ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Protección de Infraestructuras Críticas y Servicios Esenciales: Ciberseguridad para Entidades Públicas

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



Amplía tu formación con el Curso de Formación Permanente en Protección de Infraestructuras Críticas y Servicios Esenciales: Ciberseguridad para Entidades Públicas de ICUFOR. En un contexto donde la digitalización ha transformado sectores estratégicos como la energía, el transporte, la sanidad o las administraciones públicas, la protección de estos entornos se ha convertido en una prioridad nacional y europea. Este programa responde a la creciente demanda de profesionales capacitados para garantizar la continuidad y seguridad de los servicios que sostienen el funcionamiento de nuestra sociedad.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la protección de infraestructuras críticas y los servicios esenciales, analizando sus interdependencias, efectos en cascada y la convergencia entre seguridad física y ciberseguridad.

Conocer el marco normativo y regulatorio europeo y español aplicable a la protección de infraestructuras críticas y la ciberseguridad, diferenciando las obligaciones derivadas de cada instrumento legal y del Sistema PIC.

Diseñar modelos de gobernanza de la ciberseguridad en entidades públicas, integrando políticas de seguridad, marcos de referencia internacionales y programas de formación y concienciación del personal.

Aplicar metodologías de análisis y gestión de riesgos en entornos críticos, elaborando planes de tratamiento y estrategias de mitigación adaptados a los activos y servicios esenciales.

Identificar el panorama de ciberamenazas, actores hostiles y vectores de ataque contra infraestructuras críticas, clasificando sus técnicas mediante marcos de referencia y fuentes de inteligencia de ciberamenazas.

Dominar las arquitecturas de ciberseguridad y las medidas técnicas de protección en entornos IT y OT, distinguiendo las especificidades de los sistemas de control industrial y su aplicación a los principales sectores de servicios esenciales.

Desarrollar capacidades de monitorización, detección, respuesta ante incidentes y continuidad operativa, implementando planes de ciberresiliencia y procedimientos de recuperación ante desastres en servicios esenciales.

Analizar los mecanismos de cooperación interinstitucional y las tecnologías emergentes, valorando su impacto presente y futuro en la protección de infraestructuras críticas y la ciberseguridad del sector público.

Temario

01 Fundamentos de la protección de infraestructuras críticas y los servicios esenciales

1.1. Concepto, alcance y caracterización de las infraestructuras críticas en el contexto actual
1.2. Definición y clasificación de los servicios esenciales para el funcionamiento de la sociedad
1.3. Evolución histórica de la protección de infraestructuras críticas como disciplina
1.4. Interdependencias entre infraestructuras críticas y análisis de efectos en cascada
1.5. El papel de las entidades públicas y la convergencia entre seguridad física y ciberseguridad en entornos críticos

Temario

02 Marco normativo y regulatorio de la protección de infraestructuras críticas y la ciberseguridad

2.1. Marco normativo europeo en materia de protección de infraestructuras críticas
2.2. Legislación española: Ley 8/2011 de protección de infraestructuras críticas
2.3. Esquema Nacional de Seguridad (ENS) y su aplicación a las entidades públicas
2.4. Normativa sectorial específica aplicable a los distintos ámbitos de servicios esenciales
2.5. El Sistema de Protección de Infraestructuras Críticas (Sistema PIC) en España
2.6. Obligaciones de los operadores críticos y de las entidades públicas designadas
2.7. Régimen sancionador y mecanismos de supervisión, inspección y control del cumplimiento

Temario

03 Gobernanza y organización de la ciberseguridad en entidades públicas

3.1. Modelos de gobernanza de la ciberseguridad en el sector público
3.2. Políticas de seguridad de la información: diseño, aprobación e implementación efectiva
3.3. Integración de la ciberseguridad en la planificación estratégica institucional
3.4. Marcos de referencia y estándares internacionales aplicables a la gestión de la ciberseguridad
3.5. Cultura de ciberseguridad: programas de formación, concienciación y capacitación del personal
3.6. Gestión de proveedores, cadena de suministro y cumplimiento normativo

Temario

04 Análisis de riesgos y evaluación de amenazas en infraestructuras críticas

4.1. Fundamentos del análisis y la gestión de riesgos en entornos críticos
4.2. Metodologías de análisis de riesgos aplicables a infraestructuras críticas y servicios esenciales
4.3. Identificación, inventario y valoración de activos críticos en entidades públicas
4.4. Catálogo de amenazas específicas para infraestructuras críticas y servicios esenciales
4.5. Evaluación sistemática de vulnerabilidades técnicas y organizativas
4.6. Determinación del impacto potencial y cálculo del nivel de riesgo residual
4.7. Estrategias de tratamiento del riesgo y elaboración de planes de mitigación
4.8. Monitorización continua del nivel de riesgo y revisión periódica de las evaluaciones

