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

La empresa ya consolidada tiene la seguridad lógica ya implementada, pero desean realizarle algunas mejoras y recibir asesoría respecto a esta implementación. Teniendo en cuenta que se tenga el menor impacto a los cambios que puedan experimentar los empleados.

Respecto a la seguridad física se requiere un plan de implementación, debido a que en estos aspectos son vulnerables, cabe notar que la empresa cuenta con los recursos económicos para su desarrollo.

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

1. Seguridad lógica:

Realizar actualización de los sistemas que se encuentran operando actualmente y capacitación a sus empleados de su uso adecuado.

2. Seguridad física:

Implementar uso de elementos de seguridad física como extintores, detectores de humo, alarmas contra intrusos y pararrayos, Uso de ups en los equipos, creación de backup en discos duros externos con protocolos de tiempos y clases de datos para guardar la información.

3. Seguridad pasiva:

* Realizar copia de seguridad de los datos en más de un dispositivo.
* Escaneo frecuente para detectar malware y validar que el antivirus funcione correctamente.
* Dividir la información (archivos y backup) en diferentes particiones del disco duro, en una ubicación diferente al del sistema operativo.

4. Seguridad activa:

* Validar que las contraseñas sean seguras, es decir que sean alfanuméricas y que no estén relacionadas con datos personales fáciles de descifrar.
* Instalación de software de seguridad informática, como antivirus, antiespías y cortafuegos.
* Encriptación de datos para permitir el acceso a la información mediante una clave.

5. Controles de medidas de seguridad: Como medidas proactivas se proponen algunas medidas disuasivas al usar el sistema y preventivas. Así como la implementación de medidas reactivas detectivas y correctivas

6. Medidas de vulnerabilidades: Evaluar y corregir las dificultades que se encuentren en las redes de la empresa y su infraestructura, revisar los permisos de acceso a cada tipo de información, revisar protocolos de control y verificación de copias de seguridad en donde se pruebe que funcionan e implementar auditorias para garantizar el estado de la información.