el phishing. RA3. Colaborar en los procedimientos para minimizar el impacto de los incidentes de seguridad.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 2: Protección de datos y privacidad

Introducción

Este módulo dota al alumnado de las competencias esenciales para salvaguardar los datos en la era digital. Abarca aspectos clave de la protección de datos, como la clasificación de datos, el manejo responsable de información sensible, la privacidad, la propiedad intelectual y las complejidades de la guerra cibernética. Se hace hincapié en el RGDP y otras normativas de protección de datos, junto con el cifrado eficaz de los datos, las prácticas de almacenamiento seguro y la respuesta ante incidentes de violación de datos. El módulo fomenta actitudes que priorizan la privacidad, la ética y la adaptabilidad en ciberseguridad, permitiendo a los alumnos contribuir activamente a la defensa digital y convertirse en vigilantes protectores de los datos y la privacidad.

Objetivo

Dotar al alumando de los conocimientos, habilidades y actitudes necesarios para proteger y gestionar eficazmente los datos, garantizando el cumplimiento de la normativa sobre protección de datos y salvaguardando la privacidad en ciberseguridad.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Definir los conceptos relacionados con los datos, incluida la información sensible, la propiedad intelectual y la ciberguerra.	**Habilidades**	S1. Relacionar las técnicas de cifrado adecuadas con los distintos tipos de datos.	**Responsabilidad y autonomía**	RA1. Sensibilizar sobre la protección de datos y el respeto del derecho a la intimidad de las personas.
	K2. Diferenciar la normativa de protección de datos relacionada con los datos personales, los datos digitales y el Reglamento General de Protección de Datos (RGPD).		S2. Aplicar las mejores prácticas de almacenamiento seguro de datos, incluidos el cifrado, los controles de acceso y las copias de seguridad periódicas.		RA2. Adoptar un enfoque ético en el tratamiento de los datos y la propiedad intelectual.
	K3. Explicar la importancia de fomentar una mentalidad que dé prioridad al tratamiento responsable de los datos.		S3. Crear planes de gestión de las violaciones de datos teniendo en cuenta la gravedad de las mismas.		RA3. Desarrollar una actitud resistente y adaptable frente a las amenazas y normativas de ciberseguridad en constante evolución.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 3: Gestión de riesgos y cumplimiento

Introducción

Este módulo imparte competencias esenciales para gestionar los riesgos de ciberseguridad y garantizar el cumplimiento de la normativa. Integra la gestión de riesgos cibernéticos en las prácticas de gestión de riesgos de toda la empresa, reconociendo que la eliminación completa del riesgo es inalcanzable. Se centra en la reducción de los impactos de las amenazas a través de programas eficaces de gestión de riesgos cibernéticos. El módulo presenta al alumnado las normas reconocidas internacionalmente, en particular el Sistema de Gestión de la Seguridad de la Información (SGSI), esbozando los pasos clave y las listas de comprobación para su cumplimiento. Además de los conocimientos y habilidades, el módulo subraya el desarrollo de actitudes relacionadas con la aplicación de esquemas de cumplimiento de SGSI y recomendaciones en el análisis, reconocimiento y mitigación de riesgos, capacitando a los alumnos para abordar y gestionar proactivamente las amenazas a la ciberseguridad fomentando un enfoque sistémico de la seguridad de la información.

Objetivo

Dotar al alumnado de los conocimientos, habilidades y actitudes necesarios para aplicar eficazmente las metodologías de gestión de riesgos también referidas a las normas internacionales de cumplimiento de la ciberseguridad.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Definir los componentes y requisitos del Sistema de Gestión de la Seguridad de la Información. K2. Identificar la Gestión del Riesgo de la Información como función del Sistema de Gestión de la Seguridad de la Información. K3. Describir el enfoque de las normas de cumplimiento de la ciberseguridad	**Habilidades**	S1. Identificar los principales componentes del Sistema de Gestión de la Seguridad de la Información. S2. Esquemas de gestión de riesgos de diseño aplicados a las PYME S3. Examinar los requisitos de las normas de cumplimiento de la ciberseguridad	**Responsabilidad y autonomía**	RA 1. Colaborar en la definición del Sistema de Gestión de la Seguridad de la Información de las PYME. RA2. Cumplir el proceso de gestión de riesgos RA3. Abordar la adopción de normas de cumplimiento en materia de ciberseguridad

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 4: Ingeniería social y suplantación de identidad (phishing)

