



Instituto Politécnico Nacional
Escuela Superior de Computo



Sistemas Distribuidos

Tarea 3

Implementación de una VPN VNet-to-VNet

Nombre del alumno:

García Quiroz Gustavo Ivan

Grupo: 7CV4

Nombre del profesor: Guerrero Carlos Pineda

Fecha de entrega: 11/10/2025

ÍNDICE

1	INTRODUCCIÓN	1
2	Objetivos	3
2.1	Objetivo General	3
2.2	Objetivos Particulares	3
3	FUNDAMENTACIÓN TEÓRICA.....	4
3.1	Virtual Network (VNet)	4
3.2	Gateway de Red Virtual	4
3.3	VPN VNet-to-VNet (Route-Based).....	4
3.4	Subred GatewaySubnet.....	5
4	DISEÑO DE LA SOLUCIÓN	6
4.1	Nomenclatura Oficial Usada	6
4.2	Regiones Seleccionadas	6
4.3	Plan de Direccionamiento	7
4.4	Diagrama Lógico	8
5	Procedimiento Detallado en el Portal de Azure	10
5.1	Creación de Resource Groups.....	10
5.2	Creación de la Primera Red Virtual (T3-2022630278-vnet-1).....	15
5.3	Creación de la Segunda Red Virtual (T3-2022630278-vnet-2)	23
5.4	Creación de las subredes GatewaySubnet.....	33
5.4.1	Crear GatewaySubnet en la primera VNet (T3-2022630278-vnet-1).....	33
5.4.2	Crear GatewaySubnet en la segunda VNet (T3-2022630278-vnet-2)	36
5.4.3	Verificación consolidada (OPCIONAL).....	40
5.5	Creación de IPs públicas para los Gateways.....	41
5.5.1	Crear la primera IP pública (T3-2022630278-ip-1).....	41

5.5.2	Crear la segunda IP pública (T3-2022630278-ip-2).....	45
5.6	Creación de los Virtual Network Gateways	49
5.6.1	Crear el primer Virtual Network Gateway (T3-2022630278-gateway-1) ..	49
5.6.2	Crear el segundo Virtual Network Gateway (T3-2022630278-gateway-2)	54
5.6.3	Verificación consolidada de ambos gateways.....	57
5.7	Creación de las Conexiones VNet-to-VNet.....	58
5.7.1	Conexión 1: Desde Gateway 1 hacia Gateway 2.....	58
5.7.2	Conexión 2: Desde Gateway 2 hacia Gateway 1	62
5.8	Creación de las Máquinas Virtuales Ubuntu	65
5.8.1	Máquina Virtual 1 (VM1)	65
5.8.2	Máquina Virtual 2 (VM2)	72
5.9	Configuración de reglas ICMP (NSG)	75
5.10	Verificación de conectividad (ping).....	79
5.11	Visualización de topología de red	86
6	Eliminación (limpieza) de recursos.....	91
6.1	Procedimiento de eliminación	91
7	Enlace al chat de la IA GitHub Copilot	93
8	REFERENCIAS.....	94

1 INTRODUCCIÓN

La computación en la nube ha revolucionado la manera en que las organizaciones diseñan, implementan y gestionan su infraestructura tecnológica. Microsoft Azure, como una de las plataformas de nube más robustas del mercado, ofrece servicios avanzados de redes virtuales que permiten crear arquitecturas distribuidas y seguras a escala global. En el contexto de los sistemas distribuidos, la capacidad de interconectar recursos de cómputo ubicados en diferentes regiones geográficas de manera privada y segura representa un pilar fundamental para garantizar la disponibilidad, el rendimiento y la protección de datos en aplicaciones empresariales modernas.

La presente práctica se centra en la implementación de una red privada virtual (VPN) tipo VNet-to-VNet en Azure, configurando un túnel seguro IPsec/IKE entre dos redes virtuales (VNets) desplegadas en regiones geográficas distintas. Esta arquitectura permite establecer comunicación privada entre recursos distribuidos sin exponerlos a la Internet pública, manteniendo el tráfico dentro de la infraestructura backbone de Microsoft Azure. A diferencia del peering de VNets, que opera a nivel de red mediante conexión directa, la VPN VNet-to-VNet utiliza gateways de red virtual que cifran el tráfico, proporcionando una capa adicional de seguridad mediante protocolos criptográficos estándar de la industria.

