DigitalHouse>
Coding School

Certified Tech Developer
The Ultimate Degree

Grupo 6

- **Dante Rubio**
- **Carol Suarez**
- **Paola Gomez**
- **Leiva Nelida**
- **Yanina Leiba**
- **Andres Lopez**

Práctica de diseño de plan de seguridad

Práctica integradora

Objetivo

Para empezar a poner en práctica los conocimientos adquiridos, realizaremos la siguiente actividad. Se crearán grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Microdesafío 📌

La empresa que se les haya asignado 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. Un análisis de la situación actual de cada empresa que se les haya asignado.
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 debe ser presentada en un documento que pueda ser compartido con otras personas, especificando el grupo que son y el escenario que les tocó.

Escenario para grupos 2, 4, 6, 8, 10 , 12

- Empresa ya consolidada que se dedica a brindar servicios informáticos. La mayoría de sus empleados trabajan de forma remota, pero hay algunos que lo hacen on site. Necesitan una intranet más segura. La información confidencial de la empresa tiene buena seguridad lógica, pero muy poca física, aunque igualmente desean tener asesoramiento en seguridad lógica. No tienen problemas en invertir dinero, pero sus empleados se resisten al cambio de nuevas restricciones. Poseen una página web donde brindan sus servicios y los clientes pueden contactarse a través de la misma.

- Seguridad Lógica:

  Sugerir inversión en licenciamiento y actualización de software de antivirus de las pcs de los trabajadores remotos y actualización de antivirus de los servidores y firewalls. Generar control de accesos no autorizados remotos e internos dando niveles de acceso a cada usuario.

- Seguridad Física:

  Proponer implementación de dispositivos de seguridad en los servidores , con sistemas de vigilancia, monitoreo y prevención de intrusión a la instalaciones implementando elementos de acceso personalizados para cada trabajador.

  Proponer implementación de UPS (Uninterruptable Power Supply) para servidor principal y servidor del sistema redundante.

  Proponer trasladar infraestructura de los servidores a la nube

  Proponer implementación de tarea automática de generación de backups (diferencial , transaccional y full) para subida y recuperación de datos a la nube.

  Proponer implementación de sistema de recuperación de desastres DRP (Disaster Recovery Plan)

- Seguridad activa:

  Continuar con las implementaciones propuestas en la seguridad lógica.

  Cifrar los datos para que sólo puedan ser leídos si se conoce la clave de cifrado.

- Seguridad Pasiva

  Usar un hardware adecuado contra averías y accidentes.

  Comprobar si el antivirus funciona correctamente cuando hay una infección por un virus.

  Escanear el sistema al completo y, si se encuentra algún malware, limpiarlo.

  Realizar copias de seguridad de los datos y del sistema operativo en distintos soportes y ubicaciones físicas.

  Crear particiones del disco duro para almacenar archivos y backups en una unidad distinta a la del sistema operativo.

  Desconectar la máquina de la red hasta que se encuentre una solución.

- Controles y Vulnerabilidades:

  Proponer implementación de escaneos periódicos de los equipos

  Proponer auditorías para detectar vulnerabilidades de los equipos y mejorar los controles internos de seguridad de la empresa.