Tema 8 – Seguridad Informática

CFGS DAW – Sistemas Informáticos

Seguridad en Sistemas Informáticos

- Definición de **seguridad** → combinación de los siguientes principios:

		Amenazas
Confidencialidad	→	Intercepción (del mensaje…)
Verificación (no repudio)	→	Generación (del mensaje…)
Autenticación/autorización	→	Intrusión
Integridad (del mensaje/del archivo, etc.)	→	Modificación
Disponibilidad	→	Interrupción

- Cualquier sistema es vulnerable → minimizar (lo máximo posible) dicha vulnerabilidad.
- **Principio fundamental de la seguridad**: menor privilegio, simplicidad (instalar lo sólo necesario), actualización y participación universal.

Términos y definiciones relacionados con la seguridad

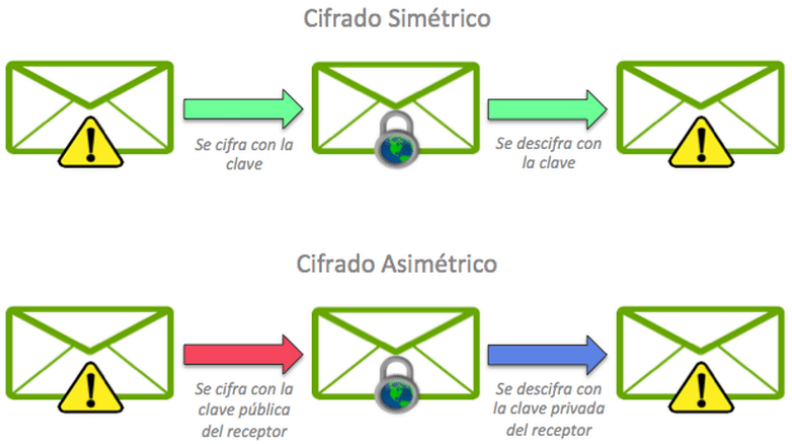
- Elementos que participan en la seguridad de los sistemas informáticos:
  - Usuarios / personal técnico → principal elemento, por el que llegan la mayor parte de fallos de seguridad.
  - Protección lógica → *software*.
    - E.g. antivirus, actualización del software, permisos, etc.
  - Protección física → *hardware*.
    - E.g. protección de los equipos informáticos y sus instalaciones (contra incendios, inundaciones, suministro eléctrico, etc.).
  - Medidas administrativas → Normas implantadas por el dueño del sistema para su uso.
    - E.g. cambio de contraseñas a menudo, concienciación contra el *phishing*, etc.
  - Medidas legales → Normas estatales, etc.
    - E.g. cumplimiento legislación relacionada como RGPD, mensajes de acceso, etc.

Términos y definiciones relacionados con la seguridad (II)

- Programas maliciosos (*malware*):
  - Virus → se realiza copias de sí mismo y se inserta en otros programas o ficheros.
  - Gusano → se puede copiar a sí mismo sin infectar ficheros y se transmite por la red para infectar otros ordenadores.
  - Troyano
  - *Ransomware*: deniega el acceso a los archivos del usuario y pide rescate.
  - *Spyware*, *adware*, *hijacking*.
- Intrusos:
  - *Hackers* (*White hat*, *black hat*, *grey hat*…)
- Otros:
  - DoS, DDoS → Denegación de servicio.
  - *Eavesdropping* → Escucha; TEMPEST.
  - *Phishing* → Intento de obtener información sensible (contraseñas, tarjetas de crédito, etc.) directamente de los usuarios mediante engaño (ingeniería social).
  - *Spoofing* → Falsificar algo (IP, MAC, email, etc.)
  - *Tampering* → Modificación maliciosa del programa o los datos.
- ¿Errores? de programación:
  - *Zero-day* → vulnerabilidad desconocida por desarrolladores
  - *Backdoors* (puerta trasera).

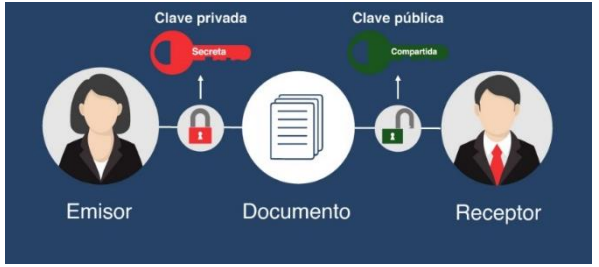
Técnicas y medidas de seguridad

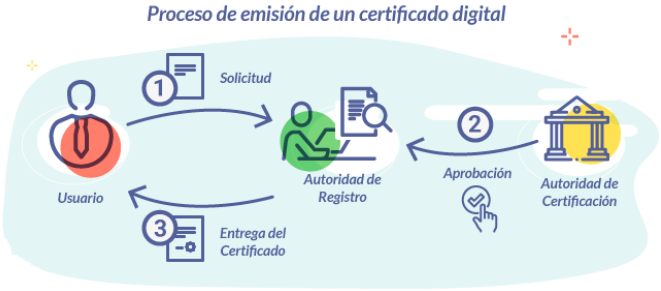
- Cifrado:
  - Utilización de claves para modificar un mensaje.
  - Proporciona confidencialidad e integridad.
  - Tipos:
    - Simétrico → misma clave para cifrar y descifrar
      - Ejemplos: 3DES (obsoleto), AES…
    - Asimétrico → par de clave, si con una se cifra, con la otra se descrifra.
      - Firma digital → proporciona verificación (no repudio).
      - Otros ejemplos: Diffie-Hellman (usado para generar claves entre dos extremos en red).



Técnicas y medidas de seguridad (II)

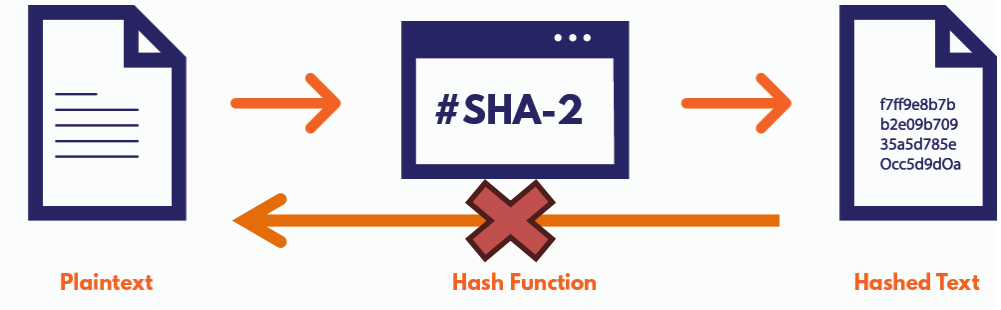
- Cifrado (continuación):
  - Asimétrico (cont.):
    - Firma digital (cont.):
      - Cada usuario tiene un par de claves: privada (sólo la conoce él) y una pública (la conoce cualquiera).
      - Hay una Autoridad de Certificado (CA) → de confianza.
        - Proporciona el par de certificados / revoca el par de certificados.
        - Puede existir una cadena de confianza entre CA → E.g. una CA emite certificados a otra CA que emite tu certificado.
      - Hay una Autoridad de Registro (AR) → de confianza.
        - Asocia el par de claves a la identidad del usuario.
        - A veces, CA y RA pueden ser la misma entidad.
      - En la firma del documento, se realiza un *Hash* del mismo y éste se firma con la clave privada del firmante. El resultado es la firma, que se añade al documento.



