ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Análisis de Riesgos y Políticas de Seguridad de la Información en Organizaciones 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



Especialízate con el Curso de Formación Permanente en Análisis de Riesgos y Políticas de Seguridad de la Información en Organizaciones Públicas de ICUFOR, una propuesta académica diseñada para profesionales que buscan liderar la protección de sistemas y datos en el ámbito de la Administración Pública. En un entorno donde la transformación digital exige garantías sólidas de confidencialidad, integridad y disponibilidad, este programa te prepara para afrontar los desafíos actuales del sector público.

A lo largo de la formación, profundizarás en el marco normativo vigente, incluyendo el Esquema Nacional de Seguridad, la Directiva NIS2 y el RGPD, así como en metodologías reconocidas como MAGERIT y la herramienta PILAR.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la seguridad de la información en el sector público, identificando sus dimensiones esenciales y los desafíos derivados de la transformación digital de las administraciones.

Conocer el marco normativo y regulatorio multinivel, distinguiendo las obligaciones derivadas de la legislación europea, nacional y autonómica aplicable a las organizaciones públicas.

Analizar los modelos de gobernanza de la seguridad de la información, diferenciando los roles, responsabilidades y estructuras organizativas establecidos por el Esquema Nacional de Seguridad.

Dominar las metodologías de análisis de riesgos, aplicando marcos como MAGERIT y la herramienta PILAR para la identificación y valoración de activos, amenazas y vulnerabilidades en entornos públicos.

Definir estrategias de tratamiento del riesgo, elaborando planes que integren salvaguardas y controles de seguridad adecuados al contexto y categorización de los sistemas.

Diseñar políticas y normativas de seguridad de la información, desarrollando la estructura documental exigida por el Esquema Nacional de Seguridad y su proceso de adecuación y certificación.

Implementar procedimientos de gestión de incidentes y continuidad de servicios públicos, incorporando capacidades de detección, respuesta, recuperación ante desastres y coordinación institucional.

Aplicar procesos de auditoría y mejora continua del sistema de gestión de la seguridad, utilizando métricas, indicadores y planes de acciones correctivas para garantizar el cumplimiento normativo.

Temario

01 Fundamentos de la seguridad de la información en el contexto de las organizaciones públicas

1.1. Concepto y dimensiones de la seguridad de la información: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad
1.2. Evolución histórica de la seguridad de la información en la Administración Pública
1.3. Particularidades y desafíos específicos de la seguridad de la información en organizaciones públicas
1.4. El ecosistema de amenazas actual frente al sector público: ciberamenazas, ingeniería social y amenazas internas
1.5. Transformación digital y cultura de seguridad de la información en la Administración Pública

Temario

02 Marco normativo y regulatorio aplicable a la seguridad de la información en el sector público

2.1. Estructura del marco jurídico multinivel en materia de seguridad de la información
2.2. El Esquema Nacional de Seguridad (Real Decreto 311/2022): estructura, principios y ámbito de aplicación
2.3. El Reglamento General de Protección de Datos y la Ley Orgánica 3/2018 en su relación con la seguridad de la información
2.4. Ley 36/2015 de Seguridad Nacional y su encuadre en la estrategia de ciberseguridad
2.5. Normativa sobre administración electrónica y su vinculación con la seguridad: Ley 39/2015 y disposiciones de desarrollo
2.6. Organismos competentes y de referencia en materia de ciberseguridad pública
2.7. Estándares y marcos de referencia internacionales aplicables al sector público

Temario

03 Gobernanza y organización de la seguridad de la información en entidades públicas

3.1. Concepto de gobernanza de la seguridad de la información y su importancia estratégica en la gestión pública
3.2. Modelos organizativos para la gestión de la seguridad de la información en administraciones públicas
3.3. Roles y responsabilidades definidos por el Esquema Nacional de Seguridad
3.4. Coordinación interinstitucional y cooperación entre administraciones en materia de seguridad
3.5. Planificación estratégica de la seguridad: planes directores y hojas de ruta para organizaciones públicas
3.6. Indicadores clave de rendimiento (KPI) y cuadros de mando para la gestión de la seguridad de la información

Temario

04 Fundamentos y metodologías de análisis de riesgos en seguridad de la información

4.1. Concepto de riesgo en el ámbito de la seguridad de la información: componentes, factores y relaciones
4.2. Objetivos y beneficios del análisis de riesgos como herramienta de toma de decisiones en la gestión pública
4.3. Enfoques metodológicos para el análisis de riesgos: cualitativo, cuantitativo y mixto
4.4. La metodología MAGERIT: marco de referencia para la Administración Pública española
4.5. Otras metodologías y marcos de análisis de riesgos de aplicación complementaria
4.6. Criterios para la selección de la metodología más adecuada según el tipo y tamaño de la organización pública
4.7. Fases del proceso de análisis de riesgos: de la planificación al informe de resultados
4.8. Integración del análisis de riesgos de seguridad de la información con otros sistemas de gestión de riesgos institucionales

