MONITORIZACIÓN DEL SISTEMA Y GESTIÓN DE SERVICIOS

1. MONITOR DE RENDIMIENTO

Todo sistema operativo basa su funcionamiento en una correcta ejecución de los procesos que lo componen. Estos procesos corresponden, entre otras cosas, a las aplicaciones que en cada momento ejecuta el usuario. Sin embargo, además de los asociados al navegador o al juego de turno, nos encontramos con otros llamados "de sistema", que sostienen el funcionamiento general de Windows.
Todo sistema operativo basa su funcionamiento en una correcta ejecución de los procesos que lo componen. Estos procesos corresponden, entre otras cosas, a las aplicaciones que en cada momento ejecuta el usuario. Sin embargo, además de los asociados al navegador o al juego de turno, nos encontramos con otros llamados "de sistema", que sostienen el funcionamiento general de Windows.

¿Para qué sirve el monitor de rendimiento?

El monitor de recursos se utiliza para ver cuántos recursos del sistema consumen los programas o servicios que se están ejecutando en Windows 7. Windows 7 proporciona la herramienta Monitor de rendimiento con la que se puede visualizar la evolución del rendimiento en una gráfica actualizada en tiempo real.
Además, con este monitor podemos realizar un seguimiento del comportamiento de elementos como el procesador, la memoria, el disco duro, el rendimiento de la red, o componentes del sistema más concretos como la función Readyboost y otros componentes de Windows.

Proporciona una interfaz gráfica para la personalización de conjuntos de recopiladores de datos y sesiones de seguimiento de eventos. La recopilación de datos y el registro se realiza mediante conjuntos de recopiladores de datos. Desde una única consola se permite:

- Supervisar el rendimiento de las aplicaciones y del hardware en tiempo real
- Personalizar qué datos se desea recopilar en los registros
- Definir umbrales para alertas y acciones automáticas
- Generar informes y ver datos de rendimientos en diferentes formatos

Empleo del monitor de rendimiento

Abrir el Monitor de rendimiento. 2 opciones:

- Ir al Panel de Control - Sistema y Seguridad – Herramientas administrativas - Monitor de rendimiento.
- Hacer click en Inicio, después click en el cuadro Iniciar búsqueda, escribimos monitor y presionamos la tecla Enter.

Agregar componentes para monitorización

OJO, cuantos más componentes agreguemos más confusa será la gráfica que se mostrará. Para agregar nuevos componentes:

- Click sobre el símbolo
- En la parte superior izquierda seleccionaremos los componentes que vamos a monitorizar. Se puede seleccionar una instancia concreta o que contabilice el total. Si vamos a monitorizar varios componentes, es mejor elegir Total si es posible.

2. SERVICIOS

Los servicios en Windows se ejecutan en segundo plano, y son transparentes para el usuario ya que no cuentan con interfaz de usuario. Windows de forma predeterminada inicia diversos servicios al inicio del sistema, otros están a la espera en modo automático, son activados por aplicaciones del sistema o por otros servicios. Estos consumen memoria y pueden ralentizar el equipo

El paquete de servicios está programado de forma tal que el equipo sea funcional en multitud de situaciones diversas, por lo que gran parte de ellos nunca nos serán necesarios. Un buen administrador, teniendo en cuenta el entorno donde se utilice el equipo, deberá decidir qué servicios desactivar completamente. Siempre antes de desactivar un servicio hay que informarse bien de su función.

Acceso a los servicios:

➢ ruta: Inicio ->Panel de control ->Sistema y seguridad → Herramientas administrativas ->Servicios.
➢ Hacer click en Inicio, después click en el cuadro Iniciar búsqueda, escribimos services.msc y presionamos la tecla Enter.

Esta herramienta muestra un listado de los servicios junto con su descripción, el tipo de inicio y otras características. Además de permitir la consulta, también se pueden iniciar o desactivar los servicios que se ejecutan en Windows.

Ejemplos

- Servicios de Escritorio remoto: TermService, SessionEnv, UmRdpService
- Tarjeta inteligente SCardSvr: Administra el acceso a tarjetas inteligentes.
- Registro remoto RemoteRegistry: Modificar registro a usuarios remotos.
- Ubicador de llamada a procedimiento remoto RpcLocator
- Windows Search WSearch: Indexa los archivos, el correo electrónico y otros contenidos para hacer búsquedas con más rapidez.
- Servicio del Reproductor de Windows Media WMPNetworkSvc: Comparte las bibliotecas del Reproductor de Windows Media con otros dispositivos.
- Tarjetas inteligentes SCPolicySvc: Permite configurar el sistema para bloquear el escritorio al extraer la tarjeta inteligente.
- Parental Controls WPCSvc: Control parental.
- Archivos sin conexión CscService: Realiza actividades de mantenimiento en la caché de archivos sin conexión.
- Agente de Protección de acceso a redes napagent: Administra información de los equipos de una red.
- Net Logon Netlogon: Autentica usuarios y servicios.
- Servicio del iniciador iSCSI de Microsoft MSiSCSI
- Aplicación auxiliar IP iphlpsvc
- Cliente de seguimiento de vínculos distribuidos TrkWks: Mantiene los vínculos entre archivos NTFS dentro de un equipo o entre equipos de una red.
- Propagación de certificados CertPropSvc
- BranchCache PeerDistSvc: Caché del contenido de la red en red local.
- Servicio de compatibilidad con Bluetooth bthserv: Permite la detección y asociación de dispositivos Bluetooth remotos.
- Servicio de detección automática de proxy web WinHTTP WinHttpAutoProxySvc
- Servicio Informe de errores de Windows WerSvc, Envío de informes sobre los errores a Microsoft.
- Servicio Cifrado de unidad BitLocker BDESVC
- Sistema de cifrado de archivos EFS, para almacenar archivos cifrados en particiones NTFS.
- Fax Fax
- Acceso a dispositivo de interfaz humana hidserv.