Temario

05 Panorama de ciberamenazas, actores hostiles y vectores de ataque contra infraestructuras críticas

5.1. Panorama actual de ciberamenazas contra infraestructuras críticas a nivel global
5.2. Actores de amenaza: tipología, motivaciones y nivel de capacidad técnica
5.3. Principales vectores y técnicas de ataque empleados contra entornos críticos
5.4. Análisis de incidentes de referencia en infraestructuras críticas a nivel internacional
5.5. Uso del framework MITRE ATT&CK y ATT&CK for ICS para la caracterización de amenazas
5.6. Inteligencia de ciberamenazas (Cyber Threat Intelligence) aplicada a la protección de infraestructuras críticas

Temario

06 Arquitecturas de ciberseguridad y medidas técnicas de protección en entornos críticos

6.1. Principios de diseño seguro y defensa en profundidad en infraestructuras críticas
6.2. Segmentación de redes, zonificación y control de flujos en entornos corporativos
6.3. Gestión de identidades, autenticación y control de accesos (IAM)
6.4. Protección criptográfica de la información y las comunicaciones
6.5. Seguridad en los endpoints y bastionado de sistemas
6.6. Protección del correo electrónico, navegación web y servicios expuestos a Internet
6.7. Gestión de actualizaciones, parches de seguridad y configuraciones seguras

Temario

07 Protección de sistemas de control industrial y tecnología operacional (OT)

7.1. Fundamentos de los sistemas de control industrial (ICS) y la tecnología operacional
7.2. Convergencia IT/OT y desafíos de seguridad derivados de la digitalización industrial
7.3. Vulnerabilidades específicas y superficie de ataque de los sistemas de control industrial
7.4. Protocolos de comunicación industrial y sus debilidades de seguridad inherentes
7.5. Estrategias de defensa en profundidad y arquitecturas de seguridad para entornos industriales
7.6. Normativas y estándares de ciberseguridad industrial aplicables

Temario

08 Ciberseguridad aplicada a los principales sectores de servicios esenciales

8.1. Ciberseguridad en el sector energético: generación, transporte y distribución de energía
8.2. Ciberseguridad en el sector del transporte y las infraestructuras de movilidad
8.3. Ciberseguridad en el sector del agua: redes de abastecimiento y saneamiento
8.4. Ciberseguridad en el sector sanitario y los servicios de salud pública
8.5. Ciberseguridad en las administraciones públicas y los servicios digitales al ciudadano
8.6. Ciberseguridad en el sector de las telecomunicaciones y las redes de comunicaciones electrónicas
8.7. Análisis comparado de enfoques sectoriales y lecciones aprendidas de carácter transversal

Temario

09 Monitorización, detección y respuesta ante ciberincidentes en infraestructuras críticas

9.1. Arquitectura de monitorización y capacidades de detección en infraestructuras críticas
9.2. Centros de operaciones de seguridad (SOC) para entidades públicas e infraestructuras críticas
9.3. Tecnologías y herramientas de monitorización, detección y alerta temprana
9.4. Gestión de incidentes de ciberseguridad: fases, procedimientos y protocolos de actuación
9.5. Equipos de respuesta ante incidentes de ciberseguridad (CSIRT/CERT) de referencia en España
9.6. Obligaciones legales de notificación de incidentes según la normativa vigente
9.7. Análisis forense digital en entornos de infraestructuras críticas

Temario

10 Continuidad de negocio, recuperación ante desastres y ciberresiliencia en servicios esenciales

10.1. Conceptos fundamentales de continuidad operativa y ciberresiliencia
10.2. Análisis de impacto en el negocio (BIA) aplicado a servicios esenciales e infraestructuras críticas
10.3. Diseño y desarrollo de planes de continuidad de negocio (BCP) para entidades públicas
10.4. Pruebas, ejercicios y simulacros de validación de los planes de continuidad
10.5. Estándares de referencia: ISO 22301 y guías del Centro Criptológico Nacional (CCN)
10.6. Integración de la continuidad de negocio en el ciclo integral de gestión de riesgos

11 Cooperación interinstitucional, intercambio de información y ciberejercicios

11.1. Marco institucional de cooperación en ciberseguridad de infraestructuras críticas
11.2. Intercambio de información sobre ciberamenazas: protocolos, estándares y herramientas
11.3. Mesas de coordinación cibernética y otros mecanismos operativos de colaboración
11.4. Ciberejercicios nacionales e internacionales como herramienta de preparación
11.5. Diplomacia cibernética, estrategias nacionales de ciberseguridad y cooperación internacional

Temario

12 Tecnologías emergentes y tendencias futuras en la protección de infraestructuras críticas

12.1. Impacto de la transformación digital acelerada en la seguridad de las infraestructuras críticas
12.2. Internet de las Cosas (IoT) e IoT industrial (IIoT): oportunidades y nuevos riesgos de seguridad
12.3. Inteligencia artificial y aprendizaje automático aplicados a la ciberseguridad de infraestructuras
12.4. Redes 5G, computación en la nube y nuevos modelos de servicio para el sector público
12.5. Impacto de la computación cuántica en la criptografía y los sistemas de seguridad actuales
12.6. Tendencias regulatorias y evolución previsible del marco de protección a medio y largo plazo

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.



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

