ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Ciberseguridad en Pymes y Organizaciones: Políticas Básicas, Copias de Seguridad y Respuesta ante Incidentes

6 ECTS | 150 horas | Online, a tu ritmo

Formación acreditada por
Universidad de Vitoria-Gasteiz EUNEIZ



Acerca de ICUFOR

ICUFOR es un centro privado de formación online, Centro Acreditado y Autorizado por la Universidad EUNEIZ de Vitoria-Gasteiz. Diseñamos e impartimos Cursos de Formación Permanente universitarios, pensados para la actualización y la especialización de profesionales en activo.

Nuestros cursos se estudian a tu ritmo en un campus virtual propio y terminan con el diploma de la Universidad EUNEIZ y con certificados de ICUFOR verificables.

Centro acreditado
Universidad EUNEIZ

100 % online
Campus virtual propio

Equipo docente
Disponible todo el curso



Metodología de estudio

Campus virtual propio
Estudias desde cualquier lugar y dispositivo, sin horarios.

Aprendizaje autónomo, pero acompañado
Tú marcas el ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

Contenido del curso en PDF
El material principal, para estudiarlo a fondo, tema a tema.

Abstract de cada tema
Su síntesis, para situarte al empezar y repasar al final.

Presentación con los aspectos clave
Lo esencial de cada bloque, para jerarquizar y fijar.

Cuestionarios de evaluación
De respuesta múltiple, uno por tema.



Campus virtual

Mis cursos
Tu progreso y el siguiente tema por estudiar

Materiales
Contenido en PDF, Abstract y presentación con los aspectos clave

Cuestionarios de evaluación
Tu nota y la revisión de tus respuestas

Equipo docente
Consulta por escrito, chat y asesor de IA a cualquier hora

Secretaría
Certificados en PDF con código de verificación

Pagos y facturas
Descarga de facturas en PDF



Presentación del programa



Especialízate con este programa formativo diseñado para profesionales que buscan proteger eficazmente los activos digitales de pequeñas y medianas empresas. En ICUFOR comprendemos que las pymes enfrentan amenazas cibernéticas cada vez más sofisticadas, pero frecuentemente carecen de los recursos y conocimientos especializados de las grandes corporaciones. Por ello, hemos desarrollado esta formación que proporciona herramientas prácticas y adaptadas a la realidad del tejido empresarial actual.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la ciberseguridad en el entorno empresarial, identificando las principales amenazas, vulnerabilidades y actores de riesgo que afectan específicamente a pymes y organizaciones.

Aplicar metodologías de análisis de riesgos en ciberseguridad, elaborando mapas de riesgos y seleccionando estrategias adecuadas de tratamiento adaptadas a los recursos de la organización.

Dominar los principios de seguridad en redes, sistemas y dispositivos, aplicando medidas de protección, bastionado y monitorización en los entornos tecnológicos de la organización.

Elaborar planes de continuidad de negocio y respuesta ante incidentes de ciberseguridad, describiendo los procedimientos de detección, contención, erradicación, recuperación y análisis post-incidente.

Conocer el marco normativo y regulatorio aplicable a la ciberseguridad, distinguiendo las obligaciones derivadas de la legislación europea, la normativa nacional y los estándares internacionales de referencia.

Diseñar e implementar políticas básicas de ciberseguridad organizacional, definiendo normas de control de accesos, clasificación de la información, uso aceptable de recursos y gestión de proveedores.

Desarrollar estrategias integrales de copias de seguridad, planificando su implementación técnica, verificación periódica y protección frente a amenazas como el ransomware.

Fundamentar la importancia del factor humano en la ciberseguridad, diseñando programas de concienciación y formación del personal e incorporando mecanismos de auditoría y mejora continua del sistema de gestión de seguridad.

Temario

01 Fundamentos de ciberseguridad en el entorno empresarial actual

1.1. Concepto y evolución histórica de la ciberseguridad en el contexto organizacional
1.2. El panorama actual de amenazas cibernéticas para pymes y organizaciones
1.3. Principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad
1.4. Especificidades y vulnerabilidades de las pymes frente a las grandes corporaciones en materia de ciberseguridad
1.5. Impacto de los ciberincidentes y responsabilidades dentro de la organización

