**VActividad Seguridad Informática - Clase 25**

**Plan de Seguridad**

**Aplicar seguridad física:**

* Dispositivos físicos de protección: Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.
* UPS.
* Respaldo de Datos local y remoto.
* Servidores redundantes.

**Aplicar seguridad Lógica:**

* Control de acceso: Al utilizar conexiones remotas es importante reforzar los controles de acceso.
* Cifrado de datos: Establecer un cifrado de datos mediante el uso de VPN.
* Antivirus.
* Firewalls.

**Aplicar seguridad activa:**

* Uso y empleo adecuado de contraseñas.
* Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
* Encriptar los datos importantes.

**Aplicar seguridad pasiva:**

* La realización de copias de seguridad de los datos en varios dispositivos o ubicaciones.
* Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
* Crear particiones en el disco duro para almacenar archivos y backups en una unidad distinta a donde tenemos nuestro sistema operativo.
* Comprobación de antivirus.

**Medidas de seguridad adicionales:**

* Realizar auditorías.
* Realizar capacitaciones sobre seguridad informática.
* Comprobar que las copias de seguridad funcionen correctamente.
* Restringir el acceso a la información del sistema solo a personas calificadas y capacitadas. Por ejemplo asignando perfiles para los distintos niveles de acceso.

**Vulnerabilidades detectadas:**

* La intranet de la empresa es insegura, ya que las credenciales de acceso al sistema no tienen un alto nivel de seguridad.
* Parte del personal podría tener dificultades para adaptarse a los nuevos servicios de seguridad informática.
* Un posible ataque DDoS ante la falta de seguridad física en los servidores.