CASO PRÁCTICO 1

CONFIGURACIÓN DE UN CORTAFUEGOS

INTRODUCCIÓN

En el contexto actual de las empresas, el uso de Internet es una herramienta imprescindible para el desarrollo de la actividad profesional, pero también puede convertirse en un problema cuando no se gestiona de forma adecuada. Como administrador de sistemas, considero fundamental garantizar que los recursos tecnológicos de la empresa se utilicen de manera eficiente, segura y alineada con los objetivos corporativos.

En este caso práctico, parto de una situación realista en la que el uso de aplicaciones de redes sociales como **X** y **TikTok** por parte de los empleados afecta negativamente tanto a la **productividad** como al **ancho de banda disponible** de la red corporativa. Este tipo de aplicaciones, aunque útiles en el ámbito personal, no resultan necesarias para el trabajo diario en una empresa de reparación de motocicletas, por lo que su acceso debe ser controlado.

Desde el punto de vista de la **Seguridad y Alta Disponibilidad**, el uso de un cortafuegos se presenta como una medida clave dentro de la política de seguridad de la organización. En concreto, el **Firewall de Windows 11**, integrado de forma nativa en el sistema operativo, ofrece las herramientas necesarias para aplicar reglas de filtrado que permitan controlar el tráfico saliente y restringir el acceso a determinadas aplicaciones sin necesidad de instalar software adicional.

A lo largo de esta actividad explicaré, en primera persona y de forma detallada, cómo he llevado a cabo la configuración del Firewall de Windows 11 para bloquear el acceso a las aplicaciones X y TikTok, justificando cada decisión técnica adoptada y comprobando posteriormente la eficacia de las medidas aplicadas. Con ello, se busca no solo cumplir con los requisitos planteados por la dirección de la empresa, sino también reforzar la seguridad de la red y optimizar el uso de los recursos disponibles desde una perspectiva profesional y crítica.

1. Acceso al Firewall de Windows 11

Para comenzar el procedimiento de configuración del cortafuegos, lo primero que hice fue acceder al **Firewall de Windows 11**, ya que cualquier acción de control del tráfico de red debe realizarse desde esta herramienta para garantizar su correcta aplicación. Iniciar el proceso por este punto es fundamental, puesto que permite verificar el estado general de la seguridad del sistema antes de aplicar configuraciones más específicas.

Accedí al Firewall desde la ruta **Configuración → Privacidad y seguridad → Seguridad de Windows → Firewall y protección de red**, seleccionando posteriormente la opción **Configuración avanzada**. Esta acción abre la consola **Firewall de Windows Defender con seguridad avanzada**, que proporciona un entorno de administración más completo y preciso que la interfaz básica del sistema.

Desde un punto de vista técnico, la utilización de la consola avanzada resulta imprescindible en un entorno profesional, ya que permite la **creación y gestión detallada de reglas de entrada y salida**, así como la aplicación de políticas diferenciadas según los perfiles de red (dominio, privado y público). Este nivel de control es clave para poder actuar sobre el tráfico saliente de aplicaciones concretas, que es la necesidad planteada en este caso práctico.

Antes de continuar con la configuración de las reglas, comprobé que el Firewall estuviera **activado en todos los perfiles de red**. Este paso es especialmente relevante desde la perspectiva de la seguridad, ya que una desactivación parcial del cortafuegos podría dejar sin efecto las restricciones que se definan posteriormente. En la situación mostrada, el **perfil público se encuentra activo**, lo que incrementa la exposición del equipo y refuerza la necesidad de aplicar medidas restrictivas adicionales.

Además, en esta consola se puede observar el comportamiento por defecto del Firewall de Windows: las **conexiones entrantes que no coinciden con una regla están bloqueadas**, mientras que las **conexiones salientes se permiten automáticamente**. Esta política explica por qué es necesario crear reglas específicas de salida para bloquear aplicaciones como X y TikTok, ya que, sin una intervención explícita, el sistema permitiría su acceso a Internet.

Desde una perspectiva crítica y reflexiva, este paso inicial no debe entenderse como un simple acceso a una herramienta, sino como la base sobre la que se construye toda la política de seguridad del sistema. Acceder a la consola avanzada y verificar el estado del cortafuegos garantiza que las decisiones técnicas posteriores sean eficaces, coherentes y alineadas con una gestión responsable de la seguridad de la red corporativa.

En la **figura 1** donde se comprueba el estado del cortafuegos en los distintos perfiles de red y se habilita el entorno necesario para la creación de reglas de filtrado.

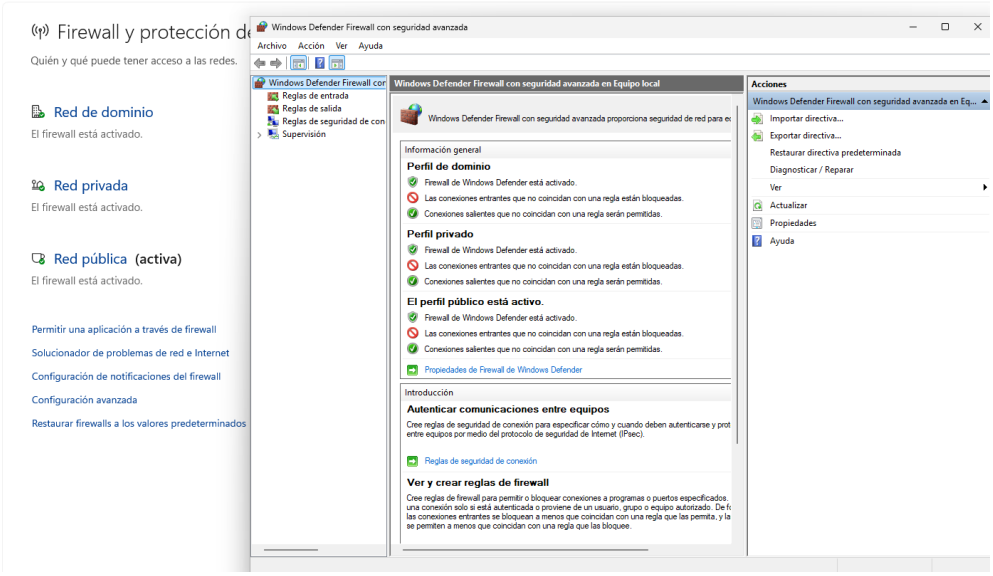


Figura 1: Acceso a la consola de Firewall de Windows Defender con seguridad avanzada,

Para abordar la problemática de la disminución de la productividad y el uso ineficiente del ancho de banda detectado en el taller de motocicletas, he seleccionado el **Firewall de Windows**

Defender con seguridad avanzada como herramienta principal de control y restricción del acceso a Internet.

Esta decisión se fundamenta en que se trata de una solución **nativa e integrada en Windows 11**, lo que permite un despliegue inmediato sin costes adicionales de licenciamiento ni la necesidad de instalar software de terceros en los equipos corporativos. Desde el punto de vista de la administración de sistemas, el uso de herramientas integradas reduce la superficie de ataque, simplifica el mantenimiento y garantiza una mayor compatibilidad con el sistema operativo.

El cortafuegos nativo actúa como una barrera de seguridad persistente que inspecciona y filtra el tráfico de red en función de reglas definidas por el administrador. En este caso práctico, el enfoque se centra exclusivamente en las **Reglas de salida**, ya que el tráfico no deseado tiene su origen en aplicaciones instaladas localmente en los equipos de los empleados que intentan establecer conexiones externas hacia los servidores de las plataformas X y TikTok.

Dada la complejidad de las aplicaciones modernas y las limitaciones de la interfaz gráfica del firewall para gestionar aplicaciones UWP, se ha diseñado una **estrategia de defensa en profundidad**, combinando dos metodologías complementarias con el objetivo de garantizar un bloqueo efectivo, preciso y sostenible en el tiempo:

- **Filtrado por Ámbito (Capa 3 del modelo OSI):**
  Se restringe el acceso a las direcciones IP asociadas a X y TikTok, previamente identificadas mediante resolución DNS utilizando la herramienta nslookup. Este método permite aplicar un bloqueo selectivo desde la interfaz gráfica del firewall, evitando un corte general del acceso a Internet.
- **Filtrado por Identidad de Aplicación (Capa 7 del modelo OSI):**
  Se utiliza el identificador único del paquete UWP (*PackageFamilyName*) para interceptar el tráfico directamente en el origen, independientemente de la dirección IP de destino. Esta técnica se implementa mediante PowerShell y permite un control mucho más preciso sobre las aplicaciones modernas instaladas desde la Microsoft Store.

La combinación de ambos enfoques refuerza la política de seguridad aplicada, ya que garantiza que, incluso si las plataformas de redes sociales modifican su infraestructura de red o utilizan nuevas direcciones IP, el firewall seguirá siendo capaz de identificar y bloquear el tráfico generado por las aplicaciones en función de su **identidad digital única**. Este planteamiento refleja una aproximación profesional y alineada con las buenas prácticas de seguridad en entornos corporativos.

2.Configuración de la regla de salida mediante la interfaz gráfica (GUI)

Selección del tipo de regla

Para iniciar la creación de la regla de salida, accedí al asistente del **Firewall de Windows Defender con seguridad avanzada** y, en el primer paso, seleccioné el tipo de regla **Personalizada**.

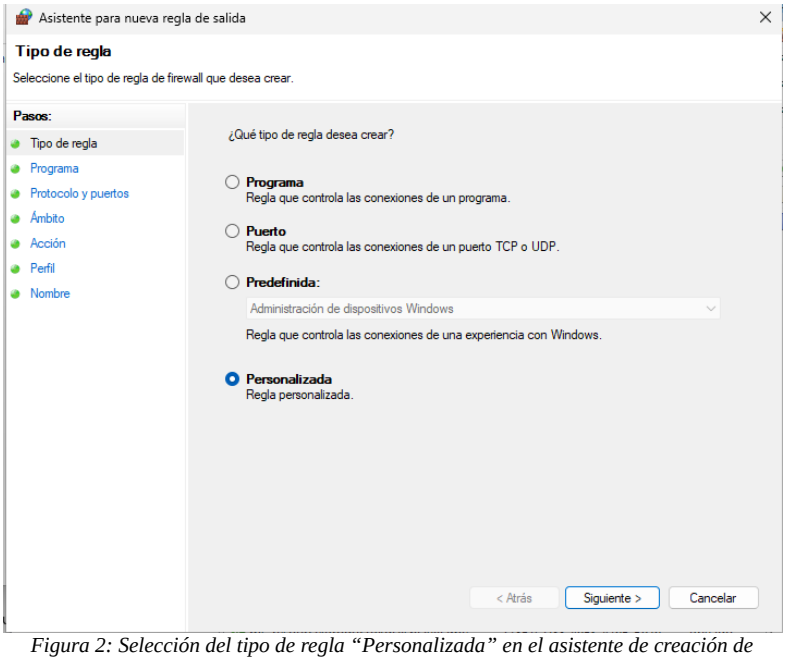


Figura 2: Selección del tipo de regla "Personalizada" en el asistente de creación de reglas de salida del Firewall de Windows Defender.

En la **Figura 2** se observa que el asistente ofrece varias opciones de configuración —Programa, Puerto, Predefinida y Personalizada—, cada una pensada para escenarios distintos. Tras analizar estas alternativas, seleccioné la opción **Personalizada**, ya que es la única que permite definir manualmente y con precisión todos los parámetros implicados en el filtrado del tráfico de red.

Esta elección está directamente condicionada por la naturaleza de las aplicaciones a bloquear. X y TikTok, al estar instaladas desde la Microsoft Store, son aplicaciones **UWP (Universal Windows Platform)** y no disponen de un ejecutable Win32 accesible que permita su gestión directa mediante reglas de tipo "Programa". Asimismo, las reglas basadas únicamente en puertos o en configuraciones predefinidas no ofrecen la flexibilidad necesaria para aplicar un bloqueo selectivo sin afectar al resto del tráfico del sistema.

Desde un punto de vista profesional, optar por una regla personalizada garantiza un mayor control sobre el comportamiento del firewall y evita configuraciones genéricas que podrían derivar en bloqueos excesivos o ineficaces. De este modo, se establecen unas bases sólidas para una política de seguridad coherente y alineada con las necesidades reales de la empresa.

2.1 Configuración del apartado Programa

En el segundo paso del asistente, correspondiente al apartado **Programa**, seleccioné la opción **"Todos los programas"**.

