Seguridad de la Información | **Confidencialidad, seguridad física y protección de datos personales (RGPD)**

Detalles del curso:

Duración: 3 h.

Modalidad: Teleformación

Información e inscripción:

685 457 610 - 615 844 193

formacion@laberit.com

LÃBERIT | CENTRO DE FORMACIÓN TIC.

Introducción

La confidencialidad es la garantía de que la información de la organización será protegida para que no sea divulgada sin su consentimiento. Dentro de la organización, cada uno de nosotros debe manejar la información en forma correcta para garantizar que el acceso a la misma sólo sea posible por las personas que están autorizadas.

Un acuerdo de confidencialidad es el mecanismo mediante el cual se regulan los aspectos relativos a la confidencialidad de la información sensible que manejamos en nuestra actividad diaria dentro de nuestra organización. Siempre existe el riesgo de que se produzca una fuga de información, por esta razón es fundamental conocer y cumplir estos acuerdos que tienen el objetivo de garantizar la protección de la información confidencial.

En la actualidad, las compras con tarjetas de crédito o débito son cada vez más frecuentes. Como individuos tenemos derecho a que otras personas y organizaciones hagan un uso adecuado de los datos de nuestras tarjetas. Al mismo tiempo, si en nuestra actividad laboral manipulamos información de tarjetas de terceros, es nuestra responsabilidad hacerlo de manera segura.

Existe un estándar de Seguridad de Datos para la Industria de Pagos con Tarjeta (PCI DSS por sus siglas en inglés), el cual debe ser cumplido rigurosamente por las organizaciones que procesan, almacenan y/o transmiten datos de titulares de tarjetas. El estándar establece un conjunto de normas mínimas de seguridad, para proteger la información en las ventas o compras con tarjeta.

En la antigüedad se buscaba proteger los bienes más tangibles. Hoy en día se busca además resguardar uno de los activos más preciados que tenemos, nuestra información, intangible pero igualmente importante. La seguridad física se define como la aplicación de barreras físicas y procedimientos de control como medidas de prevención y resguardo de los recursos y de la información confidencial ante todo tipo de amenazas.

Debemos ser conscientes del derecho que tenemos como individuos de que otras personas y organizaciones hagan un uso adecuado de nuestros datos personales. *El derecho a la protección de datos personales faculta a los interesados para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento.* Pero también debemos garantizar la protección de los datos personales de terceros y que utilizamos a diario en nuestro trabajo: datos de clientes, proveedores, trabajadores, etc.

¿Por qué hacer este curso?

Para empezar, es un curso divertido y se hace fácil; conocerás los principales riesgos y buenas prácticas relacionados con la confidencialidad de los datos de la organización, así como la protección de datos personales.

Una de las mayores preocupaciones hoy en día si trabajas en entornos digitales e informáticos es estar prevenido ante los constantes peligros a los que te enfrentas cuando no protegemos la confidencialidad de los datos de nuestra organización los datos personales.

¿Para qué sirve la formación en Confidencialidad, seguridad física y protección de datos personales?

Con este curso conocerás los riesgos y peligros que podemos encontrarnos si no se cumplen una serie de normas en el uso de datos confidenciales de nuestra organización y de nuestros propios datos personales. En este curso no sólo conocerás todos estos riesgos, sino que aprenderás a evitarlos utilizando una serie de normas y buenas prácticas.

En definitiva, el objetivo de este curso es facilitar la adopción de nuevos hábitos de seguridad, concienciar de la responsabilidad de cada persona al utilizar datos confidenciales de la organización y conocer nuestros derechos en relación con los datos personales.

El conocimiento que aporta es un valor añadido que, sin duda, se convierte en una ventaja competitiva definitiva.

¿A quién va dirigido?

Este curso está dirigido a todas aquellas personas que usan equipos informáticos y dispositivos móviles de empresa o particulares y quieran aprender a proteger de la mejor forma posible su entorno digital e información privada.

De esta forma, cualquier persona habituada al uso de medios informáticos y digitales en su entorno laboral o personal puede sacar provecho de esta formación.

Objetivos didácticos

Los principales objetivos didácticos de esta acción formativa son:

- Conocer los aspectos más importantes relacionados con la confidencialidad de los datos dentro de una organización.
- Conocer los aspectos más importantes relacionados con los acuerdos de confidencialidad en una organización.
- Conocer los estándares y riesgos de seguridad de datos confidenciales para pagos con tarjeta.
- Conocer las buenas prácticas en relación con las copias de seguridad de la información.
- Conocer los riesgos y buenas prácticas relacionados con la seguridad física para el resguardo de la información confidencial.
- Conocer el derecho a la protección de datos personales propios y de terceros, las medidas básicas de seguridad de la información, cómo se producen las brechas/incidentes de seguridad y la fuga de información, y los peligros de la ingeniería social.

