Instalación de un sistema de correo

La instalación de un sistema de correo es un proceso esencial para garantizar una comunicación eficiente, segura y adaptada a las necesidades de las organizaciones. En este apartado se presenta una guía completa para diseñar, implementar y configurar un sistema de correo electrónico. Esto incluye la selección de hardware y software, la instalación y configuración de servidores SMTP, POP/IMAP y webmail, así como la implementación de medidas de seguridad como el bastionamiento, filtros antivirus/antispam y autenticación de usuarios. También se abordan aspectos legales relacionados con la normativa vigente, asegurando el cumplimiento de los estándares.

Microsoft Exchange Server y Postfix son dos soluciones de servidor de correo electrónico que representan diferentes enfoques según las necesidades y el entorno operativo. Exchange Server, una plataforma de pago robusta, es ideal para grandes organizaciones que requieren herramientas avanzadas de colaboración, como gestión de calendarios, tareas y contactos, junto con funcionalidades de alta disponibilidad, integración con Microsoft 365 y protección avanzada contra amenazas. Por su parte, Postfix, una solución gratuita y ampliamente utilizada en sistemas Linux, se destaca por su estabilidad, flexibilidad y compatibilidad con protocolos estándar como SMTP. Es una opción preferida en entornos empresariales que buscan control total sobre la configuración y el rendimiento del servidor.

En los siguientes apartados, se desarrollarán los aspectos específicos de la configuración de un servidor de correo en dos sistemas operativos diferentes: Postfix en Linux y Microsoft Exchange Server en Windows, una solución gratuita y eficiente diseñada para pequeñas y medianas empresas que necesitan un servidor de correo funcional y fácil de configurar.

1. Diseño del sistema correo.

El diseño de un sistema de correo electrónico es una de las fases más críticas al implementar una solución de mensajería para una organización. Este proceso implica identificar las necesidades específicas de la organización, definir los recursos técnicos necesarios y garantizar que el sistema cumpla con las normativas legales aplicables.

1.1. Requisitos funcionales, operativos y de seguridad.

Como ya sabemos, al diseñar un sistema de correo electrónico, lo primero que debe determinarse son los requisitos que garantizarán que el sistema cumpla con las expectativas y necesidades de los usuarios. Estos requisitos se dividen en tres categorías principales: funcionales, operativos y de seguridad.

Requisitos funcionales

Los requisitos funcionales definen qué debe hacer el sistema de correo. Algunos ejemplos específicos incluyen:

- Capacidad de envío y recepción: El sistema debe poder gestionar el volumen esperado de correos electrónicos, ya sea decenas o miles al día.
- Soporte para adjuntos grandes: Si los usuarios necesitan enviar archivos de gran tamaño, el sistema debe permitirlo o integrarse con soluciones de almacenamiento en la nube.
- Compatibilidad con protocolos estándar: El sistema debe ser compatible con SMTP, POP3 e IMAP para garantizar que pueda integrarse con distintos clientes de correo.
- Acceso multiplataforma: Los usuarios deben poder acceder al correo desde ordenadores, tablets y teléfonos móviles.

Requisitos operativos

Los requisitos operativos definen cómo funcionará el sistema de correo en el día a día. Por ejemplo:

- Disponibilidad: Un servidor de correo debe garantizar una alta disponibilidad, idealmente del 99,9%, minimizando el tiempo de inactividad.
- Facilidad de mantenimiento: El sistema debe ser fácil de administrar, con herramientas claras para realizar actualizaciones, respaldos y resolución de problemas.
- Escalabilidad: Si la organización crece, el sistema debe poder adaptarse para soportar un mayor número de usuarios y correos.

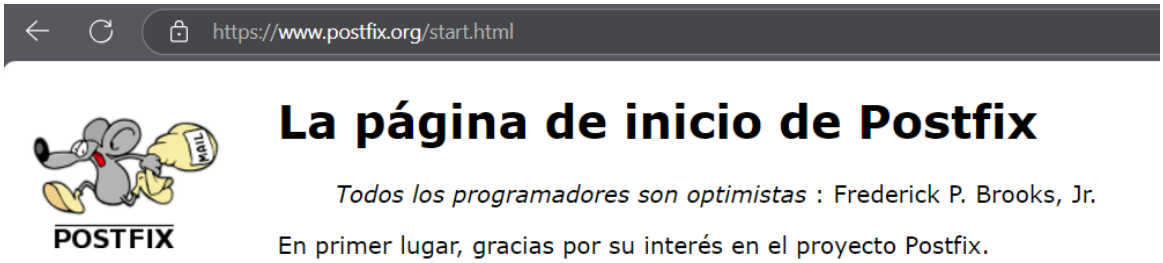
Requisitos de seguridad

La seguridad es un aspecto crítico en cualquier sistema de correo, ya que estos sistemas suelen ser un objetivo frecuente de ciberataques. Los requisitos de seguridad incluyen:

- Cifrado de extremo a extremo: Garantizar que los correos no puedan ser interceptados durante su envío.
- Filtros antispam y antivirus: Proteger a los usuarios contra correos no deseados y software malicioso.
- Autenticación fuerte: Implementar métodos como autenticación multifactor para proteger las cuentas de los usuarios.
- Cumplimiento de normativas de privacidad: El sistema debe cumplir con el Reglamento General de Protección de Datos (RGPD).

Por ejemplo, una empresa pequeña con 50 empleados necesitará un sistema que soporte 10.000 correos al mes, acceso desde dispositivos móviles, integración con herramientas de colaboración y un filtro de spam avanzado para evitar correos no deseados. En cambio, una organización con 1.000 empleados podría requerir un sistema más complejo con múltiples servidores y redundancia para garantizar la disponibilidad.

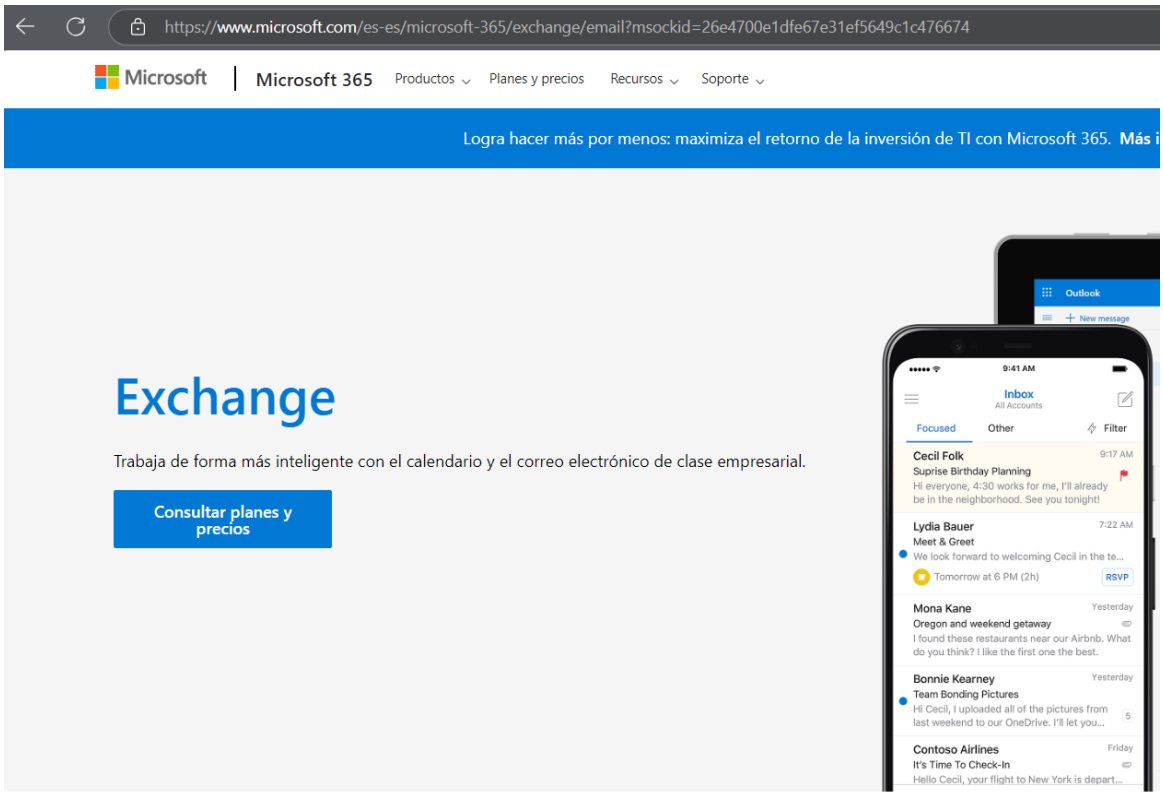
Postfix en Linux



Postfix en Linux es una solución ampliamente utilizada debido a su eficiencia, flexibilidad y coste (es gratuito). Se adapta tanto a pequeñas empresas como a grandes organizaciones.

- Funcionalidad:
  Postfix soporta SMTP y se puede integrar fácilmente con Dovecot para proporcionar acceso POP3 e IMAP. Esto garantiza la compatibilidad con cualquier cliente de correo como Thunderbird o Outlook. Además, permite configurar límites personalizados, como el tamaño máximo de adjuntos, y gestionar múltiples dominios.
- Operatividad:
  Postfix se puede configurar para ofrecer alta disponibilidad mediante redundancia, distribuyendo la carga entre varios servidores. Su mantenimiento es sencillo gracias a la gestión centralizada mediante archivos de configuración como main.cf y master.cf.
- Seguridad:
  Postfix incluye soporte para TLS, lo que permite cifrar la comunicación entre servidores y clientes. Además, se integra con herramientas como SpamAssassin para bloquear correos no deseados y ClamAV para proteger contra malware.

Microsoft Exchange Server en Windows



Microsoft Exchange Server es una solución integral para organizaciones que necesitan un sistema de correo avanzado con herramientas de colaboración.

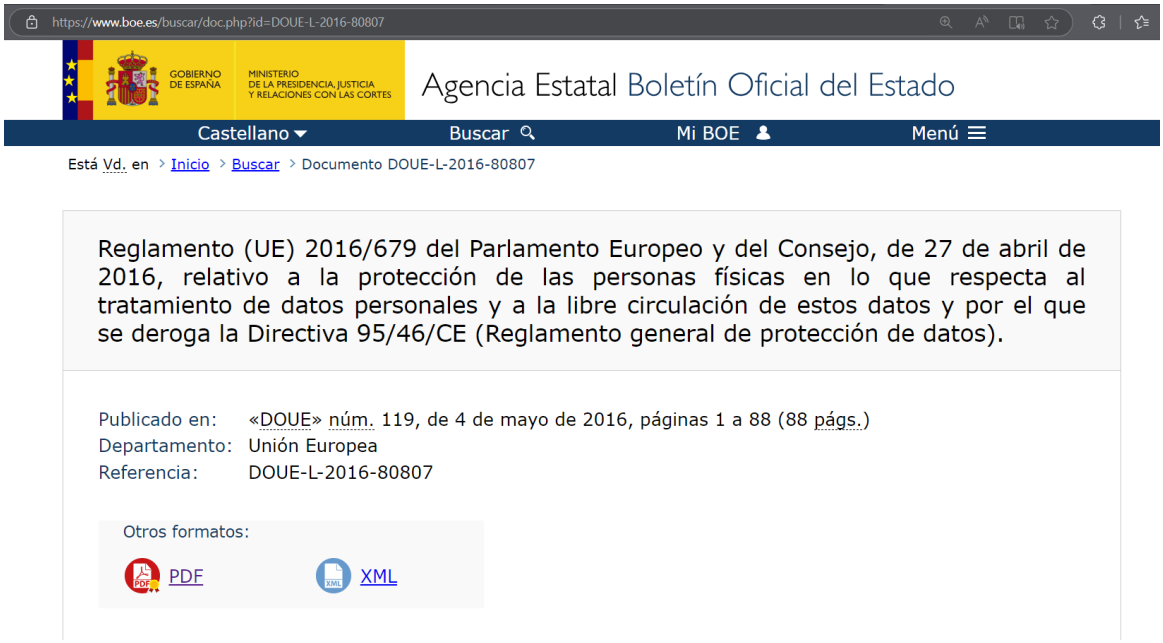
- Funcionalidad:
  Exchange permite gestionar correo, calendarios, tareas y contactos desde una única plataforma. Su integración con Outlook y Microsoft 365 ofrece una experiencia unificada. Además, soporta adjuntos grandes y permite configurar reglas avanzadas de filtrado.
- Operatividad:
  Exchange incluye soporte para alta disponibilidad mediante clustering, asegurando que el sistema funcione incluso si un servidor falla. También ofrece copias de seguridad automáticas para proteger los datos.

- Seguridad:
  Exchange implementa cifrado TLS y soporte para autenticación multifactor (MFA). Además, incluye protección avanzada contra amenazas como phishing y ransomware mediante Microsoft Defender.