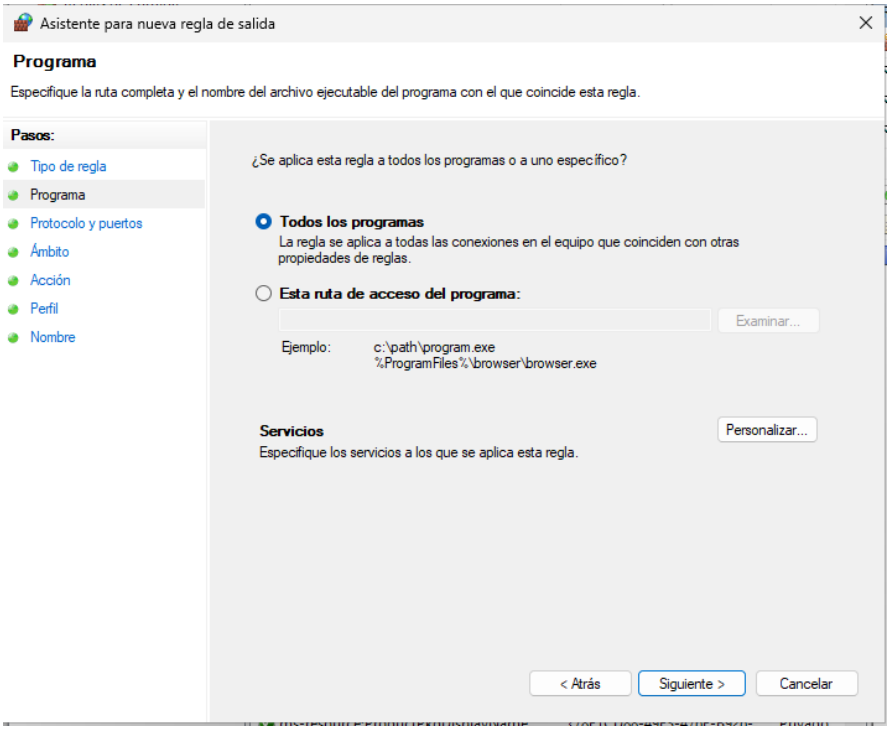


Figura 3: Configuración del apartado Programa aplicando la regla a todos los programas.

Tal y como se aprecia en la **Figura 3**, el asistente permite dos alternativas principales: aplicar la regla a **todos los programas** o vincularla a **una ruta de acceso específica de un ejecutable**. Tras analizar ambas opciones, opté por aplicar la regla a todos los programas, ya que las aplicaciones X y TikTok, al estar instaladas desde la Microsoft Store, pertenecen al modelo de aplicaciones **UWP (Universal Windows Platform)** y no disponen de un archivo ejecutable Win32 accesible que pueda seleccionarse mediante la opción “Esta ruta de acceso del programa”.

A primera vista, esta selección podría interpretarse como un bloqueo excesivamente amplio. Sin embargo, esta decisión está plenamente justificada desde un punto de vista técnico. Debido a las limitaciones de la interfaz gráfica del Firewall de Windows Defender para identificar aplicaciones UWP de forma individual, no resulta viable asociar la regla directamente a un ejecutable concreto sin recurrir a métodos avanzados, como la creación de reglas específicas mediante PowerShell.

Por este motivo, opté por aplicar inicialmente la regla a todos los programas, con el objetivo de **refinar posteriormente el bloqueo** mediante criterios más precisos, concretamente el filtrado por **direcciones IP remotas** en el apartado de **Ámbito**. De este modo, aunque la regla se aplique de forma global a nivel de programa, su efecto real queda limitado únicamente al tráfico dirigido a las infraestructuras de X y TikTok.

Desde un punto de vista profesional, esta configuración no supone un riesgo siempre que se combine con un ámbito correctamente definido. De hecho, este enfoque permite superar las restricciones de la interfaz gráfica sin provocar un bloqueo general del acceso a Internet. Esta decisión refleja una aproximación progresiva y consciente a la configuración del firewall, priorizando la coherencia técnica y la precisión del resultado final frente a soluciones forzadas o incorrectas.

2.2 Configuración del apartado Protocolo y puertos

En el siguiente paso del asistente, correspondiente a **Protocolo y puertos**, configuré la regla para que se aplicase a **cualquier tipo de protocolo** y a **todos los puertos**, tanto locales como remotos.

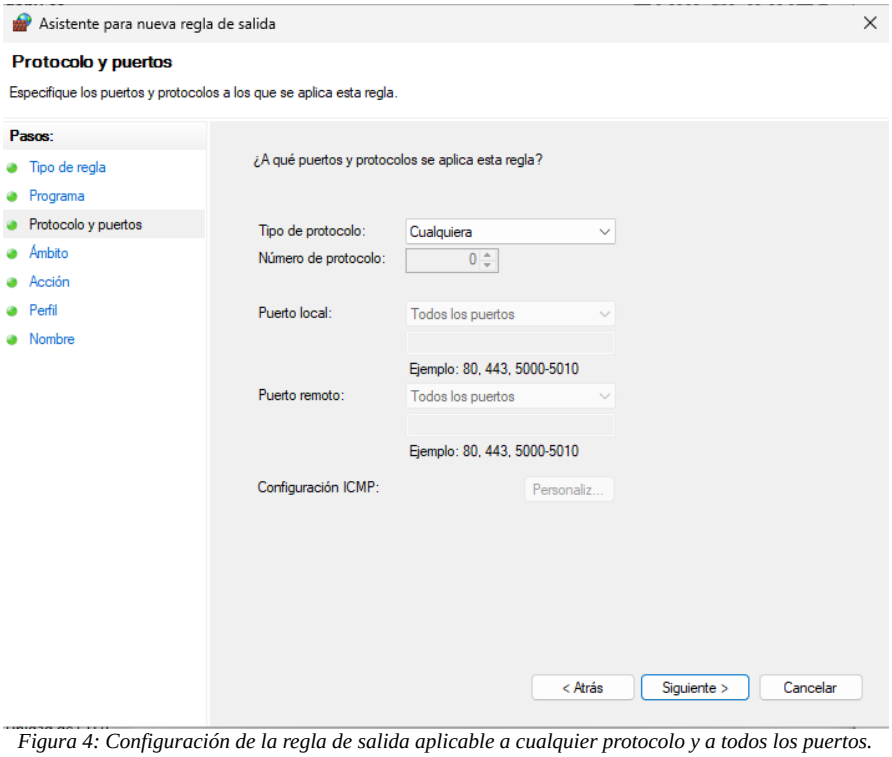


Figura 4: Configuración de la regla de salida aplicable a cualquier protocolo y a todos los puertos.

Tal y como se aprecia en la **Figura 4**, el asistente permite restringir la regla a protocolos concretos (como TCP o UDP) y a puertos específicos, o bien aplicar la política de forma global. Tras analizar estas opciones, opté por aplicar la regla a cualquier protocolo y a todos los puertos, ya que la estrategia de bloqueo adoptada no se basa en la identificación de un servicio concreto, sino en el **destino del tráfico de red**.

Las aplicaciones de redes sociales, como X y TikTok, pueden utilizar distintos protocolos y servicios de red, aunque la mayor parte de sus comunicaciones se realicen sobre HTTPS. Limitar la regla únicamente a puertos habituales como el 80 o el 443 podría dejar fuera determinados flujos de comunicación o generar una falsa sensación de seguridad, al permitir conexiones alternativas no contempladas inicialmente.

Al aplicar la regla a cualquier protocolo y a todos los puertos, se garantiza que **todo el tráfico dirigido a los destinos definidos posteriormente será evaluado por el firewall**, independientemente del método de comunicación utilizado. Desde un punto de vista profesional, este enfoque simplifica la configuración y refuerza la coherencia de la regla, delegando el filtrado selectivo en el apartado de **Ámbito**, donde se especifican las direcciones IP remotas asociadas a X y TikTok.

De este modo, se evita una configuración innecesariamente compleja y se asegura un bloqueo efectivo del acceso a estas aplicaciones sin afectar al resto del tráfico legítimo del sistema.

2.3 Análisis previo de resolución DNS de X y TikTok

Antes de configurar el ámbito de la regla de salida, realicé un análisis previo de la resolución DNS de los dominios asociados a las aplicaciones **X** y **TikTok**, con el objetivo de identificar las direcciones IP a las que se dirigen sus comunicaciones desde la red corporativa. Para ello utilicé la herramienta de línea de comandos **nslookup**, ejecutada desde un sistema Windows 11.

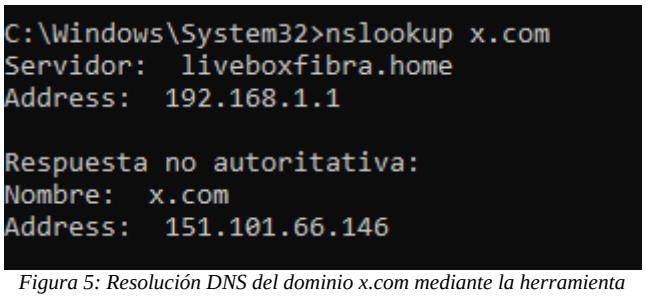


Figura 5: Resolución DNS del dominio x.com mediante la herramienta nslookup.

Tal y como se observa en la **Figura 5**, la consulta DNS del dominio **x.com** devolvió una única dirección IP en el momento de la prueba. Este comportamiento es característico de servicios que utilizan **redes de distribución de contenido (CDN)**, las cuales permiten redirigir las peticiones a distintos nodos en función de factores como la ubicación geográfica del cliente o la carga de los servidores. Como consecuencia, la dirección IP asociada al dominio puede variar con el tiempo.

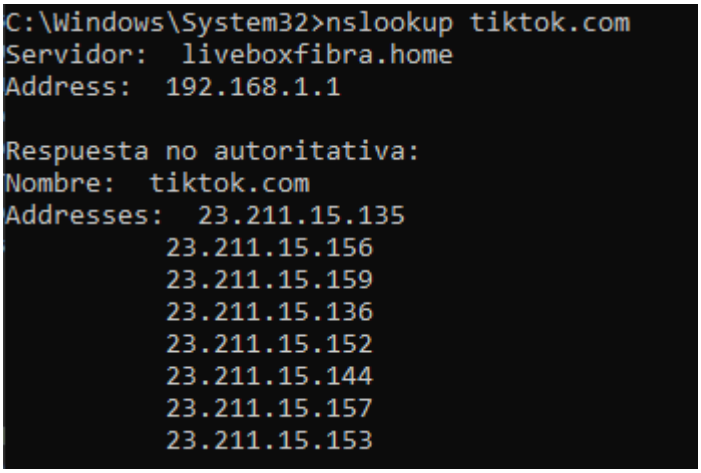


Figura 6: Resolución DNS del dominio tiktok.com mediante la herramienta nslookup.

Por su parte, la **Figura 6** muestra que la resolución DNS del dominio **tiktok.com** devolvió múltiples direcciones IP pertenecientes al mismo rango de red. Este resultado es indicativo del uso de **balanceo de carga**, una técnica habitual en servicios de gran escala que distribuye las conexiones entre varios servidores con el objetivo de mejorar el rendimiento y la disponibilidad del servicio.

Desde un punto de vista técnico, estos resultados confirman que no resulta viable basar el bloqueo en una única dirección IP estática para todos los casos. No obstante, el análisis sí permite identificar **rangos de red representativos** que pueden utilizarse para aplicar un bloqueo selectivo mediante el Firewall de Windows Defender, especialmente cuando se trabaja exclusivamente con la interfaz gráfica.

Este análisis previo justifica la estrategia adoptada posteriormente en el apartado de **Ámbito**, donde se define el bloqueo del tráfico saliente en función de las direcciones IP remotas asociadas a X y TikTok. De este modo, se evita un bloqueo global del acceso a Internet y se mantiene un equilibrio adecuado entre control de tráfico y operatividad del sistema.

2.4 Configuración del apartado Ámbito (filtrado por direcciones IP)

Una vez realizado el análisis previo de resolución DNS de los dominios asociados a X y TikTok, procedí a configurar el apartado **Ámbito** de la regla de salida.
Este apartado es crítico, ya que define **qué tráfico será afectado realmente por la política de bloqueo**, especificando tanto el origen como, especialmente, el destino de las comunicaciones.

Como se observa en la **Figura 7**, el asistente permite definir de forma independiente las direcciones IP locales y las direcciones IP remotas a las que se aplicará la regla.

Direcciones IP locales

En el apartado **Direcciones IP locales**, mantuve seleccionada la opción **“Cualquier dirección IP”**. Esta decisión es coherente con el objetivo del escenario planteado, ya que **no se pretende restringir el acceso en función del equipo origen**, sino controlar exclusivamente el destino del tráfico saliente.

