
Sistema Operativo Windows

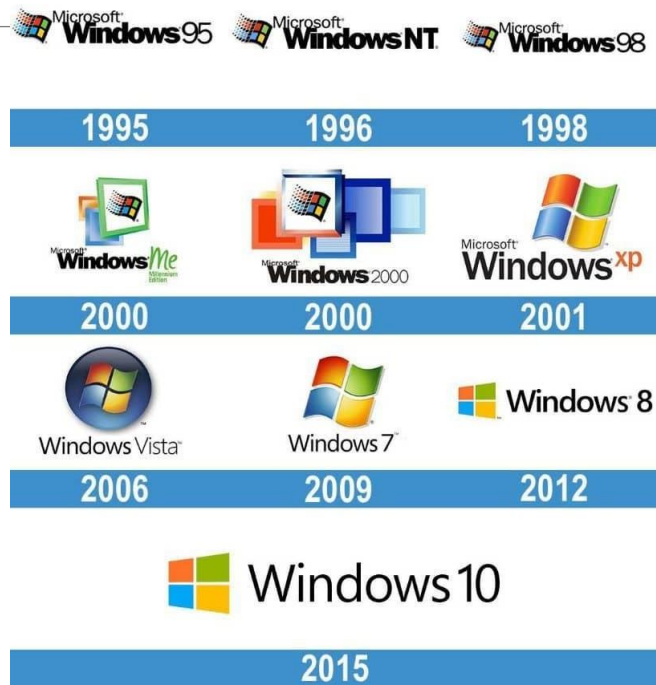
A solid blue horizontal bar spanning the entire width of the slide at the bottom.

Historia de Windows



Versiones de Windows Desktop

- Desde 1993, han habido más de 20 lanzamientos de Windows que están basados en el sistema operativo NT (OS)
- Las computadoras y los sistemas operativos de 64 bits son compatibles con programas anteriores de 32 bits, pero los programas de 64 bits no se pueden ejecutar en hardware anterior de 32 bits.
- Con cada nuevo lanzamiento de Windows, el sistema operativo se ha mejorado con la incorporación de más funciones.
- Microsoft ha anunciado que Windows 11 es la última versión de Windows.



Versiones de Windows Server

SO	Versiones
Windows Server NT	Professional, Server, Advanced Server, Datacenter Server
Windows Server 2000/2003	Web Edition, Standard Edition, Enterprise Edition, Datacenter Edition, Small Business Edition
Windows Server 2008 R2	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server y para sistemas con procesadores Itanium
Windows Server 2012	Foundation, Essentials, Standard, Datacenter
Windows Server 2012 R2	Foundation, Essentials, Standard, Datacenter
Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server
Windows Server 2019	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server
Windows Server 2022	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server

Vulnerabilidades del Sistema Operativo

- Los sistemas operativos consisten en millones de líneas de código. Todo este código acarrea vulnerabilidades.
- Una vulnerabilidad es una imperfección o debilidad que puede ser aprovechada por un atacante para reducir la viabilidad de la información de una computadora.
- Para aprovechar una vulnerabilidad de un sistema operativo, el atacante debe utilizar una técnica o herramienta para atacarla.
- El atacante puede utilizar la vulnerabilidad para hacer que la computadora actúe de una manera diferente a la prevista en su diseño.
- En general, el objetivo es hacerse con el control no autorizado de la computadora, cambiar permisos o manipular datos.



[Investiguemos un poco con Shodan](#)

Vulnerabilidades del Sistema operativo

Estas son algunas recomendaciones de seguridad habituales del sistema operativo Windows:

Recomendación	Descripción
Protección contra virus o malware	<ul style="list-style-type: none">• De manera predeterminada, Windows utiliza Windows Defender para la protección contra el malware• Windows Defender ofrece un conjunto de herramientas de protección incorporado en el sistema.• Si Windows Defender está desactivado, el sistema es más vulnerable a los ataques y al malware.
Servicios Desconocidos o no administrados	<ul style="list-style-type: none">• Existen muchos servicios que se ejecutan en segundo plano.• Es importante asegurarse de que cada servicio pueda identificarse y sea seguro.• Con un servicio desconocido ejecutándose en segundo plano, la computadora puede ser vulnerable a los ataques.
Cifrado	<ul style="list-style-type: none">• Cuando los datos no se encuentran encriptados pueden ser fácilmente reunidos y explotados.• Esto no es solamente importante para computadoras de escritorio, sino especialmente para dispositivos móviles.
Política de seguridad	<ul style="list-style-type: none">• Se debe configurar una buena política de seguridad y debe cumplirse.• Muchos ajustes en el control de la política de seguridad de Windows pueden evitar ataques.

Vulnerabilidades del Sistema operativo

Recomendación	Descripción
Firewall	<ul style="list-style-type: none">• Por defecto, Windows utiliza el Firewall de Windows para limitar la comunicación con dispositivos en la red con el tiempo, es posible que las reglas ya no se apliquen.• Es importante revisar la configuración del firewall periódicamente para asegurarse de que las reglas todavía estén vigentes y eliminar aquellas que ya no lo estén.
Permisos de archivo y uso compartido	<ul style="list-style-type: none">• Estos permisos deben ser aplicados correctamente. Es fácil otorgar el control total al grupo "Todos", pero esto permite que todas las personas accedan a todos los archivos.• Es mejor otorgar a cada usuario o grupo los permisos mínimos necesarios para todos los archivos y carpetas.
Contraseña débil o sin contraseña	<ul style="list-style-type: none">• Muchas personas eligen una contraseña débil o no utilizan contraseñas del todo.• Es especialmente importante asegurarse de que todas las cuentas, especialmente la cuenta de administrador, tengan una contraseña muy fuerte.
Iniciar sesión como administrador	<ul style="list-style-type: none">• Cuando el usuario inicia sesión como administrador, cualquier programa que ejecuten tendrá los privilegios de esa cuenta.• Es mejor iniciar sesión como un usuario estándar y utilizar solamente la contraseña de administrador para realizar determinadas tareas.

Arquitectura y Operaciones

A solid blue horizontal bar spanning the entire width of the slide at the bottom.

Sistemas de archivos de Windows

Un sistema de archivos es una forma de organizar la información en los medios de almacenamiento. La siguiente tabla enumera los sistemas de archivos compatibles con Windows:

Sistema de archivos de Windows	Descripción
exFAT	<ul style="list-style-type: none">• Este es un sistema de archivos simple compatible con muchos sistemas operativos diferentes.• FAT tiene limitaciones en la cantidad de particiones, tamaños de partición y tamaños de archivo que puede abordar, por lo que generalmente ya no se usa para discos duros o unidades de estado sólido.• Tanto FAT16 como FAT32 están disponibles para su uso, siendo FAT32 el más común ya que tiene muchas menos restricciones que FAT16.
Sistema de archivos jerárquico + (HFS+)	<ul style="list-style-type: none">• Este sistema de archivos se usa en computadoras MAC OS X y permite nombres de archivo, tamaños de archivo y tamaños de partición mucho más largos.• Aunque no es compatible con Windows sin software especializado, Windows es capaz de leer datos de particiones HFS+.

