PLAN DE SEGURIDAD

Grupo 2

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, física, pasiva, activa y
controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

Seguridad Física: UPS, alarma contra incendio, extintores, alarma contra intrusos, detecto de humos, sistema redundante, backup de datos.

Seguridad Lógica: control de acceso, cifrado de datos (VPN), antimalware y firewares

Seguridad Pasiva: La realización de copias de seguridad de los datos en más de un dispositivo o en distintas ubicaciones físicas.
Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.
Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
Es importante que cuando haya una infección por un virus, se compruebe que el antivirus funcione correctamente.

Seguridad Activa:

Uso y empleo adecuado de contraseñas. Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos. Encriptar los datos importantes.

6 PASOS – GRUPO 2

1.- Inspección y auditoria de la seguridad física en el área de trabajo (las instalaciones de los servidores y conexiones de red de la empresa).

2.- Inspección y auditoria de la seguridad lógica del sistema de trabajo y comunicación remota (sistemas de uso para conexión a intranet, seguridad de sistemas operativos).

3.- En caso de no existir una adecuada seguridad física utilizaremos UPS para respaldo de energía, alarma y detector de humos contra incendio, extintores, alarma contra intrusos. En caso de no existir respaldo de información implementaremos un sistema redundante y backup de datos.

4.- En caso de no existir una adecuada seguridad lógica en el desempeño de los usuarios remotos, implementaremos la adecuada adopción por parte de los usuarios de una red VPN para cifrado de datos, instalación de antivirus para evitar entradas de archivos maliciosos y que realice escaneo diario del sistema operativo del usuario.

5.- Incentivaremos el uso adecuado de contraseñas seguras, educando a los usuarios sobre la correcta implementación de contraseñas e implementaremos un sistema automático de caducidad de contraseñas para que el usuario la cambie de forma recurrente.

6.- Detección e identificación permanente de vulnerabilidades se los diferentes sistemas utilizados en la empresa, para actualizar rápidamente (los parches) y mantener una adecuada defensa de los sistemas.