RESUMEN HERRAMIENTAS / TÉCNICAS DE SEGURIDAD

1. HERRAMIENTAS Y TÉCNICAS DE SEGURIDAD.....2
1.1 CLASIFICACIÓN UNO.....3
1.2 CLASIFICACIÓN DOS.....5
2. MODELOS DE RED Y HERRAMIENTAS DE SEGURIDAD.....6
2.1 SEGURIDAD EN LA RED DE UN HOGAR.....6
2.2 SEGURIDAD EN LA RED DE UNA EMPRESA.....7
2.3 PLANTEAMIENTO GENERAL DE LA SEGURIDAD.....8

1. HERRAMIENTAS Y TÉCNICAS DE SEGURIDAD

Una misma técnica o herramienta puede aportar mejoras en distintos aspectos de la seguridad informática.

1.1 CLASIFICACIÓN UNO

HERRAMIENTA / TÉCNICA DE SEGURIDAD	CONFIDENCIALIDAD	INTEGRIDAD	RESPONSABILIDAD	DISPONIBILIDAD	ACTIVA	PASIVA	FÍSICA	LÓGICA
Active Directory / LDAP / Samba/ ACL/ Aranque seguro (control de acceso x usuario/rol) Mínimo de servicios x usuario/rol								
Antivirus – Antimalware					P			
Cortafuegos local								
Cortafuegos de red								
Copia de seguridad de los datos (política de copia)								
Administración remosta segura (SSH) (SFTP) (VPN)								
Política de contraseñas								
Proxy								
DMZ (si ofrecemos servicios en Internet)								
VPN de acceso remoto (si trabajamos desde casa)								
VPN punto a punto (si tenemos sucursales)								
Proteger la BIOS								
Cuentas locales diferenciadas								
Proteger el gestor de arranque								
RAID								
Imagen del sistema (para los clientes)								
Copia de seguridad de la configuración de los servicios								
Cifrado de datos								
Cifrado de las comunicaciones								
Identificación digital – Autoridad de certificación								
Limitación de usuarios								
Monitorización del sistema								
Monitor de red – IDS								
Log de servicios – registro de								

HERRAMIENTA / TÉCNICA DE SEGURIDAD	CONFIDENCIALIDAD	INTEGRIDAD	RESPONSABILIDAD	DISPONIBILIDAD	ACTIVA	PASIVA	FÍSICA	LÓGICA
actividad – auditorías								
Alta disponibilidad – replicación de servicios- replicación de hardware								
Servidor AAA								
Portal cautivo								
Auditoría de seguridad								
VLAN								
Wi-Fi segura								
Balanceo de carga								
Proxy inverso								
SAI								
Extintores, Cerraduras, videovigilancia, Antihumedad...								

1.2 CLASIFICACIÓN DOS

TIPOS DE SEGURIDAD	HERRAMIENTAS O TÉCNICAS
Seguridad activa	Antivirus Control de acceso (AD, LDAP, permisos, recursos compartidos, contraseña, bios, arranque, cerraduras,…) Proxy Administración remota segura (SSH, SFTP,...)
Seguridad pasiva	Copia de seguridad (de los datos) SAI RAID 1, RAID 5 Imagen del sistema Antivirus
Seguridad física	Control de acceso (AD, LDAP, permisos, recursos compartidos, contraseña, bios, arranque, cerraduras,…) SAI Colocación segura Monitorización del sistema Replicar hadware
Seguridad lógica	Control de acceso Antivirus - Antimalware Cortafuegos local y de red VLAN Cifrado de datos
Para mejorar la confidencialidad	Control de acceso (AD, LDAP, permisos, recursos compartidos, contraseña, bios, arranque, cerraduras,…) Criptografía (SSH, HTTPS, SFTP, Certificados digitales, cifrado de datos almacenados…) VLAN
Para mejorar la integridad	Control de acceso (AD, LDAP, permisos, recursos compartidos, contraseña, bios, arranque, cerraduras,…) RAID 1, RAID 5 Servicios replicados Criptografía (SSH, HTTPS, SFTP, Certificados digitales, cifrado de datos almacenados…)
Para mejorar la disponibilidad	Control de acceso (AD, LDAP, permisos, recursos compartidos, contraseña, bios, arranque, cerraduras,…) RAID 1, RAID 5 Servicios replicados
Para mejorar la responsabilidad	Control de acceso (AD, LDAP, permisos, recursos compartidos, contraseña, bios, arranque, cerraduras,…) Criptografía (SSH, HTTPS, SFTP, Certificados digitales, cifrado de datos almacenados…)

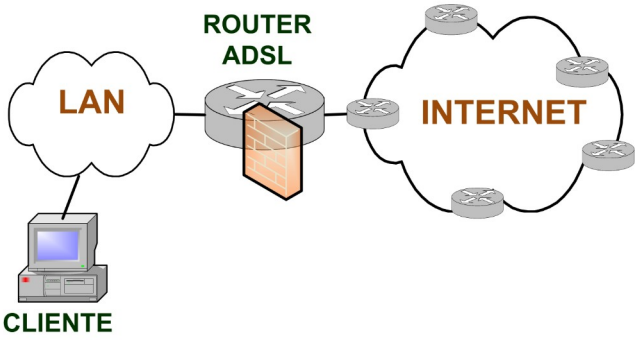
2. MODELOS DE RED Y HERRAMIENTAS DE SEGURIDAD

2.1 SEGURIDAD EN LA RED DE UN HOGAR

Planteamiento de seguridad
MODELO GENÉRICO DE LA RED UN HOGAR
Herramientas y técnicas de seguridad básicas