Sistema de Archivos

Arquitectura de Windows y Operaciones

de Windows

Sistema de archivos de Windows	Descripción
Sistema de archivos extendido (EXT)	<ul style="list-style-type: none">• Este sistema de archivos es utilizado con computadoras basadas en Linux.• Aunque no es compatible con Windows, Windows es capaz de leer datos de particiones EXT con software especializado.
Sistema de archivos de nueva tecnología (NTFS)	<ul style="list-style-type: none">• Este es el sistema de archivos usado más comúnmente cuando está instalado en Windows. Todas las versiones de Windows y Linux admiten NTFS.• Los equipos Mac-OS X sólo pueden leer una partición NTFS. Son capaces de escribir en una partición NTFS después de instalar controladores especiales.

Sistema de Archivos de Windows FAT

La FAT o Tabla de Asignación de Archivos es un sistema de archivos utilizado por los sistemas operativos para localizar los archivos en un disco.

Debido a la fragmentación, los archivos pueden estar dispersos y divididos en secciones. El sistema FAT mantiene un registro de todas las partes del archivo.

La FAT ha existido como sistema de archivos desde la aparición de los ordenadores personales.

Sistema de Archivos de Windows FAT

Características

- Nombre del archivo:
 - El sistema FAT en MS DOS sólo permite nombres de archivo de 8 caracteres
 - El sistema de archivos FAT en Windows admite nombres de archivo largos, con una ruta de archivo completa de hasta 255 caracteres
 - El nombre del archivo debe comenzar con caracteres alfanuméricos
 - Los nombres de archivo pueden tener cualquier carácter excepto "/ = [],? ^"“
 - Los nombres de archivo pueden tener más de un punto y espacios.
 - Los caracteres que vienen después del último punto en el nombre de archivo completo se consideran como la extensión del archivo.

Sistema de Archivos de Windows FAT

Características

- El sistema de archivos FAT no admite la seguridad de carpetas y local. Esto significa que los usuarios que inician sesión en un ordenador de forma local tendrán acceso completo a las carpetas y archivos que se encuentran en las particiones FAT.
- Proporciona un acceso rápido a los archivos. La velocidad depende del tamaño de la partición, el tamaño del archivo, el tipo de archivo y el número de archivos en la carpeta.

Sistema de Archivos de Windows FAT 32

Se trata de una versión avanzada del sistema de archivos FAT y puede utilizarse en unidades de 512 MB a 2 TB.

Características:

- Es más eficiente en cuanto al almacenamiento y admite un tamaño de hasta 2 TB
- Proporciona un mejor uso del espacio en disco
- Facilita el acceso a los archivos en particiones de menos de 500 MB o de más de 2 GB
- La figura siguiente muestra la disposición de las particiones en los sistemas de archivos FAT y FAT 32.

Sistema de Archivos de Windows FAT y FAT 32



FAT File System



FAT 32 File System

Sistema de Archivos de Windows NTFS

El sistema de archivos NTFS significa Sistema de Archivos de Nueva Tecnología.

Características:

- Nombre:
 - El nombre del archivo puede tener hasta 255 caracteres
 - Los nombres de archivo pueden tener cualquier carácter que no sea / " :*
• No distinguen entre mayúsculas y minúsculas
- Proporciona seguridad de carpetas y archivos. Esto se hace pasando el permiso NTFS a los archivos y carpetas. La seguridad funciona tanto a nivel local como de red. Cada archivo y carpeta de la lista tiene una Lista de Control de Acceso que incluye los usuarios, el identificador de seguridad y los privilegios de acceso que se conceden a los usuarios.

Sistema de Archivos de Windows NTFS

- El tamaño de los archivos y las particiones es mayor en NTFS que en FAT. Una partición NTFS puede tener un tamaño de hasta 16 Exabytes, pero prácticamente está limitada a 2TB.
- El tamaño de los archivos puede oscilar entre 4 GB y 64 GB.
- Proporciona una compresión de archivos de hasta el 50%.
- Es un sistema de archivos fiable y recuperable que hace uso de los registros de transacciones para actualizar los archivos y las carpetas automáticamente.
- Proporciona un mapeo de clústeres defectuosos. Esto significa que puede detectar clusters malos o espacios erróneos en el disco, recuperar los datos en esos clusters y almacenarlos en otro espacio. Para evitar que se sigan almacenando datos en esos espacios, los clústeres malos se marcan para detectar errores.

Sistema de Archivos de Windows NTFS



NTFS File System

Sistema de Archivos de Windows

Features	NTFS	FAT32	FAT16	FAT12
Max Partition Size	2TB	32GB	4GB	16MB
Max File Size	16TB	4GB	2GB	Less than 16MB
Cluster Size	4KB	4KB to 32KB	2KB to 64KB	0.5KB to 4KB
Fault Tolerance	Auto Repair	No	No	No
Compression	Yes	No	No	No
Security	Local and Network	Only Network	Only Network	Only Network
Compatibility	Windows 10/8/7/XP/Vista/2000	Windows ME/2000/XP/7/8.1	Windows ME/2000/XP/7/8.1	Windows ME/2000/XP/7/8.1

Inicio de Windows

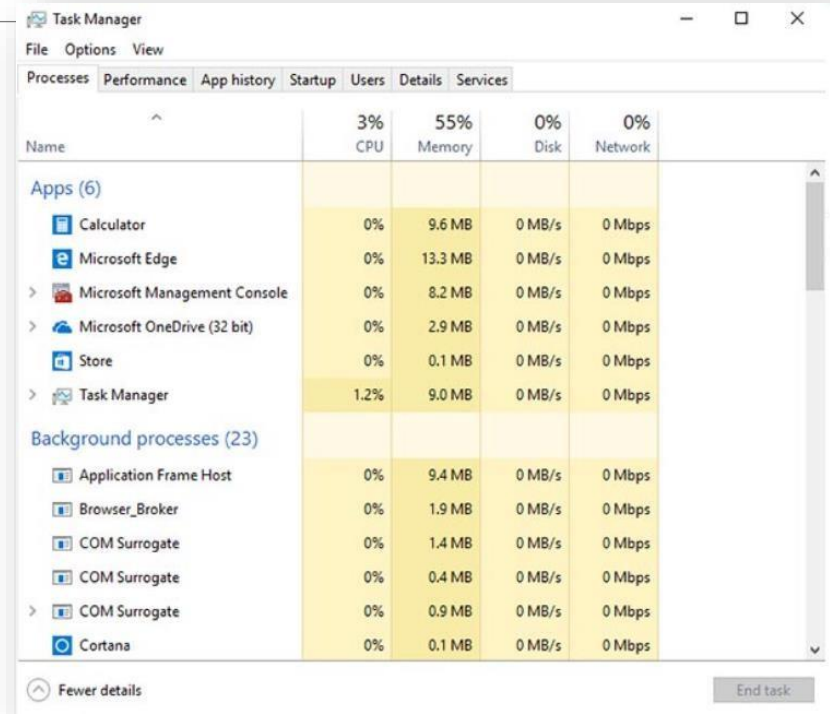
- Hay dos elementos importantes del registro que se utilizan para iniciar automáticamente aplicaciones y servicios:
 - **HKEY_LOCAL_MACHINE** - Varios aspectos de la configuración de Windows se almacenan en esta clave, incluida la información sobre los servicios que comienzan con cada inicio.
 - **HKEY_CURRENT_USER** En esta clave se almacenan varios aspectos relacionados con el usuario que ha iniciado sesión, incluida la información sobre los servicios que se inician solo cuando el usuario inicia sesión en la computadora.
- La presencia de entradas diferentes en estas ubicaciones del registro definen qué servicios y aplicaciones se iniciarán, según lo que indiquen sus tipos de entrada.
- Estos tipos son Run, RunOnce, RunServices, RunServicesOnce y Userinit. Estas entradas se pueden ingresar manualmente en el registro, pero es mucho más seguro usar la herramienta **Msconfig.exe**.