1.2. Normativa legal.

En España, y en toda la Unión Europea, los sistemas de correo electrónico están sujetos a normativas legales diseñadas para proteger los datos personales y garantizar la seguridad de la información. Es imprescindible que cualquier sistema de correo cumpla con estas leyes para evitar sanciones y proteger los derechos de los usuarios.

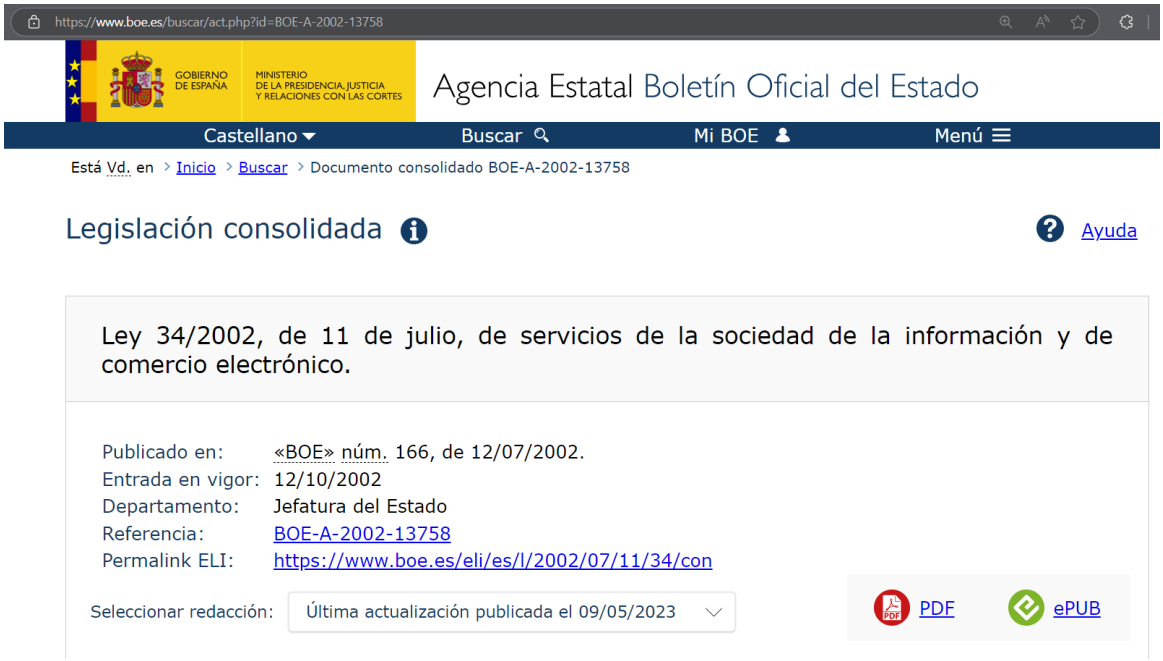
Reglamento General de Protección de Datos (RGPD)



El RGPD establece que cualquier sistema que gestione datos personales debe garantizar la privacidad y la seguridad de dichos datos. En el caso de los sistemas de correo electrónico, esto implica:

- Obtención del consentimiento: Si los correos contienen datos personales, como direcciones o nombres, los usuarios deben haber dado su consentimiento explícito para que se procesen.
- Protección de datos en tránsito: Implementar medidas como el cifrado TLS para proteger los correos mientras se envían.
- Derecho al olvido: Los usuarios tienen derecho a solicitar que se eliminen sus datos personales de los servidores.

Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE)



Esta normativa regula el envío de comunicaciones electrónicas con fines comerciales. Según la LSSI-CE:

- Los correos comerciales solo pueden enviarse a usuarios que hayan dado su consentimiento previo.
- Los correos deben incluir una forma clara y sencilla para que el receptor se dé de baja de futuras comunicaciones.

Responsabilidad del administrador del sistema

El administrador del sistema de correo es responsable de garantizar el cumplimiento de estas normativas. Esto incluye:

- Mantener registros de auditoría para demostrar el cumplimiento.
- Configurar el sistema para evitar usos indebidos, como el envío de correos masivos no autorizados.

Postfix en Linux

Postfix, al ser una solución de código abierto, permite configuraciones personalizadas para cumplir con normativas legales como el RGPD y la LSSI-CE:

Protección de datos personales:

Configurando TLS (smtpd_use_tls = yes), Postfix garantiza que los correos viajen cifrados. Además, los registros de actividad (/var/log/mail.log) permiten auditar quién envió y recibió correos.

Control de spam:

Postfix puede configurarse para rechazar correos de dominios sin registros SPF válidos, reduciendo el riesgo de suplantación.

Microsoft Exchange Server en Windows

Exchange Server está diseñado para cumplir con normativas legales como el RGPD y la LSSI-CE.

Protección de datos personales:

- Exchange cifra los datos en reposo y en tránsito mediante TLS. También permite auditar el acceso a las cuentas de correo, asegurando que los administradores puedan rastrear actividades sospechosas.

Cumplimiento con la LSSI-CE:

- Exchange permite configurar políticas de retención de datos para asegurarse de que los correos se gestionen de acuerdo con las leyes españolas.

1.3. Selección hardware y software.

La selección del hardware y software adecuado garantiza el funcionamiento eficiente y seguro del sistema de correo. Esto implica elegir servidores, sistemas operativos y software de gestión que se adapten a las necesidades específicas de la organización.

Hardware

El hardware necesario dependerá del tamaño y las necesidades de la organización. Para pequeñas empresas, un servidor básico con 8 GB de RAM y 500 GB de almacenamiento podría ser suficiente. Para grandes organizaciones, se necesitarán servidores más potentes con características como:

- Procesadores multinúcleo para manejar grandes volúmenes de correos.
- Almacenamiento redundante (RAID) para evitar la pérdida de datos.
- Fuentes de alimentación redundantes para garantizar la continuidad del servicio.
- Software de servidor de correo

Factores que deben considerarse en la selección

- Compatibilidad: Verificar que el software sea compatible con el sistema operativo y los clientes de correo utilizados por la organización.
- Escalabilidad: Asegurarse de que el software pueda manejar un aumento en el número de usuarios o correos.
- Coste: Evaluar si una solución de código abierto o una comercial es más adecuada en función del presupuesto.
- Soporte técnico: Las soluciones comerciales suelen incluir soporte técnico, mientras que las de código abierto pueden requerir más conocimientos técnicos por parte del administrador.

Postfix en Linux

- El hardware recomendado es:
  - Pequeñas empresas: Un servidor con 4 GB de RAM y un procesador de 2 núcleos.
  - Grandes organizaciones: Servidores con 16 GB de RAM, almacenamiento RAID y procesadores multinúcleo.

El software necesario es:

- Sistema operativo: Ubuntu Server o Debian.
- Complementos:
  - Dovecot: Para gestionar POP3 e IMAP.
  - SpamAssassin: Para filtrar spam.

- ClamAV: Para protección contra malware.

Microsoft Exchange Server en Windows

Hardware recomendado:

- Medianas empresas: Un servidor con 8 GB de RAM, almacenamiento SSD y un procesador de 4 núcleos.
- Grandes organizaciones: Un clúster de servidores con 32 GB de RAM, almacenamiento redundante y procesadores multinúcleo.

Software necesario:

- Sistema operativo: Windows Server 2019 o superior.

Complementos:

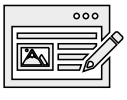
- Microsoft Defender for Office 365: Para protección avanzada contra phishing y malware.
- Microsoft 365: Para integración con otras herramientas de productividad.

Tabla de contextos en los que es mejor elegir Postfix o Microsoft Exchange

Situación	Postfix	Exchange
Una startup tecnológica con presupuesto ajustado necesita gestionar correos internos y externos.	Ideal, ya que es una solución de código abierto sin costes por licencias. Permite configurar POP3 e IMAP con herramientas gratuitas como Dovecot.	No recomendado, ya que requiere licencias costosas y un equipo de TI para la implementación y soporte continuo.
Una gran empresa multinacional requiere una solución centralizada con integración de herramientas de productividad.	Puede gestionar correos, pero carece de integración directa con herramientas como Microsoft 365. Podría no ser la mejor opción para grandes flujos colaborativos.	Ideal, ya que Microsoft Exchange Server se integra directamente con Microsoft 365, SharePoint y otras herramientas, ofreciendo una solución centralizada.
Una universidad necesita un servidor de correo para estudiantes, con gran volumen de usuarios y mensajes.	Recomendado, ya que puede manejar grandes volúmenes de correos si está configurado con hardware adecuado (RAID, procesadores multinúcleo) y herramientas antispam como SpamAssassin.	No recomendado si el presupuesto es ajustado, ya que los costes de licencias y hardware pueden ser elevados.
Una organización gubernamental busca un sistema de correo con máximo control de datos y seguridad.	Ideal, ya que al ser de código abierto, Postfix permite un control total sobre el servidor, la seguridad y la configuración sin depender de terceros.	No recomendado, ya que puede depender de servicios externos (por ejemplo, Microsoft 365) que podrían no cumplir con estrictos requisitos de soberanía de datos.
Una empresa mediana busca soporte técnico completo y soluciones rápidas a problemas de correo.	No recomendado, ya que requiere conocimientos técnicos avanzados para la configuración y el mantenimiento. El soporte depende de la comunidad.	Ideal, ya que Microsoft Exchange Server incluye soporte técnico oficial de Microsoft y opciones avanzadas para la gestión de problemas.
Una empresa pequeña necesita enviar correos masivos con configuraciones personalizadas.	Ideal, ya que permite personalizar totalmente el servidor y configurar sistemas para envío masivo mediante herramientas complementarias.	No recomendado, ya que no está diseñado para configuraciones altamente personalizadas ni para correos masivos sin licencias específicas.

Actividad 5

Si una organización cualquiera, no necesariamente grande pero tampoco pequeña, decide implementar un sistema que soporte tareas adicionales al correo básico sin exceder en funcionalidades, ¿cuál sería la solución más compatible en términos de presupuesto y escalabilidad, siempre y cuando se tenga en cuenta que puede requerir o no soporte técnico, dependiendo de las herramientas integradas o no integradas con el sistema principal?



2. Instalación del operativo del servidor.

La correcta instalación del sistema operativo en un servidor de mensajería electrónica es un paso fundamental para garantizar un entorno estable, eficiente y seguro. Este proceso implica seleccionar una configuración mínima que permita optimizar los recursos del servidor y aplicar medidas de securización (bastionamiento) para proteger el sistema contra posibles amenazas.

Esta etapa consiste en preparar el servidor con el sistema operativo que será la base para todas las aplicaciones y servicios que se ejecutarán en él. Un sistema operativo de servidor, como Windows Server, Ubuntu Server o CentOS, está diseñado específicamente para soportar tareas avanzadas como la gestión de usuarios, la virtualización, el almacenamiento de datos y, por supuesto, el funcionamiento de servicios como el correo electrónico.

Los objetivos principales son:

- Proporcionar el entorno base: El sistema operativo es el entorno donde se ejecutará el software del servidor. Es como instalar los cimientos de una casa antes de construir las habitaciones.
- Gestión de hardware: Permite que el servidor reconozca y utilice correctamente el hardware, como discos duros, procesadores y tarjetas de red.
- Configuración de red básica: Durante la instalación, se configura el acceso a la red, incluyendo parámetros como IP, puerta de enlace y servidores DNS.
- Seguridad inicial: Incluye configuraciones iniciales de cortafuegos, permisos de usuario y actualización de paquetes esenciales para proteger el sistema.

2.1. Instalación mínima.

La instalación mínima de un sistema operativo consiste en configurar el servidor únicamente con los paquetes esenciales y necesarios para su función principal, en este caso, gestionar la mensajería electrónica. Este enfoque tiene varias ventajas: reduce el uso de recursos, minimiza la superficie de ataque al eliminar software innecesario y facilita el mantenimiento al simplificar el sistema. Una instalación mínima también es ideal para servidores que requieren alto rendimiento o deben operar de manera continua sin interrupciones significativas.

Ventajas de la instalación mínima	
Reducción de recursos	El sistema utiliza menos memoria y procesamiento al instalar únicamente los paquetes esenciales.
Superficie de ataque minimizada	Menos software instalado reduce las posibles vulnerabilidades y puntos de ataque.
Facilidad de mantenimiento	Un sistema más simple es más fácil de administrar, actualizar y depurar.
Rendimiento mejorado	Es ideal para servidores que necesitan alta capacidad de respuesta y operación continua.
Operación continua	La instalación mínima minimiza las interrupciones, lo que es clave para servidores críticos.

Antes de instalar el software del servidor de mensajería electrónica, es imprescindible preparar el sistema operativo del servidor, que actúa como la base para todos los servicios. La selección del sistema operativo debe basarse en las necesidades específicas de la organización, como estabilidad, soporte técnico a largo plazo y facilidad de configuración. Tanto en entornos Linux como Windows, es posible optar por versiones optimizadas para servidores que prioricen el rendimiento y la seguridad.