EL ADMINISTRADOR DE TAREAS DE WINDOWS

1. ACCESO AL ADMINISTRADOR

El administrador de tareas de Windows –Task Manager– es una de las aplicaciones internas más antiguas del sistema operativo de Microsoft. Una herramienta de gestión muy útil para profesionales o usuarios medios-avanzados que quieran controlar a fondo el funcionamiento de su equipo o resolver algunos problemas que se derivan de su uso. La aplicación fue una de las herramientas internas más mejoradas en el lanzamiento de Windows 10 y Microsoft ha ido añadiendo novedades en cada una de las actualizaciones. Varias formas:

- Ctrl + Alt + Supr. Este es el método más conocido, pero no es el más rápido
- Ctrl + Shift + Esc. Más directo que el anterior, lanza inmediatamente el administrador de tareas y además tiene la ventaja que por la posición del teclado se puede ejecutar con una sola mano.
- Barra de tareas. Si haces clic derecho con el ratón en la barra de tareas hay una opción para acceder al administrador.
- Menú de usuario avanzado. Haz clic en el botón derecho en el botón de inicio para acceder al menú avanzado y también encontrarás este Task Manager.
- Ejecutar. Pulsa el atajo de teclado Win + R y escribe el comando "taskmgr".

2. FUNCIONES DEL ADMINISTRADOR

El administrador de tareas de Windows permite varias funcionalidades:

- Comprobar si una aplicación está congelada

Función más común para la cual se utiliza el administrador de tareas. Es necesario comprobar correctamente que la aplicación esté congelada, ya que simplemente puede estar ejecutándose consumiendo un mayor tiempo. Existe la función «analizar» que puede ayudar a identificar el problema y evitar tener que cerrar la aplicación manualmente, evitando una posterior pérdida de datos. Solo está disponible en la pestaña detalles.

- Reiniciar el explorador de Windows

Cuando algunas partes del sistema no están respondiendo, reiniciar el ordenador puede resolver el problema, pero antes es posible reiniciar el explorador mediante el administrador de tareas.

- Monitorización de rendimiento y recursos

Aquí es donde el administrador de tareas de Windows 10 realmente brilla. No sólo proporciona una visión general de todos los procesos en ejecución y las aplicaciones sino que tiene varias herramientas para supervisar eficazmente el rendimiento del sistema y cómo se asignan los recursos.
Incluye un montón de información, desde el monitor de recursos (RAM, procesador...) que ofrece visualización de datos en tiempo real; información de diagnóstico con logs que se pueden compartir para evaluaciones; detalles de red y otros recursos de interés.

- Búsqueda en línea de procesos sospechosos

Se emplea para analizar procesos desconocidos en el administrador de tareas. Mediante clic derecho sobre el proceso sospechoso, se podrá activar la búsqueda en línea. Esto iniciará una búsqueda en el navegador con el nombre de la aplicación y el nombre del proceso

- Agregar columnas adicionales para más detalle y Cambiar entre valores y porcentajes

La herramienta sólo muestra cinco columnas cuando se enumeran los procesos: Nombre, CPU, memoria, disco y red que son las más importantes, pero se pueden añadir hasta seis columnas más simplemente haciendo clic derecho en el área de encabezado.
Adicionalmente, las columnas Memoria, Disco y Red pueden mostrar valores reales o porcentajes. Para modificar estos valores, simplemente se hace clic derecho en cualquier proceso, se accede al submenú de recursos y se intercambia entre uno y otro.

- Administrar aplicaciones de Windows fácilmente

Para acceder a esta función, hay que hacer clic en la flecha desplegable junto a la aplicación que desea administrar. Se ofrecen cinco acciones, desde traer al frente, maximizar, minimizar o finalizar la tarea.

- Ubicación de archivos de la aplicación abierta

Clic derecho en cualquier proceso y se selecciona «abrir ubicación de archivos». Esta acción llevará directamente a la carpeta que contiene el archivo ejecutable del proceso. Funciona para aplicaciones, procesos en segundo plano y procesos de Windows.

- Iniciar símbolo del sistema directamente

Al clicar en Archivo y seleccionar «ejecutar una nueva tarea» se inicia el cuadro de diálogo ejecutar. Permite reiniciar manualmente un explorador congelado y acceder a la terminal.

- Función Inicio del Configurador del sistema

Al ejecutar el comando «msconfig» para configurar el sistema, se observa que la función de inicio se ha trasladado al administrador de tareas. Esta pestaña permite configurar las aplicaciones que se iniciarán en el arranque. La herramienta ofrece información del impacto de cada aplicación en el rendimiento del sistema y permite desactivarlas de inicio.

ADMINISTRACIÓN DE USUARIOS Y GRUPOS LOCALES. SEGURIDAD DE LAS CONTRASEÑAS.

1. TIPOS DE USUARIOS

Cuentas de usuarios locales

- Gestionadas en la BD de usuarios del equipo local (usuarios asociados a un equipo)
- Solo permiten acceder al equipo donde resise la BD
- La BD es parte de Windows y se almacena en el fichero %SYSTEMROOT%\System32\config\SAM
- Tipos: Administrador, Usuarios solicitados por el instalador de Windows e Invitados

Cuentas de usuarios globales:

- Gestionadas de forma centralizada en una BD de usuarios compartida (usuarios no asociados a ningún equipo en concreto)
- La BD es implementada mediante un servicio de directorio
- La implementación Windows del servicio de directorio X.500, accedido mediante el LDAP, se denomina "Active Directory" (AD), y está ligada a las redes Windows de tipo dominio

2. GRUPOS DE USUARIOS

- También se pueden clasificar en locales y globales.
- Facilitan la asignación de derechos y permisos, evitando tener que operar a nivel de usuario individual.
- Un usuario puede ser miembro de más de un grupo.
- Los grupos locales:
  - Cuyos miembros pueden ser administrados manualmente:
    - "Administradores"
    - "Usuarios avanzados"
    - "Invitados"
    - "Usuarios"
    - "Usuarios de escritorio remoto"
    - "Operadores de copia"
  - Cuyos miembros no pueden ser administrados manualmente:
    - "Todos (Everyone)"
    - "Usuarios autenticados (AuthenticatedUsers)"

3. HERRAMIENTAS PARA ADMINISTRAR CUENTAS Y GRUPOS LOCALES DE USUARIOS

Botón "Cambiar contraseña" de la ventana que aparece tras Ctrl + Alt + Supr

Aplicación "Asistente para Cuentas de usuario", del "Panel de control". Accesible desde:

- Panel de Control à Cuentas de usuario
- control.exe nusrmgr.cpl
- control.exe userpasswords

Aplicación "Cuentas de usuario" del Panel de Control.