Investiguemos un poco msconfig.exe



Procesos, subprocessos y servicios

- Una aplicación de Windows se compone de procesos. Un proceso es cualquier programa que se esté ejecutando actualmente.
- Cada proceso en ejecución está compuesto de, al menos, un subprocesso. Un subprocesso es una parte del proceso que puede ejecutarse.
- Para configurar los procesos de Windows, busque el Administrador de tareas. La pestaña Procesos del Administrador de tareas se muestra en la figura.
- Todos los subprocessos dedicados a un proceso están contenidos dentro del mismo espacio de direcciones, lo que significa que estos hilos no pueden acceder al espacio de direcciones de ningún otro proceso. Esto evita el daño de otros procesos.



Task Manager

File Options View

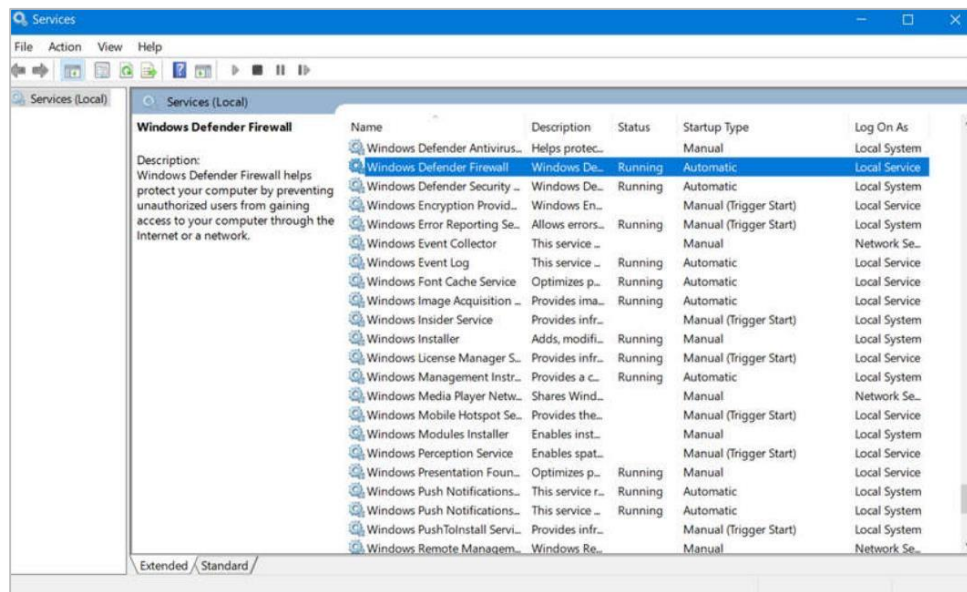
Processes Performance App history Startup Users Details Services

Name	3% CPU	55% Memory	0% Disk	0% Network
Apps (6)				
Calculator	0%	9.6 MB	0 MB/s	0 Mbps
Microsoft Edge	0%	13.3 MB	0 MB/s	0 Mbps
Microsoft Management Console	0%	8.2 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)	0%	2.9 MB	0 MB/s	0 Mbps
Store	0%	0.1 MB	0 MB/s	0 Mbps
Task Manager	1.2%	9.0 MB	0 MB/s	0 Mbps
Background processes (23)				
Application Frame Host	0%	9.4 MB	0 MB/s	0 Mbps
Browser_Broker	0%	1.9 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.9 MB	0 MB/s	0 Mbps
Cortana	0%	0.1 MB	0 MB/s	0 Mbps

^ Fewer details End task

Procesos, subprocessos y servicios

- Algunos de los procesos que ejecuta Windows son servicios. Son programas que se ejecutan en segundo plano para respaldar el funcionamiento del sistema operativo y de las aplicaciones.
- Los servicios proporcionan funcionalidades de duración prolongada, como la conexión inalámbrica o el acceso a un servidor FTP.
- Para configurar los servicios de Windows, busque “servicios”. El subprograma del panel de control de Servicios de Windows se muestra en la figura.
- Ser muy cuidadoso manipulando las configuraciones de estos servicios. Apagar un servicio puede afectar adversamente aplicaciones u otros servicios.



Configuración y monitoreo

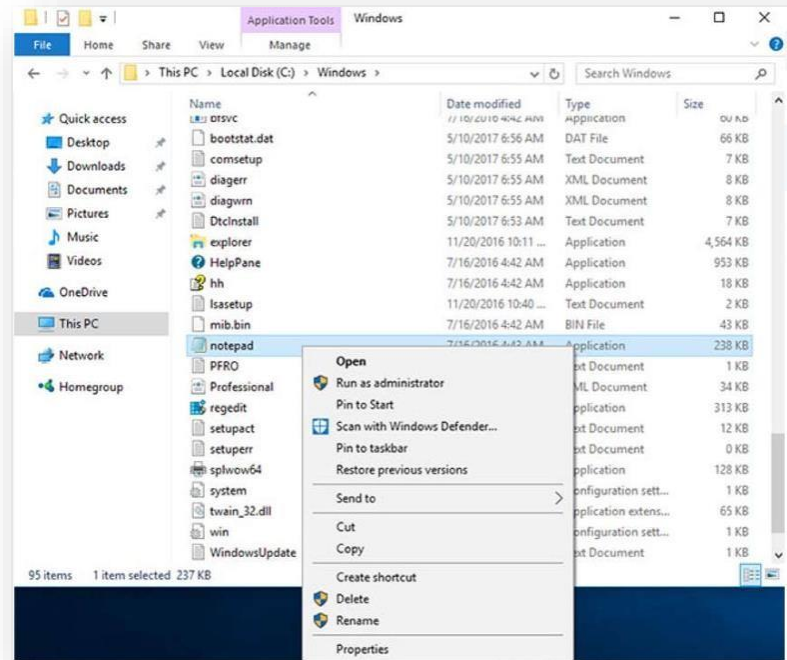
A solid blue horizontal bar at the bottom of the slide.

Ejecución como administrador

- Como mejor práctica de seguridad, no es recomendable iniciar sesión en Windows utilizando la cuenta de administrador o una cuenta con privilegios administrativos.
- Hay dos formas diferentes de ejecutar o instalar un software que requiere los privilegios del administrador.

