LÃBERIT

Boost your performance

Seguridad de la Información | Buenas prácticas para la protección de tus equipos informáticos y dispositivos móviles

Detalles del curso:
Duración: 6 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 | BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE TUS EQUIPOS INFORMÁTICOS Y DISPOSITIVOS MÓVILES? 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: BUENAS PRÁCTICAS EN LA SEGURIDAD DE LA INFORMACIÓN 5
8.2. UNIDAD DE APENDIZAJE 2: RIESGOS Y BUENAS PRÁCTICAS EN EL USO DE TUS EQUIPOS Y DISPOSITIVOS 7

1. INTRODUCCIÓN

La seguridad de la información es una competencia esencial para trabajar con solvencia en entornos digitales. Este curso permite reconocer las amenazas más habituales, adoptar hábitos de protección en equipos informáticos y dispositivos móviles, y actuar correctamente ante incidentes para reducir riesgos personales y corporativos.

La propuesta se diferencia de otras formaciones breves porque combina concienciación, ejemplos cotidianos y pautas aplicables desde el primer día. A lo largo de la formación, el alumnado refuerza el uso seguro de contraseñas, copias de seguridad, dispositivos extraíbles, aplicaciones móviles y recursos digitales, con un enfoque práctico orientado a prevenir errores frecuentes y a proteger la información en el puesto de trabajo y en movilidad.

2. ¿POR QUÉ HACER ESTE CURSO?

Trabajar con ordenadores, móviles, documentos, correo electrónico y servicios en la nube exige saber identificar riesgos y tomar decisiones seguras. Esta formación ayuda a mejorar la autonomía digital, reducir comportamientos inseguros y reforzar la confianza profesional ante situaciones como correos sospechosos, pérdida de dispositivos, uso de software no autorizado o gestión de información sensible. Inscribirse en el curso supone adquirir criterios claros para proteger los equipos, cuidar los datos propios y de la organización, y responder con mayor seguridad ante amenazas habituales.

3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE TUS EQUIPOS INFORMÁTICOS Y DISPOSITIVOS MÓVILES?

La formación se centra en el uso seguro de equipos informáticos y dispositivos móviles desde una perspectiva sencilla, práctica y cercana. El alumnado aprende a reconocer distintos tipos de malware, crear y usar contraseñas de forma responsable, respetar derechos de autor y propiedad intelectual, realizar copias de seguridad, cuidar el puesto de trabajo, manejar dispositivos de almacenamiento extraíbles y aplicar buenas prácticas en teletrabajo y aplicaciones móviles.

El objetivo es que cualquier persona que utilice tecnología en su actividad diaria pueda incorporar hábitos de prevención, detectar señales de alerta y saber cuándo y cómo comunicar un posible incidente de seguridad.

4. ¿A QUIÉN VA DIRIGIDO?

Esta formación está dirigida a personas que utilizan equipos informáticos, dispositivos móviles o información digital en su entorno laboral o personal y desean mejorar su nivel de protección.

- Profesionales de cualquier área que trabajan con equipos corporativos, correo electrónico, documentación o herramientas digitales.
- Personas usuarias de dispositivos móviles, portátiles, tablets o soportes de almacenamiento extraíbles.
- Personal que desarrolla parte de su actividad en modalidad de teletrabajo o en movilidad.
- Equipos administrativos, técnicos, comerciales o de atención al cliente que manejan información sensible o documentación interna.
- Cualquier persona interesada en reforzar sus hábitos de ciberseguridad y protección de datos en el uso cotidiano de la tecnología.

5. OBJETIVOS DIDÁCTICOS

Objetivo general:

- Adquirir hábitos seguros para proteger equipos informáticos, dispositivos móviles e información digital frente a riesgos habituales de seguridad.

Objetivos específicos:

- Identificar los riesgos relacionados con virus, malware, troyanos y ransomware.
- Aplicar buenas prácticas en la creación, custodia y uso de contraseñas.
- Reconocer situaciones que puedan afectar a los derechos de autor y a la propiedad intelectual.
- Comprender la importancia de las copias de seguridad y del respaldo de la información.
- Detectar riesgos asociados al uso de equipos informáticos, periféricos y puestos de trabajo.
- Utilizar dispositivos de almacenamiento extraíbles de forma prudente y segura.
- Aplicar pautas de protección en dispositivos móviles, portátiles y entornos de teletrabajo.
- Valorar los riesgos derivados de aplicaciones móviles, permisos y códigos QR.

- Conocer criterios básicos para notificar incidentes de seguridad y minimizar su impacto.

6. METODOLOGÍA

La formación se desarrolla en modalidad de teleformación y combina exposición guiada de contenidos con situaciones prácticas, preguntas de comprobación y ejemplos orientados al uso cotidiano de la tecnología. El alumnado avanza de forma secuencial por los contenidos y consolida lo aprendido mediante ejercicios vinculados a escenarios reales de seguridad.

El curso se apoya en recursos didácticos disponibles en la plataforma de teleformación, entre ellos la guía del alumno y las unidades didácticas estructuradas en capítulos, temas, páginas y ejercicios. Una vez completados los contenidos, el alumnado puede volver a consultarlos libremente como material de referencia.

7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL

Aunque se trata de una formación transversal de concienciación y buenas prácticas, completar el curso puede reforzar el desempeño en cualquier puesto que implique uso de información, herramientas digitales, equipos corporativos o dispositivos móviles. También aporta valor en procesos de incorporación, reciclaje profesional, cumplimiento interno y mejora de competencias digitales.

