Equipo 4

Caso: 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

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.