02 Marco normativo y regulatorio aplicable a la ciberseguridad en pymes y organizaciones

2.1. Legislación europea en materia de ciberseguridad: Directiva NIS2 y Reglamento DORA
2.2. Normativa nacional de ciberseguridad y protección de infraestructuras críticas
2.3. El Reglamento General de Protección de Datos (RGPD) y su relación con la ciberseguridad
2.4. Estándares internacionales de referencia: ISO 27001, ISO 27002 y el marco NIST
2.5. El Esquema Nacional de Seguridad (ENS) y su aplicabilidad a organizaciones y pymes
2.6. Responsabilidades legales de la dirección en materia de ciberseguridad y gobernanza digital

Temario

03 Análisis de riesgos y gestión de amenazas en pymes y organizaciones

3.1. Conceptos fundamentales del análisis de riesgos en ciberseguridad
3.2. Metodologías de análisis de riesgos aplicables a pymes y organizaciones
3.3. Identificación y catalogación de amenazas específicas del entorno pyme
3.4. Evaluación de vulnerabilidades técnicas y organizativas en los sistemas de información
3.5. Estrategias de tratamiento del riesgo: mitigación, transferencia, aceptación y evitación
3.6. Elaboración del mapa de riesgos y priorización de actuaciones de seguridad
3.7. Monitorización continua y revisión periódica del análisis de riesgos de la organización

Temario

04 Diseño e implementación de políticas básicas de ciberseguridad

4.1. Concepto, tipología y estructura de las políticas de ciberseguridad organizacional
4.2. Política de seguridad de la información como documento rector de la organización
4.3. Política de control de accesos y gestión de identidades en la organización
4.4. Política de uso aceptable de recursos tecnológicos por parte del personal
4.5. Política de clasificación y protección de la información corporativa
4.6. Política de seguridad en el trabajo remoto y uso de dispositivos móviles corporativos
4.7. Política de gestión de proveedores y terceros desde la perspectiva de la ciberseguridad
4.8. Estrategias para la implantación, comunicación y cumplimiento de las políticas en la organización

Temario

05 Gestión de la seguridad en redes, sistemas y dispositivos de la organización

5.1. Fundamentos de seguridad en redes de comunicaciones para pymes y organizaciones
5.2. Protección de servidores, estaciones de trabajo y dispositivos endpoint
5.3. Seguridad en servicios en la nube utilizados por la organización
5.4. Securización del correo electrónico corporativo y protección frente a ataques de phishing
5.5. Gestión de vulnerabilidades y bastionado de sistemas de la organización
5.6. Seguridad en aplicaciones web y servicios expuestos a Internet
5.7. Monitorización y registro de eventos de seguridad mediante logs y sistemas SIEM

Temario

06 Estrategias y políticas de copias de seguridad en entornos empresariales

6.1. Importancia estratégica de las copias de seguridad en el entorno empresarial
6.2. Conceptos fundamentales en la planificación de copias de seguridad: RPO, RTO y ventana de backup
6.3. Tipos de copias de seguridad: completa, incremental, diferencial y sintética
6.4. La regla 3-2-1-1-0 como marco de referencia para el diseño de la estrategia de backup
6.5. Diseño de la política de copias de seguridad de la organización
6.6. Protección de las copias de seguridad frente a ransomware y accesos no autorizados

Temario

07 Implementación técnica y gestión operativa de copias de seguridad

7.1. Medios y tecnologías de almacenamiento para copias de seguridad
7.2. Herramientas y soluciones de software de backup para pymes y organizaciones
7.3. Planificación y automatización de las tareas de copia de seguridad en la organización
7.4. Copias de seguridad de entornos específicos de la organización
7.5. Verificación, pruebas de restauración y validación de la integridad de las copias de seguridad
7.6. Monitorización, alertas y mantenimiento operativo del sistema de backup
7.7. Elaboración del plan de restauración ante escenarios de pérdida de datos

Temario

08 Continuidad de negocio y recuperación ante desastres en pymes y organizaciones

8.1. Fundamentos de la continuidad de negocio y su relación con la ciberseguridad
8.2. Análisis de impacto en el negocio (BIA) y determinación de procesos críticos
8.3. Diseño del plan de continuidad de negocio adaptado a pymes y organizaciones de menor tamaño
8.4. Elaboración del plan de recuperación ante desastres (DRP)
8.5. Pruebas, mantenimiento y actualización periódica de los planes de continuidad y recuperación