- Accesible mediante la ejecución de control.exe userpasswords2
- Permite configurar la forma en que los usuarios pueden iniciar sesiones.

Consola "Usuarios y grupos locales". Accesible mediante la ejecución de la consola lusrmgr.msc

Comandos importantes:

- **NET USER [<usuario>]** Obtención de información sobre cuentas de usuario
- **NET USER <usuario> [<contraseña> | *] /ADD [<opciones>]** Creación de cuentas de usuario
- **NET USER <usuario> [< contraseña > | *] <opciones>** Modificación de cuentas de usuario
- **NET USER < usuario > /DELETE** Eliminación de una cuenta de usuario

Opciones importantes del comando NET USER:

- /ACTIVE:YES | NO
- /EXPIRES:<fecha> | NEVER
- /PASSWORDCHG:YES | NO
- /PASSWORDREQ:YES | NO
- /LOGONPASSWORDCHG:YES | NO
- /TIMES:<periodos> | ALL

Comando NET LOCALGROUP (comando externo):

- **NET LOCALGROUP** Obtención de la lista de grupos locales
- **NET LOCALGROUP <grupo>** Obtención de la lista de miembros de un grupo local
- **NET LOCALGROUP <grupo> /ADD** Creación un grupo local
- **NET LOCALGROUP <grupo> /DELETE** Eliminación de un grupo local
- **NET LOCALGROUP <grupo> <usuario> /ADD** Inclusión de un usuario en un grupo local
- **NET LOCALGROUP <grupo> <usuario> /DELETE** Eliminación de un usuario de un grupo local

4. CONCEPTOS RELACIONADOS CON LA SEGURIDAD EN LOS SO

Autentificación: Al abrir una sesión de trabajo (login) proporcionando al sistema un nombre de usuario y una contraseña nos estamos autentificando en un SO. En caso de no tener una cuenta de usuario abierta en el sistema, será imposible entrar en el mismo.

Autorización: Cada vez que un usuario quiera usar un recurso (un fichero, una carpeta, una impresora, etc.) el sistema comprobará si está autorizado o no para realizar esa acción. Los administradores del sistema pueden modificar estas autorizaciones mediante unas listas de acceso.

5. ADMINISTRACIÓN DE GRUPOS Y CUENTAS DE USUARIO LOCALES

En Windows 7 existen **tres tipos de cuentas de usuario locales:**

Cuenta de usuario estándar: Tiene privilegios limitados, puede usar la mayoría de los programas instalados en el equipo, pero no se puede instalar o desinstalar software ni hardware, eliminar archivos que son necesarios para que el equipo funcione, o cambiar opciones de configuración en el equipo que afecten a otros usuarios.

Cuenta de administrador: Tiene el máximo control sobre el equipo y sólo se debe utilizar cuando se lleven a cabo tareas de administración que requieran estos privilegios. Este tipo de cuenta permite realizar cambios que afectan a otros usuarios como la configuración de seguridad, la instalación de software y hardware, la obtención de acceso a todos los archivos en un equipo.

Cuenta de Invitado: Suele ser utilizada por usuarios temporales del equipo. Aunque tiene derechos muy limitados, hay que tener cuidado al utilizarla porque se expone al equipo a problemas de seguridad potenciales. El riesgo es tan alto que la cuenta de invitado viene deshabilitada con la instalación de Windows 7.

Windows identifica los usuarios a través de su SID (Security Identifier - Identificador de Seguridad), que es un número de identificación único para cada usuario.

Cuando eliminamos una cuenta de usuario, ésta se borra definitivamente del sistema. No podemos recuperarla creando otra con el mismo nombre con el objeto de conseguir los mismos permisos de la cuenta antigua. Esto es debido a que cuando creamos otra cuenta nueva, el sistema asigna un nuevo SID distinto de la cuenta antigua.

Tres tipos de grupos en Windows 7:

Grupos locales: Definidos en un equipo local y utilizados sólo en dicho equipo local.

Grupos de seguridad: Pueden tener descriptores de seguridad asociados. Se utiliza un servidor Windows para definir grupos de seguridad en dominios.

Grupos de distribución: Se utilizan como lista de distribución de correo electrónico. No pueden tener descriptores de seguridad asociados.

- Grupos de usuarios predefinidos en el sistema creados por defecto cuando se instala Windows 7:

Administradores.	Operadores de copia de seguridad.	Operadores criptográficos.	Lectores del registro de eventos.	Invitados.
Operadores de configuración de red.	Usuarios del registro de rendimiento.	Usuarios del monitor del sistema.	Usuarios avanzados*.	Usuarios autenticados.
Usuarios de escritorio remoto.	Duplicadores.	Usuarios*.		

Usuarios. Los usuarios miembros de este grupo son los que realizan la mayor parte de su trabajo en un único equipo Windows 7. Estos usuarios tienen más restricciones que privilegios. Pueden conectarse a un equipo de manera local, mantener un perfil local, bloquear el equipo y cerrar la sesión del equipo de trabajo.*

Usuarios avanzados. Tienen derechos adicionales a los del grupo Usuarios. Algunos de estos derechos extra son la capacidad de modificar configuraciones del equipo e instalar programas.*

6. HERRAMIENTAS PARA ADMINISTRAR LA SEGURIDAD DE LAS CONTRASEÑAS

En propiedades de un usuario de la consola de usuarios locales y grupos, que ya hemos visto anteriormente (LUSRMGR.MSC) tenemos 3 pestañas:

1. General: Podemos indicar el nombre completo de la cuenta, una descripción, e indicar algunas opciones de la cuenta:
   - El usuario debe cambiar la contraseña en el siguiente inicio de sesión. Cuando el usuario inicie sesión la próxima vez se verá obligado a cambiar su contraseña.
   - El usuario no puede cambiar la contraseña. Prohibimos que el usuario pueda cambiar su contraseña.
   - La contraseña nunca caduca. Mediante esta opción indicamos que la contraseña podrá usarse sin que caduque
   - Cuenta deshabilitada: No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.
   - La cuenta está bloqueada: Por determinados mecanismos de seguridad se puede llegar a bloquear una cuenta, que implicará que se deshabilite. Desde esta opción podemos volver a desbloquearla, simplemente desmarcando la casilla.