Introducción

Esta unidad de aprendizaje se centra en la concienciación sobre la ingeniería social y el phishing, vitales en nuestro mundo conectado digitalmente. Estos temas son tan críticos como el impacto transformador de los sistemas en la nube en las empresas. Al final de la unidad, el alumando definirá la ingeniería social, comprenderán sus motivaciones (como el beneficio económico y el robo de datos) y reconocerán diversas técnicas de phishing y vectores de ataque utilizados por los ciberdelincuentes. Esto mejora sus capacidades de detección y respuesta ante amenazasEl alumnado también comprenderán las implicaciones legales y éticas de los ataques de ingeniería social, promoviendo prácticas de ciberseguridad responsables. La unidad inculca la conciencia ética, fomenta la colaboración en la respuesta a incidentes y hace hincapié en el cumplimiento legal. Capacita a los profesionales de las TI, propietarios de empresas, estudiantes de FP o cualquier persona interesada en reforzar los conocimientos de ciberseguridad para un futuro digital seguro con confianza e integridad.

Objetivo

Esta unidad de aprendizaje pretende dotar a los participantes de los conocimientos, las habilidades y las actitudes éticas necesarios para definir la ingeniería social, identificar las técnicas de phishing y comprender sus implicaciones legales y éticas de forma eficaz.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Definir la ingeniería social y sus motivaciones en el contexto de las PYME.	**Habilidades**	S1. Describir las principales motivaciones que impulsan los ataques de ingeniería social.	**Responsabilidad y autonomía**	RA1. Promover la conciencia ética a la hora de definir los motivos de la ingeniería social para un uso responsable y basado en principios del conocimiento.
	K2. Identificar las técnicas de phishing y los vectores de ataque que hacen vulnerables a las PYME.		S2. Reconocer métodos como el spear phishing, el vishing (phishing de voz) y el pretexting.		RA2. Colaborar con los equipos para mitigar las amenazas de phishing al identificar técnicas y vectores de ataque.
	K3. Recordar las implicaciones legales y éticas de la ingeniería social en el contexto de las PYME.		S3. Comprender las posibles consecuencias tanto para los agresores como para las víctimas.		RA3. Cumplir con independencia las leyes, garantizando la legalidad en las acciones y prácticas de ingeniería social.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 5: Seguridad en la nube para PYME

Introducción

Esta unidad se centra en abordar los retos de seguridad únicos que presentan los sistemas en la nube para las PYME, que dependen cada vez más de estos sistemas por su flexibilidad, escalabilidad y rentabilidad. Está diseñada para proporcionar a las PYME los conocimientos y habilidades necesarios para gestionar eficazmente la seguridad en la nube. La unidad está adaptada a las necesidades y limitaciones específicas de las PYME, y ofrece conocimientos prácticos y estrategias prácticas para mitigar los riesgos, proteger la información confidencial y garantizar el cumplimiento de las normativas del sector. El alumnado explorará los principios básicos de la seguridad en la nube, las tecnologías de vanguardia y adquirirán experiencia práctica en la aplicación de medidas de seguridad. Ya se trate de un empresario, un profesional de las TI, un estudiante de FP o alguien que desee mejorar sus conocimientos sobre seguridad en la nube, este plan de estudios dota a los alumnos de las herramientas necesarias para asegurar eficazmente el futuro digital de su PYME.

Objetivo

Esta unidad pretende que el alumnado conozca las ventajas, los posibles riesgos y las instrucciones para maximizar el impacto del uso de sistemas en la nube para una PYME.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Identificar las ventajas de utilizar sistemas en la nube para una PYME. K2. Describir y mitigar los posibles riesgos del uso de sistemas en la nube. K3. Esbozar las medidas preventivas que podrían considerarse para la seguridad de la computación en nube de las PYME.	**Habilidades**	S1. Analizar en qué aspecto y cómo pueden utilizar las PYME la computación en nube. S2. Presentar consultas relacionadas con la seguridad en un contexto de gestión de riesgos y proponer soluciones. S3. Ilustrar diferentes tipos de requisitos legales que podrían tener un impacto en el uso de sistemas en la nube.	**Responsabilidad y autonomía**	RA1. Garantizar la seguridad de la nube de conformidad con datos personales en la UE y legislación nacional sobre protección. RA2. Colaborar con los colegas para proporcionar un escenario de ejemplo sobre cómo tener un sistema en la nube. RA3. Dirigir un equipo para evaluar las oportunidades de seguridad en una adquisición.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 6: Fundamentos de la seguridad de las redes

