LÃBERIT

Boost your performance

Seguridad de la Información | Seguridad y Peligros en Internet

Detalles del curso:
Duración: 5 horas
Modalidad: Teleformación

Información e inscripción:
685 457 610
615 844 193
960 075 817 (Ext. 274)
formacion@laberit.com

La información contenida en este documento va dirigida exclusivamente al destinatario/grupos de personas y contiene información confidencial. No se puede realizar ninguna revisión, copia, distribución, otro uso, u otra acción basada en ella, sin el permiso explícito por parte del propietario de este documento: Laberit Sistemas S.L. con C.I.F. B98064462.

IÃ Rev. 1

ÍNDICE

1. INTRODUCCIÓN 3
2. ¿POR QUÉ HACER ESTE CURSO? 3
3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | SEGURIDAD Y PELIGROS EN INTERNET? 3
4. ¿A QUIÉN VA DIRIGIDO? 4
5. OBJETIVOS DIDÁCTICOS 4
6. METODOLOGÍA 5
7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL 5
8. PROGRAMA 5
8.1. UNIDAD DE APENDIZAJE 1: SEGURIDAD EN INTERNET Y EN LA NAVEGACIÓN WEB 5
8.2. UNIDAD DE APENDIZAJE 2: SEGURIDAD EN LAS REDES SOCIALES, GROOMING, FAKE NEWS, Y COMPRAS SEGURAS 6

1. INTRODUCCIÓN

Internet forma parte de la actividad diaria de cualquier persona y organización: permite comunicarse, trabajar, almacenar información, comprar, aprender y relacionarse. Esta formación ayuda a reconocer los riesgos más habituales del entorno digital, adoptar buenas prácticas de prevención y proteger mejor la información personal y profesional cada vez que se navega, se usa el correo electrónico, se trabaja en la nube, se participa en redes sociales o se realizan compras online.

A diferencia de otras acciones más genéricas, el curso aborda la seguridad desde situaciones cercanas y fáciles de identificar, con escenarios sobre navegación web, enlaces maliciosos, uso de la nube, correo electrónico, redes sociales, grooming, fake news y comercio online. Su enfoque es breve, práctico y orientado a la concienciación, para que el alumnado pueda aplicar desde el primer momento pautas sencillas, realistas y eficaces en su vida digital.

2. ¿POR QUÉ HACER ESTE CURSO?

La seguridad en Internet se ha convertido en una competencia transversal para trabajar, estudiar, comunicarse y realizar gestiones online con mayor confianza. Realizar este curso permite mejorar la autonomía digital, reducir errores cotidianos, prevenir incidentes que pueden afectar a datos, dispositivos o reputación, y reforzar el perfil profesional en entornos donde el uso seguro de herramientas digitales es cada vez más necesario. Además, ayuda a desarrollar una actitud preventiva, responsable y crítica ante amenazas frecuentes, lo que aporta tranquilidad y capacidad de respuesta ante situaciones de riesgo.

3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | SEGURIDAD Y PELIGROS EN INTERNET?

La formación en Seguridad y Peligros en Internet consiste en aprender a identificar amenazas comunes y a actuar de forma segura ante ellas. El curso explica, con un lenguaje claro y accesible, cómo proteger la navegación web, reconocer direcciones maliciosas, usar la nube con precaución, detectar correos sospechosos, gestionar la exposición en redes sociales, comprender riesgos como el grooming, contrastar la información frente a las fake news y comprar online de forma más segura.

El objetivo es que el alumnado incorpore hábitos digitales más seguros y sepa tomar decisiones prudentes antes de hacer clic, compartir información, abrir archivos, aceptar contactos, introducir credenciales o confiar en contenidos que circulan por Internet.

4. ¿A QUIÉN VA DIRIGIDO?

Esta formación está dirigida a cualquier persona que utilice Internet de forma habitual y quiera proteger mejor su entorno digital, su información privada y sus dispositivos.

- Personas usuarias de Internet que desean adquirir hábitos básicos de ciberseguridad.
- Profesionales que trabajan con correo electrónico, herramientas en la nube, plataformas digitales o redes sociales.
- Personal administrativo, comercial, docente, técnico o de atención al cliente que gestiona información online.
- Familias, educadores/as y personas interesadas en conocer riesgos asociados al uso de Internet por parte de menores.
- Cualquier perfil que quiera navegar, comunicarse, comprar y compartir información con más seguridad.

5. OBJETIVOS DIDÁCTICOS

Objetivo general:

- Adquirir hábitos de uso seguro de Internet para reconocer riesgos habituales, prevenir incidentes y proteger la información personal y profesional en entornos digitales.

Objetivos específicos:

- Identificar los principales riesgos asociados a la navegación web y aplicar pautas básicas de protección.
- Reconocer amenazas relacionadas con el uso de servicios en la nube y la compartición de archivos.
- Detectar direcciones de Internet maliciosas, enlaces engañosos y sitios web no seguros.
- Aplicar buenas prácticas en el uso del correo electrónico para reducir la exposición a fraudes, SPAM y archivos maliciosos.
- Comprender los riesgos de las redes sociales y adoptar medidas para proteger la privacidad y la reputación digital.
- Identificar situaciones de grooming y conocer pautas preventivas y de actuación ante este riesgo.
- Reconocer fake news y aplicar criterios básicos para contrastar información antes de compartirla.

- Realizar compras online con mayor seguridad, especialmente en tiendas digitales, marketplaces y redes sociales.

