



Cybersecurity Bootcamp

U2M2 - Análisis Forense y Respuesta ante Incidentes (DFIR)
Contención

Índice

Contención	3
Configuración de una red corporativa	3
4.1. Configuración inicial del servidor.	4
4.2. Configuración inicial de los workstations.	6
4.3. Creación y asignación a unidades organizativas del dominio.	8
Recomendaciones ante compromiso de usuarios	10
4.4. Revisión de cuentas de usuario del Active Directory.	10
Securización mediante políticas de grupo	11
4.5. Trata de identificar en los siguientes logs de eventos de Windows actividad maliciosa o ilegítima.	11
4.6. Directiva para bloquear la descarga desde internet mediante powershell.	12
4.7. Instala y configura el rol FSRM en Windows Server 2016 para crear un filtro de archivos que permita mitigar el riesgo de infección por ransomware.	17
Anexos	22
Listado de usuarios y equipos del dominio GRUPOLARA	22

Contención

Configuración de una red corporativa

Para poder llevar a cabo los siguientes ejercicios, en los que aplicaremos políticas de grupo de forma centralizada, definiéndolas en el controlador de dominio y replicándolas en el resto de equipos autenticados contra el dominio, debemos primeramente configurar las máquinas necesarias para crear una red corporativa que siga el siguiente esquema:

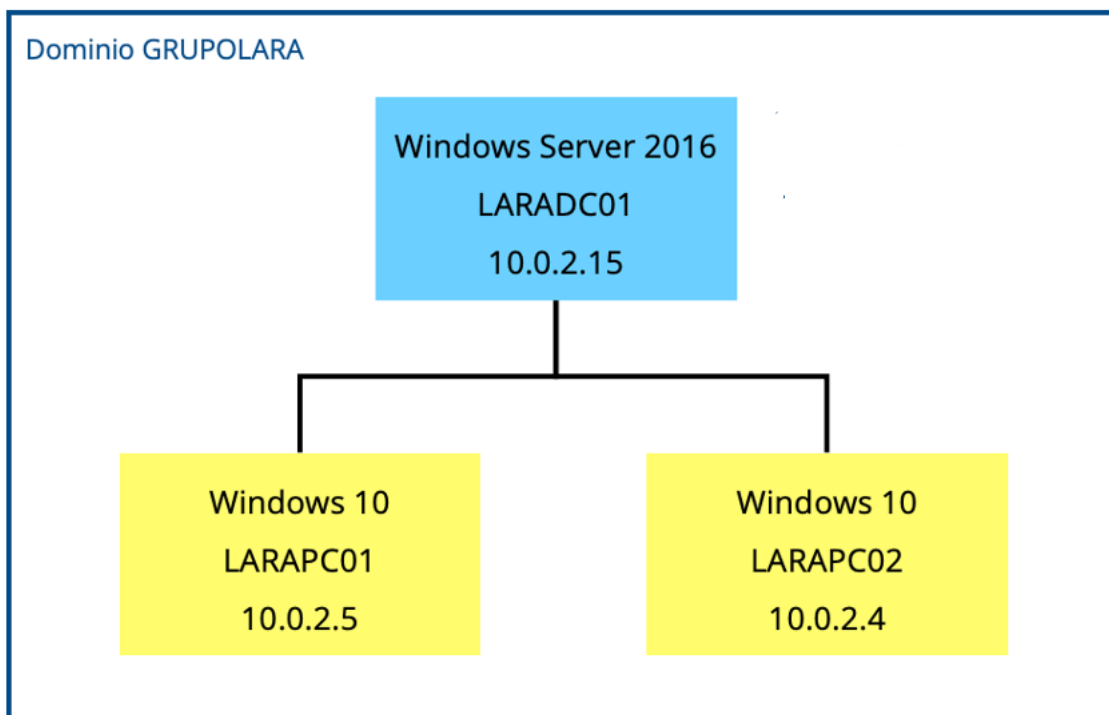


Ilustración 1. Mapa de red del entorno a virtualizar para el dominio GRUPOLARA

Asimismo, las máquinas virtuales que configuraremos para simular esta red corporativa de la organización ficticia Grupo Lara deberán cumplir los siguientes requisitos:

- Todas las workstations tienen la cuenta por defecto de Administrador local habilitada con contraseña.
- El servidor operará con las siguientes funcionalidades:
 - Controlador de dominio (**GRUPOLARA.local**)
 - Servidor de ficheros (con un mapeo de las carpetas de archivos en cada uno de los workstations a través de shares \$)
- Los usuarios pertenecientes a grupos de administración del dominio podrán conectarse mediante Escritorio Remoto al servidor y workstations, mientras que el resto de usuarios no podrán conectarse remotamente a ningún otro equipo de la red.

Para montar la red desde VirtualBox, primero seleccionaremos la opción **Herramientas > Preferencia > Red** desde la ventana del administrador, y seleccionaremos la opción de añadir una nueva red NAT, introduciendo los siguientes valores de configuración:

- Habilitar red: Sí
- Nombre de red: GrupoLara
- Red CIDR: 10.0.2.0/24
- Soporta DHCP: Sí
- Soporta IPv6: No

- Reenvío de puertos: no hay que configurar ninguno

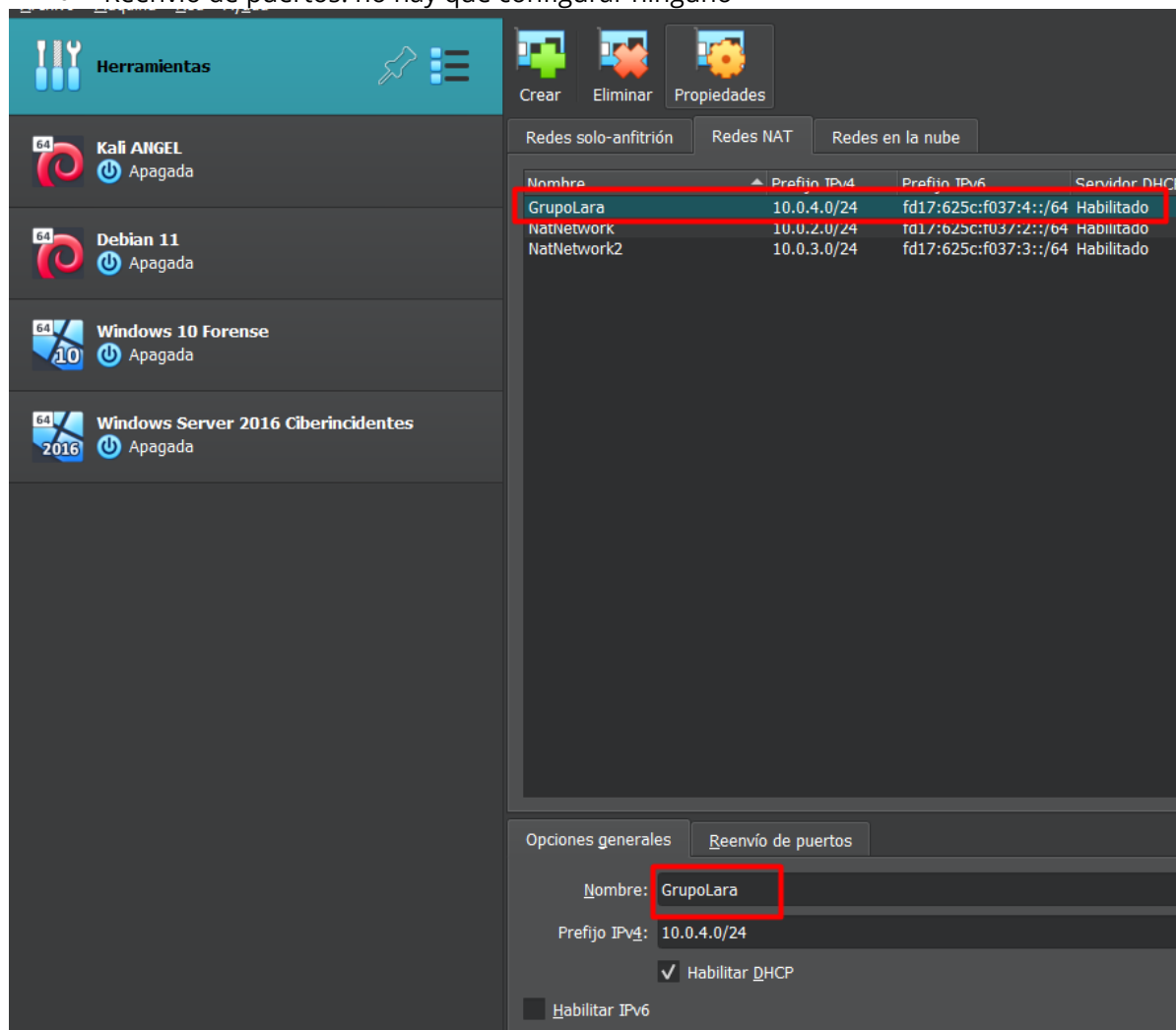


Ilustración 2. Configuración de red NAT en VirtualBox

Una vez definida la red NAT a la que conectaremos nuestras máquinas, debemos indicarles a qué red deben conectarse antes de levantarlas. Para ello, para cada máquina seleccionaremos la opción **Configuración > Red > Conectado a: Red NAT** e indicaremos la red **GrupoLara** recién creada. En las opciones avanzadas, únicamente debemos comprobar que la opción de “Cable conectado” se encuentra habilitada.

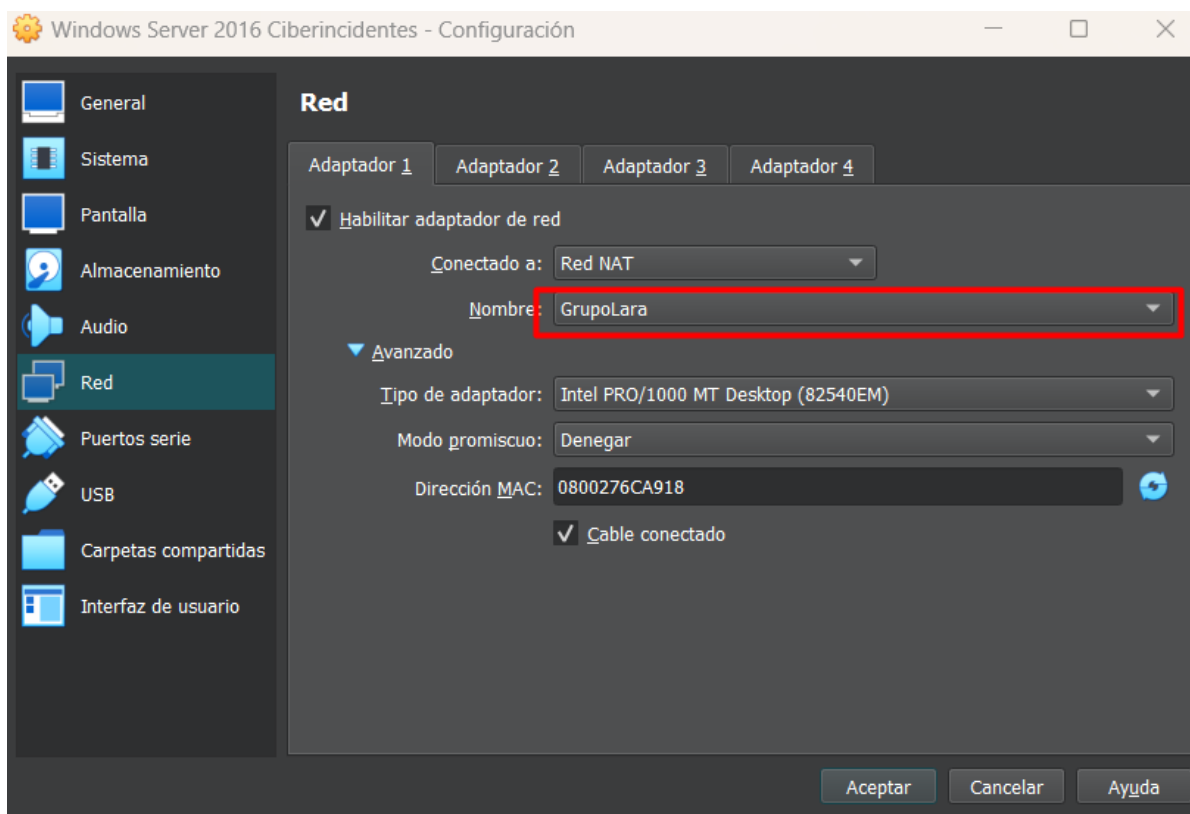


Ilustración 3. Inclusión de las máquinas virtuales a la red NAT creada

Una vez configurados estos parámetros, podemos proceder a levantar la máquina Windows Server 2016, ya que deberemos comenzar la configuración desde dicha máquina.

4.1. Configuración inicial del servidor.

Iniciamos sesión con las credenciales de **admin_jcrojo**³ usuarios ficticio administrador de sistemas cuya cuenta emplearemos para las gestiones relacionadas con el servidor del Grupo Lara.

Primeramente, debemos configurar las direcciones IP para nuestro servidor, de forma que sea visible para los demás workstations que conectaremos con posterioridad, así como disponer de salida a Internet.

