**Seguridad Lógica**

Actualizar su antivirus a la última versión y automatizar las actualizaciones de versiones.

El administrador del sistema debe asegurarse de que el firewall de cada computadora (de la intranet) esté activo y que sea un permiso solo de administrador.

**Seguridad física**

**Elementos físicos de seguridad:** revisar colocación de extintores, revisar/actualizar el cableado de la oficina, presencia de estabilizadores en todas las máquinas de la intranet, control con tarjeta magnética + medidas biométricas del personal a la empresa.

**Respaldo de datos:** Deberán realizarlos de manera sistemática, por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales.

**UPS**: Sugerimos un sistema de UPS interactivo en el servidor o nodos críticos (Los sistemas de UPS interactivos ofrecen un acondicionamiento de la energía y un respaldo con baterías. Esta tecnología es particularmente eficaz en áreas donde casi no se dan cortes, pero donde las fluctuaciones de energía son comunes. Los sistemas de UPS interactivos soportan una amplia variedad de fluctuaciones de voltaje de entrada antes de transferirse al respaldo con baterías.

Además del respaldo con baterías, un UPS interactivo ofrece un control mucho mayor de las fluctuaciones de energía que los sistemas sin conexión. La ventaja crítica de los UPS interactivos son los circuitos de carga rápida y el rango de voltajes de entrada compatibles con el UPS. Entre mayor sea el rango, mayor será la protección total que tendrá.)

**Seguridad pasiva:**

Organizar un servicio de administración de software (nuestra empresa se lo ofrece por una módica suma) que se encargue de ejecutar periódicamente en todas las computadoras de intranet y en las de extranet a través de escritorios remoto, limpiadores y buscadores de malware.

Establecer manual de protocolo de seguridad de cómo actuar ante un ataque: desconectar el equipo en la red, dar aviso al administrador, no abrir links personales o inseguros o externos en las computadoras de la empresa.

**Seguridad activa**

Gestor de contraseñas: contratar un software de gestión de contraseñas.

Encriptación de datos críticos en cada nodo.

**Controles de medidas de seguridad y vulnerabilidades:**

Vulnerabilidad de datos de clientes en el website: activar el código de autentificación por imágenes además de usuario y contraseña.

Establecer encriptado y copias virtuales de las base de datos de clientes para evitar la vulnerabilidad de los datos personales de los clientes.