Boletín de actividades
Administración básica del sistema (Windows II)

Actualmente los sistemas Windows incorporan varias utilidades desde la que realizar tareas de administración del equipo.

Tradicionalmente, el **Panel de control** es la aplicación que agrupa las principales funciones de administración del sistema. Dentro de ella, las **Herramientas administrativas** es una de las opciones más utilizadas.

Windows 10 incorpora una nueva aplicación de administración conocida como **Configuración**. En el futuro podría llegar a reemplazar a otras aplicaciones de administración. Comprueba cómo acceder a esta nueva herramienta.

Actividad 1. Usuarios y grupos.
Las cuentas de usuario permiten dar un uso personal al equipo y los grupos sirven para facilitar la administración de varios usuarios.

Para empezar, comprueba los tipos de cuentas de usuario y grupos disponibles en Windows 10.
Consulta el *Apartado 2.1. Tipos de cuentas de usuario y grupos locales.*

Actividad 2. Usuarios y grupos.
Imagina el siguiente caso práctico:

Un equipo va a ser utilizado en un aula en la que se imparten clases de DAW en modalidad presencial (mañana) y semipresencial (tarde). El equipo debe disponer de una configuración personal para un alumno y un profesor de cada ciclo.

Crea los usuarios y grupos adecuados para este equipo teniendo en cuenta las siguientes consideraciones:

- Se facilite la gestión de los usuarios.
- Los usuarios alumnos tengan siempre la misma contraseña y no puedan cambiarla.
- Los usuarios profesores tengan que cambiar su contraseña periódicamente por seguridad.

Consulta los apartados: *Apartado 2.2.1. Gestión de cuentas de usuario y grupos locales (II)* y *Apartado 2.2.2. Gestión de cuentas de usuario y grupos locales (III)*.

Actividad 3. Seguridad de los recursos.
Una de las principales tareas de administración en un equipo es mantener la seguridad de los recursos del sistema. Para ello, se asocia a cada recurso una Lista de Control de Acceso (ACL, Access Control List) que determina los permisos de cada usuario sobre dicho recurso.

Entender el funcionamiento de las listas de control es una característica imprescindible para cualquier administrador de sistemas. Revisa el apartado *3.1. Permisos de archivos y carpetas (I)* para conocer sus puntos clave.

Actividad 4. Seguridad de los recursos.
Indica si las siguientes afirmaciones sobre las Listas de Control son verdaderas o falsas y corrígelas en este último caso:

1. Cuando un usuario intenta acceder a un recurso, se comprueba si aparece el SID de algún grupo al que pertenezca el usuario y en caso contrario, se comprueba si aparece el SID del usuario.

2. Cuando un usuario intenta acceder a un recurso, si en la ACL no aparece su SID, el sistema le concederá acceso al usuario.

3. Si el SID de un usuario aparece en la ACL de un recurso, el sistema comprueba la acción que quiere realizar (leer, borrar, escribir, etc.). Si está permitida, le autoriza a hacerlo, en caso contrario se lo impide.

4. En caso de existir en una ACL permisos contradictorios para un usuario, lo que más pesa es la concesión explícita del permiso. Si un permiso se ha concedido se le permite al usuario realizar la acción.

5. Si se ha concedido un permiso para el grupo al que pertenece un usuario pero no explícitamente para el usuario concreto, el permiso se deniega al usuario.

Actividad 5. Seguridad de los recursos.
Continuando con el caso práctico anterior:

Se pretende que los usuarios del equipo puedan almacenar sus ficheros de forma segura en una carpeta *Instituto* ubicada en el directorio raíz del sistema. Los alumnos pueden leer y escribir en ella, los profesores pueden leer pero no escribir y el resto de usuarios del equipo no pueden ni leer ni escribir en ella.

Consulta los apartados *3.1.1. Permisos de archivos y carpetas (II)* y *3.1.2. Permisos de archivos y carpetas (III)*.

Actividad 6. Seguridad de los recursos.
Indica si las siguientes afirmaciones sobre las Listas de Control son verdaderas o falsas y corrígelas en este último caso:

1. Cuando una carpeta se crea dentro de otra, ésta hereda automáticamente la ACL de la carpeta padre.

2. La única forma de deshabilitar los permisos heredados es eliminarlos totalmente y crear una nueva ACL desde 0.

3. Al editar una ACL no se deben eliminar los grupos como Creator Owner o System.

4. Al editar una ACL no se deben eliminar los grupos Usuarios o Usuarios autentificados.

5. Existen permisos avanzados para una mayor especificidad en las operaciones permitidas.

Actividad 7. Seguridad en los recursos.
Conocer los permisos avanzados o especiales es fundamental para realizar una correcta gestión de la seguridad de los recursos. Al seleccionar *Control total*, *Modificar*, *Leer y ejecutar*, *Mostrar el contenido de la carpeta*, *Lectura* o *Escritura* no estamos más que seleccionando un subconjunto de estos permisos.

