sedian

Seguridad Digital
de Andalucía

Configuración Segura en Windows

- 2ª sesión -

Junta de Andalucía

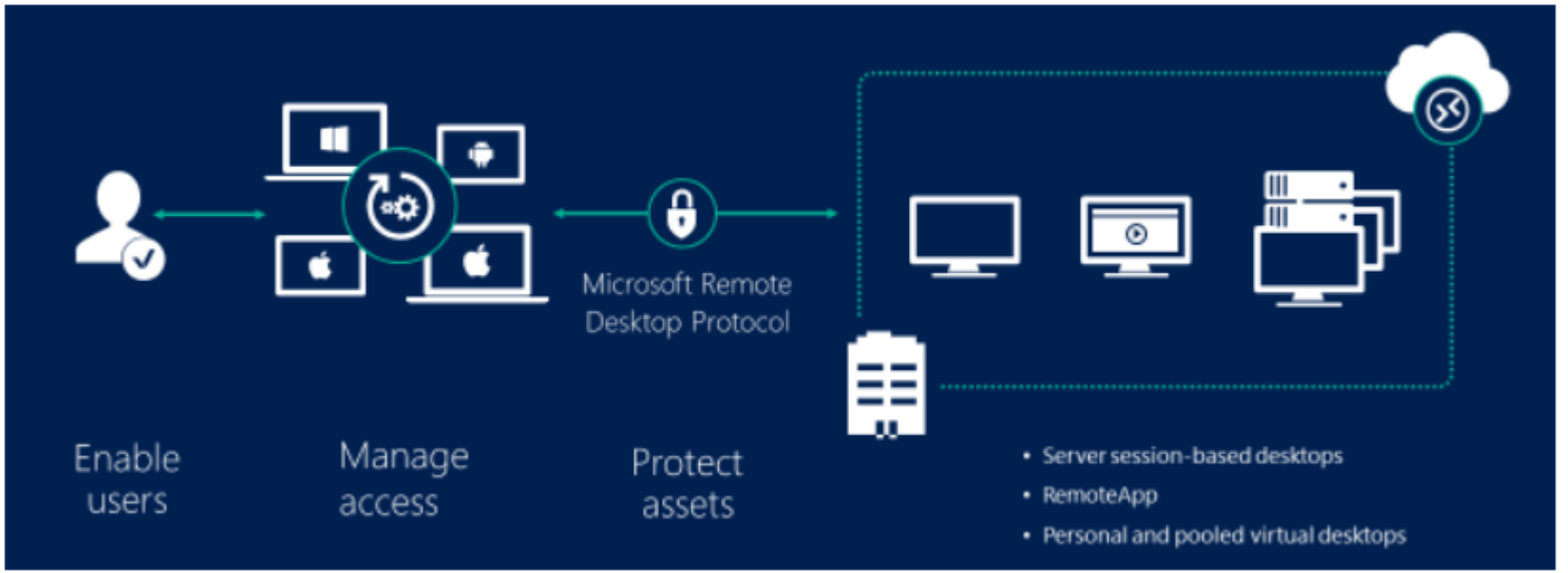
Unidades didácticas

Sincronización de Hora
Acceso remoto con Direct Access.
Acceso remoto VPN tradicional.
Acceso remoto por medio de Servicios de Escritorio Remoto (RDS)
Windows Defender Firewall con seguridad avanzada.
Protección frente a malware.
Bastionado de sistemas Windows por medio de líneas base.
Protección de las cuentas locales.
El visor de eventos de Windows.
La auditoría de Windows.
Cifrado del almacenamiento secundario.
Implementación del acceso inalámbrico en Windows.

Acceso remoto por medio de (RDS)

Servicios de Escritorio remoto (RDS) es la plataforma elegida para la creación de soluciones de virtualización que cubran todas las necesidades del cliente final. Incluye

- La entrega de aplicaciones virtualizadas individuales.
- Proporcionar acceso seguro al escritorio remoto.
- Proporcionar a los usuarios finales el capacidad para ejecutar sus aplicaciones y escritorios desde la nube.



Acceso remoto por medio de (RDS)

Puedes configurar la solución RDS para la virtualización basada en sesión, como una infraestructura de escritorio virtual (VDI), o como una combinación de ambos:

Virtualización basada en sesión: Aprovecha la eficacia de proceso de Windows Server para proporcionar un entorno multisesión rentable que impulse las cargas de trabajo diarias de los usuarios.