En sistemas Linux, es recomendable elegir distribuciones ligeras y estables como Ubuntu Server o CentOS, que ofrecen soporte a largo plazo (LTS) y cuentan con herramientas robustas para la administración de servidores. Por ejemplo, Ubuntu Server 24.04.1 LTS es una opción comúnmente utilizada en entornos empresariales. Una vez descargada la ISO desde la página oficial, es necesario crear un medio de instalación, como un USB. Durante el proceso de instalación, se deben seleccionar únicamente los paquetes esenciales, evitando la instalación de entornos gráficos, ya que consumen recursos innecesarios y pueden complicar la gestión remota.

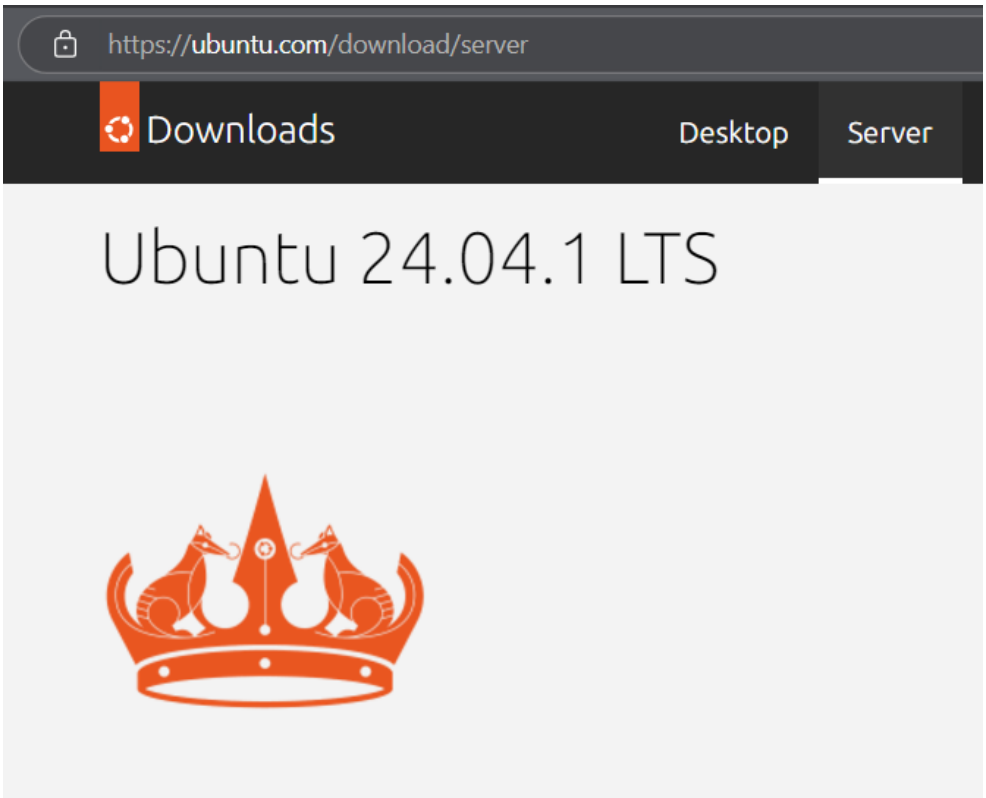
En el contexto de un servidor de correo, la instalación mínima implica que solo se incluyan los servicios necesarios para el correcto funcionamiento del sistema, como herramientas de red, utilidades básicas y dependencias específicas del software de mensajería (Postfix en Linux o Exchange en Windows).

Implementación de una instalación mínima

En Linux:

1. Seleccionar la distribución adecuada:

→ Elegir una distribución ligera y estable, como Ubuntu Server o CentOS, que ofrezca soporte de largo plazo (LTS). Descargar la ISO desde su página oficial y prepararla en un medio de instalación, como un USB.



Pie de imagen: Web de descarga de Ubuntu 24.04.1 LTS

2. Proceso de instalación:

→ Durante la instalación, elegir únicamente los paquetes esenciales. La mayoría de los instaladores de servidores ofrecen opciones como "Mínima" o "Servidor base".

→ Evitar instalar entornos gráficos (GUI), ya que consumen recursos innecesarios en servidores.

3. Configurar la red:

→ Asignar una dirección IP estática es un paso fundamental para garantizar que el servidor sea siempre accesible en la misma dirección dentro de la red. En las versiones modernas de Ubuntu Server, como la 18.04 y posteriores, esta configuración se realiza a través de Netplan, una herramienta que utiliza archivos YAML para definir el comportamiento de las interfaces de red. Por ejemplo, el archivo /etc/netplan/01-netcfg.yaml puede modificarse para especificar una IP estática, como se muestra a continuación:

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

Sabías que…

Un servidor, como el que usaremos para un sistema de mensajería electrónica, necesita una dirección IP fija (o estática) para que otros dispositivos puedan localizarlo siempre en la misma dirección dentro de la red. Si usamos una IP dinámica (asignada automáticamente por DHCP), esa dirección puede cambiar, lo que causaría problemas, especialmente en servicios como DNS o correo electrónico, que requieren estabilidad en la red.

Por ejemplo, supongamos que configuramos un servidor de correo con una dirección dinámica. Hoy podría tener la dirección 192.168.1.10, pero mañana el router podría asignarle 192.168.1.20, rompiendo las configuraciones de DNS o haciendo inaccesible el servidor desde otras máquinas.

¿Qué es el archivo /etc/netplan/01-netcfg.yaml?

En las versiones modernas de Ubuntu (como Ubuntu Server 18.04 y posteriores), la configuración de red se realiza a través de Netplan, una herramienta que utiliza archivos YAML para definir cómo se comportarán las interfaces de red.

El archivo /etc/netplan/01-netcfg.yaml es donde se define la configuración de la red, como las direcciones IP, las puertas de enlace (gateway) y los servidores DNS. Este archivo es clave para asignar una IP estática.

¿Cómo configurar una IP estática?

- Editar el archivo de configuración:
  Abre el archivo /etc/netplan/01-netcfg.yaml (o el archivo YAML correspondiente en tu servidor, ya que puede variar ligeramente el nombre). Usa un editor como nano:

```
sudo nano /etc/netplan/01-netcfg.yaml
```

- Configurar la red:
  Modifica el contenido del archivo para que tenga una estructura similar a esta (adaptando las direcciones IP a tu red):

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.10/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
```

- Desglose del contenido:
  - version: 2: Especifica la versión de configuración de Netplan.
  - ethernets: Define las interfaces de red, en este caso, enp0s3 (el nombre puede variar en tu máquina; usa ip addr para verificar el nombre de tu interfaz).
  - dhcp4: no: Desactiva el DHCP, ya que asignaremos una IP manualmente.
  - addresses: Aquí defines la IP estática, junto con su máscara de red (/24 equivale a 255.255.255.0).
  - gateway4: Es la puerta de enlace predeterminada, normalmente la dirección del router.
  - nameservers: Especifica los servidores DNS. En este ejemplo usamos los públicos de Google (8.8.8.8 y 8.8.4.4).

4. Aplicar los cambios:

→ Esta configuración asegura que el servidor tenga una dirección fija, evitando problemas con servicios como DNS o correo electrónico, que requieren estabilidad. Por ejemplo, si el servidor usara una IP dinámica y esta cambiara, otros dispositivos no podrían localizarlo, interrumpiendo los servicios. Una vez configurado el archivo YAML, los cambios se aplican ejecutando el comando:

```
sudo netplan apply
```

5. Actualizar el sistema:

→ Mantener el sistema actualizado es esencial para evitar vulnerabilidades. Ejecutar:

```
sudo apt update && sudo apt upgrade
```

En Windows:

1. Preparar el servidor:
2. Descargar e instalar Windows Server 2019 o 2022 en su modo "Server Core" para una instalación mínima sin interfaz gráfica, lo que reduce el uso de recursos.

Anotación

Server Core es una opción de instalación disponible en algunas versiones de Microsoft Windows Server. Se trata de una versión mínima del sistema operativo diseñada para ofrecer un entorno de servidor optimizado y seguro, eliminando las características no esenciales, como la interfaz gráfica de usuario (GUI). Esta opción está pensada para reducir la superficie de ataque, mejorar el rendimiento y minimizar los requisitos de mantenimiento, como las actualizaciones.

3. Durante la instalación, elegir la opción "Server Core (sin experiencia de escritorio)".
4. Configuración básica mediante sconfig:
5. Asignar una IP estática.
6. Configurar el nombre del equipo.
7. Instalar actualizaciones y habilitar roles básicos como DNS si se requiere.
8. Instalar herramientas esenciales.
9. Si es necesario, habilitar funcionalidades mínimas para la administración remota, como PowerShell y herramientas de gestión remota (RSAT).

Actividad 6

Relaciona cada elemento del Grupo A con su correspondiente descripción o acción en el Grupo B.

Grupo A: Conceptos y acciones

Instalación mínima

Configuración básica de red

Server Core

Archivo /etc/netplan/01-netcfg.yaml

Asignar una IP estática

Actualizar el sistema

Selección de distribución Linux

Habilitar roles básicos (Windows)

Aplicar configuraciones en Netplan

Interfaz gráfica (GUI)

Grupo B: Descripciones

A. Configuración en Windows Server que permite optimizar el sistema eliminando la interfaz gráfica y características no esenciales para mejorar el rendimiento y reducir la superficie de ataque.

B. Seleccionar Ubuntu Server o CentOS como opción ligera y estable, con soporte a largo plazo (LTS) y herramientas robustas para administración.

C. Archivo YAML utilizado en distribuciones modernas de Ubuntu para definir el comportamiento de las interfaces de red, como la asignación de una dirección IP fija.

D. Configuración que garantiza que el servidor tenga siempre la misma dirección dentro de la red, asegurando la estabilidad de servicios como DNS y correo electrónico.

E. Proceso de instalar solo los paquetes esenciales necesarios para que el servidor cumpla su función principal, evitando la inclusión de software innecesario que consuma recursos.

F. Proceso de ejecutar el comando sudo netplan apply para activar la configuración definida en el archivo /etc/netplan/01-netcfg.yaml.

G. Acción recomendada después de la instalación del sistema operativo para corregir vulnerabilidades conocidas y garantizar la seguridad.

H. Configuración realizada durante la instalación de Windows Server para asignar una IP fija, configurar el nombre del servidor y habilitar servicios mínimos como DNS.

I. Interfaz de usuario eliminada en instalaciones mínimas para servidores, ya que consume recursos innecesarios y complica la gestión remota.

J. Parámetro que se configura durante la instalación del sistema operativo para definir el acceso a la red del servidor, incluyendo IP, puerta de enlace y servidores DNS.

2.2. Securización (bastionamiento).

El bastionamiento es el proceso de reforzar la seguridad del servidor mediante configuraciones específicas que minimicen la exposición a vulnerabilidades. En servidores de correo, que suelen ser objetivos frecuentes de ataques como spam, suplantación de identidad y malware, el bastionamiento es especialmente importante para proteger tanto el servidor como la información confidencial gestionada en él.

Las técnicas de bastionamiento incluyen:

- Deshabilitar servicios innecesarios.
- Configurar cortafuegos para limitar el acceso a puertos esenciales.
- Aplicar políticas de seguridad como restricciones de acceso y cifrado de datos.

Aplicación de bastionamiento en Linux (Postfix)

En servidores Linux, el bastionamiento se centra en proteger los puntos de entrada del sistema, como los servicios abiertos, las conexiones remotas y la configuración del software.

1. Configurar un firewall:

→ Un firewall es fundamental para controlar el acceso a los puertos del servidor. En Postfix, solo se deben abrir los puertos esenciales, como SMTP (25 y 587) para el envío de correos y, si es necesario, POP3/IMAP (110, 143, 993) para la recepción. Una herramienta comúnmente utilizada en distribuciones como Ubuntu Server es ufw (Uncomplicated Firewall), que se puede configurar fácilmente:

```
nsudo apt install ufw
sudo ufw allow 25,587/tcp
sudo ufw enable
```

2. Proteger SSH:

→ El acceso remoto mediante SSH debe configurarse de manera segura para evitar accesos no autorizados. Esto incluye deshabilitar el inicio de sesión como root y habilitar la autenticación por claves públicas. Estas configuraciones se realizan en el archivo /etc/ssh/sshd_config:

```
PermitRootLogin no
PasswordAuthentication no
```

→ Una vez realizadas estas modificaciones, es necesario reiniciar el servicio SSH:

```
sudo systemctl restart ssh
```

3. Instalar fail2ban:

→ Fail2ban es una herramienta que protege el servidor contra ataques de fuerza bruta, como intentos repetidos de acceso no autorizado. Monitorea los registros del sistema y bloquea automáticamente las direcciones IP sospechosas. Se instala con:

