ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Ciberseguridad para Empleados Públicos: Buenas Prácticas y Prevención de Incidentes

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 Ciberseguridad para Empleados Públicos: Buenas Prácticas y Prevención de Incidentes de ICUFOR. En un contexto donde la transformación digital de las Administraciones Públicas avanza a ritmo acelerado, la protección de los sistemas de información se ha convertido en una responsabilidad compartida por todos los profesionales del sector público. Este programa formativo responde a la necesidad urgente de capacitar al personal funcionario y laboral en las competencias esenciales para salvaguardar los activos digitales de la ciudadanía.



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 sus principios, dimensiones y activos críticos que requieren protección.

Conocer el marco normativo aplicable a la seguridad de la información en el sector público, distinguiendo las obligaciones del empleado público derivadas del ENS, el RGPD, la Directiva NIS2 y las políticas internas de la organización.

Identificar las principales ciberamenazas y tipologías de ataques dirigidos al sector público, reconociendo sus vectores de infección, motivaciones y señales de alerta asociadas.

Analizar las técnicas de ingeniería social, phishing y manipulación psicológica, aplicando procedimientos de verificación, actuación y notificación ante comunicaciones sospechosas.

Dominar las buenas prácticas en gestión de contraseñas y autenticación multifactor, implementando mecanismos de control de acceso seguro en el puesto de trabajo.

Aplicar pautas de uso seguro del correo electrónico, la navegación web, las herramientas colaborativas y los dispositivos móviles, incorporando medidas de protección tanto en el entorno presencial como en el teletrabajo.

Conocer los criterios de clasificación, tratamiento y protección de datos e información sensible, utilizando técnicas de cifrado, destrucción segura y almacenamiento en ubicaciones corporativas autorizadas.

Desarrollar la capacidad de prevención, detección temprana y notificación de incidentes de ciberseguridad, colaborando activamente en la respuesta ante incidentes y en la consolidación de una cultura organizacional de seguridad.

Temario

01 Fundamentos de la ciberseguridad en el contexto de las Administraciones Públicas

1.1. Concepto y alcance de la ciberseguridad en el ámbito de la función pública
1.2. La transformación digital de la Administración y sus implicaciones en materia de seguridad
1.3. Principios fundamentales de la seguridad de la información
1.4. Activos de información críticos en las Administraciones Públicas y su necesidad de protección
1.5. Principales actores en el ecosistema de ciberseguridad pública y el papel del empleado público como primera línea de defensa

Temario

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

2.1. El Esquema Nacional de Seguridad (ENS): principios, requisitos y categorización de los sistemas
2.2. El Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD)
2.3. Ley 40/2015 de Régimen Jurídico del Sector Público y Ley 39/2015 de Procedimiento Administrativo Común en relación con la seguridad digital
2.4. Directiva NIS2 y su transposición al ordenamiento jurídico español: implicaciones para las entidades del sector público
2.5. Políticas de seguridad internas de las organizaciones públicas: estructura, difusión y cumplimiento obligatorio
2.6. Régimen sancionador y consecuencias disciplinarias derivadas del incumplimiento de las normas de ciberseguridad

Temario

03 Panorama de amenazas y tipología de ciberataques dirigidos al sector público

3.1. Evolución reciente del panorama de ciberamenazas contra las Administraciones Públicas
3.2. Malware: tipos, vectores de infección y consecuencias para los sistemas de la Administración
3.3. Ataques de denegación de servicio (DoS y DDoS) y su impacto en la disponibilidad de servicios al ciudadano
3.4. Vulnerabilidades en aplicaciones web y portales de la Administración electrónica
3.5. Amenazas internas: errores humanos, negligencias y acciones malintencionadas del personal
3.6. Ataques a la cadena de suministro tecnológico de las Administraciones Públicas
3.7. Amenazas emergentes: inteligencia artificial generativa como herramienta de ataque y deepfakes aplicados a la suplantación institucional

Temario

04 Ingeniería social, phishing y técnicas de manipulación dirigidas a empleados públicos

4.1. Fundamentos psicológicos de la ingeniería social: principios de persuasión y explotación de sesgos cognitivos
4.2. Phishing por correo electrónico: anatomía de un ataque, indicadores de alerta y ejemplos reales en la Administración
4.3. Variantes del phishing: smishing (SMS), vishing (llamadas telefónicas) y phishing a través de redes sociales
4.4. Ataques de pretexting, baiting y quid pro quo aplicados al entorno laboral público
4.5. Procedimiento de actuación del empleado público ante la recepción de una comunicación sospechosa
4.6. Ejercicios y simulaciones de phishing como herramienta formativa y de concienciación organizacional