La capacitación resulta especialmente útil para profesionales que desean asumir con mayor solvencia responsabilidades relacionadas con la gestión segura de la información, el trabajo remoto, la atención a clientes, la administración documental o el uso responsable de recursos tecnológicos.

8. PROGRAMA

8.1. UNIDAD DE APENDIZAJE 1: BUENAS PRÁCTICAS EN LA SEGURIDAD DE LA INFORMACIÓN

Capítulo 1. Virus

- Tema 1.1.: Introducción a los virus.
- Tema 1.2.: Escenario 1: Descarga de programas falsos de Internet.
- Tema 1.3.: Escenario 2: Mensaje de correo con archivo adjunto malicioso.
- Tema 1.4.: Escenario 3: Propagación de software malicioso a través de un dispositivo externo infectado.

- Tema 1.5.: Conclusión.

Capítulo 2. Contraseñas

- Tema 2.1.: Introducción a las contraseñas.
- Tema 2.2.: Escenario 1: Contraseñas compartidas.
- Tema 2.3.: Escenario 2: Dejar la sesión abierta en tu equipo.
- Tema 2.4.: Escenario 3: Accesos no autorizados a nuestro equipo y documentación.
- Tema 2.5.: Conclusiones.

Capítulo 3. Derechos de autor y propiedad intelectual

- Tema 3.1.: Introducción. Material protegido y políticas de seguridad
- Tema 3.2.: Escenario 1: Instalación de software crakeado.
- Tema 3.3.: Escenario 2: Instalación de software gratuito.
- Tema 3.4.: Escenario 3: Reenvío de documentación protegida.
- Tema 3.5.: Conclusión.

Capítulo 4. Copias de seguridad de la información

- Tema 4.1.: Introducción. Respaldo de la información.
- Tema 4.2.: Escenario 1: Enlaces maliciosos y suplantación de identidad.
- Tema 4.3.: Escenario 2: Daños irreparables en nuestros equipos.
- Tema 4.4.: Escenario 3: Pérdidas irreparables de nuestros dispositivos y otros incidentes
- Tema 4.5.: Conclusiones.

Capítulo 5. Reporte de incidentes de seguridad de la información

- Tema 5.1.: Introducción. Incidentes más comunes.
- Tema 5.2.: Escenario 1: Mensajes de correo sospechosos. Robo de información confidencial

- Tema 5.3.: Escenario 2: Ciberataques. Gestión de incidentes.
- Tema 5.4.: Escenario 3: Procedimientos contra los incidentes en nuestros dispositivos.
- Tema 5.5.: Reportar incidentes. Conclusión.

8.2. UNIDAD DE APENDIZAJE 2: RIESGOS Y BUENAS PRÁCTICAS EN EL USO DE TUS EQUIPOS Y DISPOSITIVOS

Capítulo 1. Equipos informáticos y periféricos

- Tema 1.1.: Introducción a los equipos informáticos y periféricos.
- Tema 1.2.: Escenario 1: Instalación de nuevos programas.
- Tema 1.3.: Escenario 2: Difusión de archivos comprometedores.
- Tema 1.4.: Escenario 3: Descuidos que cuestan caro.
- Tema 1.5.: Escenario 4: Configuraciones en nuestro equipo no autorizadas.
- Tema 1.6.: Escenario 5: Acceso sin autorización al equipo de otra persona.
- Tema 1.7.: Escenario 6: Utilización de dispositivos de almacenamiento externo.
- Tema 1.8.: Escenario 7: Utilizar aplicaciones sin autorización.
- Tema 1.9.: Conclusión.

Capítulo 2. Riesgos en el puesto de trabajo

- Tema 2.1.: Introducción. Cuidemos la información.
- Tema 2.2.: Escenario 1: Siempre cerremos la puerta y la sesión.
- Tema 2.3.: Escenario 2: Cuidado con el uso de medios de almacenamiento extraíbles.
- Tema 2.4.: Escenario 3: Nuestras contraseñas son nuestra responsabilidad.
- Tema 2.5.: Conclusión.

Capítulo 3. Riesgos en el uso de dispositivos de almacenamiento extraíbles

- Tema 3.1.: Introducción a los riesgos en el uso de dispositivos de almacenamiento extraíbles.
- Tema 3.2.: Escenario 1: Cuidado con conectar medios extraíbles desconocidos.

- Tema 3.3.: Escenario 2: Cuidado con los descuidos y negligencias.
- Tema 3.4.: Escenario 3: Cuidado con el borrado no seguro de datos.
- Tema 3.5.: Conclusiones.

Capítulo 4. Equipos y dispositivos móviles en el teletrabajo

- Tema 4.1.: Introducción a los equipos y dispositivos móviles en el teletrabajo.
- Tema 4.2.: Escenario 1: Uso del portátil en las reuniones con clientes.
- Tema 4.3.: Escenario 2: Uso del portátil en el domicilio particular.
- Tema 4.4.: Escenario 3: Uso de dispositivos móviles en viajes y traslados.
- Tema 4.5.: Conclusiones.

Capítulo 5. Uso seguro de aplicaciones móviles

- Tema 5.1.: Introducción. Las Apps.
- Tema 5.2.: Escenario 1: Cuidado con la concesión de permisos. SMS Premium
- Tema 5.3.: Escenario 2: Cuidado con la instalación de apps gratuitas y/o no oficiales.
- Tema 5.4.: Escenario 3: Cuidado con el escaneo de códigos QR.
- Tema 5.5.: Conclusión.

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