2.Miembro de: desde esta pestaña podemos introducir al usuario en grupos. Los grupos se usan para dar permisos y derechos a los usuarios más fácilmente, sin tener que ir usuario por usuario. Si introducimos a un usuario como miembro del grupo Administradores, le estaremos dando todos los permisos del grupo Administradores. También veremos todos los grupos a los que el usuario pertenece actualmente. Si le damos al botón agregar podremos escribir directamente el nombre de un grupo donde agregarlo. Si queremos escoger dicho grupo de una lista de los grupos posibles, hay que escoger la opción Avanzada y luego Buscar ahora, que nos mostrará una lista de todos los grupos del sistema. Basta con seleccionar el que queramos (o los que queramos) y pulsar aceptar.

3. Perfil. Ésta nos permite indicar la ruta del perfil, los archivos de inicio de sesión y las carpetas personales del usuario.

UAC (User Account Control, Control de Cuentas de Usuario)

Es una característica de seguridad que se encarga de notificar alertas de seguridad del sistema al usuario. Lanza mensajes de alerta cuando se quiere realizar alguna acción que influya en el sistema, tal como la instalación de determinados programas, la modificación el registro de Windows, la creación de servicios, etc. User account Control (UAC) es el responsable de mensajes como "Un programa no identificado desea tener acceso a este equipo" o "Necesita confirmar esta operación", y aunque, en ocasiones, estos mensajes pueden llegar a ser algo molestos, evita básicamente que se instale software sin el consentimiento del usuario.

Para acceder al UAC nos dirigimos al Panel de Control → Sistema y seguridad → Centro de Actividades → Cambiar configuración de Control de cuentas de usuario.

✓ Directivas

Una directiva es un conjunto de reglas de seguridad que se pueden implementar en un sistema. Con las Directivas de seguridad local veremos cómo aplicar distintas restricciones de seguridad sobre las cuentas de usuario y contraseñas. Por otro lado, las Directivas de grupo local nos permiten configurar equipos de forma local o remota, instalar o eliminar aplicaciones, restringir los derechos de los usuarios, entre otras acciones. Ambas opciones cuentan con consolas para facilitar la configuración de las directivas.

- Directivas de cuenta de la consola Directivas de seguridad local. Accesible desde:
  - Panel de Control → Herramientas administrativas →Directiva de seguridad local
  - Ejecución de secpol.msc

- Directivas de grupo local. Accesible desde gpedit.msc
  - Modificar políticas que se encuentran en el registro del sistema. El registro del sistema es una gran base de datos en la que se configuran cientos de comportamientos de Windows 7. Desde las políticas de grupo podemos acceder a estas características y modificarlas, de una forma mucho más simple que mediante la edición pura del registro.
  - Asignar scripts que se ejecutaran automáticamente cuando el sistema se encienda, se apague, un usuario inicie sesión o cierre sesión.
  - Especificar opciones especiales de seguridad.
  - Dentro de las directivas de grupo locales tenemos dos opciones: Configuración del equipo y Configuración del usuario. En el caso de estar trabajando en grupo de trabajo es prácticamente indistinto trabajar con una opción u otra.
  - Para aprender más de una directiva en concreto, simplemente tendremos que seleccionarla con el ratón, y veremos una descripción detallada de dicha directiva en el panel central.
  - Algunas directivas aparecen tanto en la configuración del equipo como en la configuración del usuario. En caso de conflicto, la configuración del equipo siempre tiene preferencia.
  - Respecto a la configuración, veremos que podemos en esta consola:

    - **No configurar la directiva,** con lo que se comportará según el criterio por defecto para dicha directiva.
    - **Habilitarla**, con lo que la pondremos en marcha en el sistema.
    - **Deshabilitarla,** con lo que impediremos que se ponga en marcha dicha directiva.

Algunas directivas especiales permiten especificar otras informaciones. Se recomienda leer cuidadosamente la explicación de cada directiva para entender sus efectos sobre el sistema y decidir habilitarla o no.

También podemos editar el UAC desde el Editor de directivas de grupo local. Para ello, desde el campo de búsqueda del menú de Inicio, escribimos gpedit.msc y pulsamos Enter, se nos abrirá el editor de directivas. Dentro de éste buscamos la cadena Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad y encontraremos varias entradas referentes al UAC..

Cada entrada indica su utilidad en su nombre, tendremos que decidir si se activan o se desactivan. En cualquier caso, es posible que los cambios requieran de un reinicio para funcionar.

Comandos importante NET ACCOUNTS:

- NET ACCOUNTS → Obtención de información sobre cuentas de usuario
- NET ACCOUNTS <opciones> → Modificar la configuración de seguridad de contraseñas
  - /MINPWLEN: <longitud>
  - /MAXPWAGE: <No de días> | UNLIMITED
  - /MINPWAGE: <No de días>
  - /UNIQUEPW: <número>

7. IDENTIFICACIÓN Y ACREDITACIÓN DE USUARIOS

Windows identifica internamente a cada usuario y grupo mediante un SID (SecurityIDentifier)

- **Para obtener el SID de un determinado usuario o grupo:**
  wmic useraccount where name = 'damian' get sid
  ejemplo salida: S-1-5-21-1640792398-2097240683-3316014058-1004

  wmic group where name= 'administradores' get sid
  ejemplo salida: S-1-5-32-544

- **Para obtener el nombre de usuario a partir de un SID**
  wmic useraccount where sid= 'S-1-5-21-1640792398-2097240683- 3316014058-1004' get name
  ejemplo salida: Damián

- **Para obtener el nombre de grupo a partir de un SID**
  wmic group where sid = 'S-1-5-32-544' get name
  ejemplo salida: Administradores

- **Para averiguar el SID del usuario actual** → whoami/user

- **Para averiguar el SID de los grupos a los que pertenece el usuario actual** → whoami/groups

Cuando un usuario accede interactivamente a un sistema Windows, éste construye para él una acreditación denominada SAT(Security Access Token), que incluye:

- SID del usuario.
- Lista de los SID de los grupos a los que pertenece el usuario.
- Lista de los derechos que el usuario tiene otorgados, por si mismo, o por pertenencia a grupos.