Seleccionamos el **icono de adaptador de red** a la derecha de la barra de tareas de Windows, **Configuración de red > Cambiar opciones del adaptador**. Hacemos **click derecho** sobre el adaptador **Ethernet > Propiedades** y en la ventana que se abra, seleccionamos del listado mostrado la opción "Protocolo de Internet versión 4 (TCP/IPv4). Clickamos en la opción **Propiedades** y comprobamos que, en la pestaña **General**, se encuentran seleccionadas las siguientes opciones:

- Obtener una dirección IP automáticamente
- Obtener la dirección DNS del servidor automáticamente

Para poder definir estos campos de forma estática y que el resto de workstations que vamos a agregar al dominio a continuación puedan encontrar nuestro controlador de dominio, debemos consultar qué direcciones IP nos asigna el resolutor DHCP de la red NAT creada, y copiar dichos valores en las propiedades de Internet versión 4.

Para ello, abrimos una consola de comandos (**cmd**) y ejecutamos el comando **ipconfig/all**.

```

C:\Users\admin_jcrojo>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : LARADC01
Sufijo DNS principal . . . . : GRUPOLARA.local
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: GRUPOLARA.local

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-6C-A9-18
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::9187:4f37:1e41:587e%15(Preferido)
Dirección IPv4. . . . . : 10.0.4.4(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 12 de diciembre de 2023 16:40:27
La concesión expira . . . . . : martes, 12 de diciembre de 2023 17:10:26
Puerta de enlace predeterminada . . . . : 10.0.4.1
Servidor DHCP . . . . . : 10.0.4.3
IAID DHCPv6 . . . . . : 50855975
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2B-8C-07-16-08-00-27-6C-A9-18
Servidores DNS. . . . . : ::1
                        212.230.135.1
                        212.230.135.2
                        192.168.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
Dirección física. . . . . : 08-00-27-B1-C4-DF
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::34b2:f052:1747:6c4b%6(Preferido)
Dirección IPv4. . . . . : 10.0.2.22(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 12 de diciembre de 2023 16:40:39
La concesión expira . . . . . : martes, 12 de diciembre de 2023 17:10:37
Puerta de enlace predeterminada . . . . : 10.0.2.1
Servidor DHCP . . . . . : 10.0.2.3
IAID DHCPv6 . . . . . : 319291431
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2B-8C-07-16-08-00-27-6C-A9-18
Servidores DNS. . . . . : 212.230.135.1
                        212.230.135.2
                        192.168.1.1

```

Ilustración 4. Configuración de red asignada automáticamente por el DHCP de la red NAT para el servidor

³ Para más detalle de las credenciales de usuarios del dominio, consultar el [Anexo](#).

Las direcciones que se indiquen en los campos **Dirección IPv4**, **Máscara de subred**, **Puerta de enlace predeterminada** y **Servidores DNS** son los que deberemos introducir manualmente en la ventana de Propiedades: Protocolo de Internet versión 4 /TCP/IPv4) que hemos consultado con anterioridad.

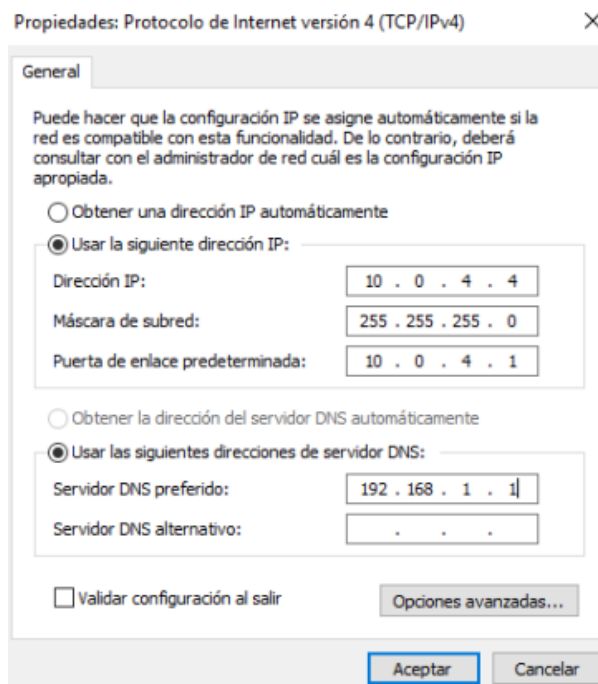
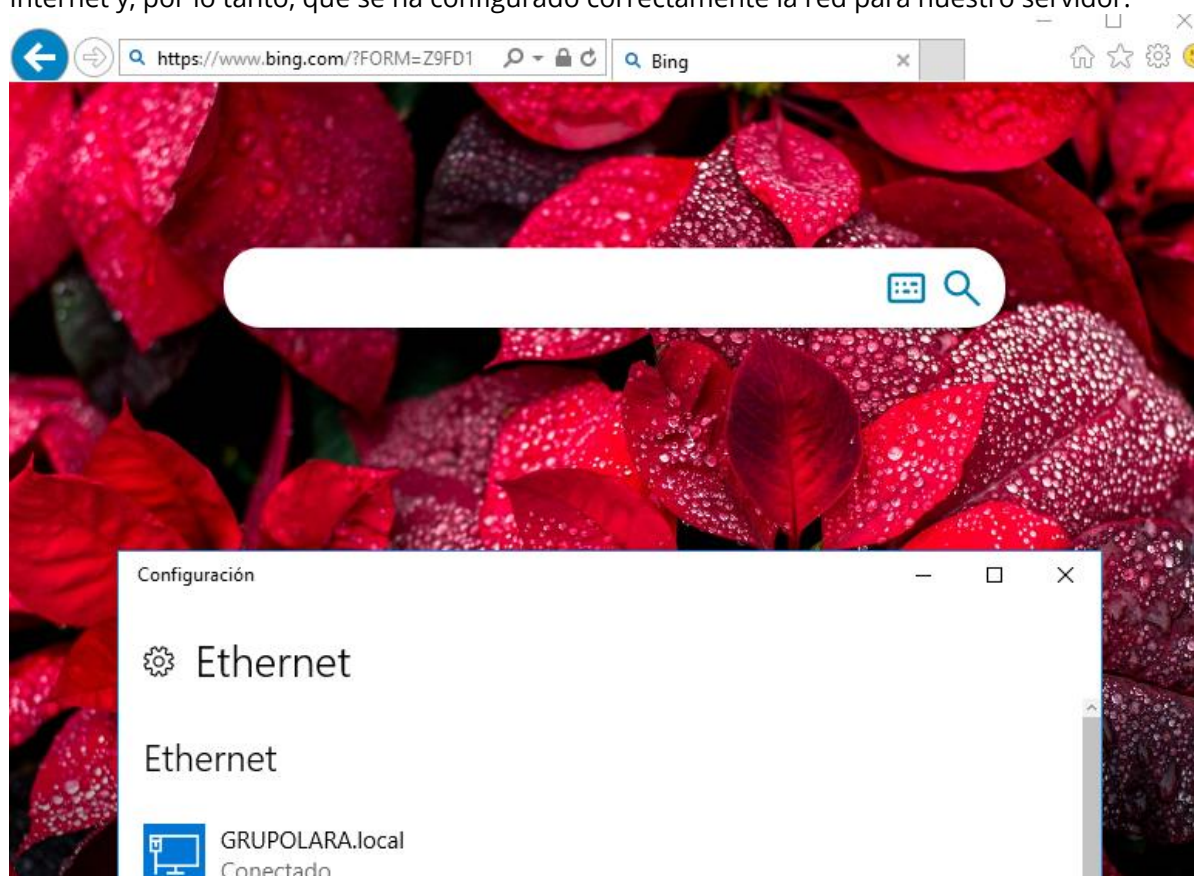


Ilustración 5. Configuración final de red para el servidor LARADC01

Una vez finalizado este paso, comprobaremos que seguimos disponiendo de conexión a Internet y, por lo tanto, que se ha configurado correctamente la red para nuestro servidor.



4.2. Configuración inicial de los workstations.

Para añadir un equipo corporativo a la red del dominio, de forma que puedan autenticarse usuarios del dominio en dicha máquina, haciendo la comprobación de credenciales contra el

servidor que opera como DC, debemos modificar también su configuración de red como hemos hecho con el servidor.

Seleccionamos el icono del adaptador de red a la derecha en la barra de tareas de Windows, **Configuración de red e Internet > Cambiar opciones del adaptador**. Hacemos **click derecho** sobre el adaptador **Ethernet > Propiedades** y en la ventana que se abra, seleccionamos del listado mostrado la opción “Protocolo de Internet versión 4 (TCP/IPv4). Clickamos en la opción **Propiedades** y comprobamos que, en la pestaña **General**, se encuentran seleccionadas las siguientes opciones:

- Obtener una dirección IP automáticamente
- Obtener la dirección DNS del servidor automáticamente

En este caso, sólo necesitamos **modificar el valor del resolutor DNS**, ya que queremos que sea nuestro servidor. Por ello, seleccionaremos la opción Usar las siguientes direcciones de servidor DNS y estableceremos como DNS preferido la dirección IP de nuestro servidor que hemos consultado y configurado en el paso anterior.

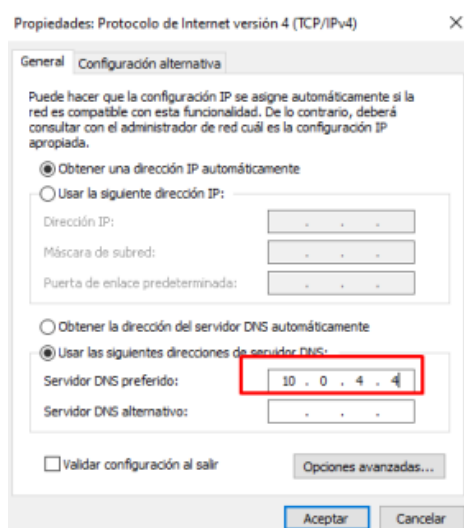


Ilustración 6. Configuración de red para los workstations

A continuación, procedemos a incluir nuestro Workstation en el dominio de GRUPOLARA gestionado por el servidor LARADC01.

Para ello, seleccionamos con el **botón derecho** sobre **Este equipo > Propiedades**, y en la venta que se nos muestre con información del sistema, en el subapartado “Configuración de nombre, dominio y grupo de trabajo del equipo”, seleccionamos **Cambiar configuración**.

En la ventana que se nos muestre, en la pestaña **Nombre de equipo** seleccionaremos el botón **Cambiar...**, y en **Miembro del**, seleccionaremos **Dominio** e introduciremos **GRUPOLARA.local**. Para facilitar la identificación de equipos en la misma red, se recomienda asimismo **modificar el nombre del equipo** por LARAPC01. Seleccionamos Aceptar, y tras introducir las credenciales de un usuario con privilegios de administrador del dominio (admin_jcrojo:P@ssw0rd, por ejemplo), tras unos segundos nos indicará que nuestra máquina se ha unido exitosamente al dominio.

