



**Proyecto Final de Ciberseguridad: "Red Team vs Blue Team en la Nube:
Ataque y Defensa en Azure"**

Vargas Ramírez Kendall

Retana Mora Fabián Andrés

Sanabria Alpizar Gustavo Adolfo

Palacio Solorzano Luis Fernando

Marín Fallas Kevin

Bejarano Cubero María Fernanda

Facultad de Ingeniería, Universidad Fidélitas

CY-302 Programación Avanzada

Andrés Felipe Vargas Rivera

09 de octubre de 2025

Integrantes

Integrantes Red Team:

- Kendall Vargas Ramírez
- Luis Palacio
- María Fernanda Bejarano

Integrantes Blue Team:

- Gustavo Sanabria
- Fabián Retana
- Kevin Marín

IP Virtual Machine objetivo

IP Local: 152.231.218.174

IP pública: 20.9.140.242

Puertos permitidos (NSG)

Puerto 22 (SSH): Permitido para permitir acceso remoto seguro a la VM a través de SSH.

Puerto 80 (HTTP): Permitido para permitir tráfico web a través del protocolo HTTP.

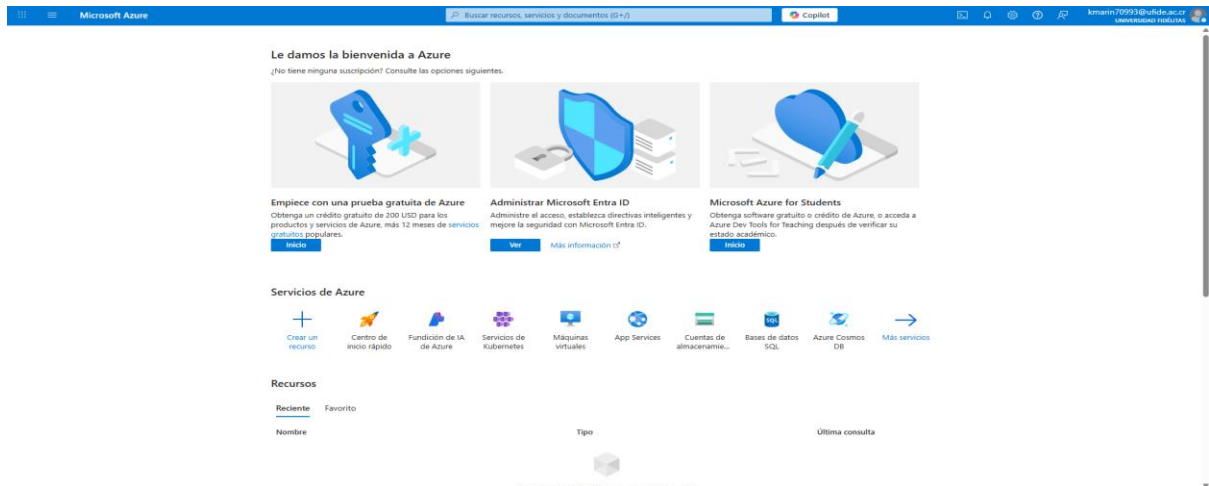
Puerto 443 (HTTPS): Permitido para permitir tráfico web seguro a través del protocolo HTTPS.

Filtrar por nombre						
Puerto == todo Protocolo == todo Origen == todo Destino == todo Acción == todo						
Prioridad ↑↓	Nombre ↑↓	Puerto ↑↓	Protocolo ↑↓	Origen ↑↓	Destino ↑↓	Acción ↑↓
<input type="checkbox"/> 300	SSH	22	TCP	Cualquiera	Cualquiera	Allow
<input type="checkbox"/> 310	HTTP	80	TCP	Cualquiera	Cualquiera	Allow
<input type="checkbox"/> 311	HTTPS	443	TCP	Cualquiera	Cualquiera	Allow