Metodología

Se van a aplicar varias metodologías didácticas.

- **Deductiva**. Se expone la teoría de tal forma que el alumno va accediendo a los contenidos de manera secuencial, de menor a mayor importancia, complejidad, etc.
- **Inductiva**. Se plantean preguntas a modo de ejercicios para explicar la teoría. El alumno aprende sobre la acción que va realizando, con ejemplos y contraejemplos, y de las consecuencias de dicha práctica (negativa y positiva).

La idea es generar actividad entre las alumnas y los alumnos, haciendo que se sientan involucrados en el proceso de aprendizaje.

El curso está desarrollado siguiendo los estándares técnicos y funcionales que tiene la plataforma de Teleformación Moodle de Lãberit.

Una vez se accede al curso, podrás acceder a los siguientes recursos didácticos:

- **Guía del alumno**

  Se trata de una guía donde se exponen los objetivos, contenidos, organización e instrucciones de manejo del curso.

- **Unidad didáctica**

  Son los contenidos propiamente dichos del curso. Están estructurados en Capítulos y/o Temas y éstos, a su vez, en páginas y ejercicios prácticos relacionados con el contenido aprendido. Para la navegación por la unidad de aprendizaje dispondrás de una serie de botones tanto en el margen superior como inferior de la pantalla.

A través del curso, podrás trabajar de dos maneras:

- **FORMACIÓN:** El curso tiene una navegación **secuencial** si es la primera vez que accedes a él; es decir, es obligatorio ver los contenidos de cada página en el orden que se muestran en el índice de contenidos y dentro de cada tema. Además, será obligatorio realizar las acciones que se piden en cada página.

- **CONSULTA:** Una vez hayas visto todo el contenido de una página, tema o el curso completo, la navegación por esa página, tema o curso quedará abierta y ya podrás navegar libremente por sus contenidos, sin necesidad de volver a verlos de forma secuencial.

Programa

El curso “Confidencialidad, seguridad física y protección de datos personales (RGPD)” consta de cinco capítulos. Los títulos y contenidos son los siguientes:

Capítulo 1. Confidencialidad

Tema 1.1.: Introducción a la confidencialidad.
Tema 1.2.: Escenario 1: Compartir datos de la empresa.
Tema 1.3.: Escenario 2: Llevar trabajo a casa.
Tema 1.4.: Escenario 3: Uso de datos confidenciales de la empresa para fines particulares.
Tema 1.5.: Escenario 4: Devolución de información confidencial.
Tema 1.6.: Conclusión.

Capítulo 2. Acuerdos de confidencialidad

Tema 2.1.: Introducción a los acuerdos de confidencialidad.
Tema 2.2.: Escenario 1: Documentación confidencial al descubierto. Fuga de información.
Tema 2.3.: Escenario 2: Facilitar información confidencial. Acuerdos de confidencialidad.
Tema 2.4.: Escenario 3: Destrucción incorrecta de información confidencial.
Tema 2.5.: Conclusiones.

Capítulo 3. Estándares de seguridad de datos confidenciales para pagos con tarjeta

Tema 3.1.: Introducción. Material protegido y políticas de seguridad
Tema 3.2.: Escenario 1: Destrucción incorrecta de datos confidenciales.
Tema 3.3.: Escenario 2: Fuga de información confidencial.
Tema 3.4.: Escenario 3: Terminal de pago defectuosa.
Tema 3.5.: Conclusiones.

Capítulo 4. Seguridad física para el resguardo de información confidencial

Tema 4.1.: Introducción. Seguridad física.
Tema 4.2.: Escenario 1: Accesos no autorizados a información confidencial.
Tema 4.3.: Escenario 2: Descuidos y negligencias con nuestros equipos.
Tema 4.4.: Escenario 3: Accidentes inesperados. Amenazas naturales.
Tema 4.5.: Acciones a tomar y reportes de incidentes. Conclusión.

Capítulo 5. Protección de datos personales. RGPD

Tema 5.1.: Introducción. La protección de datos.
Tema 5.2.: El RGPD. Gestión de la protección de los datos personales (principios).
Tema 5.3.: Escenarios.
Tema 5.4.: Medidas básicas de seguridad de la información.
Tema 5.5.: Brechas/incidentes de seguridad. Fuga de información.
Tema 5.6.: Ingeniería social.
Tema 5.7.: Conclusión.

LÄBERIT | CENTRO DE FORMACIÓN TIC.

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 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