VDI: Aprovecha el cliente de Windows para proporcionar el alto rendimiento, la compatibilidad de aplicaciones y la familiaridad que los usuarios esperan de su experiencia de escritorio de Windows.

Acceso remoto por medio de (RDS)

En estos entornos de virtualización tienes mayor flexibilidad con respecto a lo que publicas para los usuarios:

Escritorios: Ofrece a los usuarios una experiencia de escritorio completa con varias aplicaciones que se instalan y administran. Es ideal para aquellos usuarios que proceden de clientes ligeros.

RemoteApps: Especifica aplicaciones individuales que se hospedan o ejecutan en la máquina virtualizada, pero aparecen como si se ejecutaran en el escritorio del usuario como aplicaciones locales. Es ideal para implementar aplicaciones en un entorno remoto seguro.

Acceso remoto por medio de (RDS)

Windows 10 y Windows Server 2016 tienen nuevas capas de protección integradas en el sistema operativo para protección adicional contra las vulneraciones de seguridad, ayudan a bloquear ataques malintencionados y mejoran la seguridad de máquinas virtuales, aplicaciones y datos.

Tipo de colección de VDI	Administrada, agrupada	Administrada, personal	No administrada, agrupada	No administrada, personal
Credential Guard	Sí	Sí	Sí	Sí
Device Guard	Sí	Sí	Sí	Sí
Credential Guard remoto	No	No	No	No
VM blindadas y compatibles con cifrado	No	No	VM compatibles con cifrado, con configuración adicional	VM compatibles con cifrado, con configuración adicional

Acceso remoto por medio de (RDS)

Credential Guard:

Presentado en Windows10 Enterprise y Windows Server 2016.

La protección de credenciales de Windows Defender usa la seguridad basada en la virtualización para aislar secretos, de modo que solo el software de sistema privilegiado pueda acceder a ellos.

El acceso no autorizado a estos secretos puede derivar en ataques de robo de credenciales, como ataques pass-the-hash o pass-the-ticket.

Credential Guard de Windows Defender impide estos ataques mediante la protección de los hash de contraseña NTLM, los vales de concesión de vales de Kerberos y las credenciales que almacenan las aplicaciones como credenciales de dominio.

Acceso remoto por medio de (RDS)

Device Guard:

Presente en Windows 10, Device Guard es una característica que integra medidas de seguridad tanto a nivel de software como de hardware.

Puede determinar si la firma digital de algún programa es confiable o no.

Manejando los dispositivos con Device Guard, las empresas serán capaces de bloquear los dispositivos y hacer que solo puedan instalar el software que haya sido aprobado.

Se parece al control de AppLocker de la GPO, pero las políticas de Device Guard se aplican con Intune y Windows Defender, que veremos más adelante.

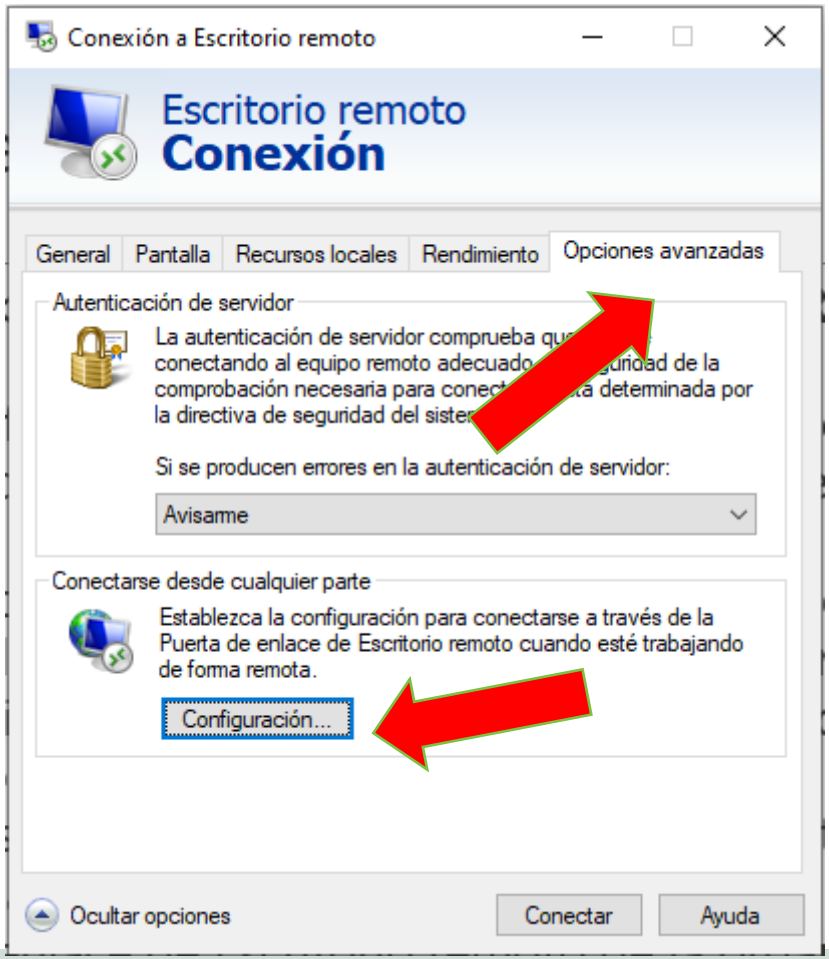
Acceso remoto por medio de (RDS)

