1. Windows

Arquitectura de Windows

- Kernel: Es el corazón del sistema operativo que maneja funciones criticas como: el manejo de la memoria, planificación de los procesos y el acceso a los dispositivos. A diferencias de otros sistemas en Windows el kernel es hibrido ya que combina características de un kernel monolítico y de un micro kernel, esto para mejorar la eficiencia y el modularidad. Este diseño híbrido equilibra rendimiento y flexibilidad.
- HAL o Hardware Abstraction Layer: Es la capa de abstracción de hardware, esta capa permite que el kernel opere independientemente del hardware subyacente, en otras palabras, aísla las peculiaridades del hardware permitiendo un desarrollo y mantenimiento del software más coherente y de forma más eficiente.
- WIN32 y UWP: Es la plataforma universal de Windows, concretamente son subsistemas a nivel de usuario que ofrecen APIs para que las aplicaciones interactúen con el hardware por medio del kernel. Hay diferencias entre estas 2:
  - Win32: Es el conjunto de APIs que forman parte del entorno de usuario en Windows. Este mismo, no interactúa directamente con el hardware, sino que hace llamadas al kernel a través de la API de Windows.
  - UWP (Universal Windows Platform): Es un plataforma de desarrollo más moderna, esta diseñada para crear aplicaciones universales que funcionen en múltiples dispositivos, como: PC, tablets, Xbox y dispositivos IoT, estas aplicaciones se ejecutan en un entorno sandbox, lo que mejora la seguridad y la portabilidad. En si, no es un subsistema, si no un marco de desarrollo.
- Windows Manager: Los gestores de ventana controlan la presentación visual de la interfaz gráfica, incluyendo: la gestión de ventanas, interacción con el usuario y los efectos gráficos.
- Network subsystem: Este gestiona todas las comunicaciones de red incluyendo el acceso a internet y la conectividad de la red local donde esté conectado el dispositivo. Incluye el soporte para protocolos como TCP/IP y permite la comunicación entre aplicaciones y redes locales o remotas.
- Device Drivers: Proporcionan la interfaz necesaria para que el kernel y el hardware pueden interactuar de forma eficiente.Windows Driver Model (WDM) y el Windows Driver Framework (WDF), que son las arquitecturas modernas para el desarrollo de controladores en Windows.
- Windows Registry: Es una base de datos centralizada que almacena configuraciones y opciones en la cual los usuarios pueden personalizar el sistema. Almacena configuraciones tanto del sistema como de aplicaciones y controladores.

- Windows Services: Es la parte del software que utiliza Windows para realizar tareas específicas a nivel del sistema operativo y de aplicaciones, por lo general lo hace de forma transparente al usuario.Service Control Manager (SCM), es el componente encargado de gestionar el ciclo de vida de estos servicios.
- CMD: Es un emulador de terminal que permite interactuar con el sistema operativo por medio de comandos, es un componente heredado. En la actualidad, PowerShell es la interfaz de línea de comandos más moderna y potente de Windows.
- Security Subsystem: Acá el sistema puede gestionar el control acceso y la auditoría. Su motivo principal es mantener la integridad y la seguridad del sistema operativo y de los datos del usuario. Entre sus componentes clave están: Local Security Authority Subsystem Service (LSASS), el Security Account Manager (SAM) y el Active Directory (en entornos de dominio). Además de ellos, es el encargado de gestionar políticas de seguridad, autenticación y autorización.

Tipos de software

En Windows existen 3 tipos de licencias:

- OEM (Original Equipment Manufacturer): Este tipo de licencias por lo general vienen preinstaladas en dispositivos nuevos y están vinculados a un hardware en específico, no son transferibles de un equipo a otro. El soporte técnico en este caso lo brinda la empresa, no Microsoft.
- RETAIL (Full Packaged Product - FPP): Estas licencias se pueden transferir entre dispositivos, siempre y cuando la licencia se desactive del dispositivo anterior antes de activarse en el nuevo dispositivo. Se compran de manera independiente.
- VOLUMEN (Volume Licensing): Las licencias de volumen están orientadas a empresas, organizaciones o entornos educativos, ya que con ella se permite la activación en múltiples dispositivos dentro de una red corporativa.