```
sudo apt install fail2ban
```

Y se configura para proteger servicios como SSH y Postfix.

4. Cifrado de comunicaciones:

→ Configurar TLS (Transport Layer Security) en Postfix asegura que las comunicaciones entre servidores de correo estén cifradas. Esto se logra añadiendo los siguientes parámetros al archivo /etc/postfix/main.cf:

```
smtpd_tls_cert_file=/etc/ssl/certs/server.crt
smtpd_tls_key_file=/etc/ssl/private/server.key
smtpd_use_tls=yes
```

Aplicación de bastionamiento en Windows (Exchange Server)

En entornos Windows, el bastionamiento se enfoca en configurar el firewall, proteger los datos almacenados y asegurar las comunicaciones de Exchange Server.

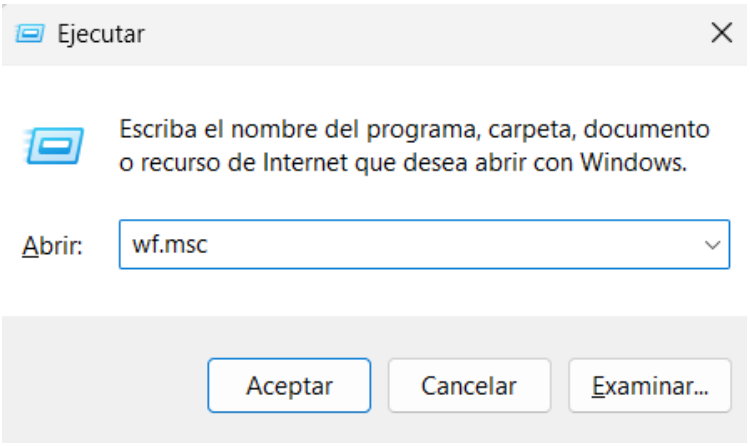
Configurar el firewall de Windows:

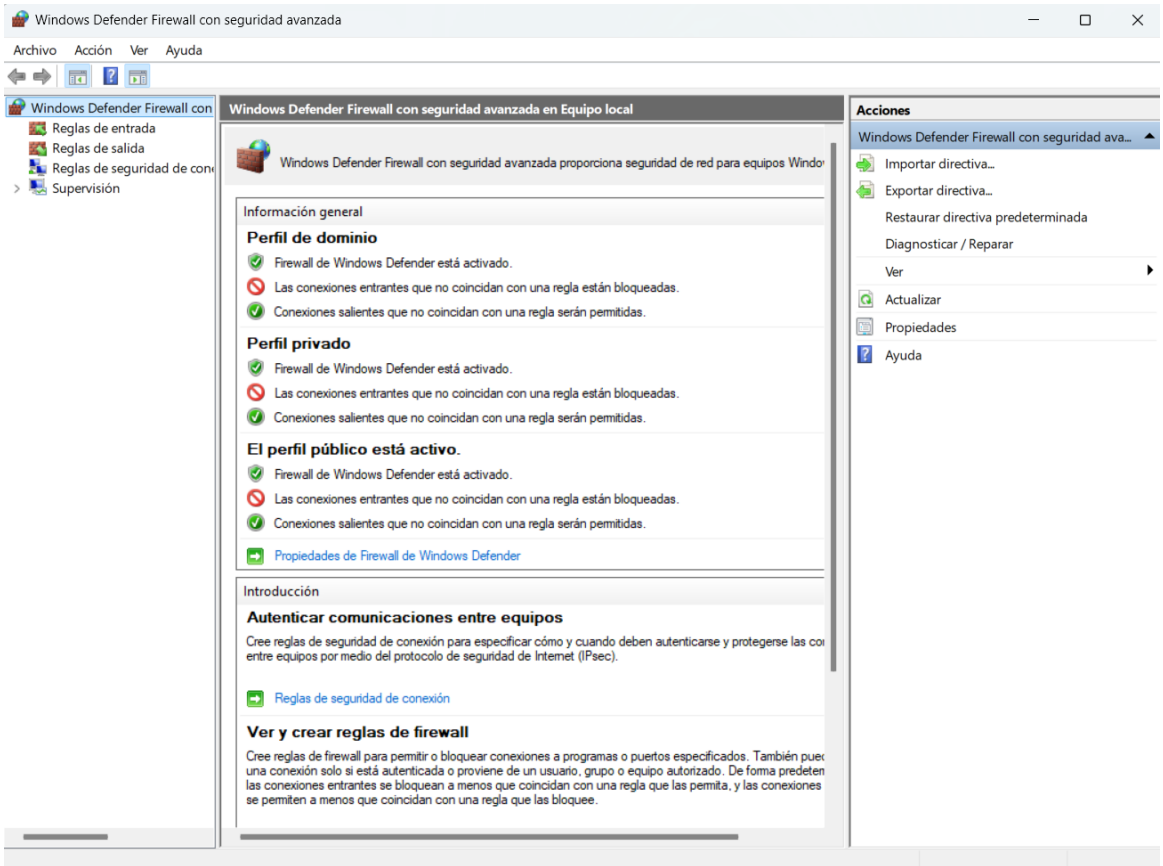
→ Abrir únicamente los puertos necesarios desde el Firewall Avanzado de Windows:

- 25: SMTP.
- 443: HTTPS (para acceso a OWA y EAC).

Para ello:

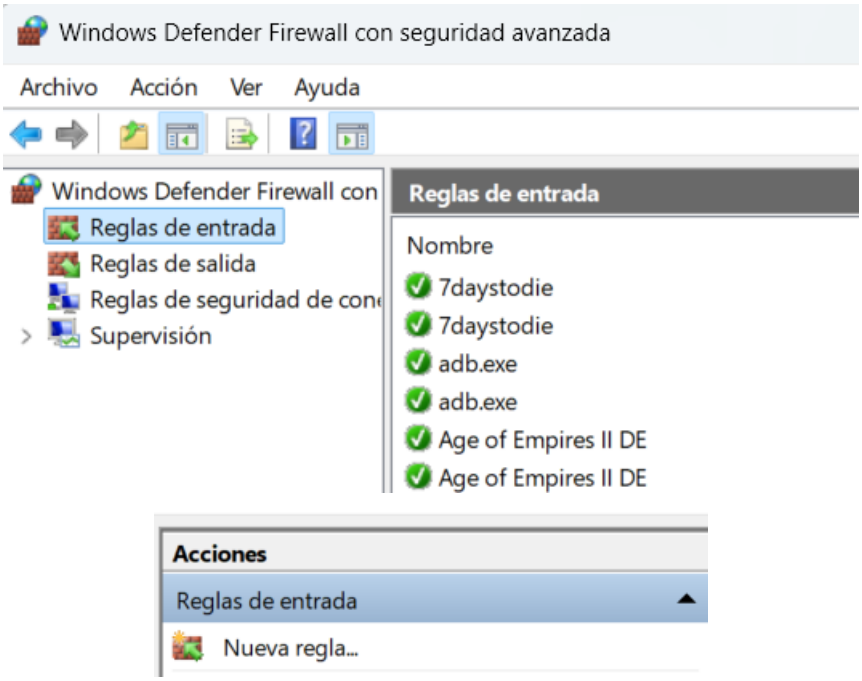
a. Acceder al Firewall Avanzado de Windows. Presiona Windows + R, escribe wf.msc y pulsa Enter. Esto abrirá el "Firewall de Windows con seguridad avanzada":