Uso de una puerta de enlace para los servicios RDS

Los usuarios finales pueden conectarse a los recursos de red internos de manera segura desde fuera del firewall corporativo a través de Puerta de enlace de Escritorio remoto.

Esta funcionalidad recibe el nombre de “Conectarse desde cualquier parte”

Se hace entrando en “opciones avanzadas” y luego en “configuración”

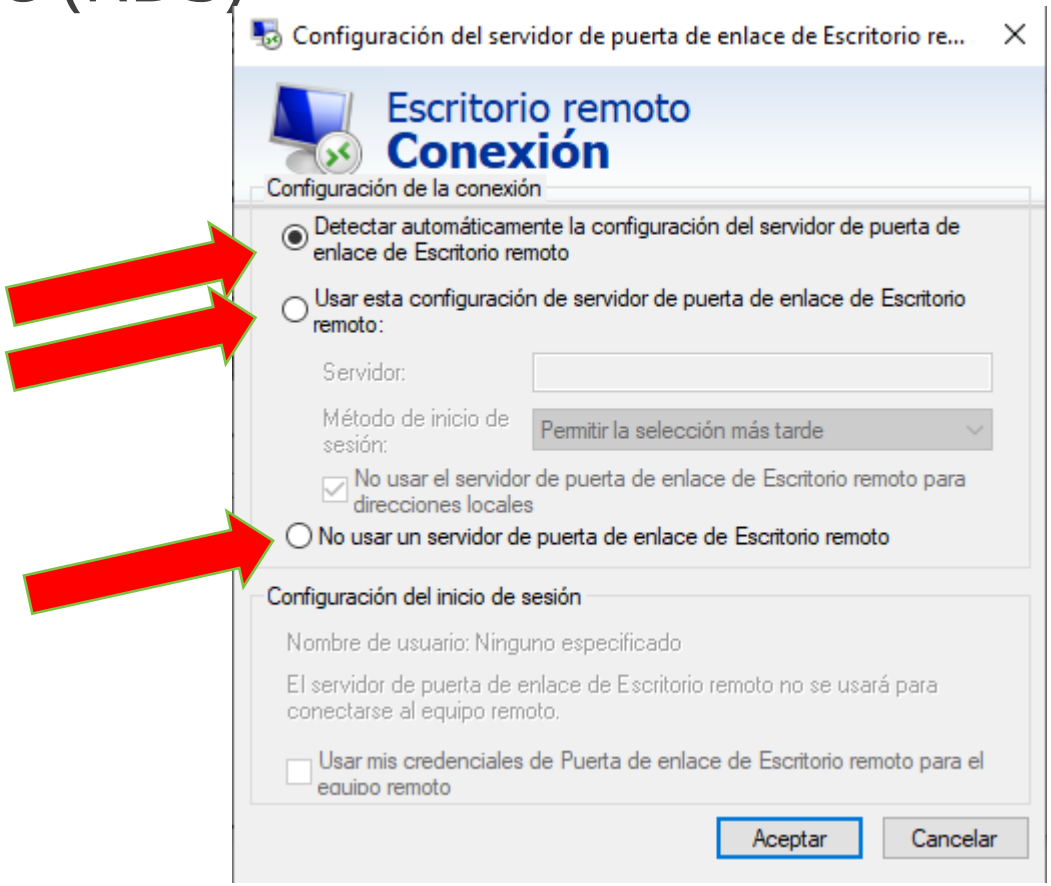


Acceso remoto por medio de (RDS)

Uso de una puerta de enlace para los servicios RDS

El cliente mstsc tiene diferentes formas de localizar o utilizar el servidor de puerta de enlace.