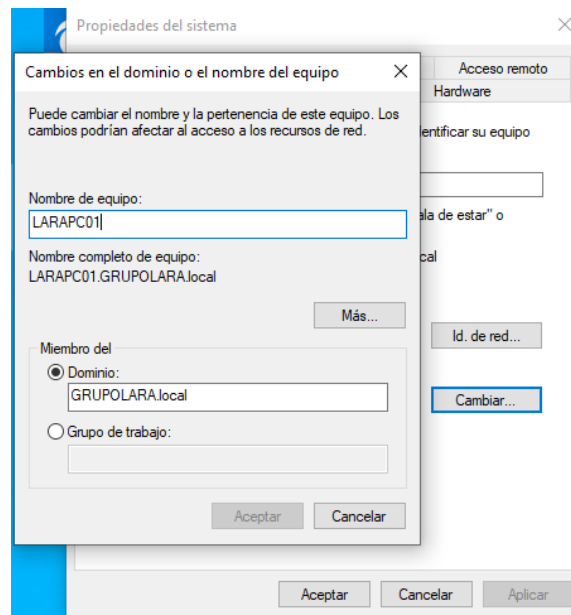
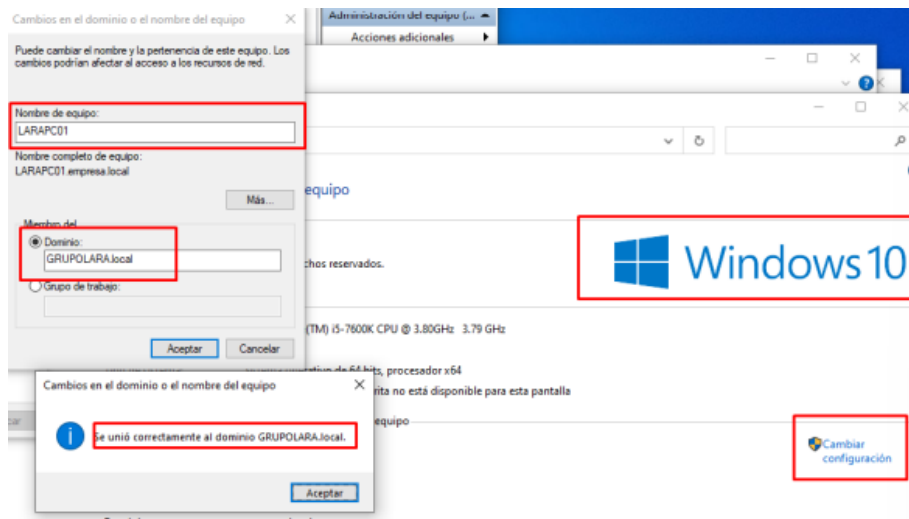
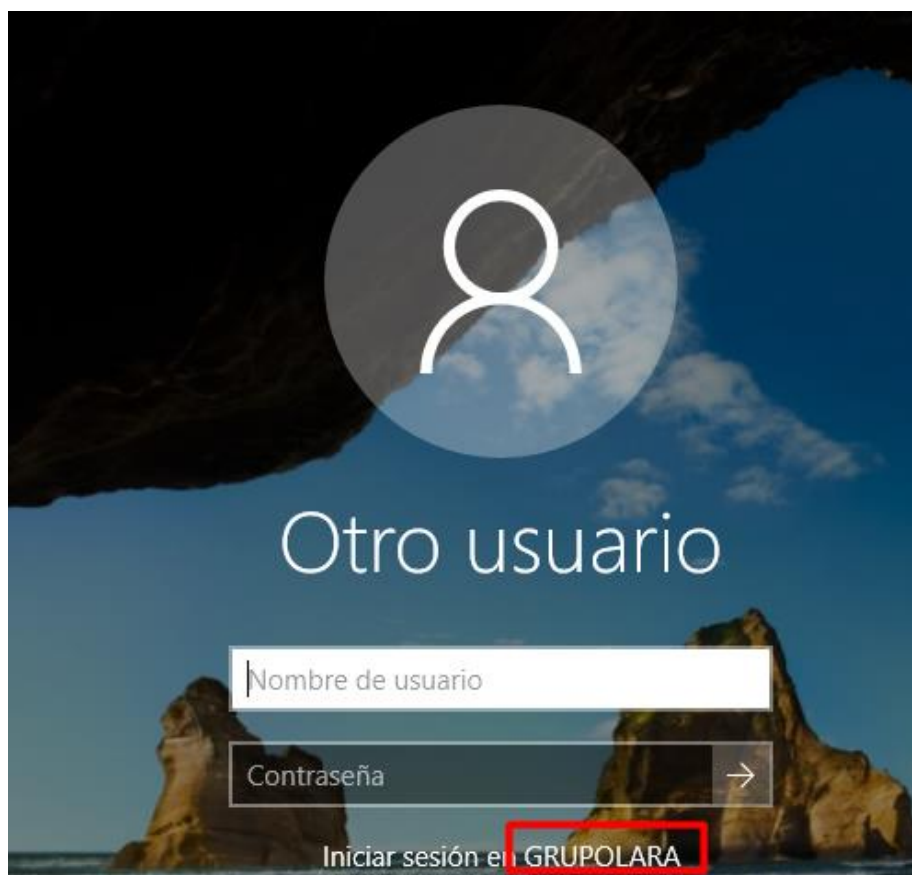


Ilustración 7. Pasos para añadir un workstation al dominio GRUPOLARA



Procedemos a reiniciar para que se apliquen los cambios, y ahora podemos **probar a iniciar sesión con el usuario admin_jcrojo** que, si bien no es un usuario local del equipo LARAPC01, al ser un usuario del dominio, dicho usuario procederá a autenticarse contra el controlador de dominio en nuestro servidor que se encuentra conectado a la misma red, y nos creará una sesión nueva para este usuario.



4.2.1. Requisitos para administración remota

De cara a poder gestionar la aplicación y actualización de directivas de grupo desde el controlador de dominio de forma remota y centralizada, es necesario que se habiliten una serie de permisos y comunicaciones a nivel de Firewall en los workstations para que, desde el controlador de dominio, ciertas funciones de estos workstations sean accesibles y editables a nivel de red de dominio.

Para ello, deberemos seleccionar en el equipo con Windows 10, **Panel de Control > Sistema y Seguridad > Permitir una aplicación a través del firewall de Windows**. En la lista de opciones, deberemos seleccionar las que se indican a continuación, únicamente para el checkbox del **Dominio**, requisito necesario para habilitar la comunicación remota con el workstation desde el DC:

- Administración remota de tareas programadas
- Asistencia remota
- Instrumental de administración de Windows (WMI)

Una vez habilitadas estas reglas en el firewall, ya deberíamos tener permisos para forzar la actualización de directivas de grupo remotamente desde el DC.

Permitir a las aplicaciones comunicarse a través de Firewall de Windows Defender

Para agregar, cambiar o quitar aplicaciones y puertos permitidos, haga clic en Cambiar la configuración.

¿Cuáles son los riesgos de permitir que una aplicación se comunique?

[Cambiar la configuración](#)

Aplicaciones y características permitidas:

Nombre	Dominio	Privada	Pública
<input type="checkbox"/> Administración remota de servicios	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Administración remota de tareas programadas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Administración remota de Windows	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Administración remota de Windows (compatibilidad)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Administración remota del volumen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Agregar una cuenta profesional o educativa	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Asistencia remota	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache: cliente de caché hospedada (usa HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache: detección del mismo nivel (usa WSD)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache: recuperación de contenido (usa HTTP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache: servidor de caché hospedada (usa HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Calculadora de Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Detalles...](#) [Quitar](#)

[Permitir otra aplicación...](#)

4.3. Creación y asignación a unidades organizativas del dominio.

Una vez completada la configuración para el primer workstation, se recomienda clonar la máquina virtual Windows 10 y añadir una segunda máquina al dominio (LARAPC02) siguiendo los mismos pasos, que nos ayude a entender a la hora de aplicar políticas de grupo cómo se replican las mismas.

Es importante destacar que, al clonar la máquina, se mantiene la misma configuración que la original, incluido nombre de equipo, y que, si bien se encuentra presuntamente asociada al dominio, en nuestro DC no nos aparecerá ya que no hemos seguido el procedimiento para asociarla. Por lo tanto, es importante para este segundo workstation repetir los pasos del apartado 4.2, desasociando la máquina del dominio GRUPOLARA y volviendo a asociarla tras cambiar el nombre del equipo a LARAPC02.

No obstante, en caso de no ser factible esta opción de levantar dos workstations por no disponer de suficientes recursos en la máquina host, continuaremos con un único equipo LARAPC01.

Adicionalmente, aunque los workstations ya aparecen asociados al dominio y puede comprobarse que efectivamente aparecen desde el **Administrador del servidor > Herramientas > Usuarios y equipos del Active Directory**, en la subcategoría **Equipos** del árbol de la izquierda, debemos **crear una unidad organizativa** (OU, por sus siglas en inglés) y mover estos workstations a la misma, de forma que cuando creemos una directiva de grupo, podamos indicar que se aplique únicamente a ciertas OU.

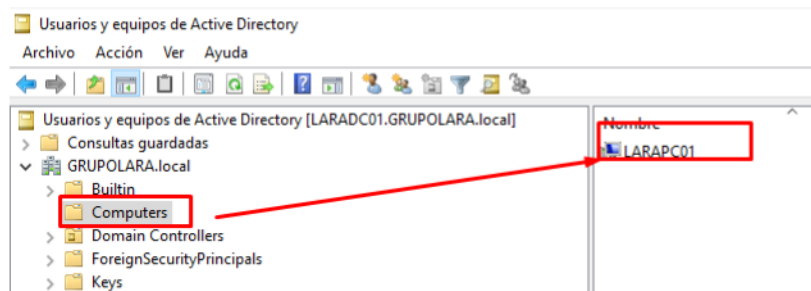


Ilustración 8. Equipos asociados al dominio

Esta categorización sirve principalmente para segmentar el entorno tecnológico de la organización y conseguir un mayor nivel de atomicidad que nos permita aplicar una política de mínimos privilegios efectiva, asignando permisos únicamente a aquellos equipos o usuarios que realmente los necesitan para el desarrollo de sus funciones.

Para crear una OU, seleccionamos en el árbol de la izquierda el dominio principal (en nuestro caso, GRUPOLARA.local), hacemos click derecho, **Nuevo > Unidad organizativa**.

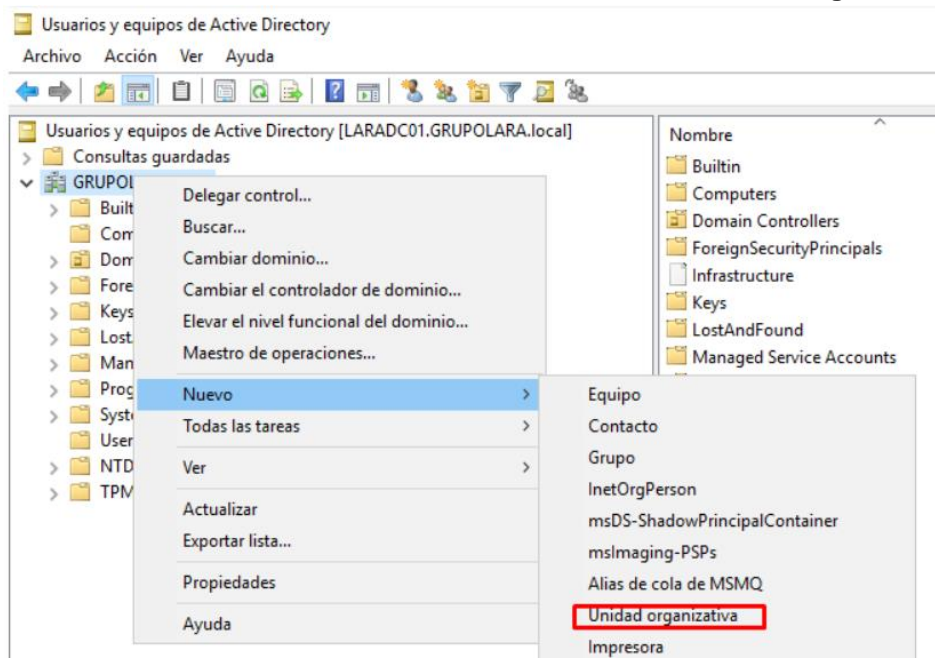


Ilustración 9. Creación de una nueva OU

Se mostrará un campo donde debemos introducir simplemente el nombre que queremos dar a nuestra OU, que denominaremos **Workstations**, y seleccionamos Aceptar.

El siguiente paso que debemos hacer es mover los equipos LAPC a nuestra OU. Para ello, desde Equipos en el árbol de directorios de la izquierda, seleccionamos el equipo que queremos mover y hacemos click derecho, **Mover...** Seleccionamos la carpeta Workstations, Aceptar, y podremos comprobar que LAPC ha desaparecido del grupo Equipos y ahora aparece en Workstations.

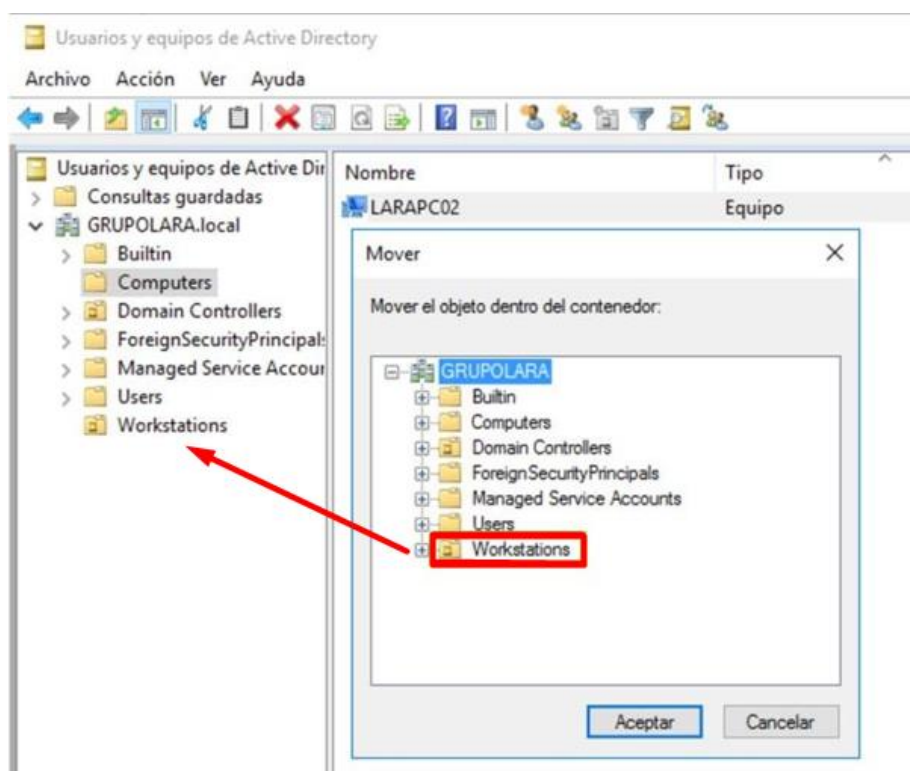


Ilustración 10. Mover equipos a una OU

Una vez asignados los equipos a la unidad organizativa correspondiente, desde el Administrador de directivas de grupo podremos forzar la actualización de políticas directamente para toda la OU como veremos en los próximos apartados.

