



# Configuración del Firewall de Windows y Windows Defender

Alfredo Abad

ISO-04-042-ConfigRedFirewallWIN.pptx

17-oct-2023

1  
Alfredo Abad



## Historia del firewall

- En Windows 2000 y XP el Firewall era muy rudimentario, con funcionalidades básicas de apertura y cierre de puertos, así como de unas pocas excepciones configuradas por defecto (escritorio remoto, compartición de impresoras, etc.)
  - Sin embargo, desde Windows Vista disponemos de un Firewall avanzado (más parecido a los firewall físicos)
- El nuevo cortafuegos de Windows dispone de la posibilidad de bloquear tanto conexiones entrantes como salientes
  - Algo muy necesario en la lucha contra los malware de tipo bot o troyanos reversos, que se conectan a un Panel de Control remoto (generalmente web)
- Actualmente, Windows ha integrado su firewall en Windows Defender

2  
Alfredo Abad



# Cómo Configurar Firewall Windows 11

3

Alfredo Abad



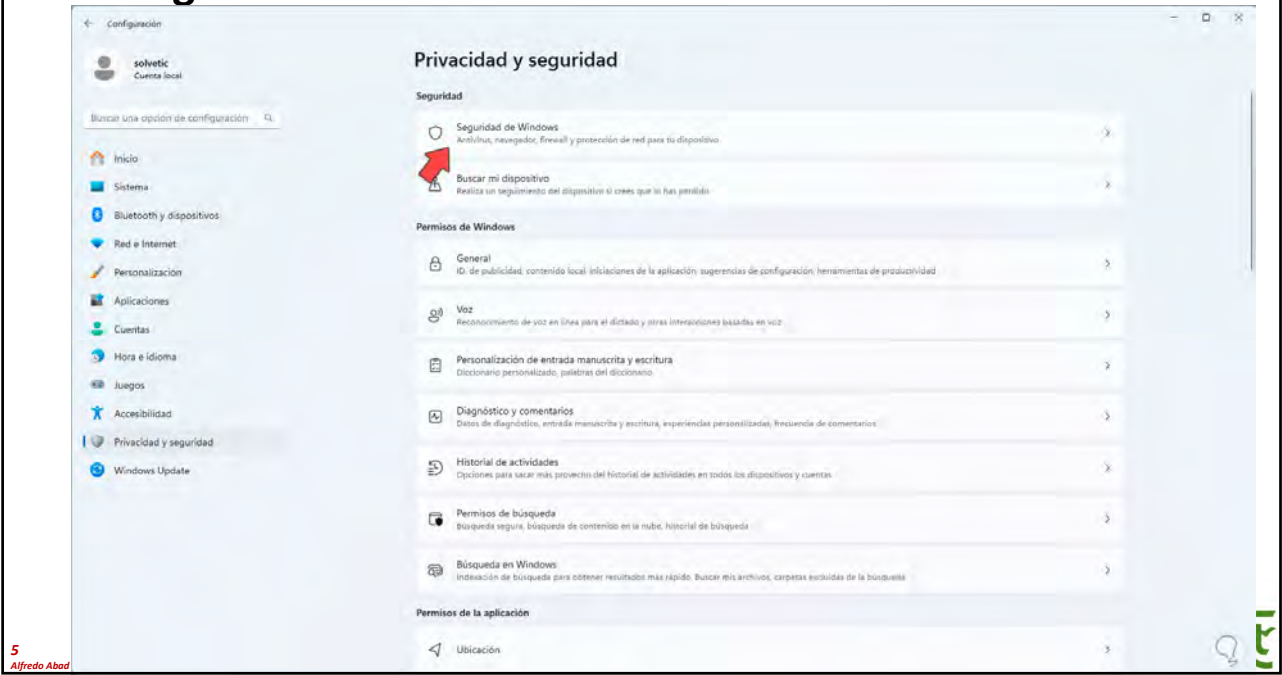
- Uno de los elementos que cuenta con un impacto mas relevante en Windows 11 es el Firewall, recordemos que este Firewall se encarga de proteger el equipo de todos los paquetes y datos de red tanto entrantes como salientes, es ideal para que no se camuflen amenazas como troyanos o malware y aplicaciones que pueden contener en su interior código malicioso.
- El Firewall de Windows 11 trabaja en las redes que están disponibles en el sistema las cuales son:
  - **Red privada:** es una red segura y es ideal para usar en nuestro hogar u oficina, esta red puede ser administrada por el usuario, con esto, Windows hará que todos los dispositivos que estén conectados a la red puedan conectarse entre sí.
  - **Red pública:** implica una mayor seguridad ya que el usuario no tiene el control total de la configuración, esta red se encarga de desactivar las opciones de visibilidad de nuestro dispositivo en de la red, con ello, no todos los periféricos serán visibles desde la parte externa.
  - **Red de dominio:** como su nombre lo indica, es una red que se usa dentro de un dominio, puede ser Windows Server o sistemas Linux.

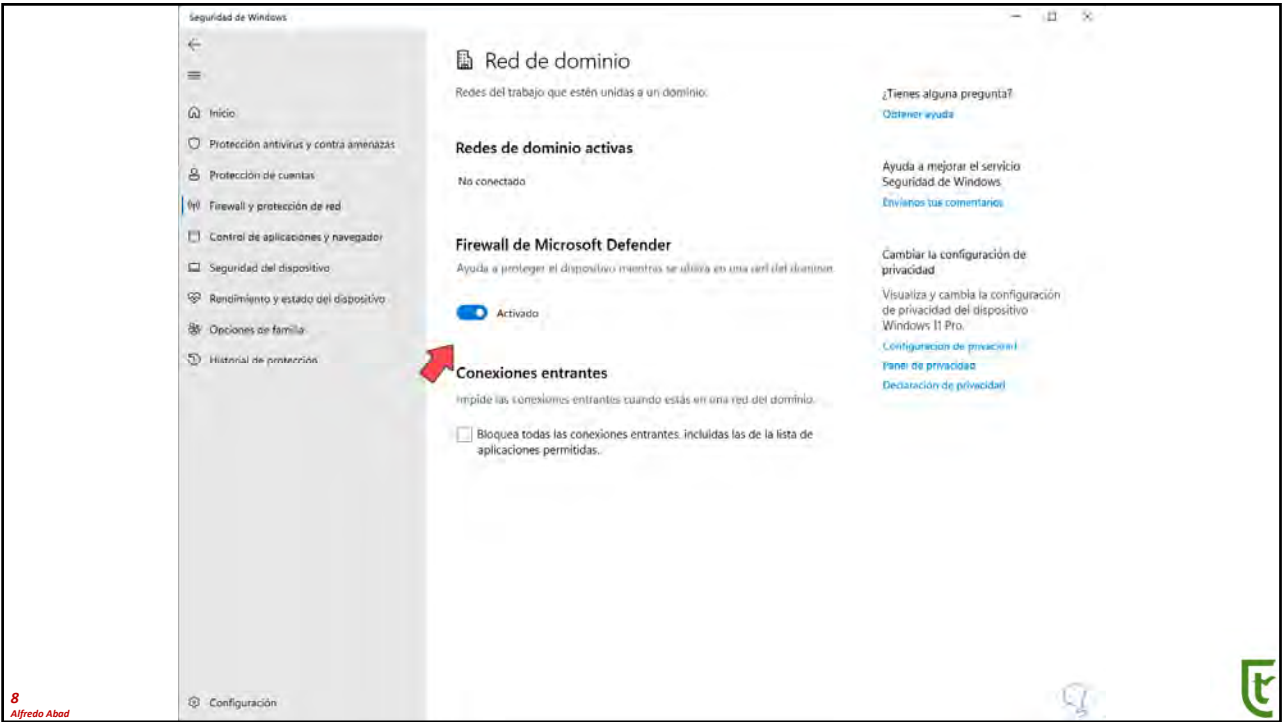
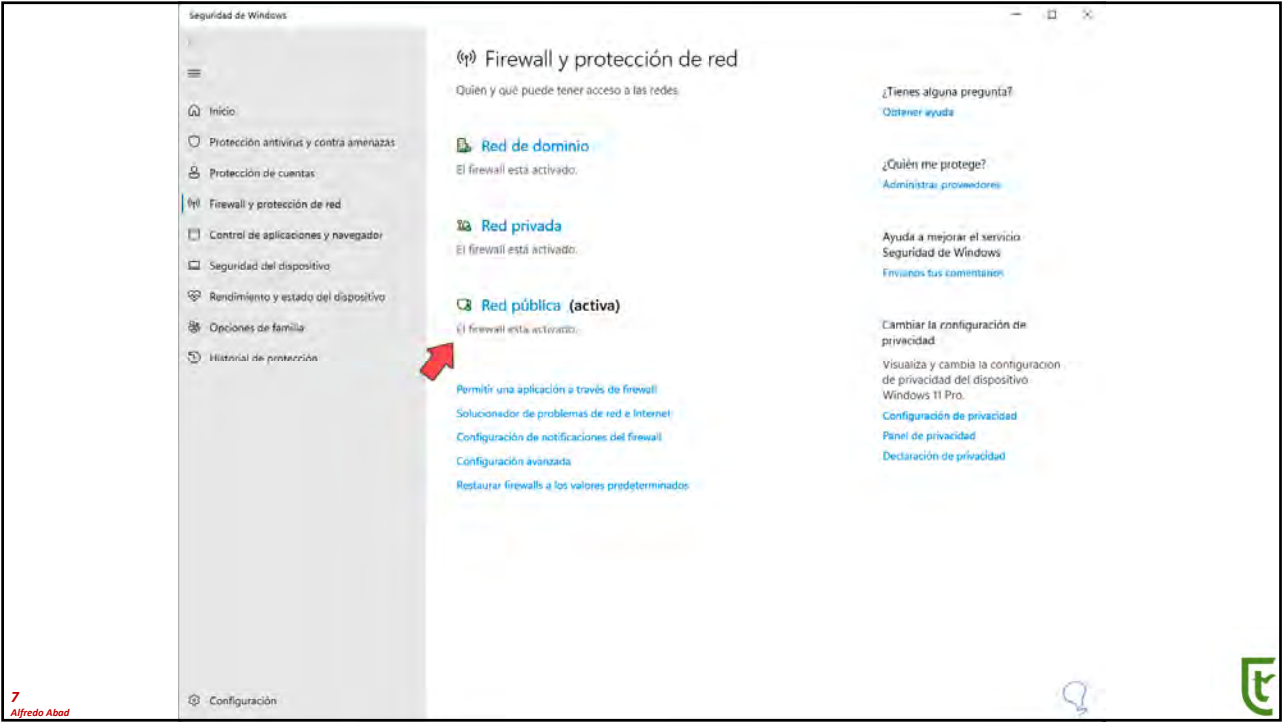
4

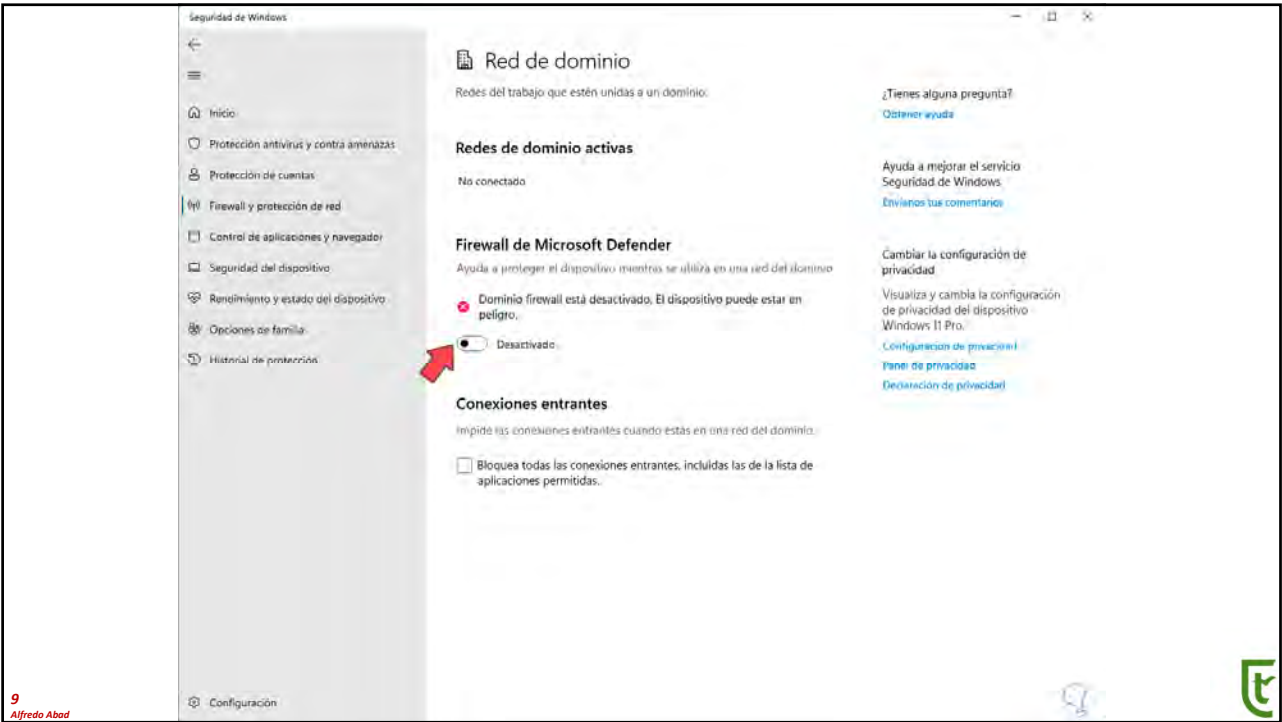
Alfredo Abad



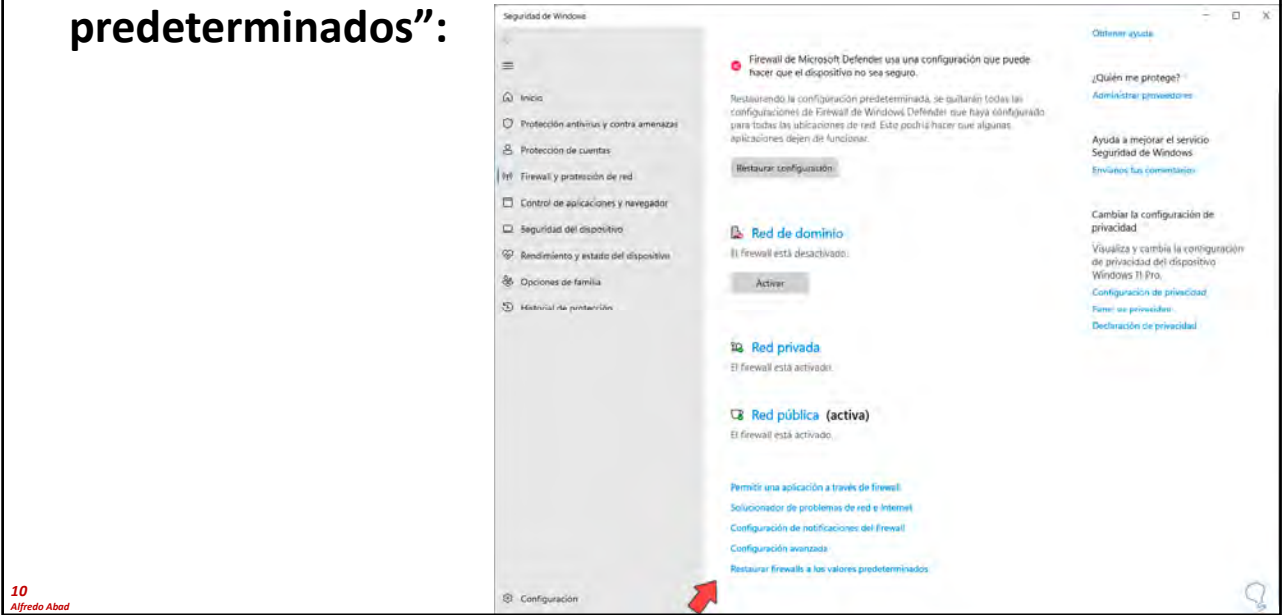
## Configurar Firewall Windows 11 habilitar o desabilitar