En la parte del servidor, la puerta de enlace es un endpoint SSL que transporta el tráfico RDP.



Acceso remoto por medio de (RDS)

Cómo funciona el acceso desde cualquier lugar

Los usuarios pueden conectar a recursos internos de manera segura desde fuera del firewall corporativo a través de Puerta de enlace de Escritorio remoto.

Los tres objetivos principales son:

- Establecer un túnel SSL cifrado entre el dispositivo del usuario final y el servidor de puerta de enlace de Escritorio remoto
- Autenticar al usuario en el entorno
- Pasar el tráfico entre el dispositivo del usuario final y el recurso.

Acceso remoto por medio de (RDS)

Para aprender más:

https://docs.microsoft.com/es-es/windows-server/remote/remote-desktop-services/welcome-to-rds

https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto

https://www.pandasecurity.com/spain/mediacenter/malware/goldbrute-botnet-rdp/

Windows Defender firewall con seguridad avanzada

Permite a los administradores configurar reglas que afectan a las comunicaciones entrante y salientes.

Las posibilidades que ofrece pasan por:

- Configurar perfiles de conexión (privado, dominio, Internet)
- Crear las reglas.
- Importar y exportar reglas desde y hacia otros equipos.
- Crear reglas mediante GPO.
- Configurar reglas de seguridad de conexión (IPSec)

Windows Defender firewall con seguridad avanzada

Configuración de los perfiles.

El firewall usa perfiles separados para definir las configuraciones:

Público: Se aplica cuando el equipo está conectado a una red pública no confiable.

Privado: Se aplica cuando el equipo está detrás de un firewall o en una red local.

Dominio: Se aplica cuando el equipo puede “ver” al controlador de dominio.

Se puede activar/desactivar los diferentes perfiles de firewall. Se recomienda tenerlos todos activados.

Windows Defender firewall con seguridad avanzada

Creación de reglas.

La regla puede ser de entrada o salida.

Podemos crear reglas de puerto o de programas (configuraciones predefinidas)

Para las reglas de puerto debemos proporcionar información de protocolo, y puertos de origen y destino.

Las reglas pueden permitir o denegar la comunicación cuando se verifican.

Debemos proporcionar un nombre apropiado a cada regla.

Existe cierta dificultad en encontrar una regla en el conjunto de reglas predefinidas.

Windows Defender firewall con seguridad avanzada

Importación/Exportación de reglas.

Están en el menú “acción” de la barra de menú.

Útiles para llevar las configuraciones de firewall de un equipo a otro.

Es recomendable usar configuraciones de firewall establecidas por GPO en el dominio.

Windows Defender firewall con seguridad avanzada

Reglas de seguridad de la conexión

Es el componente “desconocido” de Firewall de Windows.

Puede requerir o solicitar cifrado IPSec para las comunicaciones entrantes/ salientes del equipo.

Es una tecnología que se ha aplicado tradicionalmente a los servidores y que tenemos disponibles en Windows 10.

Es una alternativa a IPv6 para dotar de mayor seguridad a las comunicaciones IP. Evita ataques MitM.

Windows Defender firewall con seguridad avanzada

Creación de reglas por GPOs.

Disponibles en la rama “seguridad” de la configuración de equipos.

Las opciones de configuración son las mismas que las que podemos establecer manualmente.

Las reglas aplicadas por GPO tienen preferencia respecto a las locales (Herencia de GPO)

Al ser GPOs se puede aplicar el filtrado de seguridad o WMI para ser más precisos a la hora de su aplicación.

Protección frente al malware

Tipos de ataque y amenazas. (Como puede defendernos un antivirus)

Detección de vulnerabilidades. (https://www.cvedetails.com/)

Reconocimiento de sistemas. (Nessus)

Man in the Middle (MitM)

DNS Spoofing.