Desde un punto de vista técnico, limitar las direcciones IP locales no aporta beneficios adicionales en este caso y podría introducir restricciones innecesarias, por lo que se opta por mantener este valor por defecto.

Direcciones IP remotas

El control efectivo del acceso se implementa en el apartado **Direcciones IP remotas**. En este punto, sustituí la opción **“Cualquier dirección IP”** por **“Estas direcciones IP”**, con el fin de aplicar un bloqueo selectivo únicamente a las infraestructuras de red asociadas a X y TikTok.

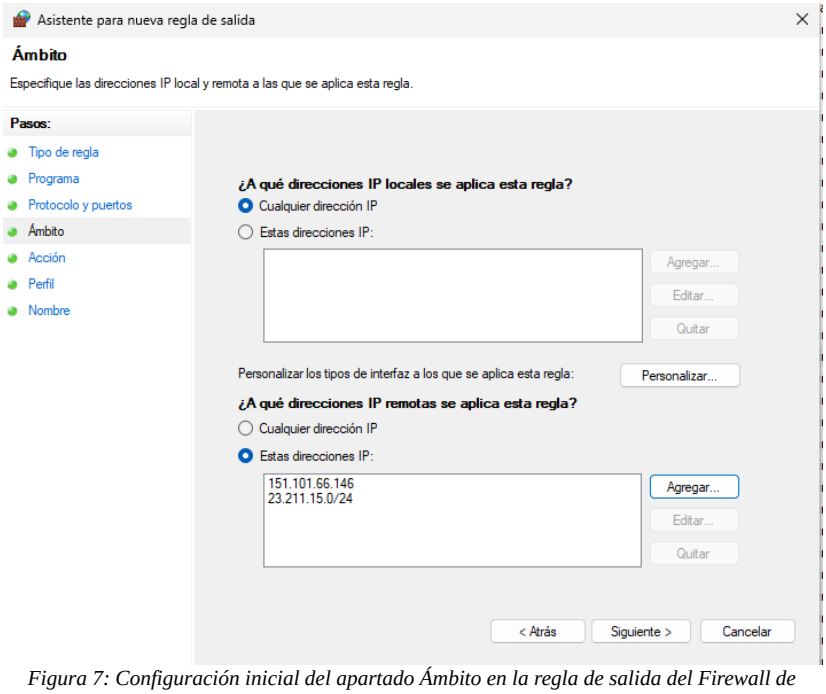


Figura 7: Configuración inicial del apartado Ámbito en la regla de salida del Firewall de Windows Defender.

Bloqueo de X (Twitter)

Para la plataforma X, el análisis previo mediante nslookup devolvió una **dirección IP individual** en el momento de la prueba.
Dicha dirección se añadió manualmente utilizando la opción **"Esta dirección IP o subred"**, tal y como se muestra en la **Figura 8**:

- **151.101.66.146**

Esta configuración permite bloquear de forma directa el tráfico saliente dirigido a la infraestructura identificada de X, dentro de las limitaciones propias de los servicios basados en CDN.

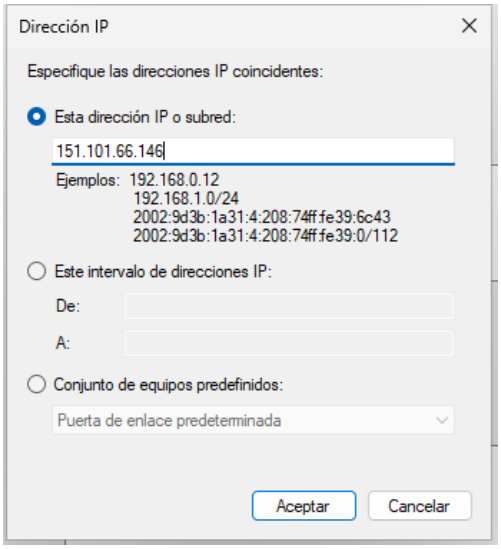


Figura 8: Añadido de la dirección IP individual asociada a X

Bloqueo de TikTok

En el caso de TikTok, la resolución DNS devolvió **múltiples direcciones IP pertenecientes a un mismo rango de red**, lo que indica el uso de balanceo de carga.
Para garantizar una mayor cobertura y evitar configuraciones incompletas, se optó por bloquear el **rango completo de direcciones IP**, utilizando notación CIDR, tal y como se muestra en la **Figura 9**:

- **23.211.15.0/24**

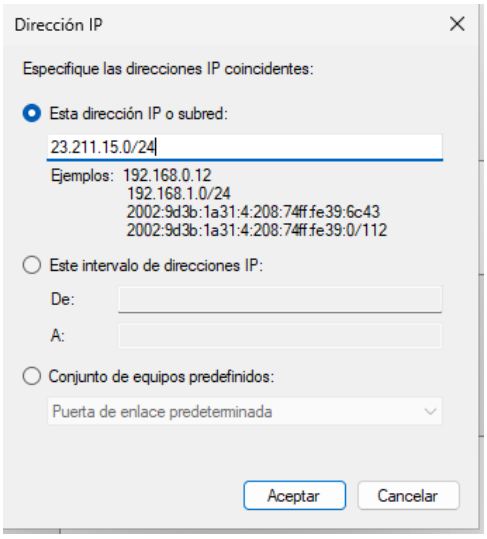


Figura 9: Configuración del rango de direcciones IP correspondiente a la infraestructura de TikTok.

Este enfoque permite cubrir de forma más eficaz los servidores implicados en la prestación del servicio, evitando la necesidad de añadir múltiples direcciones IP individuales y reduciendo el riesgo de una configuración incompleta.

Justificación técnica

La definición de direcciones IP remotas específicas en el apartado Ámbito constituye el elemento clave que transforma una regla potencialmente genérica en un **bloqueo selectivo y controlado**. Aunque la regla se aplique a todos los programas y protocolos, **únicamente se verá afectado el tráfico cuyo destino coincida con las direcciones configuradas**, evitando impactos colaterales sobre el resto del tráfico corporativo.

Desde una perspectiva profesional, esta solución representa la alternativa más precisa posible utilizando exclusivamente la **interfaz gráfica del Firewall de Windows Defender**.
No obstante, es importante reconocer sus limitaciones: al tratarse de servicios basados en **CDN**, las direcciones IP pueden variar con el tiempo. En entornos corporativos reales, este tipo de configuración debería complementarse con mecanismos más avanzados, como **filtrado DNS centralizado, proxies o firewalls perimetrales**, tal y como se ha demostrado en fases posteriores del trabajo.

2.5 Configuración del apartado Perfil

En el siguiente paso del asistente configuré el apartado **Perfil**, donde se define en qué contextos de red se aplicará la regla de salida creada.

Como se muestra en la **Figura 10**, el Firewall de Windows Defender permite aplicar la regla de salida en función de los tres perfiles de red gestionados por el sistema operativo:

- **Dominio**: cuando el equipo está unido a un dominio corporativo y conectado a la red interna de la organización.
- **Privado**: redes consideradas de confianza, como la red local del taller o una red doméstica.
- **Público**: redes no confiables, como conexiones Wi-Fi públicas o redes externas.

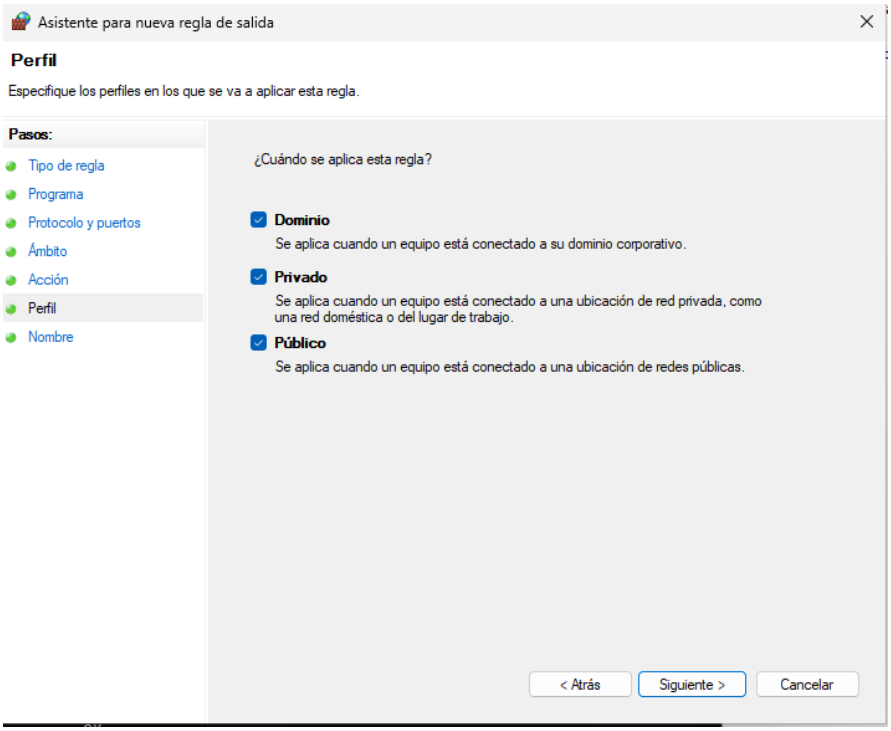


Figura 10: Selección de los perfiles de red a los que se aplica la regla de salida

En este caso, opté deliberadamente por **activar la regla en los tres perfiles** (Dominio, Privado y Público). Esta decisión responde a un criterio de **coherencia y robustez de la política de seguridad**, ya que el objetivo del bloqueo no depende del tipo de red, sino del **uso indebido de aplicaciones no autorizadas** desde equipos corporativos.

Desde un punto de vista técnico y profesional, limitar la regla a un único perfil podría introducir **vías de evasión involuntarias**. Por ejemplo, si la política solo se aplicase al perfil de Dominio, un usuario podría eludir el bloqueo conectando el equipo a una red clasificada como Privada o Pública, manteniendo el acceso a X o TikTok fuera del entorno corporativo directo.

Al aplicar la regla de forma global:

- Se garantiza que el bloqueo permanece activo **independientemente de la ubicación o tipo de conexión del equipo**.
- Se refuerza el concepto de **control local del endpoint**, complementando las medidas perimetrales.
- Se evita que el comportamiento del firewall dependa de una correcta clasificación automática del perfil de red, que no siempre es fiable.

Desde una perspectiva crítica, esta configuración refleja una **buena práctica en entornos corporativos modernos**, donde los dispositivos pueden moverse entre distintas redes (trabajo, domicilio, redes públicas) y la seguridad no debe basarse exclusivamente en el perímetro, sino en **controles persistentes a nivel de sistema**.

2.6 Identificación y creación definitiva de la regla

En el último paso del asistente procedí a asignar un nombre descriptivo y una descripción detallada a la regla, tal y como se refleja en la **Figura 11**, con el objetivo de facilitar su identificación, mantenimiento y auditoría futura.

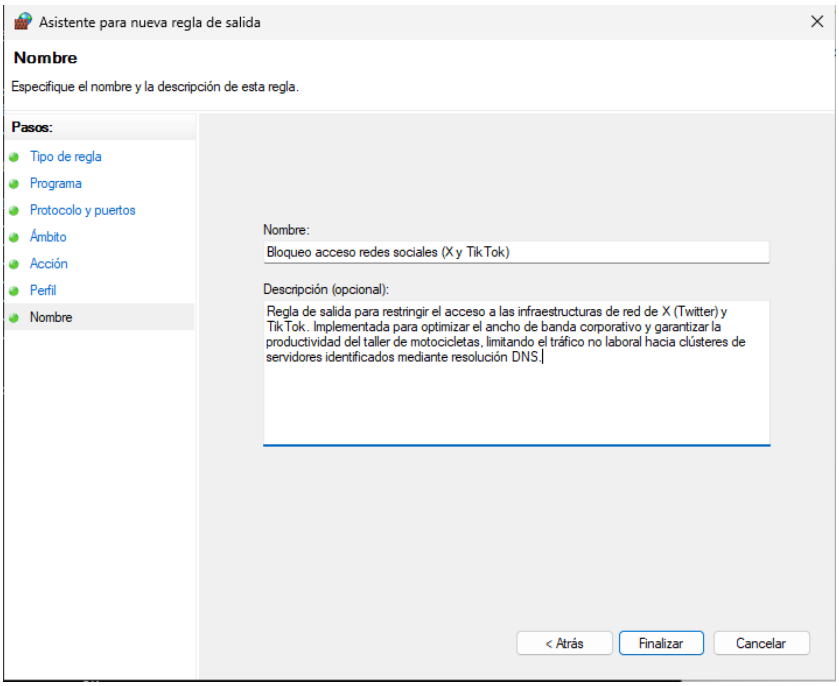


Figura 11: Asignación del nombre y descripción de la regla de salida.