Pasos rápidos para la creación de la VM

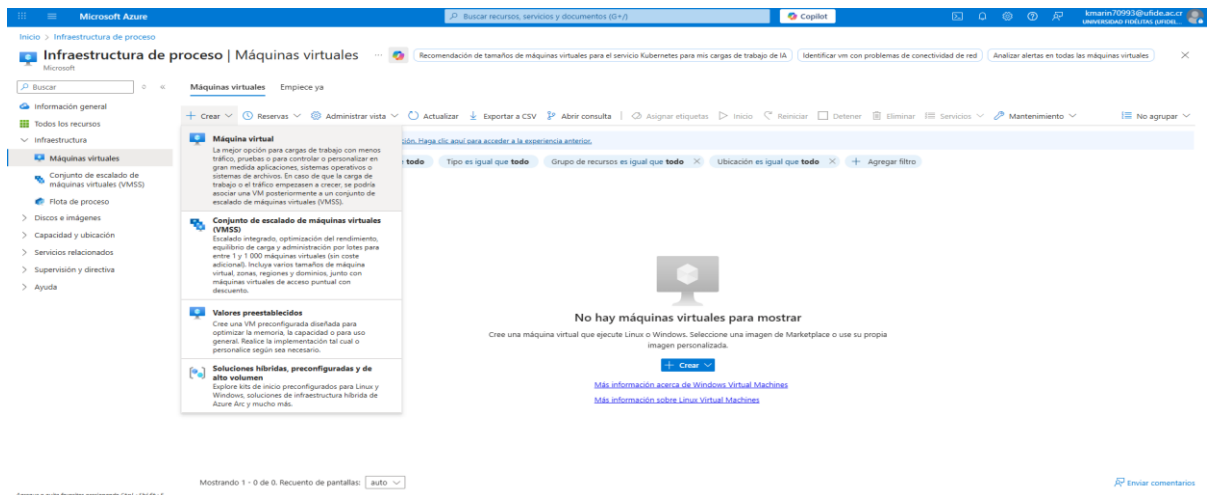
Acceso al portal de Azure

Se ingresa al portal web <https://portal.azure.com> utilizando la cuenta institucional del proyecto.



Servicio de máquinas virtuales

En la parte superior izquierda, se hace clic en el menú de navegación y luego se selecciona “Máquinas virtuales”. Después se hace clic en “Crear” y se elige la opción “Máquina virtual de Azure”.



Configuración básica

En la pestaña “Detalles del proyecto”, se completan los campos iniciales:

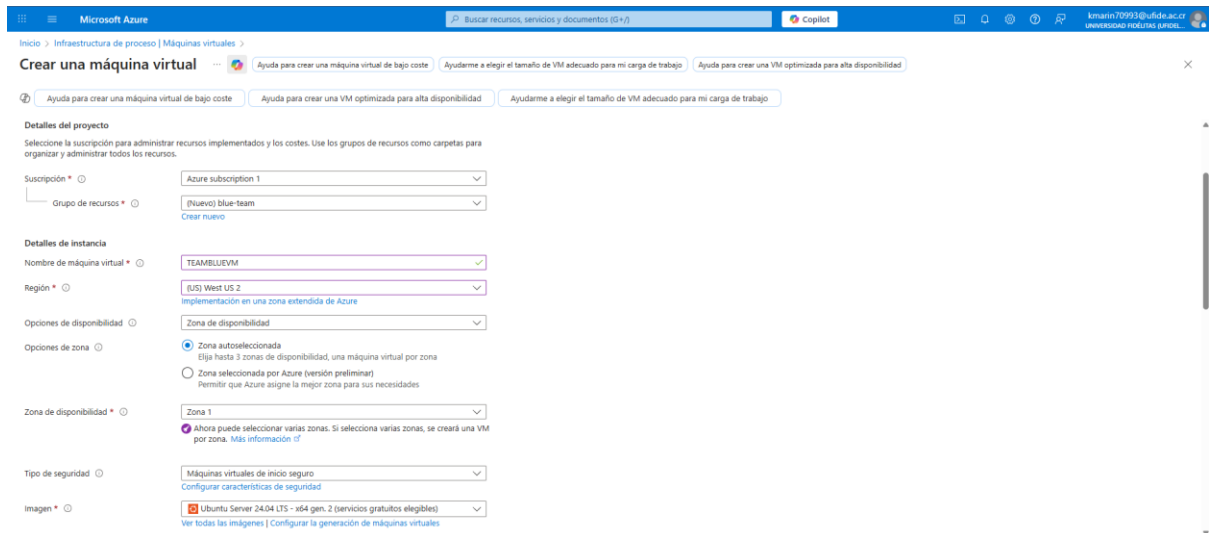
Suscripción: se selecciona la suscripción activa disponible

Grupo de recursos: se crea uno nuevo, blue-team.

