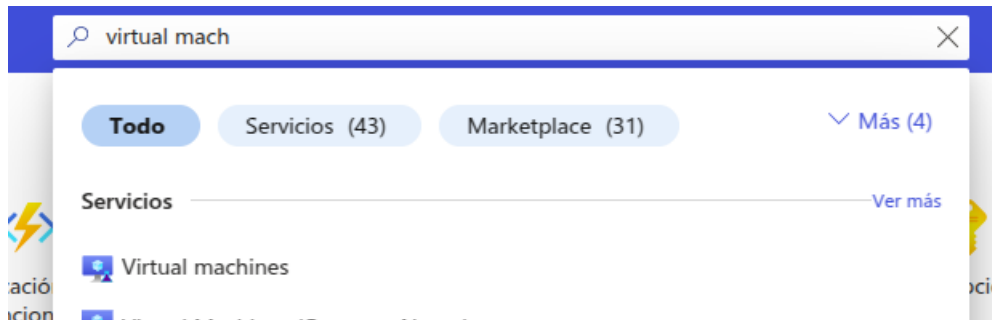
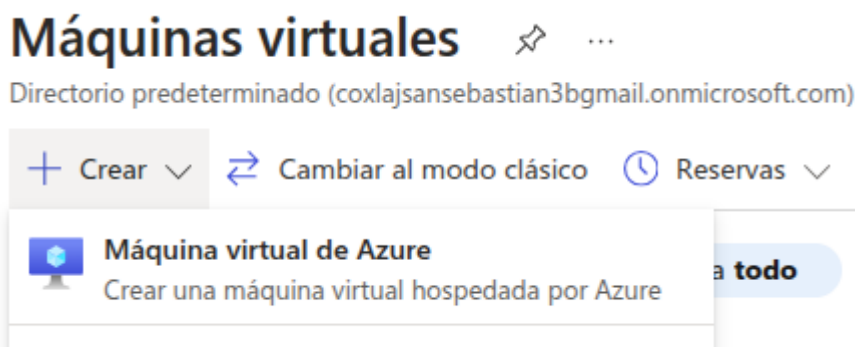


## Configuración de Virtual Machine en Azure

1. Buscar el servicio de Azure Functions.



2. Creamos un nuevo servicio y seleccionamos Máquina Virtual de Azure.



3. Se nos mostrará la siguiente ventana.

**Datos básicos** Discos Redes Administración Supervisión Opciones avanzadas Etiquetas Revisar y crear

Cree una máquina virtual que ejecute Linux o Windows. Seleccione una imagen de Azure Marketplace o use una imagen personalizada propia. Complete la pestaña Conceptos básicos y, después, use Revisar y crear para aprovisionar una máquina virtual con parámetros predeterminados o bien revise cada una de las pestañas para personalizar la configuración.  
[Más información](#)

**Detalles del proyecto**

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción \* ⓘ

Grupo de recursos \* ⓘ   
[Crear nuevo](#)

**Detalles de instancia**

Nombre de máquina virtual \* ⓘ

Región \* ⓘ

Opciones de disponibilidad ⓘ

Opciones de zona ⓘ

☒ Zona autoseleccionada  
Elija hasta 3 zonas de disponibilidad, una máquina virtual por zona

☐ Zona seleccionada por Azure (versión preliminar)  
Permitir que Azure asigne la mejor zona para sus necesidades

Zona de disponibilidad \* ⓘ

Ahora puede seleccionar varias zonas. Si selecciona varias zonas, se creará una VM

4. Seleccionamos la suscripción que tenemos y creamos un nuevo Grupo de recurso para este servicio.

Suscripción \* ⓘ

Grupo de recursos \* ⓘ

[Crear nuevo](#)

Un grupo de recursos es un contenedor que tiene los recursos relacionados de una solución de Azure.