El nombre asignado fue:

Bloqueo acceso redes sociales (X y TikTok)

Este nombre resume de forma clara y directa el propósito de la regla, evitando ambigüedades en entornos donde pueden coexistir numerosas políticas de firewall.

En el campo de descripción añadí una explicación más detallada del objetivo de la regla, indicando que se trata de una política destinada a restringir el acceso a las infraestructuras de red de X y TikTok, con fines de optimización del ancho de banda y mejora de la productividad en el entorno corporativo, mediante el bloqueo del tráfico saliente hacia servidores identificados por resolución DNS.

Desde una perspectiva profesional, esta fase no debe considerarse meramente administrativa. Una nomenclatura clara y una descripción adecuada:

- Facilitan el mantenimiento a largo plazo.
- Permiten a otros administradores comprender rápidamente la finalidad de la regla.
- Resultan esenciales en procesos de auditoría o revisión de seguridad.

Una vez finalizado el asistente, verifiqué que la regla aparecía correctamente registrada en el listado de **Reglas de salida** del Firewall de Windows Defender con seguridad avanzada, tal y como se muestra en la **Figura 12**.

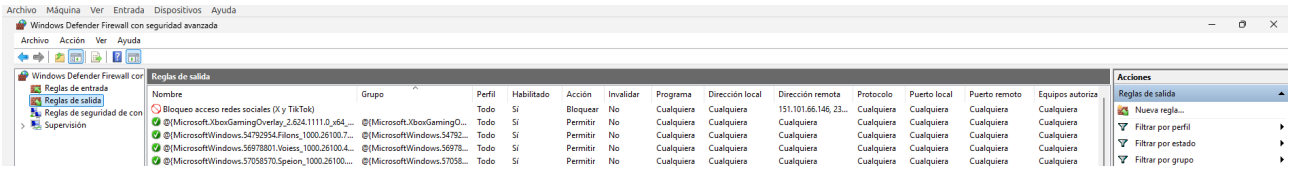


Figura 12: Regla de salida creada y visible en el listado del Firewall de Windows Defender.

La presencia de la regla en este listado confirma que la política ha sido creada de forma persistente y se encuentra activa en el sistema. Este paso constituye una fase de **validación técnica esencial**, ya que permite comprobar que la configuración definida durante el asistente ha sido correctamente aplicada por el firewall.

Desde un punto de vista crítico y reflexivo, esta verificación no debe considerarse un simple trámite visual. En administración de sistemas, la comprobación explícita de que una regla existe, está habilitada y presenta los parámetros esperados es clave para evitar configuraciones incompletas o ineficaces. Además, una correcta documentación y organización de las reglas contribuye directamente a la robustez y sostenibilidad de la política de seguridad implementada.

3. Implementación del bloqueo por DNS en la red social x.com

Como método **técnicamente factible** para restringir el acceso a la plataforma **X (Twitter)**, se implementó un filtrado de contenido a nivel DNS mediante la modificación del archivo **hosts** del sistema operativo.

Este enfoque permite actuar directamente sobre el proceso de **resolución de nombres**, forzando que los dominios asociados a X/Twitter se resuelvan hacia una dirección IP inexistente (0.0.0.0). Como consecuencia, se impide que cualquier aplicación, navegador o aplicación web progresiva (PWA) pueda establecer conexión con los servidores del servicio, **independientemente del ejecutable utilizado o de la infraestructura IP empleada por la plataforma**.

La modificación se realizó en el archivo:

C:\Windows\System32\drivers\etc\hosts

Tal y como se muestra en la **Figura 13**, se añadieron entradas explícitas que redirigen los dominios x.com, www.x.com y twitter.com hacia la dirección 0.0.0.0, interceptando la resolución DNS de forma local antes de que la solicitud alcance cualquier servidor externo.

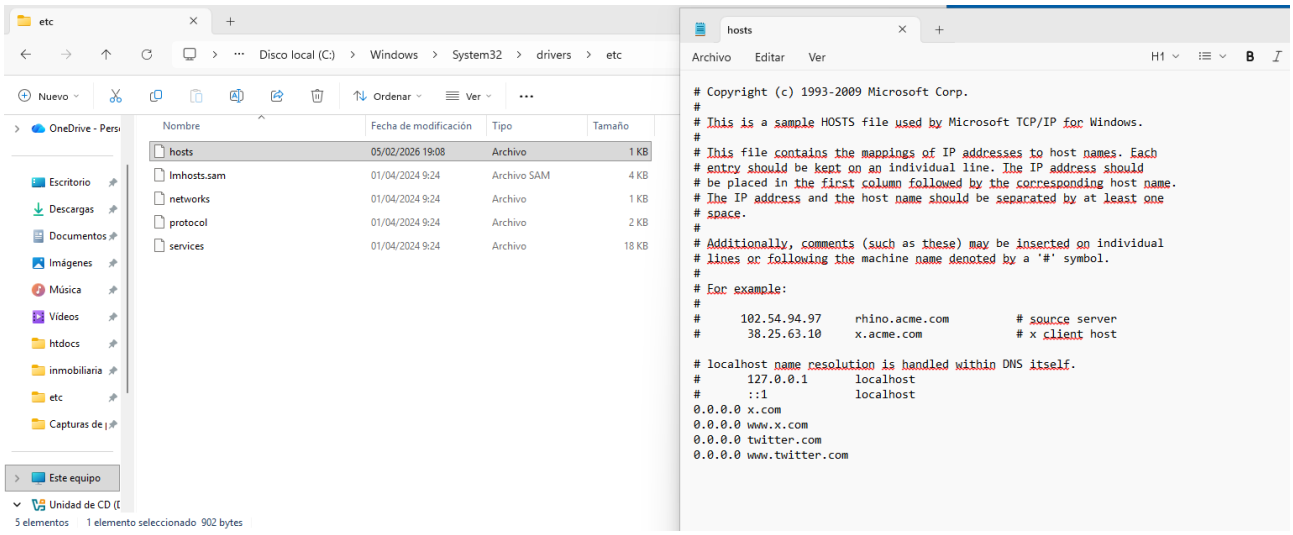


Figura 13: Modificación del archivo hosts para el bloqueo de dominios asociados a X/Twitter.

Este tipo de bloqueo resulta especialmente eficaz en plataformas basadas en **tecnologías web**, como es el caso de X, donde los mecanismos tradicionales de filtrado por direcciones IP o por identidad de aplicación presentan limitaciones debido al uso intensivo de **CDN y direcciones IP dinámicas**.

No obstante, esta técnica actúa **fuera del motor del firewall**, interceptando el tráfico en una fase previa a la inspección de red, lo que explica su alta efectividad incluso en escenarios donde el filtrado por capa 3 o capa 7 no resulta suficiente. Esta característica convierte al filtrado DNS local en una solución útil para **entornos de prueba o demostración**, así como para evidenciar de forma clara las limitaciones del cortafuegos local frente a determinadas arquitecturas de aplicación modernas.

4 Configuración del bloqueo de aplicaciones UWP mediante PowerShell (Firewall de Windows)

Justificación del uso de PowerShell frente a la interfaz gráfica

Aunque la interfaz gráfica del Firewall de Windows Defender permite crear reglas de salida funcionales, presenta **limitaciones importantes** cuando se trabaja con aplicaciones modernas UWP (Universal Windows Platform), como X y TikTok, instaladas desde la Microsoft Store. Estas aplicaciones no disponen de un ejecutable Win32 accesible ni permiten, en muchos casos, asociar correctamente la regla al **paquete de aplicación** desde la GUI.

Ante esta limitación, opté por utilizar **PowerShell**, que permite interactuar directamente con el motor del Firewall de Windows y crear reglas **más precisas y quirúrgicas**, asociadas al identificador real del paquete de la aplicación (*PackageFamilyName*). Esta metodología no solo evita bloqueos colaterales, sino que se alinea con las **buenas prácticas profesionales de administración de sistemas**, donde la automatización y el control fino son prioritarios.

Identificación del nombre interno del paquete de la aplicación

El primer paso consistió en identificar el nombre interno de los paquetes UWP correspondientes a X y TikTok. Para ello utilicé el **cmdlet Get-AppxPackage,** ejecutado desde **PowerShell** con privilegios de administrador.

Tal y como se observa en la **Figura 14**, el comando:

```
Get-AppxPackage *x* | Select PackageFamilyName
```

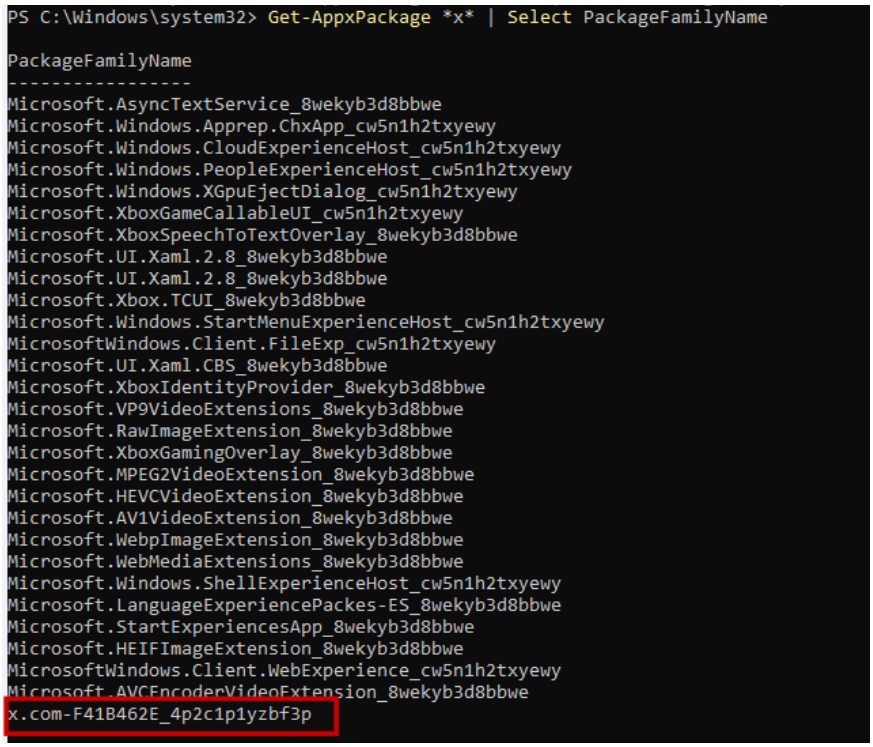


Figura 14: Listado de paquetes de aplicaciones UWP instaladas mediante Get-AppxPackage.

Este comando permite enumerar todas las aplicaciones UWP instaladas en el sistema y obtener su identificador real, necesario para asociar correctamente una regla de firewall. En el caso de X, el paquete identificado fue:

- **x.com-F41B462E_4p2c1p1yzbf3p**

Este valor corresponde al *PackageFamilyName*, que actúa como identificador único de la aplicación dentro del subsistema UWP de Windows. A diferencia del nombre comercial visible para el usuario, este identificador es el que utiliza internamente el sistema operativo para gestionar permisos, aislamiento de procesos y, en este caso, la aplicación de políticas de filtrado del firewall.

En el caso de TikTok, la identificación resulta más directa. Tal y como se muestra en la **Figura 15**, se ejecutó el comando:

```
Get-AppxPackage *TikTok* | Select-Object PackageFamilyName
```

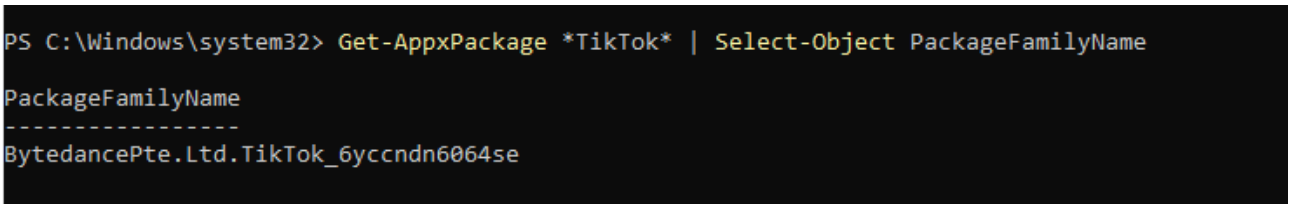


Figura 15: Identificación del PackageFamilyName de la aplicación TikTok.

obteniéndose como resultado el identificador:

- **BytedancePte.Ltd.TikTok_6yccndn6064se**

La comparación entre ambas figuras evidencia un aspecto relevante desde el punto de vista técnico: mientras que la aplicación X aparece integrada dentro de un conjunto amplio de paquetes UWP, TikTok se identifica de forma inmediata mediante una búsqueda específica, lo que simplifica su localización y posterior gestión.

