ICUFOR
Cursos de Formación Permanente Universitaria

Curso de Formación Permanente

Ciberseguridad para Usuarios: Contraseñas, Phishing, Dispositivos y Navegación Segura

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



Adquiere las herramientas necesarias para protegerte en el entorno digital con nuestro Curso de Formación Permanente en Ciberseguridad para Usuarios. En ICUFOR hemos diseñado esta formación universitaria pensando en quienes desean desenvolverse con seguridad y confianza en su día a día tecnológico, tanto en el ámbito personal como profesional. La creciente sofisticación de las amenazas digitales hace imprescindible que cualquier usuario adquiera competencias sólidas para salvaguardar su información y privacidad.

A lo largo del programa, profundizarás en la gestión segura de contraseñas y sistemas de autenticación multifactor, aprenderás a identificar y prevenir ataques de phishing e ingeniería social, y dominarás las mejores prácticas para proteger tus dispositivos y navegar de forma segura.

Duración
100 horas

Créditos
4 Créditos ECTS

Metodología
Online

Matriculación
Permanente

Objetivos del curso

Comprender los fundamentos de la ciberseguridad y el panorama actual de amenazas, identificando los principales riesgos, actores maliciosos y marcos normativos que afectan al usuario en el entorno digital.

Identificar ataques de phishing e ingeniería social, analizando sus tipologías, técnicas de manipulación psicológica e indicadores de fraude en correos electrónicos, sitios web y canales de mensajería.

Desarrollar hábitos de navegación segura en internet, utilizando configuraciones avanzadas del navegador y prácticas de verificación en transacciones de comercio electrónico, banca en línea y redes sociales.

Diseñar un protocolo de actuación ante incidentes de ciberseguridad, implementando procedimientos de detección temprana, contención del daño, preservación de evidencias y denuncia ante organismos competentes.

Dominar la gestión segura de contraseñas y sistemas de autenticación, aplicando criterios de robustez, gestores de credenciales y mecanismos de autenticación multifactor en servicios habituales.

Aplicar medidas de protección en dispositivos de uso cotidiano, configurando adecuadamente sistemas operativos, herramientas antimalware, cifrado, copias de seguridad y conexiones de red seguras.

Conocer el marco normativo de protección de datos personales, incorporando buenas prácticas de privacidad digital, cifrado de comunicaciones y ejercicio efectivo de los derechos del usuario.

Elaborar un plan personal integral de ciberseguridad, estableciendo rutinas de mantenimiento, evaluación de riesgos individuales y actualización periódica de las medidas preventivas adoptadas.

Temario

01 Fundamentos de la ciberseguridad y panorama actual de amenazas digitales

1.1. Concepto y evolución de la ciberseguridad en la sociedad de la información
1.2. Principales amenazas y riesgos en el entorno digital contemporáneo
1.3. Actores y motivaciones en el ecosistema de la ciberdelincuencia
1.4. Marco normativo y organismos de referencia en materia de ciberseguridad
1.5. La responsabilidad del usuario y la construcción de una cultura de ciberseguridad

Temario

02 Gestión segura de contraseñas y sistemas de autenticación

2.1. El papel de las contraseñas en la protección de la identidad digital
2.2. Características de una contraseña robusta y criterios fundamentales para su creación
2.3. Principales ataques dirigidos contra contraseñas y credenciales de acceso
2.4. Gestores de contraseñas: funcionamiento, selección y configuración práctica
2.5. Autenticación multifactor (MFA) como capa adicional de protección
2.6. Verificación y monitorización de filtraciones de credenciales en bases de datos comprometidas
2.7. Buenas prácticas integrales para la gestión del ciclo de vida de las credenciales

Temario

03 Identificación y prevención del phishing y la ingeniería social

3.1. Concepto, principios psicológicos y evolución de la ingeniería social
3.2. Tipología y clasificación de los ataques de phishing según canal y objetivo
3.3. Técnicas de manipulación y señuelos utilizados en campañas de phishing
3.4. Indicadores y señales para la identificación de mensajes y sitios web fraudulentos
3.5. Pretexting, baiting y otras técnicas de ingeniería social en el entorno físico y digital
3.6. Herramientas tecnológicas de protección frente al phishing
3.7. Protocolo de actuación ante la recepción de un intento de phishing o la caída en un ataque
3.8. Simulacros y entrenamiento práctico para la detección de ataques de ingeniería social

Temario

04 Protección y seguridad de dispositivos en el entorno personal y profesional

4.1. Principios generales de seguridad aplicados a dispositivos de uso cotidiano
4.2. Seguridad en equipos de escritorio y ordenadores portátiles
4.3. Seguridad en dispositivos móviles: smartphones y tabletas
4.4. Seguridad en dispositivos del Internet de las Cosas (IoT) en el hogar y la oficina
4.5. Software malicioso: tipos, vectores de infección y medidas de prevención
4.6. Gestión de actualizaciones y parches de seguridad como medida preventiva esencial
4.7. Seguridad en el uso de redes inalámbricas y conexiones de red

Temario

05 Navegación segura y protección de la privacidad en internet

5.1. Fundamentos del funcionamiento de la navegación web y sus implicaciones de seguridad
5.2. Configuración avanzada de navegadores web para una navegación segura
5.3. Identificación de sitios web seguros y detección de páginas potencialmente fraudulentas
5.4. Seguridad en transacciones de comercio electrónico y banca en línea
5.5. Gestión segura de la identidad y la privacidad en redes sociales
5.6. Motores de búsqueda, rastreo en línea y técnicas para la minimización de la huella digital

06 Protección de datos personales y marco normativo de la privacidad digital

6.1. Concepto de dato personal y marco normativo de protección de datos
6.2. Derechos digitales del usuario: acceso, rectificación, supresión, limitación y portabilidad
6.3. Buenas prácticas y herramientas para la protección activa de la privacidad digital
6.4. Procedimientos de denuncia y reclamación ante organismos de protección de datos

Temario

07 Respuesta ante incidentes de ciberseguridad y construcción de un plan personal de protección digital

7.1. Concepto de incidente de ciberseguridad y tipología de incidentes que afectan al usuario final
7.2. Señales de alerta y detección temprana de posibles incidentes de seguridad
7.3. Protocolo de actuación inmediata ante un incidente de seguridad personal
7.4. Recuperación y restauración de la normalidad operativa tras un incidente de seguridad
7.5. Diseño y elaboración de un plan personal integral de ciberseguridad
7.6. Recursos, organismos y canales de referencia para la formación continua 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 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