Nombre \*

[Aceptar](#) [Cancelar](#)

**Detalles de instancia**

Nombre de máquina virtual \* ⓘ

Región \* ⓘ

Opciones de disponibilidad ⓘ

Opciones de zona ⓘ

5. Le asignamos un nombre a la máquina virtual, seleccionamos una región y en tipo de Seguridad colocamos “Estándar”.

**Detalles de instancia**

Nombre de máquina virtual \* ⓘ

Región \* ⓘ

Opciones de disponibilidad ⓘ

Tipo de seguridad ⓘ

**i** La máquina virtual de inicio de confianza es necesaria cuando se usan imágenes de la Galería de 1P.

6. Seleccionamos una imagen, en este caso se selecciono Ubuntu 22.04, la arquitectura de x64 y el tamaño del disco lo mas bajo posible.

Imagen \* ⓘ

[Ver todas las imágenes](#) | [Configurar la generación de máquinas virtuales](#)

**✓** Esta imagen es compatible con características de seguridad adicionales. [Haga clic aquí para cambiar a la versión de inicio seguro.](#)

Arquitectura de VM ⓘ ☐ ☒

Ejecución de Azure Spot con descuento ⓘ ☐

Tamaño \* ⓘ

[Ver todos los tamaños](#)

Habilitar hibernación ⓘ ☐

**i** El tamaño seleccionado no admite la hibernación. Elija un tamaño compatible con Hibernar para habilitar esta característica. [Más información](#)

7. En la siguiente sección seleccionamos como nos podemos conectar a la VM, en este caso se recomienda usar SSH para usar herramientas como Termius. Tomar en cuenta que en “Nombre de Usuario” será el usuario con que nos conectaremos si usamos Termius, además se estará creando una clave SSH para conectarse.

#### Cuenta de administrador

Tipo de autenticación ⓘ

- ☒ Clave pública SSH  
☐ Contraseña

**i** Ahora, Azure genera automáticamente un par de claves SSH y le permite almacenarlo para usarlo en el futuro. Es una forma rápida, sencilla y segura de conectarse a la máquina virtual.

Nombre de usuario \* ⓘ

azureuser ✓

Origen de clave pública SSH

Generar un par de claves nuevo ▾

Tipo de clave SSH

- ☒ Formato RSA SSH  
☐ Formato Ed25519 SSH

**i** Ed25519 proporciona un nivel de seguridad fijo de no más de 128 bits para claves de 256 bits, mientras que RSA podría ofrecer una mejor seguridad con claves de más de 3072 bits.

Nombre de par de claves \*

backendvm\_key ✓

8. La siguiente sección es de reglas de entrada en la vm, por el momento solo dejaremos el puerto 22, el cual sirve para conectarse desde SSH.

#### Reglas de puerto de entrada

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.

Puertos de entrada públicos \* ⓘ

- ☐ Ninguno  
☒ Permitir los puertos seleccionados

Seleccionar puertos de entrada \*

SSH (22) ▾

**⚠** Esto permitirá que todas las direcciones IP accedan a la máquina virtual. Esto solo se recomienda para las pruebas. Use los controles avanzados de la pestaña Redes a fin de crear reglas para limitar el tráfico entrante a las direcciones IP conocidas.

9. En la siguiente pestaña de “Discos”, seleccionamos un disco más económico, en este caso HDD estándar.

Datos básicos **Discos** Redes Administración Supervisión Opciones avanzadas Etiquetas Revisar y crear

Las máquinas virtuales de Azure tienen un disco de sistema operativo y un disco temporal para el almacenamiento a corto plazo. Puede asociar discos de datos adicionales. El tamaño de la máquina virtual determina el tipo de almacenamiento que puede usar y la cantidad de datos que permiten los discos. [Más información](#)

#### Cifrado del disco de la máquina virtual

El cifrado de Azure Disk Storage cifra automáticamente los datos almacenados en los discos administrados de Azure en reposo (discos de datos y del sistema operativo) de forma predeterminada al guardarlos en la nube.