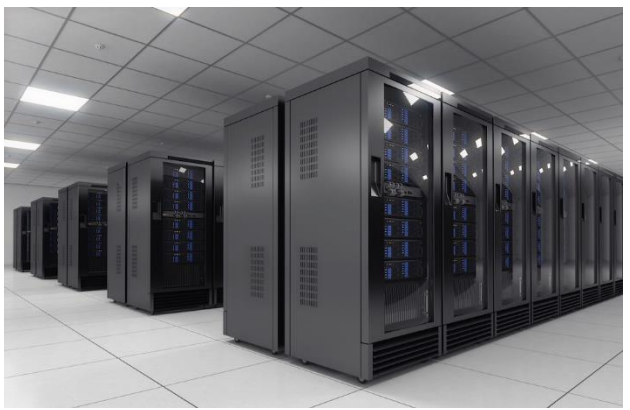


Técnicas y medidas de seguridad (III)

- Funciones *hash*:
  - Funciones resumen.
  - Funcionan en una única dirección.
  - Proporcionan confidencialidad e integridad.
  - Ejemplos: MD5, SHA-1, SHA-2, SHA-3…

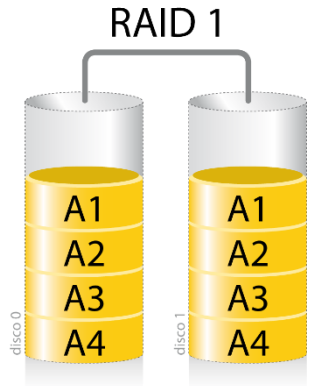


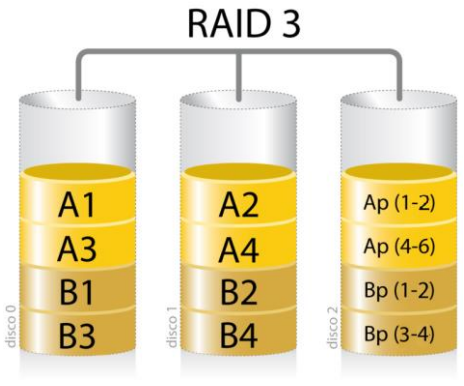
- Protección física:
  - SAI (Sistemas de Alimentación Ininterrumpida).
  - En el CPD (Centro de Proceso de Datos), además:
    - Control de temperatura y humedad.
    - Control de accesos físicos.
    - Medidas contra incendios
    - …

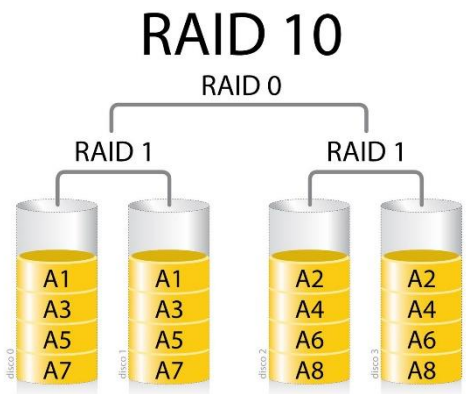


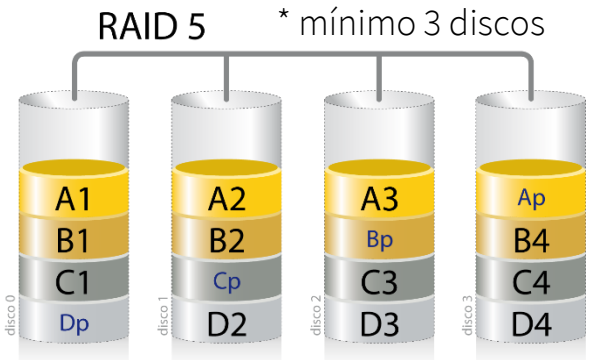
Técnicas y medidas de seguridad (IV)

- Sistemas RAID:
  - Proporcionan disponibilidad (y más cosas).
  - RAID 1.
  - RAID 3.
  - RAID 5.
  - RAID 10.
- Formación del personal.
- Monitorización del sistema.
  - Logs.
  - Rendimiento.









Técnicas y medidas de seguridad (V) y…

- Cuentas de usuario y permisos:
  - Usuario/Contraseña… ¿otras formas?
  - Proporciona autorización.
- Copias de seguridad:
  - Proporcionan disponibilidad.
  - Diferentes técnicas (3-2-1), distintos tipos de copias de seguridad, etc.
  - Tipos:
    - Completa.
    - Incremental → realiza copia de los archivos que han cambiado desde la última completa.
    - Diferencial → realiza copia de los archivos que hayan cambiado desde la última copia (ya sea completa o incremental o diferencial).

https://www.xataka.com/componentes/discos-duros-acaban-fallando-puedes-evitar-desastre-estrategia-3-2-1-backups-1

Redes

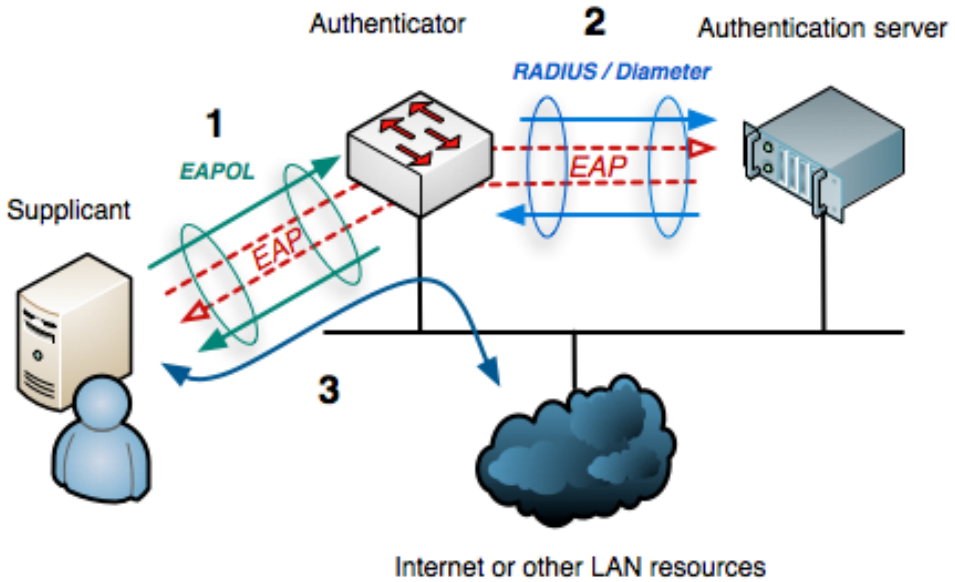
Protocolos seguros

- SSL/TLS:
  - Proporciona confidencialidad, integridad y autenticación a la comunicación → cifrado y certificados.
    - Para ser usado con TCP.
    - Alternativa para UDP → DTLS (*Datagram TLS*).
  - SSL (*Socket Secure Layer*) → obsoleto.
  - TLS (Transport Secure Layer) → actual, versión 1.3.
- HTTPS:
  - HTTP seguro → puerto 443.
  - Utiliza SSL/TLS.
- RADIUS / Diameter:
  - Proporcionan servicios de AAA (*Authentication, Authorization, Accounting*).
  - Arquitectura Cliente/Servidor.

SSL/TLS

Seguridad en redes cableadas

- Redes cableadas → Ethernet.
  - Uso del protocolo de autenticación 802.1X.
    - Controla el acceso a la red por puerto del dispositivo de red.
    - Involucra servidor de autenticación.
    - Ejemplo de uso: el cliente (ordenador conectado a un puerto del *switch*), quiere acceder a la red → Presenta credenciales al *switch* → el *switch* comprueba credenciales usando RADIUS/Diameter → el servidor de autenticación responde al *switch* con los permisos de acceso a la red del usuario → el *switch* actúa en consecuencia (permite o prohíbe acceso).

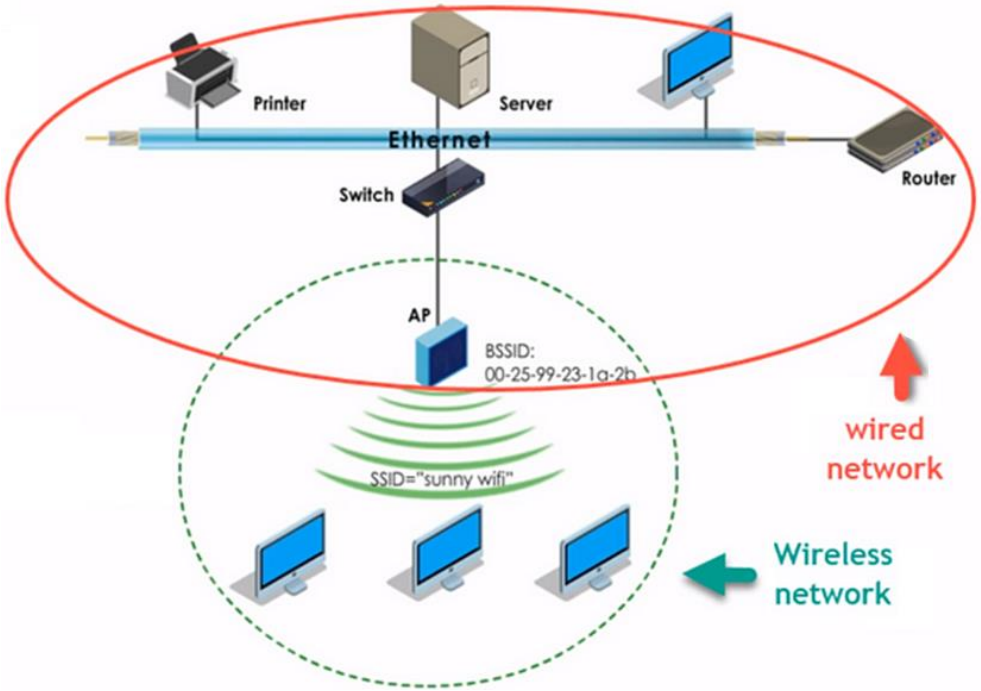


Seguridad en redes inalámbricas

- Redes inalámbricas → WiFi.
  - Uso de protocolos seguros para asegurar la comunicación inalámbrica:
    - WEP: clave simétrica de 68 o 128 bits. Muy poco robusta. No usar.
    - WPA:
      - Mejora la seguridad de WEP, generando claves dinámicas (de 128 bits) por cada paquete.
      - Tipos:
        - WPA-Personal (WPA-PSK, *Pre-Shared Key*) → usa una clave compartida de 256 bits para generar las claves temporales.
        - WPA-Enterprise (WPA-EAP, *Extensible Authentication Protocol*) → incluye autenticación de usuarios (802.1X) y mejoras del uso de las claves (no contraseñas cortas, diccionario de contraseñas…).
      - Versiones siguientes: WPA2 (AES), WPA3 (reemplaza intercambio de claves pre-compartidas).