Diferencias entre PowerShell y CMD.

En ambas se puede ejecutar código y darle ordenes al sistema para que haga lo que se desea, pero hay diferencias entre ambos.

- CMD o Command Prompt: Se basa en la interfaz de línea de comandos de MS-DOS, es una interfaz que con el tiempo no ha tenido cambios visuales y no es tan cómoda de utilizar hoy en día. A pesar se ser una herramienta útil para tareas básicas como navegación de archivos, ejecución de scripts batch y ejecución de comandos del sistema, es bastante limitada en comparación con PowerShell.
- PowerShell: Es una Shell orientada a objetos con un lenguaje de scripting completo. Su integración con .NET Framework (en Windows PowerShell) y .NET Core/5+ (en PowerShell

Core y PowerShell 7+) permite manipular no solo texto, sino objetos completos con propiedades y métodos, lo cual lo hace extremadamente potente para la administración de sistemas y automatización. Es un entorno completo que combina una shell interactiva y un lenguaje de programación robusto.

Las diferencias más notables son:

- **Potencia y flexibilidad:** PowerShell permite trabajar con objetos, lo que facilita la manipulación de datos complejos sin necesidad de parsear texto como en CMD.
- **Basado en .NET:** Esto le otorga acceso a bibliotecas y clases de .NET, expandiendo enormemente las capacidades de scripting y administración.
- **Capacidades avanzadas:** PowerShell soporta cmdlets, scripts, funciones, módulos, acceso a WMI (Windows Management Instrumentation), REST APIs, y herramientas de administración remota como WinRM.

Comandos vs Cmdlets

- **Comandos**:
  Son programas externos o ejecutables independientes del entorno de shell, que realizan tareas específicas. Ejemplos comunes incluyen `ping`, `ipconfig` y scripts batch (`.bat`, `.cmd`). Estos comandos se ejecutan tanto en CMD como en PowerShell porque PowerShell tiene compatibilidad con comandos externos de Windows.
- **Cmdlets**:
  Son comandos internos exclusivos de PowerShell, diseñados como instancias de clases .NET. Operan con objetos en lugar de texto, lo que permite acceder directamente a propiedades y métodos sin necesidad de parseo. Los cmdlets siguen la convención Verbo-Sustantivo (por ejemplo: `Get-Process`, `Stop-Service`, `New-Item`)

Directorios Importantes en Windows

C:
├── Windows
│ ├── System32 -Ficheros críticos del sistema y controladores.
│ ├── SysWOW64 -Compatibilidad para aplicaciones de 32 bits en sistemas de 64 bits.
│ ├── Temp -Archivos temporales del sistema.
│ ├── Prefetch -Ficheros de precarga para optimizar tiempos de carga.
│ ├── SoftwareDistribution
│ │ └── Download -Archivos temporales descargados por Windows Update.
│ ├── Tasks -Ficheros de tareas programadas del sistema.
│ ├── Logs -Archivos de registro del sistema.
│ └── Resources -Temas y elementos visuales del sistema operativo.

```
├── Boot -Archivos relacionados con el proceso de arranque.
├── Program Files -Aplicaciones de 64 bits instaladas.
├── Program Files (x86) -Aplicaciones de 32 bits instaladas en sistemas de 64 bits.
├── ProgramData -Configuraciones y datos compartidos de aplicaciones.
├── Users
│  ├── nom_user
│  │  ├── AppData
│  │  │  ├── Local -Configuraciones locales específicas del usuario.
│  │  │  ├── LocalLow -Configuraciones locales con menor nivel de privilegio.
│  │  │  └── Roaming -Configuraciones sincronizables entre dispositivos.
│  │  ├── Documentos -Documentos personales del usuario.
│  │  ├── Escritorio -Elementos en el escritorio del usuario.
│  │  └── Descargas -Archivos descargados por el usuario.
│  └── Default -Perfil predeterminado para nuevos usuarios.
├── Recovery -Herramientas y datos para la recuperación del sistema.
├── System Volume Information -Metadatos del volumen y puntos de restauración.
├── hiberfil.sys -Archivo oculto para la hibernación del sistema.
├── pagefile.sys -Archivo de paginación para memoria virtual.
├── Swapfile.sys -Archivo de intercambio para aplicaciones modernas.
└── Otros
├── Windows.old -Restos de versiones anteriores de Windows tras una actualización.
└── Archivos temporales -Dependiendo de configuraciones específicas.
```