Introducción

La seguridad de la red es una preocupación crucial para las PYME que quieren defenderse de las ciberamenazas. Implica un enfoque holístico, que incorpora salvaguardas físicas y basadas en software, y requiere la comprensión de toda la organización. Los alumnos adquirirán un conocimiento profundo de las precauciones, que abarcará la comprensión conceptual y las habilidades interpersonales. Conocerán las medidas disponibles para que las PYME gestionen la seguridad de la red, incluida la formación de equipos dedicados capaces de ejecutar acciones de protección. Esta unidad dota a los participantes de los conocimientos necesarios para navegar por el intrincado campo de la seguridad de las redes, garantizando que puedan proteger eficazmente a sus empresas y operaciones del cambiante panorama de las ciberamenazas.

Objetivo

Esta unidad tiene como objetivo proporcionar al alumnado unos conocimientos básicos sobre la seguridad de las redes para PYMES y sobre cómo orientar su negocio hacia la seguridad de las PYMES.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Explicar los términos y conceptos básicos de la seguridad de las redes. K2. Recuerda las topologías y estrategias básicas utilizadas en la comunicación en red. K3. Identifica los elementos físicos de conexión a la red y los procedimientos de seguridad física.	**Habilidades**	S1. Discute por qué la seguridad de la red es importante para una PYME. S2. Ilustrar los posibles riesgos y las posibles soluciones en materia de seguridad de las redes. S3. Describe las posibles amenazas a la red y cómo debe reaccionar y prevenirlas una PYME.	**Responsabilidad y autonomía**	RA1. Dirige un equipo constituido para la seguridad de la red. RA2. Proporciona recomendaciones sobre cómo una empresa puede integrar la seguridad de la red en su plan de negocio. RA3. Verificar y supervisar la aplicación de los procedimientos de seguridad de la red.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 7: Desarrollo seguro de software

Introducción

El desarrollo seguro de software es primordial ante el aumento de las ciberamenazas. Requiere integrar prácticas de seguridad en todo el ciclo de desarrollo del software, desde el diseño y la codificación hasta las pruebas, la implantación y el mantenimiento. Su objetivo es salvaguardar los datos, preservar la privacidad del usuario y garantizar la integridad y disponibilidad del sistema de software. Los principios clave son la defensa en profundidad con múltiples capas de seguridad, el privilegio mínimo para un acceso mínimo y el diseño seguro desde el inicio del proyecto. Las pruebas periódicas, incluidas las pruebas de penetración y las revisiones del código, son esenciales. El despliegue seguro, el mantenimiento y la respuesta a incidentes son cruciales para la seguridad permanente. La formación y la concienciación, junto con los recursos de apoyo, mejoran aún más la seguridad de la organización. El desarrollo seguro de software es indispensable en el panorama actual de amenazas, ya que mitiga los riesgos y preserva la confianza de los usuarios.

Objetivo

Aprender a implantar prácticas seguras de desarrollo de software, salvaguardando los sistemas, los datos confidenciales y la privacidad de los usuarios, al tiempo que minimiza los riesgos de infracciones y ciberataques, y garantiza el mantenimiento, las pruebas y la formación.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Definir las prácticas de codificación segura, las amenazas comunes a la seguridad y las normas y marcos de seguridad. K2. Aprender el ciclo de vida del desarrollo seguro y la gestión de la configuración, el despliegue seguro y el mantenimiento. K3. Determinar la evaluación de la vulnerabilidad y las pruebas de penetración, el cifrado y la criptografía, las API seguras y las integraciones.	**Habilidades**	S1. Experimentar la codificación segura, la evaluación de vulnerabilidades, las pruebas de seguridad, el cifrado y la criptografía. S2. Construir una gestión de configuración, despliegue y mantenimiento seguros, un diseño de API seguro. S3. Mejorar el cumplimiento de la normativa y la privacidad, aprendizaje continuo.	**Responsabilidad y autonomía**	RA1. Tener en cuenta que los desarrolladores tienen la responsabilidad de dar prioridad a la seguridad en sus prácticas de codificación. RA2. Tomar decisiones sobre cuestiones relacionadas con la seguridad durante el proceso de desarrollo de software. RA3. Colaborar con expertos en seguridad durante el proceso de desarrollo para garantizar que se cumplen adecuadamente los requisitos de seguridad.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 8: Protección segura de puntos finales