El laboratorio contempla la creación de dos entornos virtuales completamente funcionales, cada uno con su propia red virtual, gateway VPN y máquina virtual con sistema operativo Ubuntu 24.04 LTS. La interconexión se realizará mediante conexiones VPN bidireccionales que establecerán túneles cifrados entre los gateways, permitiendo que las máquinas virtuales se comuniquen utilizando únicamente sus direcciones IP privadas. Este escenario simula arquitecturas empresariales reales donde aplicaciones distribuidas requieren comunicación segura entre centros de datos virtuales en diferentes ubicaciones geográficas, ya sea para balanceo de carga, replicación de datos, recuperación ante desastres o distribución de servicios.

Para el desarrollo de esta práctica se utilizó Azure for Students, la suscripción académica proporcionada por Microsoft que ofrece créditos y servicios gratuitos para fines

educativos. Además, se empleó asistencia de inteligencia artificial mediante GitHub Copilot para la resolución de problemas técnicos y mejores prácticas en la implementación de servicios de red en Azure. La práctica sigue estrictamente la nomenclatura especificada basada en el número de boleta 2022630278, garantizando la trazabilidad y organización de todos los recursos desplegados en la plataforma Azure. Al finalizar, se validará la conectividad mediante pruebas ICMP bidireccionales y se procederá a la eliminación completa de recursos para optimizar el uso de créditos disponibles.

2 Objetivos

2.1 Objetivo General

Implementar y validar una conexión VPN VNet-to-VNet entre dos redes virtuales de Microsoft Azure ubicadas en diferentes regiones geográficas

2.2 Objetivos Particulares

- Diseñar e implementar dos redes virtuales (VNets) en regiones distintas de Azure con esquemas de direccionamiento IP no solapados que permitan el enrutamiento correcto del tráfico entre ambos entornos.
- Configurar y desplegar Virtual Network Gateways tipo VPN con arquitectura route-based en cada red virtual, incluyendo la creación de subredes GatewaySubnet y asignación de direcciones IP públicas estáticas.
- Establecer conexiones VPN VNet-to-VNet bidireccionales entre los gateways utilizando claves precompartidas (PSK) para autenticación, verificando el estado "Connected" de ambos túneles.
- Aprovisionar máquinas virtuales con Ubuntu 24.04 LTS (1 vCPU, 1GB RAM, 30GB disco) en la subred default de cada red virtual, configurando grupos de seguridad de red (NSG) para permitir tráfico ICMP.
- Validar la conectividad end-to-end mediante pruebas de ping bidireccionales entre las máquinas virtuales utilizando exclusivamente sus direcciones IP privadas, documentando latencia y rutas de red.
- Analizar y documentar la topología de red generada por Azure mediante las herramientas de visualización integradas, identificando todos los componentes y sus interconexiones.
- Aplicar las mejores prácticas de gestión de recursos cloud mediante la eliminación completa y ordenada de todos los componentes creados, optimizando el consumo de créditos de la suscripción Azure for Students.

3 FUNDAMENTACIÓN TEÓRICA

3.1 Virtual Network (VNet)

Una Virtual Network (VNet) es el componente fundamental de red en Microsoft Azure que proporciona aislamiento lógico y segmentación de recursos en la nube. Funciona de manera similar a una red tradicional local, pero con las ventajas de escalabilidad, disponibilidad y seguridad de la infraestructura de Azure. Las VNets permiten definir espacios de direcciones IP privadas utilizando rangos CIDR (Classless Inter-Domain Routing) según el estándar RFC 1918, subdividiéndose en subredes para organizar recursos según requisitos de seguridad y funcionalidad. Cada VNet está confinada a una región específica de Azure y a una suscripción, garantizando el aislamiento de tráfico entre diferentes entornos virtuales.

