

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.

Este plan debe ser de 6 pasos e incluir: seguridad lógica, física, pasiva, activa y controles de medida de seguridad y de vulnerabilidades que podrían explotar los atacantes.

Seguridad lógica:

- Cifrado de datos.
- Control de acceso.
- Firewall.
- Antivirus.

Seguridad física:

- UPS.
- Dispositivos físicos de protección: extintores, alarmas contra incendios, detectores de humo, alarma contra intrusos.
- Respaldo de datos: sincrónico(diariamente)/ asincrónico(una vez por semana).
- Sistemas redundantes.

Seguridad pasiva:

- Escaneo y limpieza del antivirus continuamente.
- Desconectar el equipo de la red hasta solucionar el problema.

Seguridad activa:

- Encriptar datos importantes.
- Uso y empleo adecuado de contraseñas.
- Antivirus, firewalls, otros softwares de seguridad informática.

Medidas de Seguridad Proactivas

- Uso y empleo adecuado de contraseñas.
- Establecer protocolo de seguridad.
- Charlas informativas a los empleados.
- Capacitaciones.

Medidas de Seguridad Reactivas

- Plan de ejecución frente a un ataque.
- Capacitaciones.