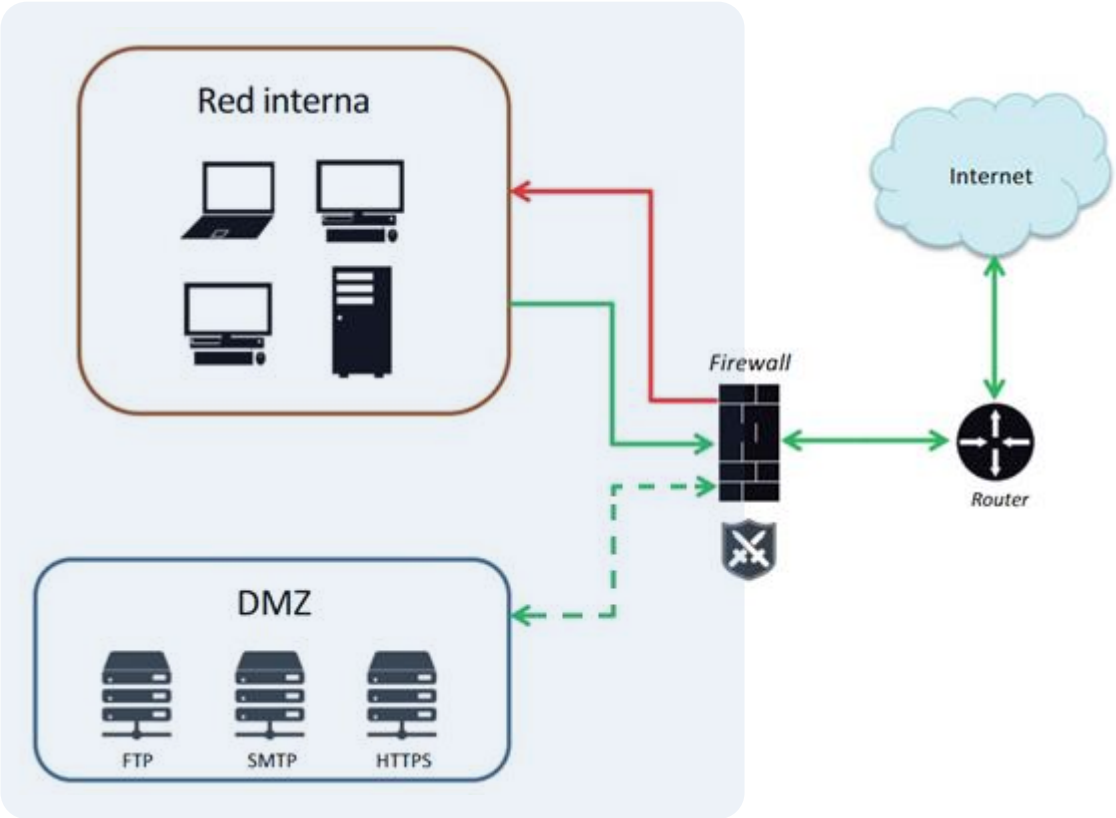
Seguridad en redes inalámbricas (II)

- Además de los protocolos de cifrado y autenticación, otras medidas para aumentar la seguridad:
  - Filtrado de MAC → se indica qué direcciones MAC tienen acceso a la WiFi.
  - Desactivar la difusión del SSID (identificador o nombre de la WiFi).
  - Cambiar el SSID y la contraseña que vienen por defecto con el *router*.
  - Cambiar la contraseña por defecto para el acceso a la página web del *router*.
  - WPS (*WiFi Protected Setup*) → para facilitar el acceso a la red (PIN, botón NFC…). Inseguro.



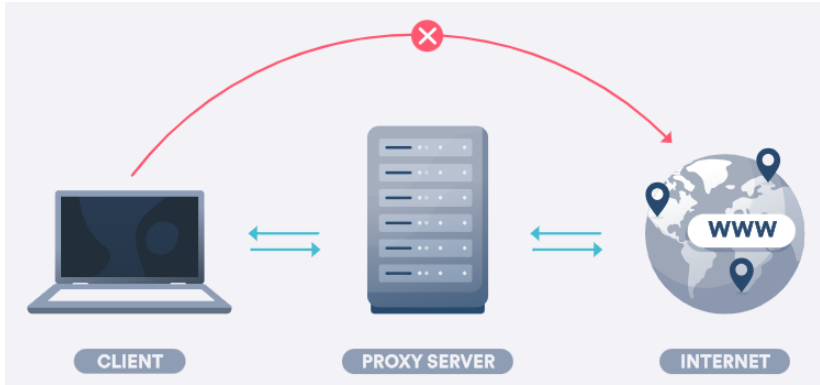
Firewall

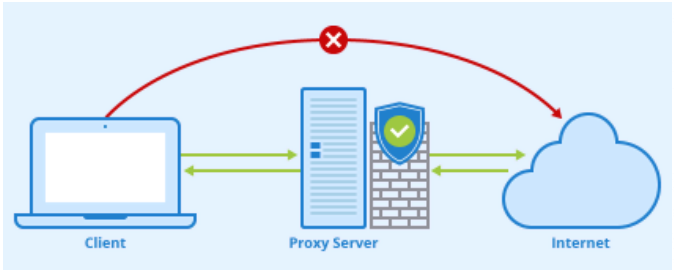
- Elemento "*hardware*" especializado.
  - Muchas veces, se utiliza *router* con *firewall* integrado.
- Proporciona protección a la red, impidiendo accesos no autorizados a la misma y permitiendo el tráfico autorizado.
  - Los más avanzados pueden inspeccionar trafico (antivirus), romper túneles cifrados…
- DMZ: zona aislada de la red a la que se puede acceder desde el exterior.

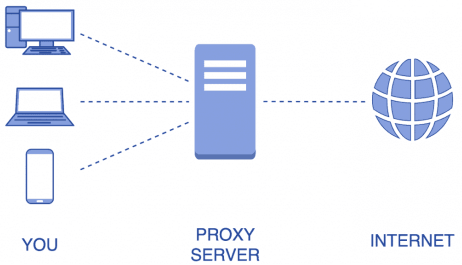


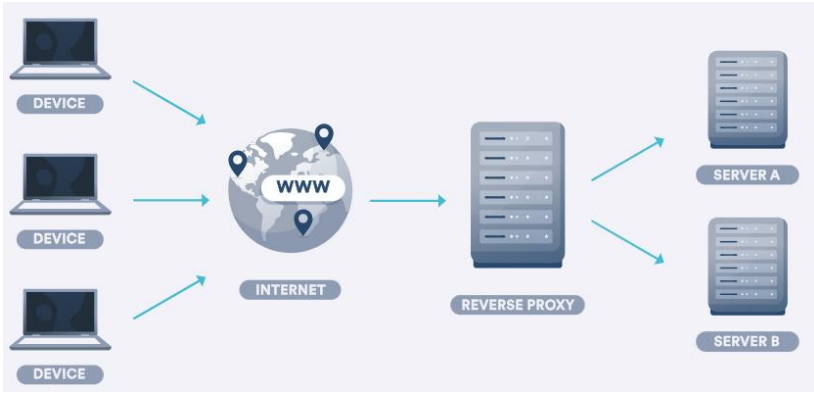
Proxy

- Hace de intermediario entre un solicitante y un destino.
- Posibles funcionalidades:
  - Forzar el paso del tráfico por el *proxy*.
    - Control y *log* del tráfico → seguridad.
    - Empleo a modo de *caché* → E.g.: si se accede mucho a una
  - Enmascarar geolocalización del cliente.
  - Balanceo de carga en servidores.