Cifrado en el host ⓘ

☐

**i** El cifrado en el host no está registrado para la suscripción seleccionada.  
[Más información](#)

#### Disco del SO

Tamaño del disco del SO ⓘ

Valor predeterminado de la imagen (30 GiB) ▼

Tipo de disco del sistema operativo \* ⓘ

HDD estándar (almacenamiento con redundancia local) ▼

El tamaño de la máquina virtual seleccionada es compatible con los discos premium. Se recomienda SSD Premium para elevadas cargas de trabajo de E/S por segundo. Las máquinas virtuales con discos SSD Premium optan al acuerdo de nivel de servicio de conectividad del 99,9%.

Eliminar con VM ⓘ

☒

10. Las otras configuraciones podemos dejarlo como están por defecto si deseamos, por lo cual podemos darle directamente en “Revisar y Crear”. Se nos mostrará un resumen de las configuraciones. Click en “Crear”.

#### Datos básicos

Suscripción	MiSuscripción
Grupo de recursos	(nuevo) vm
Nombre de máquina virtual	backendvm
Región	Central US
Opciones de disponibilidad	No se requiere redundancia de la infraestructura
Opciones de zona	Zona autoseleccionada
Tipo de seguridad	Estándar
Imagen	Ubuntu Server 24.04 LTS - Gen2
Arquitectura de VM	x64
Tamaño	Standard D2s v3 (2 vcpu, 8 GiB de memoria)
Habilitar hibernación	No
Tipo de autenticación	Clave pública SSH
Nombre de usuario	azureuser
Formato de clave SSH	RSA
Nombre de par de claves	backendvm_key
Puertos de entrada públicos	SSH
Azure de acceso puntual	No

#### Discos

Tamaño del disco del SO	Valor predeterminado de la imagen
Tipo de disco del sistema operativo	LRS de HDD estándar
Usar discos administrados	Sí

< Anterior

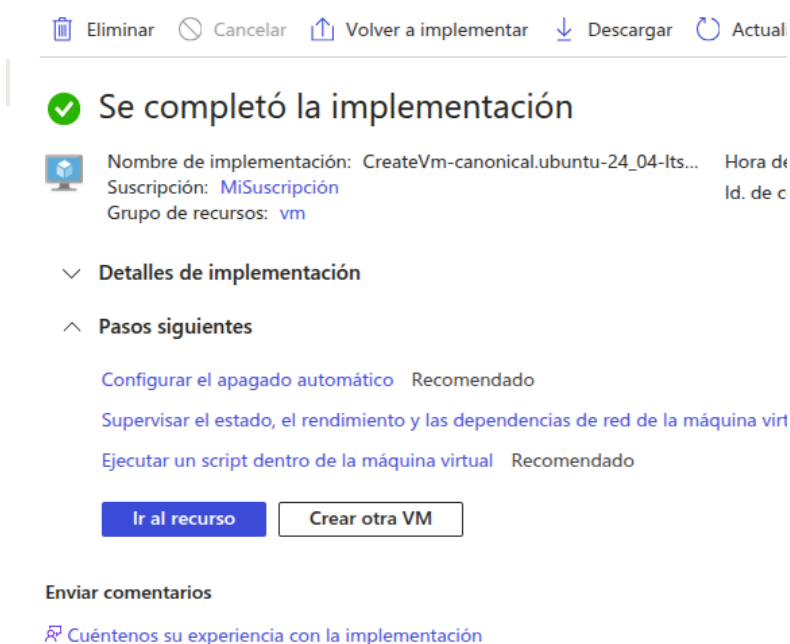
Siguiente >

Crear

11. Al darle crear nos mostrará una ventana para descargar la clave SSH, por lo cual lo descargamos.



12. Al crearse damos click en “Ir al recurso”.



13. Se nos mostrará la información general de la VM, como la ip pública que nos servirá para conectarnos.

Sistema operativo : Linux (ubuntu 24.04)

Tamaño : Standard D2s v3 (2 vcpu, 8 GiB de memoria)

Dirección IP pública : [52.176.154.160](#)

Red virtual/subred : [backendvm-vnet/default](#)

Nombre DNS : [Sin configurar](#)