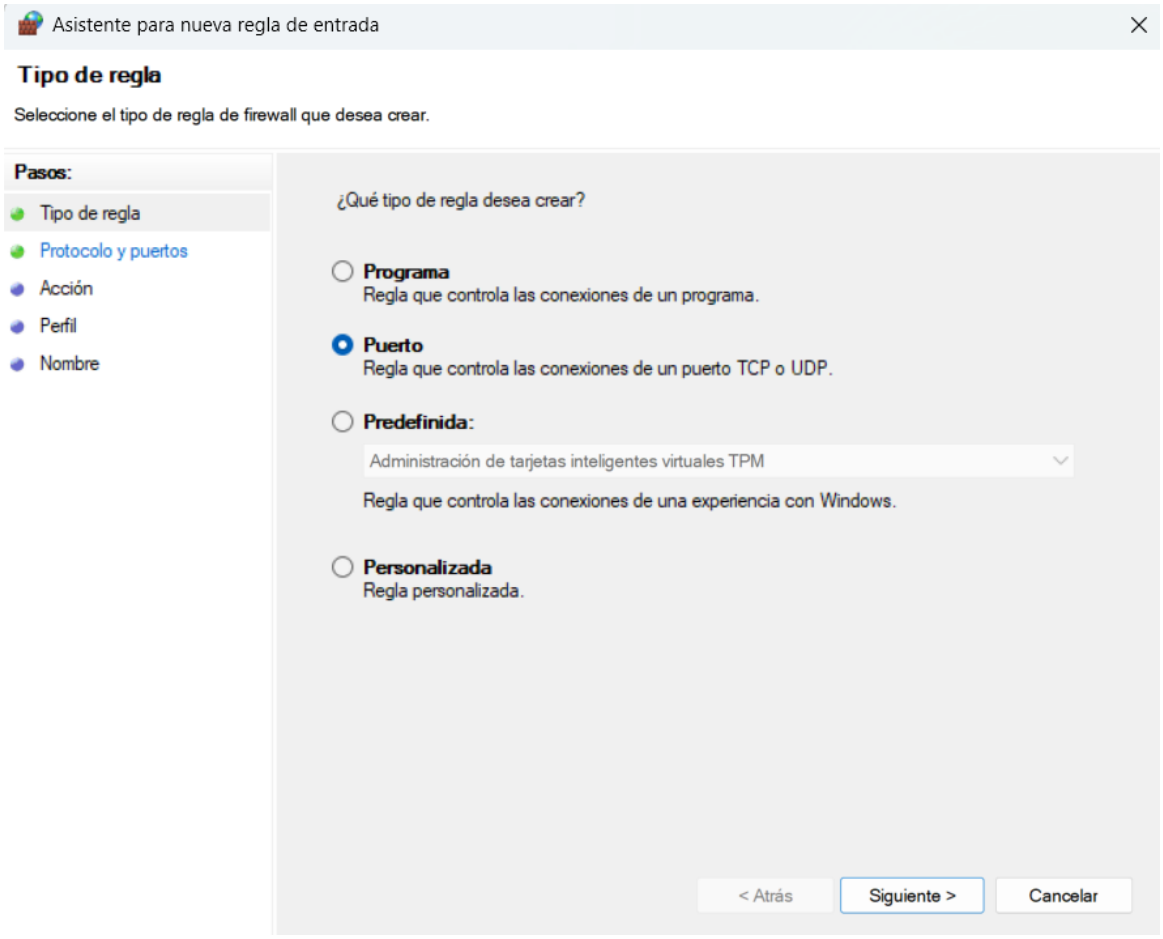


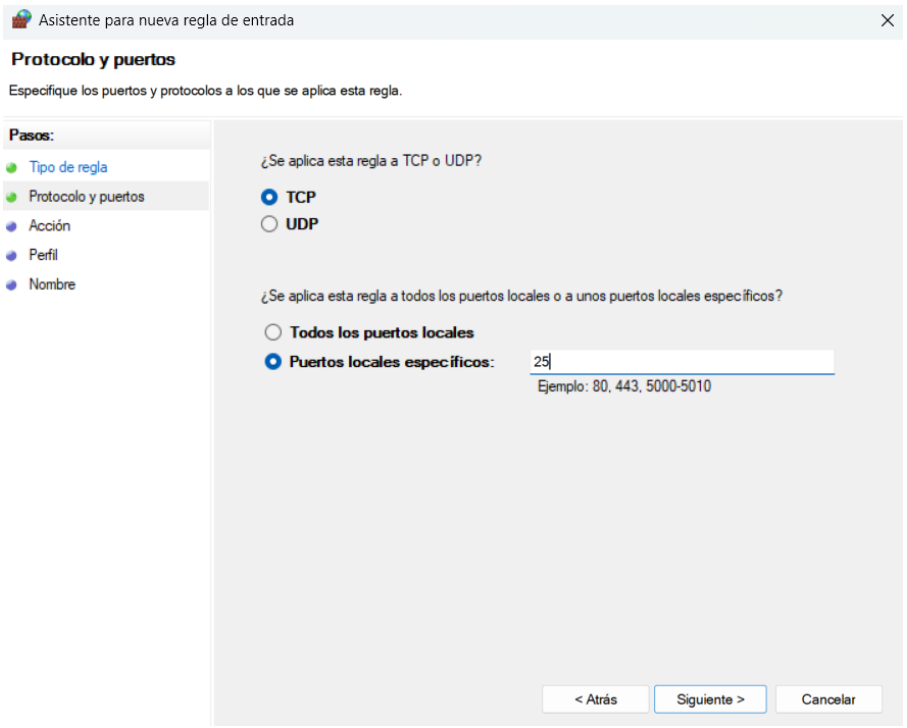
b. Crear una nueva regla para cada puerto. En el panel izquierdo, selecciona Reglas de entrada. En el panel derecho, haz clic en Nueva regla:

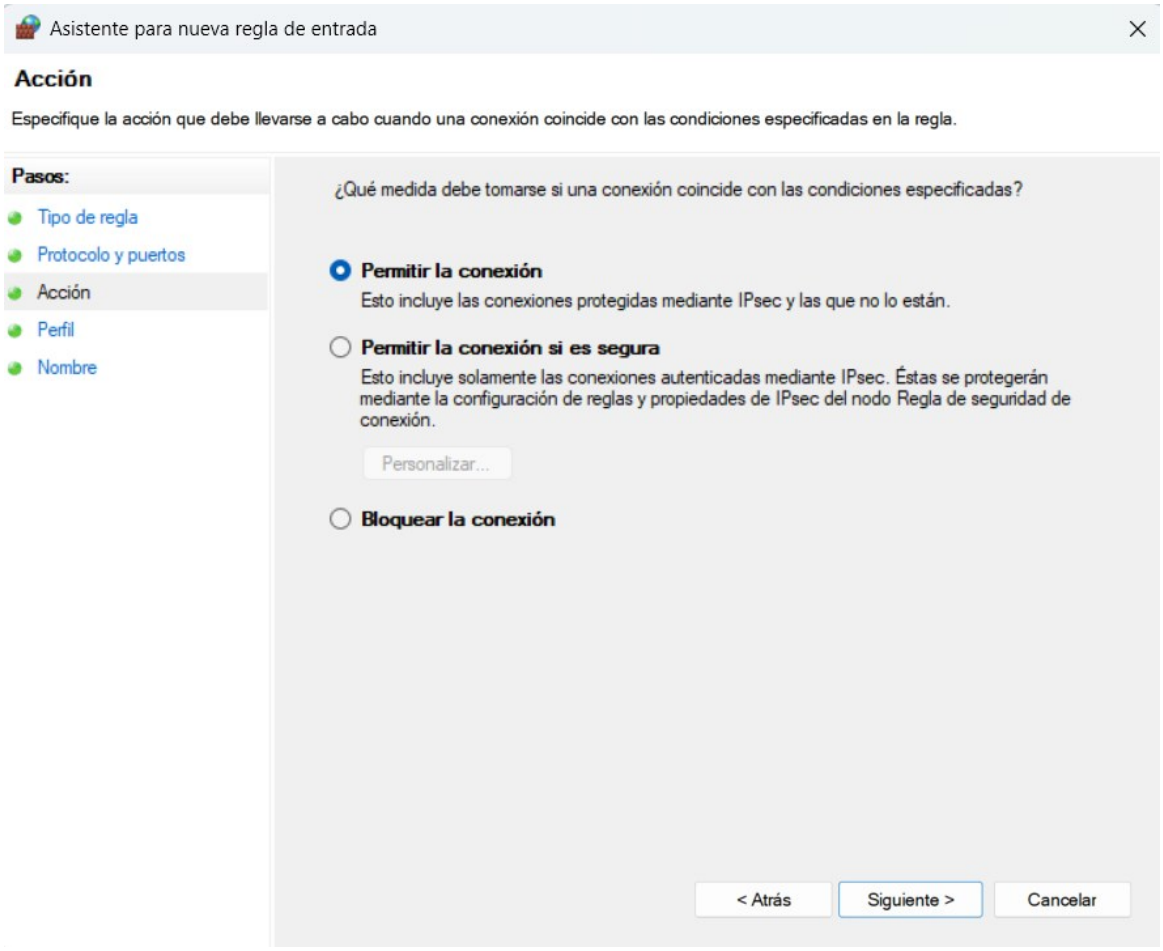
c.



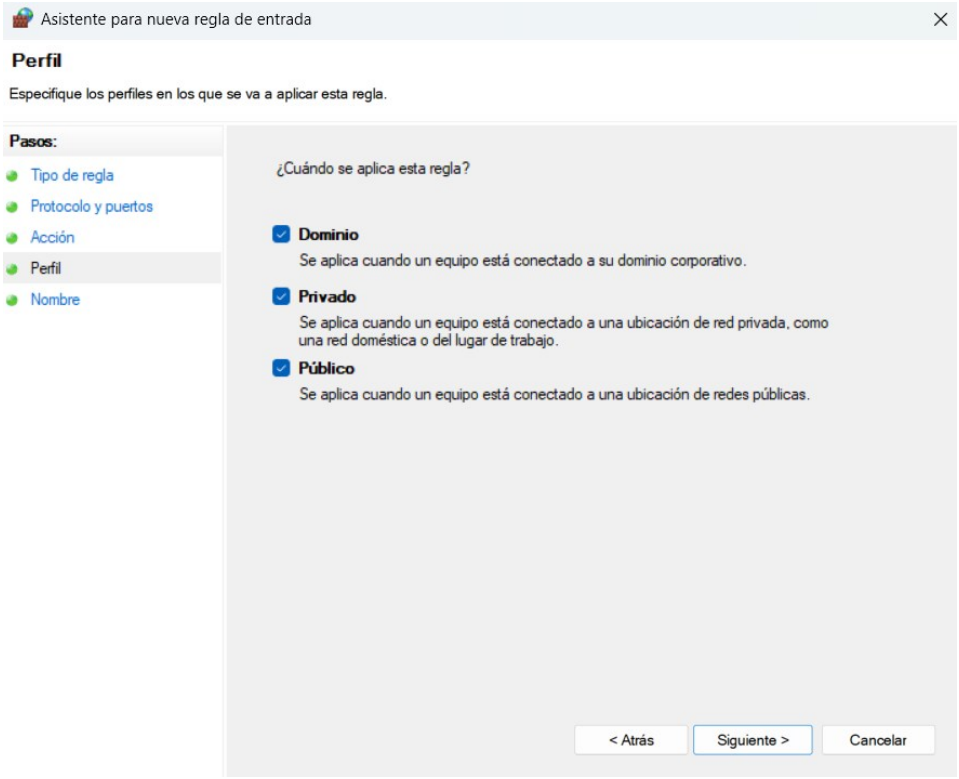
d. Configurar la regla para el puerto 25 (SMTP). Selecciona Puerto y haz clic en Siguiente. Elige TCP y especifica el puerto: 25. Selecciona Permitir la conexión y haz clic en Siguiente:



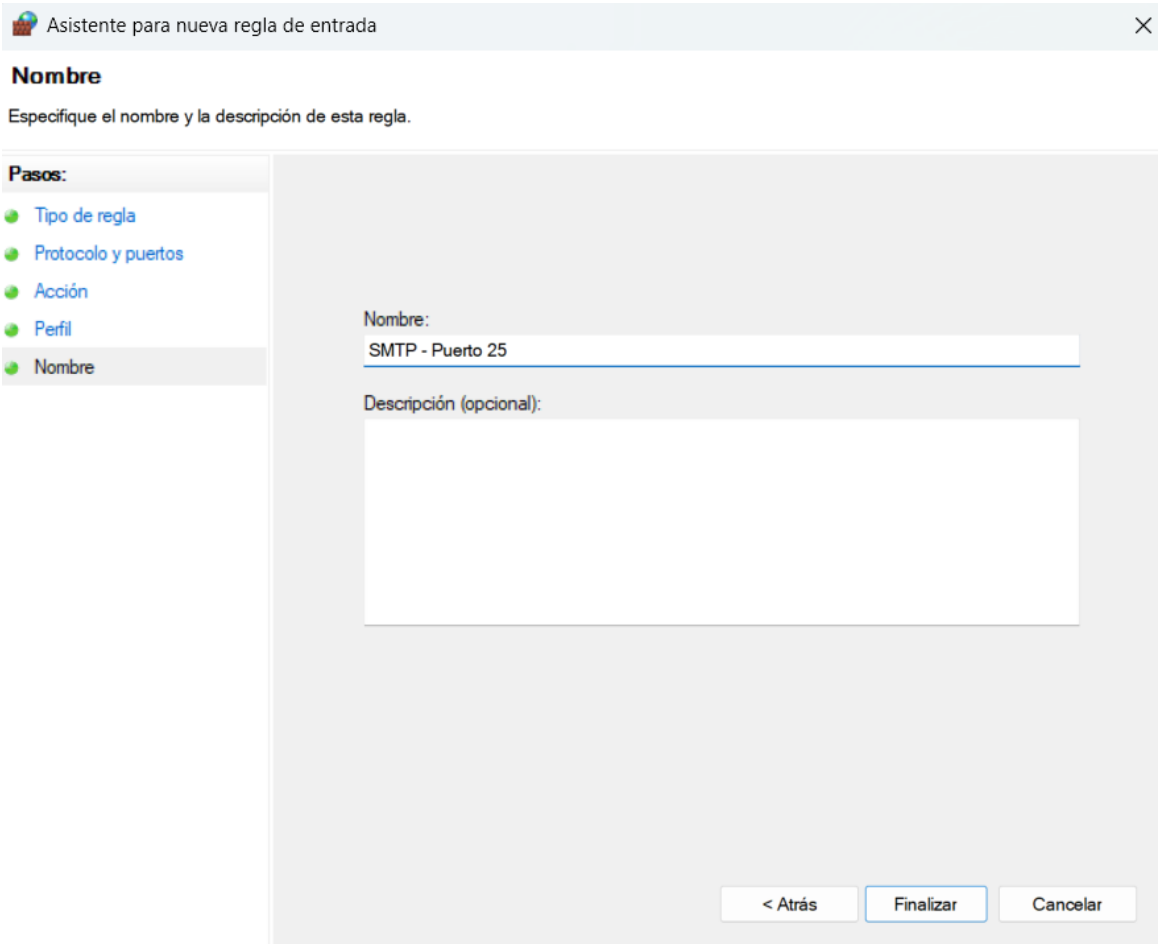




e. Aplica la regla a los perfiles que correspondan (Dominios, Privado o Público, dependiendo de tu entorno):



f. Nombra la regla como "SMTP - Puerto 25" y haz clic en Finalizar.

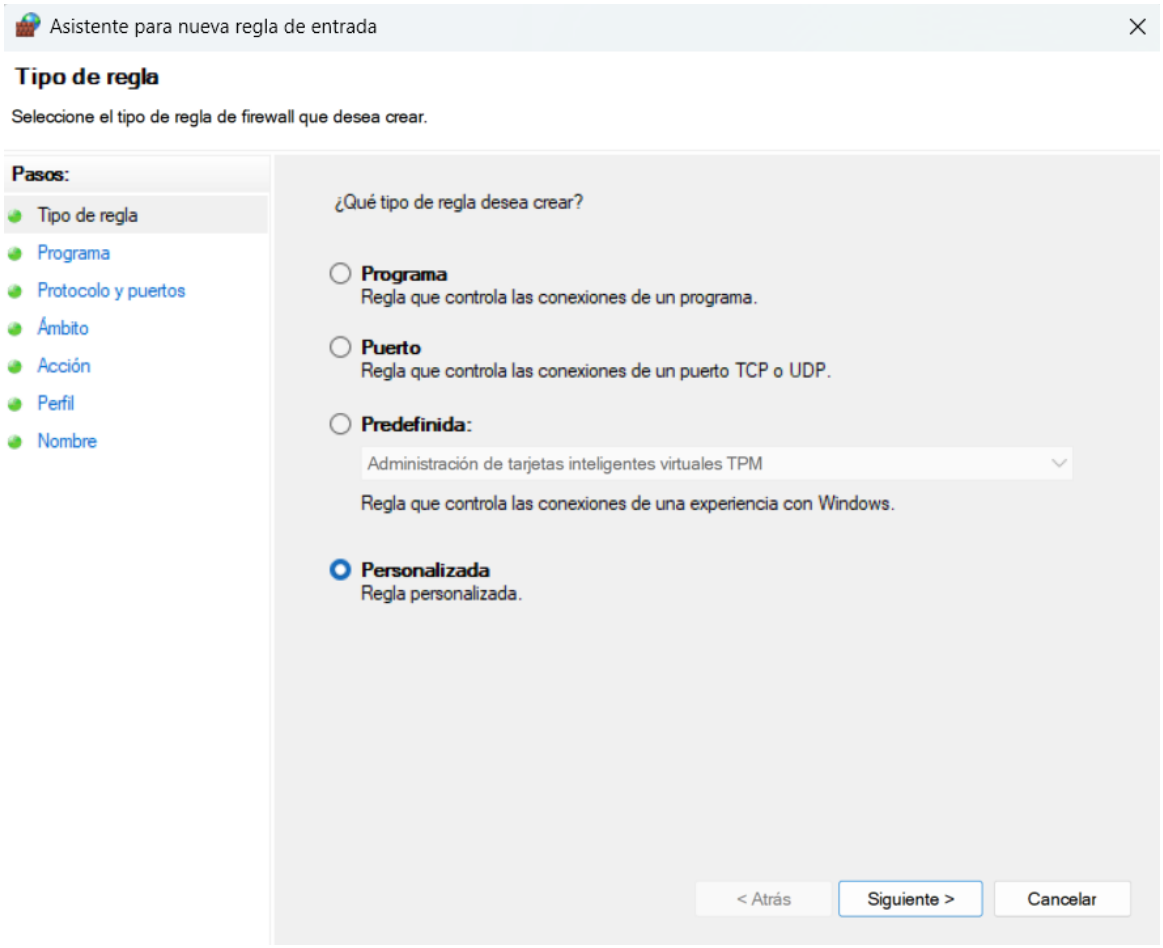


g. Repetir el proceso para otros puertos necesarios:
   i. Puerto 443 (HTTPS, para acceso a OWA y EAC):
      - Selecciona TCP y especifica 443.

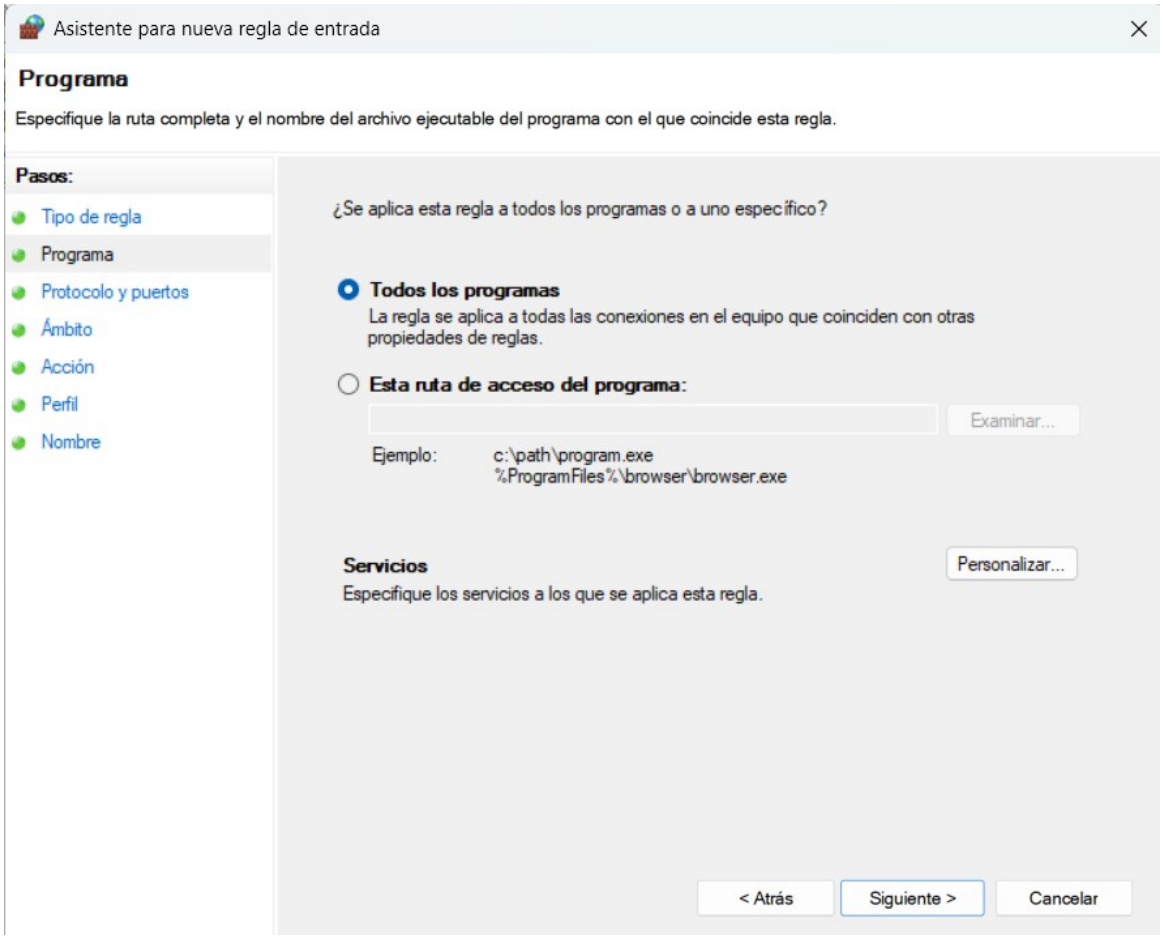
→ Configurar reglas personalizadas para permitir solo conexiones desde direcciones IP internas confiables.