Fichero Importantes

- **Ntldr y bootmgr**: Ntldr está presente en versiones inferiores a Windows vista, posterior a eso fue remplazado por **bootmgr**, el cual se usa actualmente. Ayudan a cargar el sistema operativo cuando se enciende la PC, más concretamente son gestores de arranque.
- **Ntoskrnl**: Es el núcleo de Windows y se encarga de la gestión de memoria, la gestión de procesos y la interacción con el hardware. Es fundamental para la operación del sistema y proporciona servicios esenciales como la comunicación entre el hardware y las aplicaciones.
- **Winload**: Responsable de cargar Windows durante el proceso de inicio.
- **Explorer**: Proceso del explorador de Windows, responsable de proporcionar la interfaz gráfica al usuario, incluyendo: escritorio, barra de tareas, menú de inicio, etc. Por consiguiente, consume muchos recursos del hardware.
- **Svchost**: Aloja servicios de Windows, por consecuencia varios servicios pueden compartir un único proceso svchost, esto para reducir el consumo de recursos.
- **C:\Windows\System32\Config**: Se almacenan los archivos de la base de datos del registro de Windows, los cuales contienen configuraciones cruciales para el sistema operativo, aplicaciones y hardware.

- C:\Windows\System32\Drivers: Contiene los controladores de dispositivos que permiten la interacción entre el sistema operativo y el hardware. Los controladores son programas que permiten que el sistema operativo reconozca y se comunique con los dispositivos
- Pagefile: Es un archivo utilizado para la memoria virtual. Cuando la memoria RAM física se llena, Windows utiliza el `pagefile.sys` como espacio adicional de almacenamiento temporal, lo que permite que las aplicaciones continúen ejecutándose incluso cuando no hay suficiente memoria RAM disponible.
- Hiberfil: Este archivo se utiliza cuando el sistema entra en hibernación. Almacena el contenido de la memoria RAM en el disco duro, lo que permite que, al encender el equipo nuevamente, el sistema se recupere exactamente en el mismo estado que cuando se apagó.
- C:\Windows\System32\services.exe: Es el proceso encargado de gestionar la ejecución de los servicios del sistema, tales como servicios de red, controladores, y otros procesos fundamentales para la operación de Windows.
- C:\Windows\System32\drivers\etc\hosts: El archivo `hosts` permite la asignación manual de nombres de dominio a direcciones IP. Es una forma estática de gestionar las direcciones y es utilizado por Windows antes de realizar consultas DNS.
- C:\Windows\System32\userinit.exe: Es el encargado de inicializar el entorno del usuario cuando Windows arranca. Después de la autenticación del usuario, este proceso configura el entorno del escritorio, las configuraciones de red y otros aspectos de la sesión del usuario.
- C:\Windows\System32\lsass.exe: El `lsass.exe` (Local Security Authority Subsystem Service) gestiona la política de seguridad del sistema, incluidas las verificaciones de autenticación del usuario, la seguridad de contraseñas y la implementación de las políticas de seguridad.
- C:\Windows\System32\smss.exe: Responsable de iniciar la sesión de un usuario y gestionar el entorno de los subsistemas.
- C:\Windows\memory.dmp: Este archivo se genera cuando el sistema experimenta un "pantallazo azul" (BSOD - Blue Screen of Death). El archivo de volcado de memoria contiene una copia del contenido de la memoria RAM en el momento del error, lo que permite analizar la causa del fallo.