3.2 Gateway de Red Virtual

El Virtual Network Gateway es un recurso administrado por Azure que actúa como punto de terminación para conexiones cifradas entre redes virtuales o entre redes virtuales y ubicaciones on-premises. Funciona como un conjunto de máquinas virtuales especializadas desplegadas automáticamente en la subred GatewaySubnet, ejecutando servicios de enruteamiento y túneles VPN. Soporta dos tipos principales: VPN Gateway (para conexiones cifradas sobre Internet) y ExpressRoute Gateway (para conexiones privadas dedicadas). Los VPN Gateways ofrecen dos modos de operación: policy-based (basado en políticas con túneles estáticos) y route-based (basado en rutas con enruteamiento dinámico), siendo este último el requerido para escenarios VNet-to-VNet, conexiones punto-a-sitio y configuraciones de alta disponibilidad.

3.3 VPN VNet-to-VNet (Route-Based)

La arquitectura VPN VNet-to-VNet establece túneles IPsec/IKE (Internet Protocol Security/Internet Key Exchange) entre dos Virtual Network Gateways ubicados en diferentes redes virtuales, permitiendo comunicación privada y cifrada entre recursos distribuidos geográficamente. A diferencia del VNet Peering que opera a nivel de red mediante conexión directa del backbone de Microsoft, la VPN VNet-to-VNet utiliza protocolos de seguridad estándar de la industria para encriptar todo el tráfico que

atraviesa los túneles. El modo route-based utiliza interfaces de túnel virtual y tablas de enrutamiento para determinar qué tráfico se envía a través del túnel, proporcionando flexibilidad para soportar múltiples túneles simultáneos, enrutamiento dinámico y topologías complejas. La autenticación se realiza mediante claves precompartidas (PSK - Pre-Shared Key) que ambos gateways deben conocer para establecer la asociación de seguridad.

3.4 Subred GatewaySubnet

La subred GatewaySubnet es una subred especial y obligatoria dentro de cada VNet que alojará el Virtual Network Gateway. Azure requiere que esta subred se nombre exactamente "GatewaySubnet" (sin espacios ni variaciones) para identificarla automáticamente durante el despliegue del gateway. Microsoft recomienda un tamaño mínimo de /27 (32 direcciones IP) aunque acepta hasta /29 (8 direcciones IP), considerando que el gateway puede requerir múltiples direcciones IP para operaciones de alta disponibilidad, actualizaciones sin tiempo de inactividad y escalado futuro. Esta subred no debe contener otros recursos como máquinas virtuales, servicios o grupos de seguridad de red, ya que está reservada exclusivamente para la infraestructura del gateway administrada por Azure.

4 DISEÑO DE LA SOLUCIÓN

4.1 Nomenclatura Oficial Usada

Conforme a las especificaciones del ejercicio y utilizando el número de boleta 2022630278, se emplea la siguiente nomenclatura estandarizada para todos los recursos:

Red Virtual 1:

- VNet: T3-2022630278-vnet-1
- Gateway: T3-2022630278-gateway-1
- IP Pública: T3-2022630278-ip-1
- Conexión: T3-2022630278-conexion-1
- Máquina Virtual: T3-2022630278-1

Red Virtual 2:

- VNet: T3-2022630278-vnet-2
- Gateway: T3-2022630278-gateway-2
- IP Pública: T3-2022630278-ip-2
- Conexión: T3-2022630278-conexion-2
- Máquina Virtual: T3-2022630278-2

Recursos opcionales:

- Resource Group 1: T3-2022630278-rg-1
- Resource Group 2: T3-2022630278-rg-2

4.2 Regiones Seleccionadas

Para esta implementación se seleccionaron dos regiones geográficamente separadas de Microsoft Azure:

- **Región 1:** Canadá Central
- **Región 2:** West US

Justificación: La selección de regiones en la costa oeste de Estados Unidos y el centro de Canadá proporciona separación geográfica suficiente para simular un escenario de arquitectura distribuida real que permiten pruebas prácticas de conectividad. Ambas regiones ofrecen disponibilidad completa de servicios VPN Gateway en la suscripción Azure for Students y representan ubicaciones comúnmente utilizadas en arquitecturas empresariales norteamericanas para redundancia geográfica y recuperación ante desastres.