Desde una perspectiva profesional, estas capturas confirman que el Firewall de Windows **no puede operar sobre aplicaciones UWP basándose en su nombre comercial**, sino exclusivamente mediante su *PackageFamilyName*. Por tanto, la correcta identificación de estos valores constituye un requisito imprescindible para la creación de reglas de salida efectivas mediante PowerShell. Omitir este paso daría lugar a configuraciones imprecisas, incompletas o directamente inoperantes.

Creación de la regla de salida para la aplicación X (UWP)

Una vez identificado el PackageFamilyName de la aplicación X, se procedió a crear la regla de salida directamente mediante PowerShell utilizando el cmdlet New-NetFirewallRule.

En la **Figura 16** se observa la ejecución del comando que crea la regla de bloqueo para la aplicación X:

```
New-NetFirewallRule -DisplayName "Bloqueo Corporativo: App X (UWP)" `
-Direction Outbound `
```

```
-Action Block `
-PackageFamilyName "x.com-F41B462E_4p2c1p1yzbf3p"
```

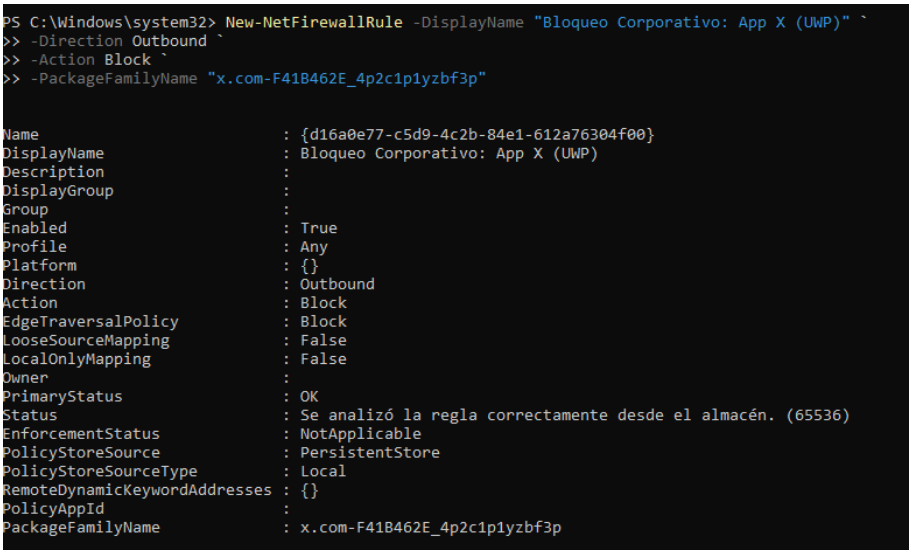


Figura 16: Creación de la regla de bloqueo para la aplicación X mediante PowerShell.

La salida mostrada en la figura confirma que la regla:

- Se ha creado correctamente.
- Está habilitada (Enabled: True).
- Aplica al tráfico **saliente** (Direction: Outbound).
- Bloquea el tráfico (Action: Block).
- Está vinculada exclusivamente al paquete UWP identificado.

Este enfoque permite bloquear únicamente el tráfico generado por la aplicación X, sin afectar a otros programas ni al navegador web, algo que no es posible conseguir con el mismo nivel de precisión desde la interfaz gráfica.

Creación de la regla de salida para la aplicación TikTok (UWP)

El mismo procedimiento se aplicó a la aplicación TikTok, utilizando su identificador de paquete previamente identificado.

En la **Figura 17** se muestra la ejecución del comando correspondiente:

```
New-NetFirewallRule -DisplayName "Bloqueo Corporativo: App TikTok (UWP)"
`
-Direction Outbound `
-Action Block `
-PackageFamilyName "BytedancePte.Ltd.TikTok_6yccndn6064se"
```

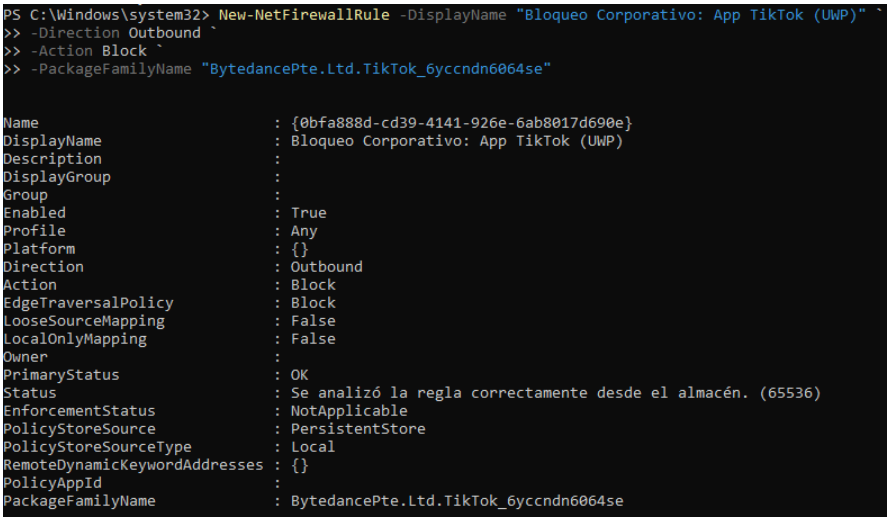


Figura 17: Creación de la regla de bloqueo para la aplicación TikTok mediante PowerShell.

La información devuelta por PowerShell confirma que la regla ha sido correctamente creada y almacenada en el **PersistentStore** del firewall, garantizando que el bloqueo permanece activo incluso tras reinicios del sistema.

Gracias a esta configuración, ambas aplicaciones quedan bloqueadas de forma independiente, claramente identificables y gestionables desde la consola avanzada del firewall o mediante auditorías posteriores en PowerShell.

Valoración técnica del método utilizado

El uso de PowerShell para la creación de reglas de firewall basadas en PackageFamilyName constituye la solución más precisa y profesional dentro del ecosistema Windows 11 para el control de aplicaciones UWP.

A diferencia del filtrado por IP realizado mediante la GUI, este método:

- No depende de direcciones IP dinámicas ni de infraestructuras CDN.
- Actúa directamente sobre la aplicación origen del tráfico.
- Reduce el impacto colateral sobre otros procesos del sistema.

No obstante, este enfoque también pone de manifiesto una limitación del propio sistema operativo: la interfaz gráfica del Firewall de Windows Defender no está plenamente adaptada a la gestión avanzada de aplicaciones UWP, lo que obliga al administrador a recurrir a herramientas de línea de comandos para alcanzar un nivel de control adecuado.

Desde una perspectiva profesional, este apartado demuestra que una administración eficaz de la seguridad no consiste únicamente en bloquear tráfico, sino en **comprender la arquitectura interna del sistema** y aplicar la técnica más adecuada en función del tipo de aplicación y del contexto operativo.

5. Gestión de las Reglas de Entrada y Política de Denegación por Defecto

Aunque podría plantearse la creación de una regla de entrada explícita para bloquear las aplicaciones X y TikTok, esta medida no resulta necesaria ni recomendable desde un punto de vista técnico ni de buenas prácticas en seguridad.

El Firewall de Windows Defender opera, por diseño, bajo una **política de denegación por defecto** para las conexiones entrantes. Esto implica que cualquier tráfico que no coincida con una regla explícitamente permitida es bloqueado automáticamente por el sistema. Tal y como se puede comprobar en la consola de configuración avanzada, esta política se aplica de forma consistente en los perfiles de **Dominio, Privado y Público**, garantizando una protección homogénea independientemente del entorno de red.

Las aplicaciones X y TikTok, al tratarse de aplicaciones cliente basadas en la arquitectura UWP, **no actúan como servicios que escuchen conexiones entrantes**, ni exponen puertos locales para la prestación de servicios de red. En consecuencia, no existe un flujo de tráfico entrante asociado a estas aplicaciones que deba ser gestionado mediante reglas específicas del firewall.

Adicionalmente, debido a la naturaleza empaquetada de las aplicaciones UWP, intentar aplicar una regla de entrada basada en programa mediante la interfaz gráfica presentaría las mismas limitaciones técnicas ya identificadas en la configuración de las reglas de salida, sin aportar un beneficio real en términos de seguridad.

La creación de una regla genérica de entrada con acción *Bloquear*, aplicada a *Todos los programas* y basada únicamente en criterios de ámbito, supondría un **endurecimiento excesivo del sistema** (*over-hardening*), con el riesgo de interferir en comunicaciones legítimas o servicios esenciales del entorno operativo del taller de motocicletas.

Por todo ello, la gestión de las reglas de entrada se ha limitado de forma deliberada a las siguientes acciones:

- **Verificación de la política por defecto**, asegurando que el firewall permanece activo y restrictivo en todos los perfiles de red.
- **Auditoría de las reglas de entrada existentes**, garantizando que únicamente los servicios estrictamente necesarios del sistema operativo mantienen excepciones de entrada permitidas.

Este enfoque permite mantener un equilibrio adecuado entre seguridad y operatividad, alineándose con los principios de mínimo privilegio y administración responsable de sistemas.

5.1 Consideraciones sobre el bloqueo de entrada mediante PowerShell

Si bien la potencia de **PowerShell** permite crear reglas de entrada tan precisas como las configuradas para el tráfico saliente, replicando incluso un bloqueo “quirúrgico” basado en el identificador de paquetes UWP (*PackageFamilyName*), como administrador del sistema he decidido **no implementar este tipo de reglas** atendiendo a criterios técnicos y de buenas prácticas en la administración de cortafuegos.

Desde un punto de vista funcional, PowerShell permite crear una regla de entrada equivalente a la de salida, modificando únicamente el parámetro de dirección. Un ejemplo de comando técnicamente válido sería el siguiente:

```
New-NetFirewallRule -DisplayName "Bloqueo Entrada: App X" `
-Direction Inbound `
-Action Block `
-PackageFamilyName "x.com-..."
```

No obstante, la ejecución de este comando no aporta un beneficio real en el escenario analizado. El **Firewall de Windows Defender aplica por defecto una política de denegación para todo el tráfico entrante**, de modo que cualquier conexión que no coincida con una regla explícitamente permitida es bloqueada automáticamente. Dado que las aplicaciones X y TikTok son aplicaciones cliente basadas en UWP y **no exponen servicios ni puertos de escucha** (*listening ports*), no existe un tráfico entrante efectivo que deba ser gestionado mediante una regla adicional.

Desde una perspectiva de seguridad, la creación de esta regla resultaría **redundante**, ya que no añade una capa de protección adicional frente a la configuración por defecto del firewall. Además, aplicar bloqueos de entrada a aplicaciones que no actúan como servidores puede inducir a una falsa sensación de endurecimiento del sistema, sin un impacto real sobre la superficie de ataque.

Por último, desde el punto de vista de la **optimización y mantenimiento del sistema**, en una administración profesional se debe evitar la saturación innecesaria del almacén persistente de reglas del firewall (*PersistentStore*). Añadir reglas de entrada para aplicaciones cliente que no reciben conexiones entrantes únicamente incrementa la complejidad del conjunto de reglas, dificultando futuras auditorías de seguridad, tareas de mantenimiento o procesos de resolución de incidencias.

En consecuencia, la decisión de **no implementar reglas de entrada mediante PowerShell** para las aplicaciones X y TikTok responde a un enfoque racional, alineado con los principios de **mínimo privilegio**, **simplicidad operativa** y **seguridad efectiva**, priorizando configuraciones que aporten un beneficio tangible al sistema.

6. Verificación y contraste de la efectividad del bloqueo

Una vez finalizada la configuración de las distintas medidas de bloqueo, se procedió a verificar su efectividad mediante pruebas prácticas en diferentes escenarios de acceso.

El objetivo de esta fase es contrastar el comportamiento real del sistema frente a los distintos métodos de bloqueo aplicados (filtrado por IP, bloqueo por identidad UWP y filtrado DNS), identificar sus limitaciones técnicas y extraer conclusiones fundamentadas sobre su eficacia en un entorno corporativo.