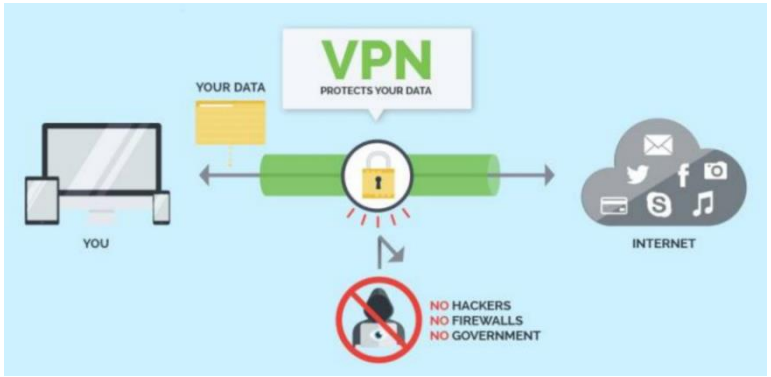






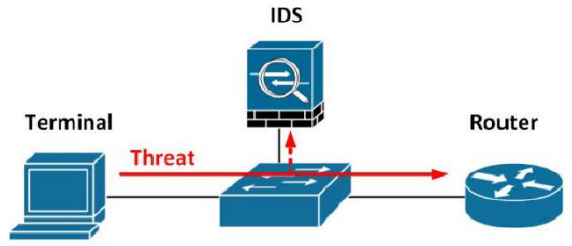
VPN

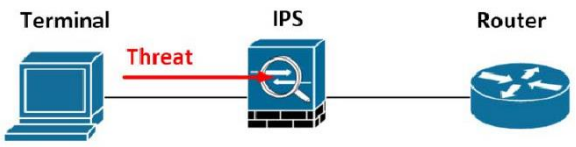
- Utiliza redes públicas para crear conexiones como si fueran a través de redes privadas.
- Establecen un túnel entre origen y destino:
  - Autenticación para acceder al túnel.
  - Cifrado de todo lo que circula por el túnel.
- Las conexiones pueden ser:
  - Entre redes → E.g. entre sedes corporativas distantes.
  - Entre ordenador y red → E.g. ordenador de un trabajador en *home office* que accede a la red corporativa como si estuviera allí.
  - Entre ordenadores.
- *Software* usual para hacer tu VPN:
  - OpenVPN, Wireward.

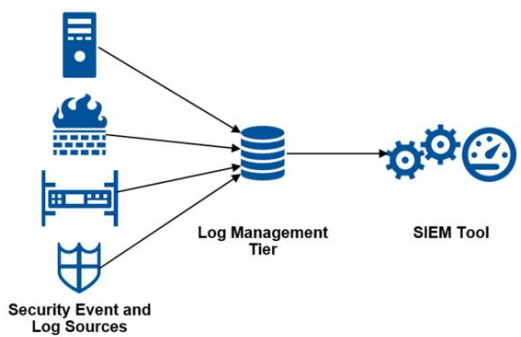


IDS / IPS / SIEM

- IDS (*Intrusion Detection System*)
  - Sistema pasivo que detecta accesos no autorizados a equipos o redes → busca intrusiones y, si las detecta, emite alarma.
- IPS (*Intrusion Prevention System*)
  - Sistema activo que protege de intrusiones→ busca intrusiones (ataques, malware…) y, si las detecta, actúa para detenerla.
- SIEM (*Security Information and Event Management*)
  - Es un sistema que centraliza la gestión de la información y alertas de seguridad en tiempo real, generadas por los distintos dispositivos *hardware* y *software* de la red.
  - Relaciona dicha información, detecta eventos de seguridad (eliminando falsos positivos) y actúa en consecuencia.







Source: Gartner (October 2016)

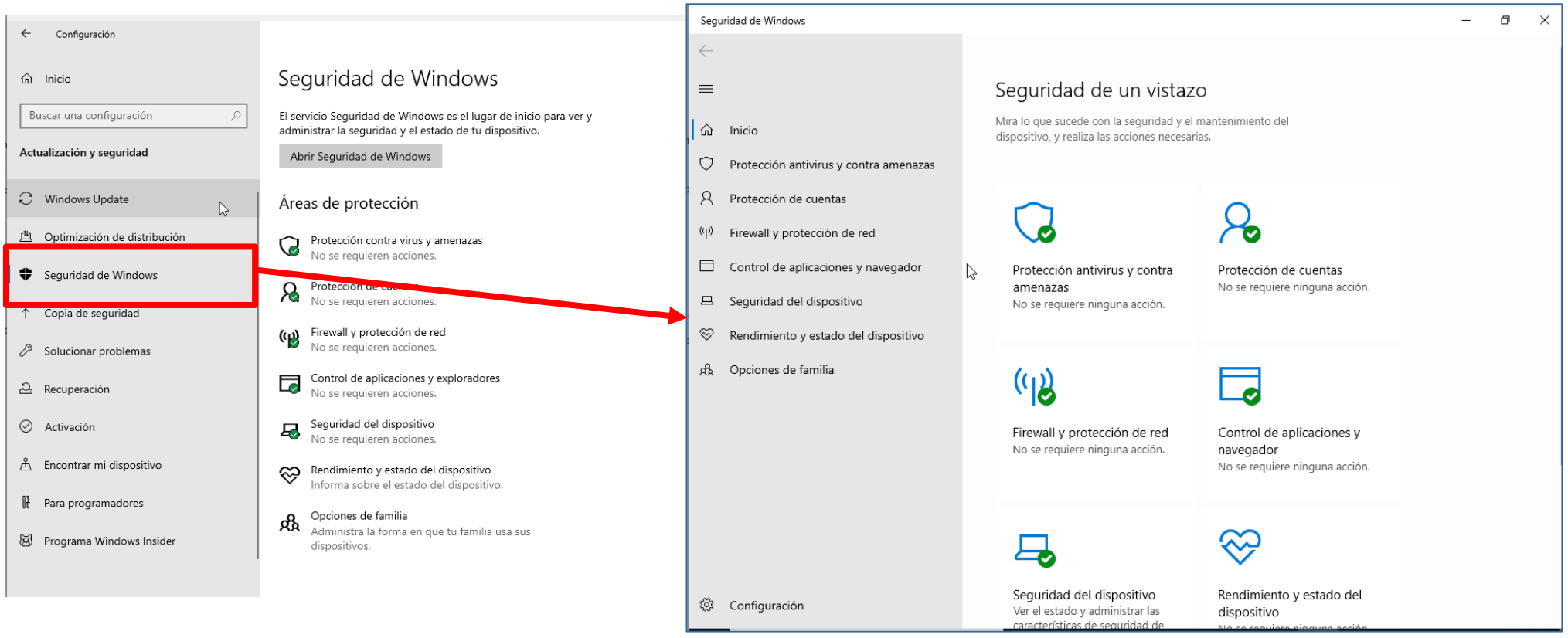
Windows

Seguridad en Windows 10

El sistema operativo Windows 10 ofrece características de seguridad informática:

- Antivirus.
- Protección de cuentas (acceso a las sesiones de usuario).
- Permisos de acceso al sistema de archivos.
- *Firewall*.
- Control de aplicaciones y navegador → para proporcionar seguridad en línea (e.g. archivos, aplicaciones y sitios web).
- Opciones de control parental.