Administrador

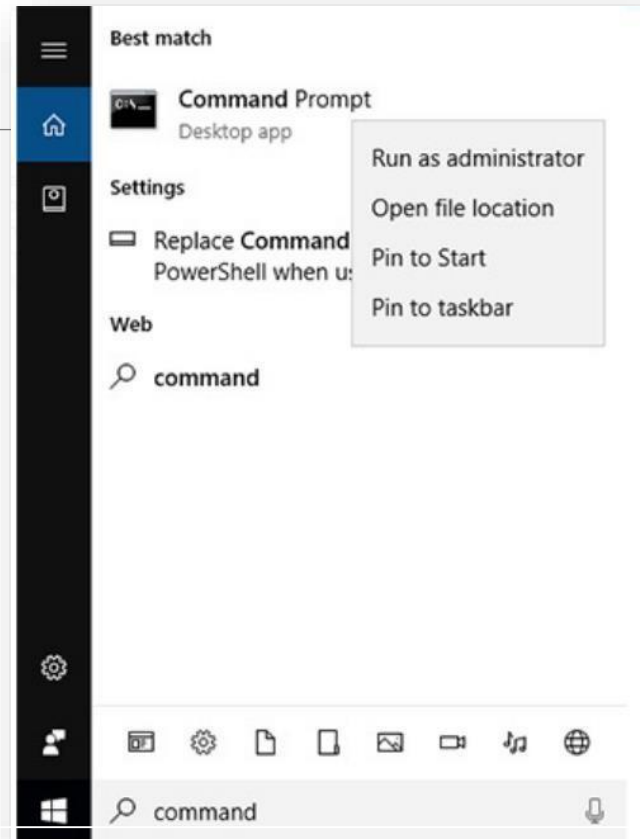
- Haga clic con el botón derecho en el comando en el Explorador de archivos de Windows y elija Ejecutar como administrador en el menú contextual.



Ejecución como administrador

Administrador Command Prompt

- Busque **command**, haga clic derecho en el archivo ejecutable y seleccione ejecutar como administrador del menú de contexto.
- Cada comando que se ejecute desde esta línea de comando se implementará con privilegios de administrador, incluida la instalación de software.

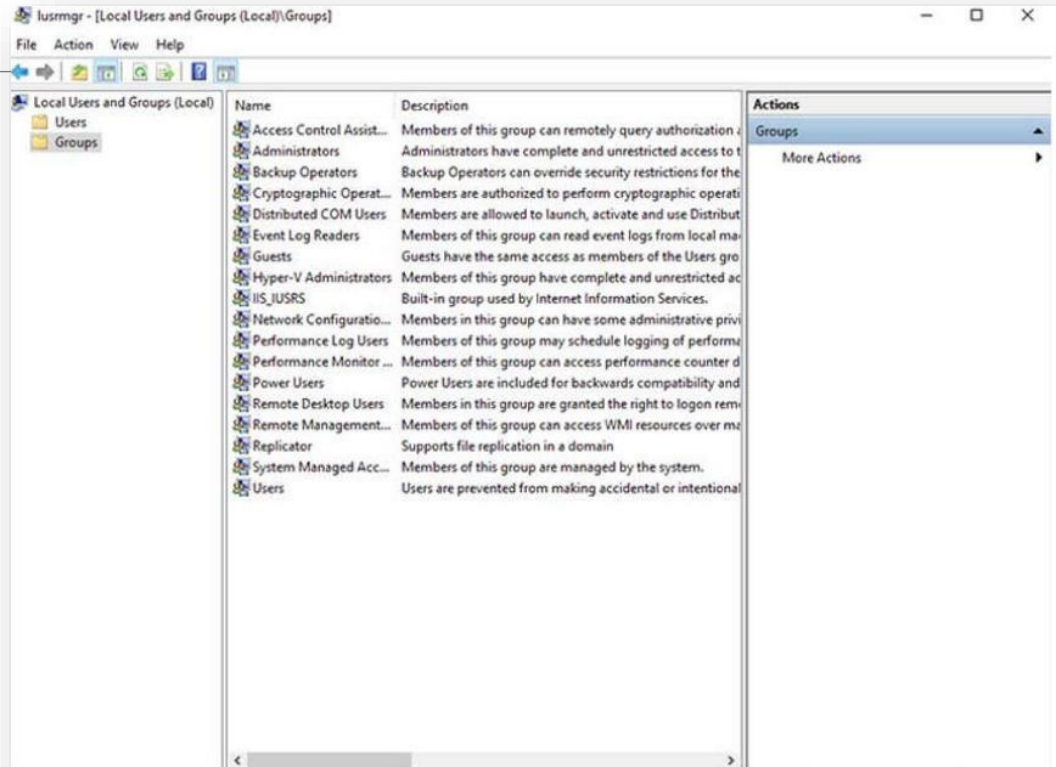


Usuarios y dominios locales

- Cuando se inicia una computadora nueva por primera vez o se instala Windows, aparecerá un mensaje para crear una cuenta de usuario. Esta se conoce como “usuario local”.
- Esta cuenta contiene todas las configuraciones de personalización, permisos de acceso, ubicaciones de archivos y muchos otros datos específicos del usuario.
- Para facilitar la administración de usuarios, Windows utiliza grupos. Un grupo tendrá un nombre y un conjunto específico de permisos asociados con él.
- Cuando se coloca a un usuario en un grupo, los permisos de ese grupo se le otorgan a ese usuario.
- Se puede colocar a un usuario en varios grupos con muchos permisos diferentes. Cuando se superponen los permisos, algunos de ellos (como “denegar explícitamente”) anulan los permisos otorgados por otro grupo.
- Hay muchos grupos de usuarios diferentes integrados en Windows que se utilizan para tareas específicas.

Usuarios locales y dominios

- Los usuarios y grupos locales se administran con el applet del panel de control **lusrmgr.msc**, como se muestra en la figura.
- Windows además utiliza dominios para definir permisos. Un dominio es un tipo de servicio de red en el que todos los usuarios, grupos, computadoras, periféricos y ajustes de seguridad se almacenan en una base de datos, que también los controla.



CLI y PowerShell

- La interfaz de línea de comandos (CLI) de Windows se puede usar para ejecutar programas, recorrer el sistema de archivos, y administrar archivos y carpetas.
- Para abrir el CLI de Windows, busque **cmd.exe** y haga clic en el programa. Estas son algunas sugerencias para recordar cuando se usa la CLI:
 - De manera predeterminada, los nombres y rutas de archivo no distinguen entre mayúsculas y minúsculas.
 - A los dispositivos de almacenamiento se les asigna una letra de referencia. Esto seguido de dos puntos y barra invertida (\).
 - Los comandos que tienen modificadores opcionales utilizan la barra inclinada (/) para delinear entre el comando y la opción de cambio.
 - Puede utilizar la tecla **Tab** para auto-completar comandos cuando referencia directorios o archivos.
 - Windows guarda un historial de los comandos que se introdujeron durante una sesión de la CLI. Acceda a comandos previamente introducidos presionando las flechas de arriba y abajo.
 - Para cambiar entre dispositivos de almacenamiento, escriba la letra del dispositivo, seguido de dos puntos y presione **Enter**.