Introducción

En el mundo interconectado de hoy en día, es esencial proteger los endpoints, incluidos portátiles, ordenadores de sobremesa, dispositivos móviles y servidores, frente a los ciberataques. La protección segura de los puntos finales implica la aplicación de una estrategia de defensa multicapa para proteger estos dispositivos frente al malware, el ransomware, el phishing y el acceso no autorizado. Esto implica desplegar un sólido software antivirus y antimalware, aprovechar los mecanismos avanzados de detección y prevención de amenazas, aplicar estrictos controles de acceso y medidas de autenticación, y actualizar periódicamente el software y los sistemas operativos. La protección segura de los puestos de trabajo es fundamental para organizaciones de todos los tamaños y sectores, ya que evita la filtración de datos, impide el acceso no autorizado a información confidencial y protege la continuidad de la actividad empresarial. Al fortalecer los puntos finales, las organizaciones pueden reducir el riesgo de ciberataques, cumplir las normativas del sector y proteger su reputación y la confianza de sus clientes.

Objetivo

Aprender a proteger portátiles, ordenadores de sobremesa, dispositivos móviles y servidores contra malware, ransomware, phishing y accesos no autorizados, reduciendo las fugas de datos y las interrupciones operativas al tiempo que garantiza el cumplimiento y preserva la confianza.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Comprender la seguridad de los puntos finales y una visión general de las medidas de protección de puntos finales seguros. K2. Define los componentes clave de la protección segura de puntos finales: antivirus, cortafuegos y cifrado. K3. Determinar las mejores prácticas para implantar una protección segura de los puntos finales, la gestión de parches, la detección de amenazas y la formación de los usuarios.	**Habilidades**	S1. Capaz de analizar y responder a las amenazas de malware, ransomware y phishing para mitigarlas eficazmente. S2. Gestionar y configurar herramientas de seguridad para puntos finales (antivirus, cortafuegos, cifrado) para un despliegue y un funcionamiento eficaces. S3. Gestión de parches, controles de acceso, cifrado de datos y concienciación de los usuarios para la seguridad de los terminales.	**Responsabilidad y autonomía**	RA 1. Proteger los puntos finales con antivirus, cortafuegos y cifrado para contrarrestar eficazmente las amenazas y vulnerabilidades. RA2. Asumir la responsabilidad de la seguridad de los puntos finales, identificando, mitigando los riesgos, realizando evaluaciones y manteniendo la seguridad. RA3. Responder rápidamente a los incidentes de seguridad, investigar, realizar análisis forenses, aplicar medidas correctoras y evitar que se repitan.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 9: Gestión y respuesta ante incidentes

Introducción

La Gestión y Respuesta ante Incidentes es esencial para mitigar una amplia gama de interrupciones y amenazas. Su objetivo es identificar, analizar y responder eficazmente a los incidentes que pueden interrumpir las operaciones o dañar los activos, la reputación y las partes interesadas de una organización. Estos incidentes abarcan ciberataques, filtraciones de datos, catástrofes naturales, accidentes y emergencias de salud pública. El objetivo principal es minimizar el impacto, restablecer las operaciones y prevenir futuros incidentes, siguiendo un marco estructurado. El éxito de la gestión de incidentes también exige una comunicación y colaboración claras entre los equipos y las partes interesadas. Una estrategia sólida permite a las organizaciones abordar los riesgos de forma proactiva, mejorar la resistencia, reducir el tiempo de inactividad, proteger los datos, cumplir la normativa y salvaguardar su reputación.

Objetivo

Aprender a responder eficazmente para minimizar el impacto del incidente, lo que incluye la detección rápida, la movilización de recursos, la respuesta coordinada y el rápido restablecimiento de las operaciones normales para la estabilidad y la seguridad generales.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Preparar la detección y notificación de incidentes, la evaluación y el análisis de incidentes. K2. Planificación y preparación de la respuesta a incidentes, contención y mitigación de incidentes. K3. Organizar la comunicación y coordinación de incidentes, la recuperación de incidentes y las lecciones aprendidas.	**Habilidades**	S1. Analizar incidentes, identificar causas y seleccionar estrategias de respuesta adecuadas utilizando sólidas capacidades de resolución de problemas. S2. Comunicarse eficazmente para la gestión y respuesta a incidentes. S3. Aplicar los conocimientos técnicos para la detección de incidentes en la gestión y respuesta eficaces a los mismos.	**Responsabilidad y autonomía**	RA1. Preparado para identificar y clasificar rápidamente los incidentes que se produzcan en una organización. RA2. Asumir la responsabilidad de coordinar y ejecutar la respuesta a los incidentes. RA3. Encargarse de documentar y notificar los incidentes.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