Captura de cuentas de usuario.

Cross-Site Scripting (XSS) , Inyección de código SQL.

Protección frente al malware

Tipos de ataque y amenazas. (Como puede defendernos un antivirus)

Ataques dirigidos (targeted) con Metasploit.

Ofuscación de malware con Veil.

Determinar el grado de detección del antivirus (virustotal.com)

Protección frente al malware

Recuperación de archivos en Windows 10

Las herramientas disponibles son:

- Copia de seguridad y restauración
- Historial de archivos.
- Azure backup.

Protección frente al malware

Recuperación de archivos en Windows 10

Para prevenir la pérdida de archivos se recomienda usar soluciones corporativas como la redirección de carpetas.

La redirección de perfiles o perfiles móviles es una tecnología obsoleta que no debemos seguir usando.

Es importante dotar un mecanismo que permita recuperar los archivos de usuario desde el propio equipo, independientemente de las soluciones corporativas desplegadas.

El objetivo es tener un RTO y RPO muy pequeño que no afecte al personal de IT.

Protección frente al malware

Recuperación de archivos en Windows 10

Las razones por las que se necesitan este tipo soluciones son:

- Borrado de archivo de forma accidental por parte del usuario.
- Infección por ransomware de un equipo que encripta los archivos de usuario.
- Es usuario modifica un archivo y lo guarda. Posteriormente quiere acceder a la versión anterior del documento.

Protección frente al malware

Recuperación de archivos en Windows 10

La herramienta “Historial de Archivos” funciona de la siguiente manera:

- Después de habilitarla, crea un backup de los archivos de usuario modificados.
- El destino del backup puede ser una unidad local, extraíble o de red.
- Por defecto se guardan las carpetas y bibliotecas del perfil del usuario, aunque podemos agregar otras ubicaciones (Por medio de “copia de seguridad usando Historial de Archivos”, que está en “backup” dentro de “Actualización y Seguridad” en “Configuración”.
- La copia se realiza cada hora, en carpetas protegidas (del malware) y se guardan indefinidamente mientras haya espacio libre en la unidad.

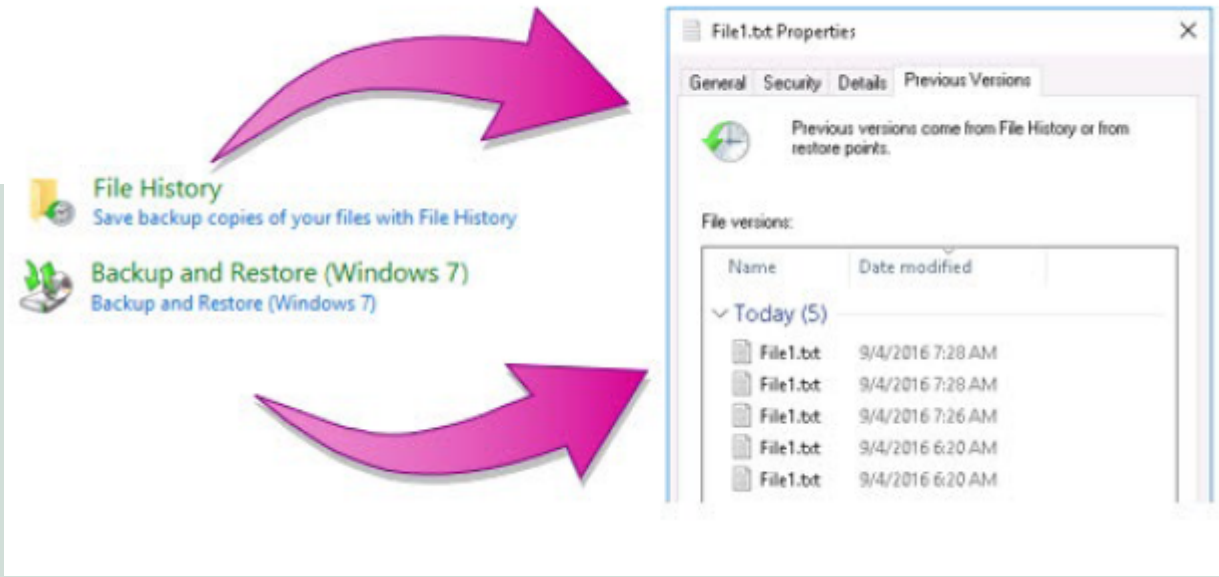
Protección frente al malware

Recuperación de archivos en Windows 10

La herramienta “Historial de Archivos” funciona de la siguiente manera:

- Se puede utilizar el Explorador de Archivos para revertir a versiones previas de los archivos protegidos por “Historial de Archivos”.

