EBENEZER IT · GUÍAS PASO A PASO

GUÍA 01 · EPISODIOS 4, 5 Y 6

Tu servidor base: contratar, preparar y proteger un VPS Ubuntu 24.04

De cero a un servidor actualizado, con tu propio usuario, acceso por clave SSH, cortafuegos en dos capas y fail2ban. La base sobre la que se monta todo lo demás del curso.

~3 horas
la primera vez, sin prisa

Nivel inicial
no hace falta saber Linux

Ubuntu 24.04 LTS
VPS de IONOS · PC con Windows

www.ebenezer.org.es · Alejandro Quevedo · Versión pública 1.0 · noviembre 2026

Índice

Antes de empezar

0 Cómo usar esta guía y tabla de valores

Parte A · Contratar el servidor y el dominio

Paso 01 Contratar el VPS

Paso 02 Registrar el dominio

Paso 03 Crear los registros DNS

Paso 04 Configurar el firewall de IONOS

Paso 05 Configurar el DNS inverso (PTR)

Parte B · Preparar el servidor

Paso 06 Primer acceso por SSH

Paso 07 Actualizar el sistema

Paso 08 Comprobar el puerto 25

Paso 09 Nombre del servidor (hostname)

Paso 10 Zona horaria y hora

Paso 11 Crear tu usuario con sudo

Paso 12 Acceso con clave SSH desde Windows

Paso 13 Memoria de intercambio (swap)

Paso 14 Actualizaciones automáticas

Parte C · Seguridad base

Paso 15 Endurecer SSH

Paso 16 Cortafuegos UFW

Paso 17 fail2ban para SSH

Paso 18 Comprobación final e instantánea

Anexos

A Problemas frecuentes y cómo salir de ellos

B Puertos abiertos al terminar esta guía

C Chuleta de comandos

Cómo usar esta guía

Tienes aquí **todos los pasos y comandos**, en orden. La explicación de cada paso (el porqué de cada línea) está en el **vídeo del episodio**.

Para copiar los comandos sin errores, usa la versión web: **https://www.ebenezer.org.es/guia-01-servidor-base.html**. Al copiar desde un PDF se pueden romper los saltos de línea y las comillas.

ANTES DE EMPEZAR

Cómo usar esta guía

Qué vas a tener al terminar

- Un VPS con Ubuntu 24.04 LTS en IONOS y un dominio propio apuntando a él.
- El servidor actualizado, con nombre completo, hora correcta y actualizaciones de seguridad automáticas.
- Tu propio usuario con permisos de administrador (`sudo`) y el acceso de `root` por SSH desactivado.
- Entrada por **clave SSH** desde tu PC con Windows, sin contraseñas que se puedan adivinar.
- Dos cortafuegos (el de IONOS y UFW) con solo el puerto 22 abierto, y **fail2ban** bloqueando a quien intente entrar a la fuerza.

Qué necesitas

- Un PC con **Windows 10 u 11**. Ya trae el cliente SSH: no hay que instalar PuTTY ni nada más.
- Una cuenta en **IONOS** con un método de pago.
- Un gestor de contraseñas o, como mínimo, un papel para apuntar los valores de la tabla de abajo.
- Unas 3 horas sin prisa. Si te cansas, para al final de cualquier paso: todo queda guardado.

Cómo se leen los bloques de código

Cada bloque dice arriba **dónde** se escribe. Fíjate siempre en el color antes de pegar:

Color	Dónde se escribe	Cómo lo reconoces
Azul	En tu PC, en **PowerShell**	La línea empieza por `PS C:\Users\...>`
Verde	En el **servidor**, por SSH	La línea empieza por `root@...#` o `usuario@mail:~$`
Morado	Contenido de un archivo	Lo pegas dentro de un archivo, no en la terminal
Gris	Salida esperada	Lo que deberías ver. No se escribe
Ocre	Panel web de IONOS	Clics en el navegador, no comandos

Las líneas que empiezan por `#` son **comentarios**: explican lo que viene y la terminal las ignora. Puedes pegarlas sin problema.

Los valores que tienes que cambiar

En los comandos verás palabras resaltadas en amarillo, como `TU_IP` o `TU_DOMINIO`. **Nunca las pegues tal cual**: sustitúyelas por tu valor real. Rellena esta tabla a medida que avances; la vas a necesitar en todas las guías del curso.

Valor	Qué es
TU_IP	La IP pública del VPS. Te la da IONOS en el paso 1. Ejemplo: `82.165.10.20`
TU_DOMINIO	Tu dominio, sin `www` ni `https://`. Ejemplo: `ebenezer-lab.es`
TU_USUARIO	Tu usuario en el servidor. En minúsculas, sin espacios, tildes ni ñ. Ejemplo: `ale`
TU_IP_CASA	La IP pública de tu conexión de casa (paso 17)
TU_ZONA_HORARIA	`Europe/Madrid` (península y Baleares) o `Atlantic/Canary` (Canarias)
Contraseña de root	La inicial que da IONOS. Guárdala: la necesitarás si algún día te quedas fuera
Contraseña de TU_USUARIO	La que crearás en el paso 11. Te la pedirá `sudo`
Frase de paso de la clave SSH	La que pondrás en el paso 12

Truco para no equivocarte al sustituir

Pega el comando primero en el **Bloc de notas**, pulsa **Ctrl+H** (reemplazar), cambia `TU_DOMINIO` por tu dominio y pulsa «Reemplazar todo». Después cópialo a la terminal. Así no se te escapa ninguno.

Cosas que sorprenden la primera vez

- **Al escribir una contraseña en Linux no aparece nada**, ni asteriscos. Es normal: escríbela a ciegas y pulsa Enter.
- **Pegar en la terminal:** en Windows Terminal y PowerShell, **Ctrl+V** o clic derecho. Para copiar texto de la terminal, selecciónalo y pulsa **Ctrl+C** (o Enter en la consola clásica).
- **Si un comando se queda «colgado»** sin devolverte el cursor, pulsa **Ctrl+C** para cancelarlo.
- **Copiar desde un PDF** a veces parte una línea larga en dos. Si un comando ocupa una sola línea en la guía, comprueba que en el Bloc de notas también queda en una sola.
- **Linux distingue mayúsculas de minúsculas**: `Archivo.txt` y `archivo.txt` son dos archivos distintos.