Unidad 10: Continuidad de la actividad y recuperación en caso de catástrofe

Introducción

La Continuidad de Negocio y la Recuperación ante Catástrofes (BCDR) forman parte integral de la estrategia de gestión de riesgos de una organización, garantizando la continuidad de las operaciones críticas de negocio y la recuperación de sistemas y datos en tiempos de interrupción. La Continuidad de Negocio implica una planificación proactiva, identificando los procesos vitales, evaluando los riesgos y desarrollando estrategias para mantener las operaciones de negocio durante y después de una interrupción. La recuperación en caso de catástrofe se centra en aspectos técnicos, como planes de copia de seguridad y recuperación, sistemas informáticos resistentes y procedimientos para restablecer rápidamente la normalidad. Ambos elementos de la BCDR exigen un conocimiento profundo de los activos, dependencias y riesgos de una organización. La colaboración y coordinación entre departamentos, la claridad de funciones, la comunicación, la formación y las pruebas son vitales. Los planes eficaces de BCDR minimizan el impacto de las interrupciones, mantienen la confianza y garantizan la resistencia operativa a largo plazo.

Objetivo

Aprender a proteger las operaciones empresariales críticas, minimizar el impacto de las interrupciones, identificar riesgos, desarrollar y probar planes para mejorar la resistencia de la organización y garantizar la viabilidad a largo plazo.

RESULTADOS DEL APRENDIZAJE

Conocimientos	K1. Definir la evaluación de riesgos y el análisis del impacto en las empresas, la planificación de la continuidad de las actividades. K2. Identificar los elementos clave de la planificación de la recuperación en caso de catástrofe informática y la gestión de crisis. K3. Conocer las estrategias de copia de seguridad y recuperación pertinentes para la continuidad de las operaciones empresariales.	**Habilidades**	S1. Ser capaz de llevar a cabo evaluaciones y análisis de riesgos para identificar posibles amenazas y vulnerabilidades para las operaciones críticas de la empresa. S2. Crear planes integrales de continuidad de la actividad y recuperación en caso de catástrofe. S3. Enumerar los procedimientos y recursos necesarios para garantizar la continuidad de las operaciones críticas y la recuperación oportuna de sistemas y datos.	**Responsabilidad y autonomía**	RA 1. Ser responsable de identificar y evaluar los riesgos y vulnerabilidades potenciales de las operaciones críticas de la empresa y de los sistemas informáticos. RA2. Estar preparado para aplicar planes integrales de continuidad de la actividad y recuperación en caso de catástrofe. RA3. Supervisar y probar periódicamente los planes de continuidad de la actividad y de recuperación en caso de catástrofe para garantizar su eficacia.

Duración

Horas de contacto	Horas prácticas	Horas de autoaprendizaje	Horas de evaluación	TOTAL
0,5	2	9	0,5	12

2. OBSERVACIONES FINALES

El plan de estudios europeo sobre ciberseguridad elaborado en el marco del proyecto Erasmus+ SecureFuture se redactó precisamente con las aportaciones realizadas por los socios del proyecto tras las consultas nacionales con 66 profesionales del ámbito de la ciberseguridad en sus países.

Tiene en cuenta los siguientes parámetros:

- Una distribución modular de los contenidos de formación en diez áreas como unidades de competencia y contenidos relacionados;
- Un conjunto de conocimientos, capacidades, responsabilidad y autonomía recopilados en un cuadro para cada una de las diez unidades de aprendizaje;
- Asignación de 6,0 puntos ECVET al conjunto de 10 unidades correspondientes a 120 horas de formación.

Este Plan de Estudios servirá de base para el desarrollo de los Contenidos de Formación Europeos en Ciberseguridad, tal y como se definen en el WP4 - Contenidos de Formación SecureFuture.

Juntos, el Marco Europeo de Cualificaciones, el Plan de Estudios y los Contenidos Formativos constituyen una propuesta de valor innovadora con un gran potencial para satisfacer las necesidades de los países europeos en materia de formación en ciberseguridad de los estudiantes de FP y los empleados de las PYME -los principales grupos destinatarios del proyecto- y preparar así a profesionales de la ciberseguridad bien formados para defender a las PYME europeas de las ciberamenazas.