DigitalHouse>
Coding School

Certified Tech Developer
The Ultimate Degree

Práctica de diseño de plan de seguridad

Práctica integradora Grupo 11

Microdesafío

Escenario:

Empresa emergente dedicada a la **venta de productos fertilizantes para campos**, con una **capacidad financiera acotada**, todos sus **empleados trabajan on site y están dispuesto a recibir capacitación**, poseen actualmente dos personas encargadas de sistemas, las cuales **manejan información sensible, pero que todos los usuarios pueden ver (no es política de la empresa)**, **no realizan copias de información** porque no las creen convenientes. Poseen una **página web donde hay catálogos y los clientes pueden hacer compras** a través de la misma.

1. Hacer un análisis de la situación actual de cada empresa que nos toque.

La seguridad de la información consiste en todas las acciones que llevamos adelante para proteger la integridad, la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. Para poder proteger a nuestra computadora tenemos dos tipos de seguridad: seguridad activa y seguridad pasiva.

Computadoras de los empleados: contienen información sensible.

Posibles fuentes de amenazas:

- Contraseñas no seguras
- No usar antivirus, antiespías y cortafuegos
- No encriptar datos
- Falta de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas
- No escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware

2. Crear un plan de seguridad: debe ser de 6 pasos e incluir, seguridad lógica, física, pasiva, activa y controles de medida de seguridad, y de vulnerabilidades que podrían explotar los atacantes

Plan de seguridad:

1. Crear contraseñas segura.
2. Instalar antivirus
3. Crear copias de seguridad de la información (hacer respaldo de datos).
4. Poner un UPS.
5. Agregar control de acceso para la información sensible.
6. Cifrar los datos.