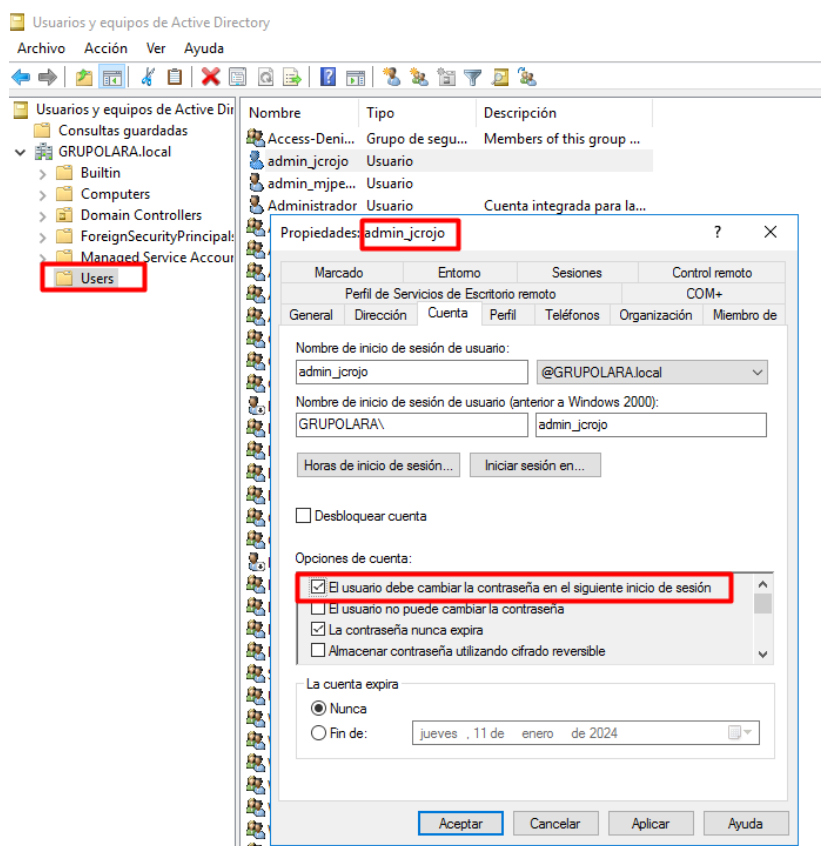
Recomendaciones ante compromiso de usuarios

4.4. Revisión de cuentas de usuario del Active Directory.

- Para todas aquellas cuentas que se identifique que cumplen malas prácticas, debe modificarse su configuración de forma que se fortalezca el entorno tecnológico del cliente.
- Entre los usuarios del dominio que se encuentran ya definidos en el Active Directory, podemos encontrar 2 administradores y 1 usuario con privilegios limitados. Identifica para dichos usuarios vulnerabilidades de seguridad en su configuración:

Nombre de usuario	Vulnerabilidad identificada
admin_jcrojo	<ul style="list-style-type: none"> • Contraseña no expira nunca
admin_mjperez	<ul style="list-style-type: none"> • No hay definido un límite temporal de sesión activa • No hay establecido un cambio periódico de contraseña para X días
invitado	<ul style="list-style-type: none"> • El tiempo para el cambio periódico de contraseña es de 1 año

- En los casos en los que se produce un incidente de seguridad, pueden haberse visto potencialmente comprometidas cuentas del dominio, usualmente las de administradores ya que se necesitan privilegios elevados para la ejecución de algunas de las piezas de malware más comunes.
- Para forzar un cambio de contraseña a todos los usuarios administradores del dominio y otros grupos de administradores que se consideren de interés, se puede configurar esta opción desde el controlador de dominio.
- Fuerza un cambio de contraseña en el siguiente inicio de sesión para los usuarios administradores del dominio, y comprueba que efectivamente al iniciar sesión con alguna de estas cuentas, se solicita forzosamente el cambio de contraseña, mientras que el usuario sin privilegios puede seguir iniciando sesión con su contraseña habitual.
- Solución del caso:
 - Desde la propia ventana de administración de **Usuarios y equipos del Active Directory**, se puede ir seleccionando uno a uno los usuarios con el click derecho, **Propiedades**, y seleccionando la pestaña **Cuenta**. En Opciones de cuenta, podremos seleccionar el checkbox correspondiente a **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.



- No obstante, para centralizar el forzado de modificación de contraseña y se aplique a todo un grupo del dominio, emplearemos un sencillo script desde el Powershell del DC, ejecutado como administrador.

```
Get-ADGroup "Admins. del dominio" | Get-ADGroupMember -Recursive | Set-ADUser -ChangePasswordAtLogon $true
```

PS C:\Users\admin_jcrojo> Get-ADGroup "Admins. del dominio" | Get-ADGroupMember -Recursive | Set-ADUser -ChangePasswordAtLogon \$true

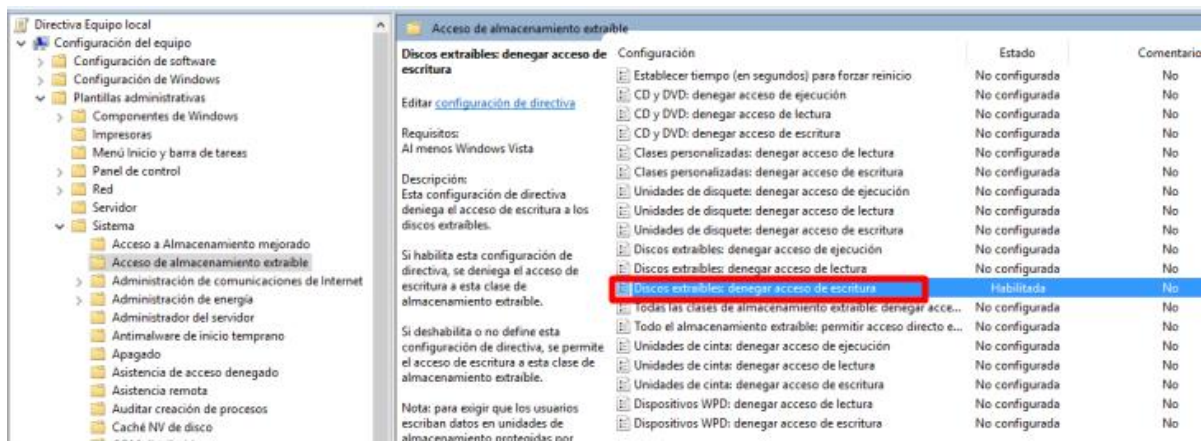
- Es importante destacar que el nombre del grupo del Active Directory que indiquemos (en este caso, Admins. del dominio) debe estar escrito tal cual nos aparece en la ventana de **Usuarios y equipos del Active Directory**.
- Podemos confirmar que efectivamente se ha aplicado bien este forzado de cambio de contraseña entrando en **Usuarios y equipos del Active Directory > admin_jcrojo > Propiedades > Cuenta**, y veremos cómo se ha seleccionado la checkbox correspondiente a **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**.
- Por otra parte, si revisamos esta misma opción para el usuario **jagonzalez** que no pertenece al grupo de Admins. del dominio, veremos que dicha checkbox no se encuentra seleccionada.
- Si por ejemplo quisiéramos forzar el cambio de contraseña en el siguiente inicio de sesión **para todos los usuarios del dominio**, independientemente de los grupos a los que pertenezcan, podríamos emplear el siguiente script:

```
Get-ADUser -Filter * | Set-ADUser -ChangePasswordAtLogon $true
```

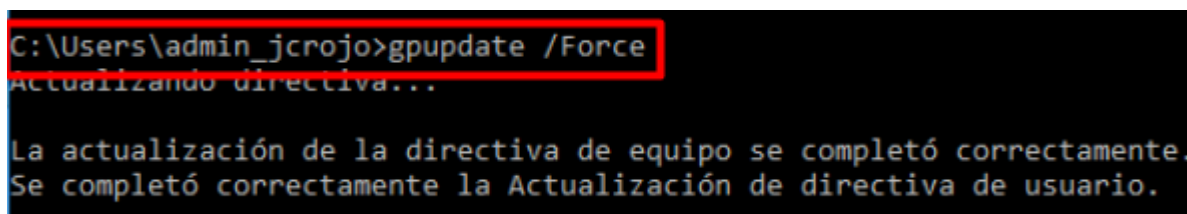
Securización mediante políticas de grupo

4.5. Trata de identificar en los siguientes logs de eventos de Windows actividad maliciosa o ilegítima.

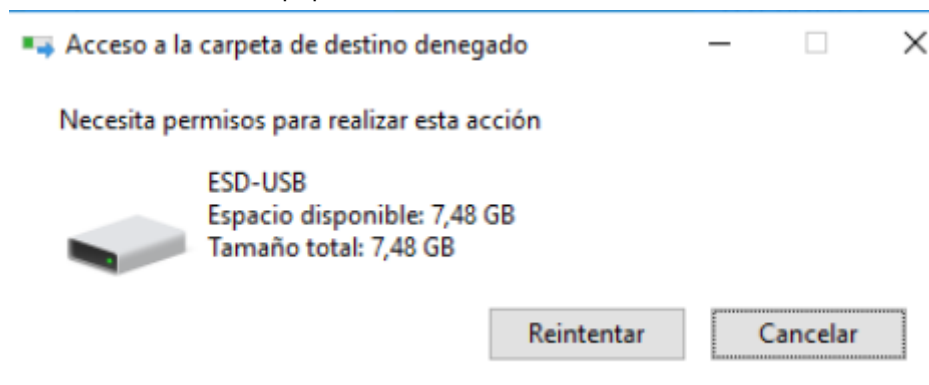
- Para poder terminar el proceso de cifrado que nos impide extraer evidencias del equipo a analizar, es necesario previamente identificar y detener dicho proceso.
- Podemos hacer uso de herramientas de la suite SysInternals de Windows.
- No obstante, para poder ejecutar dichas herramientas desde un dispositivo externo que conectemos al equipo infectado y que no se vea cifrado el contenido del mismo en el momento de la conexión, es necesario previamente establecer una restricción de escritura sobre dichos dispositivos extraíbles incluso para las cuentas con privilegios de administrador, lo cual podemos hacer a través de una política de grupo.
- Solución del caso:
 - Abrimos **gpedit.msc** desde "Ejecutar..." (• + R)
 - *Buscamos Configuración del equipo > Plantillas administrativas > Sistema > Acceso de almacenamiento extraíble*
 - Para la política "**Discos extraíbles: denegar acceso de escritura**" cambiamos el estado de "No configurada" a "Habilitada".



- Para que tenga efecto la modificación, abrimos una consola de comandos ejecutando **cmd** desde “Ejecutar...” (• + R) y escribimos **gpupdate /Force** (se pueden listar todas las opciones disponibles para el comando gpupdate con la opción **/h** en vez de **/Force**).



- Conectamos el dispositivo USB extraíble al equipo y probamos a copiar un fichero del equipo al USB.



4.6. Directiva para bloquear la descarga desde internet mediante powershell.

4.6.1. Bloqueo a nivel de Workstation mediante directiva local

- Para bloquear la descarga de código malicioso desde Internet mediante la ejecución de Powershell (como es el modus operandi de la descarga de Emotet), debemos restringir la consola de Powershell para que no pueda conectarse a Internet, tanto para el envío como para la recepción de paquetes.
- Solución del caso:
 - Abrimos la aplicación nativa de **Windows Defender Firewall con seguridad avanzada**.
 - Seleccionamos en el menú izquierdo **Reglas de entrada/Reglas de salida**

Debido a que la consola de Powershell se puede lanzar desde 4 localizaciones distintas (debido a que existe para 32 y 64 bits, y la consola de comandos y el editor IDE), deben configurarse de forma preventiva un total de 8 reglas de firewall (4 de entrada y 4 de salida).