Estado de mantenimiento : -

Hora de creación : 18/3/2025, 1:33 UTC

14. Para permitir la conexión con un frontend por ejemplo, debemos crear más reglas de entrada. Por lo cual nos debemos dirigir a configuración de Redes.

backendvm | Configuración de red

Máquina virtual

Buscar

Información general

Registro de actividad

Control de acceso (IAM)

Etiquetas

Diagnosticar y solucionar problemas

Visualizador de recursos

Conectar

Redes

Configuración de red

Equilibrio de carga

Grupos de seguridad de la aplicación

Administrador de red

Configuración

Disponibilidad y escala

Seguridad

Copia de seguridad y recuperación ante desastres

Operaciones

Supervisión

Esta es una nueva experiencia. [Proporcione comentarios](#)

Interfaz de red : backendvm511

Red virtual / subred : backendvm-vnet / default

Dirección IP pública : 52.176.154.160

Dirección IP privada : 10.0.0.4

Reglas de seguridad de ad... : 0 (Configurar)

Equilibradores de carga : 0 (Configurar)

Grupos de seguridad de la a... : 0 (Configurar)

Grupo de seguridad de red : backendvm-nsg

Redes aceleradas : Habilitado

Reglas de seguridad vigentes : 0

Reglas

Contraer todo

Grupo de seguridad de red backendvm-nsg (conectado a networkInterface: backendvm511)

Afecta a 0 subredes, 1 interfaces de red

Crear ACL del puerto

Buscar reglas

Origen == todo


Destino == todo

Protocolo == todo

Acción == todo

Prioridad ↑	Nombre	Puerto	Protocolo	Origen	Destino	Acción
Reglas de puerto de entrada (4)						
300	SSH	22	TCP	Cualquiera	Cualquiera	Allow
65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Cualquiera	Cualquiera	AzureLoadBalancer	Cualquiera	Allow
65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Deny
Reglas de puerto de salida (3)						

15. En esta sección podremos visualizar las reglas de entrada y salida.

✓  Grupo de seguridad de red **backendvm-nsg** (conectado a networkInterface: **backendvm511**)  
Afecta a 0 subredes, 1 interfaces de red




Buscar reglas		Origen == todo	Destino == todo	Protocolo == todo	Acción == todo		
Prioridad ↑	Nombre	Puerto	Protocolo	Origen	Destino		
▼	Reglas de puerto de entrada (4)						
300	⚠ SSH	22	TCP	Cualquiera	Cualquiera		
65000	AllowVnetInBound ⓘ	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork		
65001	AllowAzureLoadBalancerInBound ⓘ	Cualquiera	Cualquiera	AzureLoadBalancer	Cualquiera		
65500	DenyAllInBound ⓘ	Cualquiera	Cualquiera	Cualquiera	Cualquiera		
>	Reglas de puerto de salida (3)						


16. Damos click al grupo de seguridad para editar las reglas.


 Grupo de seguridad de red **backendvm-nsg** (conectado a networkInterface: **backendvm511**)  
Afecta a 0 subredes, 1 interfaces de red


Origen == todo Destino == todo Protocolo == todo Acción == todo


17. Al ingresar al grupo de seguridad elegimos “Configuraciones” y “Reglas de Entrada”.


 **backendvm-nsg**    
Grupo de seguridad de red


 Información general

 Registro de actividad


 Control de acceso (IAM)


 Etiquetas


 Diagnosticar y solucionar problemas

 Visualizador de recursos

✓ Configuración

 Reglas de seguridad de entrada

 Reglas de seguridad de salida

 Interfaces de red

^ I

Grupos

Ubicaciones

Suscripciones

Id. de recursos

Etiquetas

Prioridad

30

65

65

## 18. Se nos mostrarán las reglas de entrada y le damos en “Agregar”.


[+ Agregar](#) [🔍 Ocultar las reglas predeterminadas](#) [🔄 Actualizar](#) [🗑 Eliminar](#) [🗨 Enviar comentarios](#)

