Desarrollo del programa del curso

CIBERSEGURIDAD: ¿Tu empresa está protegida?

16 horas

Objetivos generales

- Al finalizar el taller, el participante será capaz de tener una visión global de cómo gestionar con seguridad la información de su empresa, así como conocer cuáles son los requisitos básicos para la protección de la información de su empresa y conocer los peligros de sufrir un ciberataque.

Contenidos

1. La información es el principal activo de la empresa (2 h.)

INTRODUCCIÓN

En esta unidad didáctica se pretende dar a conocer al participante la importancia de la información y su correcta gestión en una empresa.

OBJETIVOS

- Conocer la importancia de la información que se genera y usa en una empresa.
- Conocer los tres pilares básicos de la seguridad de la información.
- Saber los incidentes de seguridad que pueden afectar a la información de la empresa.
- Darse cuenta de la importancia de los datos de carácter personal y de privacidad de los mismos.

TEORÍA

1.1. La importancia de la información.

1.2. Los tres pilares de la seguridad.

1.3. La privacidad y la Ley.

2. La información: clasificación, cifrado y metadatos (2 h.)

INTRODUCCIÓN

Con esta unidad se pretende dar a conocer al participante cómo gestionar la información de la empresa.

OBJETIVOS

- Conocer los cuatro pasos básicos en la gestión de la Información de la empresa.
- Conocer los elementos fundamentales en el cifrado de la información
- Saber qué son los metadatos sus riesgos y su gestión correcta.

TEORÍA

2.1. Clasificación de la información.

2.2. Cifrado de la información.

2.3. Metadatos, riesgos y como eliminarlos.

3. La información: copias de seguridad, borrado y tipos de almacenamiento. (2 h.)

INTRODUCCIÓN

Con esta unidad se pretende aclarar al participante cómo y cuándo hacer copias de seguridad, la mejor forma de borrar la información y las ventajas e inconvenientes de los diferentes tipos de almacenamiento.

OBJETIVOS

- Saber lo que se considera la gestión correcta de las copias de seguridad.
- Conocer cómo realizar el borrado seguro de información.
- Conocer la ventajas e inconvenientes de cada tipo de almacenamiento.

TEORÍA

3.1. Copias de seguridad.

3.2. Borrado seguro de la información.

3.3. Almacenamiento en local, en red o en la nube.

4. El correo electrónico: principales fraudes y riesgos. (2 h.)

INTRODUCCIÓN

Con esta unidad el participante aprenderá cómo minimizar los riesgos del correo electrónico, conocer los tipos de correos fraudulentos, cómo detectarlos, y otros riesgos asociados al uso de esta herramienta de trabajo.

OBJETIVOS

- Conocer los riesgos que conlleva el uso del correo electrónico en las empresas.
- Saber los Tipos de correos fraudulentos.
- Conocer cómo detectar de correos fraudulentos.

TEORÍA

4.1. El correo electrónico como herramienta.

4.2. Tipos de correos fraudulentos.

4.3. Detección de correos fraudulentos.

4.4. Otros riesgos derivados de su uso

5. Contraseñas y medidas complementarias. (2 h.)

INTRODUCCIÓN

Con esta unidad se pretende mostrar al participante la importancia del uso de las contraseñas, y enseñarle diferentes prácticas adecuadas en su utilización.

OBJETIVOS

- Conocer lo importante que resulta el uso de las contraseñas en la gestión dela información en el trabajo.
- Conocer buenas prácticas en el uso de contraseñas y otras medidas complementarias.

TEORÍA

5.1. Importancia de las contraseñas.

5.2. Buenas prácticas en su uso.

5.2.1. Robustez

5.2.2. No compartidas

5.2.3. No usar la misma

5.2.4. Doble factor de autenticación

5.2.5. Gestores de contraseñas

6. El puesto de trabajo: medidas de protección (2 h.)

INTRODUCCIÓN

Con esta unidad se pretende enseñar al participante que medidas de protección debe tomar en su puesto de trabajo para una correcta gestión de la información de la empresa.

OBJETIVOS

- Conocer la importancia de proteger el puesto de trabajo.
- Conocer qué medidas de protección puede adoptar en su puesto de trabajo para gestionar adecuadamente la información de la empresa desde el punto de vista de la ciberseguridad.

TEORÍA

6.1. Importancia de proteger el puesto de trabajo.

6.2. Buenas prácticas:

6.2.1. Mesas limpias.

6.2.2. Bloqueo de sesión.

6.2.3. Software actualizado.

6.2.4. Antivirus y firewall.

6.2.5. Documentación sensible.

6.2.6. Contrato de confidencialidad.

6.2.7. Uso adecuado de Internet y sistemas operativos

6.2.8. Software legítimo.

6.2.9. Cómo y cuándo reportar un incidente de seguridad.

6.2.10. Uso seguro de dispositivos de almacenamiento extraíbles.

7. MÓVILES. (2 h.)

INTRODUCCIÓN

Con esta unidad se pretende mostrar al participante qué riesgos tiene el uso de móviles y el teletrabajo, y qué medidas de protección puede adoptar.

OBJETIVOS

- Conocer los riesgos que comportan el uso de dispositivos móviles.
- Conocer las medidas de protección que podemos adoptar para reducir al máximo los riesgos.
- Conocer cómo actuar en caso de pérdida o robo del dispositivo móvil.

TEORÍA

7.1. Dispositivos móviles y teletrabajo.

7.2. Riesgos asociados.

7.3. Medidas de protección.

7.3.1. Protección antimalware y sitios web peligrosos.

7.3.2. Protección contra accesos no autorizados.

7.3.3. Protección de la información.

7.3.4. Aplicaciones legítimas.

7.3.5. No recordar la contraseña.

7.3.6. No utilizar redes wifi inseguras.

7.3.7. Otras medidas de protección en caso de teletrabajo.

7.4. ¿Qué es el BYOD?

7.4.1. Principales riesgos.

7.4.2. Medidas de seguridad a tomar.

7.5. ¿Qué hacer en caso de robo o pérdida del dispositivo?

8. REDES SOCIALES. (2 h.)

INTRODUCCIÓN

8.1. Con esta unidad se pretende enseñar al participante el valor de las redes sociales, sus posibles riesgos, y qué medidas de seguridad podemos adoptar.

OBJETIVOS

- Conocer el valor de las redes sociales y los posibles riesgos de su uso.
- Conocer las principales medidas de seguridad que podemos tomar para reducir esos riesgos.

TEORÍA

8.2. El valor de las redes sociales.

8.3. Posibles riesgos de su uso.

8.2.1. Error humano.

8.2.2. Configuración de privacidad débiles.

8.2.3. Campañas de fraude: suplantación, malware, y phishing.

8.4. Medidas de seguridad.

8.3.1. Contraseña de acceso.

8.3.2. Sentido común.

8.3.3. Privacidad.

8.3.4. Malware y enlaces.

4. Evaluación final