- La recuperación es muy sencilla y se realiza por medio del menú contextual, accediendo a la pestaña “Versiones Previas”.



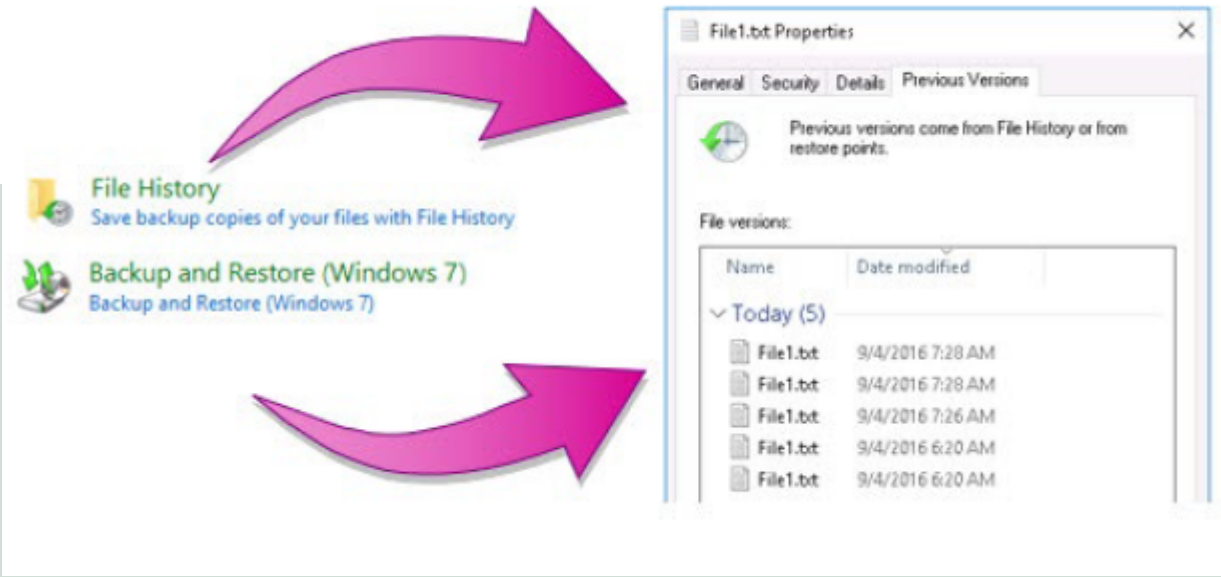
Protección frente al malware

Recuperación de archivos en Windows 10

La herramienta “Historial de Archivos” funciona de la siguiente manera:

- Las versiones previas aparecen cuando se configura la copia de seguridad con “historial de archivos” o con la herramienta de “backup y restauración (Windows 7)

- Es posible navegar por el snapshot de una versión previa para ver el estado anterior documentos modificados y eliminados, ofreciendo la posibilidad de recuperar el archivo correcto.

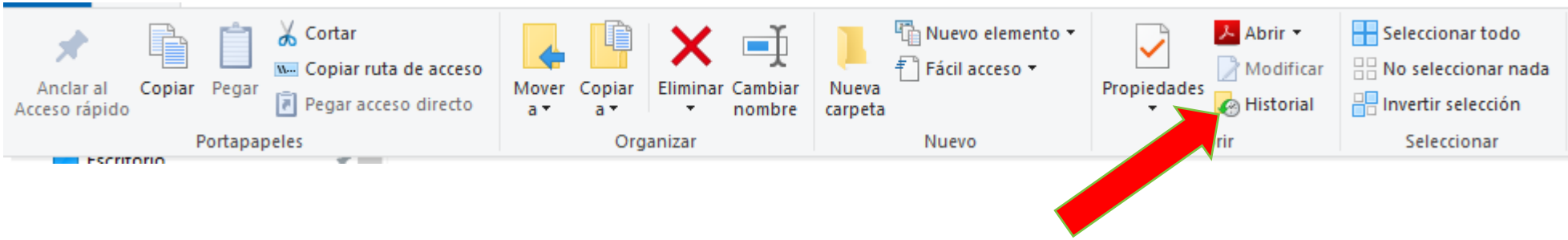


Protección frente al malware

Recuperación de archivos en Windows 10

La herramienta “Historial de Archivos” funciona de la siguiente manera:

- El Explorador de Archivos ofrece integración para poder acceder a las versiones previas de los archivos a través del historial.