Consulta la documentación oficial de Microsoft para conocer el significado y la relación de los permisos especiales: descripción de permisos avanzados y relación entre permisos.

Actividad 8. Directivas.
Las directivas en sistemas Windows son un conjunto de reglas que determinan el comportamiento del sistema. Las dos principales consolas que se utilizan para gestionar directivas son: *Directivas de seguridad local* y *Directivas de grupo local*. La primera está más relacionada con los usuarios y la segunda con el equipo en general.

Aplica las directivas adecuadas para establecer el siguiente comportamiento en el sistema:

1. Un usuario no pueda cambiar su contraseña por una que haya usado las 3 últimas veces.
2. Las contraseñas de los usuarios dejen de ser válidas después de 30 días.
3. La cuenta del usuario se bloquee después de 4 intentos fallidos de introducción de la contraseña.
4. Se impida el acceso al símbolo del sistema a todos los usuarios.

Consulta los apartados *3.2.1. Directivas de seguridad local* y *3.2.2. Directivas de grupo local.*

Actividad 9. Cuotas de disco.
Las cuotas de disco permiten establecer limitaciones en la cantidad de espacio en disco que utiliza cada usuario.

Establece cuotas de disco para los usuarios alumnos teniendo en cuenta las siguientes consideraciones:

- Cada usuario puede almacenar un máximo de 100 Mb.
- Si un usuario llega al límite, no se le debe permitir seguir almacenando información.
- Se debe registrar un evento cuando se supere el nivel de advertencia o se llegue al límite de cuota.

Comprueba que el límite de cuota se ha establecido correctamente para alguno de los alumnos. Para realizar la comprobación puedes configurar un límite cuota más bajo (por ejemplo, 200 Kb) y ocupar el espacio con algún archivo.

Actividad 10. Actualizaciones.
Windows Update es la aplicación para gestionar las actualizaciones del sistema. Utilízala para realizar las siguientes acciones:

a) Configura la aplicación para que también busque actualizaciones para otros productos de Microsoft cuando Windows se actualice.

b) Busca e instala la actualizaciones de Windows y otros productos de Microsoft que haya disponibles.

c) En ocasiones puede ser necesario desinstalar una actualización que ha provocado algún problema. Desinstala una actualización.

Consulta el apartado *4.1. Configuración de las actualizaciones automáticas.*

Actividad 11. Monitorización del sistema.
El monitor de rendimiento permite comprobar como se comportan los componentes del sistema bajo ciertas condiciones. El monitor muestra la evolución de un componente en una gráfica actualizada en tiempo real. Puede utilizarse para localizar errores o componentes que estén ralentizando el equipo.

Monitoriza las lecturas y escrituras en disco con el Monitor de Rendimiento. Sigue los siguientes pasos:

1. Elimina los contadores que tengas activos.

2. Añade los contadores *% de tiempo de escritura en disco* y *% de tiempo de lectura en disco* dentro de la categoría *Disco físico*.

3. Realiza algunas operaciones de lectura/escritura sobre el disco duro y observa como se comporta la gráfica.

Consulta el apartado *4.2. Monitorización del sistema y gestión de servicios (I): Monitor de rendimiento.*

Actividad 12. Gestión de servicios.
Los servicios son procesos en segundo plano que permiten el correcto funcionamiento del equipo. Por ejemplo, el servicio *bthserv* permite la detección y asociación de dispositivos bluetooth.

En ocasiones algunos servicios pueden no ser útiles y permanecen en el sistema consumiendo unos recursos innecesarios. Desactiva los servicios de Escritorio Remoto de Microsoft.

Consulta el apartado *4.2.1. Monitorización del sistema y gestión de servicios (II): Servicios.*

Actividad 13. Fragmentación.
La fragmentación en un disco duro se produce cuando un archivo no se almacena completamente en posiciones fisicamente contiguas. Cuando los archivos están muy fragmentados, el disco puede reducir su rendimiento al tener que saltar continuamente de una parte a otra para recuperar la información.

Windows dispone de una aplicación llamada *Desfragmentador de disco* que analiza el disco duro y redistribuye las partes de un mismo archivo para mejorar el rendimiento del disco.

Lee el siguiente artículo sobre la fragmentación en discos SSD e indica si son verdaderas o falsas las siguientes afirmaciones. Corrígelas en este último caso:

1. En los discos SSD no se produce fragmentación de archivos.

2. La incidencia de la fragmentación en los discos duros SSD en mucho menor que en los discos duros HDD.

3. Aunque no utilice la aplicación *Desfragmentador de disco*, Windows ya desfragmenta la unidades automáticamente para optimizar su rendimiento.