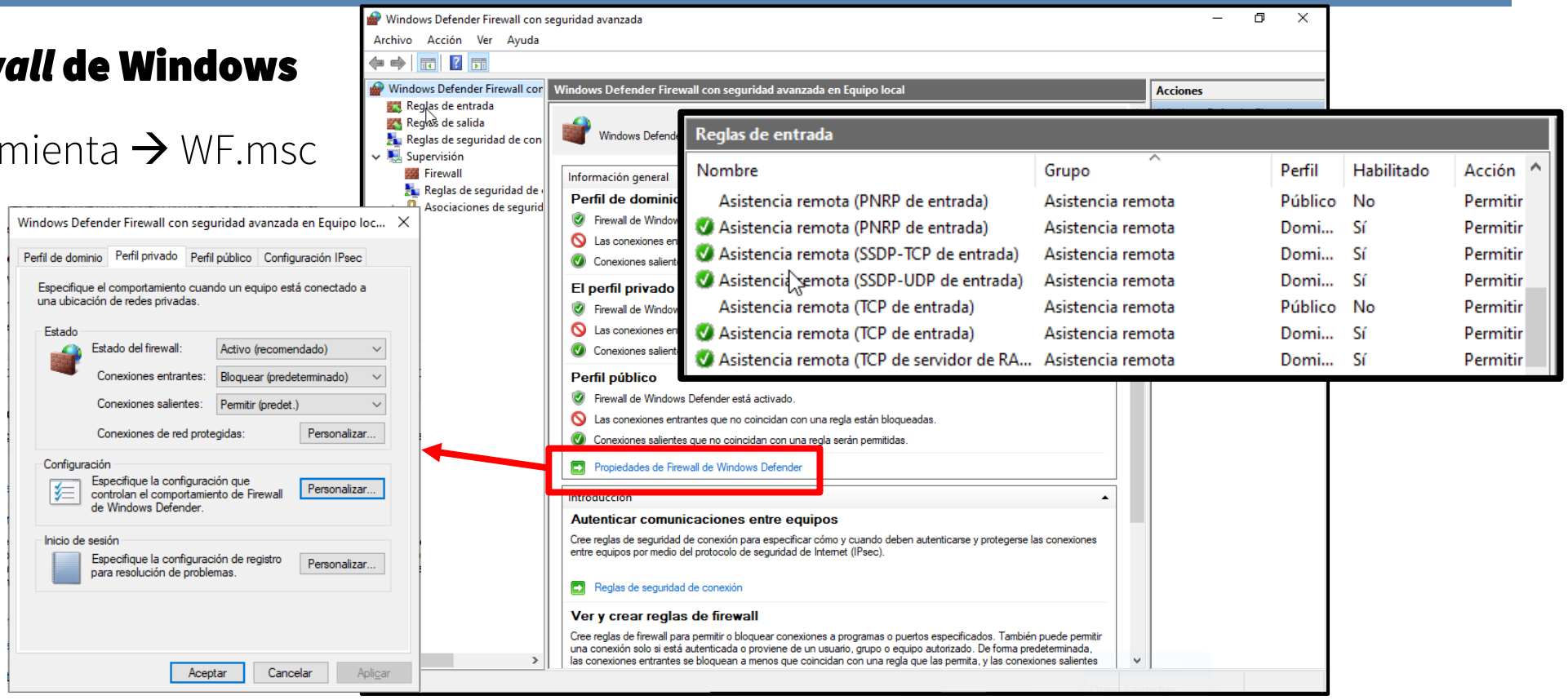
Seguridad en Windows 10 (II)



Seguridad en Windows 10 (III)

Firewall de Windows

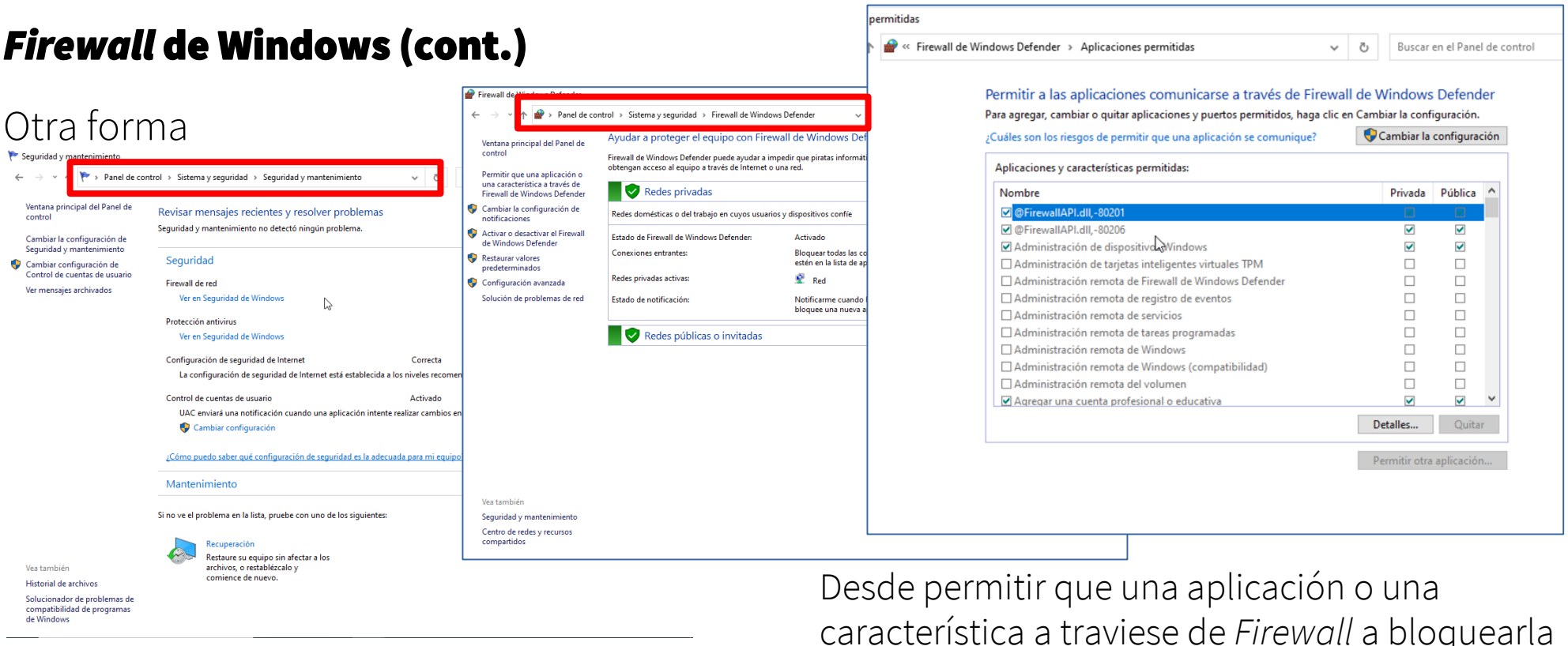
Herramienta → WF.msc



Seguridad en Windows 10 (IV)

Firewall de Windows (cont.)

Otra forma



Desde permitir que una aplicación o una característica a traviese de *Firewall* a bloquearla

Permisos

Permisos → privilegios asignados a un usuario con los que se concede (**permitir**) o deniega (**denegar**) el acceso a recursos (reglas de acceso), locales o de red.

- Denegar tiene preferencia sobre permitir.
- El usuario administrador puede modificar los permisos sobre todos los elementos del sistema.

	Tipo de permiso NTFS	Tipo de acceso permitido
Básicos	Mostrar el contenido de una carpeta	Permiten ver el contenido de la carpeta, la recorre y ejecuta archivos (sólo aplicado a carpetas)
	Lectura	Permiten ver el contenido de carpetas y archivos
	Lectura y ejecución	Permiten ver el contenido de carpetas y archivos y ejecutar programas
	Escritura	Permiten crear nuevos archivos y carpetas, así como realizar cambios en los existentes
	Modificar	Permiten leer y escribir archivos y carpetas. No puede borrar archivos ni subcarpetas, cambiar permisos ni tomar posesión del archivo o carpeta.
	Control total	Permiten realizarlo todo
	Permisos especiales	Permisos NTFS proporcionan un control de acceso más fino (ejemplo de opciones avanzadas: sincronizar, tomar posesión de archivos/carpetas, con el permiso “Modificar” no permitir que se eliminen archivos, etc.)

Permisos (II)

Special permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

- Predeterminadamente, las carpetas heredan los permisos de su carpeta principal.
- El usuario tendrá acceso a carpeta o archivo al que se le haya dado permiso (también grupos).
- Los permisos son acumulativos (también grupos).
- El usuario que crea un archivo o carpeta es el dueño de ese objeto y puede definir sus permisos para controlar el acceso.