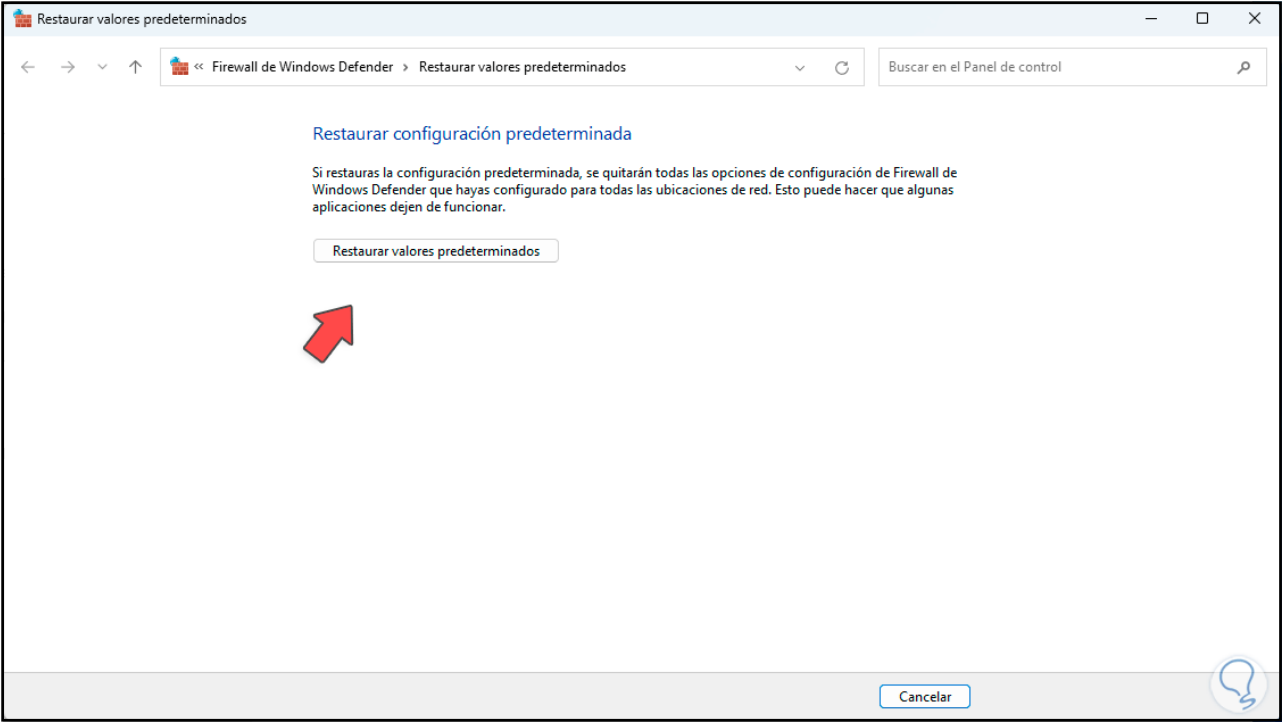






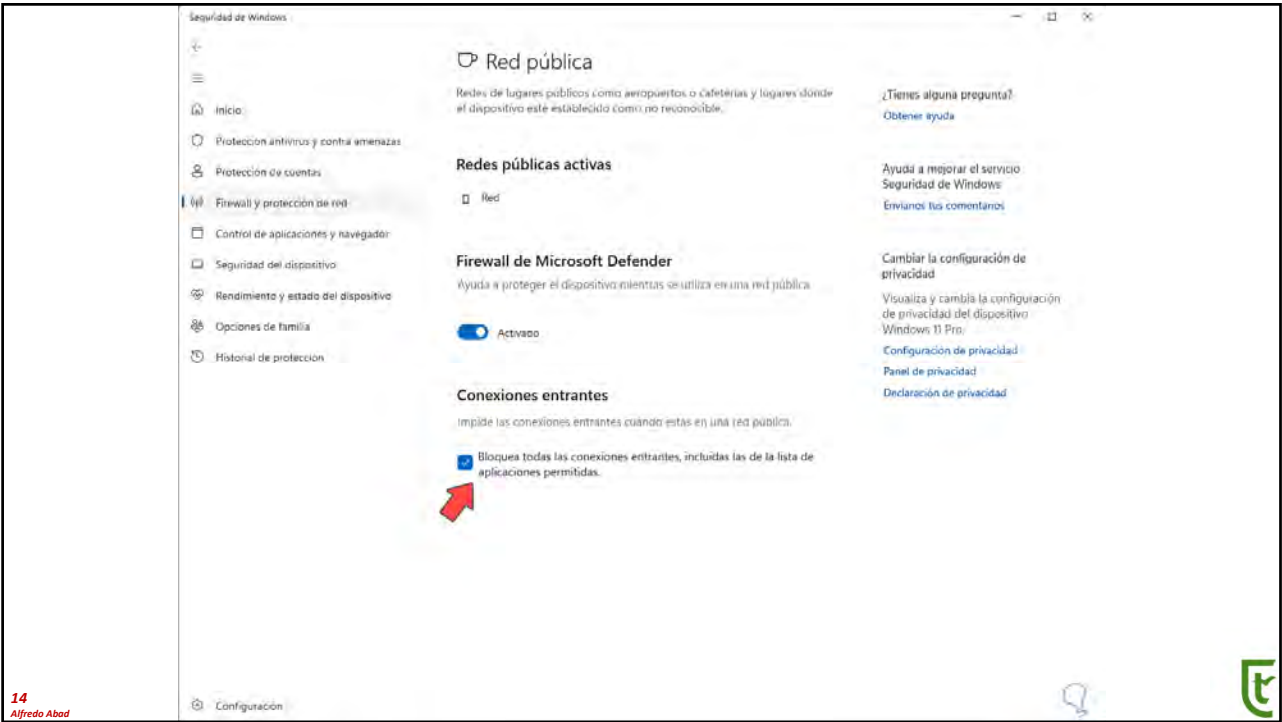
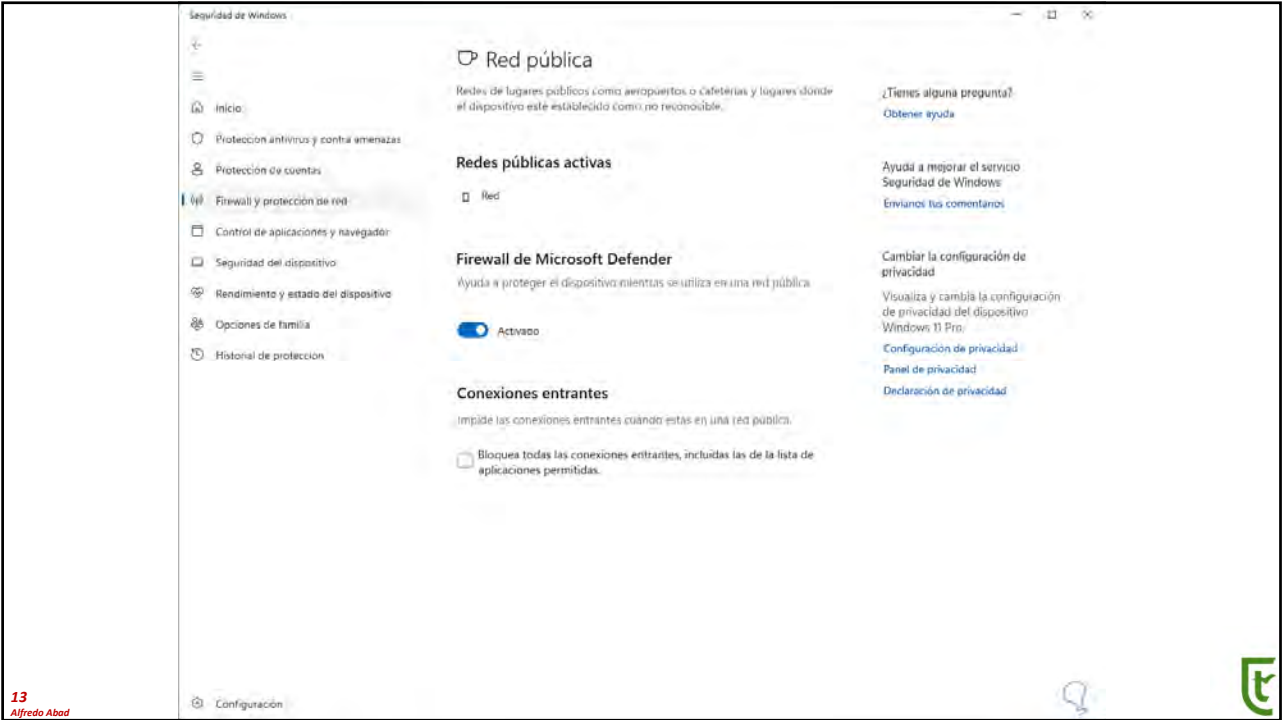
Para revertir algún cambio, en el menú principal damos clic en “Restaurar firewalls a los valores predeterminados”:



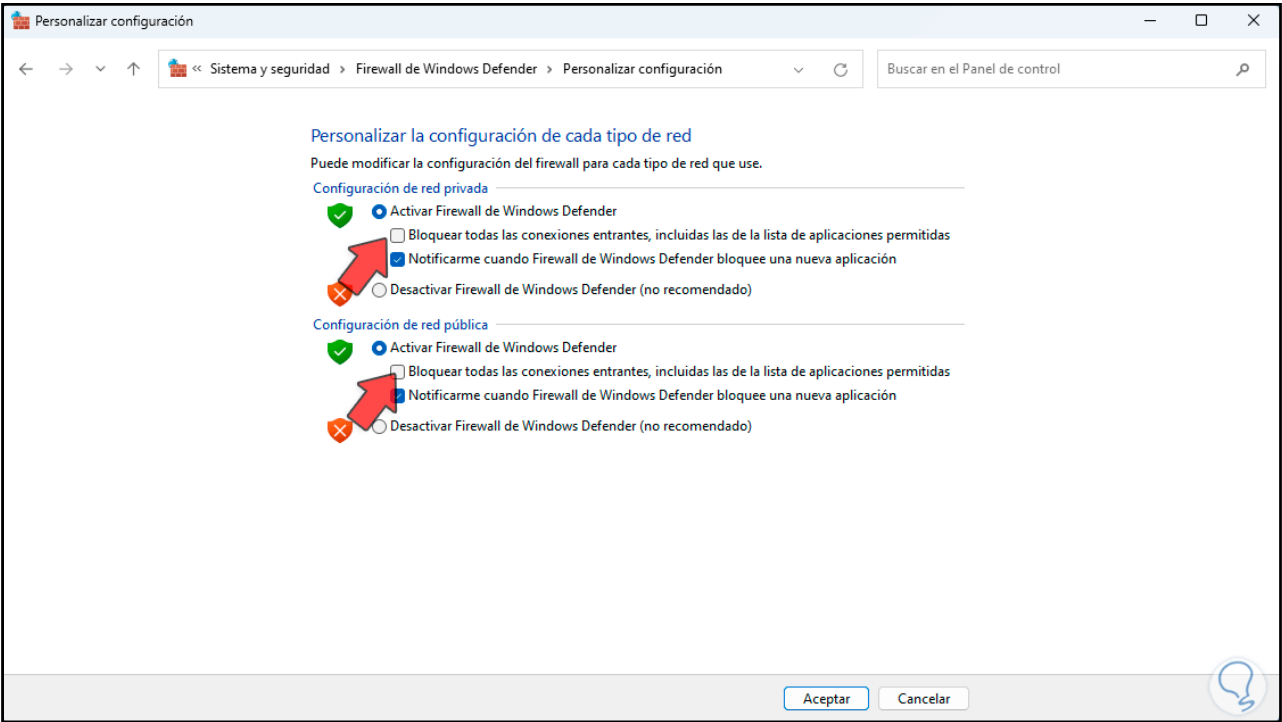
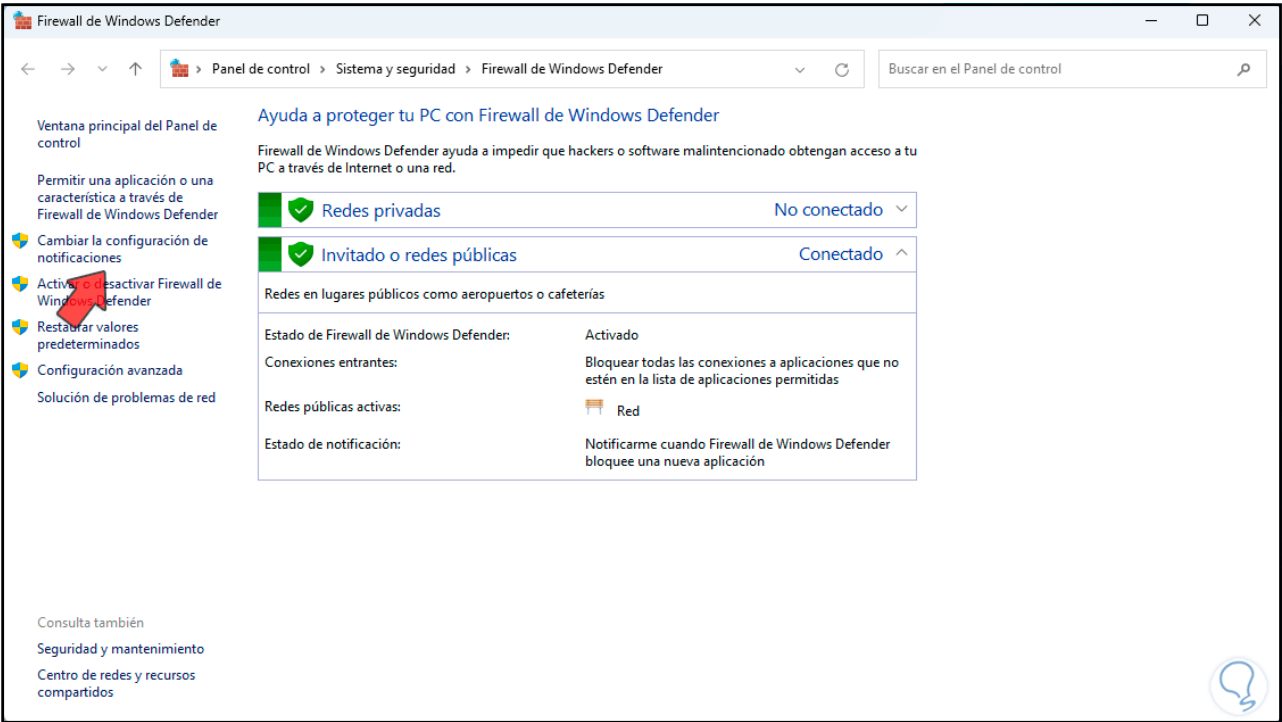


