ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Inteligencia Artificial y Ciberseguridad en la Administración Pública: Detección de Amenazas y Deepfakes

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 Inteligencia Artificial y Ciberseguridad en la Administración Pública: Detección de Amenazas y Deepfakes de ICUFOR. En un contexto donde las instituciones públicas enfrentan ciberataques cada vez más sofisticados y contenidos manipulados mediante inteligencia artificial, la protección de los sistemas de información y la confianza ciudadana se han convertido en prioridades estratégicas. Este programa está diseñado para profesionales que buscan liderar la transformación digital segura del sector público.

A lo largo de esta formación, abordarás desde los fundamentos de la inteligencia artificial aplicada a la ciberseguridad hasta técnicas avanzadas de aprendizaje automático para la detección de amenazas.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la inteligencia artificial y la ciberseguridad, identificando su convergencia y aplicación estratégica en el ámbito de la administración pública.

Clasificar las ciberamenazas y vulnerabilidades específicas de los sistemas de información públicos, analizando sus actores, motivaciones e impacto en la prestación de servicios al ciudadano.

Analizar la arquitectura y el funcionamiento de los sistemas inteligentes de detección de intrusiones y anomalías, relacionando su integración con los Centros de Operaciones de Seguridad y las arquitecturas Zero Trust.

Desarrollar capacidades de protección de la identidad digital y gestión de incidentes de ciberseguridad, utilizando sistemas de autenticación avanzada, análisis forense digital y plataformas de respuesta automatizada con apoyo de inteligencia artificial.

Conocer el marco normativo, regulatorio e institucional aplicable a la ciberseguridad y la inteligencia artificial en el sector público, diferenciando la legislación europea y nacional vigente.

Dominar las técnicas de aprendizaje automático y aprendizaje profundo orientadas a la detección de amenazas, describiendo los procesos de entrenamiento, validación y evaluación del rendimiento de los modelos.

Identificar los fundamentos tecnológicos, las tipologías y los riesgos de los deepfakes para la administración pública, aplicando técnicas, herramientas y metodologías específicas para su detección en el ámbito institucional.

Fundamentar la gobernanza ética y la planificación estratégica para la implementación de la inteligencia artificial y la ciberseguridad en la administración pública, incorporando criterios de transparencia, formación del personal y cooperación interinstitucional.

Temario

01 Fundamentos de la inteligencia artificial y su convergencia con la ciberseguridad en la administración pública

1.1. Conceptualización y evolución histórica de la inteligencia artificial
1.2. Principales ramas y técnicas de la inteligencia artificial con aplicación en ciberseguridad
1.3. La ciberseguridad como disciplina estratégica en el sector público
1.4. Convergencia entre inteligencia artificial y ciberseguridad: oportunidades y riesgos emergentes
1.5. Madurez digital y actores clave en la postura de ciberseguridad de las administraciones públicas

Temario

02 Marco normativo, regulatorio e institucional de la ciberseguridad y la inteligencia artificial en el sector público

2.1. Normativa europea en materia de ciberseguridad aplicable a las administraciones públicas
2.2. Regulación europea de la inteligencia artificial: el Reglamento de IA (AI Act)
2.3. Legislación nacional en ciberseguridad y administración electrónica
2.4. Organismos e instituciones nacionales y europeos de referencia en ciberseguridad
2.5. Estándares y marcos de referencia internacionales en ciberseguridad
2.6. Responsabilidad jurídica y régimen sancionador en materia de ciberseguridad e IA en el sector público

Temario

03 Panorama de ciberamenazas y vulnerabilidades específicas de la administración pública

3.1. Evolución y tendencias del panorama global de ciberamenazas
3.2. Taxonomía y clasificación de las ciberamenazas dirigidas al sector público
3.3. Actores de amenaza y sus motivaciones en el contexto del sector público
3.4. Vulnerabilidades específicas de los sistemas de información públicos
3.5. Impacto de los ciberataques en la prestación de servicios públicos y la confianza ciudadana
3.6. Inteligencia de amenazas (Threat Intelligence) aplicada a la protección del sector público