Temario

05 Gestión segura de contraseñas, autenticación y control de accesos

5.1. Importancia de la autenticación robusta en la protección de los sistemas públicos
5.2. Buenas prácticas en la creación, uso y renovación de contraseñas seguras
5.3. Autenticación multifactor (MFA) y mecanismos de identificación digital en la Administración
5.4. Principio de mínimo privilegio y gestión de permisos de acceso a sistemas y carpetas compartidas
5.5. Bloqueo de sesión, cierre seguro y protección del puesto de trabajo desatendido

Temario

06 Uso seguro del correo electrónico, la navegación web y las herramientas colaborativas

6.1. Buenas prácticas en el uso del correo electrónico corporativo de la Administración
6.2. Navegación web segura desde los equipos de la Administración
6.3. Seguridad en el uso de herramientas colaborativas y plataformas en la nube autorizadas
6.4. Uso responsable de herramientas de inteligencia artificial generativa y servicios en línea desde el entorno de trabajo
6.5. Uso seguro de las redes sociales y su impacto en la reputación institucional y la exposición a ataques
6.6. Gestión segura de dispositivos de almacenamiento externo: memorias USB, discos y soportes ópticos
6.7. Actualización de software y aplicaciones: importancia de los parches de seguridad y responsabilidad del usuario

Temario

07 Protección de datos, clasificación de la información y tratamiento documental seguro

7.1. Clasificación de la información en las Administraciones Públicas según su nivel de sensibilidad
7.2. Tratamiento seguro de la información en cada fase de su ciclo de vida
7.3. Protección de datos personales en las tareas cotidianas del empleado público
7.4. Cifrado de información: conceptos fundamentales y aplicación práctica para la protección de ficheros, correos y soportes
7.5. Copias de seguridad: responsabilidad del usuario en el almacenamiento en ubicaciones corporativas autorizadas
7.6. Escritorio limpio y pantalla limpia: normas de seguridad física de la información en el puesto de trabajo

Temario

08 Seguridad en el teletrabajo, dispositivos móviles y redes de comunicación

8.1. Marco específico del teletrabajo en las Administraciones Públicas y sus riesgos de ciberseguridad asociados
8.2. Configuración segura del espacio de teletrabajo doméstico
8.3. Conexión segura a la red corporativa mediante redes privadas virtuales (VPN)
8.4. Seguridad en dispositivos móviles corporativos y personales utilizados con fines laborales (BYOD)
8.5. Seguridad en las comunicaciones: precauciones en videoconferencias, mensajería instantánea y llamadas
8.6. Protocolo de actuación ante la pérdida, robo o compromiso de un dispositivo con información de la Administración

Temario

09 Prevención, detección temprana y notificación de incidentes de ciberseguridad

9.1. Concepto de incidente de ciberseguridad y su taxonomía en el marco del CCN-CERT
9.2. Evaluación de riesgos de ciberseguridad en las actividades cotidianas del puesto de trabajo
9.3. Medidas preventivas que debe adoptar el empleado público en su actividad diaria
9.4. Herramientas y tecnologías de protección que debe conocer el empleado público
9.5. Indicadores de compromiso y señales de alerta que debe reconocer el empleado público
9.6. Procedimiento de notificación interna de incidentes y comunicaciones sospechosas
9.7. Primeras acciones de contención que puede realizar el usuario antes de la intervención del equipo técnico
9.8. Papel del empleado público en la colaboración con los equipos de respuesta a incidentes (CSIRT/CERT)

Temario

10 Respuesta ante incidentes, continuidad del servicio público y cultura organizacional de ciberseguridad

10.1. Fases del ciclo de gestión de incidentes de ciberseguridad en las Administraciones Públicas
10.2. Planes de continuidad del servicio público y recuperación ante desastres
10.3. Comunicación interna y externa durante y después de un incidente de ciberseguridad
10.4. Construcción y mantenimiento de una cultura organizacional de ciberseguridad en la 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