Protección frente al malware

Recuperación de archivos en Windows 10

La herramienta “Copia de seguridad y restauración (Windows 7”):

- Sigue estando presente en Windows 10.
- Su finalidad es recuperar backup realizados sobre sistemas operativos Windows 7 en Windows 10.
- Debemos usar el historial de archivos siempre que sea posible.

Protección frente al malware

La función del Sandbox en un antivirus.

Desde la versión 1809, Windows 10 incluye un sandbox en su antivirus Windows Defender

Para poder inspeccionar por completo el sistema Windows 10, Windows defender corría con privilegios elevados.

No era lo ideal porque se podían usar vulnerabilidades presentes en el antivirus (ver cvedetails) para ganar acceso al resto del sistema.

El escalado de privilegios desde un sandbox es mucho más difícil de conseguir.

Si un malware consigue comprometer al antivirus, por ejemplo, cuando este está analizando el comportamiento del ejecutable sospechoso, los daños quedan limitados a este entorno aislado)

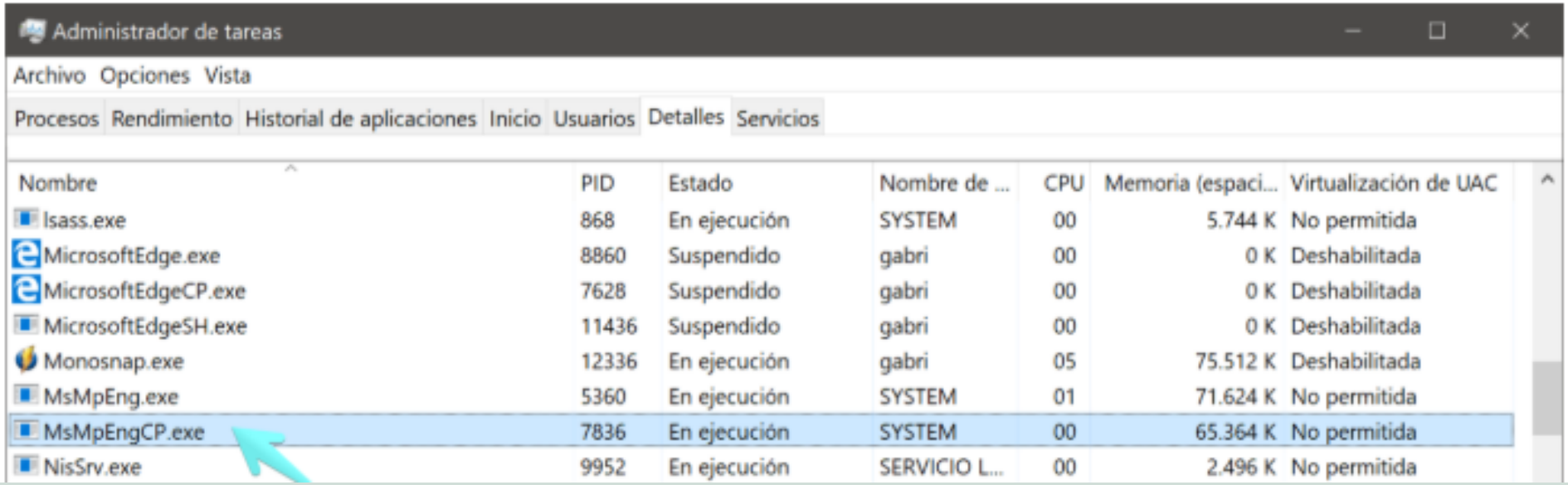
Protección frente al malware

La función del Sandbox en un antivirus.

Disponer de un sandbox no garantiza una mejora en el nivel de detección, solo limita la acción dañina del malware cuando se intenta detectar usando heurística.