- **Software Actualizado** – Seguridad Activa
- **Control de acceso**: Usuarios y Grupos locales – S. Activa
  - Seguridad BIOS, arranque
  - Separar cuentas administrador y cuentas de usuario
  - Control de permisos y recursos compartidos.
  - Cifrado de las comunicaciones: SSH, HTTPS,..
  - Cifrado de la información almacenada
- **Antivirus** – Seguridad Activa (y Pasiva)
- **Cortafuegos** Local y Cortafuegos de red – S. Activa
  - Cortafuegos Local
  - Cortafuegos de Red: en el router ADSL
- **Copia de Seguridad** – Seguridad Pasiva
  - Copia de seguridad de datos en un soporte externo
  - Partición de datos y sistema (programas) separadas
  - Imagen del sistema o punto de restauración
- **Administración remota segura** – Seguridad Activa
  - Control de los recursos compartidos
  - Quien puede acceder a nuestro equipo

- **Monitorización, Vigilancia** – S. Activa y Pasiva
- **Mejora** – Seguridad Activa y Pasiva

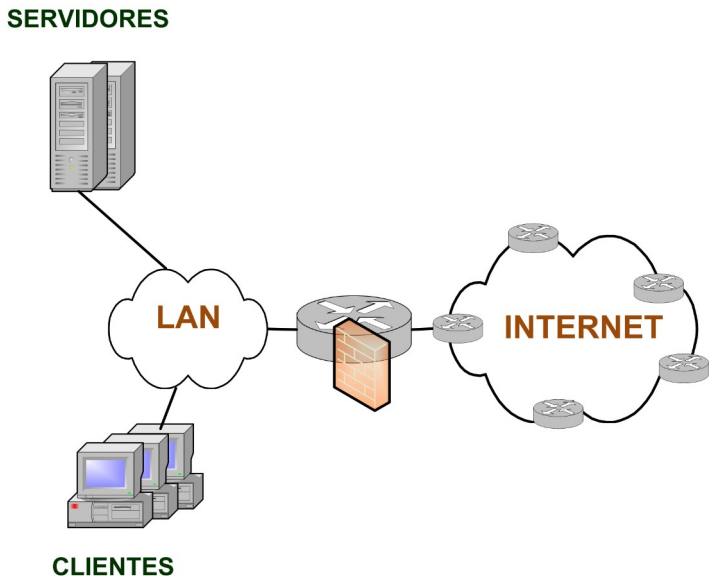


2.2 SEGURIDAD EN LA RED DE UNA EMPRESA

Planteamiento de seguridad
MODELO GENÉRICO DE LA RED DE UNA EMPRESA
Herramientas y técnicas de seguridad básicas

- **Software Actualizado** – Seguridad Activa
- **Control de acceso**: AD, LDAP, SAMBA – S. Activa
  - Seguridad BIOS, arranque
  - Control de acceso centralizado: AD, LDAP, SAMBA
  - Control de permisos y recursos compartidos.
  - Cifrado de las comunicaciones: SSH, HTTPS,..
  - Cifrado de la información almacenada
- **Antivirus** – Seguridad Activa (y Pasiva)
- **Cortafuegos** Local y Cortafuegos de red – S. Activa
  - Cortafuegos Local
  - Cortafuegos de Red: inspección de paquetes, proxy
  - DMZ (si la empresa ofrece servicios en Internet)
- **Copia de Seguridad** – Seguridad Pasiva
  - Copia de seguridad de datos del servidor de ficheros.
  - Copia de seguridad de los ficheros de configuración de máquinas y servicios.
  - Imagen del sistema para los equipos cliente
- **Administración remota segura** – Seguridad Activa
  - Control de los recursos compartidos
  - Quien puede acceder a los servidores
  - Teletrabajo – VPN
  - Sucursales de la empresa
- **Hardware redundante** – Seguridad Pasiva
  - RAID
  - CPD de respaldo
  - Línea de comunicaciones redundante
  - SAI en los servidores

- **Monitorización, Vigilancia, Auditoría** – S. Activa y Pasiva
- **Mejora** – Seguridad Activa y Pasiva



2.3 PLANTEAMIENTO GENERAL DE LA SEGURIDAD

Planteamiento de seguridad

Herramientas y técnicas de seguridad básicas

- **Software Actualizado** – Seguridad Activa
- **Control de acceso:** Usuarios, grupos, permisos – Seguridad Activa
- **Antivirus** – Seguridad Activa (y Pasiva)
- **Cortafuegos** Local y Cortafuegos de red – S. Activa
- **Copia de Seguridad** – Seguridad Pasiva
  - Copia de seguridad de datos del servidor de ficheros.
  - Copia de seguridad de los ficheros de configuración.
  - Imagen del sistema para los equipos cliente, puntos de restauración
- **Administración remota segura** – Seguridad Activa
  - Control de los recursos compartidos
- **Hardware redundante** – Seguridad Pasiva

- **Monitorización, Vigilancia, Auditoría** – S. Activa y Pasiva
- **Mejora** – Seguridad Activa y Pasiva