Esta información será utilizada cada vez que el sistema necesite comprobar sus derechos o permisos de acceso.

- Un derecho autoriza a un usuario a realizar ciertas acciones en un equipo, como hacer copias de seguridad de archivos y carpetas, o apagar el equipo.

- Un permiso es una regla asociada a un recurso que regula los usuarios/grupos que pueden tener acceso al recurso y la forma en la que acceden.

Los permisos de un recurso se guardan en una lista especial, que se conoce como ACL (Access Control List o Lista de Control de Acceso). Estas ACLs de los recursos también pueden ser modificadas para que sean usadas por los usuarios y grupos locales.

ADMINISTRACION DE USUARIOS Y GRUPOS LOCALES. PERMISOS

1. PERMISOS DE ARCHIVOS Y CARPETAS

ACL: Access Control Listo Lista de Control de Acceso

Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. El recurso comprobará entonces si en su ACL aparece el SID del usuario, y en caso contrario, comprobará si en su ACL aparece el SID de algún grupo al que pertenezca el usuario.
Si no aparece en la ACL ningún SID del usuario, el recurso niega el acceso al usuario. Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer,
borrar, escribir, etc.) está permitida para ese SID en su ACL, si lo está, le autoriza para hacerlo, en caso contrario se lo impide.
Puede ocurrir que un usuario tenga permisos contradictorios. cualquier ACL es la denegación implícita de permisos.

- Lo que mas pesa es la denegación implícita de permisos. Si un permiso esta denegado, no se sigue mirando, se deniega inmediatamente.
- Es suficiente con que un permiso esté concedido en cualquier SID para que se considere. concedido. (A excepción de la regla 1, es decir, que no esté denegado implícitamente en ningún sitio)

Los permisos de un archivo o carpeta pueden visualizarse en Propiedades/seguridad.

En la parte superior se encuentran las SID a las que concedemos permisos (usuarios y grupos) y en la parte inferior tenemos los permisos concretos que le concedemos a dicha SID. Las dos columnas por cada permiso, posibilitan Permitir o Denegar un permiso. La denegación de un permiso es la que más pesa, y se aplica inmediatamente. De hecho, se aconseja no denegar permisos, a menos que sea absolutamente necesario.

Pulsando el botón Editar se abre una nueva pantalla donde aparecen los botones Agregar y Quitar. Con ellos se pueden añadir o quitar usuarios o grupos de la ACL. En la parte inferior podemos pulsar en las casillas de Permitir y Denegar para dar y quitar permisos.

Herencia

En Windows 7, cualquier recurso que se cree, heredará automáticamente la ACL de su recurso padre si es que existe. Para romper con la herencia, se accederá al botón de Opciones Avanzadas que está en la pestaña Seguridad. En la pestaña permisos se puede observar como en la parte inferior de esta ventana esta marcada la opción de: "Incluir todos los permisos heredables del objeto primario de este objeto".

Si se desmarca dicha opción se deshabilitará la relación de herencia del recurso, y se podrá gestionar su ACL "directamente". Al quitarla el sistema da a elegir entre dos opciones:

- Si se escoge la opción Agregar, la herencia se interrumpirá, y se podrá retocar la ACL, pero dicha ACL partirá de la tenía tiene el recurso, heredada de su objeto principal.

- Si se escoge la opción Quitar, la ACL se borrará totalmente, se interrumpirá la herencia y ésta se podrá crear desde cero. Hay que tener en cuenta, si se parte desde cero, que en las ACL no sólo deben aparecer las SID de los usuarios o grupos deseados, sino que grupos como Creator Owner o System son necesarios para que el sistema pueda trabajar sin problemas con dichas carpetas. Si quitamos estos SID tendremos problemas en el futuro (copias de seguridad, auditorías, etc.)

Existe otra opción que permite activar que los objetos por debajo del recurso analizado hereden las modificaciones que se hagan en la ACL. Esto es importante tenerlo en cuenta si queremos que los cambios que hagamos en la ACL se repliquen en los objetos hijos del nuestro, ya que hemos roto la herencia y a veces tendremos que forzar dichos cambios.
Una vez eliminada la herencia de permisos se pueden eliminar grupos predeterminados de Windows que no suelen hacer falta, como por ejemplo Usuarios y Usuarios autenticados. El motivo principal para eliminarlos de la ACL es que si se mantuvieran cualquier usuario del sistema podría acceder y ver el contenido de la carpeta. Esto es así, porque cuando se crea un usuario en Windows, éste lo hace miembro automáticamente de estos grupos.

2. TIPOS DE PERMISOS

Los distintos permisos que se pueden aplicar para cada SID en la ACL no son únicamente los que se observan en las propiedades de la carpeta, si se analiza la pestaña de Seguridad en Opciones avanzadas, existirá un cuadro llamado Entradas de permisos para los distintos usuarios y grupos de la ACL. Si se hace click en el botón Cambiar permisos y después en el botón Editar, podremos indicar otro tipo de permisos.

- El permiso **Atravesar carpeta** permite o impide que el usuario pase de una carpeta a otra para llegar a otros archivos o carpetas, incluso aunque el usuario no tenga permisos para las carpetas recorridas (sólo se aplica a carpetas).

- El permiso **Leer atributos** permite o impide que el usuario vea los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

- El permiso **Escribir atributos** permite o impide que el usuario cambie los atributos de un archivo o de una carpeta, como sólo lectura y oculto. Los atributos están definidos por el sistema de archivos NTFS.

- El permiso **Tomar posesión** permite o impide que el usuario tome posesión del archivo o de la carpeta. El propietario de un archivo o de una carpeta puede cambiar los permisos correspondientes, cualesquiera que sean los permisos existentes que protegen el archivo o la carpeta.

