

Equipo 2

Planteamos para seguridad física:

- UPS por cortes de luz
- Respaldo de datos para hacer backups
- Sistemas redundantes, copia de sistemas

Planteamos para seguridad lógica:

- VPN Segura para trabajadores remotos
- Proxy para bloquear a nivel PC sitios inseguros
- Reforzar antivirus y firewalls
- Control de acceso
- Cifrado de datos en la intranet
- Cambio de claves periódicos

Equipo 1:

paso 1: le diría a los encargados de sistemas que establezcan un antivirus en todas las pc de la empresa y en sus notebook laborales

paso 2: establecer un sistema redundante donde se guarden los datos más importantes en un backup que puede ser una solución de bajo costo

paso 3: Crear particiones en el disco duro para almacenar archivos y backups (copias de seguridad) en una unidad distinta a donde tenemos nuestro sistema operativo.

paso 4: Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.

paso 5: activamos una medida preventiva para que nuestros empleados no divulguen sus contraseñas a nadie

paso 6: como la falibilidad humana tiende a notarse en cuanto a la creación de contraseñas seguras, se deberá asesorar a los empleados para que puedan crearlas con varios caracteres, entre ellos mayúsculas, minúsculas, números y caracteres especiales.

Pasos para detectar una vulnerabilidad

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

- Evaluar cómo está constituida la red e infraestructura de la empresa.
- Delimitar quién puede y debe acceder a la información confidencial.
- Probar que las copias de seguridad realizadas funcionen.
- Identificar las partes más sensibles y esenciales del sistema.
- Realizar auditorias del estado de la seguridad informática.

Vulnerabilidad detectada: no está delimitado quien puede y debe acceder a la información confidencial.

Para ello se debe realizar un software para establecer un control de acceso a los empleados según la necesidad de acceder a la misma para realizar su trabajo.