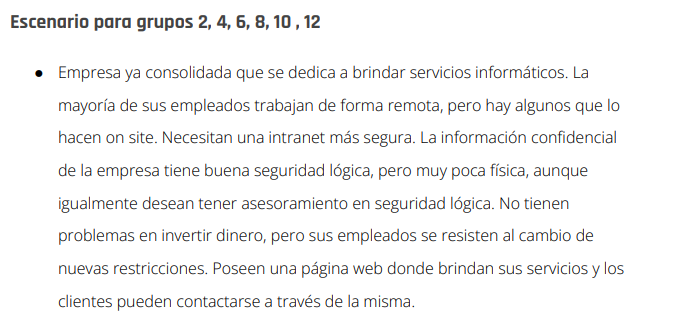
Eduardo Perez Danderfer Grupo 8  


Lo primero que hay que hacer es ver lo que queremos y necesitamos resguardar, aplicando medidas de seguridad proactivas de carácter preventivo, como segunda medida podemos proteger el entorno a partir de las siguientes medidas de seguridad física

1- Resguardar el Hardware con UPS

2- Respaldo de datos por medio de BackUps en el lugar y oficina virtual

3- Sistemas redundantes

4- Restringir el alcance de las redes dividiendo por sectores con su propia virtual LAN/Red

5- Control de acceso diferenciado

6- Endurecer las contraseñas sobre VPN

7- Mandar notificaciones preventivas para educar a los usuarios

8- Sesión de usuario más cortas

1) Seguridad Lógica:

La empresa cuenta con altos estándares de seguridad lógica, es decir, cuenta con una buena

aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita

acceder a ellos a las personas autorizadas para hacerlo.

Los puntos importantes de la seguridad lógica a reforzar son:

\* Restringir el acceso a los programas y archivos.

\* Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar

los programas ni los archivos que no correspondan.

\* Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el

procedimiento correcto.

\* Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a

otro.

\* Que la información recibida sea la misma que ha sido transmitida.

\* Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

\* Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Se sugiere establecer un tiempo definido para verificar y validar que todo esté bien. Si en esas

validaciones aparece algo anormal, se procederá a tomar medidas correctivas y preventivas.

2) Seguridad Física:

Teniendo en cuenta que la mayoría de los empleados laboran desde casa, se sugiere suministrarle

a cada funcionario una UPS con el fin de evitar pérdidas de información.

También, se recomienda establecer copias de seguridad diarias, Backups, al igual que implementar

sistemas redundantes.

Todo lo anterior, con el fin de resguardar la información confidencial de la empresa.

3) Seguridad Activa:

Con el objetivo de evitar vulnerabilidades, se recomienda a la empresa implementar las siguientes

buenas prácticas:

\* Uso y empleo adecuado de contraseñas.

\* Uso de software de seguridad informática, como antivirus, anti espías y cortafuegos.

\* 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 solo pueda ser leído

si se conoce la clave de cifrado.

4) Seguridad Pasiva:

La seguridad pasiva es la que entra en acción para minimizar los daños causados por un usuario, un

accidente o un malware en los sistemas. Para evitar este tipo de inconvenientes se sugiere la

implementación de las siguientes buenas prácticas:

\* 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.