4.3 Plan de Direccionamiento

El esquema de direccionamiento IP se diseñó garantizando ausencia total de traslape entre redes virtuales:

Componente	Red Virtual 1	Red Virtual 2
VNet Address Space	10.30.0.0/16	10.40.0.0/16
Subred default	10.30.1.0/24 (254 hosts)	10.40.1.0/24 (254 hosts)
Subred GatewaySubnet	10.30.254.0/27 (30 hosts)	10.40.254.0/27 (30 hosts)
IP VM (privada)	10.30.1.4 (dinámica)	10.40.1.4 (dinámica)

Tabla 1 Esquema de direccionamiento IP

Características del diseño:

- Espacios /16 proporcionan 65,536 direcciones por VNet, permitiendo crecimiento futuro
- Subredes default /24 ofrecen 254 hosts disponibles para máquinas virtuales y servicios
- GatewaySubnet /27 cumple con recomendación de Microsoft (30 IPs disponibles)
- Rangos 10.30.x.x y 10.40.x.x son completamente disjuntos, evitando conflictos de enrutamiento

- Subred GatewaySubnet ubicada en rango alto (.254.0) para organización lógica

4.4 Diagrama Lógico

El siguiente diagrama ilustra la arquitectura completa de la solución VPN VNet-to-VNet implementada:



IMAGEN 1: Diagrama de arquitectura completa

Descripción del flujo de comunicación:

1. La VM T3-2022630278-1 (10.30.1.4) en East US genera tráfico destinado a 10.40.1.4
2. El tráfico se enruta hacia T3-2022630278-gateway-1 según tabla de enrutamiento de la VNet
3. El gateway cifra el tráfico mediante IPsec/IKE y lo envía a través del túnel VPN establecido por T3-2022630278-conexion-1

4. El tráfico cifrado atraviesa Internet entre las IPs públicas de ambos gateways
5. T3-2022630278-gateway-2 recibe, autentica y descifra el tráfico
6. El gateway enruta el tráfico descifrado hacia la subred default 10.40.1.0/24
7. La VM T3-2022630278-2 recibe el tráfico en su interfaz privada
8. El flujo inverso sigue el mismo proceso utilizando T3-2022630278-conexion-2



IMAGEN 2: Diagrama simplificado de flujo de datos

- Diagrama de secuencia mostrando el flujo paso a paso de un ping
- Incluir proceso de cifrado/descifrado en gateways
- Mostrar headers IPsec en tráfico sobre Internet
- Indicar tiempos aproximados de latencia en cada salto

5 Procedimiento Detallado en el Portal de Azure

5.1 Creación de Resource Groups

Los Resource Groups en Azure son contenedores lógicos que agrupan recursos relacionados para facilitar su administración, control de acceso y facturación. Para esta práctica, crearemos dos Resource Groups independientes, uno para cada red virtual y sus recursos asociados.

Paso 1: Acceso al portal de Azure

1. Ingresar a <https://portal.azure.com>
2. Iniciar sesión con las credenciales de Azure for Students
3. Verificar que la suscripción activa sea "Azure for Students"