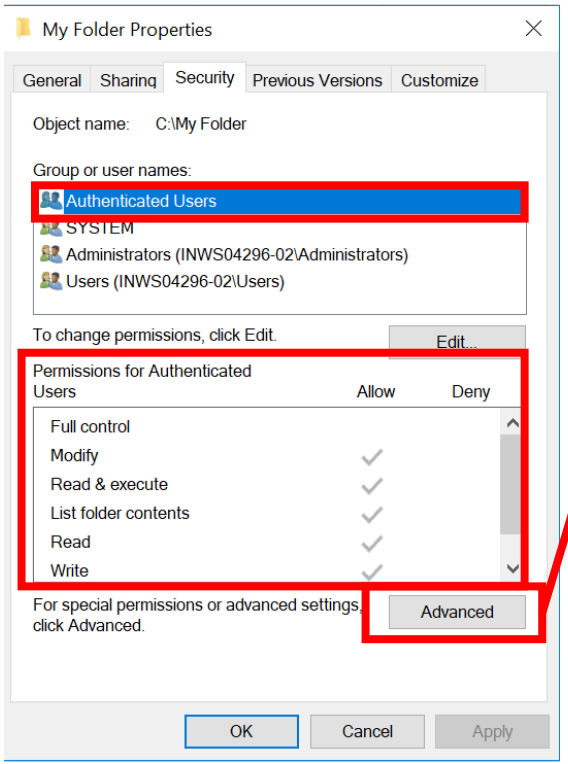
http://ntfs.com/ntfs-permissions.htm

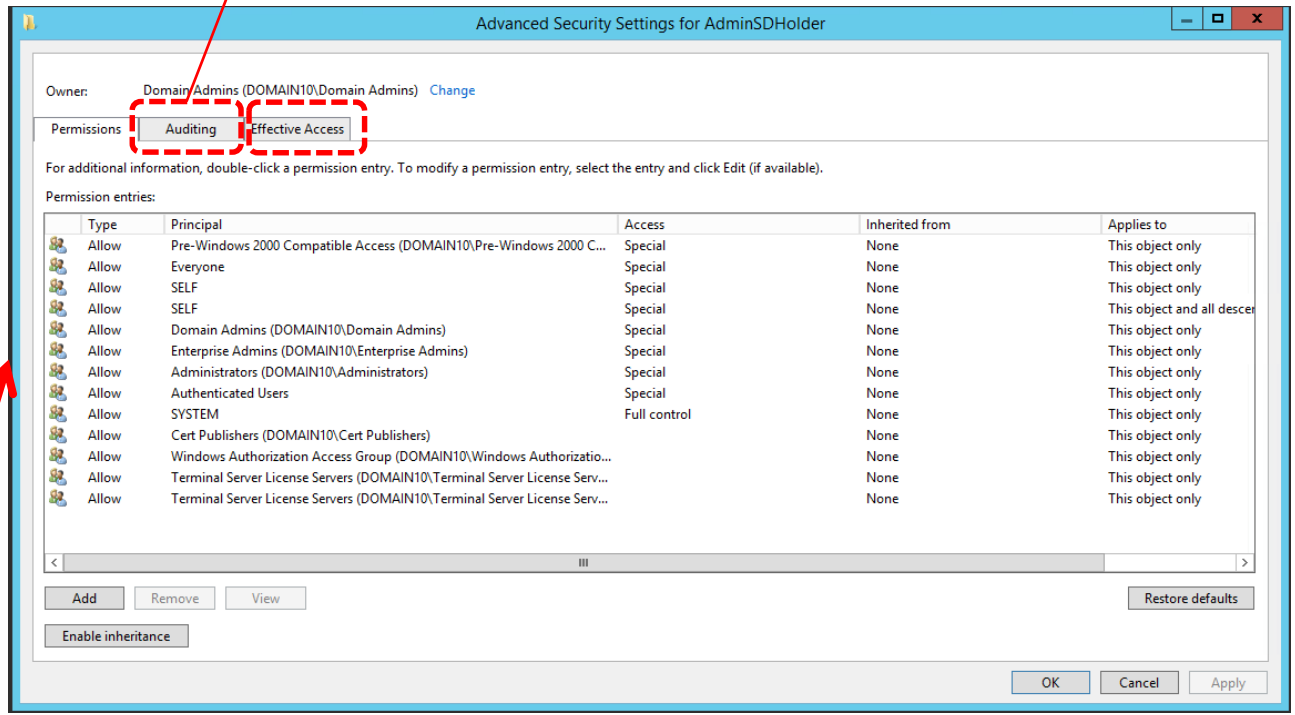
https://www.firatboyan.com/en/windows-server-2019-ntfs-sharing-sharing-permissions-file-folder-authorization-part-2.aspx

Permisos (III)

Permisos NTFS

Permite configurar y consultar si se ha accedido al objeto

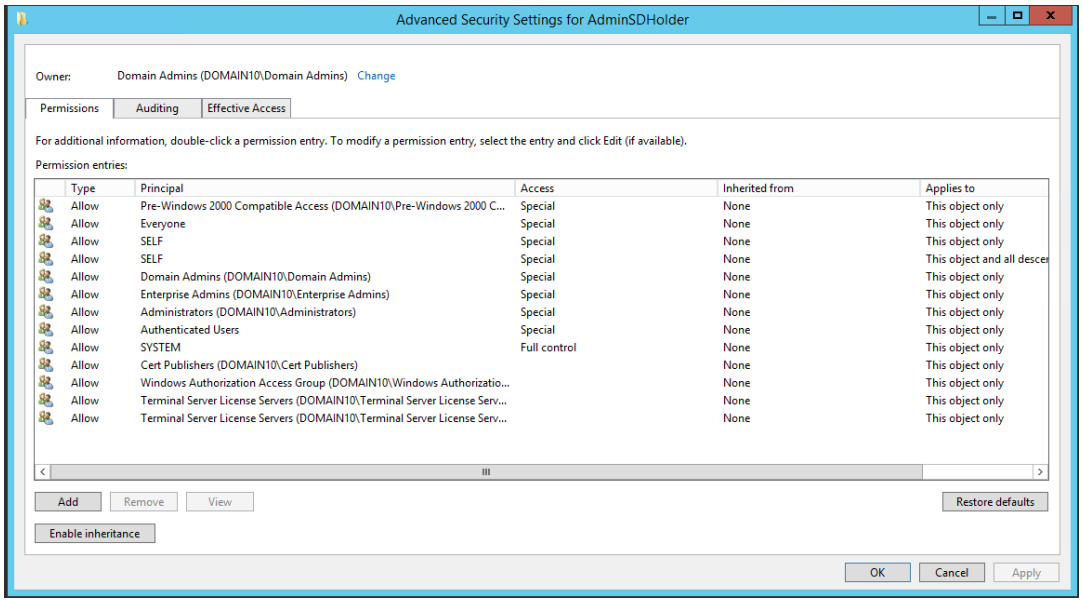




Listas de Acceso

Lista de acceso (**ACL**):

- Sirven para ampliar el control sobre los permisos asignados y el acceso de los usuarios a los distintos recursos.
- Es una lista de Entradas de Control de Acceso (**ACE**).
- Cada ACE de una ACL identifica a un usuario de confianza y especifica los **derechos de acceso** concedidos, denegados o auditados para dicho usuario.



Tipos de ACL:

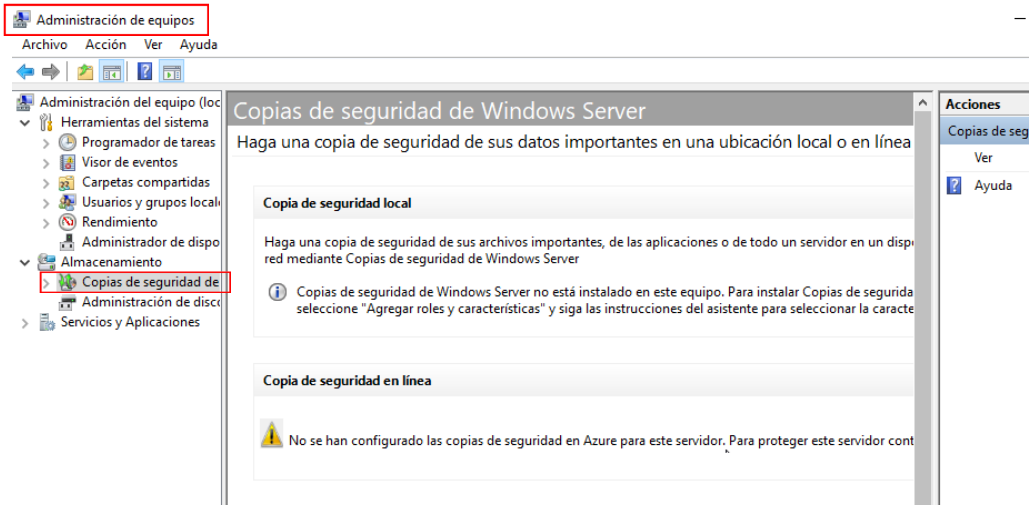
- DACL (*Discretionary* ACL): identifica a usuarios y grupos a los que se les permite (o deniega) el acceso a un objeto.
- SACL (*System* ACL): permite a los administradores registrar (auditar) intentos de acceso a un objeto.

CMD:

- icacls → Muestra, modifica, hace copias de seguridad o restaura ACL para archivos y directorios.

