DigitalHouse>
Coding School

Certified Tech Developer
The Ultimate Degree

Práctica de diseño de plan de seguridad **GRUPO 2**

FERNANDO FRAGA
JOSÉ NIEVA
RODRIGO HELUANI
FELIPE BELTRÁN

Microdesafío 📌

1. Un análisis de la situación actual de cada empresa que se les haya asignado.
    - La mayoría de empleados son remotos.
    - Algunos empleados On Site.
    - Intranet insegura.
    - Poca red física.
    - Resistencia al cambio.
    - Presupuesto abultado.
    - Desean asesoramiento en seguridad lógica.
    - Página web de la empresa con : Servicios informáticos y contacto de clientes.

2. Para cada escenario planteado, crear un plan de seguridad

Este plan consta de:

A. Seguridad lógica:
    a. Recomendamos el antivirus Bitdefender Total Security, dado que cuenta con navegación anónima, tráfico cifrado y protege puntos Wi-Fi. (*Abarca integralmente: protección de virus, cifrado de datos, control de acceso*)
    b. Recomendamos TinyWall Firewall dado que priman la sencillez y simplicidad de su software.
B. Seguridad física:
    a. Recomendamos: Pararrayos, extintores, detectores de humo, alarma contra intrusos.
    b. Es importante contar con un UPS (Uninterruptable Power Supply) para minimizar la afectación por falta de energía eléctrica.
    c. Recomendamos copias de seguridad en la nube a través de Amazon AWS, para tener un sistema redundante.
C. En seguridad pasiva recomendamos:
    a. La realización de copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas.

b. Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
c. Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.
d. Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
e. Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.

D. Seguridad activa :
   a. Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres especiales. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.
   b. Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
   c. Encriptar los datos importantes. La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información sólo pueda ser leído si se conoce la clave de cifrado.

E. Controles de medida de seguridad y de vulnerabilidades:

a. Necesitamos un área encargada de la gestión del cambio para incentivar y lograr el buen uso del sistema y sus distintos componentes de seguridad, para el buen cuidado de la información de la empresa.

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.