ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Fundamentos de Ciberseguridad para Mandos y Responsables No Técnicos

4 ECTS | 100 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



Amplía tu formación con este programa diseñado específicamente para directivos, mandos intermedios y responsables organizacionales que necesitan comprender la ciberseguridad sin requerir conocimientos técnicos especializados. En ICUFOR entendemos que la protección digital se ha convertido en un pilar estratégico para cualquier organización, y que los líderes empresariales deben tomar decisiones informadas sobre riesgos, inversiones y políticas de seguridad que afectan directamente a la continuidad del negocio.

A lo largo del temario abordarás desde los fundamentos estratégicos de la ciberseguridad hasta el panorama actual de amenazas, incluyendo ransomware, phishing e ingeniería social. Profundizarás en marcos de gobernanza como ISO 27001 o el NIST Cybersecurity Framework, gestión del ciberriesgo, cumplimiento normativo (NIS2, RGPD, ENS) y respuesta ante incidentes.

Duración
100 horas

Créditos
4 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos conceptuales y estratégicos de la ciberseguridad, identificando su alcance e impacto en la gestión organizacional.

Conocer los principales marcos de gobernanza, estándares internacionales y modelos organizativos de ciberseguridad, distinguiendo sus estructuras, funciones y criterios de aplicación.

Comprender las medidas de protección y controles tecnológicos de ciberseguridad, relacionando las soluciones disponibles con las necesidades de supervisión directiva.

Diseñar planes de gestión de incidentes y continuidad de negocio, incorporando protocolos de respuesta, comunicación de crisis y recuperación operativa.

Clasificar las amenazas, vulnerabilidades y vectores de ataque contemporáneos, diferenciando sus tipologías y dinámicas de actuación sobre las organizaciones.

Aplicar los principios de gestión del ciberriesgo, integrando su análisis, evaluación y tratamiento en la estrategia corporativa.

Dominar el marco jurídico y regulatorio en materia de ciberseguridad, identificando las obligaciones legales y responsabilidades aplicables a la dirección.

Desarrollar competencias de liderazgo estratégico en ciberseguridad, promoviendo una cultura organizacional de protección digital y fundamentando las decisiones de inversión.

Temario

01 Fundamentos conceptuales y estratégicos de la ciberseguridad para responsables organizacionales

1.1. Definición y alcance de la ciberseguridad en el contexto empresarial actual
1.2. Evolución histórica de las amenazas cibernéticas y su impacto en las organizaciones
1.3. El papel de los mandos y responsables no técnicos en la protección digital de la organización
1.4. Impacto económico, reputacional y operativo de los incidentes de ciberseguridad

02 Panorama actual de amenazas, vulnerabilidades y vectores de ataque relevantes para la dirección

2.1. Clasificación y tipología de las amenazas cibernéticas contemporáneas
2.2. Principales vectores de ataque dirigidos a organizaciones
2.3. Anatomía de un ciberataque: fases y dinámica de las intrusiones
2.4. Vulnerabilidades organizacionales más frecuentes desde la perspectiva directiva
2.5. Fuentes de inteligencia sobre amenazas accesibles para responsables no técnicos
2.6. Tendencias emergentes en el panorama de ciberamenazas

Temario

03 Marcos de gobernanza, estándares internacionales y modelos organizativos de ciberseguridad

3.1. Concepto y principios fundamentales de la gobernanza de la ciberseguridad
3.2. Marcos y estándares internacionales de referencia para la gestión de la ciberseguridad
3.3. El Esquema Nacional de Seguridad y su aplicación en organizaciones españolas
3.4. Políticas corporativas de ciberseguridad: diseño, aprobación y supervisión directiva
3.5. Modelos organizativos para la gestión operativa y estratégica de la ciberseguridad
3.6. Evaluación del nivel de madurez en ciberseguridad de la organización
3.7. Indicadores clave y cuadros de mando para la supervisión directiva de la ciberseguridad

Temario

04 Gestión del ciberriesgo desde la perspectiva directiva y su integración en la estrategia corporativa

4.1. Fundamentos de la gestión de riesgos aplicados al ámbito de la ciberseguridad
4.2. Identificación y clasificación de activos de información críticos para la organización
4.3. Metodologías de análisis y evaluación de riesgos cibernéticos
4.4. Estrategias de tratamiento del riesgo cibernético y opciones para la dirección
4.5. Supervisión continua y revisión periódica del mapa de riesgos cibernéticos
4.6. Comunicación del riesgo cibernético a órganos de gobierno y partes interesadas

Temario

05 Medidas de protección y controles de ciberseguridad: comprensión directiva de las soluciones tecnológicas

5.1. Arquitecturas y estrategias de protección: visión general para responsables no técnicos
5.2. Gestión de identidades y control de accesos como pilar de la seguridad corporativa
5.3. Protección de datos, dispositivos y comunicaciones
5.4. Seguridad en entornos cloud y servicios externalizados
5.5. Monitorización, detección y respuesta tecnológica

06 Marco jurídico, regulatorio y de cumplimiento normativo en materia de ciberseguridad

6.1. Panorama regulatorio europeo en materia de ciberseguridad y protección de datos
6.2. Legislación nacional española aplicable a la ciberseguridad corporativa
6.3. Obligaciones de notificación de incidentes y brechas de seguridad ante las autoridades
6.4. Responsabilidad legal de administradores y directivos en materia de ciberseguridad
6.5. Diseño e implementación de programas de cumplimiento normativo en ciberseguridad
6.6. Gestión contractual de la ciberseguridad en las relaciones con proveedores y terceros

Temario

07 Gestión de incidentes de ciberseguridad, comunicación de crisis y continuidad de negocio

7.1. Conceptos fundamentales de la gestión de incidentes de ciberseguridad
7.2. Planificación de la respuesta ante incidentes desde la perspectiva de la dirección
7.3. Toma de decisiones directivas durante la gestión activa de un ciberincidente
7.4. Comunicación de crisis en el contexto de incidentes de ciberseguridad
7.5. Planes de continuidad de negocio y recuperación ante desastres con componente ciber
7.6. Ejercicios de simulación y entrenamiento para equipos directivos
7.7. Relación institucional con CERT/CSIRT nacionales, sectoriales y fuerzas de seguridad

Temario

08 Liderazgo estratégico, cultura organizacional de ciberseguridad e inversión en protección digital

8.1. El rol del liderazgo directivo en la construcción de una organización ciberresiliente
8.2. Desarrollo y promoción de una cultura organizacional orientada a la ciberseguridad
8.3. Planificación estratégica e inversión en ciberseguridad: criterios para la dirección
8.4. Gestión del talento y relación efectiva con los equipos técnicos de ciberseguridad
8.5. Preparación directiva ante los retos futuros de la 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 4 créditos ECTS y 100 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