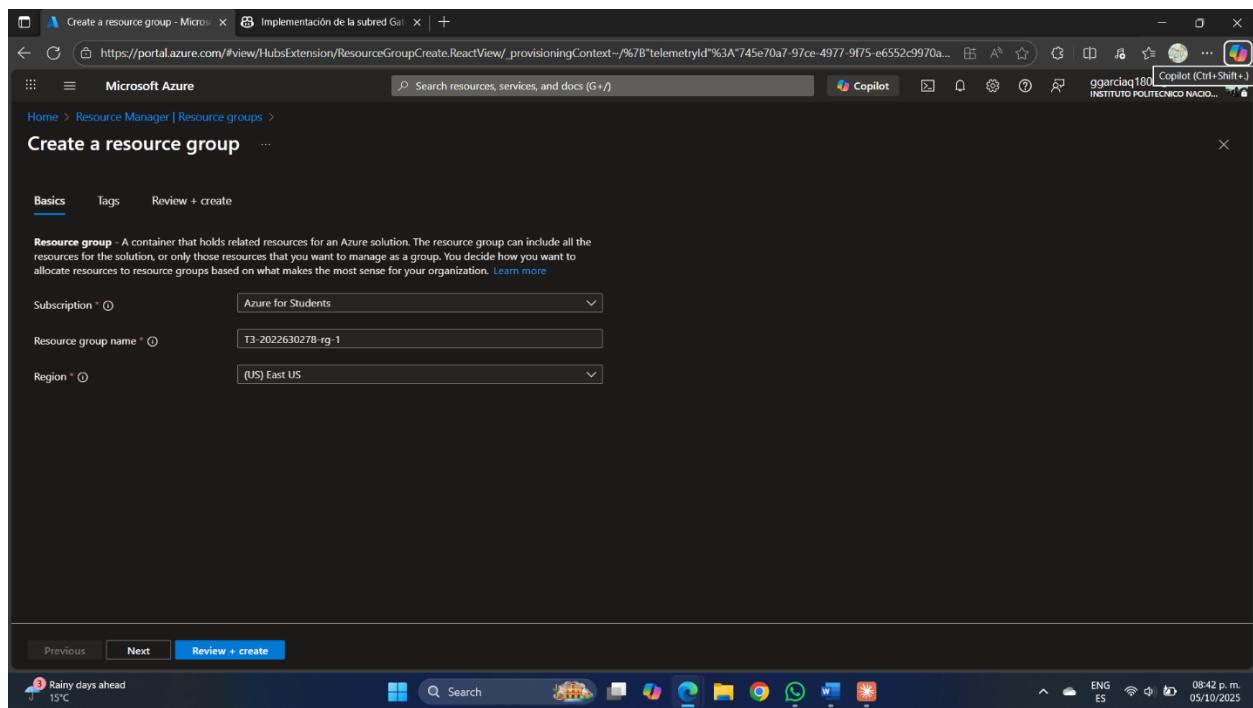
The screenshot shows the Microsoft Azure Subscriptions blade. At the top, there's a search bar and a Copilot button. Below the search bar, it says "All services > Subscriptions > Subscriptions". There are buttons for "+ Add", "Manage Policies", "View Requests", "View eligible subscriptions", and "Export to CSV". A note says "View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here". It also says "Showing subscriptions in Instituto Politecnico Nacional directory. Don't see a subscription? Switch directories". There's a filter section with "Subscriptions : Filtered (1 of 1)", "My role = all", "Status = all", and an "Add filter" button. The main table has columns: Subscription name, Subscription ID, My role, Current cost, Secure Score, Parent management group, and Status. One row is shown: "Azure for Students" with Subscription ID "fd58a3da-fcef-47d1-ac0e-5b891faa4251", My role "Owner", Current cost "\$0.48", Secure Score "100%", Parent management group "Tenant Root Group", and Status "Active". The bottom of the screen shows a taskbar with various icons and the date/time "04/10/2025 04:18 p.m."

Paso 2: Creación del primer Resource Group (RG-1)

1. En el portal de Azure, hacer clic en el menú hamburguesa (\equiv) en la esquina superior izquierda

Name	Subscription	Location
NetworkWatcherRG	Azure for Students	Mexico Central
T2-2022630278_group	Azure for Students	East US 2
T2-2022630278_group_09271755	Azure for Students	Mexico Central

2. Seleccionar "**Resource groups**" del menú lateral
3. Hacer clic en el botón "**+ Create**" ubicado en la parte superior
4. En la pestaña "**Basics**", completar los siguientes campos:
 - o **Subscription:** Azure for Students
 - o **Resource group:** T3-2022630278-rg-1
 - o **Region:** México Central (o la región seleccionada para la primera VNet)



5. Hacer clic en "Review + create"
6. Verificar que la validación sea exitosa (marca verde con "Validation passed")
7. Hacer clic en "**Create**"
8. Esperar el mensaje de confirmación "Your deployment is complete"