Las reglas de seguridad del grupo de seguridad de red se evalúan por prioridad mediante la combinación de origen, puerto de origen, destino, puerto de destino, protocolo y dirección que una regla existente. No puede eliminar las reglas de seguridad predeterminadas, pero puede invalidarlas con reglas q

Puerto == todo Protocolo == todo Origen == todo Destino == todo

	Prioridad ↑↓	Nombre ↑↓	Puerto ↑↓	Protocolo ↑↓	Origen ↑↓
<input type="checkbox"/>	300	⚠ SSH	22	TCP	Cualquiera
<input type="checkbox"/>	65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork
<input type="checkbox"/>	65001	AllowAzureLoadBalancerInBo...	Cualquiera	Cualquiera	AzureLoadBalancer
<input type="checkbox"/>	65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera

## 19. Configuramos las reglas según sea necesario, en este caso como ejemplo se configura que pueden entrar cualquier petición desde el puerto 3001, pero no es recomendable permitir que cualquier tráfico ingrese a la VM.

 **Agregar regla de seguridad de entrada** ✕  
backendvm-nsg

Origen ⓘ

Any

Intervalos de puertos de origen \* ⓘ

\*

Destino ⓘ

Any

Servicio ⓘ

Custom

Intervalos de puertos de destino \* ⓘ

3000 ✓

Protocolo

☒ Any

☐ TCP

☐ UDP

☐ ICMPv4

Acción

☒ Permitir

☐ Denegar

Prioridad \* ⓘ

310 ✓

Nombre \*

AllowAnyCustom3000Inbound ✓

Descripción

Agregar

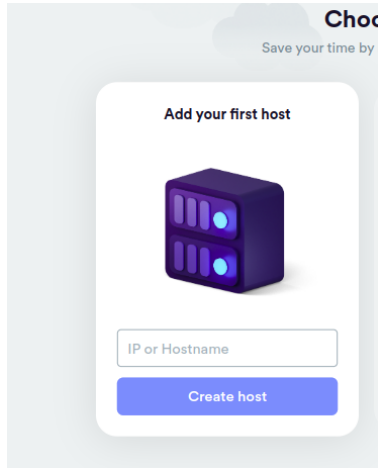
Cancelar

[🗨 Enviar comentario](#)



20. Finalmente se le da agregar. Se pueden agregar de la misma forma las reglas necesarias, para reglas de salida se realizan los mismos pasos.

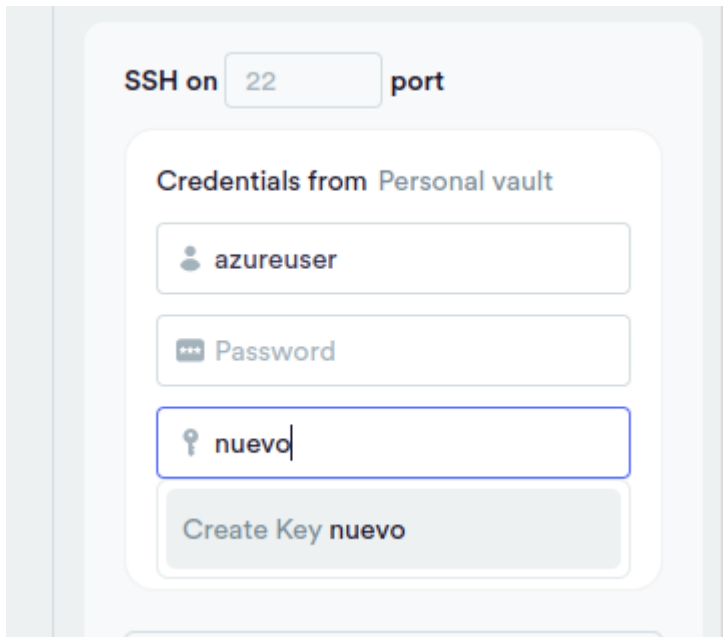
21. Para conectarnos por medio de Termius, debemos darle click en New Host.



