# Síntesis conceptual

| |
|---|
| **Grado**: Desarrollo de Aplicaciones Multiplataforma |
| **Asignatura**: Síntesis Conceptual |
| **Unidad**: 6. Gestión de recursos en una red |

## Resumen

Los usuarios de Windows tienen derechos o privilegios asociados para poder realizar o no ciertas acciones en el sistema. También cuentan con permisos que se asocian a recursos concretos del sistema. El mismo sistema asocia a los usuarios una acreditación llamada *Security Access Token (SAT)*, que dentro está compuesto por:

- El *SID* del usuario.
- La lista de los *SID* de los grupos a los que pertenece
- La lista de los derechos que tiene el usuario

Los permisos de los recursos son diferentes a los permisos NTFS del sistema, y dentro de los permisos NTFS, debemos diferenciar entre especiales y estándar. Hemos visto durante el tema, además, como realizar una compartición de recursos por red, y que hay dos métodos. Cuando compartimos un directorio en red, debemos de tener en cuenta su herencia, por si está o no deshabilitada.  Otro aspecto para tener en cuenta son los atributos de seguridad asociados a los recursos del sistema, que son:

- El SID del propietario.
- La lista de control de acceso de protección o ACL.
- La lista de control de acceso de seguridad o SACL.

Los derechos del sistema pueden ser o derechos de conexión, que son sobre todo el denegar el acceso desde la red a un equipo o el permitir el inicio de sesión local en un equipo; o privilegios, pero en este caso, solo se pueden llamar así, y no también derechos, destacan:

- Añadir equipos a un dominio.
- Realizar copias de seguridad del sistema de directorios.
- Restaurar dichas copias de seguridad.
- Cambiar la configuración del sistema.
- Impedir la instalación de controladores de dispositivos.
- Apagar el sistema.

Dentro de las directivas de seguridad de un equipo tenemos las directivas de seguridad local y las directivas de seguridad de dominio.

Hay tres tipos principales de servidores que son interesantes de conocer:

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

Un servidor de ficheros se basa en el protocolo FTP y puede ser configurado en Windows Server.

Para poder gestionar el equipo en temas de seguridad, se suele disponer mucho de la administración remota, teniendo tres herramientas principales incorporadas por Windows:

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

Como herramientas de seguridad, disponemos del cifrado, donde distinguimos entre algoritmos de clave privada, o de clave pública. Hay casos en los que el cifrado puede ser híbrido, una mezcla de los dos. Otro elemento muy importante en aspectos de seguridad son los cortafuegos.

## Conceptos fundamentales

- **Derecho o privilegio:** atributos que afectan a una cuenta de usuario de Windows o a un grupo con la función de permitir realizar ciertas acciones sobre todo el sistema y no un solo recurso.
- **SAT:** identificación que realmente el sistema Windows usa para saber quién está generando cada proceso en cada momento y así poder saber si tiene permitido realizar dicho proceso sobre dicho recurso concreto.
- **Control total:** permiso mediante el cual, el usuario privilegiado, puede realizar cualquier acción sobre el objeto del explorador de archivos de Microsoft Windows.
- **ACL:** lista en la que se incluyen los permisos que se usan para regular los usuarios que tienen permitido acceder o no a depende que recursos del sistema.
- **Privilegios:** un apartado de los derechos que indican las acciones que el usuario puede realizar en el sistema que no se encuentran contempladas en los derechos de conexión.
- **Mantenimiento:** proceso mediante el cual se va observando el funcionamiento de un servidor o aplicación además de instalar actualizaciones y parches con el objetivo de asegurar que no haya errores en el futuro.
- **FTP:** *File Transfer Protocol*, protocolo usado para el envío de ficheros mediante la red con un servidor como destino.
- **Administración remota:** es el termino usado para la acción de administrar y asegurar la seguridad de un equipo a distancia, accediendo a él mediante diversas herramientas.
- **Cifrado:** técnica mediante la cual se asegura una información usando algoritmos para que no se pueda visualizar esa información sin una clave concreta.
- **Cortafuegos:** dispositivo usado para analizar todo el tráfico que pasa por un r*outer* con la intención de clasificarlo en permitido o no permitido basándose en unas reglas preestablecidas.