-
- Firewall de Windows con seguridad avanzada
- Archivo Acción Ver Ayuda
- Firewall de Windows con seguridad avanzada
- Reglas de entrada
- | Nombre | Grupo | Perfil | Habilitado | Acción | Invaldar | Programa |
|---|-----------------------|--------|------------|----------|----------|--------------------------|
| 1 | | Todo | Sí | Bloquear | No | %SystemRoot%\SysWOW... |
| 2 | | Todo | Sí | Bloquear | No | %SystemRoot%\SysWOW... |
| 3 | | Todo | Sí | Bloquear | No | %SystemRoot%\system32... |
| 4 | | Todo | Sí | Bloquear | No | %SystemRoot%\system32... |
| Acceso a red COM+ (DCOM de entrada) | Acceso a red COM+ | Todo | No | Permitir | No | %systemroot%\system32... |
| Administración de DFS (DCOM de entrada) | Administración de DFS | Todo | Sí | Permitir | No | %systemroot%\system32... |

- ```
(New-Object Net.WebClient).DownloadString("https://www.google.es")
```

- ```
PS C:\Users\admin_jcrojo> (New-Object Net.WebClient).DownloadString("https://www.google.es")
Excepción al llamar a "DownloadString" con los argumentos "1": "No es posible conectar con el servidor remoto"
En línea: 1 Carácter: 1
+ (New-Object Net.WebClient).DownloadString("https://www.google.es")
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : WebException
```

```
PS C:\Users\admin_jcrojo> (New-Object Net.WebClient).DownloadString("https://www.google.es")
Excepción al llamar a "DownloadString" con los argumentos "1": No es posible conectar con el servidor remoto
En línea: 1 Carácter: 1
+ (New-Object Net.WebClient).DownloadString("https://www.google.es")
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : WebException

PS C:\Users\admin_jcrojo>
```

- Si procedemos a deshabilitar las reglas y volvemos a ejecutar el comando en Powershell, podremos observar cómo esta vez la consulta devuelve contenido.

```
PS C:\Users\admin_jcrojo> (New-Object Net.WebClient).DownloadString("https://www.google.es")
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="es"><head><meta content="Google.es permite
acceder a la información mundial en castellano, catalán, gallego, euskara e inglés." name="description"><meta content="n
oodp" name="robots"><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content="/images/branding/g
oogle/1x/google_standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="yZuWUVp9JydpHDKK6g2hMQ=
">(function(){window.google={kEI:'cGdrXr-ZArqKjLsPwWGoAY',kEXPI:'0,1353747,5662,730,224,5105,206,3204,10,1051,175,364,
1435,4,60,742,75,166,217,140,106,5,624,235,270,225,82,438,247,45,104,5,214,1126631,1197735,289,125,41,329077,1294,12383,
4855,32692,15247,867,28684,364,8824,8384,1326,3532,1362,283,4040,4968,3023,4744,7,3111,7915,1808,4020,978,7932,5296,2054
,920,873,1217,2975,6430,11306,2884,20,318,1981,2538,2775,519,400,1832,445,8,2796,1593,1279,2213,201,328,149,1103,840,517
,1466,8,48,820,3438,312,1137,2,2063,606,789,1050,184,1777,520,1947,747,271,1,157,1033,113,328,1284,16,445,2482,2246,474,
1339,748,1039,3227,773,2072,7,817,503,951,2534,1,793,2034,4682,1833,2661,641,2449,2459,1226,497,965,281,3654,1274,108,14
44,309,1173,481,908,2,1913,123,1519,1883,514,5419,226,281,376,338,1670,188,2,290,1767,184,3,350,201,29,157,813,183,388,3
9,134,121,373,93,923,280,218,125,1906,440,267,148,2172,1194,135,744,164,320,740,521,28,201,93,535,2,526,2,592,272,122,37
,8,42,172,219,596,1211,50,142,924,421,46,320,854,1018,1370,35,179,142,60,240,291,977,94,154,302,361,106,32,3,16,120,122,
231,60,197,150,243,284,385,2,18,35,482,562,5836606,1874,1403,1802617,4194806,162,2801054,549,333,444,1,2,80,1,900,896,1,
8,1,2,2551,1,748,141,59,736,563,1,4265,1,1,1,1,137,1,879,9,305,641,5,76,20,3,1,248,2,44,13,2,23963348,25',kBL:'17Fo'};go
ogle.sn='webhp';google.kHL='es';})();(function(){google.lc=[];google.li=0;google.getEI=function(a){for(var b;a&&(a.getA
ttribute||!(b=a.getAttribute("eid"))));a=a.parentNode;return b||google.kEI};google.getLFI=function(a){for(var b=null;a&&
(!a.getAttribute||!(b=a.getAttribute("leid"))));a=a.parentNode;return b};google.ml=function(){return null};google.time=f
unction(){return Date.now();};google.log=function(a,b,e,c,g){if(a=google.logUrl(a,b,e,c,g)){b=new Image;var d=google.lc,f
=google.li;d[f]=b;b.onerror=b.onload=b.onabort=function(){delete d[f]};google.vel&&google.vel.lu&&google.vel.lu(a);b.src
=a;google.li=f+1};google.logUrl=function(a,b,e,c,g){var d="",f=google.ls||"";e||-1!=b.search("&ei=")||!(d="&ei="+google.
getEI(c),-1!=b.search("&ei=")&&(c=google.getLFI(c)&&(d="&lei="+c));c="";!e&&google.cshid&&1==b.search("&cshid=")&&"s
lh"!="a&&(c="&cshid="+google.cshid);a=e||"/"+"(g|"gen_204")+"?atyp=i&ct="+a+"&cad="+b+d+f+"&zxx="+google.time()+c;^http://
i.test(a)&&"https:"=="window.location.protocol&&(google.ml(Error("a"),!1,{src:a,glmm:1}),a="");return a};}).call(this);(f
unction(){google.y={};google.x=function(a,b){if(a)var c=a.id;else{do c=Math.random();while(google.y[c])}google.y[c]=[a,b
];return!1};google.lm=[];google.plm=function(a){google.lm.push.apply(google.lm,a)};google.lq=[];google.load=function(a,b
,c){google.lq.push([[a,b,c]]);google.loadAll=function(a,b){google.lq.push([a,b])}.call(this);google.f={};(function()
{
```

Ilustración 12. Resultado que devuelve la consulta realizada exitosamente mediante Powershell

4.6.2. Bloqueo a nivel de dominio mediante GPO

- Para bloquear la descarga de código malicioso desde Internet mediante la ejecución de Powershell, y forzar a todos los equipos de la red de la organización a implementar esta política simultáneamente, definiremos una política de grupo (GPO) a nivel de dominio para desplegar en todos los equipos a la vez.
- Para ello, desde el Administrador del servidor, seleccionamos en el menú superior a la derecha **Herramientas > Administración de directivas de grupo**

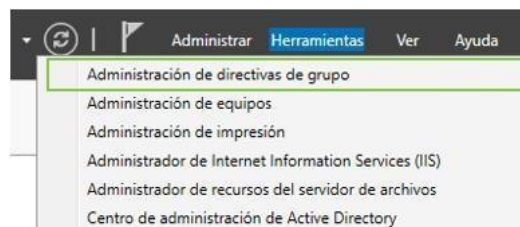


Ilustración 13. Acceso al administrador de políticas de grupo del servidor

En la ventana que se abrirá, desplegamos en el menú lateral izquierdo el **Bosque > Dominios** y clickamos con el botón derecho sobre GRUPOLOCAL.local, seleccionando **Crear un GPO en este dominio y vincularlo aquí...**

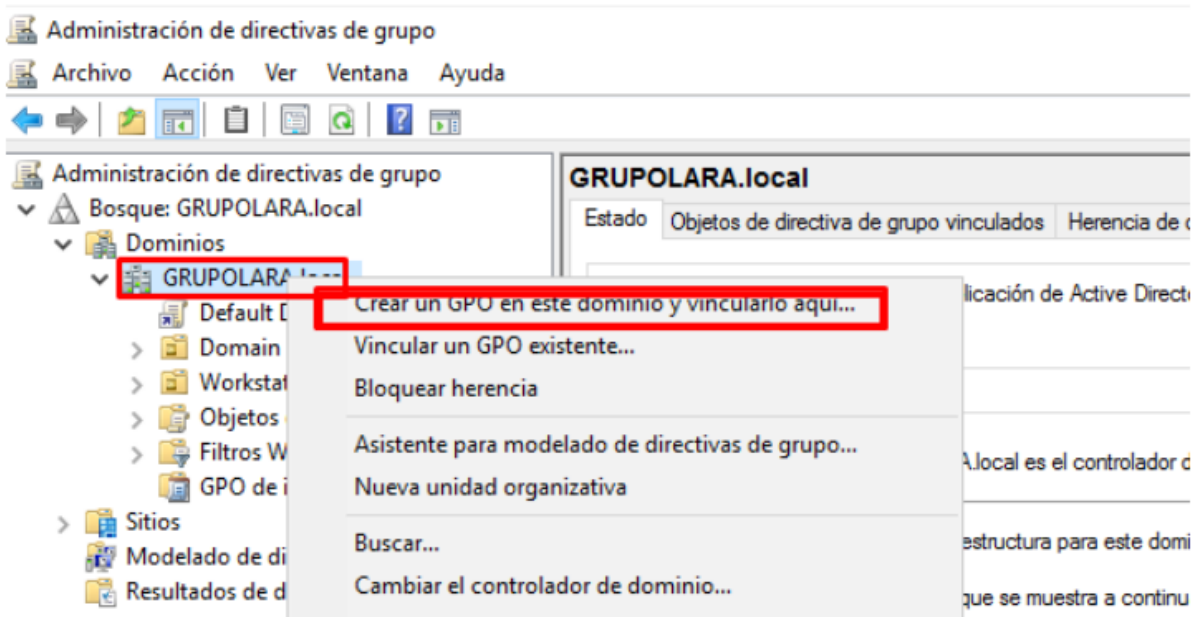
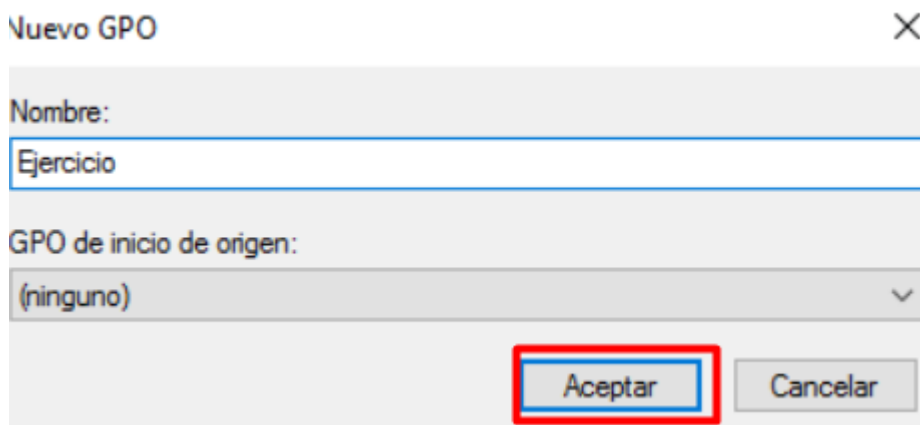
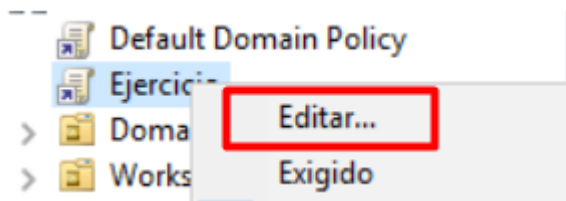






Ilustración 14. Opción para añadir una nueva GPO al dominio



- La nueva GPO aparecerá en la barra lateral con el nombre que hemos definido. Hacemos click con el botón derecho sobre esta nueva GPO, y seleccionamos **Editar...**



- En la nueva ventana del editor de políticas de grupo que aparece, seleccionamos en el desplegable de la izquierda **Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Firewall de Windows con seguridad avanzada > Firewall de Windows con seguridad avanzada > Reglas de entrada/Reglas de salida**, y creamos las reglas como en el apartado anterior (botón derecho, **Nueva regla...**).
- Creamos las diferentes reglas

Nombre	Grupo	Perfil	Habilitado
 Ejercicio 1		Todo	Sí
 Ejercicio 2		Todo	Sí
 Ejercicio 3		Todo	Sí
 Ejercicio 4		Todo	Sí

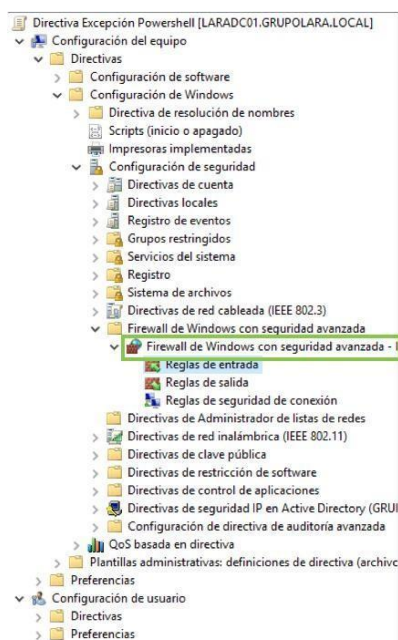


Ilustración 15. Árbol de directorios para el editor de la GPO creada

- Una vez definidas las políticas, debemos forzar su actualización en el controlador de dominio desde la consola de comandos (**cmd**) con el comando **gpupdate /Force**.

```
C:\Users\admin_jcrojo>gpupdate /Force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.
```

Ilustración 16. Actualización expresa de las GPO

- Una vez aplicado en el controlador, debemos forzar la actualización de directivas de grupo para todos los demás equipos del dominio. Para ello, desde el Administrador de directivas de grupo, seleccionamos la unidad organizativa (OU) sobre la que queremos actualizar las políticas y hacemos click derecho, **Actualización de directiva de grupo...**

