ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Gestión de Vulnerabilidades en los Sistemas de Información de la Administración Pública: Análisis y Remediación

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 Vulnerabilidades en los Sistemas de Información de la Administración Pública: Análisis y Remediación de ICUFOR, una formación diseñada para profesionales que buscan dominar las estrategias de ciberseguridad específicas del sector público. En un contexto donde las amenazas digitales evolucionan constantemente, las administraciones públicas requieren expertos capaces de proteger infraestructuras críticas y garantizar la continuidad de los servicios esenciales para la ciudadanía.

A través de este programa, desarrollarás competencias fundamentales en el marco normativo vigente, incluyendo el Esquema Nacional de Seguridad y la Directiva NIS2, así como en metodologías avanzadas de identificación, análisis y priorización de vulnerabilidades.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la seguridad de la información en la Administración Pública, identificando las ciberamenazas, los actores de amenaza y los vectores de ataque dirigidos al sector público.

Describir la arquitectura y los componentes de los sistemas de información públicos, clasificando las infraestructuras, los servicios de administración electrónica y los activos tecnológicos que conforman la superficie de ataque.

Aplicar metodologías y técnicas de identificación, análisis y priorización de vulnerabilidades, utilizando enfoques de escaneo, auditorías de configuración y criterios de priorización basados en el riesgo real de explotación.

Diseñar estrategias de remediación, gestión de parches y gestión de vulnerabilidades en la cadena de suministro, implementando procesos de corrección, verificación, tratamiento de excepciones y evaluación de proveedores.

Conocer el marco normativo y regulatorio de la ciberseguridad en las administraciones públicas, analizando el Esquema Nacional de Seguridad, la normativa europea y los estándares internacionales aplicables.

Dominar los conceptos, el ciclo de vida y los sistemas de catalogación y puntuación de vulnerabilidades, diferenciando tipologías, métricas de severidad y modelos de madurez del programa de gestión.

Conocer las herramientas y tecnologías para la gestión integral de vulnerabilidades, evaluando soluciones de escaneo, plataformas de gestión centralizada y mecanismos de automatización adaptados al sector público.

Desarrollar capacidades de monitorización continua y respuesta ante vulnerabilidades críticas, incorporando la inteligencia de amenazas, los cuadros de mando y los principios de mejora continua del programa de gestión.

Temario

01 Fundamentos de la seguridad de la información en el contexto de la Administración Pública

1.1. Conceptos esenciales de seguridad de la información: confidencialidad, integridad y disponibilidad
1.2. Panorama actual de las ciberamenazas dirigidas al sector público
1.3. Particularidades de la seguridad de la información en la Administración Pública frente al sector privado
1.4. El papel del Centro Criptológico Nacional y los equipos de respuesta ante incidentes de seguridad
1.5. Gobernanza de la seguridad y cultura de ciberseguridad en las organizaciones del sector público

02 Marco normativo y regulatorio de la ciberseguridad en las administraciones públicas

2.1. El Esquema Nacional de Seguridad: principios rectores, requisitos y categorización de los sistemas
2.2. Normativa europea en materia de ciberseguridad y su impacto en la Administración española
2.3. Legislación nacional complementaria: Ley de Seguridad Nacional y normativa de protección de datos personales
2.4. Guías y estándares del CCN-STIC aplicables a los procesos de gestión de vulnerabilidades
2.5. Marcos internacionales de referencia y su integración con la normativa nacional
2.6. Responsabilidades legales y obligaciones de notificación ante incidentes derivados de vulnerabilidades

Temario

03 Arquitectura y componentes de los sistemas de información en la Administración Pública

3.1. Tipología y clasificación de los sistemas de información desplegados en el sector público
3.2. Infraestructuras de red y comunicaciones en entornos gubernamentales
3.3. Servicios de administración electrónica y plataformas compartidas de uso común
3.4. Infraestructuras cloud en la Administración Pública: modelos de despliegue y consideraciones de seguridad
3.5. Sistemas de gestión de identidades, autenticación y control de accesos en el ámbito público
3.6. Inventario y gestión de activos tecnológicos como requisito previo a la gestión de vulnerabilidades

Temario

04 Fundamentos de la gestión de vulnerabilidades: conceptos, ciclo de vida y modelos de madurez

4.1. Definición y tipología de vulnerabilidades en los sistemas de información
4.2. Ciclo de vida completo de una vulnerabilidad: desde el descubrimiento hasta la resolución
4.3. Bases de datos y sistemas estandarizados de catalogación de vulnerabilidades
4.4. Sistemas de puntuación y clasificación de la severidad de las vulnerabilidades
4.5. Modelos de madurez para evaluar y mejorar el programa de gestión de vulnerabilidades
4.6. Integración de la gestión de vulnerabilidades en el sistema de gestión de la seguridad de la información
4.7. Indicadores clave de rendimiento para medir la eficacia y cobertura del programa

