ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Phishing e Ingeniería Social en la Administración Pública: Detección y Respuesta del Empleado Público

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



Adquiere las herramientas necesarias para proteger la información institucional y convertirte en un elemento clave de la ciberseguridad en tu organización. En ICUFOR ofrecemos este programa especializado dirigido a empleados públicos que desean comprender las amenazas digitales actuales y desarrollar competencias efectivas para detectar y responder ante ataques de phishing e ingeniería social. La Administración Pública gestiona datos de alto valor estratégico, lo que la convierte en objetivo prioritario de ciberdelincuentes cada vez más sofisticados.

A lo largo de la formación abordarás desde los fundamentos de la ciberseguridad y las bases psicológicas de la manipulación, hasta las tipologías específicas de ataques que afectan al sector público: phishing por correo electrónico, spear phishing, vishing, smishing y fraude al CEO.

Duración
150 horas

Créditos
6 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la ciberseguridad en la Administración Pública, identificando las principales ciberamenazas, la superficie de ataque y el papel crítico del factor humano en la protección de la información.

Clasificar las distintas modalidades de phishing según su canal y vector de ataque, reconociendo las técnicas de suplantación, los indicadores técnicos de fraude y la evolución reciente impulsada por la inteligencia artificial.

Conocer el marco normativo y de gobernanza aplicable a la ciberseguridad en el sector público, relacionando las obligaciones derivadas del ENS, la Directiva NIS2 y la normativa de protección de datos con la responsabilidad del empleado público.

Analizar las bases psicológicas y los principios de influencia que sustentan los ataques de ingeniería social, diferenciando sus tipologías y las fases del ciclo de ataque empleado por los ciberdelincuentes.

Identificar los ataques de ingeniería social específicamente dirigidos contra la Administración Pública, examinando casos reales de compromiso de correo corporativo, fraude al CEO y manipulación de procesos administrativos críticos.

Desarrollar la capacidad de detección e identificación de intentos de phishing, vishing, smishing e ingeniería social presencial, aplicando técnicas de análisis crítico de comunicaciones sospechosas en el entorno institucional.

Objetivos del curso

Dominar los protocolos de respuesta y actuación ante incidentes de phishing e ingeniería social, ejecutando procedimientos de notificación, contención de daños, coordinación con equipos CSIRT/CERT y elaboración de informes post-incidente.

Diseñar estrategias de formación, concienciación y mejora continua en ciberseguridad, implementando campañas de simulación de phishing, programas formativos adaptados y planes de acción personalizados para fortalecer la cultura de ciberseguridad en la Administración Pública.

Temario

01 Fundamentos de la ciberseguridad en el contexto de la Administración Pública

1.1. Concepto y alcance de la ciberseguridad en las organizaciones públicas
1.2. El panorama de ciberamenazas contra las administraciones públicas: evolución y situación actual
1.3. Conceptos clave de seguridad de la información: confidencialidad, integridad y disponibilidad
1.4. La superficie de ataque en la Administración Pública: activos, datos y servicios expuestos
1.5. El factor humano como eslabón crítico en la cadena de seguridad de la información

02 Ingeniería social: fundamentos psicológicos, principios de influencia y taxonomía de ataques

2.1. Definición y delimitación conceptual de la ingeniería social en el ámbito de la ciberseguridad
2.2. Bases psicológicas de la manipulación utilizadas en los ataques de ingeniería social
2.3. Taxonomía general de los ataques de ingeniería social
2.4. El ciclo de ataque de ingeniería social: fases y metodología del atacante
2.5. Diferenciación entre ingeniería social genérica y ataques dirigidos a objetivos específicos
2.6. Ingeniería social inversa y ataques de tipo watering hole

Temario

03 Phishing: tipologías, vectores de ataque y evolución de las técnicas

3.1. Definición, origen y evolución histórica del phishing como vector de ataque
3.2. Tipologías de phishing según el canal y el vector de ataque empleado
3.3. Técnicas de suplantación de identidad y falsificación empleadas en campañas de phishing
3.4. Evolución reciente del phishing: ataques potenciados por inteligencia artificial y deepfakes
3.5. Kits de phishing y phishing como servicio (PhaaS): la democratización y escalabilidad del ataque
3.6. Indicadores técnicos comunes presentes en un intento de phishing
3.7. Infraestructura técnica detrás de las campañas de phishing