Cómo se crean los archivos de configuración en esta guía

Para escribir un archivo de configuración usaremos siempre este patrón. Tiene la ventaja de que se pega de una vez y no hay que moverse con el teclado dentro de un editor:

EN EL SERVIDOR · PATRÓN

```
sudo tee /ruta/del/archivo.conf > /dev/null <<'EOF'
línea 1 del archivo
línea 2 del archivo
EOF
```

Después de crear un archivo, compruébalo siempre con `cat /ruta/del/archivo.conf`, que lo muestra en pantalla.

¿Y si prefiero editar con nano?

También puedes: `sudo nano /ruta/del/archivo.conf`, pegas el contenido, guardas con **Ctrl+O** y Enter, y sales con **Ctrl+X**. El resultado es el mismo.

PARTE A

Contratar el servidor y el dominio

Todo lo de esta parte se hace en el navegador, en el panel de IONOS. Al terminarla tendrás una máquina con Ubuntu encendida, tu dominio apuntando a ella y el primer cortafuegos configurado. Corresponde al **episodio 4**.

Paso 1 Episodio 4

Contratar el VPS

Por qué: necesitas un ordenador encendido las 24 horas, con una IP pública fija.

En **ionos.es** ve a **Servidores** → **VPS** y elige el plan. Para seguir el curso completo recomiendo el **VPS M+**:

Plan	CPU	RAM	Disco	Hasta dónde llegas
VPS S+	1 vCore	2 GB	60 GB	Temporadas 1 a 3 (web, Docker, VPN). El correo con base de datos irá justo
VPS M+	2 vCores	4 GB	120 GB	**Todo el curso**, con correo, chat, Docker y monitorización a la vez
VPS L+	4 vCores	8 GB	240 GB	Más de lo que necesitas para aprender

Durante el pedido:

1. **Sistema operativo:** elige **Ubuntu 24.04 LTS**. «LTS» significa soporte durante 5 años; es la versión estable para servidores. No elijas una versión con Plesk ni con panel de control.
2. **Ubicación del centro de datos:** España o Alemania. Cuanto más cerca de tus usuarios, menos latencia.
3. **Revisa el precio después de la oferta:** los primeros meses salen baratos; mira en el resumen del pedido cuánto cuesta cada mes después.
4. Completa el pago. El servidor tarda unos minutos en estar listo.

Cuando esté listo, entra en el panel: **Menú** → **Servidores & Cloud** → tu servidor. Ahí verás:

- La **IP pública** (IPv4). Apúntala en la tabla como `TU_IP`.
- Los **datos de acceso**: usuario `root` y su contraseña inicial. Guárdala en tu gestor de contraseñas.

Los nombres de los menús pueden cambiar

IONOS cambia su panel de vez en cuando. Si un botón no se llama exactamente igual, busca uno parecido en el menú del servidor; las opciones siempre son las mismas.

Comprueba antes de seguir

- Tienes apuntada `TU_IP` y la contraseña de root.
- En el panel, el servidor aparece como **encendido** (en verde).

Paso 2 Episodio 4

Registrar el dominio

Por qué: tu dominio es el nombre con el que la gente llegará a tus servicios (`mail.tudominio.es`, `chat.tudominio.es`...) y también tu identidad para enviar correo.

1. En el panel, ve a **Dominios & SSL** → **Registrar dominio**.
2. Busca un nombre **corto** y fácil de dictar, sin guiones raros. Un `.es` o un `.com` son la opción más segura.
3. Al pagar, no hace falta contratar ningún extra (correo de IONOS, constructor web, etc.): todo eso lo vas a montar tú.
4. Apunta el dominio en la tabla como **TU_DOMINIO**.

> **Un .es puede tardar en activarse**
> Los dominios `.es` a veces tardan unas horas en quedar activos. Puedes seguir con los pasos 4 y 6–18, que no dependen del dominio, y volver al paso 3 después.

> **Comprueba antes de seguir**
> En **Dominios & SSL**, tu dominio aparece como **activo**.

Paso 3 Episodio 4

Crear los registros DNS

Por qué: el DNS es la «agenda» de Internet: traduce `mail.tudominio.es` a la IP de tu servidor.

En **Dominios & SSL** → tu dominio → pestaña **DNS**. IONOS crea algunos registros por defecto que apuntan a **sus** servidores de aparcamiento (la página de «dominio en construcción»). Vamos a dejar solo los nuestros.

3.1 · Borra o edita los registros que no son tuyos

- Los registros **A** de `@` y de `www` que apunten a una IP que no es **TU_IP**: edítalos (no hace falta borrarlos y crearlos).
- Los registros **AAAA** (direcciones IPv6) que haya creado IONOS: **bórralos**. Si se quedan, los visitantes con IPv6 y Let's Encrypt irán a la página de aparcamiento de IONOS y el certificado fallará.
- Si `www` es un registro **CNAME**, bórralo y créalo como **A**.
- **No toques** los registros **NS** (servidores de nombres) ni los **MX** por ahora; los MX se configuran en la temporada de correo.

3.2 · Crea estos tres registros A

Tipo	Nombre de host	Apunta a	TTL	Para qué
A	`@`	**TU_IP**	1 hora	El dominio «a secas» (`tudominio.es`). En IONOS, `@` significa el propio dominio

Tipo	Nombre de host	Apunta a	TTL	Para qué
A	`www`	`TU_IP`	1 hora	La web con `www`
A	`mail`	`TU_IP`	1 hora	El nombre del servidor y, más adelante, del correo

> **¿Qué es el TTL?**
> Es el tiempo que los demás servidores DNS guardan la respuesta en memoria antes de volver a preguntar. Con 1 hora, si te equivocas y lo corriges, el cambio llega a todo el mundo en una hora como mucho. Los de `vpn`, `chat`, etc. se crean en sus propios episodios.