## Configurar Firewall Windows 11 activando la protección

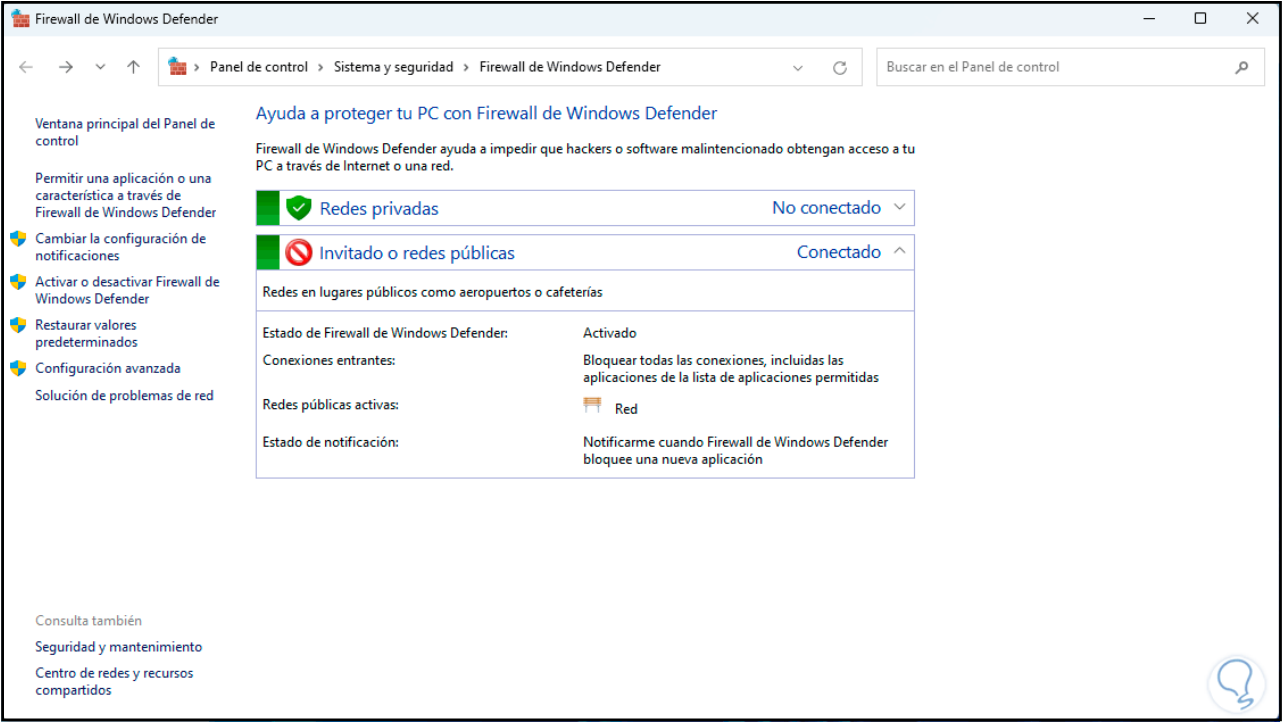
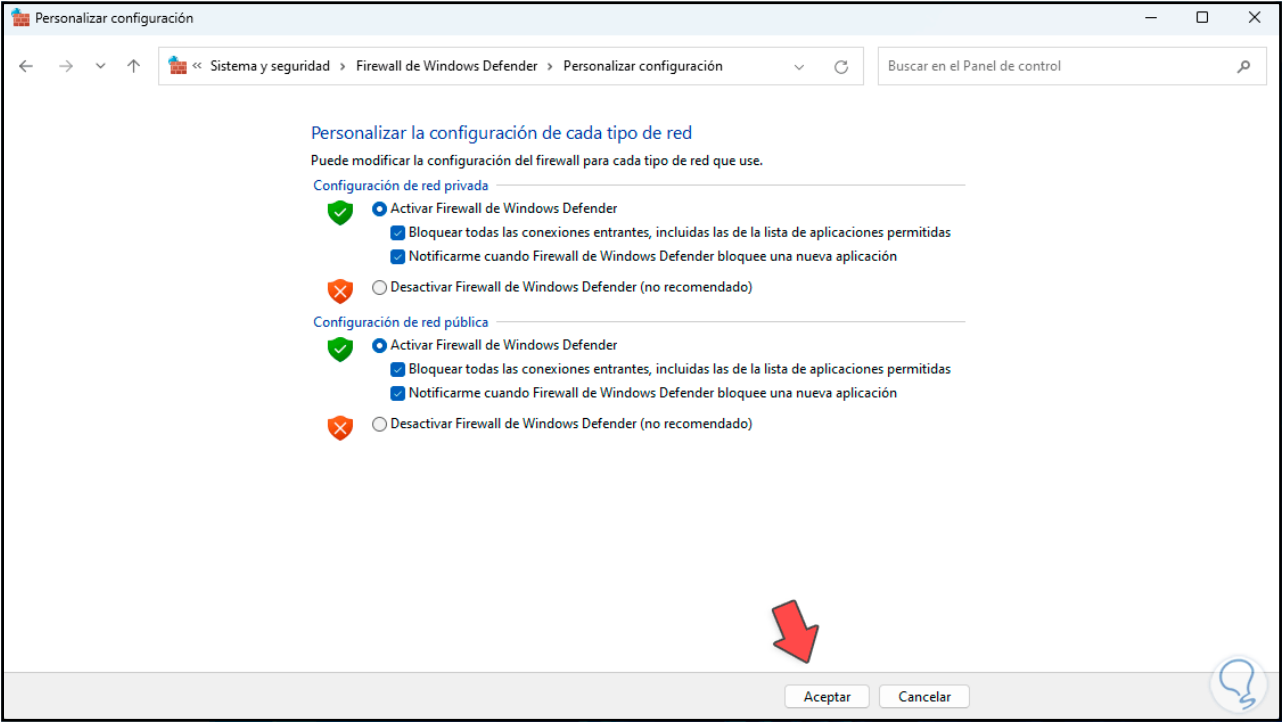




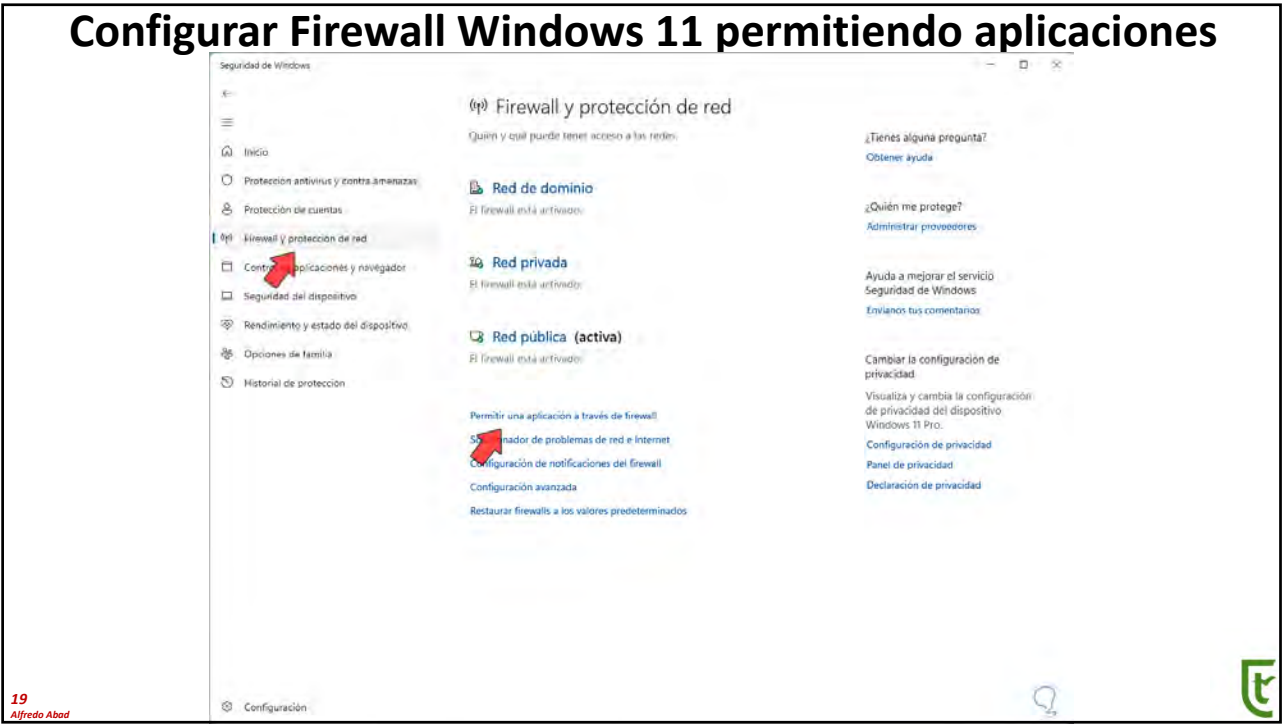




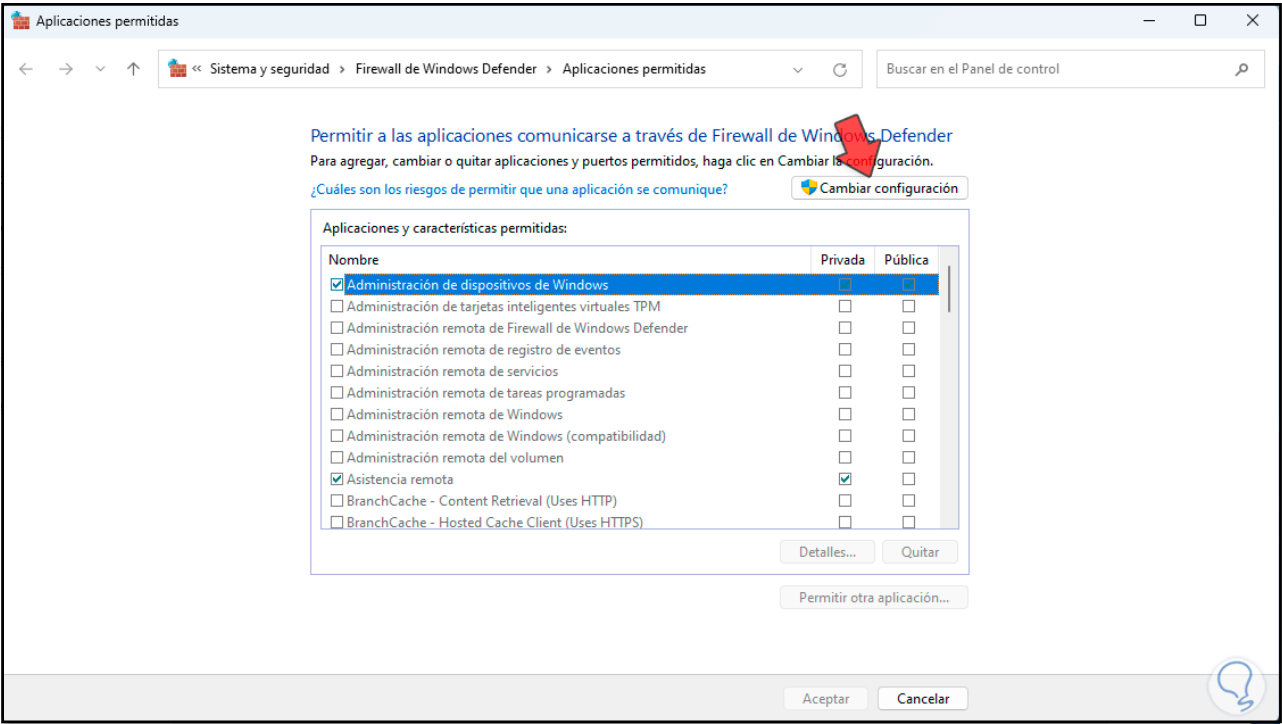


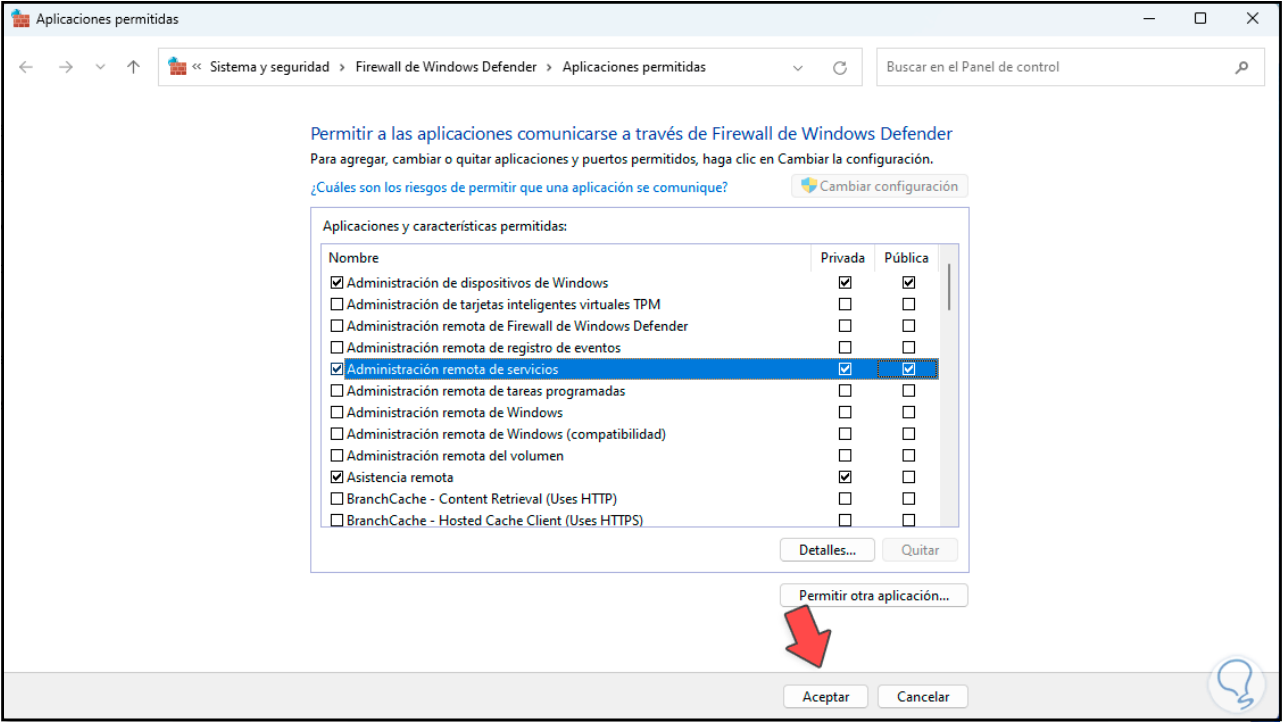
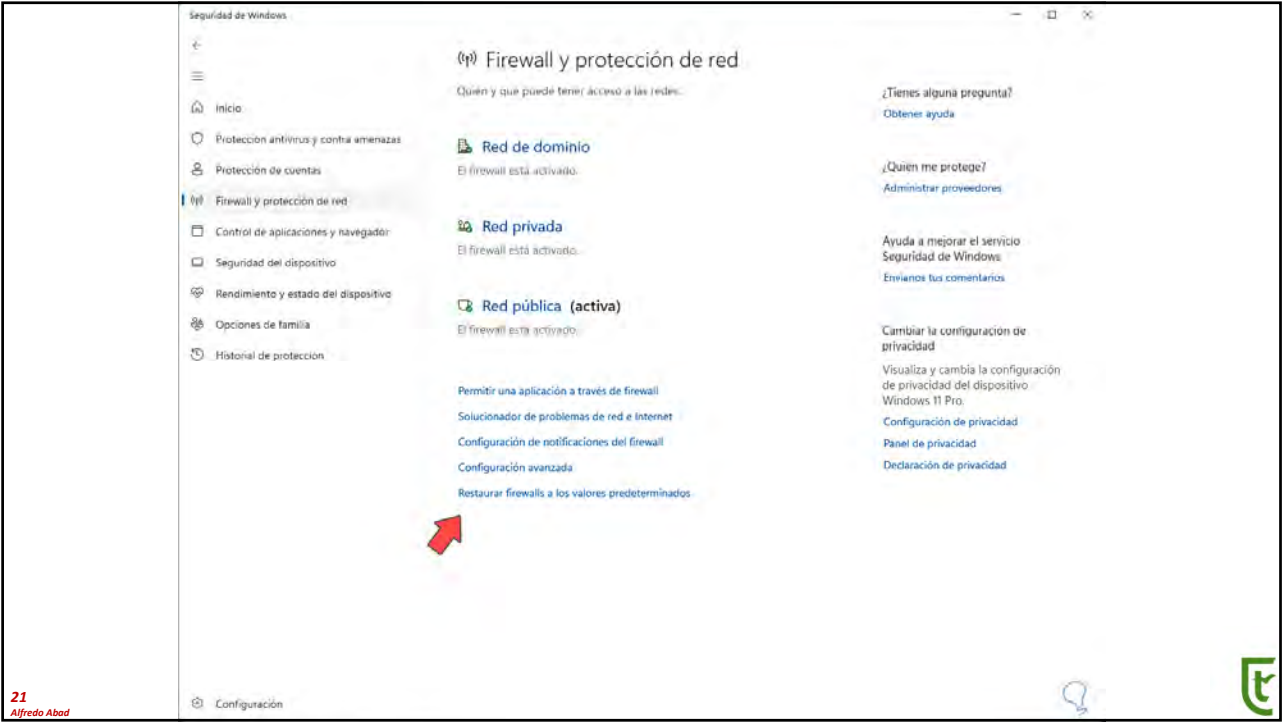


