Ciberprotegido: Buenas prácticas para un entorno digital seguro

Detalles del curso:

Duración: 25 horas

Modalidad: Teleformación

Información e inscripción:

685 457 610

615 844 193

960 075 817 (Ext. 257)

formacion@laberit.com

LÄBERIT | CENTRO DE FORMACIÓN TIC.

Ciberprotegido: Buenas prácticas para un entorno digital seguro

Introducción

Este curso ofrece al alumnado tres beneficios fundamentales: mejora de la seguridad personal y profesional frente a amenazas digitales comunes, comprensión clara y accesible de los principales riesgos cibernéticos, y adopción de buenas prácticas para el uso seguro de dispositivos y servicios online. A diferencia de otras formaciones más técnicas o teóricas, esta propuesta pone el foco en la aplicación práctica, el uso de escenarios reales y consejos útiles que cualquier persona puede implementar en su día a día digital.

¿Por qué hacer este curso?

En un contexto de creciente dependencia tecnológica, las amenazas digitales aumentan de forma constante. En este contexto este curso permite mejorar las competencias básicas en materia de seguridad digital, incrementar la empleabilidad y reducir el riesgo de incidentes de seguridad en el entorno profesional y personal. También representa una oportunidad para sentirse más preparado, seguro y autónomo en el uso de tecnología. Inscribirse en esta formación implica obtener herramientas y criterios prácticos para navegar, comunicarse y trabajar con confianza en el entorno digital actual.

¿En qué consiste la formación en Ciberprotegido: Buenas prácticas para un entorno digital seguro?

Esta formación está orientada a proporcionar conocimientos básicos, pero esenciales, sobre los principales riesgos y amenazas en el ámbito digital. A través de una metodología accesible y práctica, se enseñan medidas de protección frente a malware, phishing, amenazas en dispositivos móviles o accesos inseguros, navegación en Internet, uso de la nube y del correo electrónico. Además, se fomenta una cultura preventiva en materia de ciberseguridad y privacidad. No se requieren conocimientos técnicos previos, por lo que cualquier persona con un manejo habitual de la tecnología puede aprovechar este curso.

¿A quién va dirigido?

- Personas usuarias habituales de tecnologías de la información que deseen mejorar su seguridad digital.

- Estudiantes de ciclos formativos o grados no técnicos con interés en competencias digitales básicas.
- Personal administrativo, de atención al público o soporte que trabaja con ordenadores o correo electrónico.
- Cualquier profesional que necesite conocer prácticas de ciberseguridad esenciales en su entorno laboral o doméstico.

Objetivos didácticos

Objetivo general:

- Capacitar a los participantes en la identificación de amenazas digitales comunes y en la adopción de medidas básicas de protección y prevención, fomentando una cultura de ciberseguridad.

Objetivos específicos:

- Comprender los conceptos fundamentales de ciberseguridad.
- Identificar las principales amenazas digitales y sus riesgos asociados.
- Aplicar prácticas seguras en el uso de dispositivos, aplicaciones, navegación e intercambio de información.
- Proteger la información personal y profesional frente a ataques como phishing o ransomware.
- Reconocer situaciones de riesgo y saber cómo actuar frente a incidentes de seguridad.
- Desarrollar buenos hábitos y actitudes responsables en el uso de las TIC.

Metodología

El curso se imparte en modalidad de Teleformación mediante una plataforma online accesible 24/7. Combina contenidos teóricos y prácticos con un enfoque didáctico basado en escenarios reales y resolución de problemas. Además, incluye materiales multimedia, vídeos explicativos y ejercicios autoevaluativos. Cada unidad está acompañada de ejemplos y consejos de aplicación directa. La evaluación final, con preguntas tipo test, permitirá al alumnado comprobar los conocimientos adquiridos durante el curso de forma práctica y sencilla.

Salidas profesionales u opciones de promoción profesional

Al completar esta formación, el alumnado podrá aplicar sus conocimientos de ciberseguridad en cualquier entorno profesional que implique el uso de dispositivos, redes o servicios digitales. Personas que han cursado esta formación han logrado reducir incidentes en sus puestos de trabajo, mejorar sus competencias digitales en procesos de selección y contribuir activamente a la prevención de amenazas en sus organizaciones. Es una base recomendable para perfiles que busquen especializarse posteriormente en ámbitos más técnicos de la ciberseguridad.

Programa

A continuación, se presenta el desglose temático estructurado en siete unidades principales:

Unidad 1. Seguridad general. Introducción a la ciberseguridad

- Aspectos generales de la ciberseguridad
- Incidente de seguridad. INCIBE y OSI
- Malware: medios extraíbles, falsos antivirus, consejos de protección

Unidad 2. Seguridad en Internet

- Navegación segura y peligros comunes
- Seguridad en la nube: compartición, enlaces y accesos
- URLs maliciosas y subdominios engañosos

Unidad 3. Seguridad en el correo electrónico

- Spam, phishing y cadenas
- Descarga de archivos adjuntos peligrosos
- Ransomware desde correos y suplantación de identidad

Unidad 4. Amenazas sobre los datos personales y la privacidad

- Ingeniería social y técnicas de engaño
- Ransomware: funcionamiento y prevención
- Phishing avanzado y robo de información privada

Unidad 5. Seguridad en dispositivos móviles y accesos remotos

- Permisos de aplicaciones, fuentes fiables, códigos QR
- Seguridad en el uso personal de dispositivos y conexiones remotas

Unidad 6. Cultura de ciberseguridad

- Riesgos y reportes en el puesto de trabajo
- Normas para el uso de medios electrónicos en organizaciones
- Buenas prácticas en la creación de contraseñas

Unidad 7. Ciberseguridad e Inteligencia Artificial

- Fundamentos de la IA y su presencia en el entorno digital
- Uso de IA para fraudes: phishing automatizado, clonación de voz, deepfakes, ransomware

LÄBERIT | CENTRO DE FORMACIÓN TIC.

Acreditado:

Microsoft Imagine Academy
Program Member

CertiProf® | Partner

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Networking Academy

Linux Professional Institute

Microsoft
Technology Associate

Pearson VUE
Authorised
Test Centre

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Microsoft
Office Specialist
Authorized Testing Center

LABORA
Servei Valencià d'Ocupació i Formació

Avenida Cataluña, 11, bajo derecha. 46020 -Valencia
960 075 817 (Ext. 257) (Ext. 276) | formacion@laberit.com
formacion.laberit.com