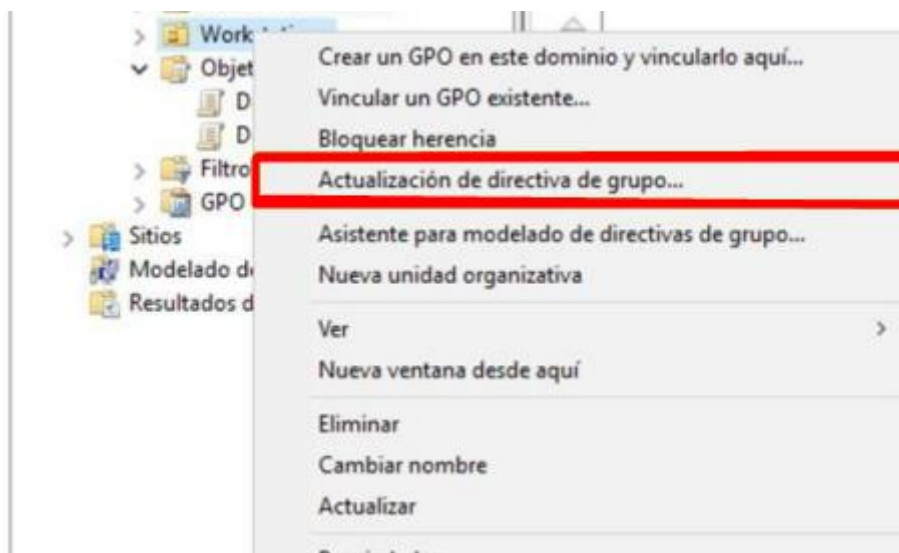
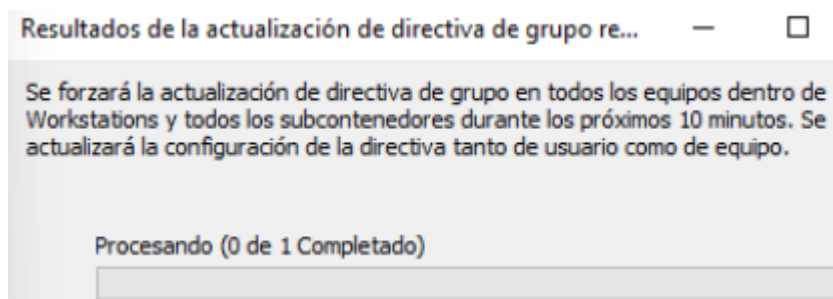
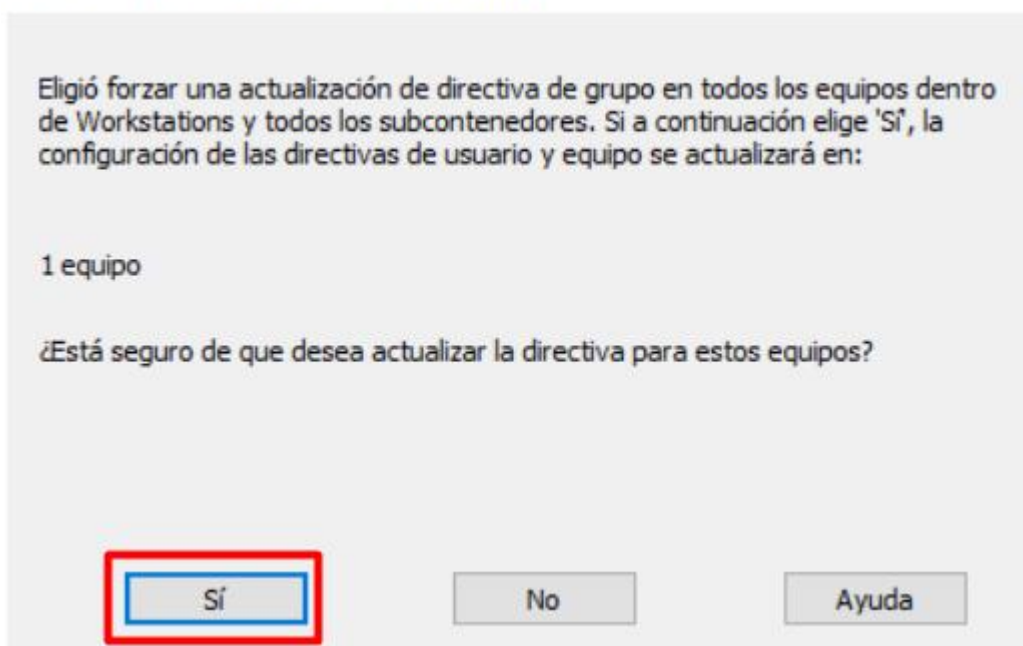


Ilustración 17. Forzar actualización de las directivas de grupo para una OU completa

Forzar actualización de directiva de grupo



- Para comprobar que se ha aplicado correctamente, vamos al workstation con Windows 10 y entramos en **Windows Defender Firewall con seguridad avanzada**. Se puede observar que se muestra un mensaje indicando que ciertas configuraciones del equipo son controladas desde una directiva de grupo.

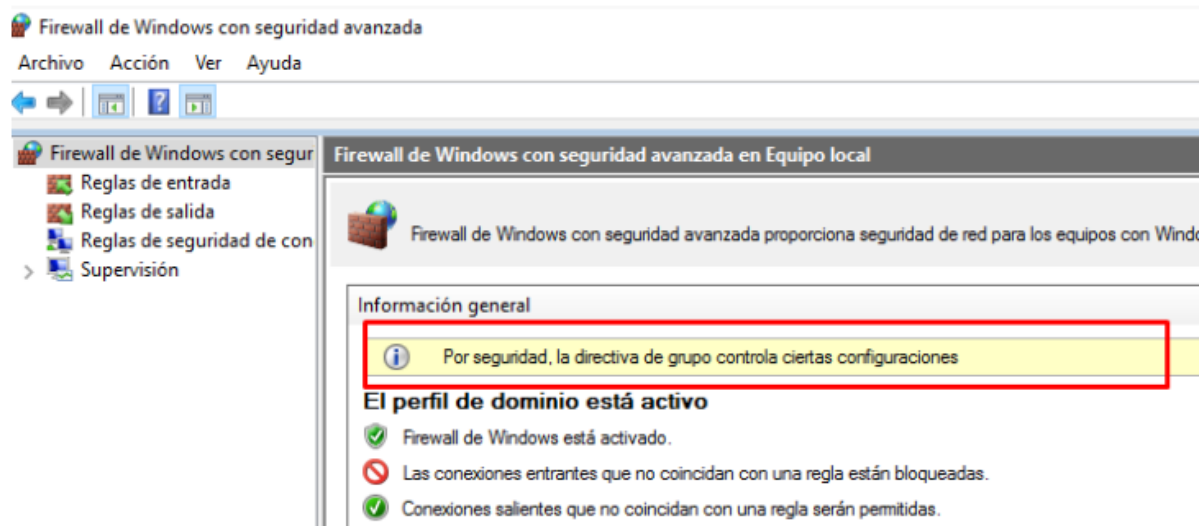


Ilustración 18. Herramienta del Firewall de un workstation conectado al dominio

- Si seleccionamos Reglas de entrada/Reglas de salida, observaremos que aparecen las reglas que se han definido desde el controlador del dominio. Adicionalmente, si hacemos doble click sobre ellas para abrir las propiedades, nos mostrará un mensaje de que la regla la aplicó el administrador del sistema y no podemos modificarla, ni siquiera con un usuario administrador.

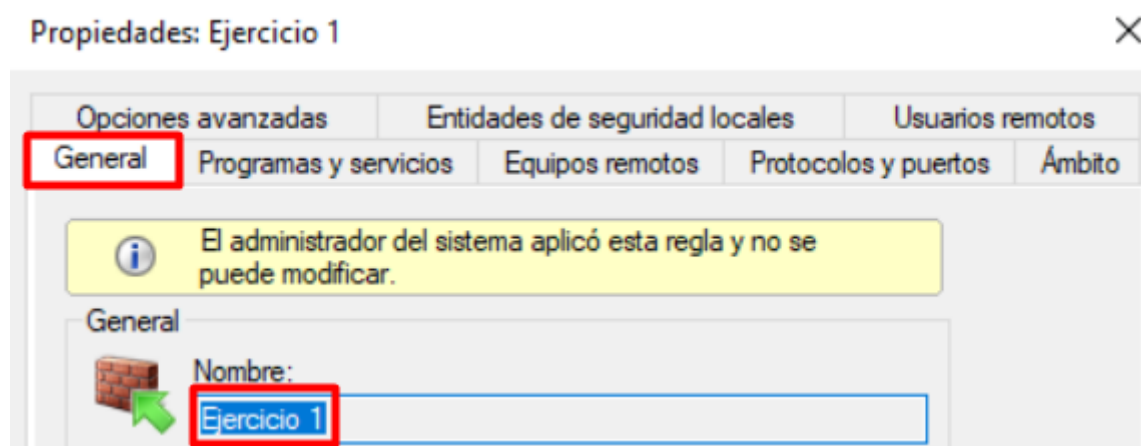
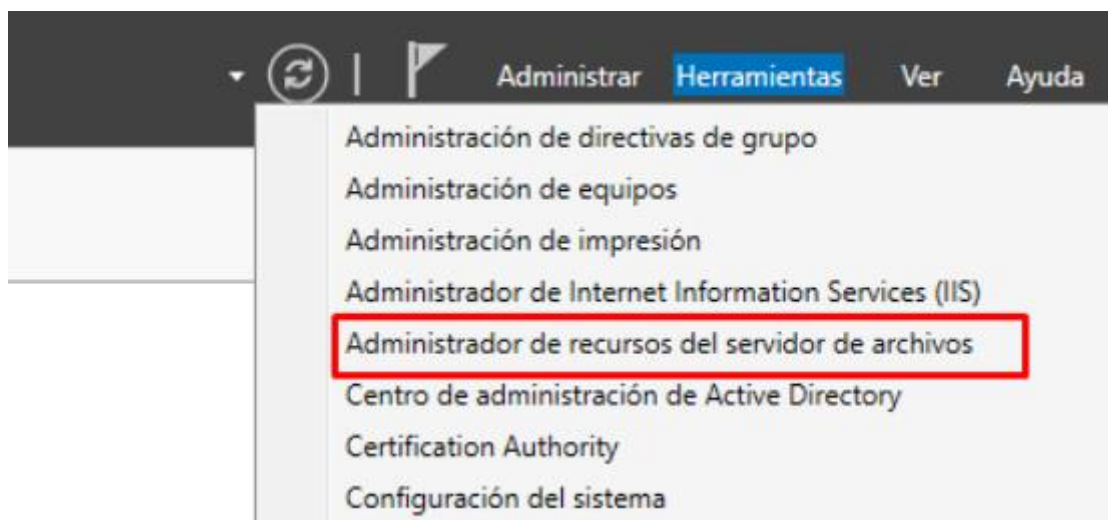


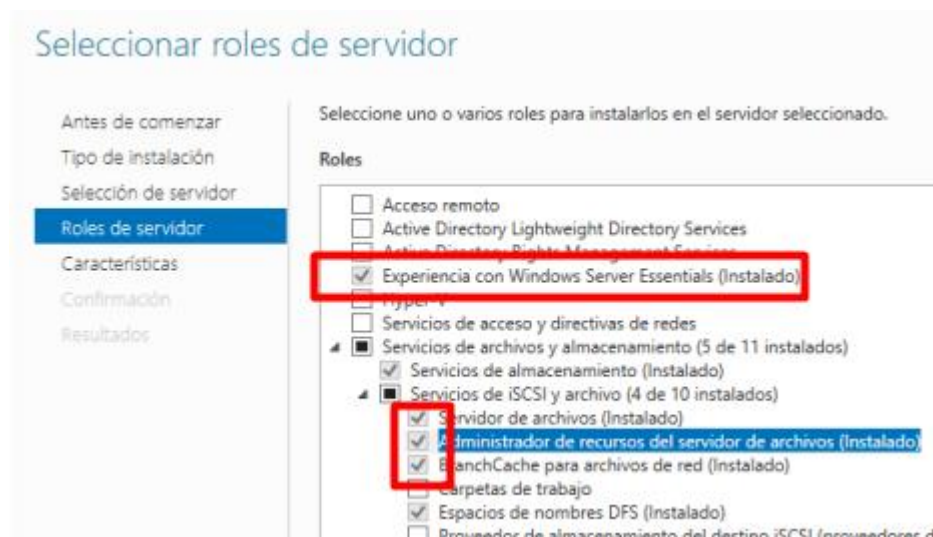
Ilustración 19. Imposibilidad de modificar una regla del firewall aplicada mediante GPO desde el controlador de dominio

4.7. Instala y configura el rol FSRM en Windows Server 2016 para crear un filtro de archivos que permita mitigar el riesgo de infección por ransomware.

- Entre las opciones disponibles a habilitar en nuestro servidor, existe una opción denominada **Administrador de recursos del servidor de archivos** (*File Server Resources Manager*, con siglas FSRM) que nos permite crear restricciones de creación de archivos dependiendo del nombre o de la extensión de los mismos.



