ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Gestión de Incidentes de Ciberseguridad y Continuidad de los Servicios Públicos Digitales

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 el Curso de Formación Permanente en Gestión de Incidentes de Ciberseguridad y Continuidad de los Servicios Públicos Digitales de ICUFOR, una propuesta académica diseñada para profesionales que desean liderar la protección de las infraestructuras tecnológicas del sector público. En un contexto donde la transformación digital de las administraciones avanza de forma acelerada, contar con expertos capaces de anticipar, detectar y gestionar ciberamenazas resulta fundamental para garantizar la prestación ininterrumpida de servicios esenciales a la ciudadanía.

A lo largo del programa, abordarás desde los fundamentos de la ciberseguridad en el ámbito público hasta el análisis del panorama de amenazas, la gestión de riesgos y los marcos normativos vigentes como el Esquema Nacional de Seguridad o la Directiva NIS2.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la ciberseguridad en las administraciones públicas, identificando los activos digitales críticos, los principios de seguridad de la información y los vectores de ataque específicos del entorno público.

Analizar el panorama de amenazas y aplicar metodologías de gestión de riesgos, elaborando mapas de riesgos y planes de tratamiento adaptados a los servicios públicos digitales.

Dominar las capacidades de detección, monitorización y alerta temprana, utilizando tecnologías SIEM, IDS/IPS, EDR/XDR y los sistemas de alerta del CCN-CERT para la protección de infraestructuras públicas.

Conocer el marco normativo, regulatorio y de gobernanza aplicable a la ciberseguridad del sector público, diferenciando las obligaciones derivadas del ENS, la Directiva NIS2, el RGPD y la legislación complementaria.

Diseñar marcos organizativos y procedimientos operativos de respuesta ante incidentes de ciberseguridad, desarrollando playbooks, métricas de rendimiento y estructuras de equipos CSIRT adecuadas al sector público.

Aplicar procedimientos de contención, erradicación, recuperación y análisis forense digital ante incidentes de ciberseguridad, garantizando la trazabilidad de acciones, la cadena de custodia y la preservación de evidencias.

Objetivos del curso

Elaborar planes de continuidad de servicios digitales y de recuperación ante desastres, definiendo estrategias de resiliencia, análisis de impacto y procedimientos de activación adaptados a las administraciones públicas.

Implementar programas de ejercicios, simulacros y mejora continua de las capacidades de respuesta y continuidad, incorporando las tendencias emergentes y los nuevos marcos regulatorios para la maduración de la ciberresiliencia en los servicios públicos.

Temario

01 Fundamentos de la ciberseguridad en el contexto de las administraciones públicas y los servicios digitales

1.1. Conceptualización de la ciberseguridad y su relevancia estratégica para el sector público
1.2. Evolución del proceso de transformación digital en las administraciones públicas españolas y europeas
1.3. Principios fundamentales de la seguridad de la información: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
1.4. Identificación y clasificación de activos digitales críticos en los servicios públicos
1.5. Superficie de exposición y cultura de ciberseguridad en las administraciones públicas

Temario

02 Marco normativo, regulatorio y de gobernanza de la ciberseguridad en el sector público

2.1. El Esquema Nacional de Seguridad (ENS): principios, categorización de sistemas y medidas de seguridad
2.2. La Directiva NIS2 y su transposición al ordenamiento jurídico español
2.3. El Reglamento General de Protección de Datos (RGPD) y la gestión de brechas de seguridad con datos personales
2.4. Legislación complementaria aplicable: Ley 40/2015, Ley 11/2022 de telecomunicaciones y normativa sectorial
2.5. Estrategia Nacional de Ciberseguridad y su articulación con los planes de seguridad autonómicos y locales
2.6. Marcos de gobernanza y roles institucionales: CCN, INCIBE, Mando Conjunto del Ciberespacio y CNPIC

03 Análisis del panorama de amenazas y gestión de riesgos en los servicios públicos digitales

3.1. Taxonomía actualizada de ciberamenazas dirigidas al sector público
3.2. Actores de amenaza relevantes: perfilado, motivaciones y tácticas habituales
3.3. Inteligencia de amenazas (Cyber Threat Intelligence) aplicada al sector público
3.4. Metodologías de análisis y gestión de riesgos en el ámbito público
3.5. Elaboración de mapas de riesgos y planes de tratamiento adaptados a servicios públicos esenciales
3.6. Monitorización continua del riesgo y actualización dinámica del perfil de amenazas

Temario

04 Marcos de referencia y modelos organizativos para la gestión de incidentes de ciberseguridad

4.1. Definición, tipología y clasificación de incidentes de ciberseguridad según las guías del CCN-CERT
4.2. Ciclo de vida de la gestión de incidentes: modelos NIST SP 800-61, ISO/IEC 27035 y ENISA
4.3. Diseño, estructura y funciones de un equipo de respuesta ante incidentes (CSIRT/CERT)
4.4. Definición de políticas, planes y procedimientos de respuesta ante incidentes
4.5. Playbooks y runbooks para escenarios de incidentes recurrentes
4.6. Métricas e indicadores clave de rendimiento (KPI) para evaluar la capacidad de respuesta
4.7. Integración de la gestión de incidentes con el sistema de gestión de seguridad de la información (SGSI)