3.3 · Comprueba desde tu PC

Abre **PowerShell** (tecla Windows, escribe *PowerShell* y Enter). No hace falta que sea como administrador. Espera 5–10 minutos después de crear los registros y escribe:

EN TU PC · POWERSHELL

```
Resolve-DnsName TU_DOMINIO -Type A -Server 1.1.1.1
Resolve-DnsName mail.TU_DOMINIO -Type A -Server 1.1.1.1
```

SALIDA ESPERADA

```
Name                Type   TTL   Section    IPAddress
----                ----   ---   -------    ---------
TU_DOMINIO           A      3600  Answer     TU_IP
```

> **Comprueba antes de seguir**
> - Los dos comandos devuelven `TU_IP`.
> - Si da error `DNS name does not exist`, espera 10 minutos más: el registro aún no se ha propagado.

Paso 4 Episodio 4

Configurar el firewall de IONOS

Por qué: es la primera capa de protección.

En el panel: **Servidores & Cloud → Red → Políticas de firewall**. Tu VPS tiene asignada una política por defecto que suele traer **varios puertos abiertos** (80, 443, 8443 y otros de paneles de control). Edítala para que quede así:

Protocolo	Puerto	Origen	Descripción
TCP	22	Todos (0.0.0.0/0)	SSH: la única puerta de entrada por ahora
ICMP	—	Todos	Opcional: permite hacer `ping` al servidor para ver si está vivo

1. Borra las demás reglas de entrada. **No te preocupes**: en cada episodio abriremos el puerto que necesite ese servicio, y solo ese.
2. Guarda y comprueba que la política está **asignada a tu servidor**.

Regla de oro del curso: un puerto, un motivo

Cada puerto abierto es una puerta por la que pueden intentar entrar. Al final de cada guía hay una tabla «Puertos abiertos» que dice qué se abrió, en qué capa y qué lo protege. Si no sabes para qué está abierto un puerto, ciérralo.

Comprueba antes de seguir

La política de tu servidor tiene solo la regla del **22/TCP** (y, si quieres, ICMP).

Paso 5 Episodio 4

Configurar el DNS inverso (PTR)

Por qué: el DNS normal traduce nombre → IP; el inverso traduce IP → nombre.

1. En el panel: **Servidores & Cloud** → **Red** → **IPs públicas**.
2. Selecciona `TU_IP` y busca la acción **«Editar DNS inverso»** (o «Reverse DNS»).
3. Escribe: `mail.TU_DOMINIO` y guarda.

El registro A de mail tiene que existir antes

IONOS solo acepta el DNS inverso si `mail.TU_DOMINIO` ya apunta a `TU_IP` (paso 3). Si da error, espera a que el paso 3 se haya propagado.

Comprueba desde PowerShell (puede tardar hasta unas horas):

EN TU PC · POWERSHELL

```
Resolve-DnsName TU_IP -Type PTR -Server 1.1.1.1
```

SALIDA ESPERADA

```
Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
xx.xx.xx.xx.in-addr.arpa       PTR    ...   Answer     mail.TU_DOMINIO
```

Comprueba antes de seguir

En `NameHost` aparece `mail.TU_DOMINIO`. Si aún sale un nombre de IONOS, sigue con la guía y vuelve a comprobarlo más tarde.

PARTE B

Preparar el servidor

A partir de aquí trabajas en la terminal. Vas a entrar en el servidor, ponerlo al día y dejarlo listo para usarlo de forma segura con tu propio usuario. Corresponde al **episodio 5**.

Paso 6 Episodio 5

Primer acceso por SSH

Por qué: SSH es la forma de controlar el servidor a distancia: lo que escribes en tu PC se ejecuta allí, y la conexión va cifrada.

EN TU PC · POWERSHELL

```
ssh root@TU_IP
```

La primera conexión a un servidor siempre muestra este aviso:

SALIDA ESPERADA

```
The authenticity of host 'TU_IP (TU_IP)' can't be established.
ED25519 key fingerprint is SHA256:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Después pega la **contraseña de root** (recuerda: no se ve nada al escribirla) y pulsa Enter. Si todo va bien, el cursor cambia a algo así:

SALIDA ESPERADA

```
root@ubuntu:~#
```

Comprueba qué tienes delante:

EN EL SERVIDOR

```
lsb_release -d
free -h
df -h /
```

Mantén esta ventana abierta

No cierres esta sesión de root hasta el paso 15. Si algo sale mal configurando el acceso, es tu red de seguridad para arreglarlo.

Comprueba antes de seguir

- El cursor muestra `root@...:~#` .
- `lsb_release -d` dice **Ubuntu 24.04**.

Paso 7 Episodio 5

Actualizar el sistema

Por qué: la imagen de Ubuntu que instala IONOS se creó hace semanas o meses.

EN EL SERVIDOR

```
apt update
apt upgrade -y
```

Ahora vas como `root`, así que no hace falta `sudo`. A partir del paso 12 trabajarás con tu usuario y escribirás `sudo` delante.

Si sale una pantalla morada: «Which services should be restarted?»

Es **needrestart**: te pregunta qué servicios reiniciar para que usen las librerías nuevas. Deja las opciones marcadas tal cual, pulsa **Tab** hasta `<Ok>` y Enter. Más adelante, cuando tengas Docker, **no marques el servicio docker** en esta pantalla, porque reiniciaría todos tus contenedores.

Si sale «Could not get lock /var/lib/dpkg/lock-frontend»

En el primer arranque, Ubuntu lanza solo sus actualizaciones automáticas y bloquea `apt` mientras tanto. **No borres ningún archivo de bloqueo.** Espera 5 minutos y repite el comando.

Comprueba si la actualización pide reiniciar (pasa cuando se actualiza el núcleo del sistema):

EN EL SERVIDOR

```
ls /var/run/reboot-required
```

- Si responde `/var/run/reboot-required`: hay que reiniciar. Escribe `reboot`, espera 1 minuto y vuelve a entrar con `ssh root@TU_IP`.
- Si responde `No such file or directory`: no hace falta reiniciar.

Comprueba antes de seguir

Un nuevo `apt update && apt upgrade -y` termina con `0 upgraded, 0 newly installed` (o «0 actualizados»).

Paso 8 Episodio 5

Comprobar el puerto 25

Por qué: el puerto 25 es el que usan los servidores para entregarse el correo entre ellos.

EN EL SERVIDOR