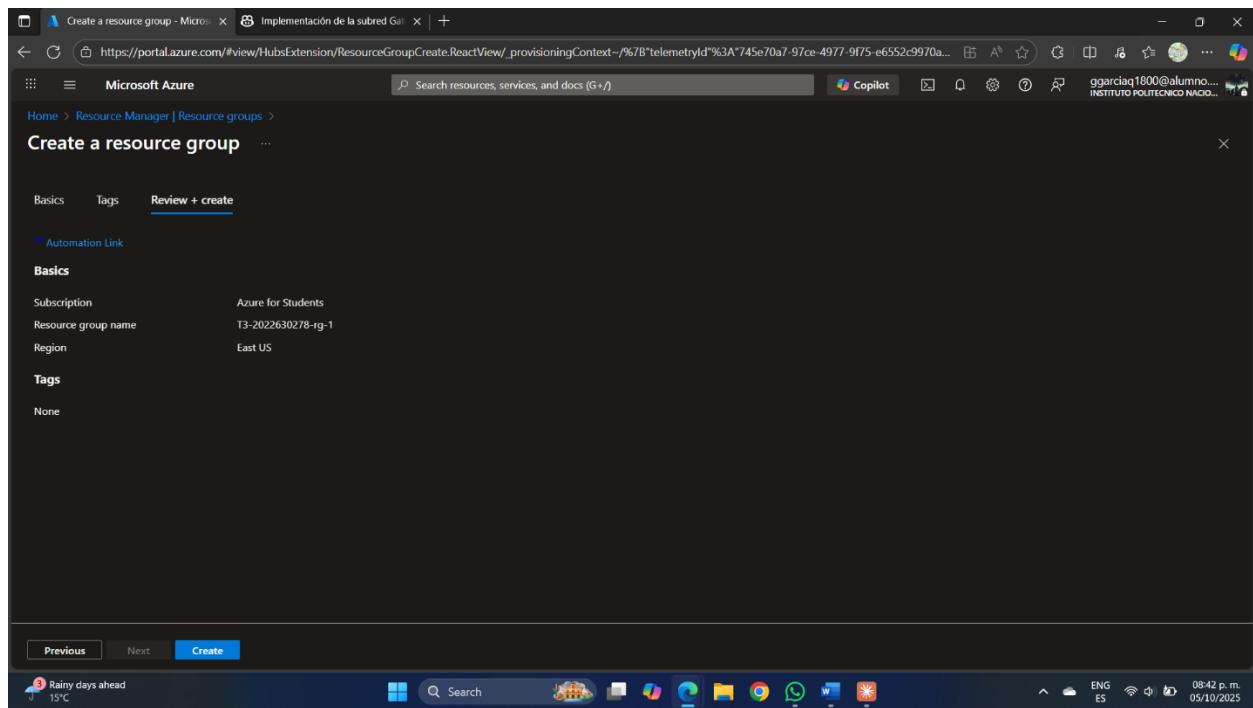
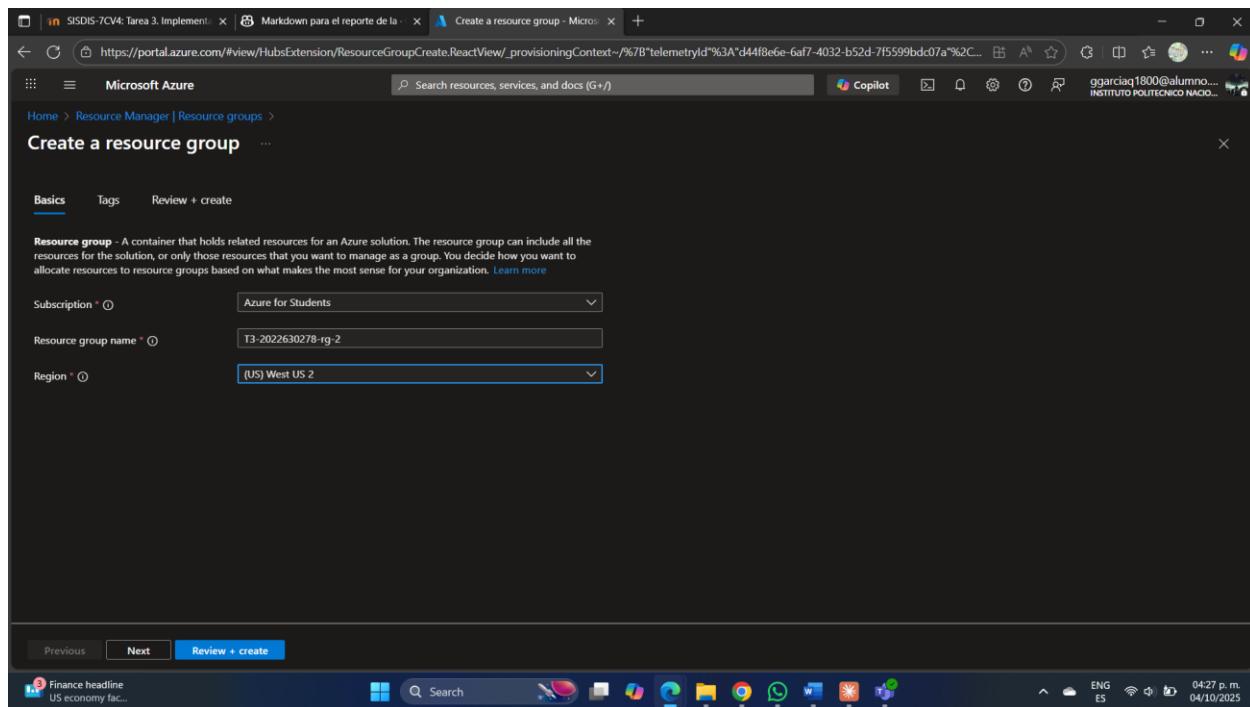