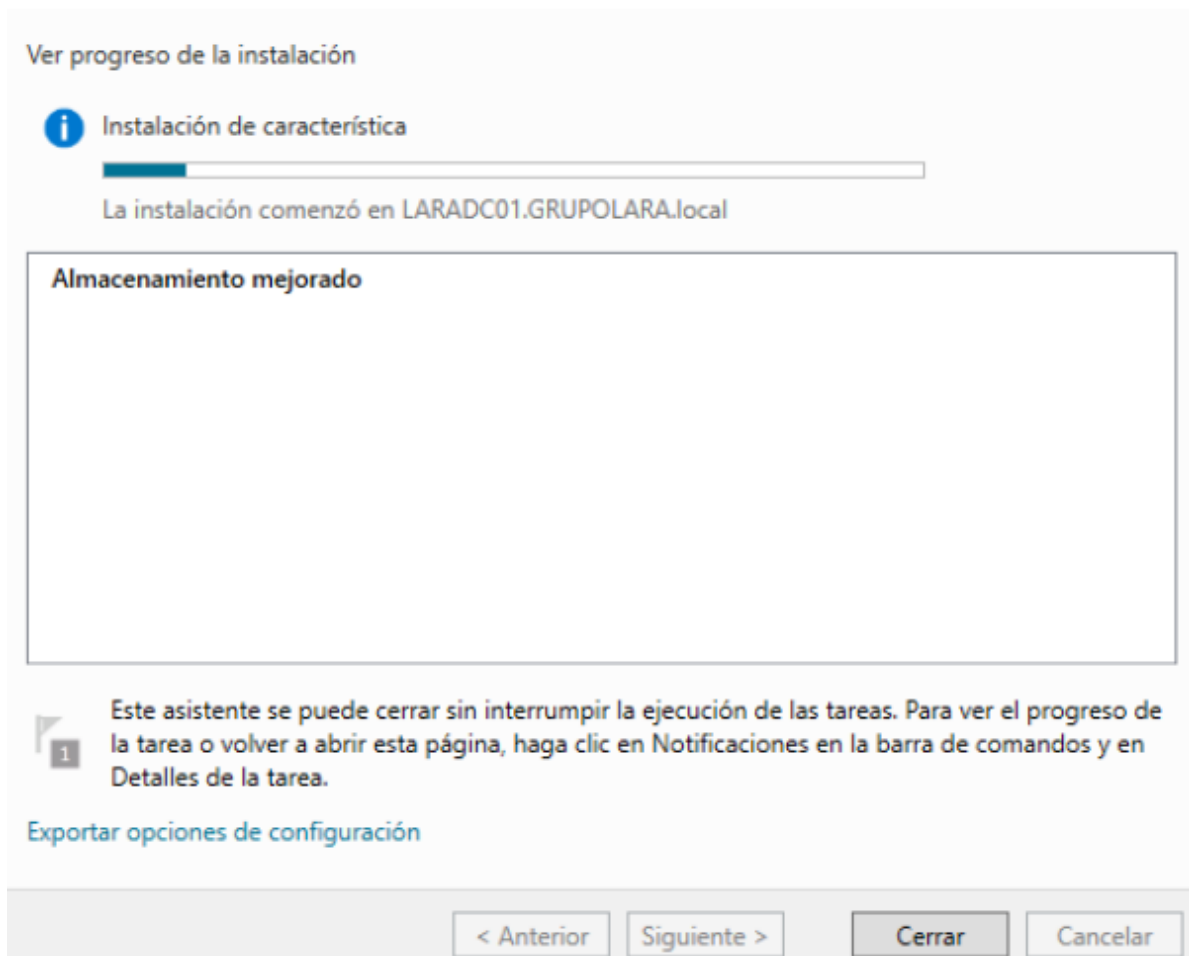
- Tal y como opera el *ransomware*, cifrando los archivos y posteriormente añadiéndoles la extensión correspondiente a la versión de *ransomware* que se haya desplegado, es posible bloquear esta actuación mediante la creación de un filtro de archivos (*File Screen* en inglés). De esta forma, en caso de intentar cifrar los archivos alojados en el servidor, el filtro definido que bloquea la creación de ficheros con ciertas extensiones impide que se complete la acción, manteniendo los ficheros en su estado original y no viéndose encriptados.
- Para habilitar esta opción, primero debemos instalarla en el servidor. Desde el Administrador del servidor, seleccionamos arriba a la derecha la opción **Administrar > Agregar roles y características**, y seleccionamos **Siguiente** durante los tres primeros pasos del asistente, dejando marcadas las opciones que se muestran por defecto.
- Una vez hemos llegado a la opción de selección Roles del servidor, buscamos en el listado que se muestra la categoría **Servicios de archivos y almacenamiento > Servicios de iSCSI y archivo > Administrador de recursos del servidor de archivos**.



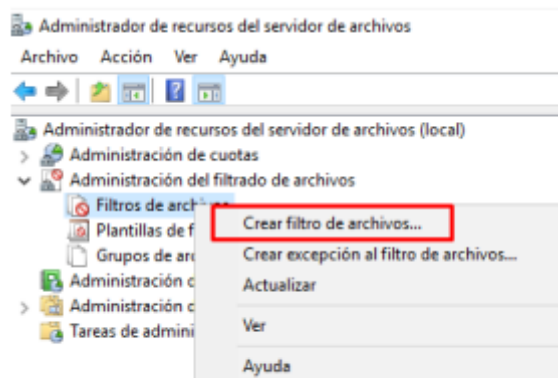
- Se mostrarán automáticamente una serie de características asociadas a la activación de este rol, aceptamos y seleccionamos **Siguiente**.
- En la ventana de Características, seleccionamos directamente **Siguiente** sin necesidad de activar características adicionales a las ya presentadas en el paso

anterior.

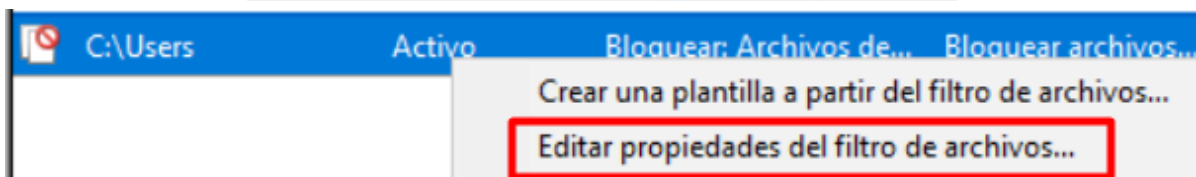
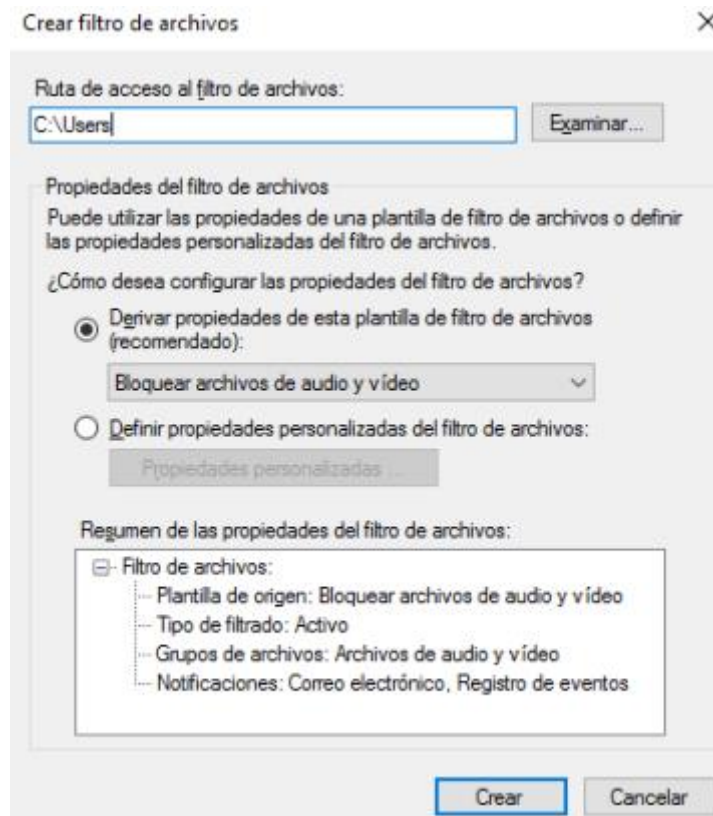
- Seleccionamos **Instalar** y esperamos a que el asistente de instalación se haya completado, y reiniciamos el servidor.



- Una vez reiniciado, abrimos el **Administrador del servidor > Herramientas > Administrador de recursos del servidor de archivos**.
- En el árbol de directorios de la izquierda, desplegamos la **opción Administración de filtrado de archivos**.
- Hacemos click derecho sobre la opción **Filtro de archivos > Crear filtro de archivos...**



- Como **ruta de acceso** a la que aplicar el filtro, indicaremos **C:\Users**.



- En caso de indicarse la ruta raíz C:\, Windows no nos permitirá en los pasos siguientes aplicar un Filtrado activo, que es el más restrictivo para evitar la creación de ficheros con extensiones de ransomware, ya que hay subdirectorios en C:\ necesarios para Windows y de esta forma, se evita que podamos bloquear por error la creación de algún fichero necesario para el sistema.
- Adicionalmente, en caso de querer aplicar asimismo un filtro para los datos almacenados en discos duros externos conectados al servidor (como por ejemplo puede ser un servidor de ficheros con discos RAID montados en unidades D:\, E:\, etc), deberemos crear un filtro de archivos por cada unidad lógica que queramos proteger, indicando en la ruta directamente la raíz de dicha unidad.
- Seleccionamos la opción **Definir propiedades personalizadas del filtro de archivos** y seleccionamos el botón **Propiedades personalizadas...**
- En la ventana que se nos abra, seleccionaremos como tipo de filtrado el **Filtrado activo**.
- En el listado que se muestra para seleccionar el grupo de archivos que deseemos bloquear, debemos crear un nuevo grupo de archivos en el botón de la derecha que indica **Crear...**
- En la nueva ventana que se nos abra, indicaremos como nombre del grupo

Extensiones de ransomware, e incluiremos en el listado Archivos incluidos todas las extensiones que queramos bloquear (por ejemplo, *.ryk).

- Es importante indicar el asterisco (*) delante para que el filtro se aplique a cualquier fichero que intente modificar su extensión a las que añadamos.

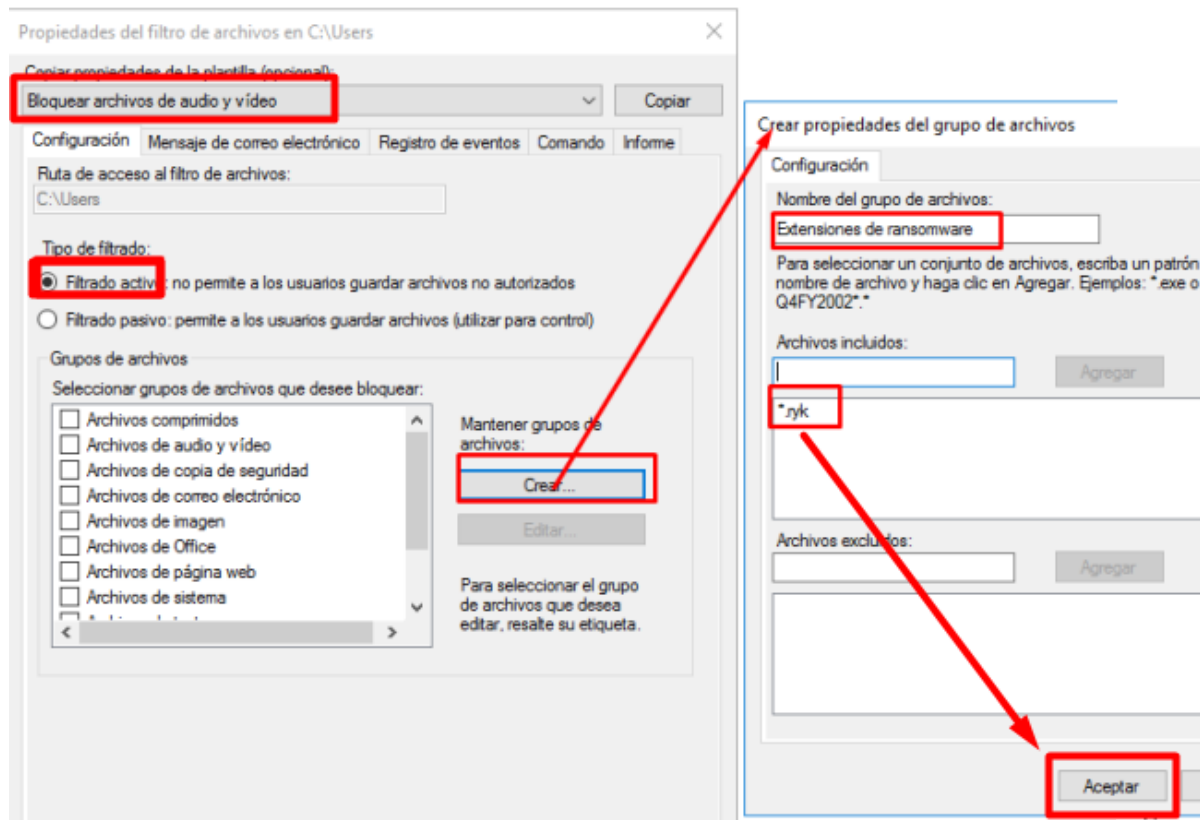


Ilustración 20. Creación de un grupo de archivos específico con las extensiones de ransomware

- Seleccionamos **Aceptar**, y en la ventana anterior seleccionamos también **Aceptar** para finalizar la creación de nuestro filtro de archivos.