# Configurar Firewall Windows 11 permitiendo aplicaciones



19  
Alfredo Abad

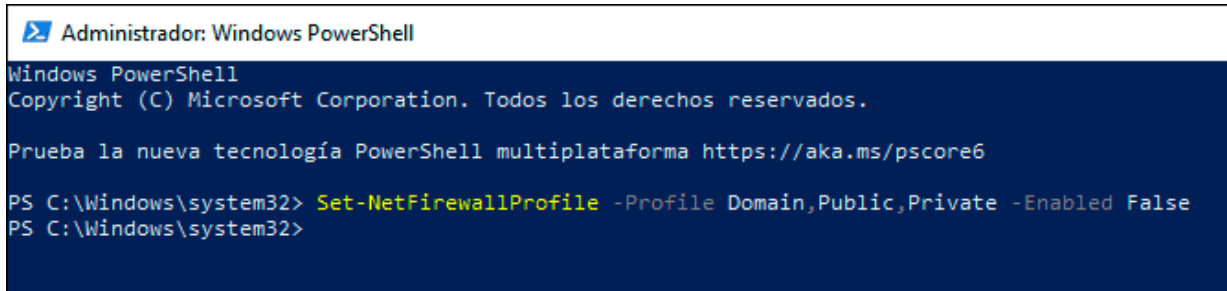




## Activar/desactivar firewall desde PowerShell:

**Desactivar:** Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False

**Activar:** Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True



```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
PS C:\Windows\system32>
```

23

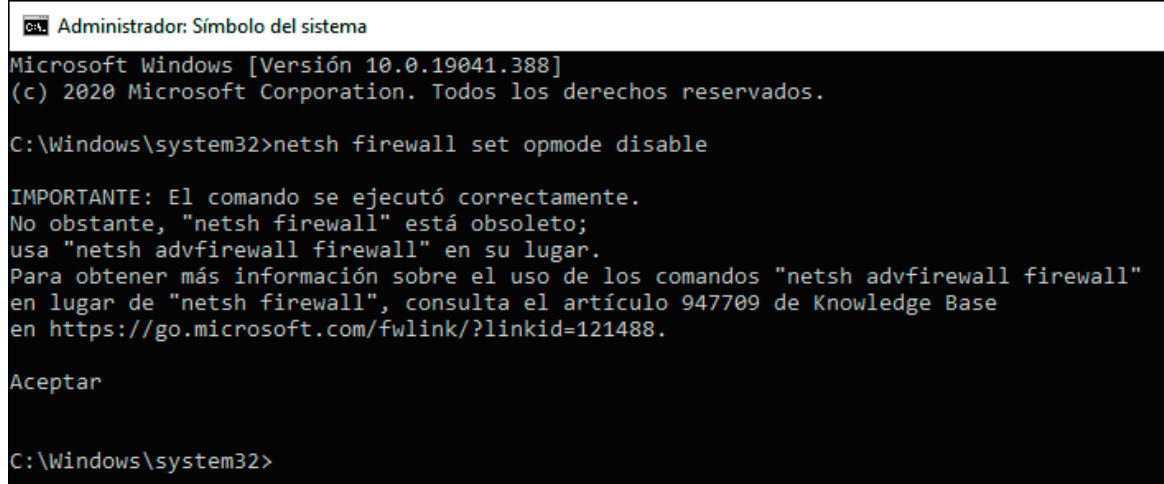
Alfredo Abad



## Desde CMD:

**Desactivar:** netsh firewall set opmode disable

**Activar:** netsh firewall set opmode enable



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19041.388]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>netsh firewall set opmode disable

IMPORTANTE: El comando se ejecutó correctamente.
No obstante, "netsh firewall" está obsoleto;
usa "netsh advfirewall firewall" en su lugar.
Para obtener más información sobre el uso de los comandos "netsh advfirewall firewall"
en lugar de "netsh firewall", consulta el artículo 947709 de Knowledge Base
en https://go.microsoft.com/fwlink/?linkid=121488.

Aceptar

C:\Windows\system32>
```

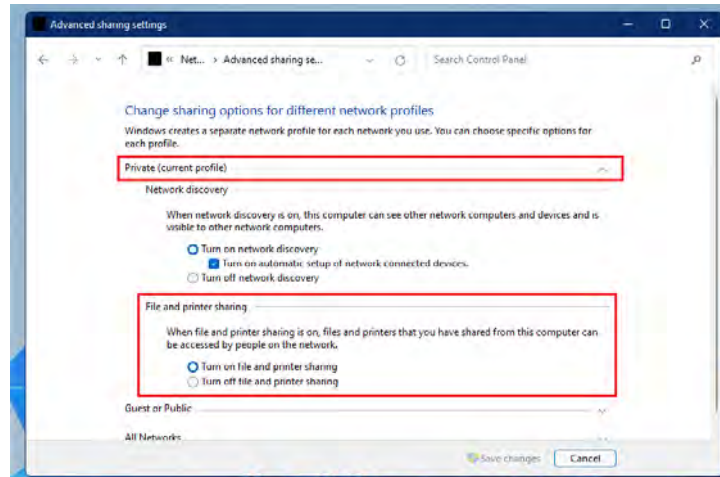
24

Alfredo Abad



## Activar o desactivar los ficheros compartidos y descubrimiento de la red en Windows con netsh

- Activar:
  - `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`
- Desactivar:
  - `netsh advfirewall firewall set rule group="Network Discovery" new enable=Yes`



25

Alfredo Abad



## Desactivar Cortafuegos Windows 11 desde PowerShell:

**Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False**

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
PS C:\WINDOWS\system32> _
```

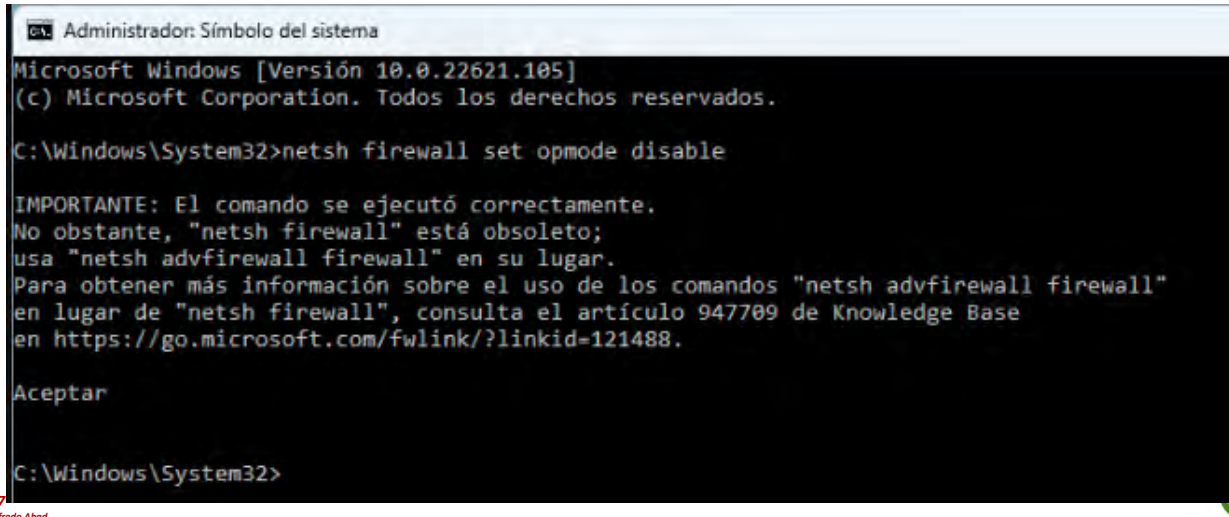
26

Alfredo Abad



## Desactivar Cortafuegos Windows 11 desde CMD:

**netsh firewall set opmode disable**



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.22621.105]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>netsh firewall set opmode disable

IMPORTANTE: El comando se ejecutó correctamente.
No obstante, "netsh firewall" está obsoleto;
usa "netsh advfirewall firewall" en su lugar.
Para obtener más información sobre el uso de los comandos "netsh advfirewall firewall"
en lugar de "netsh firewall", consulta el artículo 947709 de Knowledge Base
en https://go.microsoft.com/fwlink/?linkid=121488.