IMAGEN 2: Captura de la pantalla "Create a resource group"

Esta captura muestra la pantalla de creación del Resource Group con los campos completados correctamente. Se debe visualizar claramente el nombre T3-2022630278-rg-1 en el campo "Resource group", la suscripción "Azure for Students" seleccionada, y la región "Méjico Central". La interfaz debe mostrar la pestaña "Basics" activa antes de hacer clic en "Review + create".

Paso 3: Creación del segundo Resource Group (RG-2)

1. Regresar a la vista de "**Resource groups**"
2. Hacer clic nuevamente en "**+ Create**"
3. En la pestaña "**Basics**", completar los siguientes campos:
 - o **Subscription:** Azure for Students
 - o **Resource group:** T3-2022630278-rg-2
 - o **Region:** West US 2 (o una región diferente a la primera)



4. Hacer clic en "Review + create"
5. Verificar la validación exitosa
6. Hacer clic en "**Create**"

7. Esperar la confirmación de creación

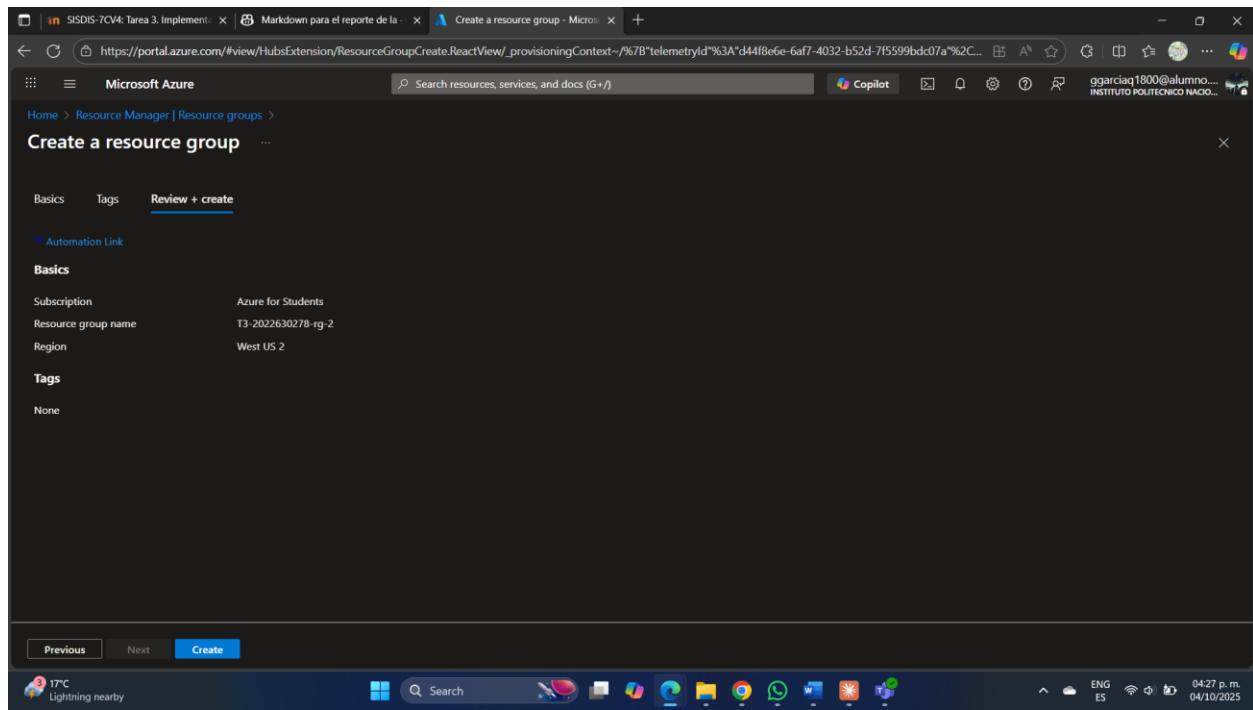


IMAGEN 3: Captura de la pantalla "Create a resource group" para RG-2

Similar a la imagen anterior, esta captura debe mostrar el formulario de creación del segundo Resource Group con el nombre T3-2022630278-rg-2 y la región "West US 2" seleccionada. Se debe apreciar que la suscripción sigue siendo "Azure for Students" y que todos los campos están correctamente llenados antes de la creación.

Paso 4: Verificación de Resource Groups creados

1. En la vista de "**Resource groups**", actualizar la lista
2. Confirmar que ambos Resource Groups aparecen:
 - T3-2022630278-rg-1
 - T3-2022630278-rg-2

Name	Subscription	Location
NetworkWatcherRG	Azure for Students	Mexico Central
T2-2022630278_group_09271755	Azure for Students	Mexico Central
T3-2022630278-rg-1	Azure for Students	East US
T3-2022630278-rg-2	Azure for Students	West US 2

IMAGEN 3-A: Lista de Resource Groups creados