Nombre de la máquina virtual: se asigna un nombre, TEAMBLUEVM.

Región: se elige el centro de datos más conveniente, West US 2.

Imagen del sistema operativo: se abre la lista desplegable y se selecciona una imagen de Linux, en nuestro caso Ubuntu Server 22.04 LTS.



Microsoft Azure

Inicio > Infraestructura de proceso > Máquinas virtuales >

Crear una máquina virtual

Ayuda para crear una máquina virtual de bajo coste | Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo | Ayuda para crear una VM optimizada para alta disponibilidad

Ayuda para crear una máquina virtual de bajo coste | Ayuda para crear una VM optimizada para alta disponibilidad | Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

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 * Azure subscription 1

Grupo de recursos * (Nuevo) blue-team
[Crear nuevo](#)

Detalles de instancia

Nombre de máquina virtual * TEAMBLUEVM

Región * (US) West US 2
[Implementación en una zona extendida de Azure](#)

Opciones de disponibilidad Zona 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 * Zona 1
[Ahora puede seleccionar varias zonas. Si selecciona varias zonas, se creará una VM por zona. Más información](#)

Tipo de seguridad Máquinas virtuales de inicio seguro
[Configurar características de seguridad](#)

Imagen * Ubuntu Server 24.04 LTS - x64 gen. 2 (servicios gratuitos elegibles)
[Ver todas las imágenes](#) | [Configurar la generación de máquinas virtuales](#)

Selección del tamaño (recursos de hardware)

En el apartado “Tamaño”, se puede ver una lista de configuraciones recomendadas.

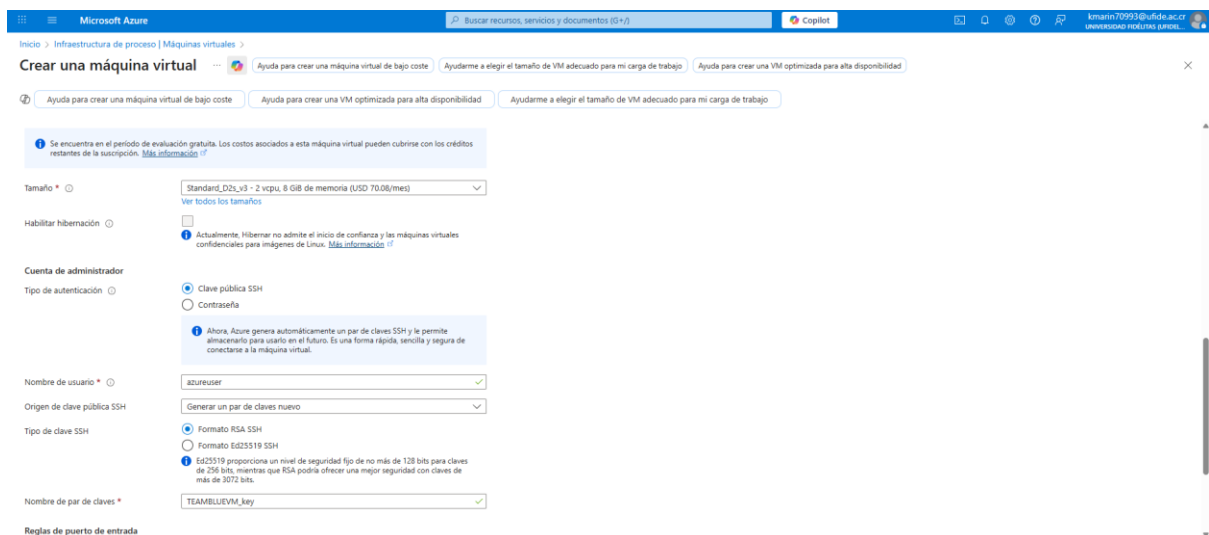
Se elige una opción equilibrada entre rendimiento y costo, por ejemplo:

Tamaño: Standard D2s v3 (2 vCPU, 8 GB de RAM).