- El permiso **Control Total** permite a un usuario eliminar cualquier cosa que haya en esa carpeta, incluso si le denegamos el permiso de eliminación en esos recursos. Hay que tener mucho cuidado al conceder este permiso

ARCHIVOS DE TRATAMIENTO POR LOTES Y TAREAS AUTOMÁTICAS

1. ¿QUÉ SON LOS ARCHIVOS POR LOTES?

En esencia, se trata de un archivo de texto que contiene un listado de ordenes o comandos del MS DOS que se ejecutan uno detrás de otro ordenando al sistema que realice tareas específicas. Todos los nombres de archivos de tratamientos por lotes deben de tener la extensión ".BAT"
Generalmente, se emplean para automatizar tareas que se realizan habitualmente como, por ejemplo, mover archivos. Para crear un archivo por lotes, no es necesario descargar ningún editor sofisticado; el programa estándar de Windows conocido como "Bloc de notas" es más que suficiente

Requisitos importantes:

- Los archivos por lotes no pueden tener el mismo nombre que cualquier otra orden del MS- DOS o programa que el ordenador pueda tener. Si se crea de forma accidental un archivo por lotes con el mismo nombre, el MS-DOS ejecutara siempre la orden y nunca el archivo por lotes.
- Todas las ordenes que el archivo por lotes contenga deberán ser escritas en cada línea del archivo, o sea una orden por línea.

2. ¿CÓMO CREAR UN ARCHIVO POR LOTE?

Pasos para realizar un archivo por lote:

1. Abre "Bloc de notas" en Windows. El bloc de notas te permite crear un código como archivo de texto y luego guardarlo cuando termines con el archivo por lotes.

2. Empleo de comandos por lotes básicos. Los archivos por lotes ejecutan una secuencia de comandos DOS; por tanto, los comandos que puedes usar son similares a ellos. Algunos de los más importantes son:

    - ECHO - Muestra el texto en la pantalla
    - @ECHO OFF - Oculta el texto que se emite normalmente
    - START - Ejecuta un archivo con su aplicación predeterminada
    - REM - Inserta una línea de comentario en el programa
    - MKDIR/RMDIR - Crea y elimina los directorios
    - DEL - Borra uno o más archivos
    - COPY - Copia uno o más archivos
    - XCOPY - Te permite copiar archivos con opciones adicionales
    - FOR/IN/DO - Este comando te permite especificar archivos.

3. Escribir el programa. Por ejemplo, se puede usar un archivo por lotes para crear rápidamente directorios múltiples. Ejemplo:

    - MKDIR c:\ejemplo1
    - MKDIR c:\ejemplo2

4. Guarda el archivo. Una vez que ingreses el código, puedes guardar el archivo al usar el tipo de archivo por lotes. Haz clic en "Archivo" "Guardar como".

5. Ingresa un nombre para el programa seguido de .bat

6. Selecciona "Todos los archivos"

Algunos consejos:

- Puedes usar un editor independiente como UltraEdit para editar tu archivo por lotes. Pero en la mayoría de casos, son una pérdida de tiempo cuando escribes archivos por lotes simples.

- Tendrás que usar comillas si quieres abrir un directorio o archivo que tenga espacios en el nombre, como iniciar "C:\Documents and Settings\".

- Los archivos por lotes pueden tener también la extensión .cmd a partir de Windows 2000. No hay ninguna diferencia en el funcionamiento, pero los archivos .cmd trabajan con 32 bits y los .bat con 16.

- Dependiendo de los comandos, el resultado puede ser peligroso. Es necesario saber y comprender los comandos para que el código no sea peligroso; por ejemplo, generar archivos por lotes para borrar archivos de manera permanente.

3. EJEMPLOS DE ARCHIVOS POR LOTES

Programa básico de copias de seguridad:

Los archivos por lotes son excelentes para ejecutar comandos múltiples, especialmente si se configuran para ejecutarlos varias veces. Con el comando XCOPY, se puede crear un archivo por lotes que copie los archivos de las carpetas seleccionadas a la carpeta de seguridad, sobrescribiendo solo los archivos que se han actualizado desde la última copia.

```
@ECHO OFF
XCOPY c:\original c:\carpetadeseguridad /m /e /y
```

Este código sobrescribe archivos desde la carpeta "original" a la carpeta "carpeta de seguridad". Estas carpetas pueden ser reemplazadas con las rutas a las carpetas que se requiera.

/m especifica que solo se copiarán los archivos actualizados, /e especifica que todos los subdirectorios del directorio listado serán copiados e /y mantiene el mensaje de confirmación que aparece cada vez que un archivo se sobrescribe.

Programa de copias de seguridad más avanzado:

Anteriormente solo se ha conseguido copiar simplemente los archivos de una carpeta a otra. Si se requiere clasificarlos los elementos copiados de manera simultanea aparece el comando "FOR/IN/DO". Se puedes usar dicho comando para indicar dónde irá el archivo en base a su extensión:

```
@ECHO OFF
cd c:\fuente
REM Esta es la ubicación de los archivos que quieres clasificar
FOR %%f IN (*.doc *.txt) DO XCOPY c:\fuente\"%%f" c:\texto /m /y
REM Este mueve cualquier archivo con una extensión .doc
REM o .txt desde c:\fuente a c:\texto
REM %%f es una variable
FOR %%f IN (*.jpg *.png *.bmp) DO XCOPY C:\fuente\"%%f" c:\imágenes /m /y
REM Este mueve cualquier archivo con una extensión .jpg, .png
REM o .bmp desde c:\fuente a c:\imágenes
```

4. ¿QUÉ SON LAS TAREAS AUTOMÁTICAS?