a. Crear una regla personalizada:

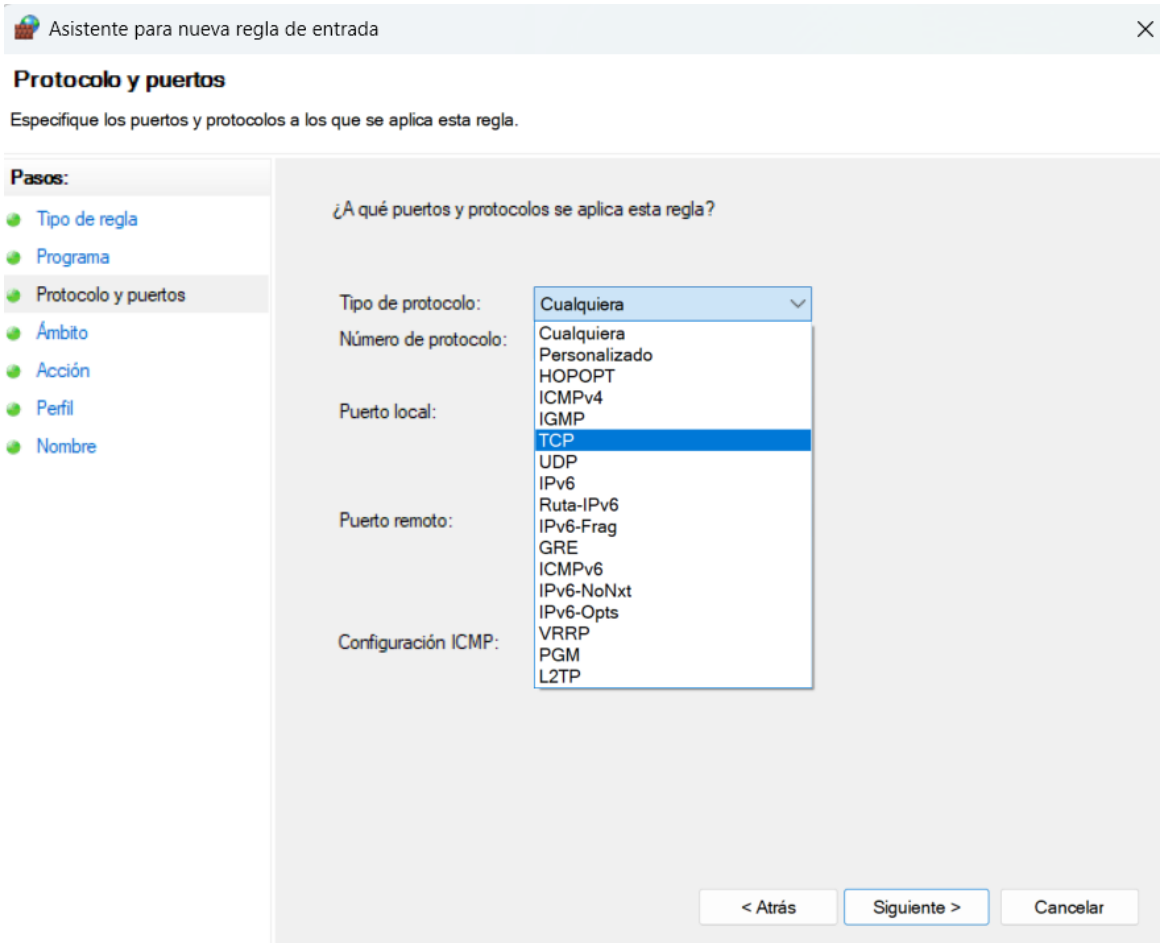
i. En el "Firewall con seguridad avanzada", haz clic en Nueva regla. Selecciona Personalizada y haz clic en Siguiente:



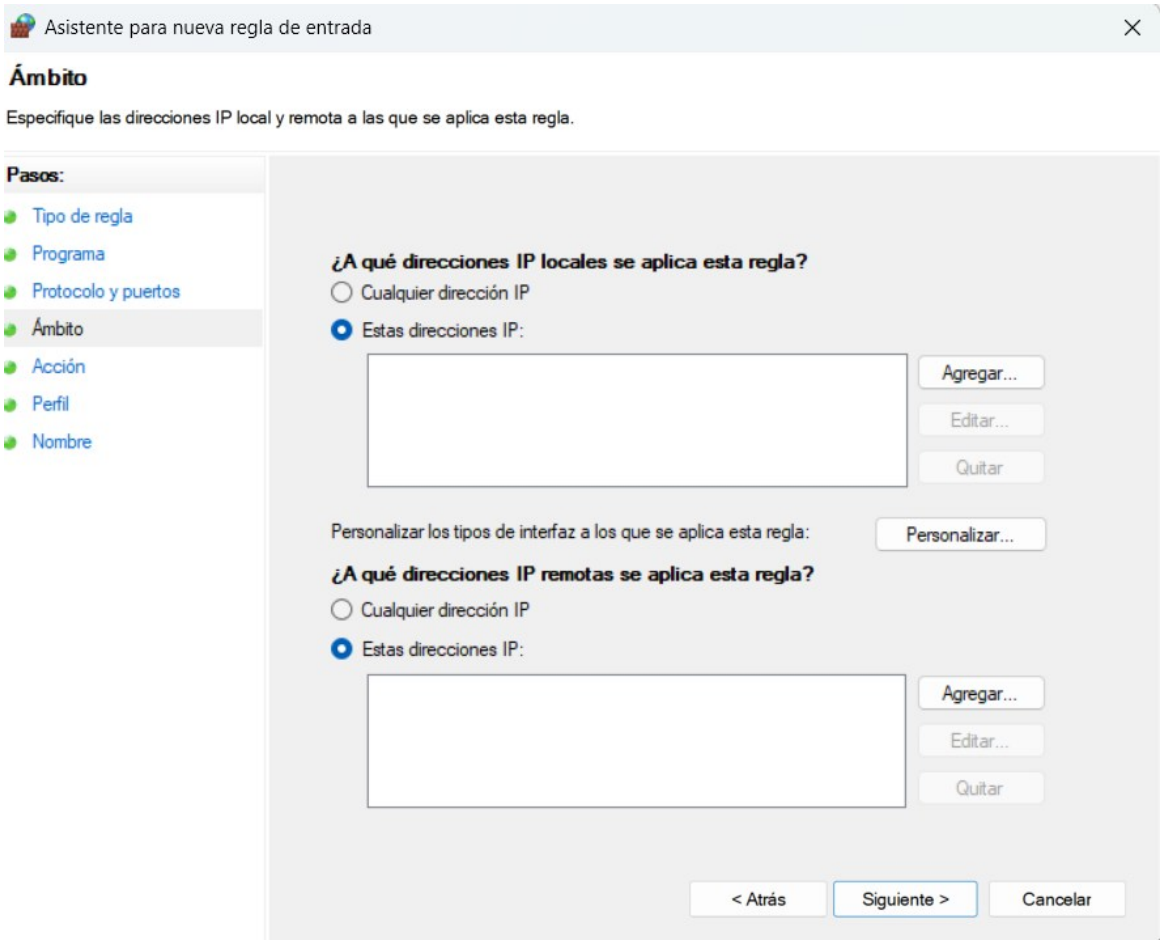
b. Especificar la regla para el programa o servicio:
    i. Selecciona Todos los programas si deseas aplicar la regla a todo el sistema, o especifica un programa o servicio en particular (por ejemplo, el ejecutable del servidor de correo):



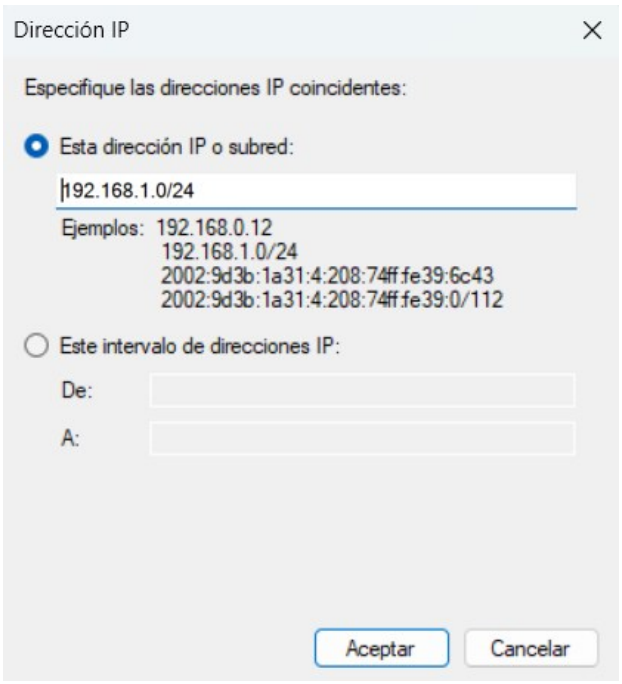
c. Definir los puertos necesarios:
   i. Selecciona TCP y especifica los puertos que deseas proteger, como 25 (SMTP) y 443 (HTTPS):

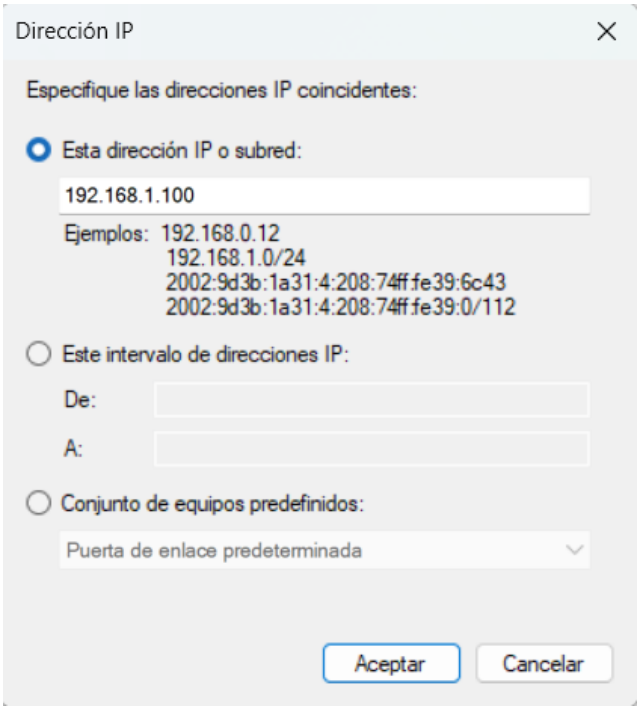


d. Configurar las direcciones IP permitidas:
   i. Selecciona Estas direcciones IP:

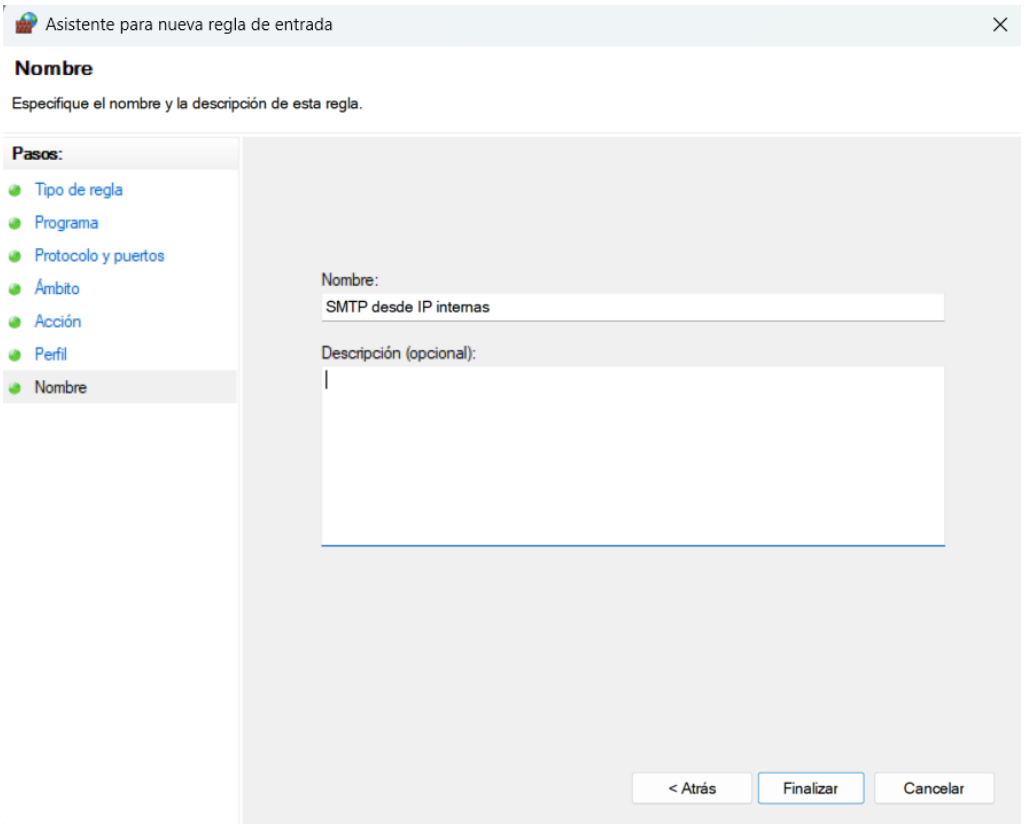


e. Haz clic en Agregar e introduce las IP internas confiables. Por ejemplo:
   i. 192.168.1.0/24 para toda una subred local o una IP específica, como 192.168.1.100.



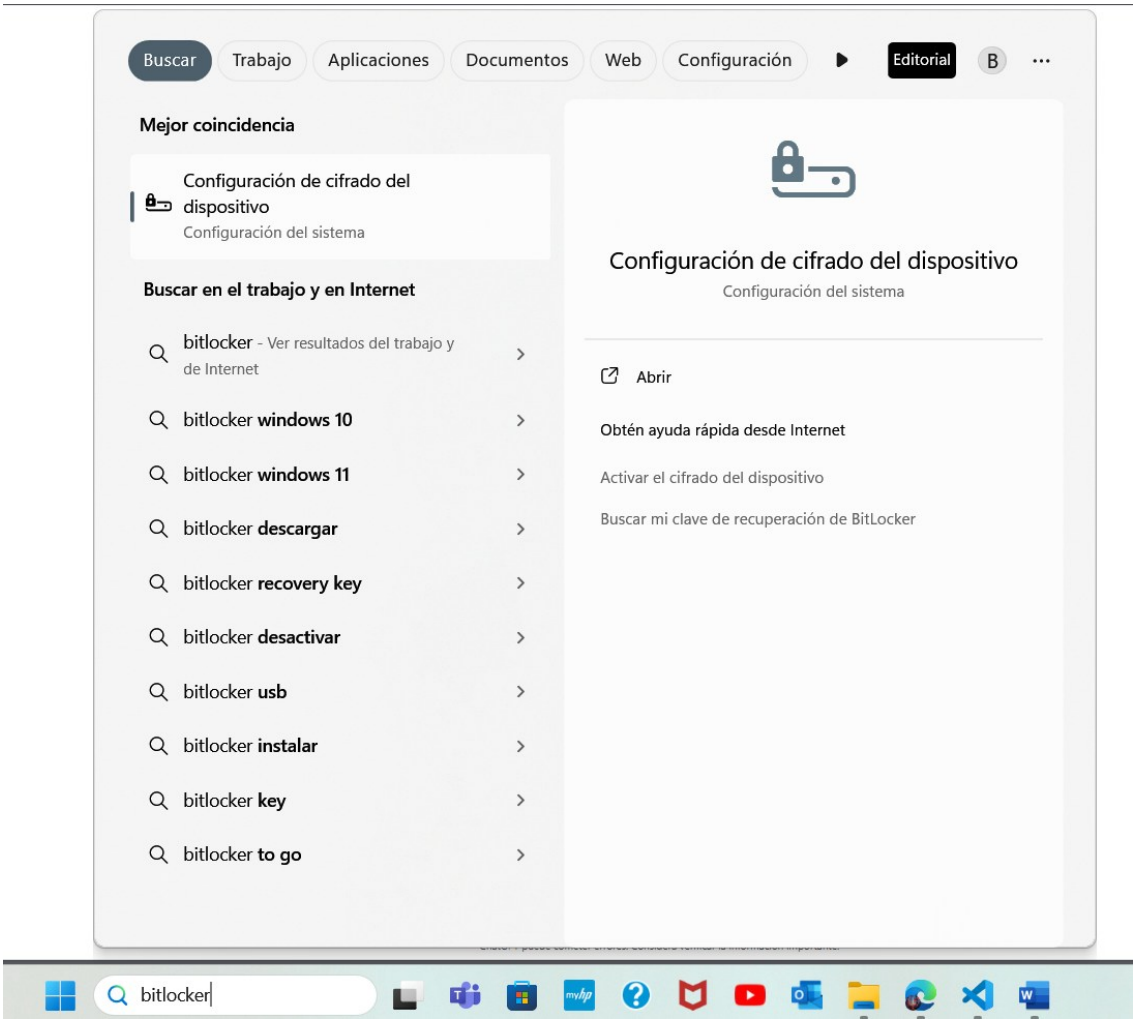


