**Introducción a la Informática - Clase 25**

**Grupo 8**

**Escenario**

* 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.

**Plan de seguridad**

**Seguridad lógica**

Si bien la empresa ya cuenta con buena seguridad lógica, se recomienda para tener una intranet más segura:

* Cifrado de datos
* Control de acceso

**Seguridad física**

Se debe reforzar la seguridad física:

* Agregar UPS
* Instalación de dispositivos físicos de protección: extintores, detectores de humo, alarma contra intrusos,etc.
* Respaldo de datos en tres servidores ubicados en distintos sitios.
* Sistemas redundantes para evitar perder datos.

**Seguridad pasiva**

* Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware
* Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
* Revisar diariamente que el Antivirus esté en funcionamiento y operando con normalidad.

**Seguridad activa**

* Encriptación de datos importantes.
* Cambiar las contraseñas cada 3 meses y exigir que sea una combinación de letras, números, mayúsculas y otros caracteres.
* Capacitación al personal en temas de seguridad informática.

**Controles de medida de seguridad**

* Implementación de medidas de seguridad Detectivas basadas en la búsqueda de potenciales ataques o peligros.

**Controles de vulnerabilidades**

* Establecer Controles de acceso en la Intranet para que sólo accedan personas autorizadas.
* Encriptación de datos importantes.
* Delimitar quién puede y debe acceder a la información confidencial.

**Auditoría a Grupo 3**

**1.** Un análisis de la situación actual de cada empresa que se les haya asignado.

Pro: El personal está trabajando on site y está dispuesto a recibir capacitaciones. Venta online.

Contra: No realizan copia de seguridad de la información. Todos tienen acceso a la información de la empresa. No se tiene clara la seguridad en la página WEB para los usuarios al momento de comprar.

**Seguridad lógica:** Colocar control de acceso a los usuarios para que no todos tengan acceso al total de la información sino depende del rol y área. Colocar un firewall para la página web para asegurar las compras online.

**Seguridad Física:** Crear un respaldo de datos / sistemas redundantes

*Nota de Auditoría: Ya que el trabajo es on site, debería hacerse hincapié en las medidas de seguridad físicas, como la instalación de una UPS ante cortes de energía eléctrica.*

**Seguridad Pasiva:** Tener partición de disco duro en cada computador de los empleados para poder recuperar en caso de algún daño o ataque, y generar back up en la nube constantemente.

**Seguridad Activa:** Que los empleados tengan contraseñas seguras para acceder a la red de la empresa, y que tengan instalados en sus computadores antivirus.

**Controles de medida de Seguridad:** Generar controles proactivos de tipo preventivas, esto con el fin de bloquear algún ataque y generar la mayor seguridad.

**Vulnerabilidades:** Delimitar quién puede y debe acceder a la información confidencial. Probar que las copias de seguridad realizadas funcionen.