Temario

04 Técnicas de aprendizaje automático y aprendizaje profundo para la detección de ciberamenazas

4.1. Fundamentos del aprendizaje automático aplicado a la detección de amenazas
4.2. Arquitecturas de aprendizaje profundo para la identificación de ciberamenazas
4.3. Técnicas de inteligencia artificial para la detección y clasificación de malware
4.4. Procesamiento y preparación de datos para modelos de detección de amenazas
4.5. Entrenamiento, validación y evaluación del rendimiento de modelos de detección
4.6. Inteligencia artificial adversarial: ataques y técnicas de evasión contra modelos de detección
4.7. Herramientas y plataformas de código abierto para la implementación de modelos de detección
4.8. Limitaciones y desafíos del aprendizaje automático en la ciberseguridad del sector público

Temario

05 Sistemas inteligentes de detección de intrusiones y análisis de anomalías en redes y sistemas públicos

5.1. Arquitectura y tipología de los sistemas de detección y prevención de intrusiones (IDS/IPS)
5.2. Detección de amenazas conocidas y desconocidas (zero-day) mediante técnicas de inteligencia artificial
5.3. Análisis de comportamiento de usuarios y entidades (UEBA) en la administración pública
5.4. Centros de Operaciones de Seguridad (SOC) potenciados con inteligencia artificial
5.5. Arquitecturas de seguridad Zero Trust y su relación con los sistemas inteligentes de detección
5.6. Casos prácticos de implementación de sistemas inteligentes de detección en organismos públicos

Temario

06 Deepfakes: fundamentos tecnológicos, tipologías y riesgos para la administración pública

6.1. Concepto, origen y evolución histórica de la tecnología deepfake
6.2. Fundamentos técnicos de la generación de deepfakes
6.3. Tipologías de deepfakes y su grado de sofisticación técnica
6.4. Amenazas específicas de los deepfakes para la administración pública
6.5. Impacto de los deepfakes en la confianza ciudadana y la integridad institucional
6.6. Evolución previsible y tendencias emergentes en la sofisticación de las técnicas de generación de deepfakes

Temario

07 Técnicas, herramientas y metodologías para la detección de deepfakes en el ámbito institucional

7.1. Fundamentos de la detección de deepfakes: enfoques metodológicos y desafíos
7.2. Técnicas de detección de deepfakes de vídeo e imagen
7.3. Técnicas de detección de deepfakes de audio y voz sintética
7.4. Herramientas y plataformas tecnológicas de detección de deepfakes
7.5. Estándares de procedencia y autenticación del contenido digital
7.6. Metodología para la implantación de capacidades de detección de deepfakes en la administración pública
7.7. Limitaciones actuales y retos futuros en la detección automatizada de deepfakes

Temario

08 Protección de la identidad digital, autenticación avanzada y prevención del fraude en el sector público

8.1. La identidad digital en la administración pública: concepto, componentes y ecosistema
8.2. Sistemas de autenticación robusta frente a amenazas basadas en inteligencia artificial
8.3. Aplicación de la inteligencia artificial en la prevención y detección del fraude documental
8.4. Tecnologías de registro distribuido y sellado para la autenticidad documental
8.5. Marco de confianza digital europeo: eIDAS 2.0 y la cartera de identidad digital europea

Temario

09 Gestión de incidentes de ciberseguridad y respuesta ante ataques con apoyo de inteligencia artificial

9.1. Ciclo de vida de la gestión de incidentes de ciberseguridad en la administración pública
9.2. Automatización de la respuesta a incidentes mediante inteligencia artificial
9.3. Planes de continuidad operativa y recuperación ante desastres en la administración pública
9.4. Análisis forense digital potenciado con técnicas de inteligencia artificial
9.5. Comunicación institucional y gestión de crisis ante ciberincidentes en el sector público
9.6. Simulacros, ejercicios de ciberseguridad y ciberresiliencia del sector público

Temario

10 Gobernanza, ética y estrategia de implementación de la inteligencia artificial y la ciberseguridad en la administración pública

10.1. Gobernanza de la inteligencia artificial en el sector público
10.2. Principios éticos en el uso de inteligencia artificial para la ciberseguridad pública
10.3. Colaboración público-privada y cooperación internacional en materia de ciberseguridad e IA
10.4. Diseño e implementación de una estrategia integral de IA y ciberseguridad en la administración pública
10.5. Formación y concienciación del personal público en ciberseguridad e inteligencia artificial
10.6. Contratación pública de soluciones de IA para ciberseguridad: criterios y buenas prácticas
10.7. Tendencias emergentes y prospectiva en inteligencia artificial y ciberseguridad para el sector público

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