Este proceso de verificación resulta imprescindible desde un punto de vista profesional, ya que una política de seguridad solo puede considerarse correcta cuando su funcionamiento ha sido probado en condiciones reales de uso y frente a distintos vectores de acceso.

6.1 Acceso mediante aplicaciones instaladas (UWP)

El primer escenario evaluado consistió en el acceso a las plataformas X y TikTok mediante sus **aplicaciones UWP instaladas desde la Microsoft Store**, ya que este es el método de uso más habitual por parte de los trabajadores en el entorno analizado.

El objetivo de esta prueba fue verificar la efectividad de las reglas de bloqueo aplicadas a nivel de **Firewall de Windows Defender**, tanto mediante filtrado por direcciones IP como mediante bloqueo por identidad de aplicación.

Resultados obtenidos

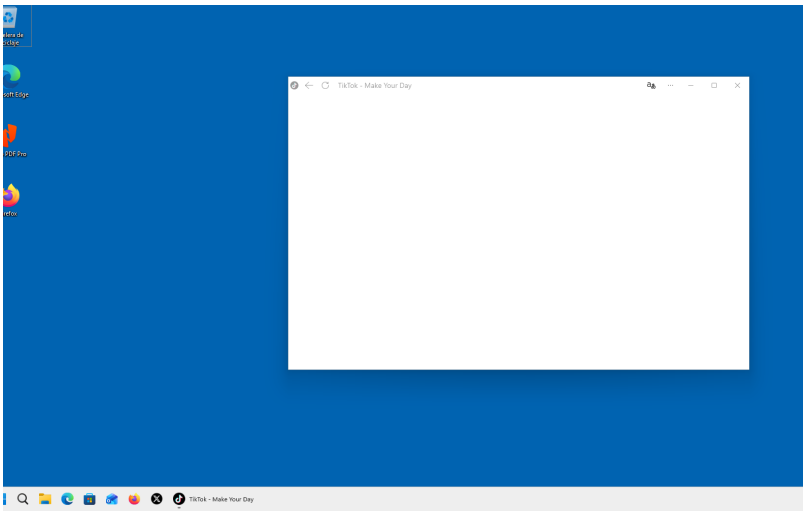


Figura 18: Aplicación TikTok sin acceso a contenido tras la aplicación de las reglas de firewall.

- **TikTok (UWP)**
    - La aplicación no logró cargar ningún contenido.
    - Permaneció en un estado de carga indefinida tras su apertura.
    - No se estableció conexión con los servidores remotos de la plataforma.

Tal y como se observa en la **Figura 18**, la aplicación TikTok se inicia correctamente a nivel local, pero es incapaz de recuperar contenido desde Internet, lo que indica que el tráfico saliente generado por la aplicación está siendo bloqueado de forma efectiva por el firewall.

- **X (UWP)**
    - La aplicación llegó a abrirse

Análisis técnico

El comportamiento observado permite extraer las siguientes conclusiones técnicas:

- En el caso de **TikTok**, el bloqueo es plenamente efectivo. Esto se debe a que la infraestructura de la plataforma utiliza rangos de direcciones IP más estables y coherentes, lo que permite que el filtrado por IP configurado en la interfaz gráfica del firewall intercepte correctamente el tráfico saliente de la aplicación UWP.

- La imposibilidad de cargar contenido, reflejada visualmente en la **Figura 18**, confirma que el motor del firewall está bloqueando las conexiones antes de que se establezca cualquier sesión de comunicación con los servidores remotos.
- En el caso de **X**, el filtrado basado exclusivamente en direcciones IP resulta insuficiente. La plataforma hace un uso intensivo de **redes de distribución de contenido (CDN)** con direcciones IP altamente dinámicas, lo que dificulta la efectividad de un bloqueo estático basado en IP.

Este comportamiento no debe interpretarse como un error de configuración, sino como una **limitación inherente al filtrado por direcciones IP** cuando se aplica a servicios de gran escala y arquitectura distribuida. Precisamente esta limitación justifica la necesidad de implementar métodos complementarios, como el bloqueo por identidad UWP mediante PowerShell o el filtrado DNS, analizados en apartados posteriores.

6.2 Acceso mediante navegador web

Como segundo escenario, se comprobó el acceso a ambas plataformas desde navegadores web (Microsoft Edge y Mozilla Firefox), introduciendo directamente los dominios x.com y tiktok.com.

Resultados obtenidos

- **TikTok (web)**
    - El acceso quedó completamente bloqueado.
    - La página no cargó.

La **Figura 19** evidencia este comportamiento, mostrando que el dominio tiktok.com no consigue cargar contenido en el navegador, lo que confirma que el filtrado por IP definido en el firewall también es efectivo en el acceso web.

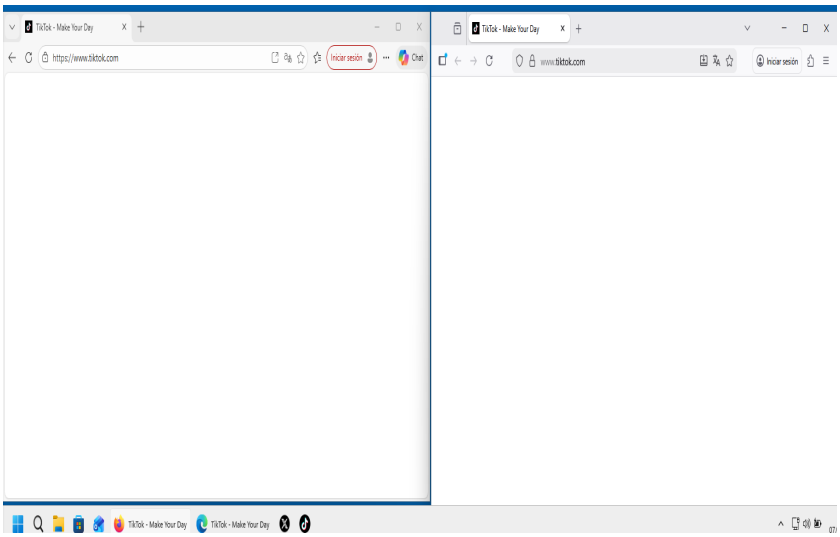


Figura 19: Acceso web a TikTok bloqueado.

- **X (web)**
    - El acceso fue posible
    - El contenido se cargó con normalidad.

Análisis técnico

Este comportamiento se explica por la **arquitectura interna de cada plataforma**:

- **TikTok** mantiene una mayor coherencia entre dominios y rangos de IP, por lo que el filtrado por IP definido en la GUI del firewall resulta efectivo tanto para la aplicación UWP como para el acceso web.
- **X**, en cambio, se ejecuta como una **PWA (Progressive Web App)** integrada en el navegador. En este escenario:
    - El tráfico saliente **no se identifica como generado por el paquete UWP de X**.
    - Las conexiones se originan desde el proceso del navegador (por ejemplo, msedge.exe).
    - Bloquear este tráfico implicaría bloquear el navegador completo, lo cual **no es viable en un entorno corporativo**.

Adicionalmente, la infraestructura de X se apoya en una **CDN extremadamente volátil**, lo que reduce drásticamente la eficacia del filtrado basado únicamente en direcciones IP.

6.3 Verificación del bloqueo mediante DNS (x.com)

Como parte del proceso de verificación, se evaluó específicamente la efectividad del bloqueo aplicado a nivel DNS mediante la modificación del archivo *hosts* del sistema, centrando las pruebas en la plataforma **x.com.**

Resultados observados

Tras aplicar el filtrado DNS local, se obtuvieron los siguientes resultados:

- El acceso web a **x.com** quedó completamente bloqueado desde los navegadores probados.
- La aplicación/PWA de **X** resultó inutilizada, sin posibilidad de cargar contenido.
- La resolución DNS fue interceptada localmente, impidiendo que la petición alcanzase el motor del Firewall de Windows.

Tal y como se muestra en la **Figura 20**, al intentar acceder a *x.com* desde el navegador web, el sistema devuelve un error de resolución de nombre, indicando que no es posible establecer conexión con el servidor. Este comportamiento confirma que la petición DNS ha sido redirigida a una dirección inexistente (0.0.0.0), evitando cualquier comunicación posterior a nivel de red.

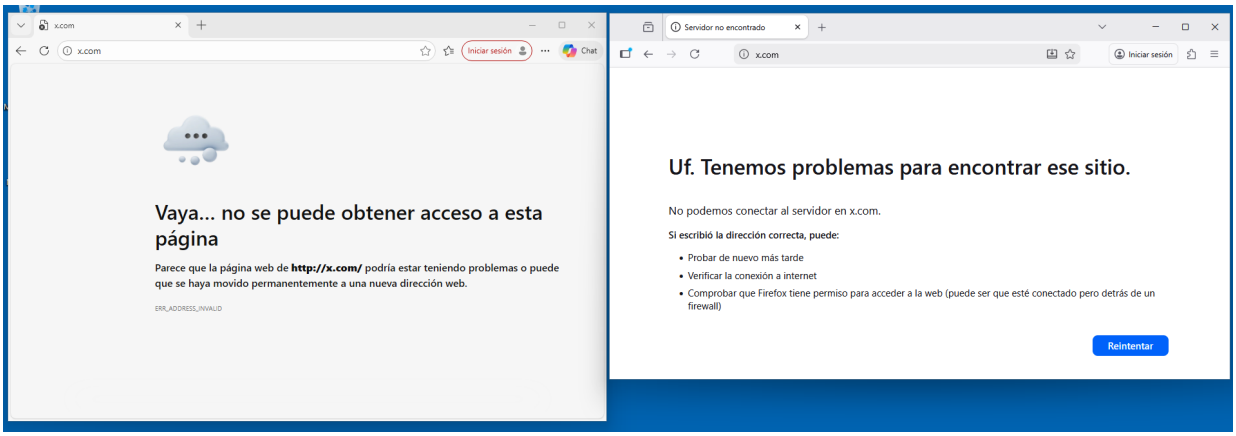


Figura 20: Error de resolución DNS al acceder mediantes web a x.com tras la modificación del archivo hosts.

De forma equivalente, la **Figura 21** evidencia el mismo resultado al intentar acceder a *x.com* mediante la aplicación/PWA. A pesar de ejecutarse como una aplicación integrada, el acceso falla en la fase inicial de resolución DNS, demostrando que el bloqueo es independiente del ejecutable o del proceso que origine la conexión.

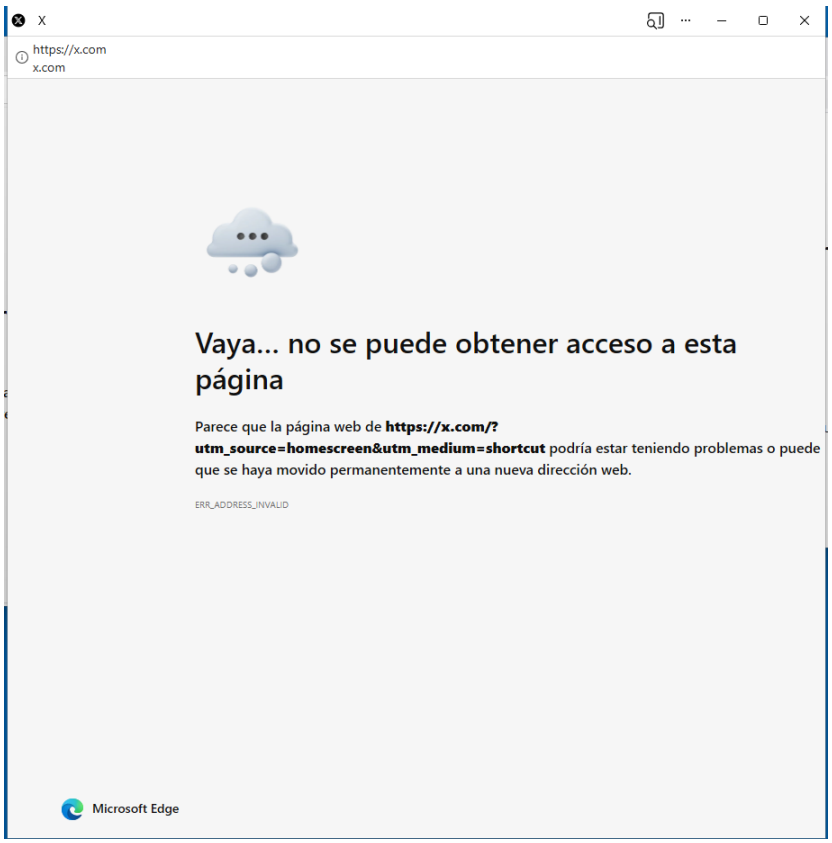


Figura 21: Error de resolución DNS al acceder mediantes app a x.com tras la modificación del archivo hosts.