Si nos paramos a pensar, seguro que hay muchas tareas que realizamos casi a diario cuando nos sentamos frente al ordenador. Acciones que necesitamos realizar cada día o de forma periódica y que nos ahorrarían mucho tiempo si se pudieran ejecutar de forma automática. En este sentido, el sistema operativo de Microsoft cuenta con una herramienta que nos permite justo esto, programar tareas para que se ejecuten automáticamente en nuestro equipo.
Las tareas automáticas son una secuencia de comandos, programas o documentos que permiten ser ejecutados autónomamente en el momento más adecuado, de acuerdo a una calendarización.
El programador de tareas de Windows es una herramienta propia de Microsoft que ha sido diseñada para ayudar a los usuarios a ejecutar ciertas tareas de forma automática. De esta manera, gracias al programador podemos indicar al sistema que algo se ejecute un día y a una hora determinada, periódicamente o cuando se produce un evento concreto.

5. ¿CÓMO CREAR UNA TAREA AUTOMÁTICA?

2 formas de acceder al programador de tareas:

- Inicio → Panel de control → Sistema y Seguridad →Herramientas administrativas →Programador de tareas
- Inicio → En el cuadro de búsqueda buscar taskschd.msc

1. En el menú seleccionamos Acción → Crear tarea
2. Ponemos un nombre a la tarea y una descripción si lo deseamos
3. Seleccionamos la pestaña Desencadenadores, donde podemos indicar la periodicidad que deseamos que se ejecute.
4. Seleccionamos la pestaña Acciones donde indicaremos que deseamos que haga nuestra tarea. Por ejemplo, queremos que nos ejecute el Notepad
5. Una vez creado, seleccionamos Biblioteca del Programadores de tareas para visualizar nuestra tarea.

PERFIL DE USUARIO

1. ¿QUÉ ES UN PERFIL DE USUARIO?

Un perfil de usuario de Windows se puede definir como un conjunto de carpetas, archivos y parámetros de registro y configuración que definen el entorno de un usuario que inicia una sesión con una cuenta de usuario específica. En función de la configuración administrativa, los usuarios pueden personalizar o no estos parámetros. Las características más importantes de los perfiles de usuario son:

- Cada cuenta dispone de un perfil de usuario (PU).
- Cada PU se almacena en %SYSTEMDRIVE%\Users\<nombre del usuario>
- La variable de entorno USERPROFILE contiene la ruta absoluta de acceso al PU.

2. ¿QUÉ CONTIENE UN PERFIL DE USUARIO?

Un perfil de usuario (PU) contiene los ficheros y la configuración que implementan el entorno de trabajo del usuario. Los ficheros de cada PU se organizan en carpetas:

- Desktop
- Documents
- Downloads
- Favorites
- ...
- AppData\Roaming\Microsoft\Windows
    - Recent
    - SendTo
    - Start Menu

La configuración de cada PU se almacena en el fichero oculto "%USERPROFILE%\ntuser.dat".

• Durante la sesión, los cambios de configuración llevados acabo por el usuario se almacenan en los ficheros ocultos:

- "%USERPROFILE%\ntuser.dat.log1".
- "%USERPROFILE%\ntuser.dat.log2".

• Al cerrar la sesión, "ntuser.dat" se actualiza con el contenido de "ntuser.dat.log1" y "ntuser.dat.log2"

• La categoría HKEY_USERS del editor del registro del sistema permite examinar y editar los ficheros "ntuser.dat.log1" y "ntuser.dat.log2" de los usuarios que tienen iniciada una sesión.

• La categoría HKEY_CURRENT_USER de la vista que cada usuario tiene del registro del sistema apuntará a la entrada correspondiente para el usuario en HKEY_USERS

3. PERFILES ESPECIALES

Existen dos perfiles especiales:

- Perfil "por defecto", almacenado en la carpeta oculta %SYSTEMDRIVE%\Users\Default →Constituye la base para la creación del PU durante el proceso de inicio de la primera sesión del usuario.

- Perfil "público",almacenado en la carpetas: %SYSTEMDRIVE%\Users\Public
  %SYSTEMDRIVE%\ProgramData
    - Permite establecer aspectos que serán comunes a todos los PPUU.

Cada vez que un usuario acceda al sistema dispondrá de un entorno de trabajo resultado de la combinación de perfil especial "público", y de su propio PU.

4. ADMINISTRACIÓN DEL PPUU

La opción "Configuración avanzada del sistema" del icono "Sistema" del "Panel de control" da acceso a una herramienta que permite administrar los PPUU existentes en el equipo local.

VARIABLES DE ENTORNO

1. ¿QUÉ SON LAS VARIABLES DE ENTORNO?

Las variables de entorno son valores parametrizados que contienen información acerca del sistema y del usuario que inició sesión actualmente. Tanto en Windows como en Linux tienen la misma función. El nombre de las variables de entorno en Windows es "case insensitive".

Dos Tipos:

1. Variables de entorno persistentes a nivel de sistema:
    - Se definen en Sistema →Configuración avanzada del sistema →Pestaña "Opciones avanzadas"→Botón "Variables de entorno" →Panel "Variables del sistema".
    - Se almacenan en el registro del sistema.
    - Serán visibles por cualquier proceso
2. Variables de entorno persistentes a nivel de usuario:
    - Cada usuario las puede definir mediante Panel de control →Cuentas de usuario → Cambiar las variables de entorno.
    - Se almacenan en el registro del sistema.
    - Serán visibles por cualquier proceso propiedad del usuario

Para crear una variable en CMD se emplea el comando "SETX": SETX VARIABLE1 VALOR1

2. LISTA DE VARIABLES DE ENTORNO

- **%ALLUSERSPROFILE%** Devuelve la ubicación de perfil Todos los usuarios.
- **%APPDATA%** Devuelve la ubicación en que las aplicaciones guardan los datos de forma predeterminada.
- **%CD%** Devuelve la cadena del directorio actual
- **%CMDCMDLINE%** Devuelve la línea de comandos exacta utilizada para iniciar el Cmd.exe actual.
- **%CMDEXTVERSION%** Devuelve el número de versión de Extensiones del procesador de comandos actual.
- **%COMPUTERNAME%** Devuelve el nombre del equipo.
- **%COMSPEC%** Devuelve la ruta de acceso exacta al ejecutable del shell de comandos.