6. METODOLOGÍA

La metodología combina exposición didáctica, ejemplos prácticos y escenarios de riesgo frecuentes para facilitar la comprensión de los contenidos. El aprendizaje se organiza de forma secuencial, permitiendo avanzar desde conceptos básicos hasta situaciones concretas de prevención y respuesta.

El curso favorece la participación activa del alumnado mediante preguntas, ejercicios de análisis, ejemplos y contraejemplos orientados a la toma de decisiones. La formación se desarrolla sobre una plataforma de teleformación e incluye guía del alumno, unidades didácticas estructuradas, navegación secuencial en la primera realización del curso y acceso posterior en modo consulta una vez revisados los contenidos.

7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL

Aunque se trata de una formación de concienciación y competencias digitales, su utilidad es transversal en múltiples puestos y sectores. Completar este curso puede mejorar la solvencia profesional de quienes trabajan con información digital, correo electrónico, documentación en la nube, atención a clientes, comercio online o comunicación en redes sociales.

También puede servir como complemento para perfiles que desean reforzar su empleabilidad o promoción en áreas administrativas, educativas, comerciales, de soporte, gestión documental, atención al usuario o cualquier función que requiera un uso responsable y seguro de Internet.

8. PROGRAMA

8.1. UNIDAD DE APENDIZAJE 1: SEGURIDAD EN INTERNET Y EN LA NAVEGACIÓN WEB

Capítulo 1. Seguridad en la navegación web

- Tema 1.1.: Introducción. Importancia de la navegación segura.
- Tema 1.2.: Escenario 1: Complementos y extensiones maliciosos.
- Tema 1.3.: Escenario 2: Instalación de aplicaciones maliciosas.
- Tema 1.4.: Escenario 3: Enlaces, botones y ventanas emergentes peligrosos.

- Tema 1.5.: Conclusiones.

Capítulo 2. Seguridad en la nube

- Tema 2.1.: Introducción. Ventajas de usar un servicio en la nube.
- Tema 2.2.: Escenario 1: Compartir carpetas de forma insegura.
- Tema 2.3.: Escenario 2: Notificaciones y enlaces inseguros de acceso a la nube.
- Tema 2.4.: Escenario 3: Cifrar nuestros archivos para prevenir riesgos.
- Tema 2.5.: Prevenir el acceso no autorizado a nuestros archivos. Conclusión.

Capítulo 3. Direcciones de Internet maliciosas

- Tema 3.1.: Introducción. Las URLs.
- Tema 3.2.: Escenario 1: Sitios Web que no son seguros.
- Tema 3.3.: Escenario 2: URLs similares.
- Tema 3.4.: Escenario 3: URLs engañosas. Subdominios.
- Tema 3.5.: Conclusiones.

Capítulo 4. Internet y correo electrónico

- Tema 4.1.: Introducción. Conceptos básicos.
- Tema 4.2.: Escenario 1: Petición de datos personales en sitios web.
- Tema 4.3.: Escenario 2: Descarga de archivos maliciosos.
- Tema 4.4.: Escenario 3: Recepción de correos basura (SPAM).
- Tema 4.5.: Conclusiones.

8.2. UNIDAD DE APENDIZAJE 2: SEGURIDAD EN LAS REDES SOCIALES, GROOMING, FAKE NEWS, Y COMPRAS SEGURAS

Capítulo 1. Redes sociales seguras

- Tema 1.1.: Introducción: Datos sensibles y privados.
- Tema 1.2.: Escenario 1: Peligro de compartir información y fotos personales.

- Tema 1.3.: Escenario 2: Peligro de aceptar solicitudes de amistad de desconocidos.
- Tema 1.4.: Escenario 3: Tener cuidado con las opiniones vertidas en las redes sociales
- Tema 1.5.: Conclusiones.

Capítulo 2. Grooming: Abuso sexual a través de Internet

- Tema 2.1.: Introducción: Qué es y objetivos del grooming.
- Tema 2.2.: Escenario 1: Juegos en línea con menores.
- Tema 2.3.: Escenario 2: Amigos en línea.
- Tema 2.4.: Escenario 3: Conocidos cercanos.
- Tema 2.5.: Cómo debemos actuar. Conclusión.

Capítulo 3. Fake News

- Tema 3.1.: Introducción. Noticias falsas y engaños deliberados.
- Tema 3.2.: Escenario 1: Estafas económicas.
- Tema 3.3.: Escenario 2: Comentarios falsos y difamatorios.
- Tema 3.4.: Escenario 3: Tratamientos y curas milagrosas.
- Tema 3.5.: Conclusiones.

Capítulo 4. Compras seguras en tiendas online y redes sociales

- Tema 4.1.: Introducción. E-commerce y Marketplace.
- Tema 4.2.: Escenario 1: Una publicidad demasiado atractiva.
- Tema 4.3.: Escenario 2: Una App engañosa y maliciosa.
- Tema 4.4.: Escenario 3: Peligro de insertar nuestras credenciales en sitios web maliciosos.
- Tema 4.5.: Reducir las publicidades en nuestras redes sociales. Conclusiones.

ACREDITADO

Microsoft Imagine Academy
Program Member

CertiProf® | Partner

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Networking Academy
cisco

Linux Professional Institute

Microsoft
Technology Associate

Pearson
Professional Assessments

CERTIPORT
A PEARSON VUE BUSINESS
AUTHORIZED TESTING CENTER

Microsoft
Office Specialist
Authorized Testing Center

LABORA
Servei Valencià d'Ocupació i Formació

IC3
DIGITAL LITERACY
CERTIFICATION