Temario

05 Capacidades de detección, monitorización y alerta temprana en infraestructuras públicas

5.1. Arquitectura de detección en profundidad: principios de diseño y estrategia de defensa por capas
5.2. Sistemas de detección y prevención de intrusiones (IDS/IPS) en redes de la administración pública
5.3. Centros de Operaciones de Seguridad (SOC): diseño, operación y modelos de externalización
5.4. Plataformas SIEM: agregación, correlación y análisis de eventos de seguridad
5.5. Herramientas de detección y respuesta en el endpoint (EDR/XDR) y su aplicación en parques informáticos públicos
5.6. Sistemas de alerta temprana del CCN-CERT: SAT-INET, SAT-ICS y servicios de notificación proactiva
5.7. Monitorización de la superficie de ataque externa: dominios, credenciales expuestas y activos en Internet

Temario

06 Procedimientos operativos de respuesta, contención y erradicación de incidentes

6.1. Activación del procedimiento de respuesta: triaje inicial, verificación y escalado del incidente
6.2. Coordinación entre equipos técnicos, gestores y decisores durante la respuesta operativa
6.3. Estrategias y técnicas de contención a corto y largo plazo
6.4. Procesos de erradicación: eliminación de artefactos maliciosos, accesos persistentes y vulnerabilidades explotadas
6.5. Procedimientos de recuperación y restauración segura de sistemas y servicios
6.6. Gestión de la toma de decisiones bajo presión durante incidentes de alto impacto
6.7. Gestión de incidentes específicos en el sector público
6.8. Documentación operativa del incidente: registro cronológico, cadena de custodia y trazabilidad de acciones

Temario

07 Análisis forense digital y gestión de evidencias en incidentes del sector público

7.1. Fundamentos del análisis forense digital aplicado a la investigación de incidentes de ciberseguridad
7.2. Proceso de adquisición y preservación de evidencias digitales
7.3. Análisis forense de sistemas operativos Windows y Linux en estaciones de trabajo y servidores públicos
7.4. Análisis forense de redes, correo electrónico y entornos cloud utilizados por la administración
7.5. Herramientas forenses de referencia: soluciones del CCN y herramientas de código abierto
7.6. Elaboración del informe pericial y técnico-forense: estructura, contenido y presentación de hallazgos

Temario

08 Planificación de la continuidad de los servicios públicos digitales

8.1. Conceptos fundamentales de continuidad de negocio aplicados al sector público: continuidad de servicio frente a continuidad de negocio
8.2. Marcos normativos y estándares de referencia para la continuidad: ISO 22301, ISO 22317 y guías del CCN
8.3. Análisis de Impacto en el Negocio (BIA) aplicado a servicios públicos digitales
8.4. Evaluación de riesgos de continuidad: amenazas que pueden provocar la interrupción de servicios esenciales
8.5. Desarrollo del Plan de Continuidad de Servicios Digitales (PCSD): estructura, alcance y contenido
8.6. Gobernanza de la continuidad: estructura organizativa y asignación de recursos
8.7. Integración de la continuidad de servicios digitales con los planes de continuidad generales de la organización pública

Temario

09 Estrategias de recuperación ante desastres y resiliencia de las infraestructuras públicas digitales

9.1. Conceptualización de la recuperación ante desastres (Disaster Recovery) y su relación con la continuidad de servicios
9.2. Diseño del Plan de Recuperación ante Desastres (DRP) para infraestructuras tecnológicas del sector público
9.3. Estrategias de respaldo y restauración de datos en entornos públicos
9.4. Recuperación ante desastres en entornos cloud e infraestructuras híbridas utilizadas por la administración
9.5. Resiliencia operativa digital: diseño de infraestructuras tolerantes a fallos y con capacidad de auto-recuperación
9.6. Pruebas y ejercicios de recuperación: tipología, planificación, ejecución y evaluación de resultados

Temario

10 Comunicación de crisis, notificación de incidentes y coordinación interinstitucional

10.1. Principios de la comunicación de crisis en el contexto de incidentes de ciberseguridad que afectan a servicios públicos
10.2. Protocolos de notificación obligatoria de incidentes de ciberseguridad en el sector público
10.3. Coordinación operativa entre CSIRT nacionales, autonómicos y sectoriales durante incidentes de gran alcance
10.4. Comunicación interna durante la gestión del incidente: flujos de información y gestión del conocimiento situacional
10.5. Relación con las fuerzas y cuerpos de seguridad del Estado y la Fiscalía en incidentes con implicaciones penales
10.6. Gestión de la dimensión política e institucional de los ciberincidentes en administraciones públicas

Temario

11 Ejercicios, simulacros y mejora continua de las capacidades de respuesta y continuidad

11.1. Importancia de los ejercicios de ciberseguridad para la validación de planes y la capacitación de equipos
11.2. Tipología de ejercicios y simulacros de ciberseguridad aplicables al sector público
11.3. Diseño y planificación de un ejercicio de gestión de incidentes para una entidad pública
11.4. Proceso de lecciones aprendidas (After Action Review) tras incidentes reales y ejercicios simulados
11.5. Marcos de mejora continua y maduración de las capacidades de respuesta y continuidad

12 Tendencias emergentes, retos futuros y evolución de la ciberresiliencia en los servicios públicos digitales

12.1. Impacto de las tecnologías emergentes en la gestión de incidentes y la continuidad de servicios públicos
12.2. Ciberresiliencia como paradigma integral: del enfoque reactivo al enfoque adaptativo y anticipatorio
12.3. Nuevos desafíos y marcos regulatorios para la ciberseguridad de los servicios públicos
12.4. Hoja de ruta para la maduración de las capacidades de gestión de incidentes y continuidad en una administración pública

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