Comando "ECHO" para visualizar el valor de la variable de entorno en CMD
Comando "set" para visualizar todas las variables y sus respectivos valores en CMD
Comando "Get-ChildItem Env:" para visualizar todas las variables y sus respectivos valores en Power Shell

- **%DATE%** Devuelve la fecha actual. Utiliza el mismo formato que el comandodate /t. Generado por Cdm.exe. Para obtener más información acerca del comando date, vea Fecha.
- **%ERRORLEVEL%** Devuelve el código de error del último comando utilizado. Usualmente, los valores distintos de cero indican que se ha producido un error.
- **%HOMEDRIVE%** Devuelve la letra de unidad de la estación de trabajo local del usuario conectada al directorio principal del usuario.
- **%HOMEPATH%** Devuelve la ruta de acceso completa del directorio principal del usuario. Se establece según el valor del directorio principal. El directorio principal del usuario se especifica en Usuarios y grupos locales.
- **%HOMESHARE%** Devuelve la ruta de acceso de red del directorio principal compartido del usuario. Se establece según el valor del directorio principal. El directorio principal del usuario se especifica en Usuarios y grupos locales.
- **%LOGONSERVER%** Devuelve el nombre del controlador de dominio que validó la sesión actual.
- **%NUMBER_OF_PROCESSORS%** Especifica el número de procesadores instalados en el equipo.
- **%OS%** Devuelve el nombre del sistema operativo. En Windows 2000 y XP se muestra el sistema operativo Windows NT.
- **%PATH%** Especifica la ruta de acceso de búsqueda para los archivos ejecutables.
- **%PATHEXT%** Devuelve una lista de extensiones de archivo que el sistema operativo considera como ejecutables.
- **%PROCESSOR_ARCHITECTURE%** Devuelve la arquitectura de chip del procesador. Valores: x86 o IA64 (basado en Itanium).
- **%PROCESSOR_LEVEL%** Devuelve el número de modelo del procesador instalados en el equipo.
- **%PROCESSOR_REVISION%** Devuelve el número de revisión del procesador.
- **%PROCESSOR_IDENTFIER%** Devuelve una descripción del procesador.
- **%PROMPT%** Devuelve la configuración del símbolo del sistema del intérprete actual. Generado por Cmd.exe.
- **%RANDOM%** Devuelve un número decimal aleatorio entre 0 y 32767. Generado por Cmd.exe.
- **%SYSTEMDRIVE%** Devuelve la unidad que contiene el directorio raíz del sistema operativo de servidor de Windows (es decir, la raíz del sistema).
- **%SYSTEMROOT%** Devuelve la ubicación del directorio del sistema operativo de servidor de Windows.

- **%TEMP% y %TMP%** Devuelve los directorios temporales predeterminados que utilizan las aplicaciones disponibles para los usuarios conectados actualmente. Algunas aplicaciones requieren TEMP y otras requieren TMP.
- **%TIME%** Devuelve la hora actual. Utiliza el mismo formato que el comando time /t. Generado por Cdm.exe. Para obtener más información acerca del comando time, vea Time.
- **%USERDOMAIN%** Devuelve el nombre del dominio que contiene la cuenta de usuario.
- **%USERNAME%** Devuelve el nombre del usuario que ha iniciado la sesión actual.
- **%USERPROFILE%** Devuelve la ubicación del perfil del usuario actual.
- **%WINDIR%** Devuelve la ubicación del directorio del sistema operativo.

3. USOS PRÁCTICOS

- Proporciona un entorno de ejecución a los programas, de forma que éstos puedan adaptarse a distintas plataformas y usuarios.
- Flexibiliza los programas y los ficheros por lotes, gracias a la inclusión de valores parametrizados en lugar de valores concretos.
- La imagen de cada proceso incluye una copia de las variables de entorno definidas.
- Cuando se lanza un programa desde un intérprete de comandos, el shell copiará las variables de entorno de su imagen a la imagen de proceso creado para la ejecución del programa.
- Proporciona un entorno de ejecución a los programas, de forma que éstos puedan adaptarse a distintas plataformas y usuarios.
- Flexibiliza los programas y los ficheros por lotes, gracias a la inclusión de valores parametrizados en lugar de valores concretos.
- La imagen de cada proceso incluye una copia de las variables de entorno definidas.
- Cuando se lanza un programa desde un intérprete de comandos, el shell copiará las variables de entorno de su imagen a la imagen de proceso creado para la ejecución del programa.

Si se crea un archivo batch para copiar un archivo determinado en la carpeta Escritorio y se desea que este puedan utilizarlo otros usuarios, es necesario usar la variable %USERPROFILE% ya que la carpeta Escritorio se encuentra dentro de la carpeta del usuario.

Variable de entorno PATH y ejecución de programas desde la línea de comandos.

✓ El intérprete de comandos CLI tratará de ejecutar cualquier cadena que el usuario introduzca (comprobaciones de CMD):

1. Si se ha especificado la ruta absoluta o relativa del fichero a ejecutar, lanzará directamente su ejecución.
2. Si no se ha especificado la ruta absoluta o relativa del fichero a ejecutar, realizará las siguientes comprobaciones:

- Comprobará si se trata de un comando interno. En caso afirmativo lo ejecutará.
- En caso de que no se trate de un comando interno, comprobará si se trata de un comando externo o de cualquier otro programa almacenado en disco. Para ello:
  - Si el fichero está en directorio actual, asumirá que se trata del fichero indicado, y lo ejecutará.
  - En caso contrario, buscará en los directorios especificados en la variable de entorno PATH.

✓ Comprobaciones de Power Shell:

1. Si se ha especificado la ruta absoluta o relativa del fichero a ejecutar, lanzará directamente su ejecución.
2. Si no se ha especificado la ruta absoluta o relativa del fichero a ejecutar, realizará las siguientes comprobaciones:

- Comprobará si se trata de un alias. En caso afirmativo, realizará la sustitución correspondiente (solo si no se ha efectuado yaanteriormente), pasando a evaluarse de nuevo por el Shell.
- En caso de que no se trate de una alias, comprobará si se trata de un cmdlet. En caso afirmativo, lo ejecutará,
- En caso de que no se trate de un comando interno, buscará en los directorios especificados en la variable de entorno PATH.