CLI y PowerShell

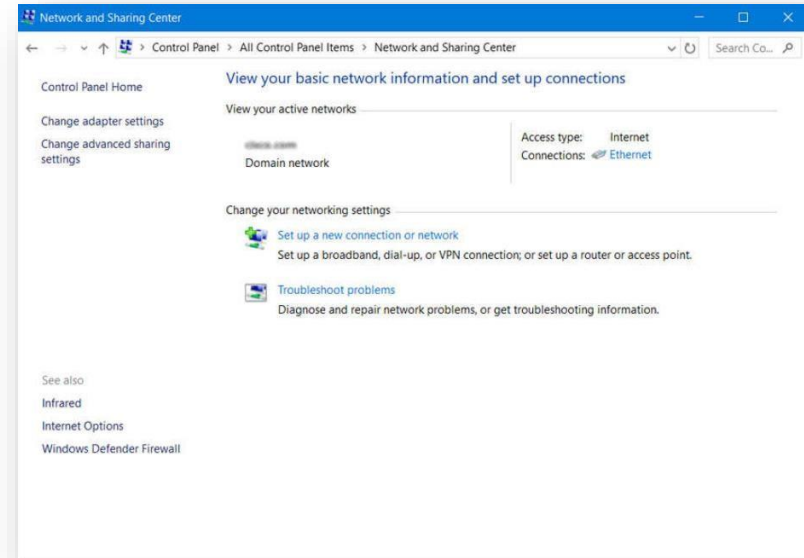
- Se puede utilizar otro entorno, llamado Windows PowerShell, para crear script con el fin de automatizar tareas que la CLI común no puede crear.
- PowerShell también proporciona una CLI para iniciar comandos.
- PowerShell es un programa integrado dentro de Windows.
- Como la CLI, PowerShell también se puede ejecutar con privilegios de administrador.
- Estos son los tipos de comandos que puede ejecutar PowerShell:
 - **cmdlets** - Estos comandos realizan la acción y devuelven una salida o un objeto luego del comando que va a ser ejecutado.
 - **PowerShell Scripts** - Estos archivos con una extensión **.ps1** que contienen comandos PowerShell que son ejecutados.
 - **Funciones del PowerShell** - Estas piezas de código pueden ser referenciadas en un script.

Redes

- Una de las características más importantes de cualquier sistema operativo es la capacidad de la computadora de conectarse a una red.
- Para configurar las propiedades de redes de Windows y probar la configuración de redes, se emplea el Centro de redes y recursos compartidos.

Centro de redes y recursos compartidos

- Se utiliza para verificar o crear conexiones de red, configurar el uso compartido de red y cambiar la configuración del adaptador de red.
- En la vista inicial, se ve un panorama general de la red activa.



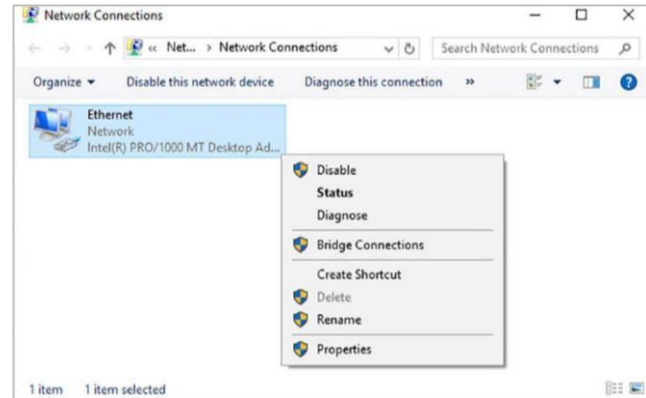
Redes

Cambiar configuración del adaptador.

- Para configurar un adaptador de red, es necesario seleccionar **Cambiar configuración del adaptador** en centro de redes y recursos compartidos a fin de ver todas las conexiones de red que están disponibles. Seleccione el adaptador que se va a configurar.
- Los siguientes son los pasos para cambiar un adaptador Ethernet para adquirir su dirección IPv4 automáticamente de la red:

Paso 1: Acceder a las propiedades del adaptador

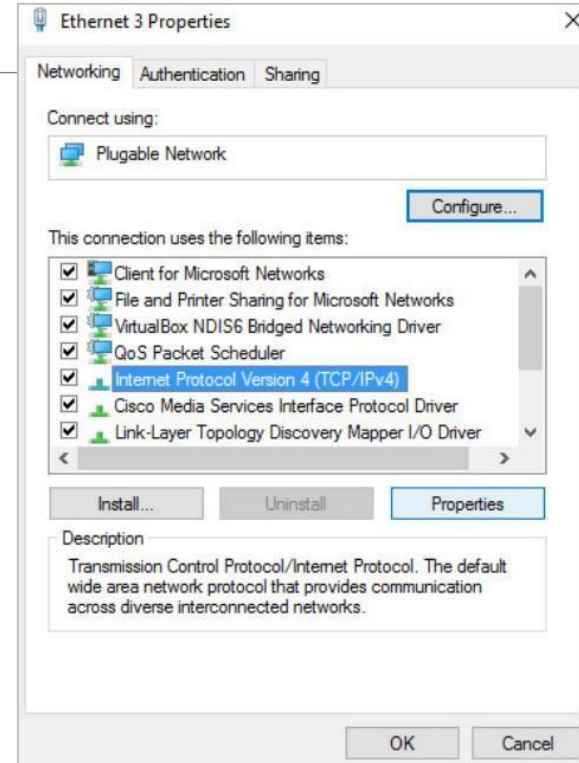
Haga clic con el botón derecho en el adaptador que desee configurar y seleccione **Propiedades**, como se ve en la Figura.



Redes

Paso 2: Acceda a las propiedades de TCP/IPv4

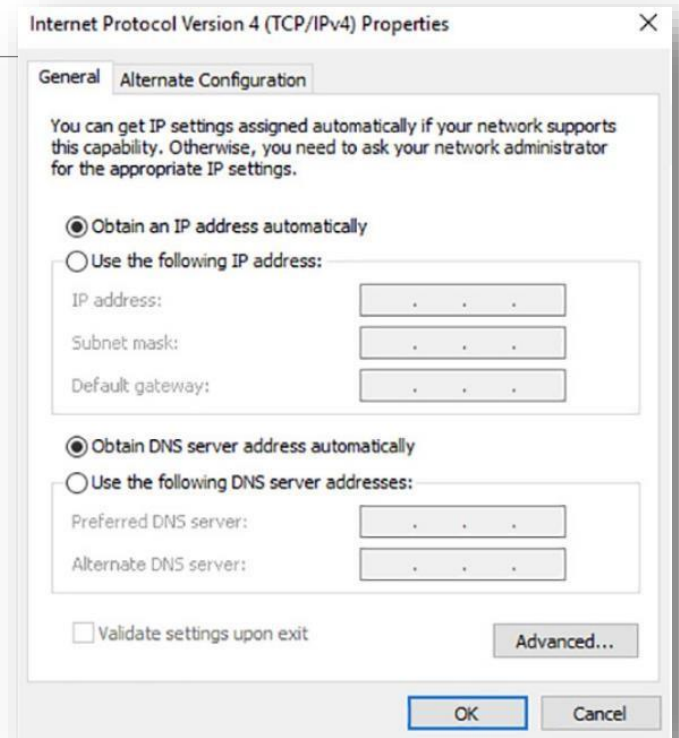
- Esta conexión utiliza **Protocolo de internet versión 4 (TCP/IPv4)** o **Protocolo de internet versión 6 (TCP/IPv6)** depende de la versión que el usuario desee utilizar.
- En la figura, IPv4 se está seleccionando.