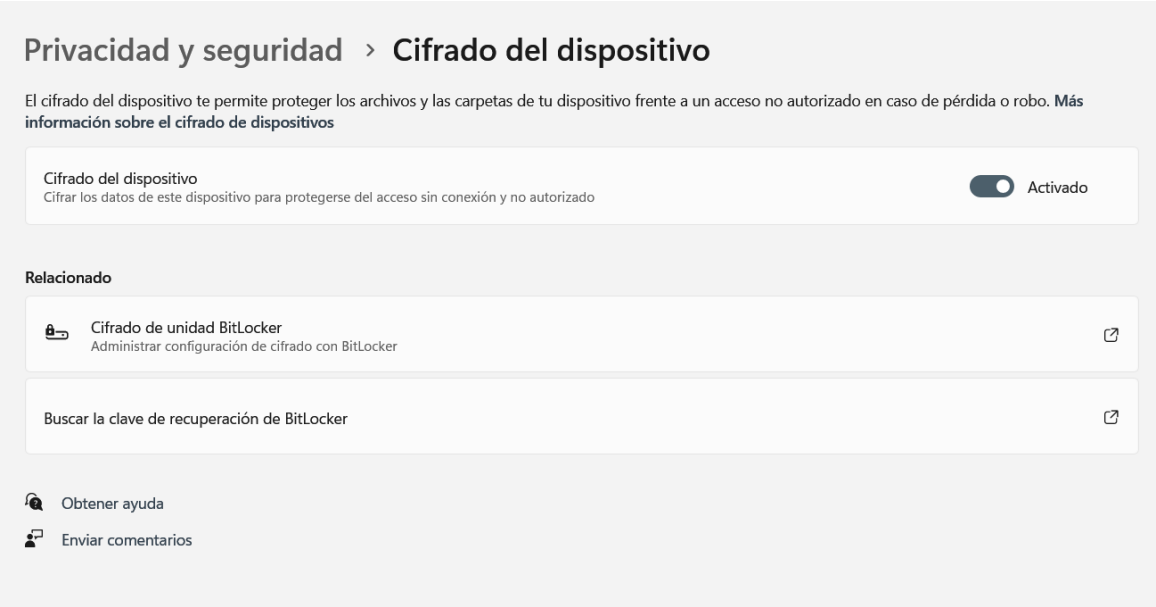
f. Permitir la conexión:
    i. Selecciona Permitir la conexión y haz clic en Siguiente.
g. Aplicar la regla a perfiles específicos:
    i. Aplica la regla a los perfiles requeridos (Dominios, Privado o Público).
h. Nombrar la regla:
    i. Asigna un nombre descriptivo, como "SMTP desde IP internas", y haz clic en Finalizar.



Habilitar BitLocker:

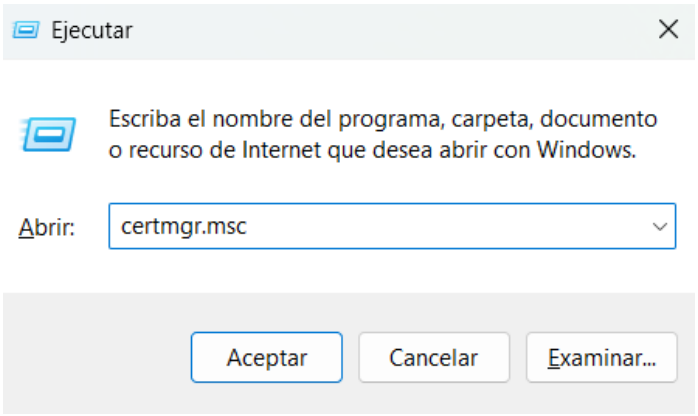
→ Para proteger los datos almacenados en los discos del servidor, BitLocker ofrece un cifrado completo del disco. Esto asegura que, incluso si el hardware del servidor es robado, los datos permanecen inaccesibles sin la clave de cifrado.

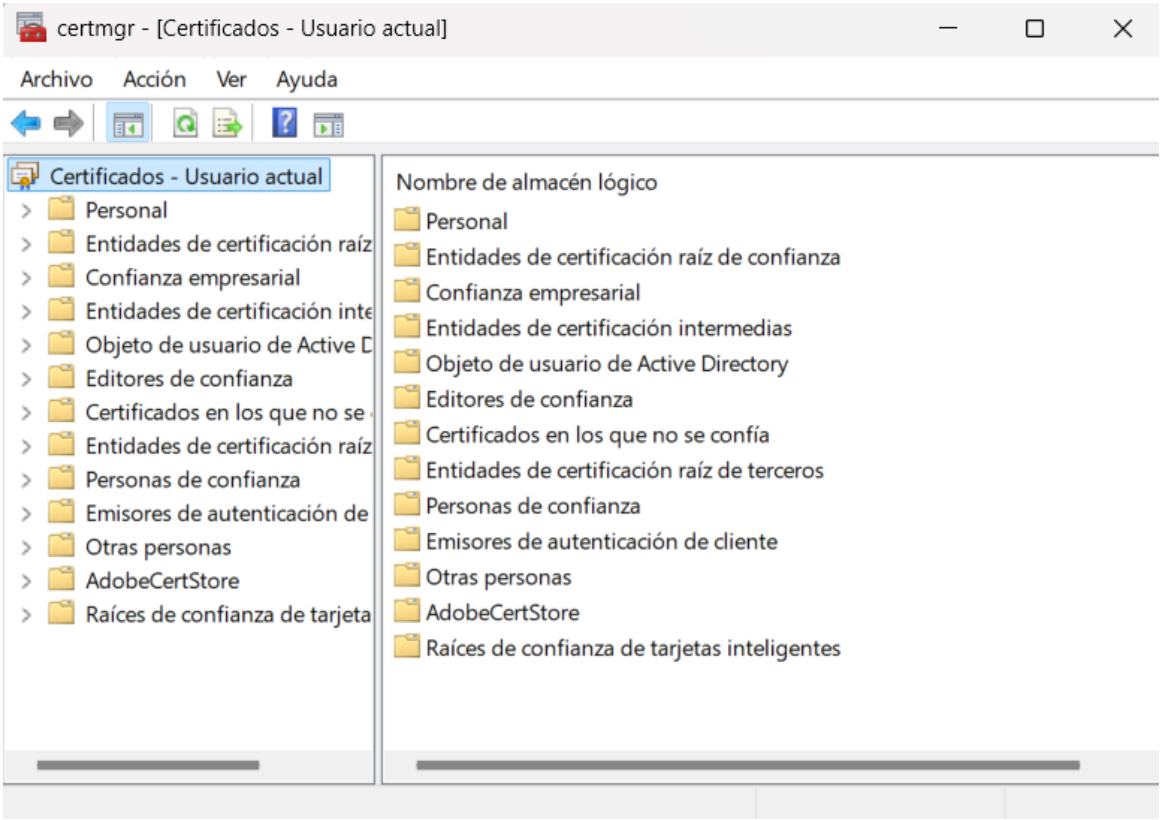


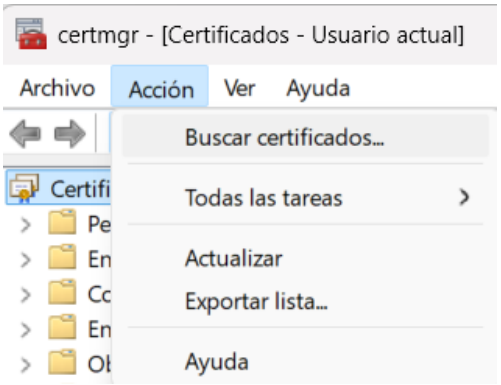


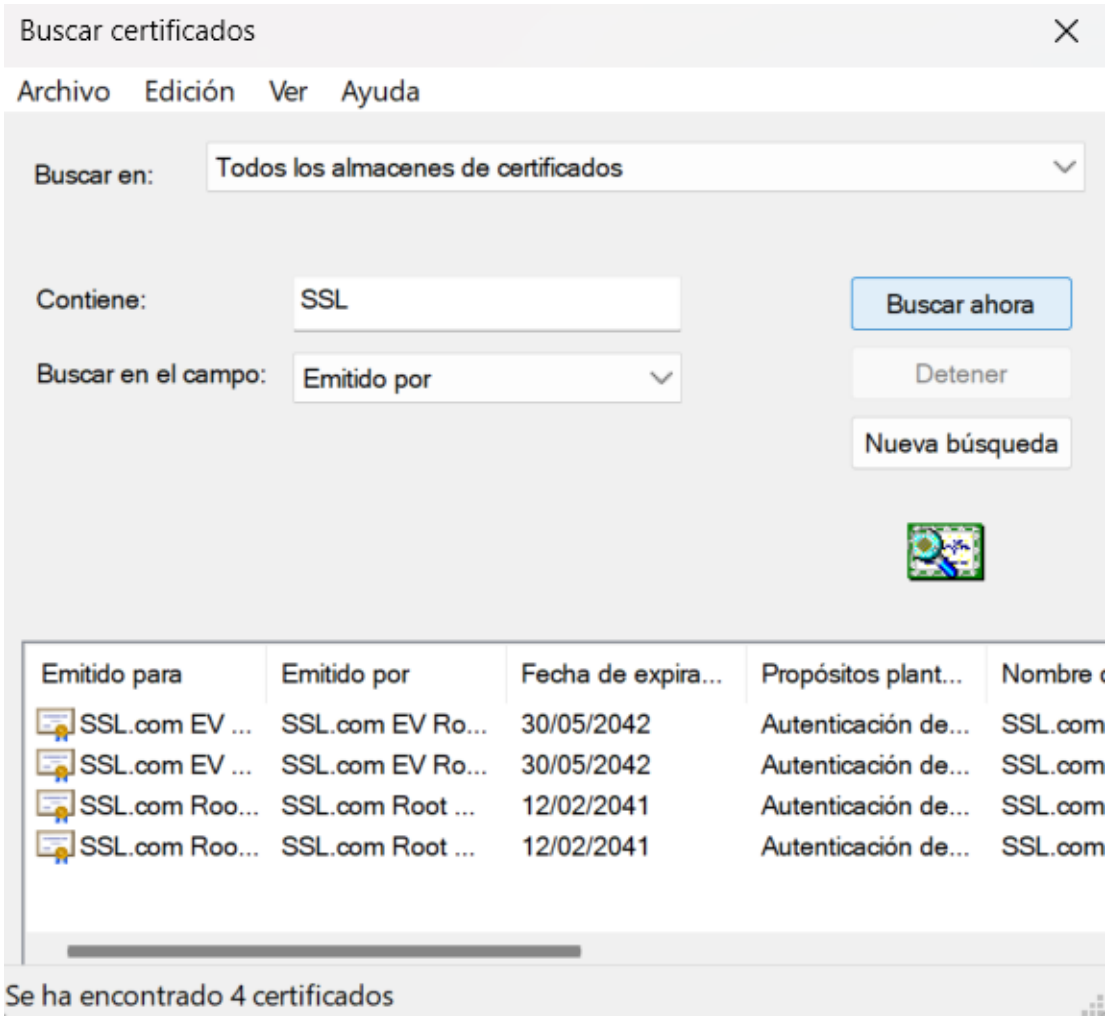
Configurar TLS:

→ Usar el Administrador de Certificados para importar un certificado SSL válido que se aplicará a las comunicaciones de Exchange:







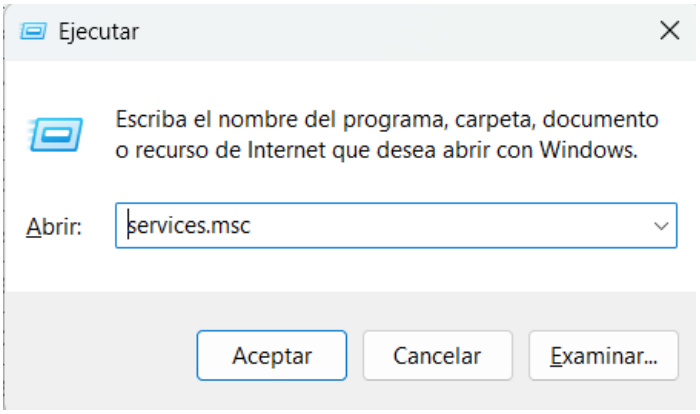


→ Configurar Exchange para usar dicho certificado mediante el Exchange Management Shell (EMS):

