Asignatura

Sistemas informáticos

UNIDAD 6
Gestión de recursos en una red

UNIVERSAE
Instituto Superior de FP

Permisos

Los derechos o privilegios de los usuarios son atributos que afectan a una cuenta de usuario o a un grupo con la función de permitir realizar ciertas acciones sobre todo el sistema y no un solo recurso.

Por otra parte, los permisos son características propias de cada recurso en concreto (o conjuntos de recursos aglomerados en otro), en el que se dirá que usuarios o grupos pueden trabajar con estos recursos y que acciones pueden realizar sobre estos.

Todos los sistemas Windows asocian a los usuarios un *Security Access Token o SAT*.

Dentro de los permisos NTFS, nativos de Windows, existen los permisos NTFS especiales y los permisos NTFS estándar.

Dentro del SAT se almacena:

- El SID.
- La lista de SID de los grupos.
- La lista de derechos del usuario.

Herencia de permisos en Windows

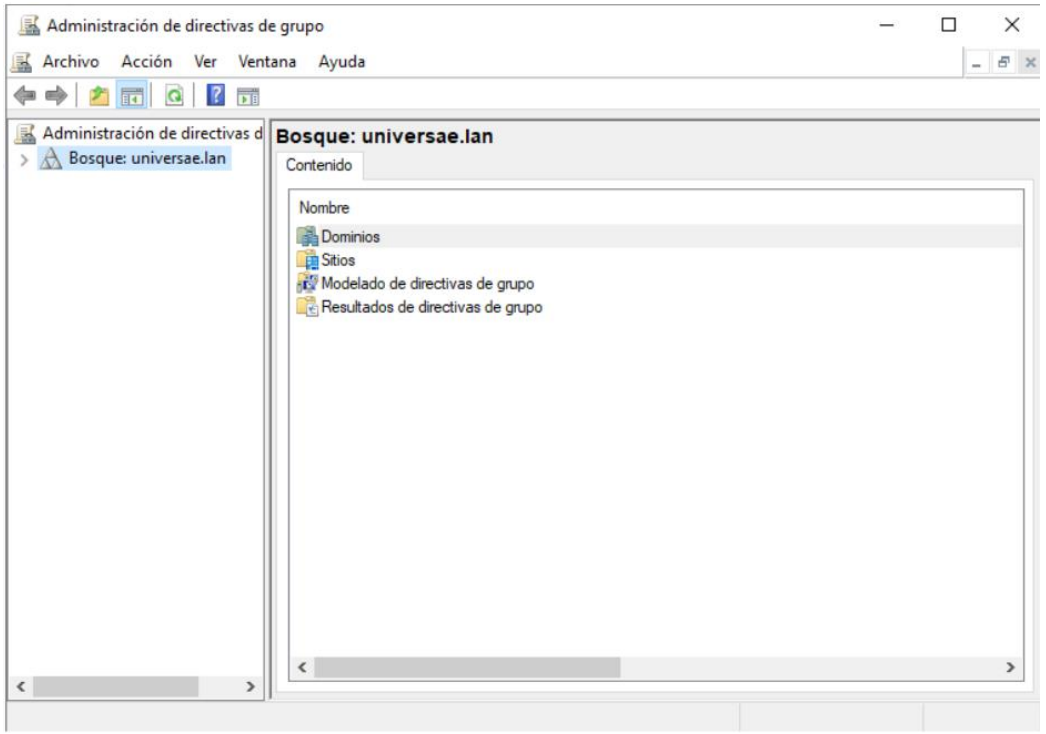
En los permisos NTFS de Windows hablamos de herencia como el mecanismo mediante el cual, cuando se crea un directorio o fichero dentro de otro directorio, se aplican los permisos que tenía el directorio padre a no ser que se deshabilite dicha herencia.

ACL en sistemas Windows

Todos los sistemas Windows con NTFS cuentan con los siguientes atributos de protección:

- El SID del propietario.
- La lista de control de acceso de protección o ACL:
    - Dentro de cada ACL existen dos DACL, lista de control de acceso discrecional, debido a la herencia.
- La lista de control de acceso de seguridad.