Los “malos” también tienen técnicas para detectar que el malware se ejecuta en un entorno de sandbox y no exponen su payload.

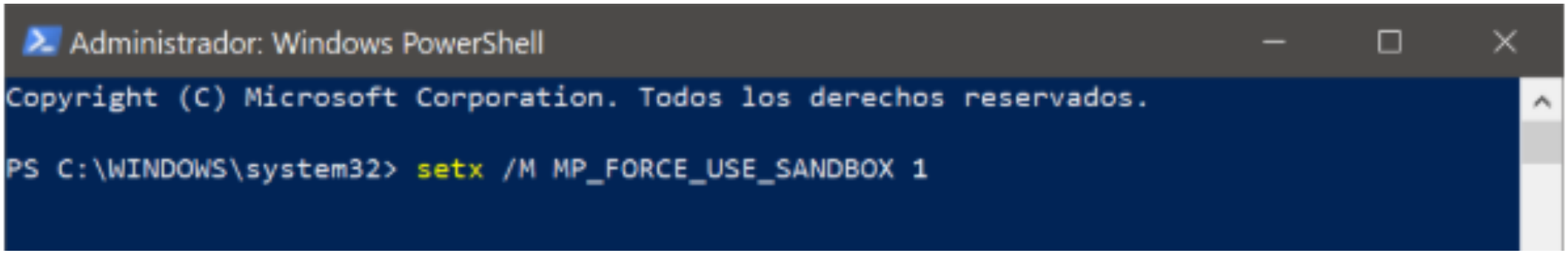
Para determinar si el sandbox de Defender está funcionando puedes examinar los proceso



Protección frente al malware

La función del Sandbox en un antivirus.

Para activar el sandbox de Windows Defender (Si no lo estuviera)



Protección frente al malware

Malware de día cero.

Difícil de gestionar con antivirus local.

Las soluciones cloud como M365 ya la implementan para el correo electrónico.

Zero hour AutoPurge (ZAP)

https://docs.microsoft.com/es-es/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Windows como Servicio

El paradigma del nuevo modelo de actualización de Windows 10.

Es un cambio conceptual muy importante a la hora de enfrentarnos a la actualización de Windows 10.

Windows como servicio es la solución de actualización que Microsoft quiere implementar. Se basa en la recogida de datos de los clientes.

https://docs.microsoft.com/es-es/Windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-levels .

Se diferencian actualizaciones de “Calidad” y de “Características”.

Windows como Servicio

Las actualizaciones de características

Aportan nuevas funcionalidades en el sistema operativo.

Dos entregas por año.

Mes 3 y 9.

El nombre de la versión de Windows 10 depende del conjunto de características disponibles: Windows 10 1809, Windows 10 1903, Windows 10 2003, ...

El ciclo de vida de una versión de Windows de 3-5 años. Después no hay soporte.

Windows como Servicio

Las actualizaciones de características

Los canales de servicio permiten elegir cuando se aplicarán las actualizaciones de características:

El canal semianual es el que está establecido por defecto y entrega dos actualizaciones de características al año, como se vio antes.

El canal de servicio de largo plazo (Long Term Servicing Channel) recibe características cada 2-3 años. Indicado para dispositivos industriales o cajeros automáticos.

Windows como Servicio

Las actualizaciones de calidad.

Aportan parches de seguridad, actualizaciones críticas, actualizaciones de servicio y de drivers. No aportan nuevas funcionalidades al sistema operativo.

Se liberan el segundo martes de cada mes (si no hay urgencias)

Se pueden retrasar hasta 30 días.

Aun es posible usar WSUS para aplicar los parches de seguridad, pero parece al medio plazo no podremos ser capaces de elegir los parches de seguridad por nosotros mismos.

Windows como Servicio

Los enlaces siguientes describen los conceptos que debemos tener claros para migrar al nuevo modelo de actualización de Windows 10.

Update Windows 10 in the enterprise
Deploy updates for Windows 10 Mobile Enterprise and Windows 10 IoT Mobile
Configure Delivery Optimization for Windows 10 updates
Configure BranchCache for Windows 10 updates
Configure Windows Update for Business
Integrate Windows Update for Business with management solutions
Walkthrough: use Group Policy to configure Windows Update for Business
Walkthrough: use Intune to configure Windows Update for Business
Manage device restarts after updates

sedian Seguridad Digital de Andalucía