Certified Tech Developer
The Ultimate Degree

Re

Práctica de diseño de plan de seguridad

Práctica integradora

Objetivo

Se dividirá a los estudiantes en 10 grupos

Microdesafío

Para empezar a poner en práctica los conocimientos adquiridos, necesitarás realizar la siguiente actividad. La empresa que les toque los contrata como asesores de seguridad ya que creen que es una parte fundamental para resguardar sus activos, en base a lo visto en clase y clases anteriores deben hacer:

1. Hacer un análisis de la situación actual de cada empresa que nos toque.
2. Para cada escenario planteado, crear un plan de seguridad
3. Este plan 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

Esta serie de pasos y sugerencias, deben ser puestas en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

Caso de Análisis:

- 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.

Plan de seguridad

1. **Control de acceso (seguridad activa/lógica): Impedir el acceso a personas no autorizadas mediante usuarios y contraseñas.**
2. **Respaldo de datos (seguridad pasiva/física): Realizar copias de seguridad o backups de los datos completos e incrementales.**
3. **Capacitación al personal y prepararlos ante la ingeniería social, acción preventiva para evitar ser engañados.**
4. **El uso de claves dinámicas (verificación de dos pasos) para protección de los datos (seguridad activa/lógica).**
5. **Uso de antivirus (seguridad pasiva/lógica): Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.**
6. **Dispositivos físicos de protección (seguridad física): Utilización de pararrayos, extintores, y otros elementos que se enfoquen en la seguridad de las herramientas físicas.**