```
timeout 5 bash -c '</dev/tcp/gmail-smtp-in.l.google.com/25' && echo "Puerto 25: ABIERTO" ||
echo "Puerto 25: BLOQUEADO"
```

Si dice **BLOQUEADO**, abre una incidencia en IONOS (**Ayuda** → **Contactar**) o llama al soporte. Puedes usar este texto:

CONTENIDO DEL ARCHIVO · TEXTO PARA EL SOPORTE

```
Asunto: Desbloqueo del puerto 25 de salida en mi VPS

Hola. Tengo el VPS con IP TU_IP y voy a montar un servidor de correo
propio para mi dominio TU_DOMINIO (ya configurado el DNS inverso
mail.TU_DOMINIO). Necesito que desbloqueéis el puerto 25 TCP de salida.
Será un servidor con SPF, DKIM y DMARC y solo para mis propias cuentas.
Gracias.
```

Comprueba antes de seguir

Sabes si el puerto 25 está abierto. Si estaba bloqueado, tienes la incidencia abierta. **Sigue con la guía**: no lo necesitas hasta la temporada de correo.

Paso 9 Episodio 5

Nombre del servidor (hostname)

Por qué: el servidor se presenta con su nombre ante otros servidores, sobre todo al enviar correo.

EN EL SERVIDOR

```
hostnamectl set-hostname mail.TU_DOMINIO
sed -i '/^127\.0\.1\.1/d' /etc/hosts
echo "127.0.1.1 mail.TU_DOMINIO mail" >> /etc/hosts
```

Que no vuelva el nombre antiguo al reiniciar

Las imágenes de los proveedores llevan **cloud-init**, un programa que configura el servidor en el primer arranque y que a veces vuelve a poner el nombre original en cada reinicio. Se lo impedimos:

EN EL SERVIDOR

```
ls /etc/cloud/cloud.cfg.d/ && tee /etc/cloud/cloud.cfg.d/99-ebenezer.cfg > /dev/null <<'EOF'
# Conservar el hostname y el /etc/hosts que configuro a mano
preserve_hostname: true
manage_etc_hosts: false
EOF
```

¿Por qué se llama 99-ebenezer.cfg?

El nombre lo eliges tú; solo es obligatorio que termine en `.cfg`. cloud-init lee primero `/etc/cloud/cloud.cfg` y después todos los `.cfg` de `cloud.cfg.d/` por orden alfabético, y si un ajuste se repite **gana el último**. El `99-` hace que el nuestro se lea de los últimos y mande; `ebenezer` es una etiqueta para reconocer que lo creaste tú (puedes llamarlo `99-hostname-manual.cfg` si prefieres). Ojo: no todos los programas funcionan igual. En SSH (paso 15) **gana el primero**, y por eso allí el archivo empieza por `01-`.

Comprueba. Cierra la sesión con `exit` y vuelve a entrar para que el cursor muestre el nombre nuevo:

EN EL SERVIDOR

```
hostname
hostname -f
cat /etc/hosts
```

SALIDA ESPERADA

```
mail.TU_DOMINIO
mail.TU_DOMINIO
127.0.0.1 localhost
...
127.0.1.1 mail.TU_DOMINIO mail
```

Comprueba antes de seguir

- `hostname -f` devuelve `mail.TU_DOMINIO`.
- Al volver a entrar, el cursor es `root@mail:~#`.
- Si al usar `sudo` más adelante sale `unable to resolve host`, revisa la línea `127.0.1.1` de `/etc/hosts`.

Paso 10 Episodio 5

Zona horaria y hora

Por qué: los registros (logs) llevan la hora de cada evento.

EN EL SERVIDOR

```
timedatectl list-timezones | grep -E 'Madrid|Canary'
timedatectl set-timezone TU_ZONA_HORARIA
timedatectl
```

SALIDA ESPERADA

```
               Local time: sáb 2026-11-07 18:30:12 WET
           Universal time: sáb 2026-11-07 18:30:12 UTC
                 Time zone: Atlantic/Canary (WET, +0000)
System clock synchronized: yes
              NTP service: active
```

Comprueba antes de seguir

`Time zone` es la tuya y `System clock synchronized` dice **yes**. Si dice **no**, espera un par de minutos y repite `timedatectl`.

Paso 11 Episodio 5

Crear tu usuario con sudo

Por qué: `root` puede hacerlo todo sin preguntar: un error tecleando como root puede borrar el sistema, y es el usuario que todos los atacantes intentan adivinar.

EN EL SERVIDOR

```
adduser TU_USUARIO
usermod -aG sudo TU_USUARIO
groups TU_USUARIO
```

SALIDA ESPERADA

```
TU_USUARIO : TU_USUARIO users sudo
```

Elige bien la contraseña

Te la pedirá `sudo` cada vez que hagas algo de administrador. Que sea larga (una frase de 4 o 5 palabras va bien) y guárdala en tu gestor de contraseñas. Aunque no se use para entrar por SSH (eso será con clave), protege los permisos de administrador.

Prueba que funciona cambiando a ese usuario:

EN EL SERVIDOR

```
su - TU_USUARIO
sudo whoami
exit
```

Comprueba antes de seguir

`sudo whoami` respondió `root` después de pedirte tu contraseña.

Paso 12 Episodio 5

Acceso con clave SSH desde Windows

Por qué: una contraseña se puede adivinar probando millones de combinaciones, y hay robots haciéndolo contra todos los servidores de Internet a todas horas.

12.1 · Mira si ya tienes claves

EN TU PC · POWERSHELL

```
Get-ChildItem $env:USERPROFILE\.ssh
```

Si aparecen archivos como `id_ed25519` o `id_rsa`, **ya tienes claves** que seguramente usas para otros servidores. **No las sobrescribas nunca**: perderías el acceso a esos servidores. Por eso vamos a crear una clave con un nombre propio para este servidor.

En PowerShell, nunca escribas %USERPROFILE%

`%USERPROFILE%` es la forma de escribir tu carpeta de usuario en la consola antigua (CMD). En PowerShell no se traduce: crearía una carpeta que se llama literalmente `%USERPROFILE%` y la clave acabaría ahí. En PowerShell se escribe `$env:USERPROFILE`.

12.2 · Crea la clave

EN TU PC · POWERSHELL