4. La desfragmentación de los discos SSD acorta de manera drástica su tiempo de vida.

Actividad 14. Desfragmentación.
Desfragmenta la unidad de disco principal del sistema.

A continuación, configura la desfragmentación automática de las unidades para que se realice de forma mensual.

Consulta el apartado *4.3. Desfragmentación y chequeo de discos (I)*.

Actividad 15. Chequeo de discos.
Windows dispone de la herramienta *Check Disk* para comprobar errores comunes en los discos. Utiliza esta utilidad para comprobar la unidad principal del sistema, localizar los sectores defectuosos y recuperar la información legible.

Consulta la documentación de Microsoft para conocer las opciones de la herramienta y el apartado *4.3.1. Desfragmentación y chequeo de discos (II).*

Actividad 16. Programación de tareas.
El *Programador de tareas* permite liberar a los administradores de tareas repetitivas a través de la ejecución automática de aplicaciones.

Programa una tarea para hacer una limpieza automática del equipo con el programa Ccleaner. Sigue las indicaciones del siguiente enlace.

Consulta el apartado *4.4. Programación de tareas de mantenimiento.*

Actividad 17. Restaurar el sistema.
Windows proporciona un mecanismo de recuperación del sistema a través de los llamados Puntos de restauración. Se recomienda su creación antes de realizar cualquier cambio crítico en el sistema.

Realiza los siguientes pasos para probar esta funcionalidad:

1. Crea un nuevo punto de restauración del sistema.

2. Instala un nuevo programa. Por ejemplo, Firefox o Chrome.

3. Imagina que la instalación anterior a provocado un estado inestable en el sistema. Restaura el equipo al punto de restauración creado anteriormente.

4. Comprueba como el equipo ya no incluye el programa instalado.

Consulta el apartado *4.5. Restaurar el sistema*.

Actividad 18. Copias de seguridad.
Mantener a salvo los datos es una de las principales tareas para los administradores. Windows proporciona la herramienta *Copias de seguridad* para realizar copias de los archivos y carpetas de los discos del sistema.

Realiza los siguientes pasos para probar esta funcionalidad:

1. Por razones obvias las copias deben almacenarse en una unidad distinta a la que se está respaldando. Por tanto, antes de utilizar la herramienta, añade un nuevo disco duro virtual a la máquina virtual. Este proceso debe realizarse con la máquina apagada. Añade un disco de 60 Gb (o del mismo tamaño del que dispone tu máquina actualmente) reservado dinámicamente.

2. Enciende de nuevo la máquina virtual y crea un nuevo volumen simple en el nuevo disco para que Windows pueda utilizarlo. Puedes realizar esta tarea desde la aplicación *Administrador de discos.* Asígnale la letra Z y la etiqueta *CopiasSeguridad*.

3. Ahora sí, realiza una copia de seguridad de la unidad del sistema en la nueva unidad.

4. Configura la herramienta de *Copias de seguridad* para que se realicen copias de seguridad sólo de la carpeta *Imágenes* cada 12 horas y las copias se mantengan durante 3 meses.

5. A continuación elimina todo el contenido de la carpeta *Imágenes* y restaura la copia de seguridad para recuperar los archivos.

Consulta el apartado *4.6. Copias de seguridad*.

Actividad 19. Protección del sistema.
El uso de programas de protección ante software malintencionado es fundamental en cualquier sistema. Windows proporciona la aplicación *Windows Defender* con este cometido. Consulta el siguiente artículo sobre su eficacia actual.

Utiliza esta herramienta para realizar un análisis que busque amenazas en el equipo.

Consulta el apartado *5.2. Windows Defender*.

Actividad 20. Prevención de ejecución de datos.
DEP (Data Execution Prevention) es una característica de seguridad de Windows que ayuda a impedir daños en el equipo producidos por virus y otras amenazas a la seguridad.

Los programas malintencionados pueden intentar atacar Windows mediante la ejecución de código desde ubicaciones de la memoria reservadas para Windows y otros programas autorizados. DEP supervisa la ejecución de estos programas para garantizar que utilizan la memoria del sistema de manera segura.

Activa DEP para todos los programas y servicios excepto para Internet Explorer.

Consulta el apartado *5.3. Prevención de ejecución de datos (DEP)*.

Actividad 21. Cifrado de archivos.
Windows permite almacenar información en el disco duro de forma cifrada utilizando el sistema de cifrado de archivos (EFS). Es el mayor nivel de protección que proporciona Windows para los usuarios.

Sigue los siguientes pasos para probar esta funcionalidad:

1. Inicia sesión con uno de los usuarios profesores y crea un fichero de texto de prueba en el Escritorio.

2. Cifra el archivo con EFS.

3. Cierra la sesión.

4. Inicia sesión con el administrador del sistema y verifica el acceso a los ficheros cifrados.

Consulta el apartado *5.4. Sistema de cifrado de archivos (I)*.