Introducción a los permisos

En Windows los permisos definen que tipo de acceso se otorga a un usuario o grupo sobre un objeto, como puede ser un archivo o carpeta. Estos permisos se pueden asignar tanto a grupos, usuarios o a otros objetos con identificadores de seguridad en el dominio; a nivel empresarial. Y a nivel de uso doméstico se pueden asignar tanto a grupos y usuarios locales (que estén en el equipo donde reside el mismo objeto).
Existen 5 tipos de permisos:

- Lectura: Permite ver archivos y carpetas.
- Escritura: Permite la modificación de los archivos o carpetas.

- **Ejecución**: Permite ejecutar archivos que sean ejecutables.
- **Modificación**: Es una combinación entre los permisos de: lectura, escritura, ejecución y la capacidad de eliminar archivos y carpetas.
- **Control total**: Otorgar todos los permisos anteriores, más la capacidad de cambiar permisos y tomar propiedad de estos archivos y carpetas.

Conceptos importantes

- **Propiedad**: Cada objeto en Windows posee un propietario, generalmente es el usuario que creo dicho objeto, por ende, el propietario tiene la capacidad de cambiar los permisos de ese objeto, independientemente de los permisos establecidos.
- **Herencia**: Es un mecanismo que permite que los objetos dentro de una carpeta hereden automáticamente los permisos de dicha carpeta, solo los permisos que están marcado para ser heredados son efectivamente heredados. La herencia puede ser desactivada, permitiendo establecer permisos específicos para ciertos objetos sin que se vean afectados por los permisos heredados.
- **Derechos de usuario**: En Windows son privilegios específicos otorgados a cuentas de usuarios o grupos, que permiten realizar acciones concretas en el sistema. *Los permisos son a nivel de objetos y los derechos a nivel de acciones*
- **Etiquetas de integridad**: Forman parte del modelo de seguridad de Windows y se utilizan para clasificar procesos y objetos según su nivel de confianza. Su función principal es prevenir que los objetos de menor integridad interactúen o afectan a procesos u objetos de mayor integridad. Posee 4 niveles: Sistema, Alto, Medio y Bajo.
- **Listas de control de acceso o ACL**: Son más utilizadas a nivel empresarias. Su funcionamiento se basa en un punto de control de acceso o ACE, define los permisos para los usuarios y grupos sobre un objeto del sistema. Permite centralizar toda la administración de permisos en un mismo lugar. Existen 2 tipos principales:
  - **DACL (Discretionary Access Control List)**: Es la lista que define qué usuarios y grupos tienen acceso y qué tipo de acceso tienen a los objetos.
  - **SACL (System Access Control List)**: Se usa para la auditoría, puede configurarse para registrar los eventos de acceso a un objeto y generar entradas de auditoría cuando se accede o modifica el objeto.

Atributos

Los atributos en Windows son marcadores que definen propiedades y comportamientos especiales en archivos y carpetas, lo que previene que un archivo sea modificado accidentalmente, los atributos son:

- **Read-Only**: Previene que un fichero sea modificado accidentalmente, ya que si el fichero posee este atributo solo se va a poder leer, no modificar. Este atributo no impide que se

elimine el archivo, solo previene su modificación.

- **Hidden**: Si un archivo posee este atributo no va a aparecer en las búsquedas normales. Los archivos ocultos pueden verse habilitando la opción "Mostrar archivos ocultos" en las opciones de carpeta del Explorador de Windows.
- **System**: Se identifican activos críticos para el funcionamiento de Windows, generalmente no deben ser modificados por los usuarios.
- **Archive**: Es marcado automáticamente por Windows cuando un archivo es modificado, indicando que necesita se respaldado.
- **Directory**: Es especifico de las carpetas e indica que el objeto es un directorio.
- **Temporary**: Es utilizados por archivos que son utilizados temporalmente y que pueden ser eliminados después de su uso. No se aplica manualmente Windows asigna este atributo automáticamente a las carpetas.
- **Offline:** Señala que los datos del archivo no están disponibles de forma inmediata.

