**Grupo n° 2 – Diseño de Plan de Seguridad**

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

Para la empresa de Servicios informáticos planteamos como propuesta para la seguridad física:

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

Y para la 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

**Auditoria de Grupo N° 1**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

La propuesta presentada por el equipo n° 1 fue:

* Paso 1: les 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, anti-espías 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.

**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.