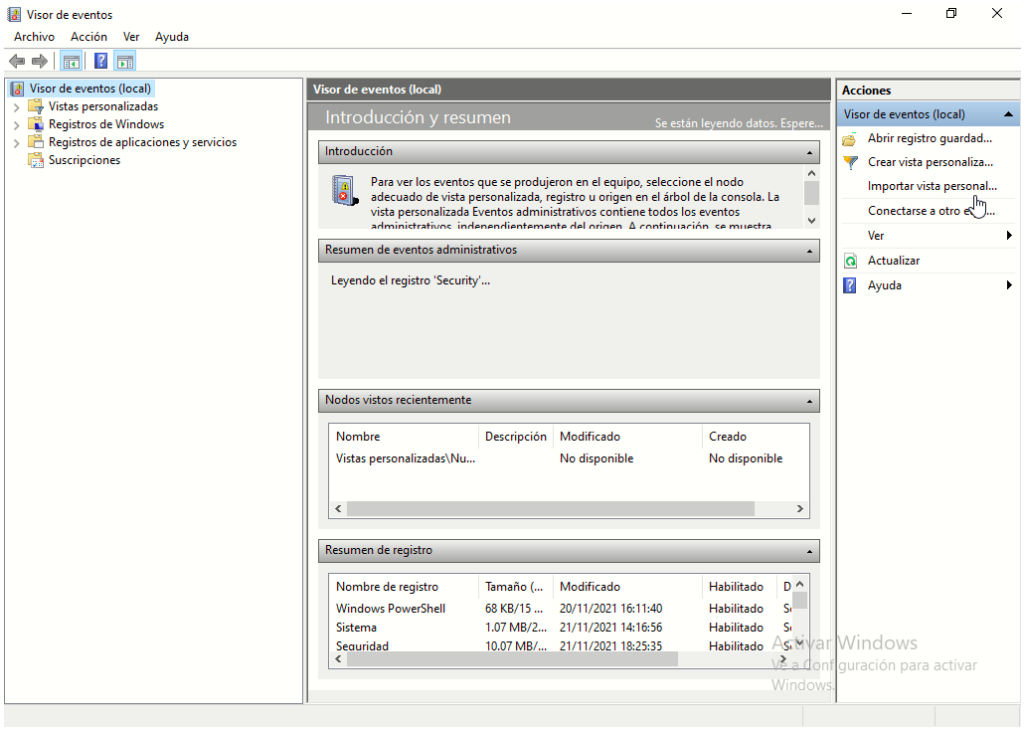
Backups

- Puntos de restauración → Copias de seguridad de elementos importantes de Windows (copia parcial del sistema) que el SO realiza de forma automática (también pueden realizarse manualmente).
- Imagen del sistema → Copia completa del sistema en el momento de realización de la imagen.
- En Windows Server → Windows Server *Backups*.
  - Requiere instalar el rol de *backup*.
  - También desde "Administración de Equipos" → "Copias de seguridad de Windows Server"



Logs

- En Windows → Visor de eventos
  - Permite ver los *logs* de eventos que ocurren en el sistema:
  - Herramienta: eventvwr.msc
  - Tipos de eventos (Windows):
    - Aplicación
    - Seguridad
    - Instalación
    - Sistema

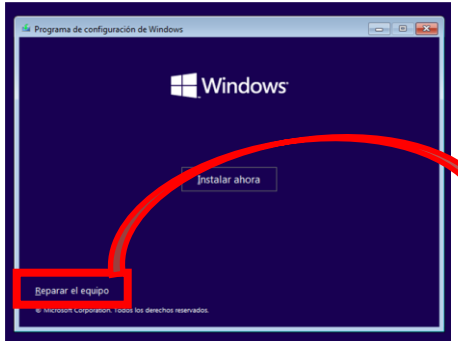


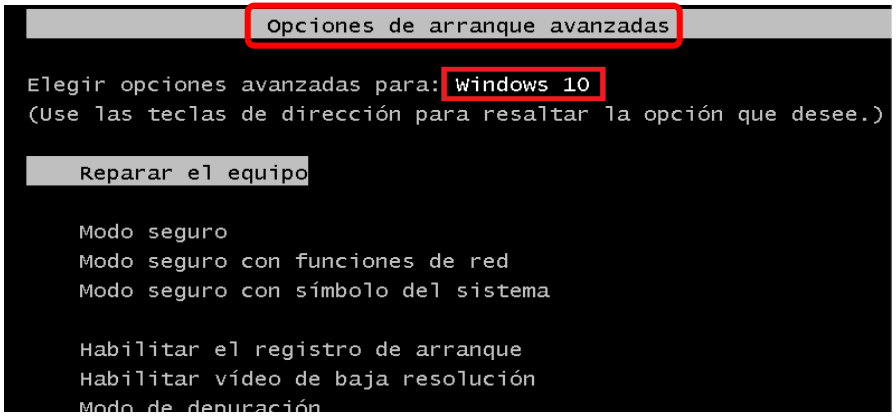
https://www.solvetic.com/tutoriales/article/3392-como-abrir-usar-visor-eventos-windows-10/

https://www.lepide.com/how-to/track-who-read-files-on-your-windows-file-servers.html

Recuperación del Sistema Operativo

- Unidad de recuperación → Unidad externa al ordenador en la que hay una copia del SO y de los *drivers* esenciales
  - Permite reparar o restablecer el sistema en caso de problema.
- WinRE → Entorno de recuperación de Windows.
  - Desde la ISO de Windows.
- Opciones de arranque avanzadas:
  - Una manera de acceder: pulsando F8 en el arranque del SO.
  - Algunas de las opciones:
    - Reparar el equipo.
    - Modo seguro.
    - La última configuración buena conocida.

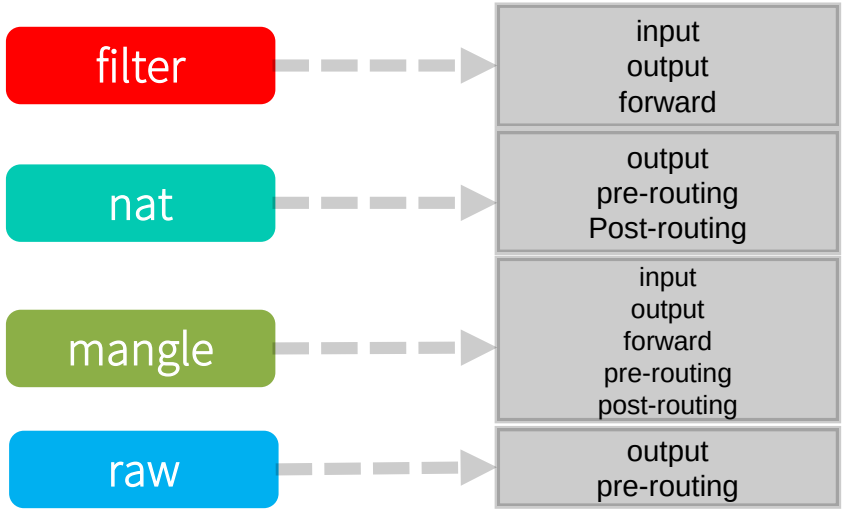




Linux

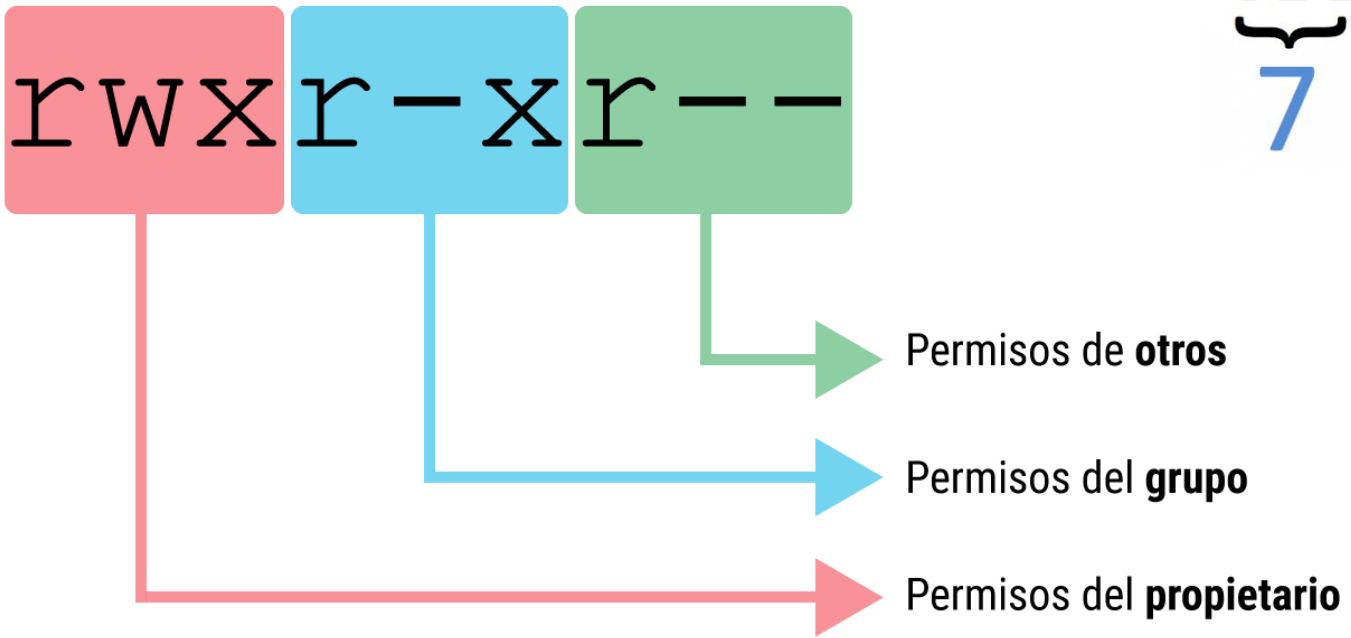
Firewall

- iptables:
  - Filtrado de paquetes según determinadas características (dirección origen, puertos, etc.)
  - Parte de Netfilter (*framework* de Linux para realizar operaciones relacionadas con el *networking*)
  - Mediante CLI. También se puede configurar desde Webmin, etc.
  - Utiliza tablas:
    - *filter* → filtrado de paquetes ("*firewall*").
    - *mangle* → manipula cualquier campo del paquete.
    - *nat* → realiza NAT.
    - *raw*, *security*.
  - ¿Qué se hace con los paquetes?
    - ACCEPT, DROP, REJECT…
  - Sucesor (futuro) → nftables.