Los atributos se pueden modificar con el comando Attrib

Comodines

Son caracteres especiales para representar uno o más caracteres en una cadena de texto, son ampliamente utilizados en búsqueda de archivos o para hacer operaciones con comandos, son los siguientes:

- **Asterisco** : Representa cualquier número de caracteres, incluyendo 0.
- **Interrogación cerrada (?)**: Representa un único carácter.
- **Corchetes ([ ])**: Hace coincidir los caracteres incluidos entre los corchetes.
- **Exclamación cerrada (!)**: Excluye los caracteres incluidos entre los corchetes.
- **Guión (-)**: Hace coincidir cualquier intervalo de caracteres. Recuerde que debe especificar los caracteres en orden ascendente
- **Almohadillas (#)**: Hace coincidir cualquier carácter numérico.

Variables

Son una serie de valores dinámicos que están dentro de un sistema operativo, en Windows se utilizan para determinar información específica, información correspondiente al entorno del sistema operativo. Estas variables incluyen información como: rutas de archivos, nombres de directorio, datos de configuración y demás información que le permite al sistema trabajar de forma más optima. Existen 2 tipos de variables:

- **Variables de usuario**: Son específicas para cada usuario en el sistema y almacenan configuraciones que solo afectan al entorno actual del usuario.

- Variables de sistema: Afectan a todos los usuarios en la máquina, ya que estas son globales y se utilizan principalmente para configurar información del sistema operativo y del software instalado.

Ejemplos de variables

- PATH: Almacena las rutas de los archivos ejecutables
- TEMP y TMP: Su valor es la ubicación donde se almacenan los archivos temporales.
- USERPROFILE: Su valor es la ruta del perfil del usuario actual.
- SYSTEMROOT: Su valor es el directorio de instalación de Windows.
- COMSPEC: Su valor es la ubicación del intérprete de Windows.
- HOMEPATH: Es la parte relativa del perfil del usuario, como `\Users\NombreUsuario`, pero sin incluir la unidad (`C:`).
- PROGRAMFILES: Su valor es el directorio de instalación de los programas.
- WINDIR: Su valor es el directorio donde está instalado Windows.
- APPDATA: Tiene como valor la ubicación para los datos de la aplicación para el usuario actual.
- LOCALAPPDATA: Funciona para el almacenamiento de datos de aplicación específicos.
- PUBLIC: Su valor es la ruta del directorio que se usa para los archivos compartidos entre usuarios.
- COMPUTERNAME: Almacena el nombre del equipo asignado en la configuración del sistema.
- USERNAME: Almacena el nombre del usuario actual.
- USERDOMAIN: Almacena el dominio donde se encuentra el usuario actual.
- ALLUSERSPROFILE: Ubicación del perfil común para todos los usuarios.
- NUMBER_OF_PROCESSORS: Número de núcleos de CPU disponibles.
- PROCESSOR_ARCHITECTURE: Arquitectura del procesador.

Para obtener la salida de cualquiera de estas variables de entorno se puede hacer de la siguiente manera:
Para CMD:

- Para ver una variable especifica (`echo %<nombre_variable>%`).
- Para ver todas las variables de entorno (`set`).

Para PowerShell:

- Para ver una variable especifica (`echo $env:<nombre_variable>`).
- Para ver todas las variables de entorno (`Get-ChildItem Env:`).

Redirecciones en PowerShell

Las redirecciones permiten manipular la información que devuelve un comando o cmdlet, para enviarla a otro comando, almacenarla o gestionarla de diferentes maneras.
Operadores de redirección:

- (>): Redirige la salida estándar a un archivo, sobrescribiendo el contenido si el archivo ya existe..
- (>>): Redirige todo el estándar output por defecto, pero no sobrescribe la información, solo la añade.
- (2>): Redirige la salida de error a un archivo, sobrescribiéndolo.
- (2>>): Redirige la salida de error a un archivo, sobrescribiéndolo.

Comandos de Windows para CMD

De gestión de variables

- set: Muestra, crea o modifica variables de entorno temporales.
- setx: Crea o modifica variables de entorno permanentes.
- echo: Muestra el valor de una variable.