09 Preparación y planificación de la respuesta ante incidentes de ciberseguridad

9.1. Concepto, tipología y clasificación de los incidentes de ciberseguridad
9.2. Marcos y modelos de referencia para la gestión de incidentes de ciberseguridad
9.3. Creación y organización del equipo de respuesta ante incidentes de ciberseguridad
9.4. Elaboración del plan de respuesta ante incidentes de ciberseguridad
9.5. Herramientas y recursos técnicos necesarios para la detección y respuesta ante incidentes
9.6. Simulacros y ejercicios de ciberincidentes: tabletop exercises y simulaciones técnicas

Temario

10 Detección, contención, erradicación y recuperación ante incidentes de ciberseguridad

10.1. Detección e identificación temprana de incidentes de ciberseguridad
10.2. Análisis forense básico y evaluación del alcance del incidente sobre la organización
10.3. Estrategias de contención del incidente a corto y largo plazo
10.4. Erradicación de la amenaza y eliminación de la causa raíz del incidente
10.5. Recuperación de sistemas, servicios y datos tras el incidente de ciberseguridad
10.6. Gestión de la comunicación y notificaciones durante y después del incidente
10.7. Análisis post-incidente y lecciones aprendidas para la mejora del sistema de seguridad

11 Cultura de ciberseguridad, concienciación del personal y mejora continua

11.1. La importancia del factor humano como elemento clave en la ciberseguridad organizacional
11.2. Diseño e implementación de programas de concienciación y formación en ciberseguridad
11.3. Construcción y mantenimiento de una cultura de ciberseguridad en la organización
11.4. Auditorías, evaluación y mejora continua del sistema de gestión de ciberseguridad

Titulación y certificados

Diploma de la Universidad EUNEIZ

Al aprobar todos los cuestionarios de evaluación recibes el **diploma en formato digital** de Curso de Formación Permanente, con sus 6 créditos ECTS y 150 horas.

Certificados de ICUFOR

Se descargan en PDF desde la Secretaría del campus, con un código único y QR para verificarlos.



Universidad de Vitoria-Gasteiz EUNEIZ

Proceso de matriculación

1 **Pulsa «Matricularme» en la ficha del curso**
Completa tus datos personales y de facturación.

2 **Elige la forma de pago**
Tarjeta, PayPal o transferencia bancaria.

3 **Entra en el campus y empieza**
Recibes por correo tus datos de acceso y, en cuanto se confirma el pago, tienes el temario completo. La matrícula está abierta todo el año.

Matricúlate | Más información



Métodos de pago

Pago único
El precio se abona una sola vez, sin cuotas ni renovaciones.

Seguridad
Pago online en la pasarela de Stripe o de PayPal.

Flexibilidad
Tarjeta de crédito o débito, PayPal o transferencia.

Acceso inmediato
Con tarjeta o PayPal, el campus se activa al momento.

Simplicidad
Matrícula y pago en dos pasos.

Facturación
Facturas en «Pagos y facturas» del campus.



¿Por qué elegir ICUFOR?

01

Formación accesible

Formación universitaria rigurosa y acreditada, íntegramente online y compatible con tu trabajo.

02

Calidad universitaria

Cada curso está acreditado por la Universidad EUNEIZ, con su memoria académica y sus créditos ECTS.

03

Impulso a tu carrera

Contenidos de utilidad práctica y una titulación que suma en méritos, concursos y bolsas de empleo.

04

Especialización

Cada curso trata una única temática a fondo: combínalos y construye tu propio itinerario.

05

Atención de calidad

Consultas al equipo docente por escrito o por chat, y un asesor de IA a cualquier hora.

¿Por qué elegir ICUFOR?

06 **Contenidos actualizados**
Los cursos se revisan periódicamente para incorporar las novedades de cada ámbito.

07 **El curso, por escrito**
Cada tema en tres formatos: contenido en PDF, Abstract y presentación con los aspectos clave.

08 **Autónomo, pero acompañado**
Tú decides tu ritmo y nuestro equipo de docentes resuelve tus dudas y orienta tu estudio.

09 **Enseñanza adaptada**
Sin horarios ni conexiones obligatorias: seis meses para terminar, ampliables si lo necesitas.

10 **Estudio sencillo e intuitivo**
Un campus virtual propio, sin instalar nada y accesible desde cualquier dispositivo.

¿Necesitas más información?

Te contamos cómo funciona el curso, los plazos y la titulación, sin compromiso.

www.icufor.com

info@icufor.com

+34 858 895 080

+34 746 044 519

Formación acreditada por Universidad de Vitoria-Gasteiz EUNEIZ