```
Enable-ExchangeCertificate -Thumbprint <CertThumbprint> -Services SMTP, IIS
```

Deshabilitar servicios innecesarios:

→ Asegurarse de que solo los servicios requeridos por Exchange Server estén habilitados. Esto puede hacerse desde el Administrador de Servicios (services.msc):



Recuerda

Principales diferencias entre el proceso de instalación del sistema operativo y la instalación del software del servidor:

Aspecto	Instalación del sistema operativo	Instalación del software del servidor
Propósito	Preparar el entorno base para cualquier servicio	Proveer una funcionalidad específica (por ejemplo, correo)
Momento en el proceso	Primer paso en la configuración del servidor	Etapa posterior a la instalación del sistema operativo
Ejemplos	Windows Server, Ubuntu Server	Exchange Server, Postfix, Apache
Nivel técnico	Configuración de hardware y red básica	Configuración de servicios específicos
Requisitos previos	Hardware funcional	Sistema operativo instalado y configurado

Actividad 7

Adivinanzas con palabras desordenadas:

Adivinanza:

Soy la base para que todo funcione,

en mí se instalan servicios y soluciones.

Sin mí, el servidor no podría operar,

en Linux o Windows me puedes encontrar.

Respuesta desordenada:

TSOISME OERPITAOV

Adivinanza:
Guardo instrucciones claras y definidas,
sobre cómo la red será dirigida.
En un archivo YAML me hallarás,
la IP estática ahí configurarás.
Respuesta desordenada:
TALNPNE /0/NTREEPCFG.YMLA

Adivinanza:
Si cambias de casa o de lugar,
nadie te encontrará al buscar.
Por eso te fijo en la red de verdad,
así siempre estarás en tu misma "ciudad".
Respuesta desordenada:
DPERIÓNICASE TÁTIAC

Adivinanza:
Soy el encargado de asignar permisos,
de abrir puertas y cerrar abismos.
Con reglas me configuro en el servidor,
para proteger tus datos con rigor.
Respuesta desordenada:
ALWIFRL E DSWONIW

Adivinanza:
Soy ligero y estable, listo para durar,
en servidores me prefieren instalar.
Me encuentras en Ubuntu o CentOS,
como base perfecta para tu correo veloz.
Respuesta desordenada:
SIBTROUCDINIÓS XVETINUAAD

3. Instalación y configuración del servidor SMTP (MTA).

Una vez que el sistema operativo está configurado y funcionando, se procede a instalar el software que proveerá el servicio específico para el que se destina el servidor. En el caso de un servidor de correo electrónico, este software es el servidor SMTP (como Postfix, Exchange Server o Sendmail). Este paso se enfoca en habilitar la funcionalidad específica que la empresa necesita, como el envío y la recepción de correos electrónicos. Un servidor SMTP (Mail Transfer Agent) es el componente encargado de enviar y recibir correos electrónicos, gestionando aspectos como la autenticación de usuarios, la seguridad en las transmisiones y la filtración de contenido no deseado.

Los objetivos principales son:

- Añadir la funcionalidad específica: El software del servidor es el que permite realizar tareas específicas, como gestionar correos electrónicos, archivos o bases de datos.
- Configuración del servicio: Aquí se define cómo el software interactuará con el sistema operativo y otros servicios, como el DNS o el directorio activo.
- Optimización del rendimiento: Incluye ajustes específicos del software para que funcione de manera eficiente en el entorno operativo instalado.

Anotación

Un servidor SMTP funciona como el intermediario en el envío y la recepción de correos electrónicos, y su configuración implica varios pasos esenciales que garantizan su correcto funcionamiento. La instalación del software establece la base para que el servidor opere, proporcionando las herramientas necesarias para gestionar los correos. La configuración como MX permite que el servidor sea el punto de recepción principal para los correos destinados a un dominio específico, lo que incluye la correcta configuración de los registros DNS y el uso de protocolos estándar como SMTP. Por otro lado, cuando el servidor actúa como MTA, se encarga de enrutar los mensajes desde el cliente hacia otros servidores, aplicando medidas de seguridad como autenticación de usuarios y cifrado.

Además, la instalación de filtros antivirus y antispam asegura que los correos no deseados, maliciosos o con contenido peligroso sean detectados y bloqueados antes de llegar al destinatario. Los procesos de arranque y parada son necesarios para realizar tareas de mantenimiento o reiniciar el servidor de forma controlada, asegurando su estabilidad. Finalmente, los registros (logs) son el sistema de monitoreo y diagnóstico del servidor, almacenando información sobre correos enviados, errores y actividades sospechosas, lo que permite identificar problemas y mantener un sistema eficiente y seguro. Cada uno de estos puntos es clave para garantizar que el servidor SMTP funcione de manera confiable, segura y adaptada a las necesidades de la organización.

3.1. Instalación software.

Antes de iniciar la instalación, es importante comprender las funciones básicas de un servidor SMTP. Este componente actúa como un intermediario que entrega mensajes a su destino y acepta correos para los dominios configurados. Al seleccionarlo, debemos considerar aspectos como la