De gestión de navegación, ficheros y directorios

- dir: Lista el contenido de un directorio.
- cd: Cambia de directorio.
  Doble punto (..): Sube un nivel en el árbol de directorios.
- md o mkdir: Crea un directorio.
- rd o rmdir: Elimina un directorio vacío.
- del: Elimina un archivo.
- copy: Copia archivos a otro directorio.
- move: Mueve archivos o renombra.
- ren: Renombra un archivo.
- attrib: Cambia atributos de archivos.

De ayuda y soporte

- help: Muestra la lista de comandos disponibles.
- help [comando]: Muestra ayuda sobre un comando específico.
- [comando] /?: Alternativa para obtener ayuda sobre un comando.

De gestión de usuario

(Requiere CMD como administrador)

- net user: Lista los usuarios del sistema.
- net user [usuario]: Muestra información de un usuario.
  /add: Crea un nuevo usuario.
  /delete: Elimina un usuario.

De gestión de grupos

(Requiere CMD como administrador)

- net localgroup: Lista los grupos locales.
- net localgroup [grupo]: Muestra miembros de un grupo.
  /add: Añade un usuario a un grupo.
  /delete: Elimina un usuario de un grupo.

De gestión de procesos

- tasklist: Lista procesos en ejecución.
- taskkill /IM [nombre_proceso] /F: Finaliza un proceso por nombre.
- taskkill /PID [ID_proceso] /F: Finaliza un proceso por su ID.

De gestión de red

- ipconfig: Muestra configuración de red.
  /all: Información detallada de la red.
  /release: Libera la dirección IP actual.
  /renew: Solicita una nueva dirección IP.
- ping [dirección]: Verifica la conectividad con una IP o dominio.
- tracert [dirección]: Muestra la ruta hacia un servidor.
- netstat: Muestra conexiones de red activas.
- nslookup [dominio]: Resuelve el nombre de dominio a IP.
- arp -a: Muestra la caché ARP (direcciones IP ↔ MAC).
- route print: Muestra la tabla de enrutamiento.

Comandos de Windows para PowerShell

De gestión de variables

- $env: [nombre_variable]: Accede a las variables de entorno.
- $Variable = "Valor": Crea o modifica variables de PowerShell (solo en la sesión actual).
- Remove-Variable: Elimina una variable.

- Get-Variable: Lista las variables de PowerShell.

De gestión de navegación, ficheros y directorios

- Get-Location:Muestra la ubicación actual.
- Set-Location: Cambia de directorio (equivalente a `cd`).
- New-Item: Crea archivos o carpetas.
- Remove-Item: Elimina archivos o carpetas.
- Get-ChildItem: Lista el contenido de un directorio (equivalente a `dir`).
- Copy-Item: Copia archivos o carpetas.
- Move-Item: Mueve archivos o carpetas.
- Rename-Item: Renombra archivos o carpetas.

De ayuda y soporte

- Get-Help: Muestra ayuda sobre un comando.
- Get-Command: Lista todos los comandos disponibles en PowerShell.
- Get-Alias: Muestra los alias de comandos (como abreviaturas).

De gestión de usuario

(Requiere permisos de administrador)

- Get-LocalUser: Lista los usuarios locales.
- New-LocalUser: Crea un nuevo usuario.
- Remove-LocalUser: Elimina un usuario.
- Set-LocalUser: Modifica las propiedades de un usuario.

De gestión de usuario

(Requiere permisos de administrador)

- Get-LocalGroup: Lista los grupos locales.
- New-LocalGroup: Crea un grupo local.
- Remove-LocalGroup: Elimina un grupo local.
- Add-LocalGroupMember: Añade un usuario a un grupo.
- Remove-LocalGroupMember: Elimina un usuario de un grupo.

De gestión de procesos

- Get-Process: Lista procesos en ejecución.
- Stop-Process: Finaliza un proceso por nombre o ID.

- Start-Process: Inicia un nuevo proceso.