Redes

Paso 3: Cambiar la configuración

- Haga clic en **Propiedades** para configurar el adaptador.
- En el cuadro de diálogo **Propiedades**, elija **Obtener una dirección automáticamente** si hay un servidor DHCP disponible en la red o si el usuario desea configurar el direccionamiento manualmente, rellene la dirección, la subred, la puerta de enlace predeterminada y los servidores DNS.
- Haga clic en **OK** para aplicar los cambios.
- Estas configuraciones también se pueden cambiar a través de Powershell o netsh



Redes

nslookup y netstat

- Sistema de Nombres de Dominio (DNS) debe ser probado por que es esencial para encontrar la dirección de los hosts traduciéndola de un nombre, a una URL.
- Use el comando **nslookup** para probar el DNS.
- Escriba **nslookup cisco.com** en la petición de ingreso de comando para encontrar la dirección del servidor web de Cisco. Si se devuelve la dirección, significa que el DNS funciona correctamente.
- Use **netstat** en la línea de comando para ver los detalles de las conexiones de red activas.

```
C:\Users\USER>netstat
```

```
Active Connections
```

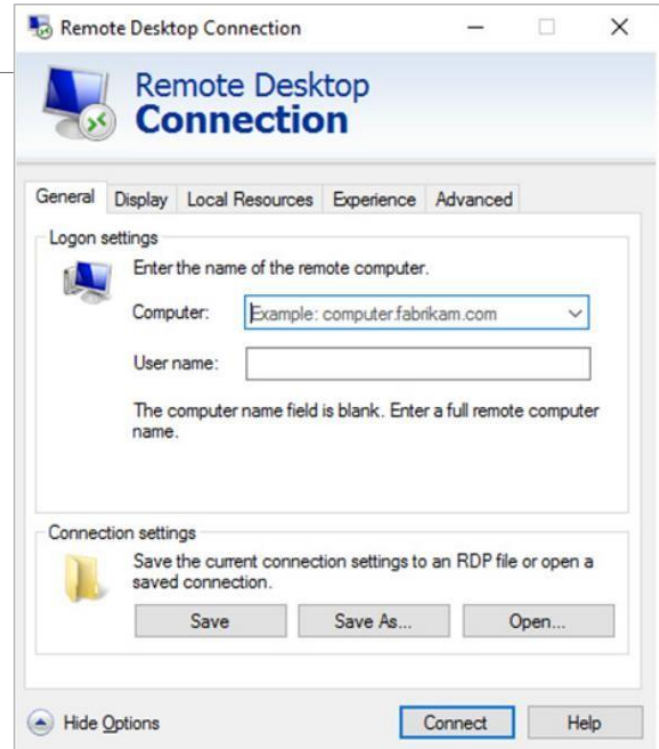
Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:3030	USER-VGFFA:58652	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62114	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62480	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62481	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62484	TIME_WAIT

Acceso a los recursos de red

- Windows utiliza redes para varias aplicaciones diferentes, como web, correo electrónico y servicios de archivo.
- El protocolo de bloqueo de mensaje del servidor (SMB) se utiliza para compartir recursos de la red. Es utilizado comúnmente para acceder a archivos o hosts remotos.
- El formato de la Convención de nomenclatura universal (UNC) se utiliza para conectarse a recursos como **\\servername\sharename\file**.
- En la UNC, servername es el servidor que aloja el recurso. El elemento sharename corresponde a la raíz de la carpeta del sistema de archivos en el host remoto, mientras que file es el recurso que el host local intenta encontrar.
- Al compartir recursos en la red, se deberá identificar el área del sistema de archivos que se compartirá. El control de acceso se puede aplicar a los archivos para restringir usuarios y grupos a funciones específicas.
- Windows también crea recursos compartidos especiales automáticamente. Estas acciones se denominan acciones administrativas y se identifican con un signo de dólar (\$) que viene después del nombre de la acción.

Acceso a los recursos de red

- Además de acceder a recursos compartidos en hosts remotos, el usuario también puede iniciar sesión en un host remoto y manipular esa computadora, como si fuera local, para realizar cambios de configuración, instalar software o solucionar un problema.
- En Windows, esta función se conoce como Protocolo de escritorio remoto (Remote Desktop Protocol, RDP). La ventana Conexión a Escritorio remoto se muestra en la figura.
- Dado que el Protocolo de escritorio remoto (RDP) está diseñado para permitir a los usuarios remotos controlar hosts individuales, es un objetivo natural para los actores de amenazas.



Servidor de Windows

- La mayoría de las instalaciones de Windows se realizan como instalaciones de escritorio en equipos de escritorio y portátiles.
- En centros de datos se utiliza principalmente otra versión de Windows: Windows Server. Se trata de una familia de productos de Microsoft que empezó con Windows Server 2003.
- Windows Server aloja muchos servicios diferentes y puede cumplir diferentes roles dentro de una empresa.
- Estos son algunos de los servicios que provee Windows Server:
 - **Servicios de red:** DNS, DHCP, Terminal Services, controladora de red y virtualización de red en Hyper-V
 - **Servicios de archivo:** SMB, NFS y DFS
 - **Servicios web:** FTP, HTTP y HTTPS
 - **Administración:** política de grupo y control de servicios de dominio de Active Directory

En esta práctica de laboratorio crearán y modificarán cuentas de usuario en Windows.



En este laboratorio, explorará algunas de las funciones de PowerShell



Ayuda para usar cualquier comando `Get-Help <comando>`

Buscar un comando `Get-Command - Name <nombre>`

Crear un nuevo directorio `mkdir ejemplo`

Copiar y borrar archivos o directorios

`Copy-Item «ruta al archivo de origen con extensión» -Destination «ruta de destino»`

`Remove-Item «ruta al archivo con extensión»`

Listado de todos los archivos dentro de una carpeta

`Get-ChildItem`

Crear archivos y carpetas

`New-Item -Path 'C:tempNueva carpeta' -ItemType Directory`

Este comando crea un nuevo archivo vacío:

`New-Item -Path 'C:tempNueva carpetafile.txt' -ItemType File`

En este laboratorio, explorará algunas de las funciones de PowerShell



Saber todo el contenido de un archivo

```
Get-Content "C:/ejemplo.txt"
```

También podemos ver 20 líneas de texto incluidos en ejemplo.txt

```
Get-Content "C:/ejemplo.txt" - TotalCount 20
```

Cambiar la política de ejecución

```
Set-ExecutionPolicy Unrestricted Set-ExecutionPolicy All Signed Set-ExecutionPolicy Remote  
Signed Set-ExecutionPolicy Restricted
```


En este laboratorio, explorará algunas de las funciones de PowerShell



Ver, iniciar, detener, suspender o reiniciar un servicio o proceso

`Start-Service <nombre del servicio>`

`Stop-Service <nombre del servicio>`

`Suspend-Service <nombre del servicio>`

`Resume-Service <nombre del servicio>`

`Restart-Service <nombre del servicio>`

Lista de los procesos abiertos

`Start-Process <nombre del proceso> Stop-Process <nombre del proceso> Wait-Service <nombre del proceso>`