```
ssh-keygen -t ed25519 -a 100 -f $env:USERPROFILE\.ssh\id_ed25519_lab -C "TU_USUARIO@lab"
```

Te pedirá una **frase de paso** (passphrase) dos veces. Es la contraseña que protege la clave privada: si alguien te roba el portátil, sin ella no puede usar la clave. Ponla y guárdala en tu gestor.

12.3 · Copia la clave pública al servidor

Windows no trae `ssh-copy-id` (el comando que se usa en Linux para esto), así que lo hacemos en una línea. **Es una sola línea**: comprueba que no se ha partido al copiarla.

EN TU PC · POWERSHELL

```
Get-Content $env:USERPROFILE\.ssh\id_ed25519_lab.pub | ssh TU_USUARIO@TU_IP "mkdir -p ~/.ssh
&& chmod 700 ~/.ssh && cat >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"
```

12.4 · Crea un atajo en tu PC

Para no escribir cada vez la IP, el usuario y la clave, crea un archivo de configuración de SSH en tu PC:

EN TU PC · POWERSHELL

```
notepad $env:USERPROFILE\.ssh\config
```

Si el Bloc de notas pregunta si quieres crear el archivo, di que sí. **Si el archivo ya existe y tiene contenido** (de otros servidores), no borres nada: añade esto al final. Pega:

CONTENIDO DEL ARCHIVO · C:\USERS\TUNOMBRE\.SSH\CONFIG

```
Host lab
    HostName TU_IP
    User TU_USUARIO
    IdentityFile ~/.ssh/id_ed25519_lab
    IdentitiesOnly yes
```

> **«lab» es un apodo tuyo, no el nombre del servidor**
>
> El nombre que va detrás de `Host` solo existe en este archivo de tu PC: lo eliges tú y el servidor nunca lo ve. No tiene relación con el hostname del servidor (`mail.TU_DOMINIO` , paso 9) ni con el DNS. Puedes tener un bloque por servidor (`Host lab` , `Host produccion` …) y entrar con `ssh lab` o `ssh produccion` . Ojo también con `HostName` : a pesar del nombre, **no** es el hostname del servidor, sino la dirección a la que conectar. Vale la IP o un nombre DNS como `mail.TU_DOMINIO` .

Guarda con **Ctrl+G** y cierra. Comprueba que se llama `config` y no `config.txt` :

EN TU PC · POWERSHELL

```
Get-ChildItem $env:USERPROFILE\.ssh
```

Si aparece `config.txt` , renómbralo: `Rename-Item $env:USERPROFILE\.ssh\config.txt config` .

12.5 · Prueba la entrada con clave

Abre una **ventana nueva** de PowerShell (deja la de root abierta) y escribe:

EN TU PC · POWERSHELL

```
ssh lab
```

Ahora te pide la **frase de paso de la clave** (`Enter passphrase for key...`), no la contraseña del servidor. Esa es la señal de que está usando la clave. El cursor será `TU_USUARIO@mail:~$`.

Opcional: que no te pida la frase de paso cada vez

Windows tiene un «agente» que guarda la clave desbloqueada mientras tu sesión de Windows está abierta. En PowerShell **como administrador**:

EN TU PC · POWERSHELL

```
Get-Service ssh-agent | Set-Service -StartupType Automatic
Start-Service ssh-agent
```

Y después, en un PowerShell normal: `ssh-add $env:USERPROFILE\.ssh\id_ed25519_lab`. Te pide la frase una vez y ya no la vuelve a pedir hasta que reinicies.

Haz copia de la clave privada

Copia `id_ed25519_lab` y `id_ed25519_lab.pub` a un pendrive o a tu gestor de contraseñas. Si se estropea el disco del PC y no tienes copia, tendrás que entrar por la consola de IONOS (Anexo A) para poner una clave nueva.

Comprueba antes de seguir

- `ssh lab` entra pidiendo la **frase de paso de la clave**.
- El cursor muestra `TU_USUARIO@mail:~$`.
- Desde aquí, todo se hace con tu usuario y `sudo`. La ventana de root sigue abierta, sin usarla.

Paso 13 Episodio 5

Memoria de intercambio (swap)

Por qué: el swap es un espacio del disco que Linux usa como RAM de reserva.

Desde aquí escribes en la sesión de tu usuario (`ssh lab`). Primero mira si ya hay swap:

EN EL SERVIDOR

```
free -h
swapon --show
```

Si `swapon --show` no muestra nada y en `free -h` la línea `Swap:` está a `0B`, créalo. Si ya hay swap, salta al paso 14.

EN EL SERVIDOR

```
sudo fallocate -l 2G /swapfile
sudo chmod 600 /swapfile
sudo mkswap /swapfile
sudo swapon /swapfile
echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
echo 'vm.swappiness=10' | sudo tee /etc/sysctl.d/99-swap.conf
sudo sysctl -p /etc/sysctl.d/99-swap.conf
```

SALIDA ESPERADA

```
NAME      TYPE SIZE USED PRIO
/swapfile file   2G   0B   -2
```

Comprueba antes de seguir

`swapon --show` muestra `/swapfile` de **2G**.

Paso 14 Episodio 5

Actualizaciones automáticas

Por qué: los fallos de seguridad se publican y se explotan en horas.

Comprueba que está activado:

EN EL SERVIDOR

```
systemctl is-enabled unattended-upgrades
cat /etc/apt/apt.conf.d/20auto-upgrades
```

SALIDA ESPERADA

```
enabled
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Si no ves esas dos líneas con `"1"`, actívalo con `sudo dpkg-reconfigure -plow unattended-upgrades` y responde **Yes**.

Ahora le añadimos tres ajustes: limpiar lo que sobra y reiniciar solo de madrugada si una actualización lo necesita.