De gestión de red

- Get-NetIPAddress: Muestra direcciones IP configuradas.
- Test-Connection: Verifica conectividad (equivalente a `ping`).
- Get-NetAdapter: Lista los adaptadores de red.
- Get-DnsClient: Muestra la configuración DNS.
- Get-NetRoute: Muestra la tabla de enrutamiento.

Alias en PowerShell

Un alias es una palabra clave o un nombre alternativo que simplifica la ejecución de comandos o cmdlets en PowerShell, permitiendo usar atajos personalizados. Los alias son temporales y solo existen durante la sesión actual, a menos que se guarden en el perfil de PowerShell.

Cmdlets de gestión de alias

- Get-Alias: Muestra los alias definidos para comandos en PS.
- New-Alias: Permite crear nuevos alias en la sesión actual.
- Remove-Alias: Elimina alias ya existentes en la sesión actual.
- Export-Alias: Exporta los alias de la sesión actual a un archivo.
- Import-Alias: Importa alias desde un archivo a la sesión actual.

Introducción a la seguridad en Windows

Aislamiento de núcleo: Es una característica de seguridad de Windows que utiliza virtualización basada en hardware para crear un entorno seguro y aislado donde se ejecutan los procesos críticos del sistema operativo. Su objetivo es proteger el kernel de Windows contra ataques avanzados como el Kernel-mode malware o las técnicas de inyección de código malicioso.
Integridad de la memoria: Es una extensión del aislamiento de núcleo, también conocida como Hypervisor-Protected Code Integrity (HVCI). Esta función asegura que solo controladores y binarios firmados digitalmente y de confianza puedan interactuar con el kernel aislado.
DEP (Data Execution Prevention): Es una función de seguridad de Windows que previene la ejecución de código desde áreas específicas de la memoria marcadas solo para almacenamiento de datos. De esta manera, impide ataques como buffer overflows o shellcode execution.
Directivas de seguridad: Son un conjunto de reglas y configuraciones que controlan la seguridad y el comportamiento del sistema. Incluyen:

- Políticas de cuenta: Reglas de contraseñas, bloqueo de cuentas, etc.

- **Asignación de derechos de usuario**: Determina qué acciones puede realizar un usuario o grupo (por ejemplo, iniciar sesión de manera local o remota).
- **Opciones de seguridad local**: Configuración de UAC (User Account Control), Firewall, cifrado, etc.

Directivas de auditoría: Son una subcategoría de las directivas de seguridad, enfocadas en el registro y monitoreo de eventos relacionados con la seguridad. Permiten auditar acciones como:

- Acceso a recursos del sistema.
- Uso de privilegios.
- Cambios en la configuración de seguridad.
- Intentos de inicio de sesión fallidos o exitosos.

Visor de eventos: Es una herramienta integrada en Windows que registra todas las acciones y eventos del sistema, agrupados en categorías como errores, advertencias, información operativa y de seguridad. Es esencial para:

- **Auditoría de seguridad:** Seguimiento de intentos de acceso, cambios en políticas, etc.
- **Diagnóstico de problemas:** Identificación de errores de software y hardware.
- **Análisis forense:** Recolección de evidencias mediante la revisión de logs históricos.

Directivas de grupo: Son configuraciones centralizadas que administran el comportamiento y las políticas de seguridad en equipos conectados a un dominio de Active Directory. Permiten aplicar configuraciones de usuario y sistema a múltiples equipos, por lo que se utilizan principalmente en entornos empresariales.
BitLocker:Es una herramienta de cifrado de disco completa integrada en Windows. Utiliza el algoritmo AES (Advanced Encryption Standard) con longitudes de clave de 128 bits o 256 bits. BitLocker cifra todo el volumen de almacenamiento y protege los datos en caso de pérdida o robo del dispositivo.
Windows Defender: Es la solución de seguridad integrada de Windows. Proporciona protección en tiempo real contra amenazas como virus, malware, ransomware, spyware y ataques basados en la web. Su ventaja principal es estar completamente integrado con el sistema operativo, ofreciendo un rendimiento optimizado sin necesidad de software adicional.