`Get-History`

En este laboratorio, explorará algunas de las funciones de PowerShell



Ejecutar aplicaciones UWP en Windows. Por ejemplo, si queremos abrir la Configuración de Windows usamos:

```
Start-Process «ms-settings:»
```

Si lo que queremos es usar una aplicación UWP como Spotify el comando a escribir sería

```
Start-Process «spotify:»
```

Desinstalar aplicaciones desde PowerShell

```
Get-Service
```

comando

```
Stop-Process <nombre del proceso>
```

Una vez hemos cerrado la aplicación, ya podemos desinstalarla desde PowerShell utilizando el siguiente comando:

```
Get-AppxPackage *nombreaplicación* | Remove-AppxPackage
```

Utilizar PowerShell para eliminar aplicaciones nativas de Windows 10 y Windows 11 el mejor método para hacerlo, ya que Windows no nos permite realizar este proceso desde la interfaz gráfica en la mayoría de las aplicaciones nativas.

Práctica de laboratorio: Administrador de tareas de Windows

En esta práctica de laboratorio, explorará el Administrador de tareas y administrará procesos desde allí.



Seguridad de Windows

A solid blue horizontal bar spanning the width of the slide at the bottom.

El comando netstat

- El comando **netstat** puede usarse para buscar conexiones entrantes o salientes no autorizadas.
- El comando **netstat** permite ver todas las conexiones de TCP activas disponibles.
- Al examinar estas conexiones, es posible determinar los programas que están escuchando conexiones que no están autorizadas.
- Cuando se sospecha que un programa es malware, el proceso se puede cerrar con el Administrador de tareas y se puede usar un software de eliminación de malware para limpiar la computadora.
- Para facilitar este proceso, las conexiones se pueden vincular a los procesos en ejecución que fueron creados por ellos en el Administrador de tareas.

Seguridad de Windows

El comando netstat

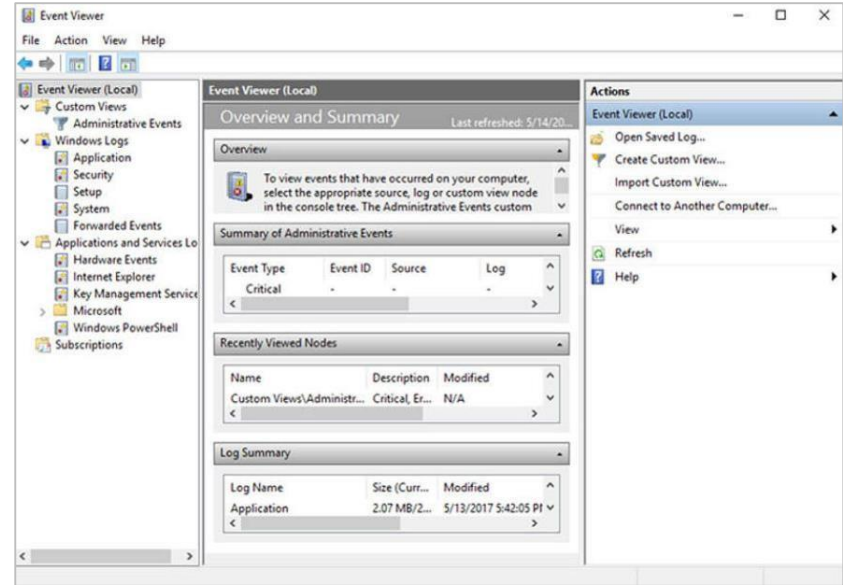
- Para hacerlo, abra el command prompt con privilegios administrativos y use el comando **netstat -abno**.
- Al examinar las conexiones de TCP activas, un analista debe ser capaz de determinar si hay programas sospechosos que escuchan conexiones entrantes en el host.
- Puede haber más de un proceso con el mismo nombre. Si este es el caso, use el PID único para encontrar el proceso correcto. Para ver los PID de los procesos en el **Administrador de tareas**, ábralo, haga clic con el botón derecho en el encabezado de la tabla y seleccione **PID**.

```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> netstat -abno

Active Connections
Proto Local Address           Foreign Address         State       PID
TCP   0.0.0.0:80               0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING   952
RpcSs
[svchost.exe]
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:623              0.0.0.0:0               LISTENING   14660
[LMS.exe]
TCP   0.0.0.0:3389             0.0.0.0:0               LISTENING   1396
TermService
[svchost.exe]
TCP   0.0.0.0:5040             0.0.0.0:0               LISTENING   9792
CDPSvc
[svchost.exe]
TCP   0.0.0.0:5357             0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:5593             0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:8099             0.0.0.0:0               LISTENING   5248
[SolarWinds TFTP Server.exe]
TCP   0.0.0.0:16992            0.0.0.0:0               LISTENING   14660
```

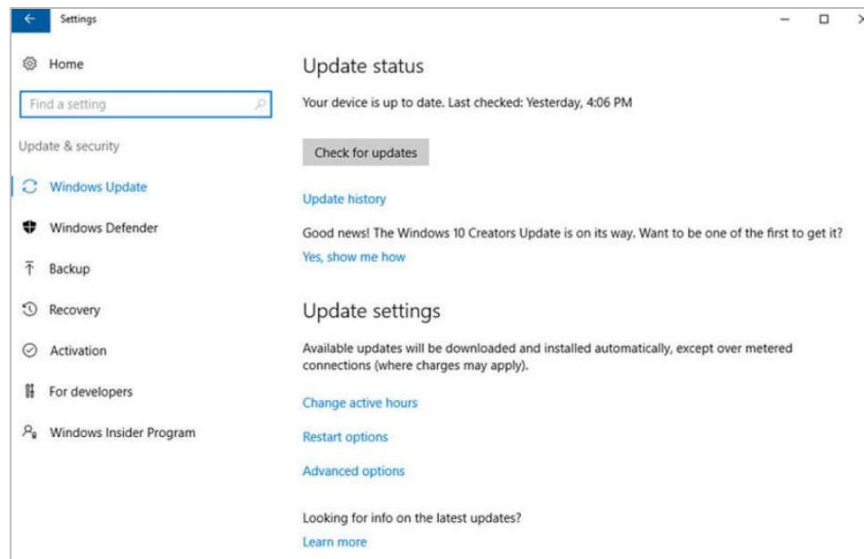
Visor de eventos

- El Visor de eventos de Windows registra el historial de eventos del sistema, de aplicaciones y de seguridad.
- Estos archivos de registro son una herramienta de resolución de problemas, ya que proporcionan la información necesaria para identificar un problema.
- Windows incluye dos categorías de registros de eventos: registros de Windows y registros de aplicaciones y servicios.
- Una vista personalizada incorporada llamada Eventos administrativos muestra todos los eventos críticos, de error y de advertencia de todos los registros administrativos.
- Los registros de sucesos de seguridad se encuentran en Registros de Windows. Utilizan ID de evento para identificar el tipo de evento.