22. Colocamos la IP pública de la VM y el nombre de Usuario que colocamos al momento de crear la VM, en este caso se dejó por defecto azureuser.

A screenshot of the Termius host configuration form. It is divided into three main sections: 'Address', 'General', and 'SSH'. The 'Address' section has a blue icon with three dots and a text input field containing '52.176.154.160'. The 'General' section has four input fields: 'EjemploConferencia', 'Parent Group', 'Tags', and 'Backspace' (with 'Default' to its right). The 'SSH' section has a label 'SSH on' followed by a text input field containing '22' and the word 'port'. Below this is a section titled 'Credentials from Personal vault' with two input fields: one containing 'azureuser' and another labeled 'Password'. At the bottom, there is a plus sign icon followed by the text 'Key, Certificate, FIDO2'.

23. Luego damos click en “+key” y seleccionamos Key. Y damos click a crear uno nuevo.



SSH on 22 port

Credentials from Personal vault

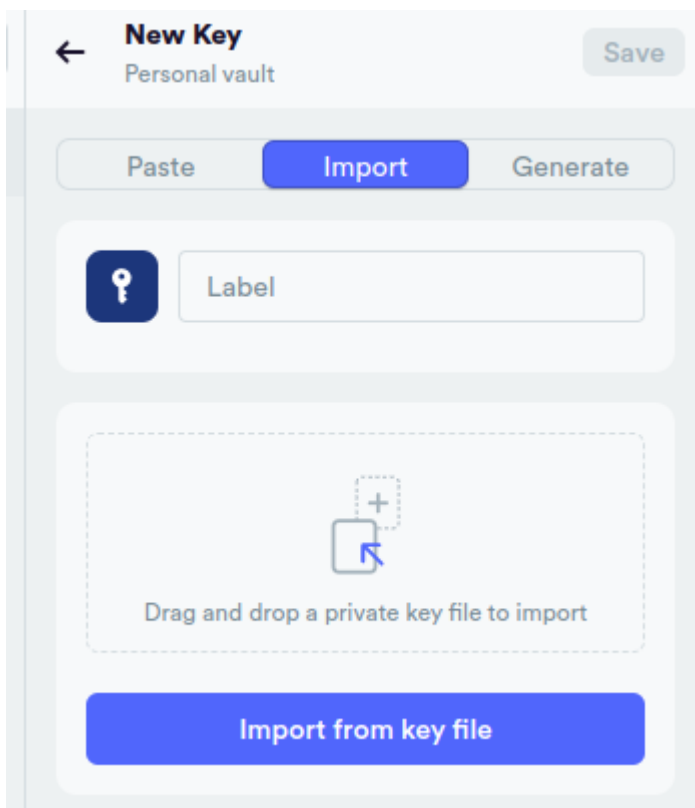
azureuser

Password

Key nuevo

Create Key nuevo

24. Seleccionamos import e importamos la llave que descargamos anteriormente y damos save.



New Key

Personal vault

Save

Paste Import Generate

Label

Drag and drop a private key file to import

Import from key file

25. Finalmente damos click en “Connet” y estaremos conectados a la VM.

≡ 🔔 🗨️ Vaults 📁 SFTP X EjemploConferencia +

Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1021-azure x86\_64)

\* Documentation: <https://help.ubuntu.com>  
\* Management: <https://landscape.canonical.com>  
\* Support: <https://ubuntu.com/pro>

System information as of Tue Mar 18 01:58:22 UTC 2025

System load:	0.1	Processes:	129
Usage of /:	5.4% of 28.02GB	Users logged in:	0
Memory usage:	3%	IPv4 address for eth0:	10.0.0.4
Swap usage:	0%		

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.  
See <https://ubuntu.com/esm> or run: `sudo pro status`

The list of available updates is more than a week old.  
To check for new updates run: `sudo apt update`

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in `/usr/share/doc/*/copyright`.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "`sudo <command>`".  
See "`man sudo_root`" for details.

azureuser@backendvm:~\$ █