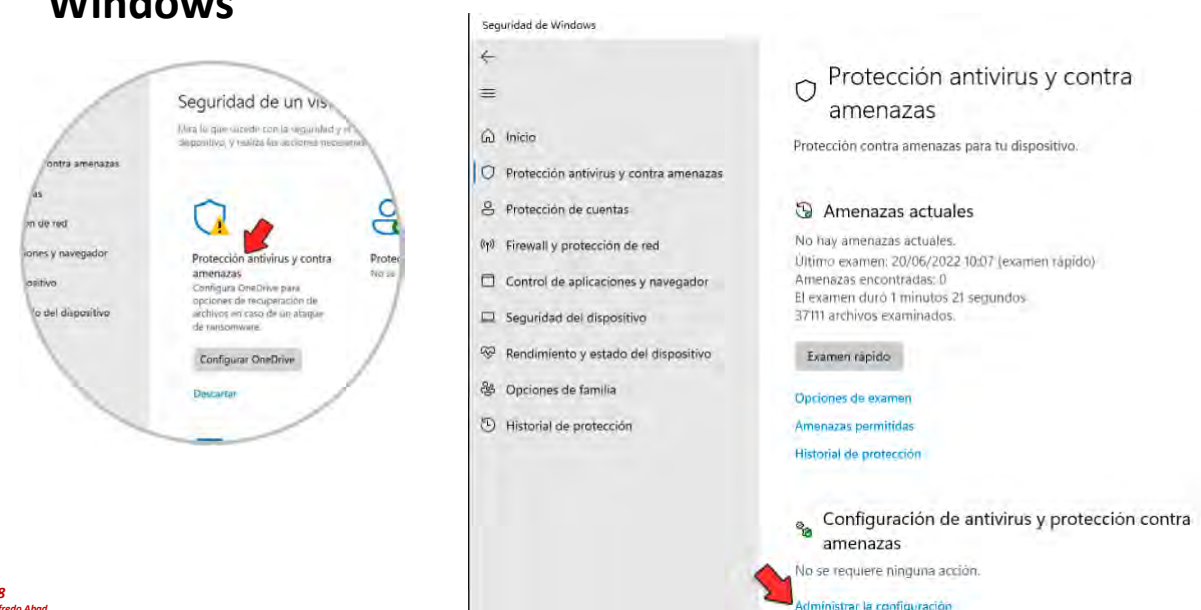
Aceptar

C:\Windows\System32>
```

27

Alfredo Abad

## Desactivar Cortafuegos Windows 11 desde Seguridad de Windows



The screenshot shows the Windows Security application. On the left, a circular navigation pane highlights 'Protección antivirus y contra amenazas'. The main area shows the 'Protección antivirus y contra amenazas' settings. Under 'Amenazas actuales', it states 'No hay amenazas actuales'. At the bottom, there is a red arrow pointing to the 'Administrar la configuración' link.

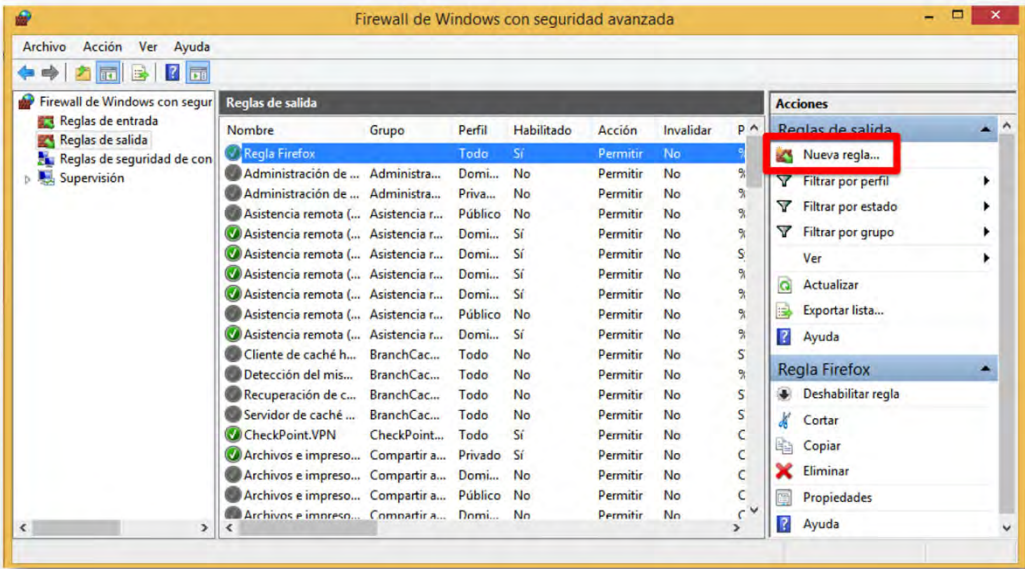
28

Alfredo Abad





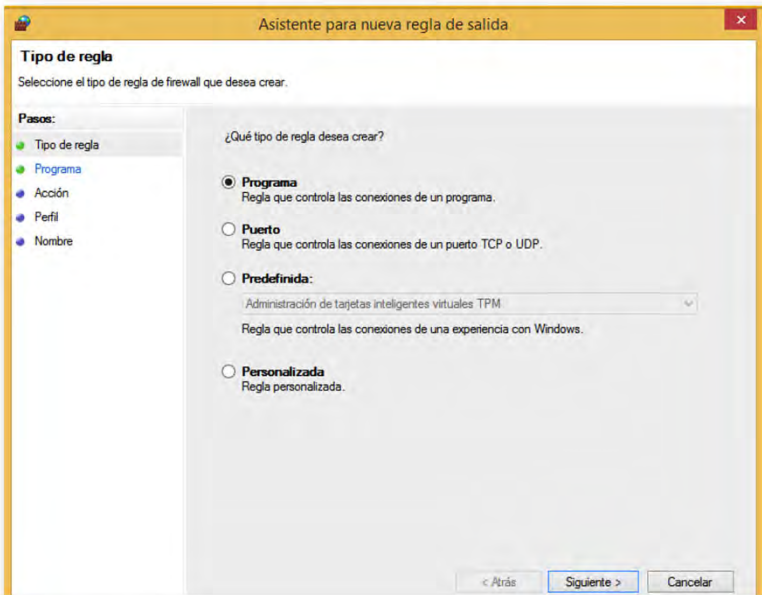
# Creamos una nueva regla



31  
Alfredo Abad



# A continuación tendremos que indicar a qué objeto queremos bloquear (programa, puerto, etc.)



32  
Alfredo Abad



Seleccionamos el programa o los programas que queremos que se vean afectados por la presente regla

**Programa**

Especifique la ruta completa y el nombre del archivo ejecutable del programa con el que coincide esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a todos los programas o a uno específico?

☐ **Todos los programas**  
La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.

☒ **Esta ruta de acceso del programa:**

%ProgramFiles%\ (x86)\Mozilla Firefox\firefox.exe

Ejemplo:  
c:\path\program.exe  
%ProgramFiles%\browser\browser.exe

< Atrás    Siguiete >    Cancelar

33  
Alfredo Abad



Seleccionamos la acción a tomar (permitir, bloquear, o permitir siempre y cuando la conexión sea segura)

**Acción**

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☐ **Permitir la conexión**  
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**  
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☒ **Bloquear la conexión**

< Atrás    Siguiete >    Cancelar

34  
Alfredo Abad



El penúltimo paso será indicar los perfiles que se verán afectados por la regla

**Perfil**  
Especifique los perfiles en los que se va a aplicar esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre

¿Cuándo se aplica esta regla?

- ☒ **Dominio**  
Se aplica cuando un equipo está conectado a su dominio corporativo.
- ☒ **Privado**  
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.
- ☒ **Público**  
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

< Atrás    Siguiente >    Cancelar

35  
Alfredo Abad



Finalmente le daremos un nombre y una descripción, para facilitar a los admins el trabajo, mientras gestionan esta y otras futuras reglas

**Nombre**  
Especifique el nombre y la descripción de esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Acción
- Perfil
- Nombre

Nombre:  
[Regla Firefox Denegar]

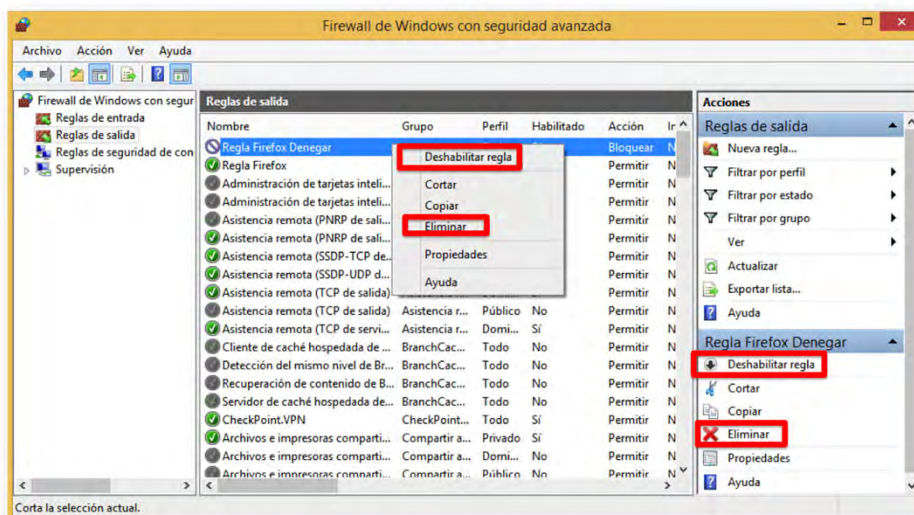
Descripción (opcional):  
[ ]

< Atrás    Finalizar    Cancelar

36  
Alfredo Abad



Una vez aplicada la regla, podremos deshabilitar o eliminarla desde el menú de acciones, o pulsando con el botón derecho sobre la regla