Permisos en el sistema de ficheros en Linux (recordatorio)

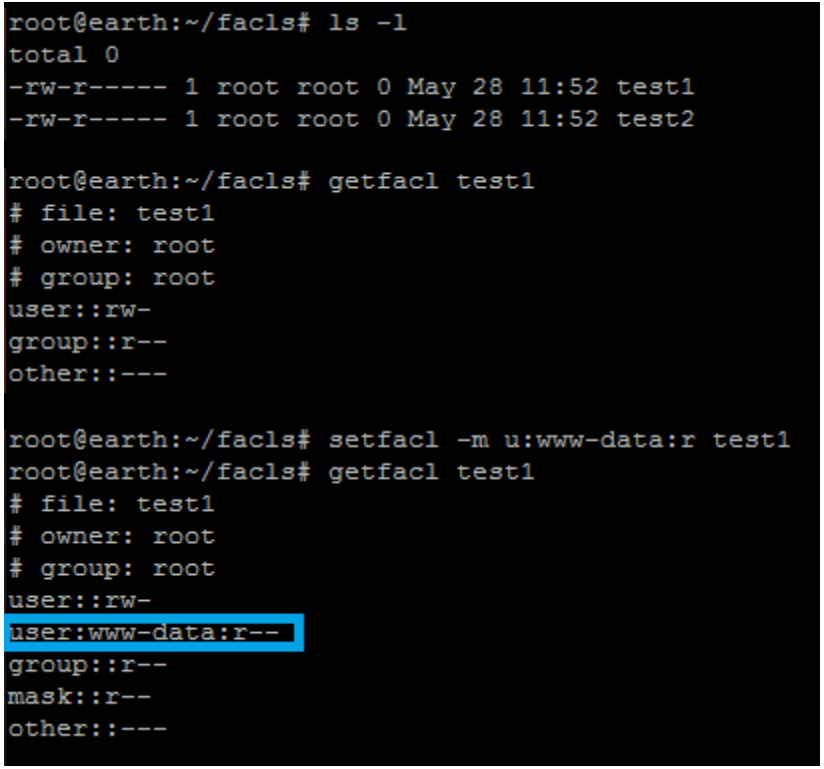
r = *read*
w = *write*
x = *eXecute*



Número Octal	Equivalente en texto	Valor binario
0	- - -	000
1	- - x	001
2	- w -	010
3	- w r	011
4	r - -	100
5	r - x	101
6	r w -	110
7	r w x	111

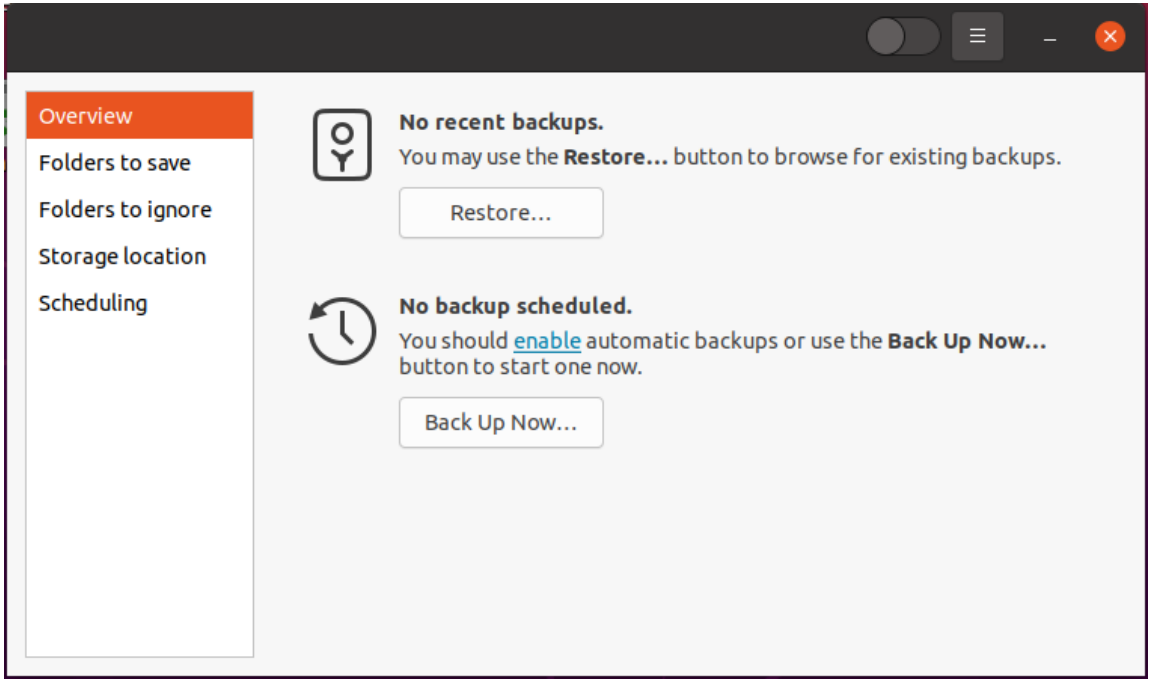
Listas de Control de Acceso

- ¿Qué sucede si queremos proporcionar una gestión de permisos más precisa, por ejemplo involucrando explícitamente otros usuarios o varios grupos? → ACL
- Para poder utilizarlas en Linux, éstas deben estar habilitadas en los sistemas de archivos.
  - En EXT4 viene habilitada por defecto.
- Además, necesita tener instalado el software que las gestiona.
  - sudo apt install acl
  - Acciones:
    - getfacl
    - setfacl



Backups (recordatorio)

- A lo fácil → mediante GUI
  - Aplicación en la distro: Backups (*Déjà Dup Backup Tool*)
  - Otras aplicaciones: grsync, SimpleBackupSuite…
- A lo *hardcore* → mediante CLI
  - con **tar + crond**



https://help.ubuntu.com/community/BackupYourSystem

Logs (recordatorio)

- *Logs* → Registros de eventos
  - •De sistema
  - •De aplicaciones
- Demonios:
  - •Systemd-journald
  - •Rsyslog
- Directorio → /var/log
  - •/var/log/syslog → contiene la mayor cantidad de información
    - •syslog.1.gz, syslog.2.gz, etc.
  - •/var/log/kern.log → registro del *kernel*
  - •/var/log/dmesg → *diagnostic message* (mensajes del núcleo: arranque del sistema, detección del hardware, depuración de aplicaciones, etc.).
    - •dmesg.1.gz, dmesg.2.gz, etc.
  - •/var/log/auth.log → registro de autenticación de usuario
  - •/var/log/… → de otras aplicaciones

https://www.ubuntizando.com/como-enviar-logs-de-linux-a-un-servidor-remoto/

https://debian-handbook.info/browse/es-ES/stable/sect.syslog.html

Recuperación del Sistema Operativo (recordatorio)

Medios de recuperación del sistema operativo (entre otros):

Comando (CLI):

- fsarchiver → comando para realizar la copia de seguridad completa del sistema
  - Requiere realizar la copia de seguridad antes del posible *crash* del sistema
  - https://www.ubuntizando.com/como-crear-copias-de-seguridad-con-fsarchiver-en-linux/

CD/DVD:

- SystemRescue → distribución de Linux para reparar un sistema que no arranca o está dañado
  - Contiene herramientas para dicha función → Gparted, fdisk, TestDisk (para recuperación de datos), etc.

Clonado del equipo:

- Clonezilla → *software Open-Source* en forma de *LiveCD* que permite crear una imagen del sistema para poder recuperarlo después

Herramientas *software* más utilizadas

Comandos y aplicaciones

- nmap:
  - Herramienta para descubrir la red → *hosts*, puertos abiertos, etc.
- Whireshark:
  - Aplicación para capturar tráfico que circula por la red.
  - Con GUI.
  - Divide la información del paquete por protocolos, indicando el contenido de sus cabeceras.
  - Muestra el contenido del paquete (datos que porta el paquete).