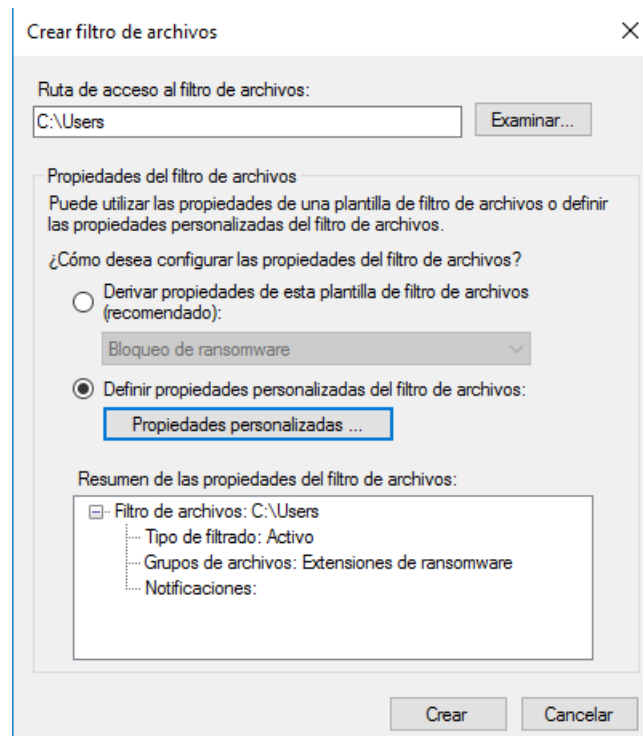


Ilustración 21. Creación de un filtro de archivos frente a ransomware para la ruta C:\Users

- Se nos mostrará entonces una ventana solicitando si queremos crear una plantilla a partir del filtro de archivos definidos, seleccionamos que sí la queremos guardar y la llamamos **Bloqueo de ransomware**.
 - La ventaja de guardar el filtro creado como plantilla es que nos permitirá posteriormente crear filtros para otras unidades lógicas de almacenamiento de archivos que puedan estar conectadas a nuestro servidor de forma más ágil.

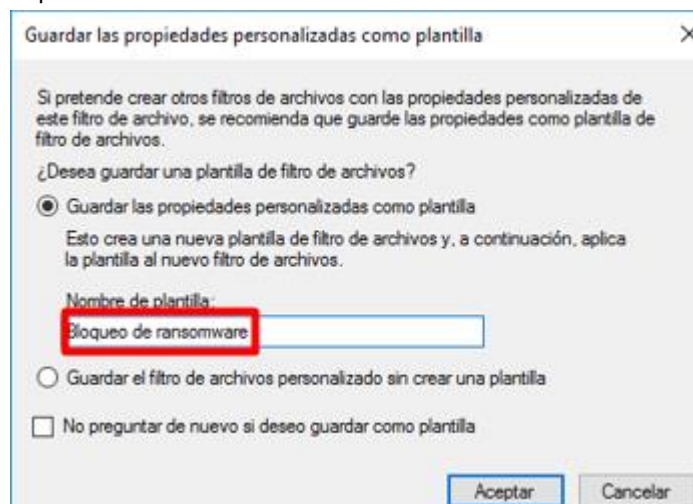


Ilustración 22. Creación de una plantilla de filtro de archivos a partir de nuestro filtro

- Una vez completado, podremos observar que aparece nuestro filtro activo, bloqueando las extensiones de *ransomware* que hayamos incluido.
 - Como hemos comentado con anterioridad, es importante destacar que en caso de tratar de crear un filtro de tipo Filtrado activo para la ruta raíz C:\, en el momento de finalizar el asistente de configuración del filtro, aparecerá por defecto y automáticamente como Filtrado pasivo, no siendo posible forzarlo a activo por existir archivos necesarios para el sistema en subdirectorios de Windows que podrías bloquear por error en caso de definir un filtro de archivos incorrectamente.

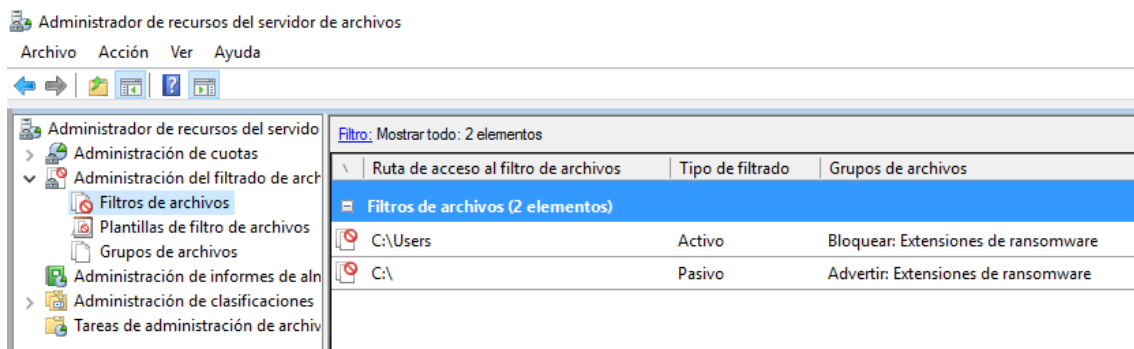
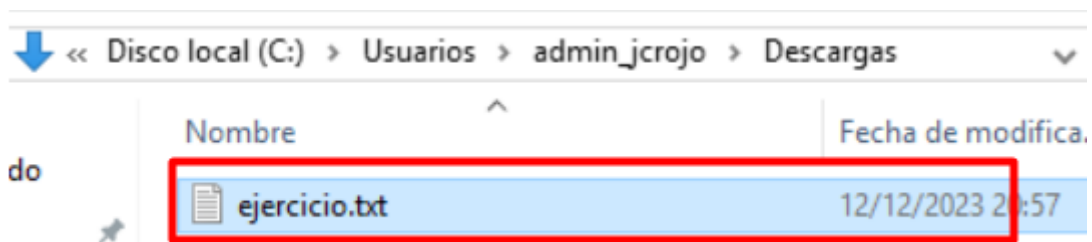


Ilustración 23. Listado de filtros de archivos existentes en el FSRM

- Prueba de concepto: para confirmar que efectivamente nuestro filtro funciona según lo esperado, vamos a tratar de renombrar un fichero a la extensión .ryk
 - Para ello, primero creamos un archivo de texto en la ruta **C:\Users\admin_jcrojo\Downloads** que llamaremos **prueba.txt**



- En caso de no encontrarse habilitado, desde el **Explorador de archivos > Vista**, marcaremos la casilla **Extensiones de nombre de archivos** para poder visualizar y modificar expresamente las extensiones de los ficheros.
- Haciendo click derecho sobre este fichero, **Renombrar**, cambiaremos la extensión **txt** por **ryk**.

- Nos solicitará confirmación expresa para proceder a cambiar la extensión, advirtiéndonos de que es posible que el archivo quede inaccesible si lo hacemos, y seleccionamos Aceptar.
- En este punto debido a que nuestro filtro se encuentra correctamente configurado, nos mostrará una ventana indicando que necesitamos permisos expresos de administrador para proceder a modificar esa extensión concreta.

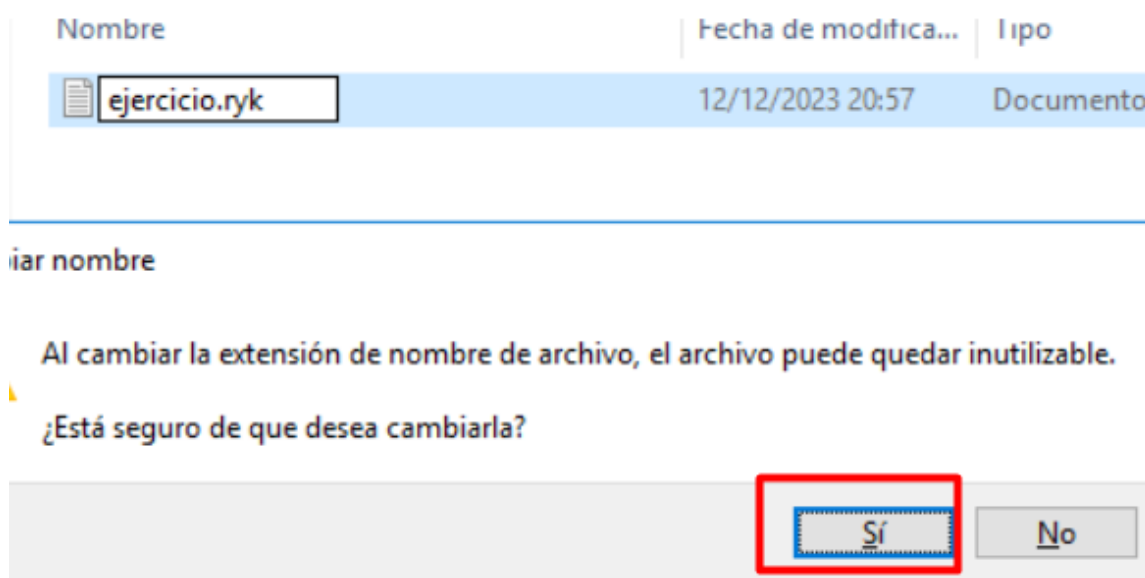


Ilustración 24. Solicitud de permisos de administrador para modificar la extensión del archivo

- Seleccionamos **Continuar**, y observaremos como, a pesar de tener la sesión iniciada con la cuenta de admin_jcrojo, que tiene privilegios de administrador del dominio, el filtro de archivos definido impide que podamos modificar la extensión del archivo y lo revierte a su estado anterior, bloqueando de esta forma una potencial infección por *ransomware*.

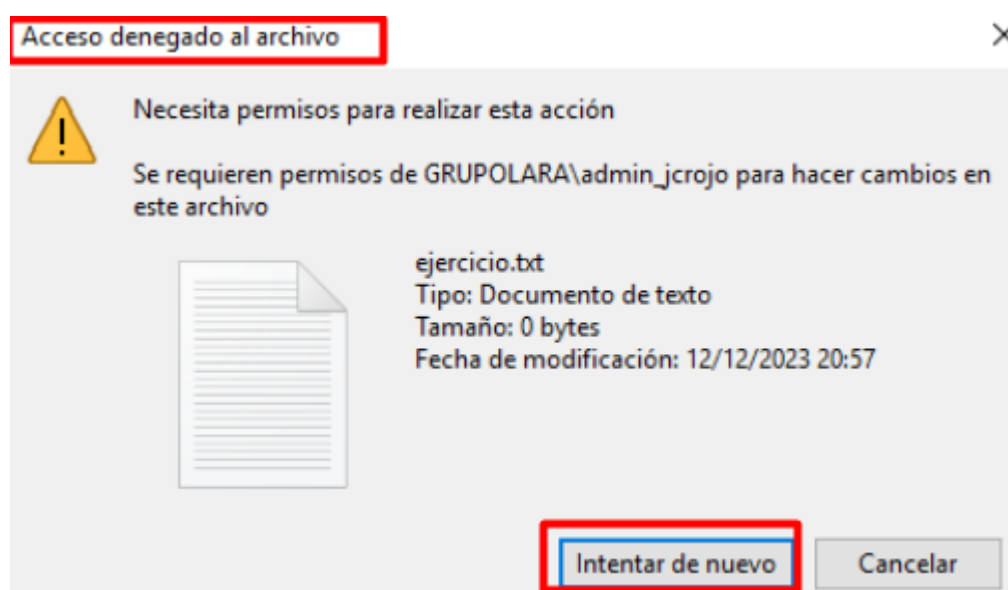


Ilustración 25. Imposibilidad de modificar la extensión a .ryk incluso con permisos de administrador

Anexos

Listado de usuarios y equipos del dominio GRUPOLARA

Para alguno de los ejercicios que hemos visto con anterioridad, será necesario modificar la contraseña de algunos usuarios en función del grupo al que pertenecen y las políticas que definamos.

Para facilitar el seguimiento de las credenciales que puedan verse modificadas, a continuación, se incluye un listado unificado de las contraseñas definidas para todos los usuarios con los que se trabajará, incluyendo una columna a la derecha de la tabla para marcar aquellos que se vean modificados y cuya contraseña en uso pase a ser la de la segunda columna.

Nombre de usuario	Contraseña original	Nueva contraseña
Administrador	123Abc..	qwerty123.
admin_jcrojo	P@ssw0rd	P@ssw0rd2
admin_mjperez	almeria81!	almeria81@

Asimismo, también se incluye a continuación la relación de usuarios del dominio y grupos a los que pertenecen, para ayudar a identificar de forma ágil con cuáles de ellos se puede verificar la correcta implementación de las políticas que se definan durante la realización de los ejercicios.

Nombre de usuario	Grupos a los que pertenece
Administrador	Usuarios del dominio, Admins. del dominio
admin_jcrojo	Usuarios del dominio, Admins. del dominio
admin_mjperez	Usuarios del dominio, Administradores de empresas