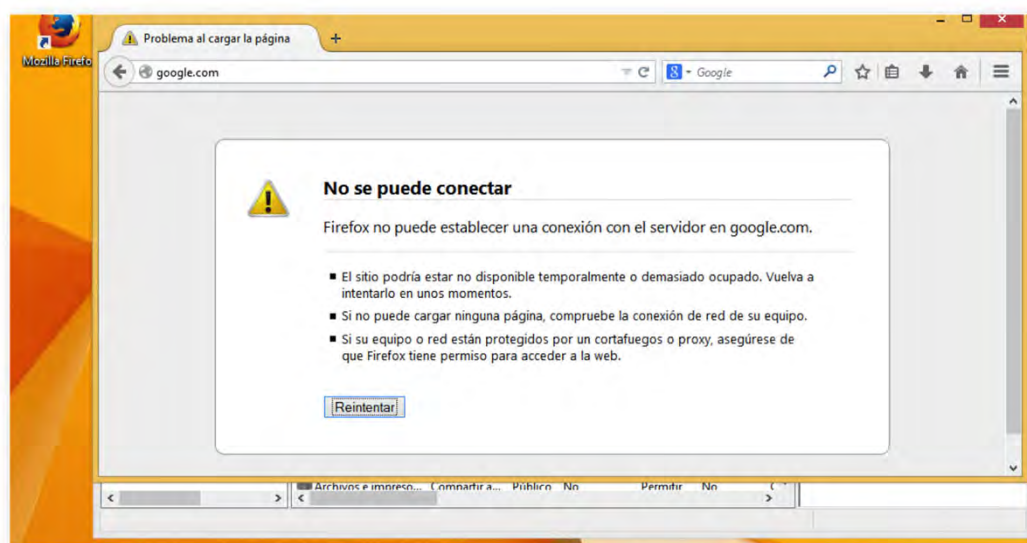


37

Alfredo Abad



Si todo ha ido correctamente, veremos si surte efecto o no la regla. En nuestro caso, bloquear el acceso a Internet del navegador Firefox



38

Alfredo Abad

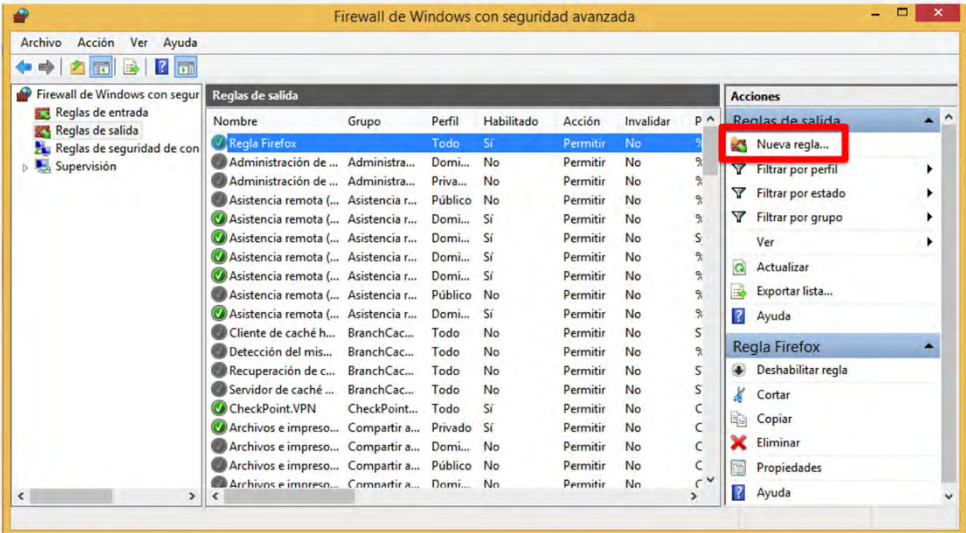




# Reglas personalizadas

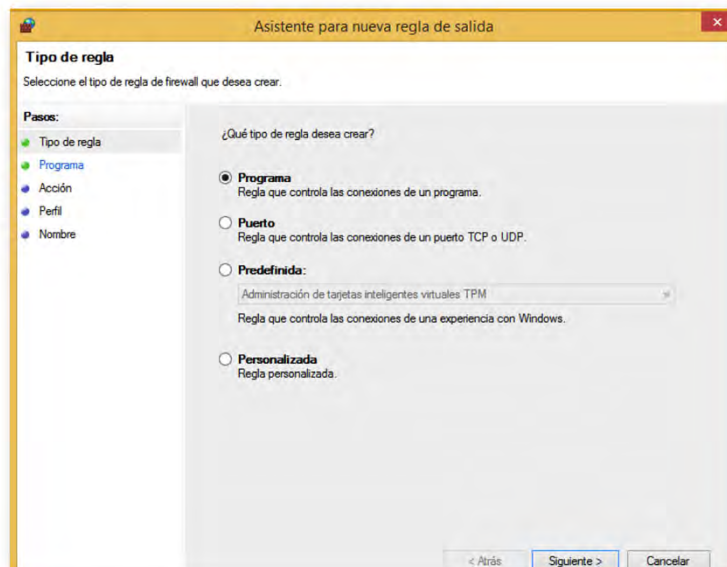


Desde esta pantalla podremos gestionar tanto reglas de entrada, como de salida





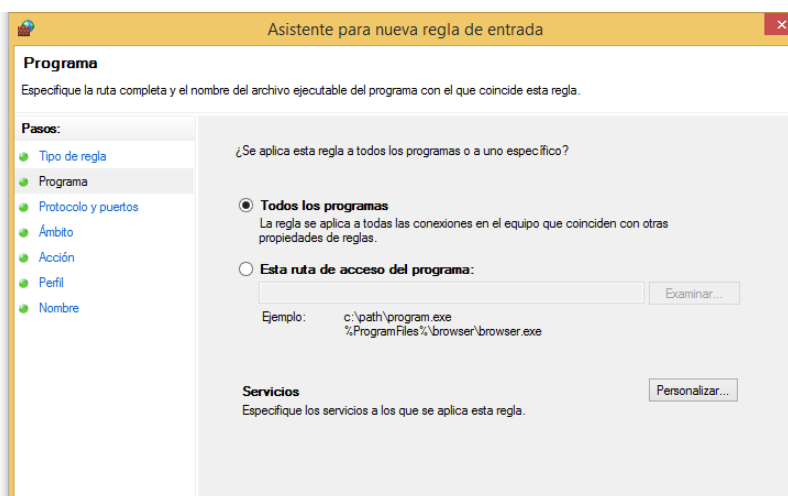
Una vez que pulsamos sobre la opción de creación de nuevas reglas, deberemos pulsar sobre "Personalizada"



41  
Alfredo Abad



En este punto el asistente cambiará para mostrarnos todas las posibles configuraciones del Firewall. En el primer menú podremos gestionar los programas a los que afectará la regla que estamos diseñando



42  
Alfredo Abad



Podremos gestionar los protocolos que se verán afectados por la regla. Podemos seleccionar los protocolos que vienen predefinidos, o bien podremos configurar uno desde cero

Asistente para nueva regla de entrada

**Protocolo y puertos**

Especifique los puertos y protocolos a los que se aplica esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Protocolo y puertos
- Ámbito
- Acción
- Perfil
- Nombre

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo:

Número de protocolo:

Puerto local:

Puerto remoto:

Configuración ICMP:

< Atrás    Siguiente >    Cancelar

43  
Alfredo Abad



Asistente para nueva regla de entrada

**Protocolo y puertos**

Especifique los puertos y protocolos a los que se aplica esta regla.

**Pasos:**

- Tipo de regla
- Programa
- Protocolo y puertos
- Ámbito
- Acción
- Perfil
- Nombre

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo:

Número de protocolo:

Puerto local:

Ejemplo: 80, 443, 5000-5010

Puerto remoto:

Ejemplo: 80, 443, 5000-5010

Configuración ICMP:

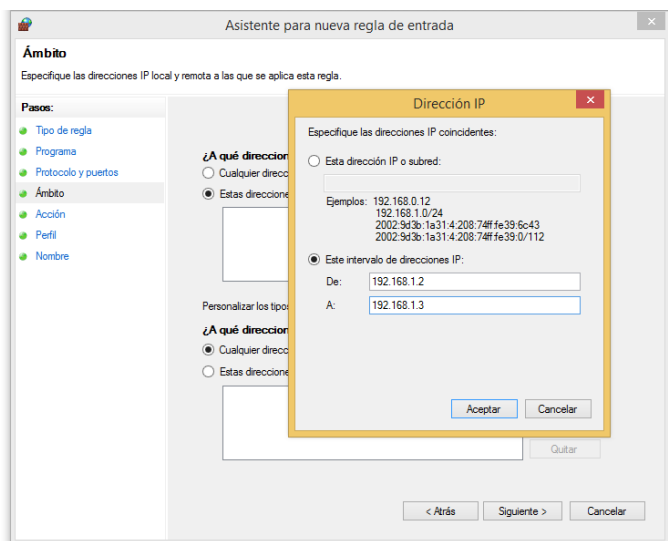
< Atrás    Siguiente >    Cancelar

44  
Alfredo Abad





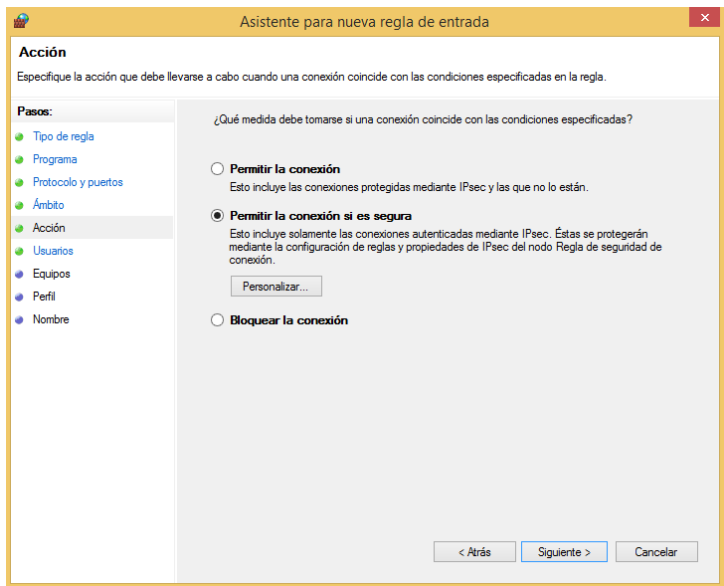
El siguiente paso será indicar las direcciones IP que se verán afectadas por la regla. Podremos filtrar para que solo se aplique a una dirección IP, a un rango de IPs, o a todas



45  
Alfredo Abad

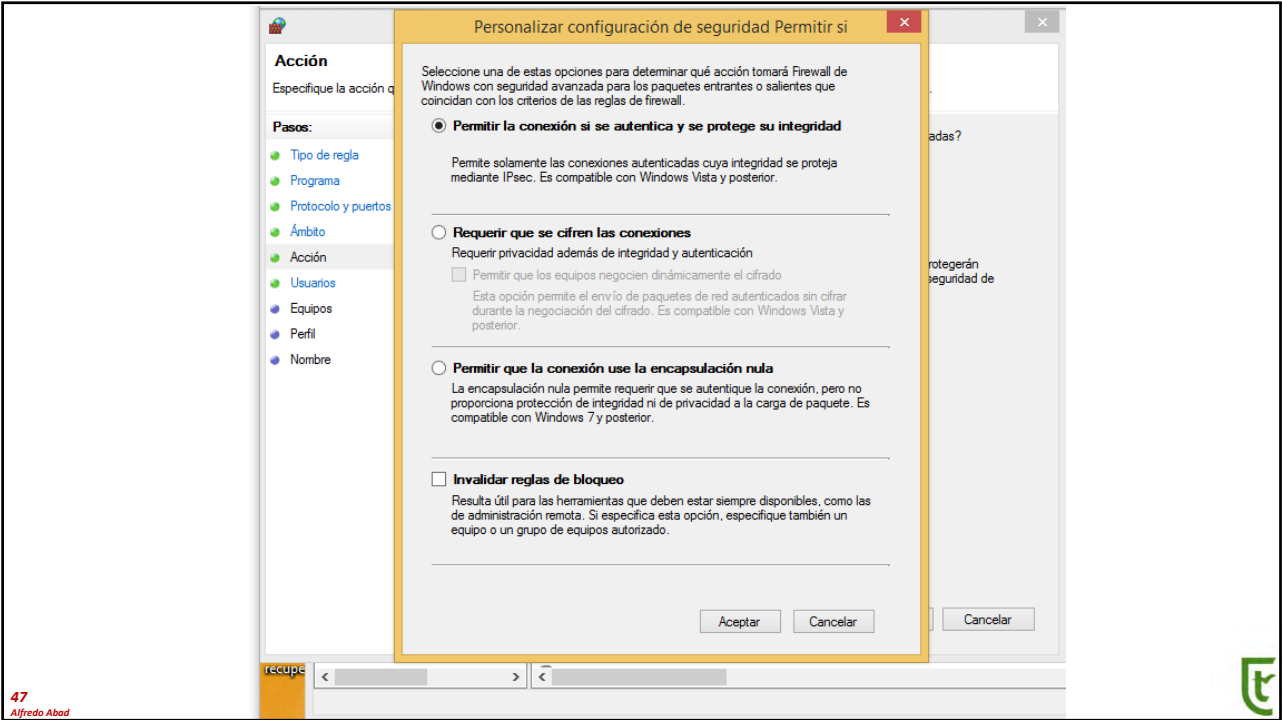


A continuación indicaremos si permitiremos la conexión, la bloquearemos, o la permitiremos únicamente si es segura



46  
Alfredo Abad

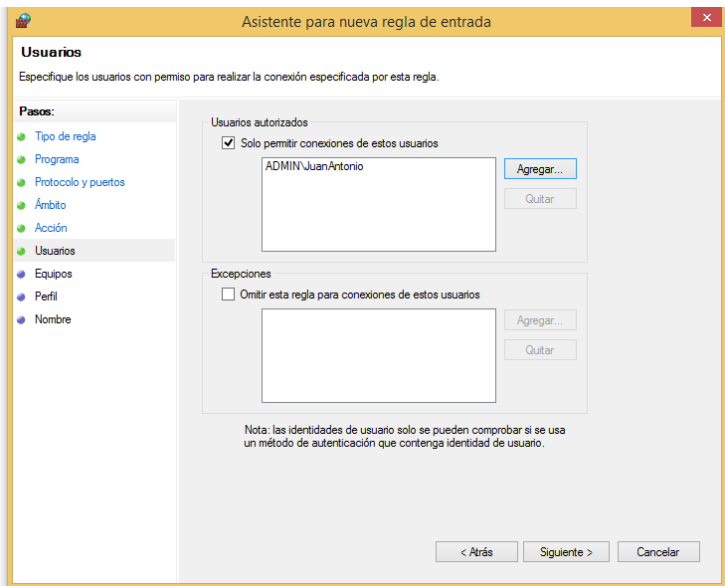




47  
Alfredo Abad



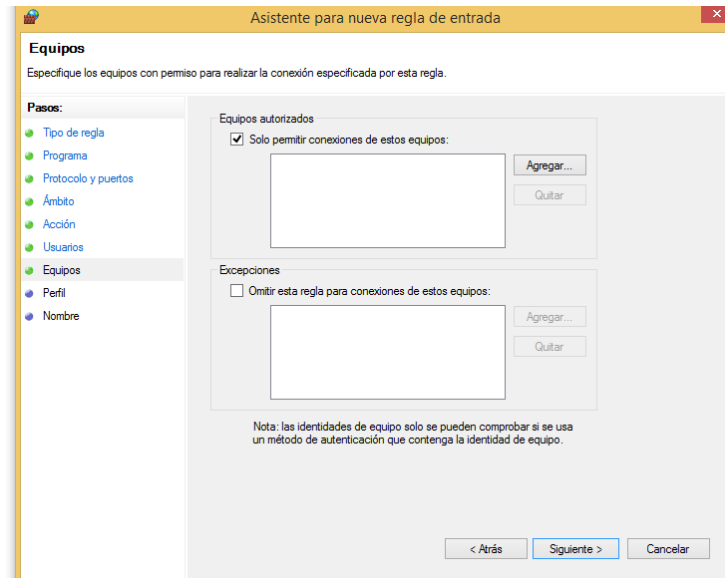
**Después indicaremos los usuarios que se verán afectados por la regla. Podremos configurar permisos y excepciones**



48  
Alfredo Abad



**Y finalmente seleccionaremos los equipos a los que se aplicará la conexión y lo asociaremos a un perfil del Firewall**



49  
Alfredo Abad



> ping \_

**Ejemplo: Habilitar ping (protocolo ICMP) en Windows**

50  
Alfredo Abad



## Por línea de comandos

### Habilitar respuesta ICMP IPv4