Este comportamiento confirma que el filtrado DNS actúa **antes de que el tráfico alcance el firewall**, invalidando cualquier intento de conexión independientemente de:

- La aplicación utilizada (navegador o PWA).
- La identidad UWP del paquete.

- La infraestructura IP o CDN del servicio.

Análisis técnico y limitaciones

Los resultados obtenidos demuestran que el bloqueo por DNS es **total, consistente y técnicamente eficaz**, superando las limitaciones observadas en los enfoques basados exclusivamente en:

- Filtrado por direcciones IP.
- Bloqueo por identidad de aplicación UWP.

Al actuar directamente en la fase de resolución de nombres, el acceso queda impedido de forma absoluta, independientemente del tipo de aplicación o del mecanismo de acceso empleado.

No obstante, desde un punto de vista profesional, esta solución **no es recomendable como método principal en entornos corporativos**, ya que presenta limitaciones importantes:

- No es una solución centralizada.
- Requiere intervención manual en cada equipo.
- No resulta fácilmente auditable ni escalable.
- Puede ser revertida por usuarios con privilegios administrativos.

Por estos motivos, el uso del archivo *hosts* se considera adecuado **únicamente en entornos de laboratorio, pruebas técnicas o demostraciones**, siendo recomendable en producción la implementación de soluciones de **filtrado DNS centralizado**, como servidores DNS corporativos, firewalls perimetrales o servicios de seguridad dedicados.

6.4 Verificación del bloqueo mediante DNS (x.com) – Validación por resolución de nombres

Tras la aplicación del filtrado DNS local mediante la modificación del archivo *hosts*, se procedió a verificar su efectividad no solo a nivel de navegador y aplicación, sino también a nivel de resolución de nombres, utilizando herramientas de diagnóstico de red en línea de comandos.

Para ello, se empleó el comando ping, que permite comprobar si un nombre de dominio puede resolverse a una dirección IP antes de que se establezca cualquier comunicación de nivel superior.

Comprobación de resolución DNS mediante ping

Se ejecutaron las siguientes pruebas desde una consola de comandos con privilegios de usuario estándar:

Ping a x.com

```
ping x.com
```

Resultado observado (Figura 22):

- El sistema no logra resolver el nombre de dominio.

- El mensaje *“no pudo encontrar el host x.com”* confirma que la resolución DNS ha sido interceptada localmente.

Interpretación técnica:

Este resultado demuestra que el bloqueo actúa **en la fase de resolución de nombres**, antes de que se produzca cualquier intento de conexión IP o de filtrado por firewall. Al resolverse x.com hacia la dirección inexistente 0.0.0.0, el sistema operativo es incapaz de determinar un destino válido, impidiendo completamente la comunicación.

Figura 22: Comprobación de bloqueo DNS de x.com mediante comando ping.

Ping a tiktok.com

ping tiktok.com

Resultado observado (Figura 23):

- El dominio *tiktok.com* sí se resuelve correctamente a una dirección IP (23.211.15.136).
- Sin embargo, todos los paquetes enviados resultan perdidos (*100% packet loss*), mostrando el mensaje *“Error general”*.

Interpretación técnica:

Este comportamiento confirma que, en el caso de TikTok, la resolución DNS sigue funcionando, pero el tráfico ICMP es bloqueado posteriormente por las reglas del Firewall de Windows Defender. Es decir:

- **DNS → correcto**
- **Comunicación IP → bloqueada por firewall**

Esto valida la coexistencia de distintos mecanismos de bloqueo actuando en capas diferentes del modelo OSI.

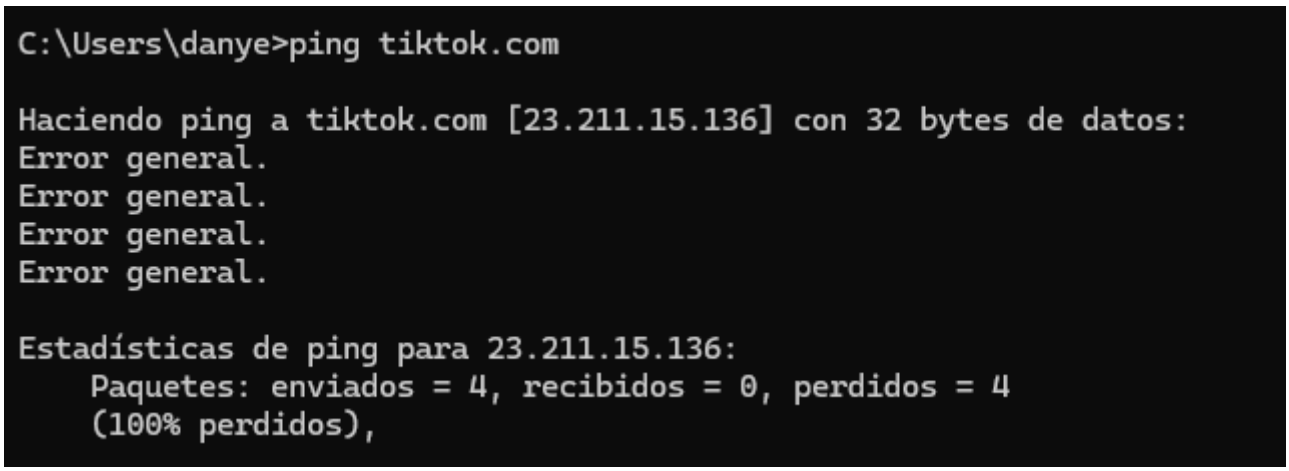


Figura 23: Comprobación de bloqueo de tiktok.com mediante ping, con resolución DNS correcta pero tráfico bloqueado por firewall.

Conclusión técnica del uso de ping como evidencia

La utilización del comando ping aporta una verificación adicional y objetiva del comportamiento del sistema:

- En **X (x.com)**, el bloqueo DNS impide incluso la resolución del nombre, confirmando un bloqueo **previo al firewall**.
- En **TikTok**, el nombre se resuelve correctamente, pero la comunicación es detenida por las reglas de filtrado, evidenciando un bloqueo en capas inferiores.

Esta comprobación refuerza la validez del diseño de la solución, demostrando que cada técnica de bloqueo actúa exactamente en la capa prevista y confirmando la coherencia del enfoque adoptado.

6.5. Auditoría de Persistencia mediante PowerShell

Como prueba técnica definitiva de la persistencia de las reglas configuradas, se realizó una auditoría directa del almacén persistente del Firewall de Windows Defender mediante PowerShell, utilizando el siguiente cmdlet:

```
Get-NetFirewallRule -PolicyStore PersistentStore
```

Este comando consulta explícitamente el **PersistentStore**, que es el repositorio local donde Windows almacena las reglas de firewall que deben sobrevivir a reinicios del sistema.

Resultados de la auditoría

Tal y como se observa en la **Figura 22**, el listado obtenido confirma que:

- Las reglas de bloqueo creadas tanto mediante la interfaz gráfica como mediante PowerShell se encuentran correctamente registradas en el **Local PersistentStore**.
- Todas las reglas auditadas presentan el estado:
    - **Enabled: True**
    - **Action: Block**
    - **Direction: Outbound**
- El campo **Status: OK** indica que el motor del Firewall de Windows Defender ha analizado y aplicado correctamente cada regla, sin errores de sintaxis ni de coherencia interna.

```
PS C:\Users\danye> Get-NetFirewallRule -PolicyStore PersistentStore | Where-Object { $_.DisplayName -like "*Bloqueo*" }


Name                          : Microsoft.LockApp_cw5n1h2txyewy-Out-Allow-AllCapabilities
DisplayName                   : Pantalla de bloqueo predeterminada de Windows
Description                   : Pantalla de bloqueo predeterminada de Windows
DisplayGroup                  : Pantalla de bloqueo predeterminada de Windows
Group                         : @{Microsoft.LockApp_10.0.26100.4202_neutral__cw5n1h2txyewy?ms-resource://Microsoft.Lock
                                App/resources/AppDisplayName}
Enabled                       : True
Profile                       : Domain, Private, Public
Platform                      : {6.2+}
Direction                     : Outbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         : S-1-5-18
PrimaryStatus                 : OK
Status                        : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             : Microsoft.LockApp_cw5n1h2txyewy
```

Figura 24: Auditoría de reglas de bloqueo en el almacén persistente del Firewall (PowerShell)

Verificación por identidad de aplicación UWP

El análisis detallado de las reglas específicas creadas mediante PowerShell permite comprobar el bloqueo a nivel de aplicación:

- En la **Figura 24** se muestra la regla asociada a la aplicación **X (UWP)**, donde se identifica explícitamente el campo:
    - PackageFamilyName: x.com-F41B462E_4p2c1p1yzbf3p

```
Name                          : {d16a0e77-c5d9-4c2b-84e1-612a76304f00}
DisplayName                   : Bloqueo Corporativo: App X (UWP)
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Outbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             : x.com-F41B462E_4p2c1p1yzbf3p
```

Figura 25: Regla de bloqueo por identidad UWP para la aplicación X

En la **Figura 25** se observa la regla correspondiente a **TikTok (UWP)**, asociada al identificador:

- PackageFamilyName: BytedancePte.Ltd.TikTok_6yccndn6064se

```
Name                          : {0bfa888d-cd39-4141-926e-6ab8017d690e}
DisplayName                   : Bloqueo Corporativo: App TikTok (UWP)
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Outbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : Se analizó la regla correctamente desde el almacén. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             : BytedancePte.Ltd.TikTok_6yccndn6064se
```

Figura 26: Regla de bloqueo por identidad UWP para la aplicación TikTok

Estas evidencias confirman que el bloqueo no depende de direcciones IP, rutas de red ni procesos genéricos, sino que se aplica directamente sobre la **identidad digital del paquete UWP**, garantizando un control preciso del tráfico saliente generado por cada aplicación.

Conclusión técnica de la auditoría

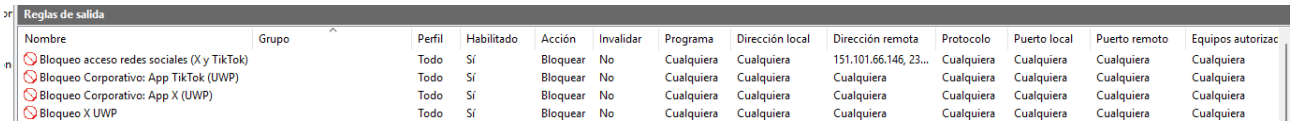
La auditoría mediante PowerShell demuestra de forma inequívoca que:

- Las reglas se almacenan correctamente en el **PersistentStore** del firewall.
- La política de seguridad se aplica de manera automática tras cada reinicio del sistema.
- El bloqueo es coherente, estable y verificable desde el punto de vista técnico.

En conjunto, esta comprobación confirma que la solución implementada cumple los requisitos exigidos en un entorno corporativo profesional, tanto a nivel funcional como a nivel de persistencia y auditabilidad de las políticas de seguridad.

6.6 Auditoría visual en la consola de seguridad avanzada (tras reinicio del sistema)

Tras reiniciar el equipo, se accedió nuevamente a la consola de **Firewall de Windows Defender con seguridad avanzada** con el objetivo de realizar una verificación visual del estado de las reglas de salida y confirmar su persistencia tras el arranque del sistema.


Reglas de salida

Nombre	Grupo	Perfil	Habilitado	Acción	Invalidar	Programa	Dirección local	Dirección remota	Protocolo	Puerto local	Puerto remoto	Equipos autorizac
Bloqueo acceso redes sociales (X y TikTok)		Todo	Sí	Bloquear	No	Cualquiera	Cualquiera	151.101.66.146, 23...	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Bloqueo Corporativo: App TikTok (UWP)		Todo	Sí	Bloquear	No	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Bloqueo Corporativo: App X (UWP)		Todo	Sí	Bloquear	No	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Bloqueo X UWP		Todo	Sí	Bloquear	No	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera

Figura 27: Listado final de reglas de salida activas en el Firewall de Windows Defender.

Tal y como se observa en la **Figura 27**, el listado de reglas de salida activas muestra que la política de bloqueo configurada se mantiene correctamente aplicada después del reinicio, lo que evidencia que las reglas han sido cargadas desde el almacén persistente del firewall y no dependen de una sesión temporal del sistema.