EN EL SERVIDOR

```
sudo tee /etc/apt/apt.conf.d/52unattended-upgrades-local > /dev/null <<'EOF'
// Ebenezer: ajustes propios de las actualizaciones automáticas
Unattended-Upgrade::Remove-Unused-Kernel-Packages "true";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Automatic-Reboot "true";
Unattended-Upgrade::Automatic-Reboot-Time "04:30";
EOF
cat /etc/apt/apt.conf.d/52unattended-upgrades-local
```

En un servidor de cliente, decide tú

Para el laboratorio, el reinicio automático es lo cómodo. En el servidor de un cliente quizá prefieras `"false"` y reiniciar tú en una ventana de mantenimiento avisada. Lo veremos en el episodio de mantenimiento mensual.

Prueba la configuración sin instalar nada (simulación):

```
EN EL SERVIDOR
sudo unattended-upgrade --dry-run --debug 2>&1 | tail -n 5
```

Comprueba antes de seguir

La simulación termina sin líneas con `Error` o `E:`. Suele acabar con algo como `No packages found that can be upgraded unattended`, porque ya actualizaste en el paso 7.

PARTE C

Seguridad base

Ahora cerramos las puertas: solo se podrá entrar con tu clave y con tu usuario, el servidor tendrá su propio cortafuegos además del de IONOS, y fail2ban bloqueará a los robots que lo intenten. Corresponde al **episodio 6**.

Paso 15 Episodio 6

Endurecer SSH

Por qué: ahora mismo el servidor aún acepta contraseñas y deja entrar a root.

Antes de empezar: dos sesiones abiertas

Este es el único paso de la guía en el que te puedes quedar fuera del servidor si te equivocas. Ten abiertas **dos ventanas**: la de root del paso 6 y la de `ssh lab`. No cierres ninguna hasta el final de la comprobación. Una sesión ya abierta no se corta al cambiar la configuración, así que siempre podrás deshacer el cambio desde ella.

15.1 · Mira qué hay ya configurado

EN EL SERVIDOR

```
ls /etc/ssh/sshd_config.d/
sudo cat /etc/ssh/sshd_config.d/*.conf
```

La configuración del servidor SSH está en `/etc/ssh/sshd_config`, y al principio de ese archivo se cargan todos los `.conf` de la carpeta `sshd_config.d/`, por orden alfabético. **Importante:** en SSH, cuando un ajuste aparece varias veces, **gana el primero que se lee**. Muchos proveedores dejan ahí un `50-cloud-init.conf` con `PasswordAuthentication yes`. Por eso nuestro archivo se llamará `01-...`: así se lee el primero y manda sobre los demás.

15.2 · Crea la configuración

EN EL SERVIDOR

```
sudo tee /etc/ssh/sshd_config.d/01-seguridad.conf > /dev/null <<'EOF'
# Ebenezer: endurecimiento de SSH
PermitRootLogin no
PasswordAuthentication no
KbdInteractiveAuthentication no
PubkeyAuthentication yes
AuthenticationMethods publickey
MaxAuthTries 3
LoginGraceTime 30
X11Forwarding no
AllowUsers TU_USUARIO
EOF
cat /etc/ssh/sshd_config.d/01-seguridad.conf
```

15.3 · Comprueba la sintaxis y aplica

EN EL SERVIDOR

```
sudo sshd -t && echo "Configuración correcta"
sudo systemctl restart ssh
```

> **Si sshd -t dice «Missing privilege separation directory: /run/sshd»**
> Es un aviso de Ubuntu 24.04, no un error de tu configuración. Ejecuta `sudo mkdir -p /run/sshd` y repite el test.

Comprueba qué valores está usando SSH de verdad (ya mezclados todos los archivos):

EN EL SERVIDOR

```
sudo sshd -T | grep -E
'^(permitrootlogin|passwordauthentication|kbdinteractiveauthentication|pubkeyauthentication|all
owusers|maxauthtries)'
```

SALIDA ESPERADA

```
permitrootlogin no
pubkeyauthentication yes
passwordauthentication no
kbdinteractiveauthentication no
maxauthtries 3
allowusers TU_USUARIO
```

15.4 · La prueba de verdad, desde una ventana nueva

Abre una **tercera** ventana de PowerShell y prueba estas tres cosas:

EN TU PC · POWERSHELL

```
ssh lab
ssh root@TU_IP
ssh -o PubkeyAuthentication=no TU_USUARIO@TU_IP
```

Comando	Resultado correcto	Qué demuestra
`ssh lab`	Entra (pidiendo la frase de la clave). Escribe `exit`	Tu acceso con clave funciona
`ssh root@TU_IP`	`Permission denied (publickey).`	root ya no puede entrar
`ssh -o PubkeyAuthentication=no ...`	`Permission denied (publickey).` sin pedir contraseña	Las contraseñas ya no sirven

Si ssh lab NO entra

No cierres las otras dos ventanas. Desde la de root, borra el archivo y reinicia SSH para volver a como estaba:

```
EN EL SERVIDOR
rm /etc/ssh/sshd_config.d/01-seguridad.conf
systemctl restart ssh
```

Después revisa el paso 12 (¿está la clave en `~/.ssh/authorized_keys` de tu usuario?) y el `AllowUsers` (¿está bien escrito tu usuario?).

Comprueba antes de seguir

- Las tres pruebas dan el resultado de la tabla.
- **Solo entonces**, cierra la ventana de root con `exit`. Ya no la necesitas: a partir de ahora siempre entrarás con `ssh lab`.

Paso 16 Episodio 6

Cortafuegos UFW

Por qué: el firewall de IONOS (paso 4) es la primera capa, fuera del servidor.

Capa	Dónde está	Qué protege si la otra falla
Firewall de IONOS	En la red de IONOS, antes de tu servidor	Un servicio mal configurado dentro del servidor
UFW	Dentro del servidor (Ubuntu)	Un error en el panel de IONOS, o un cambio de proveedor

UFW (Uncomplicated Firewall) viene instalado pero apagado. Primero las reglas, después lo encendemos. **En ese orden**: si lo enciendes sin permitir SSH, te echa del servidor.

```
EN EL SERVIDOR
sudo ufw status
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow OpenSSH comment 'SSH'
sudo ufw show added
```

Ahora sí, enciéndelo:

```
EN EL SERVIDOR
sudo ufw enable
sudo ufw status verbose
```

Al encenderlo avisa `Command may disrupt existing ssh connections. Proceed with operation (y|n)?`. Como ya permitiste SSH, responde `y`.