Luego se hace clic en “Seleccionar”.

Configuración de credenciales de acceso

Para autenticarse en la máquina virtual utilizamos la opción “Generar un par de claves nuevo” que genera dos Claves RSA SSH (recomendada para Linux).



Credenciales: Usuario: blue-team, y una contraseña segura

Configuración de red

En la pestaña “Red”, Azure crea automáticamente una red virtual (VNet) y una subred.

Se asigna una dirección IP pública para poder acceder de forma remota mediante SSH (puerto 22).

Se debe asegurar que en la sección “Puertos de entrada públicos” esté habilitado el SSH (22).

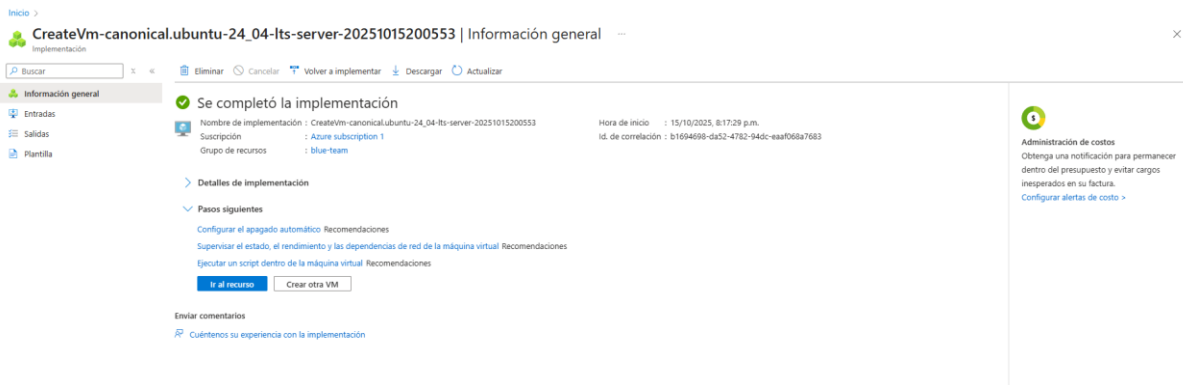
Revisión y creación de la máquina

Se hace clic en “Revisar y crear”. El sistema valida los datos y muestra el costo estimado por hora de uso.

Luego se presiona “Crear” para iniciar el despliegue de la máquina virtual.

Conexión a la máquina virtual

Una vez completada la implementación, se selecciona “Ir al recurso”. Y verificamos que se haya creado correctamente.



Buenas prácticas para usar la VM

Apagarla correctamente

- No apagarla abruptamente desde el software o sea no forzar apagado porque esto podría dañar archivos del sistema y hacer que se pierdan configuraciones, si se va a usar nuevamente pronto usar la opción de “Suspende”
- En Linux desde terminal se puede usar “sudo poweroff” o “sudo shutdown now”
- Siempre esperar a que el sistema se apague por completo antes de cerrar la ventana de la VM

Uso de contraseñas fuertes:

- Se debe asegurar que las contraseñas utilizadas para el acceso a las máquinas virtuales sean complejas y únicas. Además, es importante que se cambien periódicamente para fortalecer la seguridad.

Uso de claves SSH en lugar de contraseñas para el acceso remoto:

- En lugar de utilizar contraseñas, se recomienda el uso de claves SSH para acceder a las máquinas virtuales. Esta medida añade una capa adicional de seguridad al proceso de autenticación.

Configurar el firewall adecuadamente:

- El acceso a las máquinas virtuales debe ser restringido solo a los puertos necesarios. Se debe permitir únicamente el acceso a los puertos 22 para SSH, 80 para HTTP y 443 para HTTPS, bloqueando cualquier otro tráfico no esencial.

Realizar copias de seguridad periódicas:

- Se debe garantizar que se realicen copias de seguridad regulares de la VM y de los datos críticos. Esto permite restaurar rápidamente el sistema en caso de fallos o pérdidas de datos.

Mantener las actualizaciones al día:

- Es fundamental mantener tanto el sistema operativo como las aplicaciones actualizadas con los últimos parches de seguridad. De ser posible, se deben configurar actualizaciones automáticas para garantizar que el sistema esté siempre protegido.