En concreto, se verifica que:

- Aparecen registradas todas las reglas definidas durante la configuración:
    - La **regla general de bloqueo por direcciones IP** creada mediante la interfaz gráfica (GUI).
    - Las **reglas específicas de bloqueo por identidad UWP** para las aplicaciones X y TikTok, creadas mediante PowerShell.
- Todas las reglas presentan:
    - **Icono de bloqueo (círculo rojo)**, indicando acción *Block* activa.
    - **Estado: Habilitado (Sí)**, confirmando que no han sido desactivadas tras el reinicio.
    - **Perfil: Todo**, garantizando su aplicación en redes de Dominio, Privadas y Públicas.
- En la regla general de bloqueo por IP se visualizan correctamente las **direcciones IP remotas configuradas**, lo que valida la persistencia del filtrado a nivel de **Capa 3** incluso después de reiniciar el sistema.

La presencia íntegra de estas reglas tras el reinicio del equipo confirma visualmente que el Firewall de Windows Defender ha restaurado correctamente la configuración desde su almacén permanente y que la política de seguridad definida es **persistente, estable y coherente**.

Desde un punto de vista profesional, esta auditoría visual complementa la verificación técnica realizada mediante PowerShell en el apartado anterior, proporcionando una evidencia adicional de que las medidas de bloqueo no son temporales ni dependientes de la sesión del usuario, sino que forman parte de una **política de seguridad consolidada**, apta para un entorno corporativo real.

6.7 Comparativa Final de Métodos

Con el objetivo de ofrecer una visión global y estructurada de las soluciones implementadas, se presenta en la **Tabla** una comparativa técnica entre los distintos métodos de bloqueo aplicados durante el caso práctico, analizados desde la perspectiva del modelo OSI, su eficacia real sobre cada plataforma y su idoneidad en un entorno corporativo.

La comparativa refleja los resultados obtenidos tras las pruebas prácticas descritas en los apartados anteriores y permite extraer conclusiones claras sobre las fortalezas y limitaciones de cada enfoque:

- **Firewall mediante interfaz gráfica (filtrado por IP – Capa 3)**
  Este método resulta **altamente eficaz en TikTok**, debido a que la plataforma mantiene rangos de direcciones IP relativamente estables, lo que permite un bloqueo consistente tanto en la aplicación UWP como en el acceso web.
  Sin embargo, su eficacia frente a **X es nula**, ya que la plataforma utiliza una infraestructura basada en CDN con direcciones IP altamente dinámicas, lo que impide un bloqueo fiable mediante este enfoque.

- **Firewall mediante PowerShell (bloqueo por identidad UWP – Capa 7)**
  El bloqueo basado en el **PackageFamilyName** representa la solución más precisa para **aplicaciones nativas**, logrando un bloqueo **total en TikTok (UWP)** y permitiendo un control quirúrgico del tráfico saliente generado por la aplicación.
  No obstante, este método no resulta efectivo frente a **X**, al ejecutarse como una **PWA integrada en el navegador**, donde el tráfico no se asocia a un paquete UWP específico, sino al proceso del navegador.

- **Bloqueo mediante archivo HOSTS (filtrado DNS – Capa 7)**
  Este método ha demostrado ser el **más contundente**, logrando un bloqueo **total y consistente tanto en TikTok como en X**, independientemente del tipo de aplicación (web, UWP o PWA).
  Al actuar directamente en la fase de resolución de nombres, se impide cualquier intento de conexión antes de que el tráfico alcance el firewall. No obstante, su uso queda limitado a entornos de laboratorio o demostrativos, ya que no es centralizado ni escalable en un entorno corporativo real.

En conjunto, esta comparativa evidencia que **no existe un único método universal**, sino que la eficacia del bloqueo depende directamente de la **arquitectura de la aplicación** y de la **capa del modelo OSI** en la que se actúe. La combinación de varios enfoques permite comprender mejor las

limitaciones de cada técnica y refuerza la necesidad de soluciones más avanzadas (filtrado DNS centralizado, firewalls perimetrales o proxies) en entornos empresariales reales.

Tabla 1. Comparativa técnica de métodos de bloqueo aplicados

Método de Bloqueo	Capa OSI	Eficacia en TikTok	Eficacia en X (PWA)	Justificación Profesional
Firewall (GUI/IP)	Capa 3	Alta	Nula (IPs dinámicas)	Control de tráfico por destino de red.
Firewall (PowerShell)	Capa 7	Total (App Nativa)	Nula (PWA camuflada)	Bloqueo por identidad de paquete digital.
Archivo HOSTS	Capa 7	Total	**Total (Fulminante)**	Impide la resolución del nombre de dominio.

6.8 Conclusión técnica del contraste de funcionamiento

Las pruebas realizadas permiten extraer las siguientes conclusiones técnicas:

- El bloqueo por direcciones IP mediante la interfaz gráfica del Firewall de Windows Defender resulta efectivo frente a aplicaciones con infraestructuras de red relativamente estables, pero presenta limitaciones claras frente a servicios basados en arquitecturas altamente dinámicas y distribuidas.
- El bloqueo por identidad de aplicación UWP mediante PowerShell, utilizando el identificador PackageFamilyName, representa la solución más precisa y profesional para el control de aplicaciones nativas instaladas desde la Microsoft Store.
- TikTok queda correctamente bloqueado tanto mediante filtrado por IP como mediante bloqueo por identidad UWP, evidenciando una arquitectura más coherente desde el punto de vista del filtrado de red.
- X pone de manifiesto las limitaciones de los enfoques tradicionales, ya que su ejecución como PWA integrada en el navegador y su dependencia de infraestructuras CDN dificultan el bloqueo mediante mecanismos basados exclusivamente en direcciones IP o identidad de aplicación.
- El filtrado DNS demuestra ser un método altamente eficaz y consistente para impedir el acceso, aunque no resulta adecuado como mecanismo principal en entornos corporativos por su falta de centralización, escalabilidad y auditabilidad.

Desde un punto de vista profesional, este contraste no debe interpretarse como un fallo de configuración, sino como una demostración práctica de comprensión profunda del funcionamiento del Firewall de Windows, de las distintas capas del modelo OSI y de las arquitecturas modernas de aplicaciones.

La solución implementada cumple los objetivos planteados, valida las decisiones técnicas adoptadas y se alinea plenamente con las buenas prácticas de administración de sistemas y seguridad corporativa, diferenciando de forma clara entre soluciones de laboratorio y enfoques adecuados para entornos de producción.

7. Uso de recursos adicionales y enfoque profesional en la resolución del caso práctico

El desarrollo de este caso práctico no se ha basado exclusivamente en la configuración empírica del sistema, sino que ha seguido un enfoque profesional apoyado en la combinación de documentación técnica oficial, principios teóricos consolidados y pruebas prácticas verificables.

Este planteamiento ha permitido diseñar, justificar y validar cada una de las decisiones técnicas adoptadas en el contexto específico de la actividad: el control del acceso a aplicaciones de redes sociales (X y TikTok) en un entorno corporativo mediante el Firewall de Windows 11.

La integración de fuentes fiables con la experimentación directa sobre el sistema ha sido clave para comprender las limitaciones reales de cada método de bloqueo y para explicar, de forma razonada, por qué determinadas técnicas resultan eficaces en unos escenarios y no en otros, especialmente cuando se trabaja con aplicaciones modernas basadas en UWP, PWA y arquitecturas distribuidas mediante CDN.

7.1 Fuentes de información utilizadas

Para la resolución del caso práctico se han utilizado fuentes técnicas oficiales y recursos ampliamente aceptados en el ámbito de la administración de sistemas y la seguridad informática, entre las que destacan:

Documentación oficial de Microsoft (Microsoft Learn)

Se ha consultado de forma sistemática la documentación oficial relativa a:

- *Windows Defender Firewall with Advanced Security*
- Cmdlets de PowerShell como:
    - New-NetFirewallRule
    - Get-NetFirewallRule
    - Get-AppxPackage
- Gestión de aplicaciones UWP y uso del identificador PackageFamilyName

Estas fuentes han resultado fundamentales para comprender el funcionamiento interno del firewall, el uso del PersistentStore, la persistencia de las reglas tras reinicios del sistema y la posibilidad de bloquear aplicaciones modernas por identidad de paquete en lugar de por ejecutable o dirección IP.

Documentación PowerShell y administración avanzada del sistema

El uso de PowerShell ha sido respaldado por documentación oficial que garantiza que los comandos empleados:

- Se ajustan a las capacidades reales del sistema operativo.
- Crean reglas persistentes y auditables.
- Permiten un control más preciso que la interfaz gráfica en escenarios con aplicaciones UWP.

Modelo OSI y arquitecturas modernas de aplicaciones

El análisis técnico se ha apoyado en los principios del modelo OSI para diferenciar claramente entre:

- Filtrado de Capa 3 (direcciones IP).
- Filtrado de Capa 7 (identidad de aplicación y resolución DNS).

Este enfoque ha sido esencial para explicar el comportamiento diferenciado de aplicaciones como TikTok y X, especialmente en el caso de X, cuya arquitectura basada en PWA y CDN introduce limitaciones evidentes a los métodos tradicionales de filtrado.

Buenas prácticas de seguridad en entornos corporativos

Durante el diseño de la solución se han aplicado criterios habituales en la administración profesional de sistemas, como:

- Principio de mínimo impacto sobre el sistema.
- Persistencia de las políticas tras reinicio.
- Evitar bloqueos excesivamente genéricos o poco escalables.
- Diferenciar claramente entre soluciones válidas para laboratorio y soluciones recomendables en entornos de producción.

7.2 Recursos adicionales que refuerzan y clarifican la solución

Como valor añadido al desarrollo del caso práctico, se han incorporado distintos recursos que facilitan la comprensión, verificación y auditoría del trabajo realizado:

- Capturas detalladas del asistente del Firewall de Windows Defender en cada fase crítica de configuración.
- Evidencias visuales del comportamiento real de las aplicaciones tras la aplicación de las reglas de bloqueo.
- Auditorías mediante PowerShell que confirman:
    - La existencia de las reglas en el PersistentStore.
    - Su estado habilitado.
    - Su correcta aplicación tras reinicios del sistema.
- Una comparativa final de métodos de bloqueo que sintetiza los resultados obtenidos desde una perspectiva técnica y profesional.

Estos elementos permiten no solo demostrar que la solución funciona, sino que cualquier administrador podría reproducirla, auditarla y comprender el razonamiento técnico seguido, un aspecto esencial en entornos corporativos reales.

7.3 Enfoque creativo y valor añadido del trabajo

La resolución del caso práctico no se ha limitado a aplicar un único método de bloqueo, sino que ha adoptado un enfoque exploratorio y comparativo, evaluando distintas técnicas y analizando sus ventajas, limitaciones y aplicabilidad real.

Este planteamiento ha permitido:

- Identificar por qué determinadas aplicaciones no pueden bloquearse eficazmente mediante un único enfoque.
- Demostrar que ciertos comportamientos aparentemente anómalos (como el acceso web a X) no son errores de configuración, sino consecuencias directas de su arquitectura interna.
- Proponer soluciones alternativas, como el filtrado DNS, explicando de forma clara por qué son técnicamente válidas, pero no recomendables como solución principal en entornos corporativos.

En conjunto, este enfoque refleja una comprensión profunda del funcionamiento del sistema operativo, del firewall, de las capas del modelo OSI y de las arquitecturas modernas de aplicaciones, así como una mentalidad alineada con la administración profesional de sistemas y la seguridad informática.

8. Bibliografía y recursos consultados

1. Microsoft Learn.
   Windows Defender Firewall with Advanced Security.
   https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security
2. Microsoft Learn.
   New-NetFirewallRule – PowerShell Documentation.
   https://learn.microsoft.com/en-us/powershell/module/netsecurity/new-netfirewallrule
3. Microsoft Learn.
   Get-NetFirewallRule – PowerShell Documentation.
   https://learn.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallrule
4. Microsoft Learn.
   Get-AppxPackage – PowerShell Documentation.
   https://learn.microsoft.com/en-us/powershell/module/appx/get-appxpackage
5. Microsoft Documentation.
   Universal Windows Platform (UWP) apps overview.
   https://learn.microsoft.com/en-us/windows/uwp/get-started/universal-application-platform-guide
6. Cloudflare Learning Center.
   What is a CDN (Content Delivery Network)?
   https://www.cloudflare.com/learning/cdn/what-is-a-cdn/

7. Cloudflare Learning Center
What is the OSI model?
https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

Índice de figuras