```
netsh advfirewall firewall add rule name="Habilitar respuesta ICMP IPv4"  
protocol=icmpv4:8,any dir=in action=allow
```

### Habilitar respuesta ICMP IPv6

```
netsh advfirewall firewall add rule name="Habilitar respuesta ICMP IPv6"  
protocol=icmpv6:8,any dir=in action=allow
```

### Deshabilitar respuesta ICMP IPv4

```
netsh advfirewall firewall add rule name="Deshabilitar respuesta ICMP IPv4"  
protocol=icmpv4:8,any dir=in action=block
```

### Deshabilitar respuesta ICMP IPv6

```
netsh advfirewall firewall add rule name="Deshabilitar respuesta ICMP IPv6"  
protocol=icmpv6:8,any dir=in action=block
```

### Mostrar reglas firewall:

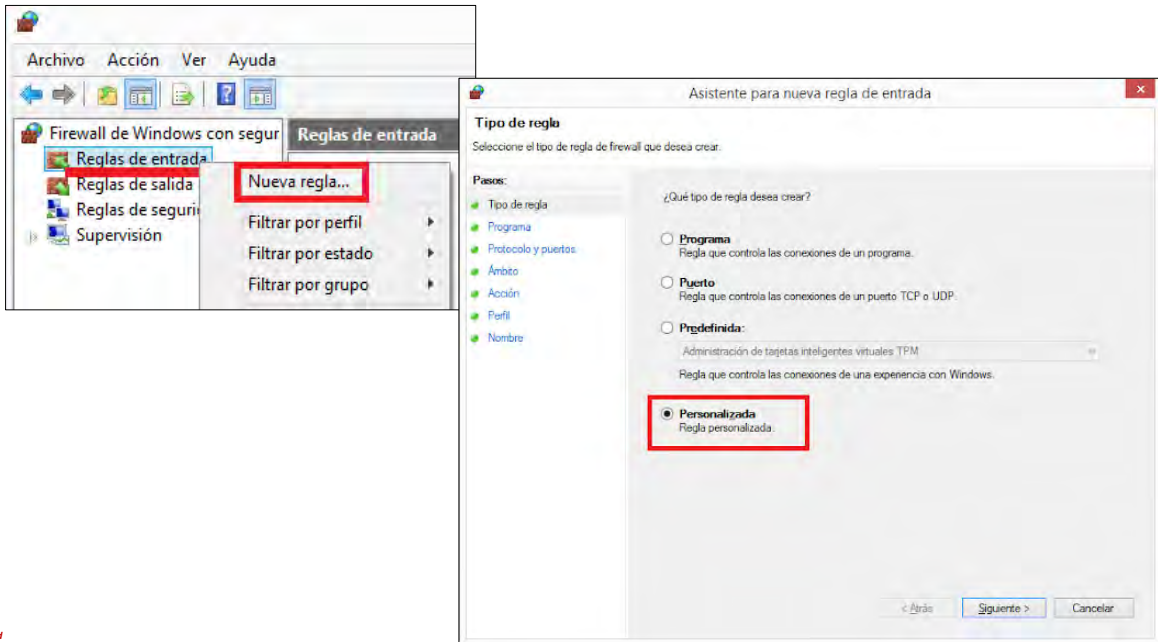
```
netsh advfirewall firewall show rule name=all
```

51

Alfredo Abad



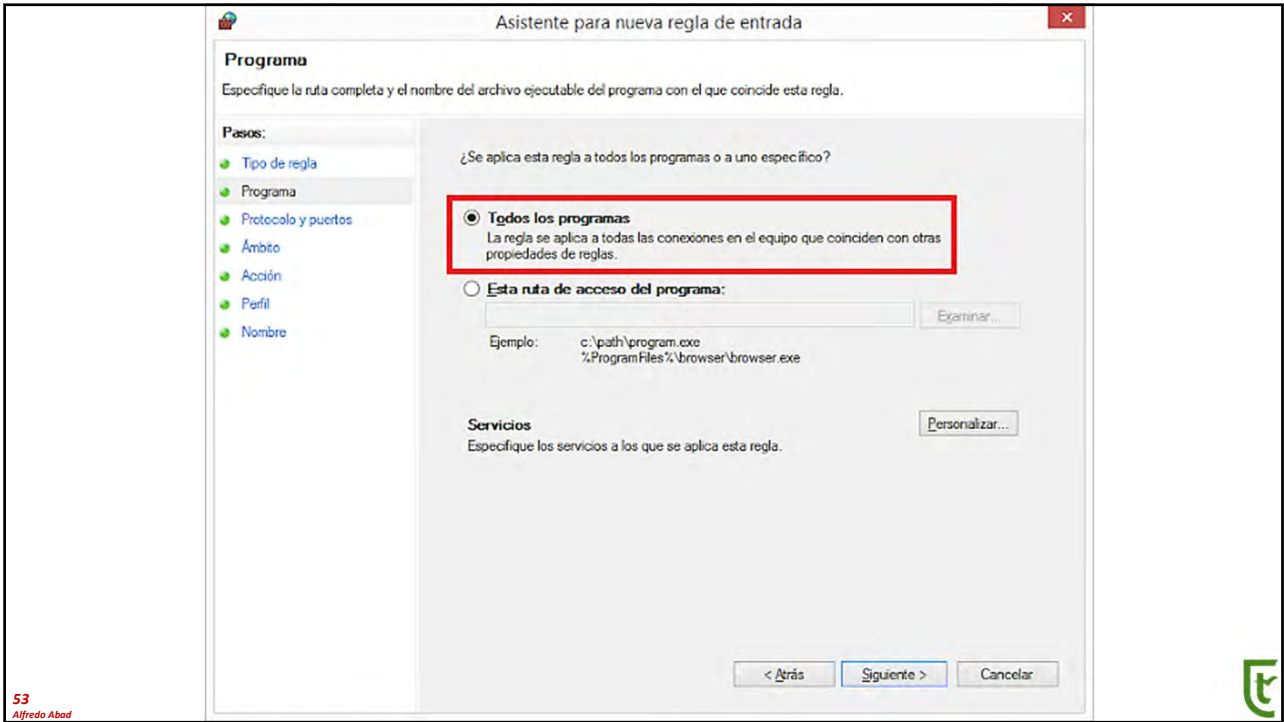
## Mediante interfaz gráfica



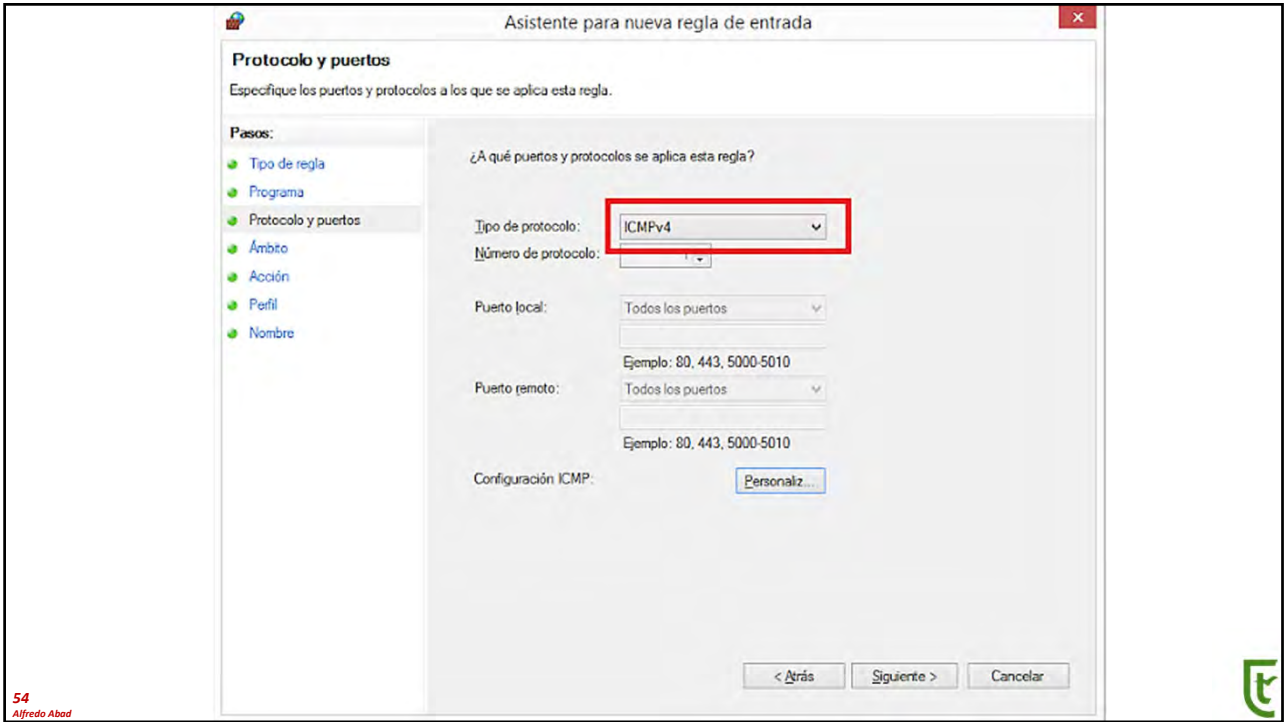
52

Alfredo Abad



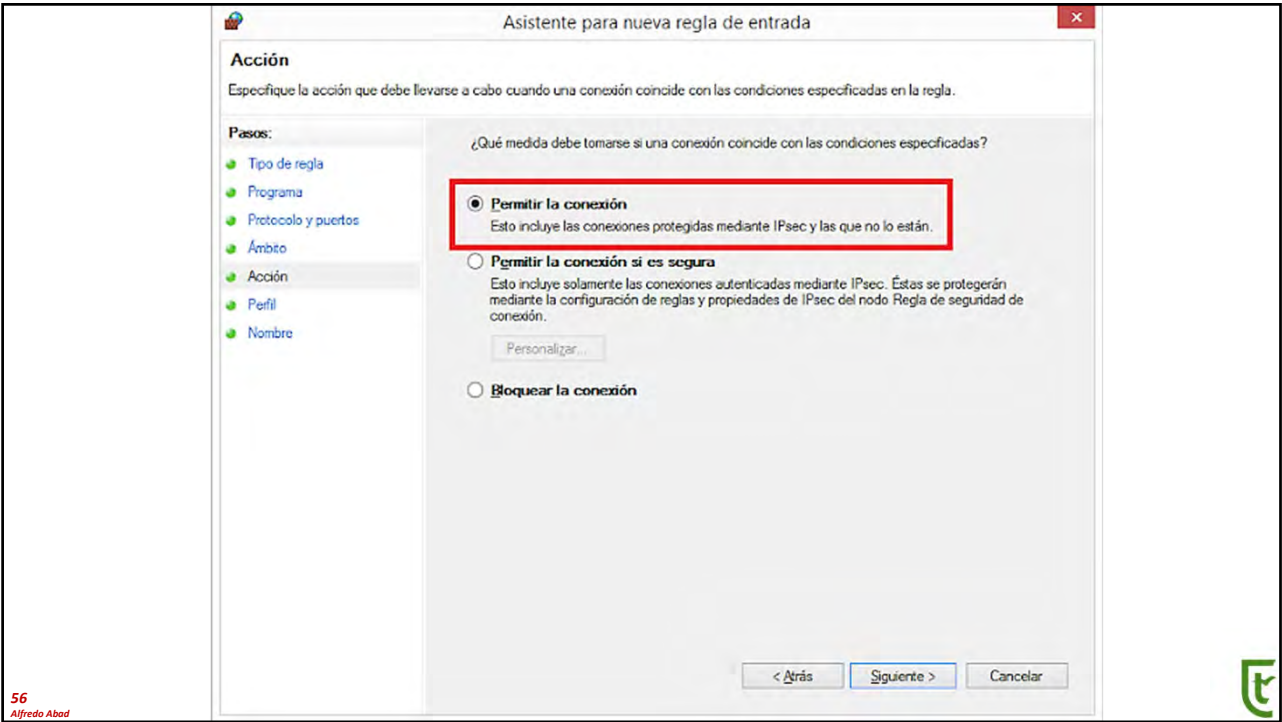
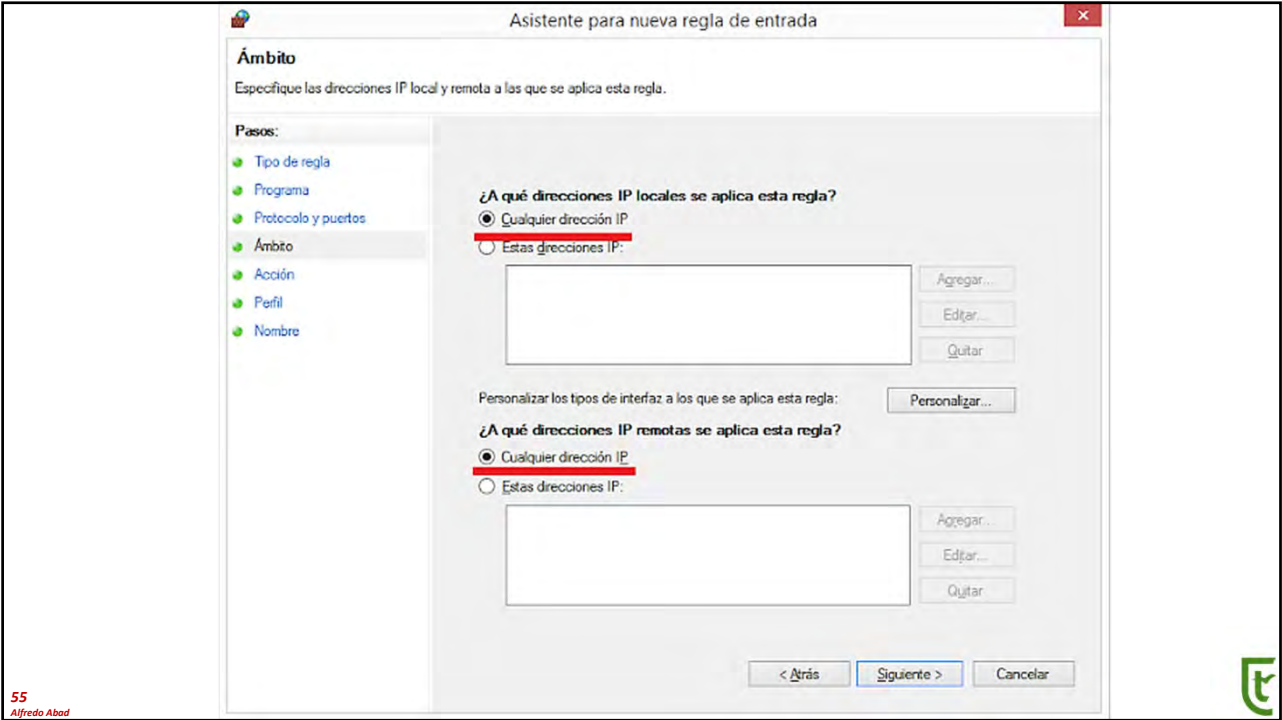


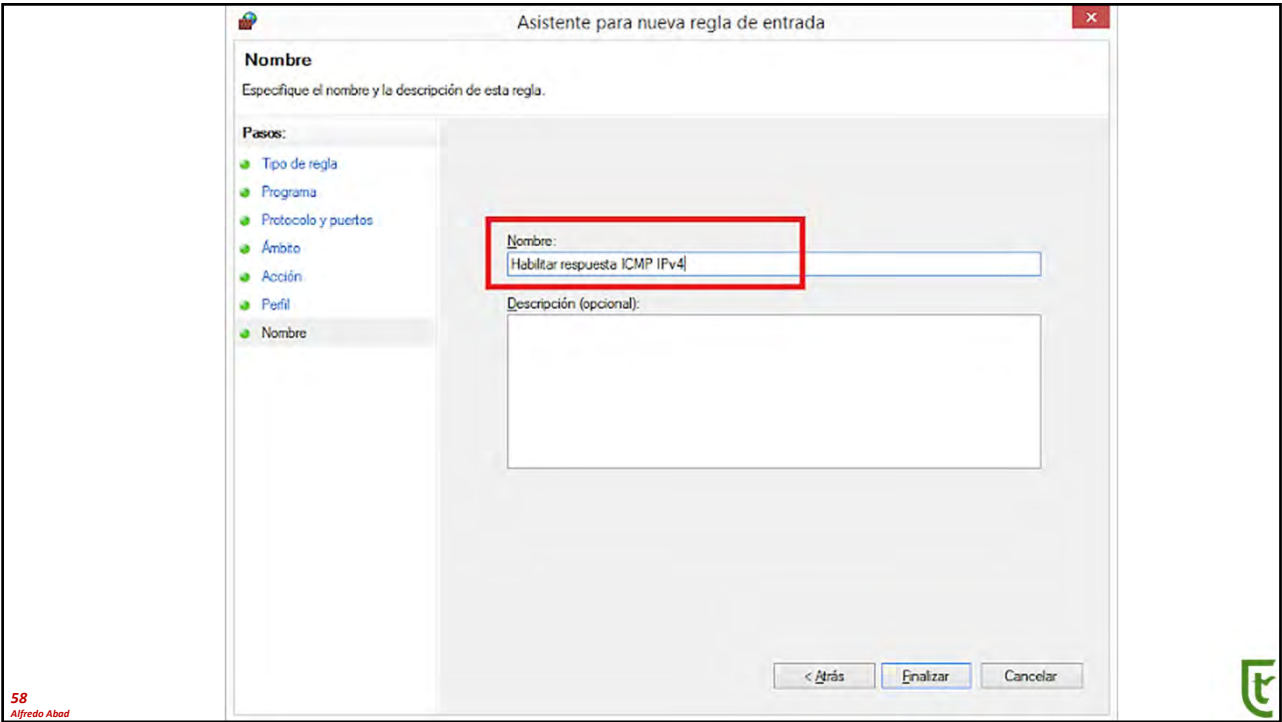
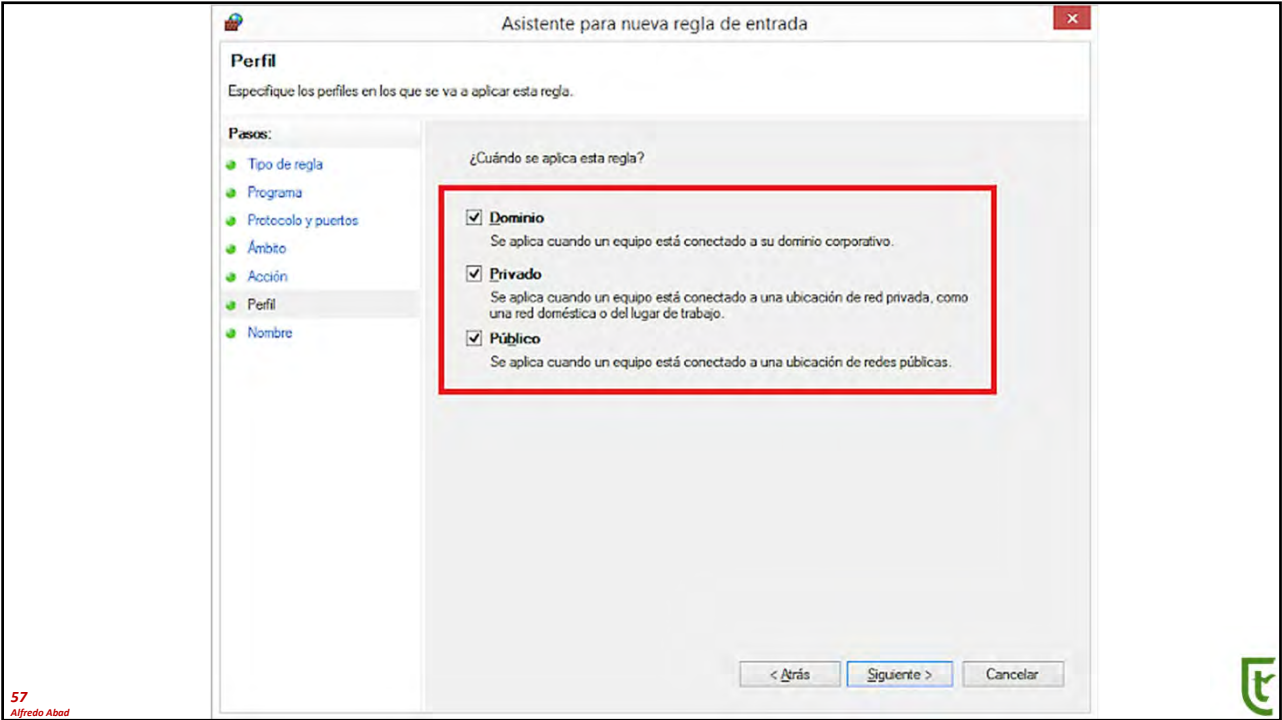
53  
Alfredo Abad



54  
Alfredo Abad











## Ejemplo: abrir un puerto en WS2022

- <https://www.solvetic.com/tutoriales/article/9839-abrir-puertos-windows-server-2022-firewall/>



## How to Manage Windows Firewall Rules with PowerShell

<https://www.cloudsavvyit.com/4269/managing-firewall-rules-with-powershell-in-windows/>





## Ejemplo: configuración del firewall de Windows

<https://www.redeszone.net/tutoriales/seguridad/configuracion-firewall-windows-10/>

61  
Alfredo Abad



## Ejemplo: Respuesta PING (habilitar o deshabilitar en Linux)

62  
Alfredo Abad



En sistemas Linux, por defecto la respuesta a ping (protocolo ICMP - Internet Control Message Protocol) está habilitada a nivel de kernel.

Para modificar este comportamiento, tenemos varias formas:

#### 1) Modificar los parámetros de carga del kernel:

Al cargar el kernel, se leen los parámetros indicados en el fichero `/etc/sysctl.conf`.

Especial cuidado en modificar de forma incorrecta el contenido de este fichero.

También se pueden modificar los parámetros en caliente modificando los ficheros situados en: `/proc/sys/`

Dentro de `/proc/sys/` encontraremos varios directorios, entre ellos el directorio `net/`, para configuraciones de red.

Modificar directamente `/proc/sys/` hará que los cambios sean temporales, es decir, se perderán los cambios al reiniciar el equipo.

Una buena práctica es primero modificar `/proc/sys/`, verificar si el comportamiento es el esperado y luego modificar `/etc/sysctl.conf` para configurar los cambios de forma permanente.

63  
Alfredo Abad



#### 2) Configurar el firewall del equipo:

La otra forma que tenemos para bloquear la respuesta a ping, es configurar el firewall del equipo.

Con el firewall del equipo, podemos configurar reglas que descarten los paquetes ICMP entrantes, tanto para IPv4 como para IPv6.

**Veamos como habilitar o deshabilitar la respuesta ICMP a nivel de kernel:**

##### Configuración temporal:

Para habilitar que el ICMP sea ignorado:

```
echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Para deshabilitar que el ICMP sea ignorado:

```
echo 0> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

##### Configuración permanente:

Editamos el fichero: `/etc/sysctl.conf`

Para habilitar que el ICMP sea ignorado:

64  
Alfredo Abad



Configuración temporal:

Para habilitar que el ICMP sea ignorado:

```
echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Para deshabilitar que el ICMP sea ignorado:

```
echo 0> /proc/sys/net/ipv4/icmp_echo_ignore_all
```

Configuración permanente:

Editamos el fichero: /etc/sysctl.conf

Para habilitar que el ICMP sea ignorado:

```
net.ipv4.icmp_echo_ignore_all=1
```

Para deshabilitar que el ICMP sea ignorado:

```
net.ipv4.icmp_echo_ignore_all=0
```

Otra forma de bloquear las respuestas ICMP es utilizando iptables:

Para bloquear tráfico ICMP entrante sobre IPv4:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
```

Para bloquear tráfico ICMP entrante sobre IPv6:

```
iptables -A INPUT -p icmpv6 --icmp-type echo-request -j DROP
```

65

Alfredo Abad



**Saber si ping es bloqueado por el firewall o no hay respuesta porque el sistema está apagado o desconectado**

66

Alfredo Abad



Si no podemos acceder al firewall del equipo remoto y este está bloqueando el protocolo ICMP, con ping, no podemos saber si el equipo destino está encendido o apagado.

Si el equipo destino está en el mismo segmento de red y no hay ningún router entre medio, podemos utilizar la siguiente técnica:

- Realizamos un ping al equipo destino.
- El destino no contesta.
- Verificamos la tabla ARP (Address Resolution Protocol) del equipo origen: Si la dirección MAC del equipo destino figura en la tabla, significa que el firewall del equipo destino está bloqueando el protocolo ICMP utilizado por el ping.

### Laboratorio 1: El ping lo bloquea el firewall

67  
Alfredo Abad