Temario

04 Ataques de ingeniería social específicamente dirigidos contra la Administración Pública

4.1. Características diferenciales del sector público como objetivo prioritario de ataque
4.2. Ataques de compromiso de correo electrónico corporativo (BEC) en entornos institucionales públicos
4.3. Fraude al CEO y suplantación de altos cargos de la Administración en comunicaciones internas
4.4. Ataques dirigidos a procesos administrativos críticos
4.5. Ataques a la cadena de suministro y a proveedores de servicios tecnológicos de las administraciones
4.6. Casos reales y análisis de incidentes en administraciones públicas españolas y europeas

Temario

05 Marco normativo, regulatorio y de gobernanza de la ciberseguridad aplicable a la Administración Pública

5.1. El Esquema Nacional de Seguridad (ENS) y su aplicación a la protección frente a la ingeniería social
5.2. Normativa europea en materia de ciberseguridad y su transposición al ordenamiento español
5.3. Protección de datos personales y su relación directa con los ataques de ingeniería social
5.4. Responsabilidad jurídica y administrativa del empleado público ante brechas de seguridad causadas por ingeniería social
5.5. Organismos de referencia y marcos de gobernanza de la ciberseguridad en la Administración Pública

Temario

06 Detección e identificación de ataques de phishing e ingeniería social por parte del empleado público

6.1. Desarrollo de la capacidad de análisis crítico ante comunicaciones sospechosas o no solicitadas
6.2. Identificación de señales de alerta en correos electrónicos recibidos en el entorno institucional
6.3. Identificación de ataques de vishing: señales, patrones y técnicas de verificación
6.4. Identificación de ataques de smishing y phishing a través de mensajería
6.5. Detección de intentos de manipulación e ingeniería social en entornos presenciales y de acceso físico
6.6. Identificación de sitios web fraudulentos y portales falsos de captura de credenciales
6.7. Análisis de contexto situacional: factores que incrementan la vulnerabilidad del empleado público
6.8. Errores frecuentes en la detección y falsos negativos: por qué fallan los filtros humanos

Temario

07 Protocolos de respuesta y actuación del empleado público ante incidentes de phishing e ingeniería social

7.1. Principios generales de actuación inmediata ante un ataque sospechado o confirmado
7.2. Canales internos y procedimientos formales de notificación del incidente de seguridad
7.3. Protocolo específico de actuación ante el compromiso de credenciales institucionales
7.4. Protocolo de actuación ante la ejecución inadvertida de malware o archivos adjuntos maliciosos
7.5. Coordinación del empleado público con los equipos de respuesta a incidentes (CSIRT/CERT)
7.6. Gestión de la comunicación interna y externa durante y después del incidente de seguridad
7.7. Análisis post-incidente y elaboración de informes de lecciones aprendidas

Temario

08 Herramientas y tecnologías de protección frente al phishing y la ingeniería social en la Administración

8.1. Soluciones de filtrado, análisis y protección del correo electrónico institucional
8.2. Herramientas de protección del puesto de trabajo del empleado público
8.3. Autenticación multifactor (MFA) y gestión segura de credenciales
8.4. Plataformas de notificación y reporte de phishing accesibles para los usuarios finales
8.5. Soluciones de inteligencia de amenazas aplicadas a la detección temprana de campañas de phishing

Temario

09 Formación, concienciación y construcción de una cultura de ciberseguridad en la Administración Pública

9.1. Fundamentos pedagógicos de los programas de concienciación en ciberseguridad para empleados públicos
9.2. Diseño e implementación de programas de formación continua adaptados a la Administración Pública
9.3. Campañas de simulación de phishing como herramienta de evaluación y refuerzo formativo
9.4. Indicadores de medición del nivel de madurez y de la cultura de ciberseguridad organizacional
9.5. El papel del liderazgo directivo en la promoción y consolidación de la ciberseguridad institucional
9.6. Buenas prácticas internacionales en programas de concienciación en ciberseguridad para el sector público

10 Casos prácticos integradores, simulacros de incidentes y evaluación de la capacidad de respuesta

10.1. Metodología para el diseño y desarrollo de ejercicios prácticos y simulacros de ciberseguridad
10.2. Ejercicios prácticos integradores de detección y respuesta ante ataques de phishing e ingeniería social
10.3. Evaluación de la capacidad de respuesta organizacional e individual del empleado público
10.4. Diseño de un plan de mejora continua y acción personalizada en ciberseguridad

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