SALIDA ESPERADA

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp (OpenSSH)           ALLOW IN    Anywhere                   # SSH
22/tcp (OpenSSH (v6))      ALLOW IN    Anywhere (v6)              # SSH
```

Para más adelante: Docker y UFW

Cuando instales Docker (episodio 8) verás que Docker puede abrir puertos **saltándose UFW**. No es un fallo de esta guía: lo explicamos y lo resolvemos en ese episodio.

Comprueba antes de seguir

- `sudo ufw status` dice **active** con solo el 22.
- Desde una ventana nueva, `ssh lab` sigue entrando.

Paso 17 Episodio 6

fail2ban para SSH

Por qué: aunque los robots ya no pueden entrar (no tienen tu clave), siguen intentándolo miles de veces al día: llenan los registros y gastan recursos.

17.1 · Instálalo

EN EL SERVIDOR

```
sudo apt install -y fail2ban python3-systemd
cat /etc/fail2ban/jail.d/defaults-debian.conf
```

17.2 · Averigua la IP de tu casa

Para no bloquearte a ti mismo si te equivocas varias veces, le diremos a fail2ban que nunca bloquee tu conexión de casa. En tu PC:

EN TU PC · POWERSHELL

```
curl.exe -4 -s ifconfig.me
```

Apúntala como TU_IP_CASA.

Si tu IP de casa cambia

La mayoría de conexiones domésticas tienen IP dinámica: cambia cada cierto tiempo o al reiniciar el router. No pasa nada: la línea solo deja de protegerte a ti. Si un día te bloquea, mira el Anexo A. Si no quieres poner tu IP, borra TU_IP_CASA de la línea y deja solo `127.0.0.1/8 ::1`.

17.3 · Configúralo

Los ajustes propios se ponen en `jail.local`. El archivo principal (`jail.conf`) no se toca nunca, porque las actualizaciones lo sobrescriben.

EN EL SERVIDOR

```
sudo tee /etc/fail2ban/jail.local > /dev/null <<'EOF'
[DEFAULT]
# Nunca bloquear: el propio servidor y tu conexión de casa
ignoreip = 127.0.0.1/8 ::1 TU_IP_CASA
# Tiempo de bloqueo, ventana de vigilancia e intentos permitidos
bantime  = 1h
findtime = 10m
maxretry = 5
# Cada vez que una IP reincide, el bloqueo dura más (hasta 1 semana)
bantime.increment = true
bantime.maxtime   = 1w

[sshd]
enabled = true
mode    = aggressive
EOF
cat /etc/fail2ban/jail.local
```

Los comentarios, siempre en su propia línea

En los archivos de fail2ban, un comentario al final de una línea (`bantime = 1h # una hora`) se lee como parte del valor y rompe la configuración. Por eso todos los comentarios de esta guía van solos en su línea.

17.4 · Arranca y comprueba

EN EL SERVIDOR

```
sudo systemctl enable fail2ban
sudo systemctl restart fail2ban
sudo fail2ban-client status
sudo fail2ban-client status sshd
```

SALIDA ESPERADA

```
Status for the jail: sshd
├─ Filter
|  ├─ Currently failed: 2
|  ├─ Total failed:     14
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   ├─ Currently banned: 1
   ├─ Total banned:     1
   `- Banned IP list:   203.0.113.45
```

Si `status` da error, mira el motivo con `sudo journalctl -u fail2ban -n 30 --no-pager`. Casi siempre es una errata en `jail.local`.

Si te bloqueas a ti mismo

Desde otra conexión (los datos del móvil, por ejemplo) o desde la consola de IONOS:

```
EN EL SERVIDOR
sudo fail2ban-client set sshd unbanip LA_IP_BLOQUEADA
```

Comprueba antes de seguir

- `sudo fail2ban-client status` muestra `Jail list: sshd`.
- Vuelve en una hora y repite `status sshd`: verás intentos fallidos y, probablemente, alguna IP bloqueada.

Paso 18 Episodio 6

Comprobación final e instantánea

Por qué: antes de construir nada encima, comprobamos que todo está como debe y que sobrevive a un reinicio.

18.1 · Repaso de todo

```
EN EL SERVIDOR
hostname -f
timedatectl | grep -E 'Time zone|synchronized'
swapon --show
systemctl is-active unattended-upgrades
sudo sshd -T | grep -E '^(permitrootlogin|passwordauthentication)'
sudo ufw status
sudo fail2ban-client status sshd | grep -E 'Currently|Total'
```

Comprobación	Resultado correcto
`hostname -f`	`mail.TU_DOMINIO`
Zona y hora	Tu zona y `synchronized: yes`
Swap	`/swapfile` de 2G
Actualizaciones automáticas	`active`
SSH	`permitrootlogin no` y `passwordauthentication no`
UFW	`Status: active` con solo `22/tcp`
fail2ban	Muestra contadores (aunque estén a 0)

18.2 · Reinicia y vuelve a comprobar