Temario

05 Identificación, clasificación y valoración de activos de información en organizaciones públicas

5.1. Concepto de activo de información y su papel central en el análisis de riesgos
5.2. Tipología de activos de información en el entorno de la Administración Pública
5.3. Metodología para la elaboración del inventario de activos de información
5.4. Criterios y escalas de valoración de activos según las dimensiones de seguridad
5.5. Clasificación de la información en el sector público: niveles de sensibilidad y criterios de etiquetado
5.6. Gestión del ciclo de vida de los activos de información

06 Análisis de amenazas, vulnerabilidades e impacto en organizaciones públicas

6.1. Identificación y taxonomía de amenazas relevantes para las organizaciones del sector público
6.2. Identificación y evaluación de vulnerabilidades en los sistemas de información públicos
6.3. Estimación de la probabilidad de materialización de las amenazas
6.4. Análisis del impacto potencial sobre la organización y los servicios públicos
6.5. Construcción del mapa de riesgos: representación, priorización y comunicación de resultados

Temario

07 Evaluación, tratamiento y gestión integral del riesgo en seguridad de la información

7.1. Evaluación del riesgo: comparación del nivel de riesgo estimado con los criterios de aceptación definidos
7.2. Estrategias de tratamiento del riesgo y su aplicación en organizaciones públicas
7.3. Selección, diseño e implantación de salvaguardas y controles de seguridad
7.4. Elaboración del plan de tratamiento de riesgos: contenido, plazos, recursos y responsables
7.5. Gestión del riesgo residual: monitorización, revisión periódica y comunicación a la dirección
7.6. Declaración de aplicabilidad y documentación formal del proceso de gestión de riesgos
7.7. Integración del ciclo de gestión de riesgos en el sistema de mejora continua de la organización (PDCA)

Temario

08 Diseño, desarrollo e implantación de políticas de seguridad de la información en el sector público

8.1. Concepto, naturaleza jurídica y función de la política de seguridad de la información en la Administración Pública
8.2. Requisitos de la política de seguridad según el Esquema Nacional de Seguridad
8.3. Estructura documental del sistema de gestión de la seguridad de la información
8.4. Metodología para la elaboración de políticas y normativas de seguridad de la información
8.5. Ámbitos específicos que deben cubrir las normativas de seguridad en organizaciones públicas
8.6. Comunicación, difusión y formación sobre las políticas de seguridad al personal de la organización
8.7. Revisión periódica y actualización de las políticas ante cambios normativos, organizativos o tecnológicos

Temario

09 El Esquema Nacional de Seguridad como marco integral de referencia para las organizaciones públicas

9.1. Objetivos, ámbito de aplicación y sujetos obligados por el Esquema Nacional de Seguridad
9.2. Proceso de categorización de los sistemas de información según el ENS
9.3. Medidas de seguridad del Anexo II: marco organizativo, marco operacional y medidas de protección
9.4. Perfiles de cumplimiento específicos y su utilidad para distintos tipos de entidades públicas
9.5. Proceso de adecuación y certificación de conformidad con el ENS
9.6. Instrucciones técnicas de seguridad y relación del ENS con otros marcos normativos

Temario

10 Gestión de incidentes de seguridad de la información en organizaciones públicas

10.1. Concepto, tipología y clasificación de los incidentes de seguridad de la información en el sector público
10.2. Marco de referencia para la gestión de incidentes: guía CCN-STIC 817 y normativa aplicable
10.3. Diseño y organización de la capacidad de respuesta ante incidentes
10.4. Fases del ciclo de gestión de un incidente de seguridad
10.5. Obligaciones de notificación de incidentes a autoridades competentes: CCN-CERT, AEPD y organismos sectoriales
10.6. Coordinación con el CCN-CERT y otros CSIRT de referencia nacional e internacional

Temario

11 Planes de continuidad de los servicios públicos y recuperación ante desastres

11.1. Concepto y alcance de la continuidad de los servicios públicos en el contexto de la seguridad de la información
11.2. Marco normativo y requisitos en materia de continuidad del servicio
11.3. Análisis de impacto en el negocio (BIA) aplicado a los servicios públicos esenciales
11.4. Diseño, elaboración y prueba de los planes de continuidad y recuperación
11.5. Integración de la gestión de la continuidad con el análisis de riesgos y la gestión de incidentes

12 Auditoría, cumplimiento normativo y mejora continua en seguridad de la información en el sector público

12.1. Concepto, objetivos y tipos de auditoría de seguridad de la información en organizaciones públicas
12.2. Planificación, ejecución y resultados de la auditoría de seguridad de la información
12.3. El ciclo de mejora continua (PDCA) aplicado al sistema de gestión de la seguridad de la información
12.4. Tendencias, retos emergentes y evolución futura de la seguridad de la información en las administraciones públicas

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