```

C:\>
C:\>arp -a 1
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet Dirección física
192.168.150.2 00-50-56-f3-96-99 dinámico
192.168.150.255 ff-ff-ff-ff-ff-ff estático
224.0.0.22 01-00-5e-00-00-16 estático
224.0.0.252 01-00-5e-00-00-fc estático

C:\>arp -d * 2
C:\>arp -a 3
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet Dirección física
224.0.0.22 01-00-5e-00-00-16 estático

C:\>ping 192.168.150.111 4
Haciendo ping a 192.168.150.111 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.150.111:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),

C:\>arp -a 5
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet Dirección física
192.168.150.2 00-50-56-f3-96-99 dinámico
192.168.150.111 00-0c-29-b0-03-3b dinámico
224.0.0.22 01-00-5e-00-00-16 estático
  
```

68  
Alfredo Abad





- 1) Visualizamos el contenido de la tabla ARP con el comando: arp -a.
- 2) Eliminamos el contenido de la tabla ARP con el comando: arp -d \*
- 3) Visualizamos el contenido de la tabla ARP con el comando: arp -a. No aparece ninguna dirección IP del segmento propio de red.
- 4) Realizamos un ping a la dirección IP del equipo destino. Vemos que el equipo destino, no contesta. La respuesta es: "Tiempo de espera agotado para esta solicitud".
- 5) Visualizamos el contenido de la tabla ARP con el comando: arp -a. Vemos como aparece la dirección IP destino.

Conclusión: El equipo destino está online, pero el firewall de Windows del equipo destino está bloqueando los paquetes ICMP.

**Laboratorio 2: El ping no lo bloquea el firewall, el equipo destino está apagado.**

69  
Alfredo Abad



```

Administrator: CMD

C:\>arp -a 1
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet  Dirección física
192.168.150.2          00-50-56-f3-96-99    dinámico
192.168.150.111       00-0c-29-b0-03-3b    dinámico
224.0.0.22            01-00-5e-00-00-16    estático

C:\>arp -d * 2
C:\>arp -a 3
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet  Dirección física
224.0.0.22            01-00-5e-00-00-16    estático

C:\>ping 192.168.150.111 4
Haciendo ping a 192.168.150.111 con 32 bytes de datos:
Respuesta desde 192.168.150.10: Host de destino inacces
Respuesta desde 192.168.150.10: Host de destino inacces
Respuesta desde 192.168.150.10: Host de destino inacces
Respuesta desde 192.168.150.10: Host de destino inacces

Estadísticas de ping para 192.168.150.111:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),

C:\>arp -a 5
Interfaz: 192.168.150.10 --- 0xc
Dirección de Internet  Dirección física
224.0.0.22            01-00-5e-00-00-16    estático

C:\>_
  
```

70  
Alfredo Abad



- 1) Visualizamos el contenido de la tabla ARP con el comando: arp -a.
- 2) Eliminamos el contenido de la tabla ARP con el comando: arp -d \*
- 3) Visualizamos el contenido de la tabla ARP con el comando: arp -a. No aparece ninguna dirección IP del segmento propio de red.
- 4) Realizamos un ping a la dirección IP del equipo destino. Vemos que el equipo destino, no contesta.
- 5) Visualizamos el contenido de la tabla ARP con el comando: arp -a. Vemos como no aparece la dirección IP destino.

Conclusión: El equipo destino no está online o no se dispone de conectividad con el mismo. No es el firewall de Windows del equipo destino que está bloqueando los paquetes ICMP, ya que no aparece la dirección IP destino en la tabla ARP.

71  
Alfredo Abad



## El filtro SmartScreen de Windows 10

72  
Alfredo Abad





## Características de SmartScreen

- SmartScreen es un mecanismo para proteger el equipo de sitios web y aplicaciones de phishing o malware.
  - Esto evitará que sean descargados archivos potencialmente maliciosos que ponen en riesgo la integridad del equipo.
  - Esta es una función integrada por defecto y Microsoft Defender SmartScreen se encarga de analizar si una página es potencialmente malintencionada usando métodos como los siguientes.
- Métodos
  - Usando el análisis del sitio web visitado para determinar si este posee algún margen de comportamiento sospechoso.
  - Llevando a cabo una comprobación de los sitios web contra una lista dinámica de sitios de phishing y sitios de software malicioso que han sido denunciados de forma global.
- Características
  - Dentro de sus características encontramos:
  - Protección de aplicaciones y URL basada en la reputación
  - Soporte anti-phishing y anti-malware
  - Integración del sistema operativo Windows 10
  - Gestión a través de políticas de grupo y Microsoft Intune
  - Datos heurísticos y de diagnóstico mejorados

73  
Alfredo Abad



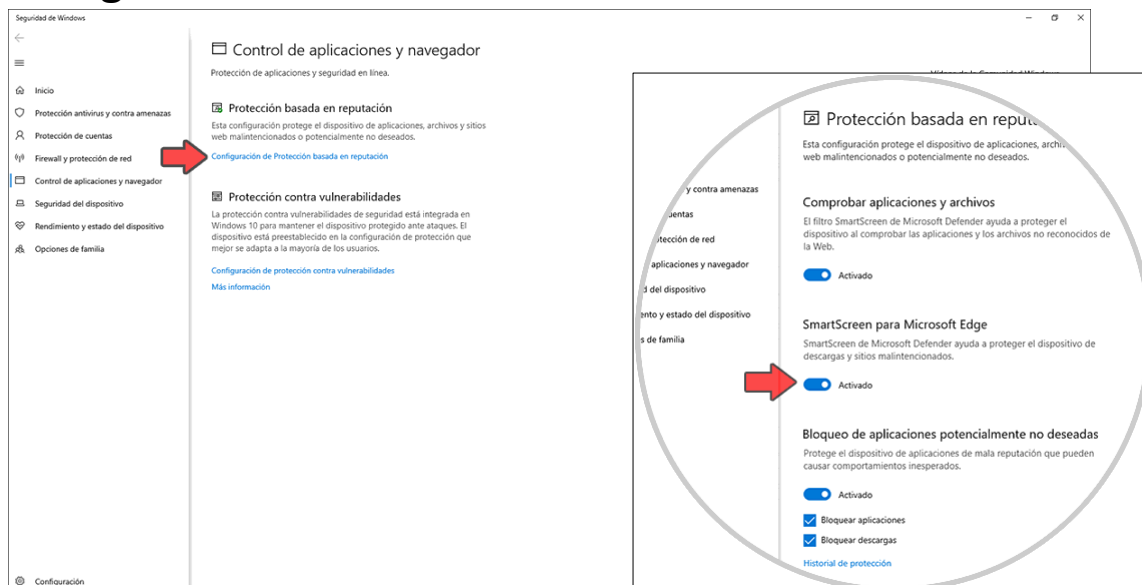
## Deshabilitar filtro de SmartScreen Windows 10 desde las propiedades de Internet

The screenshot illustrates the process of disabling the SmartScreen filter in Windows 10 through the Internet Properties dialog. It shows the 'Ejecutar' (Run) dialog box with 'inetcpl.cpl' entered, the 'Internet Properties' window with the 'Content Advisor' tab selected, and the 'Content Advisor Configuration' window where 'SmartScreen for Windows Defender' is disabled. A red arrow points to the 'Desactivar' (Disable) option for 'SmartScreen for Windows Defender'.

74  
Alfredo Abad



## Deshabilitar filtro de SmartScreen Windows 10 desde Configuración

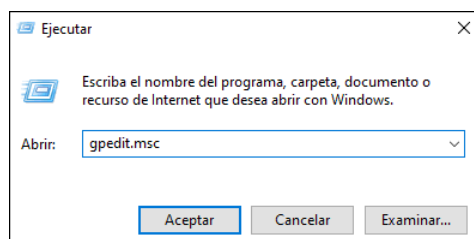


75

Alfredo Abad

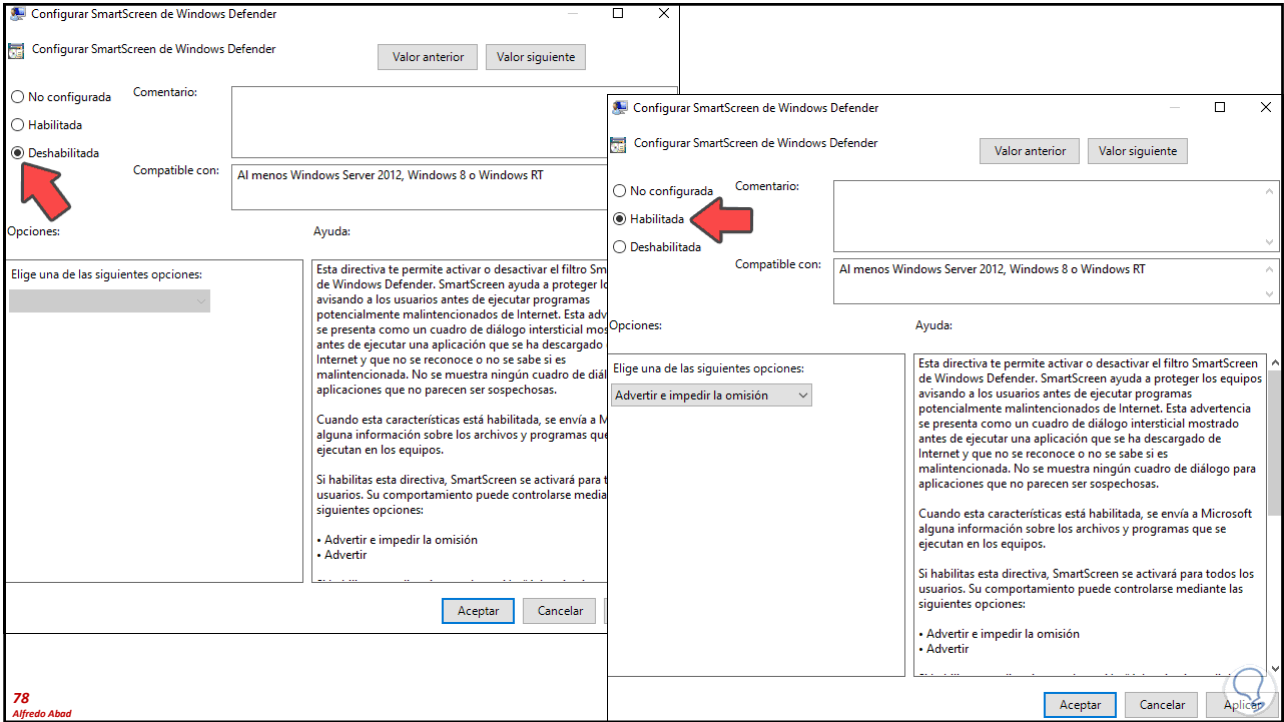
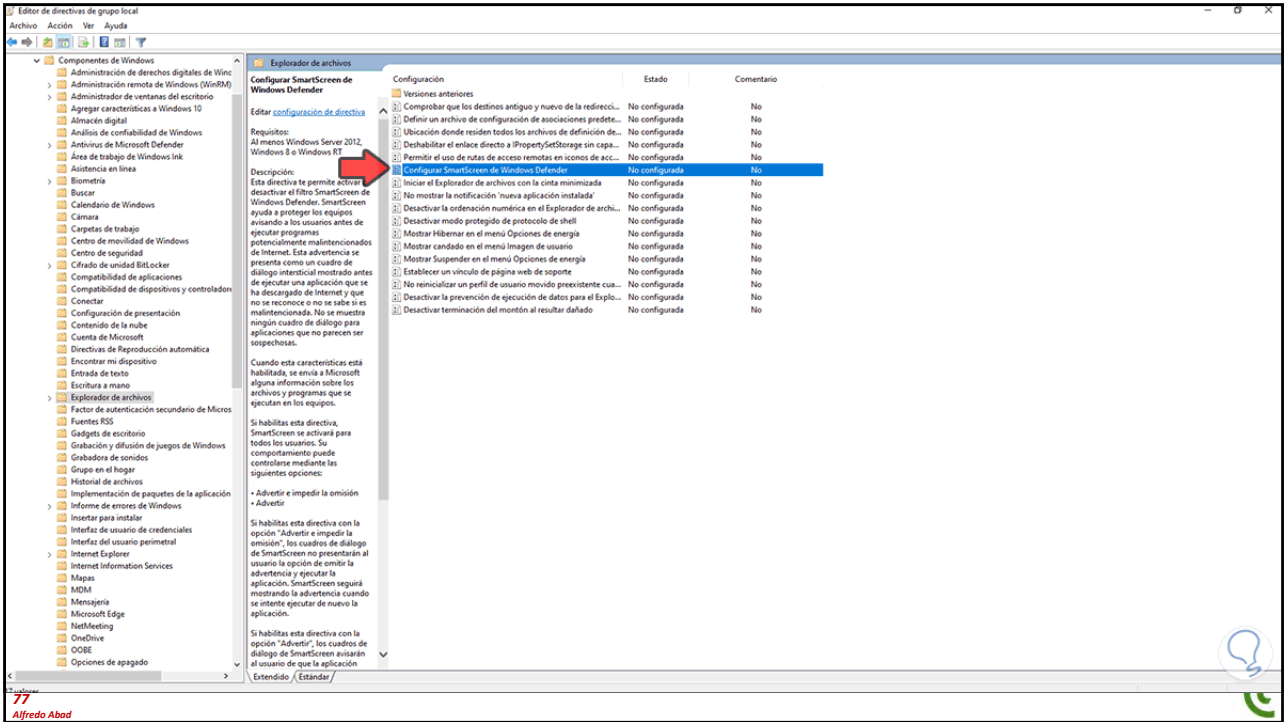
## Deshabilitar filtro de SmartScreen Windows 10 desde las políticas de grupo

- En la ventana de las políticas vamos a la ruta:
  - Configuración del equipo
  - Plantillas administrativas
  - Componentes de Windows
  - Explorador de archivos
  - Ubicamos la política llamada "Configurar SmartScreen de Windows Defender":



76

Alfredo Abad



Eficacia de antivirus personales (2022)

	OFFLINE Detection Rate	ONLINE Detection Rate	ONLINE Protection Rate	False Alarms
Avast	93.9%	98.8%	100%	5
AVG	93.9%	98.8%	100%	5
Avira	93.8%	97.4%	99.98%	0
Bitdefender	94.9%	94.9%	99.98%	8
ESET	92.5%	92.5%	99.91%	0
G DATA	96.0%	96.0%	100%	4
K7	89.8%	89.8%	99.97%	30
Kaspersky	80.6%	91.1%	99.96%	0
Malwarebytes	87.4%	96.9%	99.81%	16
McAfee	82.5%	99.6%	100%	7
Microsoft	69.8%	98.1%	99.99%	19
NortonLifeLock	85.7%	99.4%	99.99%	3
Panda	52.8%	83.8%	99.93%	59
Total AV	93.8%	96.8%	99.97%	1
Total Defense	94.9%	94.9%	99.96%	8
Trend Micro	41.1%	82.3%	97.41%	6
VIPRE	94.9%	94.9%	99.97%	8