```
EN EL SERVIDOR
sudo reboot
```

La conexión se corta (es normal). Espera un minuto, vuelve a entrar con `ssh lab` y repite el bloque 18.1. Todo debe seguir igual. Así compruebas que nada depende de algo que solo estaba en memoria, y que cloud-init no ha deshecho el nombre del paso 9.

18.3 · Haz una instantánea

1. En el panel de IONOS: **Servidores & Cloud** → tu servidor → **Instantáneas** (Snapshots) → **Crear**.
2. Ponle un nombre que diga en qué punto está: `01-servidor-base`.
3. Espera a que termine (unos minutos).

> **Para qué sirve**
>
> Antes de cada temporada del curso, haz una instantánea nueva. Si un episodio sale mal, restauras la instantánea y repites desde ese punto. Es exactamente lo que harás tú antes de grabar cada vídeo.

> **Comprueba antes de seguir**
>
> - El repaso 18.1 da todo correcto **después** del reinicio.
> - La instantánea `01-servidor-base` aparece en el panel.
> - **Enhorabuena: tienes un servidor base seguro.** La siguiente guía (episodio 7) monta Nginx con certificados HTTPS sobre él.

ANEXOS

Para cuando algo no sale

Consulta esto antes de pedir ayuda: la mayoría de los atascos de esta guía están aquí.

Anexo A · Problemas frecuentes y cómo salir de ellos

Lo que ves	Qué pasa	Qué hacer
`Connection timed out` al hacer `ssh`	Nada responde en ese puerto: firewall de IONOS sin el 22, IP mal escrita o servidor apagado	Revisa la IP, la política de firewall (paso 4) y que el servidor esté encendido en el panel
`Connection refused`	El servidor responde, pero SSH no está funcionando	Entra por la consola de IONOS (abajo) y mira `sudo systemctl status ssh`
`Permission denied (publickey)` con `ssh lab`	El servidor no acepta tu clave: usuario mal escrito, clave no copiada o archivo `config` mal	Prueba `ssh -v lab`: el modo detallado dice qué clave intenta usar. Revisa el paso 12
`WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!`	La huella del servidor cambió. Normal si has **reinstalado** el VPS o restaurado una instantánea antigua	Si has reinstalado: `ssh-keygen -R TU_IP` en tu PC y vuelve a conectar. Si no has tocado nada, no conectes y averigua por qué
`Could not get lock /var/lib/dpkg/lock-frontend`	Otra instalación (normalmente las actualizaciones automáticas) está en marcha	Espera 5 minutos y repite. No borres archivos de bloqueo
`sudo: unable to resolve host mail.TU_DOMINIO`	Falta o está mal la línea `127.0.1.1` de `/etc/hosts`	Repite el paso 9
`TU_USUARIO is not in the sudoers file`	El usuario no está en el grupo sudo	Desde la consola de IONOS como root: `usermod -aG sudo TU_USUARIO`
fail2ban te ha bloqueado	Has fallado demasiadas veces seguidas	Espera 1 hora, o entra desde los datos del móvil y ejecuta `sudo fail2ban-client set sshd unbanip TU_IP_CASA`
El nombre vuelve a ser `ubuntu` tras reiniciar	cloud-init lo restaura	Revisa el archivo `/etc/cloud/cloud.cfg.d/99-ebenezer.cfg` del paso 9
El Bloc de notas guardó `config.txt`	Windows añadió la extensión	`Rename-Item $env:USERPROFILE\.ssh\config.txt config`

Te has quedado fuera del todo: la consola de IONOS

Aunque SSH esté roto o te hayas bloqueado, siempre puedes entrar por la **consola remota** del panel: **Servidores & Cloud** → tu servidor → **Acciones** → **Consola remota** (KVM). Es como tener una pantalla y un teclado conectados al servidor: no pasa por la red, así que no le afectan ni SSH ni los cortafuegos.

- Entra como `root` con la **contraseña de root** (por eso hay que guardarla). `PermitRootLogin no` solo prohíbe root **por SSH**, no en la consola.
- La consola no admite pegar texto con fiabilidad: escribe los comandos a mano, y cortos.

- Para deshacer el endurecimiento de SSH: `rm /etc/ssh/sshd_config.d/01-seguridad.conf` y `systemctl restart ssh`.
- Para apagar UFW mientras arreglas algo: `ufw disable` (y vuelve a activarlo al terminar).

> **Si también has perdido la contraseña de root**
>
> En el panel de IONOS hay una opción para **restablecer la contraseña de root** en el menú del servidor. Si no la encuentras, restaura la instantánea del paso 18.

Anexo B · Puertos abiertos al terminar esta guía

Este bloque aparece al final de cada guía. Es tu inventario: si un puerto no está aquí, debe estar cerrado.

Puerto	Servicio	Firewall de IONOS	UFW	Qué lo protege
22/TCP	SSH	Abierto	Abierto	Solo clave (sin contraseñas), sin root, `AllowUsers`, fail2ban

Para comprobar qué está escuchando de verdad en el servidor:

```
EN EL SERVIDOR
sudo ss -tulpn
```

Ahora mismo deberías ver el **22** (sshd), el **53** en `127.0.0.53` (el DNS interno de Ubuntu, que solo escucha dentro del propio servidor) y quizá el **68** o **546** (DHCP, para recibir la configuración de red). Nada más hacia fuera.

Anexo C · Chuleta de comandos

Para...	Comando
Entrar al servidor	`ssh lab`
Salir del servidor	`exit`
Actualizar todo a mano	`sudo apt update && sudo apt upgrade -y`
Saber si hay que reiniciar	`ls /var/run/reboot-required`
Reiniciar el servidor	`sudo reboot`
Ver el estado de un servicio	`systemctl status ssh` (sal con **q**)
Ver los registros de un servicio	`sudo journalctl -u ssh -n 50 --no-pager`
Seguir los registros en directo	`sudo journalctl -u ssh -f` (sal con **Ctrl+C**)
Probar la configuración de SSH	`sudo sshd -t`
Reglas del cortafuegos	`sudo ufw status numbered`
Abrir un puerto en UFW	`sudo ufw allow 443/tcp comment 'HTTPS'`
Borrar una regla de UFW	`sudo ufw delete NÚMERO` (el de `status numbered`)
Estado de fail2ban	`sudo fail2ban-client status sshd`
Desbloquear una IP	`sudo fail2ban-client set sshd unbanip IP`
Puertos en escucha	`sudo ss -tulpn`
Memoria y disco	`free -h` · `df -h`
Quién ha entrado por SSH	`last -n 10`

Si te atascas

Antes de pedir ayuda, copia tres cosas: el **comando exacto** que escribiste, el **mensaje de error completo** y la salida de `sudo journalctl -u NOMBRE_DEL_SERVICIO -n 30 --no-pager`. Con eso, el 90 % de los problemas se resuelven a la primera.