LÃBERIT

Boost your performance

Seguridad de la Información | Teletrabajo y Ciberseguridad

Detalles del curso:
Duración: 2 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.

ÍNDICE

1. INTRODUCCIÓN 3
2. ¿POR QUÉ HACER ESTE CURSO? 3
3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | TELETRABAJO Y CIBERSEGURIDAD? 3
4. ¿A QUIÉN VA DIRIGIDO? 4
5. OBJETIVOS DIDÁCTICOS 4
6. METODOLOGÍA 4
7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL 5
8. PROGRAMA 5
8.1. Capítulo 1. Teletrabajo: lejos de la oficina, cerca de la información 5
8.2. Capítulo 2. Dispositivos móviles y teletrabajo 5
8.3. Capítulo 3. Consejos para mejorar la ciberseguridad en el teletrabajo 6

1. INTRODUCCIÓN

La formación en Seguridad de la Información | Teletrabajo y Ciberseguridad proporciona una visión clara y práctica para teletrabajar con mayor seguridad, proteger la información corporativa y personal, y reconocer los riesgos más habituales asociados al uso de ordenadores, portátiles y dispositivos móviles. En poco tiempo, el alumnado adquirirá pautas aplicables desde el primer día para reducir la exposición a ciberataques, mejorar sus hábitos digitales y actuar con más criterio ante situaciones de riesgo.

Frente a otras acciones formativas más generales, este curso destaca por su enfoque directo, su orientación a escenarios cotidianos de teletrabajo y su lenguaje accesible. La formación no se limita a explicar conceptos: conecta ventajas, amenazas y recomendaciones de seguridad con situaciones reales como el uso de redes poco fiables, el intercambio de archivos o la protección de dispositivos fuera de la oficina.

2. ¿POR QUÉ HACER ESTE CURSO?

El teletrabajo forma parte de la actividad profesional diaria en muchas organizaciones, pero también exige una mayor responsabilidad en la protección de la información. Saber identificar prácticas inseguras, anticiparse a amenazas y aplicar medidas básicas de ciberseguridad permite trabajar con más confianza, reforzar el perfil profesional y contribuir a entornos digitales más seguros. Esta formación ayuda al alumnado a sentirse más preparado, a reducir errores habituales y a incorporar hábitos de seguridad que mejoran tanto su desempeño individual como la protección de la empresa.

3. ¿EN QUÉ CONSISTE LA FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN | TELETRABAJO Y CIBERSEGURIDAD?

La formación consiste en un recorrido breve y práctico por los principales aspectos de seguridad que deben tenerse en cuenta al trabajar fuera de la oficina. El alumnado aprenderá qué implica teletrabajar de forma segura, qué riesgos aparecen al utilizar dispositivos móviles y qué buenas prácticas permiten proteger la información cuando se accede a recursos corporativos, se comparten archivos o se trabaja desde conexiones no siempre fiables.

El curso está planteado para que cualquier persona usuaria de tecnología en su entorno laboral pueda comprender los riesgos sin necesidad de conocimientos técnicos avanzados y pueda adoptar medidas sencillas, realistas y eficaces para mejorar su seguridad digital.

4. ¿A QUIÉN VA DIRIGIDO?

Esta formación está dirigida a personas que teletrabajan o utilizan habitualmente equipos informáticos y dispositivos móviles en su actividad profesional o personal, especialmente a quienes desean proteger mejor su entorno digital y la información que gestionan.

- Profesionales que trabajan en remoto o en modalidad híbrida.
- Usuarios/as de ordenadores, portátiles, smartphones o tablets en entornos laborales.
- Personas que acceden a recursos corporativos, correo electrónico, archivos compartidos o plataformas de empresa desde fuera de la oficina.
- Equipos de organizaciones que necesitan reforzar hábitos básicos de seguridad de la información.
- Cualquier persona interesada en mejorar su protección digital durante el teletrabajo.

5. OBJETIVOS DIDÁCTICOS

Objetivo general:

- Adquirir hábitos y criterios básicos de seguridad para teletrabajar protegiendo los equipos, los dispositivos móviles y la información corporativa y personal.

Objetivos específicos:

- Conocer las características, ventajas y riesgos del teletrabajo.
- Identificar amenazas habituales asociadas al uso de dispositivos móviles y equipos informáticos fuera de la oficina.
- Reconocer situaciones de riesgo vinculadas a conexiones no seguras, enlaces compartidos y archivos enviados por medios inseguros.
- Aplicar recomendaciones básicas para mejorar la ciberseguridad durante el teletrabajo.
- Concienciar sobre la responsabilidad individual en la protección de la información y los recursos corporativos.

6. METODOLOGÍA

La metodología combina una exposición clara y secuencial de los contenidos con el análisis de situaciones prácticas relacionadas con el teletrabajo y la ciberseguridad. El curso se apoya en escenarios habituales, preguntas de refuerzo y ejemplos que facilitan

la comprensión progresiva de los riesgos y de las medidas de protección más adecuadas.

La formación se desarrolla en modalidad de teleformación a través de una plataforma online, con recursos didácticos como guía del alumno, unidades de aprendizaje, ejercicios prácticos y navegación secuencial en la primera revisión de contenidos. Una vez completadas las unidades, el alumnado podrá consultar nuevamente los materiales de forma libre.

7. SALIDAS PROFESIONALES U OPCIONES DE PROMOCIÓN PROFESIONAL

Completar esta formación contribuye a reforzar competencias transversales cada vez más valoradas en entornos digitales, especialmente en puestos que requieren teletrabajo, movilidad, manejo de información corporativa o uso habitual de herramientas conectadas. También puede apoyar la promoción profesional en organizaciones que priorizan la seguridad de la información, la protección de datos y la autonomía responsable en el trabajo remoto.

Además, esta capacitación ayuda a consolidar un perfil profesional más consciente, preventivo y fiable en el uso de tecnologías, lo que resulta útil para equipos administrativos, técnicos, comerciales, de soporte, gestión o cualquier área que trabaje con información sensible fuera del entorno físico de la oficina.

8. PROGRAMA

8.1. Capítulo 1. Teletrabajo: lejos de la oficina, cerca de la información

- Tema 1.1.: Introducción.
- Tema 1.2.: Escenario 1: Uso personal del ordenador de empresa.
- Tema 1.3.: Escenario 2: Protección de la información.
- Tema 1.4.: Escenario 3: Conexiones poco fiables.
- Tema 1.5.: Conclusiones finales.

8.2. Capítulo 2. Dispositivos móviles y teletrabajo

- Tema 2.1.: Introducción.
- Tema 2.2.: Escenario 1: Uso del portátil en las reuniones con clientes.
- Tema 2.3.: Escenario 2: Uso del portátil en el domicilio particular.
- Tema 2.4.: Escenario 3: Uso de dispositivos móviles en viajes y traslados.

- Tema 2.5.: Conclusiones finales.

8.3. Capítulo 3. Consejos para mejorar la ciberseguridad en el teletrabajo

- Tema 3.1.: Introducción.
- Tema 3.2.: Escenario 1: Conexiones no seguras.
- Tema 3.3.: Escenario 2: Enlaces compartidos con demasiadas personas.
- Tema 3.4.: Escenario 3: Archivos compartidos utilizando medios inseguros.
- Tema 3.5.: Conclusiones finales.

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