Derechos de usuarios y directivas de seguridad



Tenemos dos tipos principales de derechos en Windows:

- Derechos de conexión:
    - Denegar el acceso desde la red a este equipo.
    - Permitir el inicio de sesión local.
- Privilegios, algunos ejemplos son:
    - Añadir equipos a un dominio.
    - Cambiar la configuración del sistema.
    - Impedir la instalación de controladores de dispositivos

Las directivas de seguridad en Windows son una serie de normas donde se refleja el comportamiento que debe de tener el equipo en todo lo referente a seguridad y existen dos tipos principales:

- Directivas de seguridad local:
    - Menú de inicio → Herramientas administrativas → Directivas de seguridad local
- Directivas de seguridad de dominio:
    - Inicio → Herramientas administrativas → Administración de directivas de grupo.
    - Además, dentro de estas, existen las directivas de seguridad del controlador de dominio.

Servidores

Aunque existen multitud de servidores que se pueden implementar, los tres más interesantes para un desarrollador son:

- Servidor de ficheros.
- Servidor de impresión.
- Servidor de aplicaciones

Conexión remota. Herramientas

El término administración remota hace referencia a la realización de acciones desde un equipo que manejamos pero que realmente se ejecutan en otro equipo al que no podemos acceder de manera física. Las tres principales herramientas para la administración remota son:

- Servicios de escritorio remoto.
- Escritorios remotos.
- Asistencia remota.

Herramientas de seguridad

Cifrado

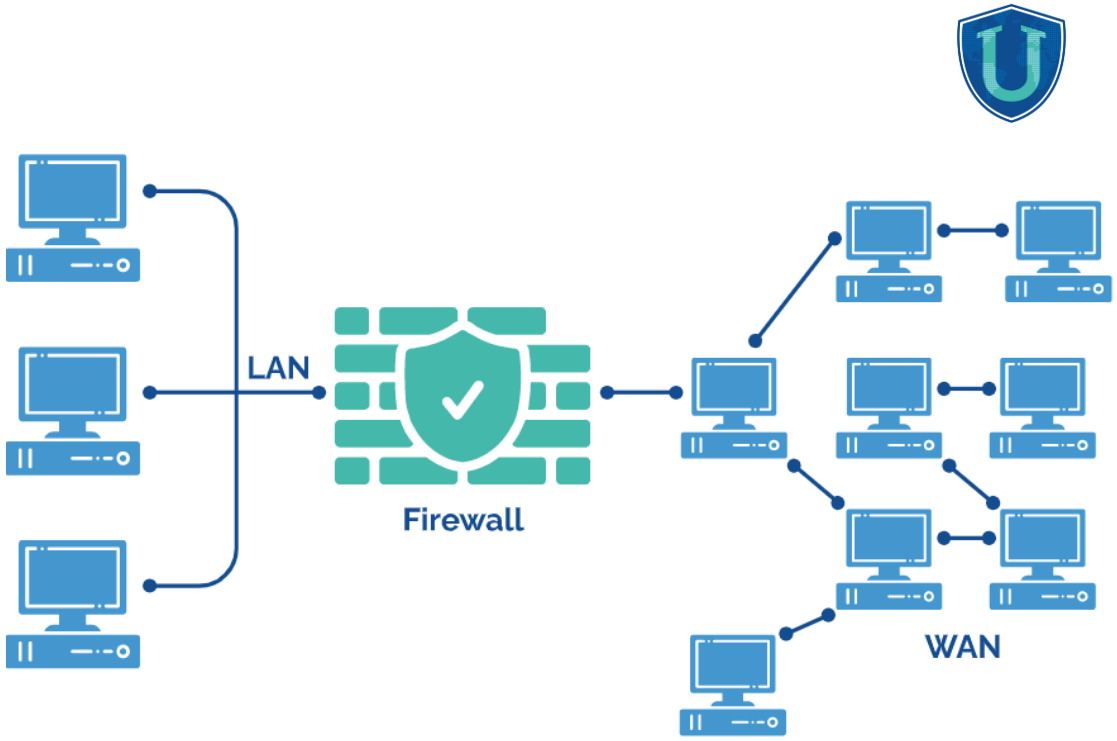
- Algoritmos simétricos o de clave privada.
- Algoritmos asimétricos o de clave pública.

Principales algoritmos de cifrado

- Simétricos: DES, TDES, RC2, ICE, IDEA, **AES** y Blowfish.
- Asimétricos: **RSA, DSA** y ECC.

Cortafuegos

Dispositivo o *software* encargado de filtrar el tráfico de red entrante, también llamados *firewalls*.



UNIVERSAE

CHANGE YOUR WAY