Temario

05 Identificación y descubrimiento de vulnerabilidades en entornos de la Administración Pública

5.1. Estrategias y enfoques metodológicos para el descubrimiento de vulnerabilidades
5.2. Escaneo de vulnerabilidades en infraestructuras de red y sistemas operativos
5.3. Análisis de vulnerabilidades en aplicaciones web y servicios de administración electrónica
5.4. Identificación de vulnerabilidades en entornos cloud e infraestructuras virtualizadas
5.5. Detección de vulnerabilidades en dispositivos de red, sistemas IoT y entornos de tecnología operacional
5.6. Auditorías de configuración y verificación del cumplimiento de líneas base de bastionado
5.7. Pruebas de penetración como complemento cualitativo al escaneo automatizado de vulnerabilidades

Temario

06 Análisis, evaluación y priorización de las vulnerabilidades detectadas

6.1. Proceso de validación y triaje de los resultados obtenidos en las fases de escaneo
6.2. Contextualización de las vulnerabilidades en función del entorno organizativo y la arquitectura
6.3. Metodologías avanzadas de priorización basadas en el riesgo real de explotación
6.4. Análisis de la explotabilidad: disponibilidad de exploits y actividad observada en el entorno de amenazas
6.5. Elaboración de informes técnicos y ejecutivos sobre el estado de las vulnerabilidades
6.6. Integración de la evaluación de vulnerabilidades con el análisis de riesgos institucional

07 Herramientas y tecnologías para la gestión integral de vulnerabilidades

7.1. Escáneres de vulnerabilidades de infraestructura: arquitectura, despliegue y configuración operativa
7.2. Herramientas especializadas en el análisis de seguridad de aplicaciones web y APIs
7.3. Plataformas de gestión centralizada de vulnerabilidades y orquestación de la remediación
7.4. Soluciones de gestión de la superficie de ataque externa (EASM) en organizaciones públicas
7.5. Automatización y scripting aplicados a los procesos de gestión de vulnerabilidades
7.6. Criterios de selección, evaluación e implantación de herramientas en la Administración Pública

Temario

08 Gestión de vulnerabilidades en la cadena de suministro de software y componentes de terceros

8.1. Riesgos de seguridad en la cadena de suministro de software de la Administración Pública
8.2. Software Bill of Materials (SBOM): transparencia y trazabilidad de los componentes de software
8.3. Análisis de composición de software y gestión de dependencias de terceros
8.4. Evaluación de la postura de seguridad de proveedores y contratistas tecnológicos
8.5. Respuesta coordinada ante vulnerabilidades en componentes de la cadena de suministro

Temario

09 Estrategias y procesos de remediación de vulnerabilidades en los sistemas de información públicos

9.1. Diseño del proceso de remediación: definición de roles, responsabilidades y flujos de trabajo
9.2. Opciones de tratamiento de vulnerabilidades: remediación, mitigación, aceptación y transferencia del riesgo
9.3. Aplicación de parches de seguridad: planificación, pruebas previas y despliegue controlado
9.4. Remediación de vulnerabilidades de configuración y aplicación de guías de bastionado de sistemas
9.5. Corrección de vulnerabilidades en el ciclo de desarrollo seguro de software público
9.6. Verificación y comprobación de la eficacia de las acciones de remediación aplicadas
9.7. Gestión de excepciones y tratamiento de vulnerabilidades no remediables a corto plazo
9.8. Coordinación entre equipos y gestión del cambio en los procesos de remediación

Temario

10 Gestión de parches y actualizaciones en las infraestructuras tecnológicas de la Administración Pública

10.1. Fundamentos y objetivos de un programa de gestión de parches en el contexto del sector público
10.2. Diseño e implantación de una política corporativa de gestión de parches y actualizaciones
10.3. Herramientas y plataformas de gestión centralizada de parches en entornos heterogéneos
10.4. Automatización del ciclo completo de vida de los parches: detección, aprobación, despliegue y verificación
10.5. Retos específicos del parcheado en la Administración Pública
10.6. Métricas e indicadores para la evaluación y la mejora continua del programa de gestión de parches

Temario

11 Monitorización continua, respuesta ante vulnerabilidades críticas y mejora del programa de gestión

11.1. Principios y arquitectura de un modelo de monitorización continua de vulnerabilidades
11.2. Gestión de la inteligencia de amenazas aplicada a la priorización dinámica de vulnerabilidades
11.3. Procedimientos de respuesta acelerada ante la publicación de vulnerabilidades críticas y de día cero
11.4. Cuadros de mando, reporting periódico y comunicación a la dirección y los órganos de gobierno
11.5. Auditoría, mejora continua y evolución futura del programa de gestión de vulnerabilidades

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

