ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Ingeniería Social y Fraudes Digitales: Reconocimiento y Prevención en el Entorno Laboral

4 ECTS | 100 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 Ingeniería Social y Fraudes Digitales: Reconocimiento y Prevención en el Entorno Laboral de ICUFOR. En un contexto donde las amenazas cibernéticas evolucionan constantemente, el factor humano se ha convertido en el principal objetivo de los atacantes. Este programa te preparará para identificar, prevenir y responder eficazmente ante las técnicas de manipulación más sofisticadas que ponen en riesgo la seguridad de cualquier organización.

A lo largo de la formación, profundizarás en los fundamentos psicológicos que explotan los ciberdelincuentes, desde los principios de persuasión hasta los sesgos cognitivos que facilitan el engaño. Dominarás la identificación de ataques como phishing, vishing, fraude BEC y las nuevas amenazas basadas en inteligencia artificial y deepfakes.

Duración
100 horas

Créditos
4 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos conceptuales de la ingeniería social y los fraudes digitales, identificando el factor humano como eslabón crítico en la cadena de seguridad organizacional.

Clasificar las distintas tipologías y técnicas de ataques de ingeniería social, distinguiendo sus vectores, modalidades y grados de sofisticación en entornos corporativos.

Aplicar metodologías de reconocimiento y detección de amenazas, utilizando marcos de referencia, indicadores de compromiso y herramientas de análisis para la identificación temprana de intentos de ataque.

Analizar las bases psicológicas y los mecanismos de manipulación empleados por los atacantes, diferenciando los sesgos cognitivos y principios de persuasión explotados en contextos laborales.

Identificar las modalidades de fraude digital y las tendencias emergentes, describiendo el impacto de tecnologías como los deepfakes y la inteligencia artificial generativa en la sofisticación de los ataques.

Diseñar estrategias de prevención y programas de concienciación en ciberseguridad, implementando políticas corporativas, controles técnicos y acciones formativas orientadas a construir una cultura organizacional resiliente.

Objetivos del curso

Conocer el marco jurídico-normativo aplicable a los delitos de ingeniería social y fraude digital, relacionando la legislación española y europea con las obligaciones y responsabilidades de las organizaciones y sus empleados.

Dominar los protocolos de respuesta ante incidentes y gestión de crisis, elaborando planes de actuación que integren la detección, contención, recuperación, preservación de evidencias y mejora continua del sistema de seguridad organizacional.

Temario

01 Fundamentos conceptuales de la ingeniería social y los fraudes digitales en el contexto organizacional

1.1. Definición y delimitación conceptual de la ingeniería social y los fraudes digitales como vectores de amenaza organizacional
1.2. Evolución histórica de las técnicas de manipulación social en el ámbito digital
1.3. El factor humano como eslabón crítico en la cadena de seguridad organizacional
1.4. Panorama actual de amenazas e impacto económico, reputacional y operativo de los ataques de ingeniería social y fraude digital en las organizaciones

02 Bases psicológicas y mecanismos de manipulación utilizados en los ataques de ingeniería social

2.1. Principios psicológicos de la persuasión y la influencia social aplicados a la ciberdelincuencia
2.2. Sesgos cognitivos explotados por los atacantes en contextos laborales
2.3. Técnicas de construcción de rapport y creación de confianza fraudulenta en interacciones profesionales
2.4. Perfilado de víctimas: recopilación de información y selección estratégica de objetivos
2.5. La dimensión emocional en la toma de decisiones bajo presión y situaciones de engaño
2.6. Diferencias individuales en la susceptibilidad a la manipulación social dentro de las organizaciones

Temario

03 Tipología y técnicas de ataques de ingeniería social en entornos laborales

3.1. Clasificación general de los ataques de ingeniería social según vector, modalidad y grado de sofisticación
3.2. Ataques basados en comunicaciones electrónicas: phishing y sus variantes
3.3. Ataques de compromiso del correo electrónico corporativo (BEC)
3.4. Ataques de ingeniería social presenciales y de proximidad física
3.5. Ataques mediante dispositivos y medios físicos comprometidos
3.6. Ataques de ingeniería social a través de redes sociales y plataformas colaborativas corporativas
3.7. Técnicas combinadas y ataques multicanal de alta sofisticación dirigidos a organizaciones
3.8. Análisis de casos reales de ataques de ingeniería social en organizaciones de diversos sectores

Temario

04 Fraudes digitales: modalidades, vectores de ataque y tendencias emergentes

4.1. Definición, caracterización y diferenciación del fraude digital respecto a la ingeniería social convencional
4.2. Fraudes financieros en línea dirigidos a organizaciones y empleados con responsabilidades económicas
4.3. Suplantación de identidad digital y robo de credenciales corporativas
4.4. Ransomware y extorsión digital como consecuencia de ataques previos de ingeniería social
4.5. Fraudes asociados al comercio electrónico corporativo y la cadena de suministro digital
4.6. Tecnologías emergentes y nuevas superficies de ataque en el fraude digital
4.7. Indicadores de compromiso y señales tempranas de actividad fraudulenta digital en entornos corporativos

Temario

05 Reconocimiento y detección de amenazas de ingeniería social y fraude digital en el entorno laboral

5.1. Metodologías y marcos de referencia para la identificación sistemática de amenazas en organizaciones
5.2. Identificación de señales de alerta en comunicaciones electrónicas sospechosas
5.3. Reconocimiento de intentos de manipulación en interacciones telefónicas y presenciales
5.4. Detección de actividades anómalas en sistemas, redes y cuentas corporativas
5.5. Identificación de riesgos específicos según el rol, departamento y nivel de acceso del empleado
5.6. Ejercicios prácticos de reconocimiento: simulaciones guiadas y análisis de escenarios reales de ataque

Temario

06 Estrategias de prevención, políticas de seguridad y construcción de una cultura organizacional resiliente frente a la ingeniería social

6.1. Diseño e implementación de políticas corporativas de prevención frente a ingeniería social y fraude digital
6.2. Controles técnicos y tecnológicos de protección frente a ataques de ingeniería social
6.3. Programas de concienciación y formación continua en ciberseguridad para empleados de todos los niveles
6.4. Construcción de una cultura organizacional de seguridad basada en la responsabilidad compartida
6.5. Gestión de riesgos de terceros, proveedores y cadena de suministro en relación con la ingeniería social
6.6. Auditorías de seguridad, pruebas de penetración social y evaluaciones de vulnerabilidad humana
6.7. Adaptación de las estrategias preventivas a entornos de trabajo remoto, híbrido y políticas BYOD

Temario

07 Marco jurídico-normativo, respuesta ante incidentes y gestión integral de crisis derivadas de ataques de ingeniería social y fraude digital

7.1. Marco legal aplicable a los delitos de ingeniería social y fraude digital en España y la Unión Europea
7.2. Protocolos de respuesta ante incidentes de ingeniería social y fraude digital
7.3. Preservación de evidencias digitales y colaboración con cuerpos y fuerzas de seguridad del Estado
7.4. Gestión de crisis corporativa derivada de incidentes graves de ingeniería social y fraude digital
7.5. Lecciones aprendidas y retroalimentación para la mejora continua del sistema de seguridad organizacional

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 4 créditos ECTS y 100 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