Administración de actualizaciones de Windows

- Para garantizar el más alto nivel de protección contra los ataques, asegúrese siempre de que Windows esté actualizado con los últimos paquetes de servicios y parches de seguridad.
- El estado de actualización, que se muestra en la figura, le permite buscar actualizaciones manualmente y ver el historial de actualizaciones de la computadora.
- Los parches son actualizaciones de códigos que proporcionan los fabricantes para evitar que un virus o gusano recientemente descubierto logre atacar con éxito.



Administración de actualizaciones de Windows

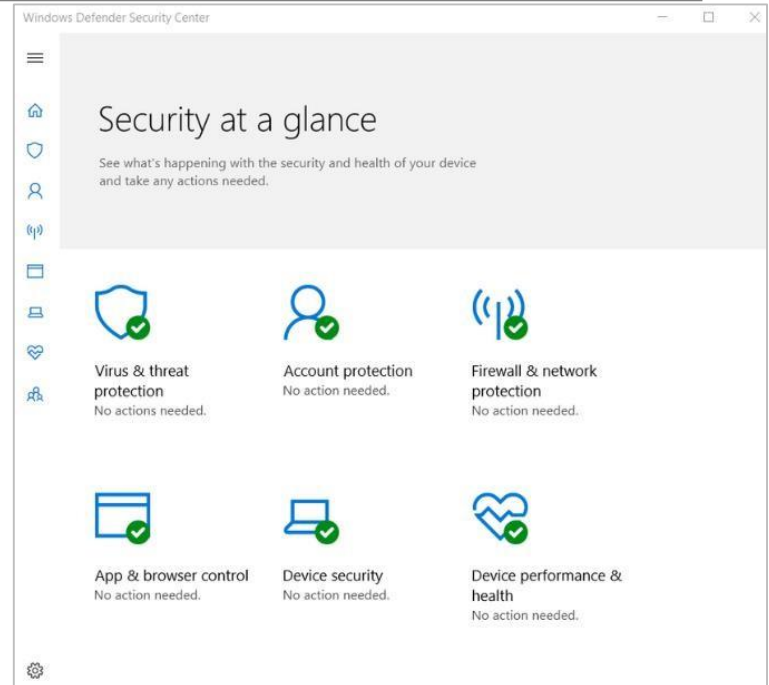
- Periódicamente, los fabricantes combinan parches y actualizaciones en una aplicación de actualización integral denominada paquete de servicios.
- Numerosos ataques de virus devastadores podrían haber sido mucho menos graves si más usuarios hubieran descargado e instalado el último paquete de servicios.
- Es muy deseable que las empresas utilicen sistemas que distribuyan, instalen y realicen un seguimiento automático de las actualizaciones de seguridad.
- Windows verifica sistemáticamente el sitio web de Windows Update en busca de actualizaciones de alta prioridad que ayuden a proteger una computadora de las amenazas de seguridad más recientes.
- También hay opciones para no permitir que la computadora se reinicie en determinados horarios, por ejemplo, durante el horario laboral.
- Las opciones avanzadas también están disponibles para elegir cómo se instalan las actualizaciones y cómo se actualizan otros productos de Microsoft.

Windows Defender

- El malware incluye virus, gusanos, troyanos, registradores de teclado, spyware y adware. Estos están diseñados para invadir la privacidad, robar información y dañar la computadora o los datos.
- Es importante proteger las computadoras y los dispositivos móviles usando software de antimalware de confianza. Los siguientes tipos de software de antimalware se encuentran disponibles:
 - **Protección antivirus:** este programa monitorea continuamente en busca de virus. Cuando se detecta un virus, se advierte al usuario y el programa intenta eliminar el virus o ponerlo en cuarentena.
 - **Protección contra adware:** este programa busca constantemente programas que muestran anuncios publicitarios en la computadora.
 - **Protección contra suplantación de identidad:** este programa bloquea las direcciones IP de sitios web conocidos por realizar suplantación de identidad y advierte al usuario acerca de sitios sospechosos.
 - **Protección contra spyware:** El programa busca registradores de teclado y otro tipo de spyware.
 - **Fuentes confiables o no confiables:** este programa le advierte si está por instalar programas inseguros o visitar sitios web inseguros.

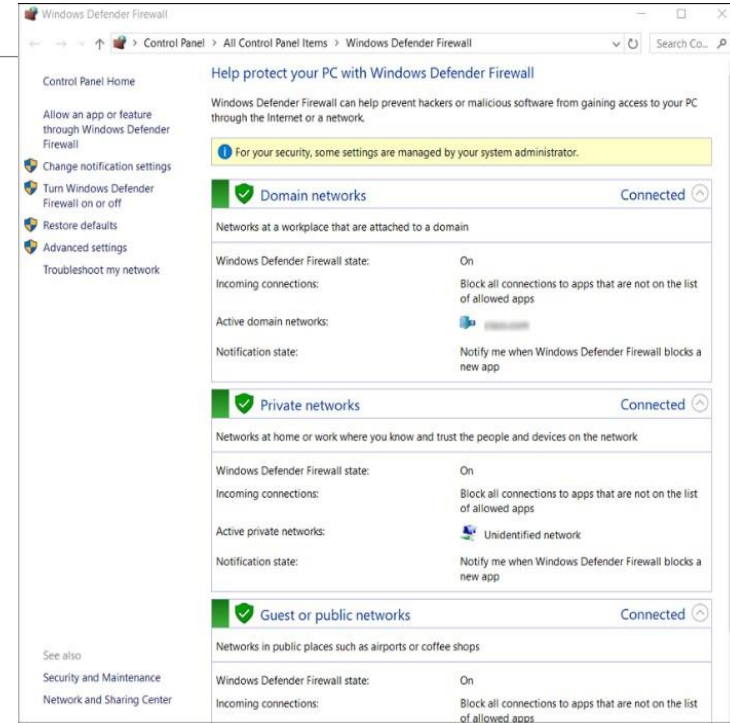
Windows Defender

- Pueden ser necesarios varios análisis para eliminar por completo todo el software malicioso. Ejecute solo un programa de protección contra malware a la vez.
- Varias organizaciones de seguridad como McAfee, Symantec y Kaspersky ofrecen protección integral contra malware para computadoras y dispositivos móviles.
- Windows trae preinstalada una protección contra virus y spyware llamada Windows Defender.
- Windows Defender está activado de forma predeterminada para proporcionar protección en tiempo real contra infecciones.
- Aunque Windows Defender funciona en segundo plano, el usuario puede realizar análisis manuales de la computadora y los dispositivos de almacenamiento.



Firewall de Windows Defender

- Un firewall deniega selectivamente el tráfico a una PC o a un segmento de red.
- Para permitir el acceso al programa a través del Firewall de Windows Defender, busque **Paneles de control**. En **Sistemas y seguridad**, busque **Firewall de Windows Defender**. Haga clic en **Permitir una aplicación o una función a través de Firewall de Windows**, como se muestra en la figura.
- Para deshabilitar el firewall de Windows, haga clic en **Activar o desactivar Firewall de Windows**.
- Se pueden encontrar muchas configuraciones adicionales en diferentes aspectos del firewall.
- **Configuración avanzada.** Aquí, se pueden crear reglas de tráfico entrante o saliente y se pueden supervisar



Fin módulo

A solid blue horizontal bar at the bottom of the slide.