Esta captura muestra la lista completa de Resource Groups en la suscripción. Deben ser visibles al menos los dos Resource Groups recién creados: T3-2022630278-rg-1 y T3-2022630278-rg-2, con sus respectivas regiones (East US y West US). La columna "Type" debe mostrar "Resource group" y el estado debe indicar que están activos.

5.2 Creación de la Primera Red Virtual (T3-2022630278-vnet-1)

Una Virtual Network (VNet) es el componente fundamental de red privada en Azure. Permite que los recursos de Azure se comuniquen entre sí de forma segura. En este paso crearemos la primera VNet con su espacio de direcciones y subred predeterminada.

Paso 1: Iniciar creación de Virtual Network

1. En el portal de Azure, hacer clic en "**+ Create a resource**" (esquina superior izquierda)
2. En la barra de búsqueda, escribir "**Virtual Network**"
3. Seleccionar "**Virtual Network**" de los resultados (Publisher: Microsoft)
4. Hacer clic en "**Create**"

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation under 'Virtual network' is expanded, showing options like Overview, Virtual networks, NAT gateways, Public IP addresses, Network interfaces, Network security groups, Application security groups, Bastions, Route tables, Route servers, and Private Link. The 'Virtual networks' option is selected. The main content area displays a table titled 'Network foundation | Virtual networks'. The table has columns for Name, Resource group, Location, and Subscription. One record is listed: 'T2-2022630278-vnet' under 'Resource group T2-2022630278_group_09271755', located in 'Mexico Central' and belongs to 'Azure for Students'. The table includes filters for 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. The bottom of the screen shows the Windows taskbar with various pinned icons.

Paso 2: Configuración básica de la VNet-1

1. En la pestaña "**Basics**", completar:
 - **Subscription:** Azure for Students
 - **Resource group:** Seleccionar T3-2022630278-rg-1 del dropdown
 - **Name:** T3-2022630278-vnet-1
 - **Region:** México Central (debe coincidir con la región del RG-1)
2. Hacer clic en "Next: IP Addresses"

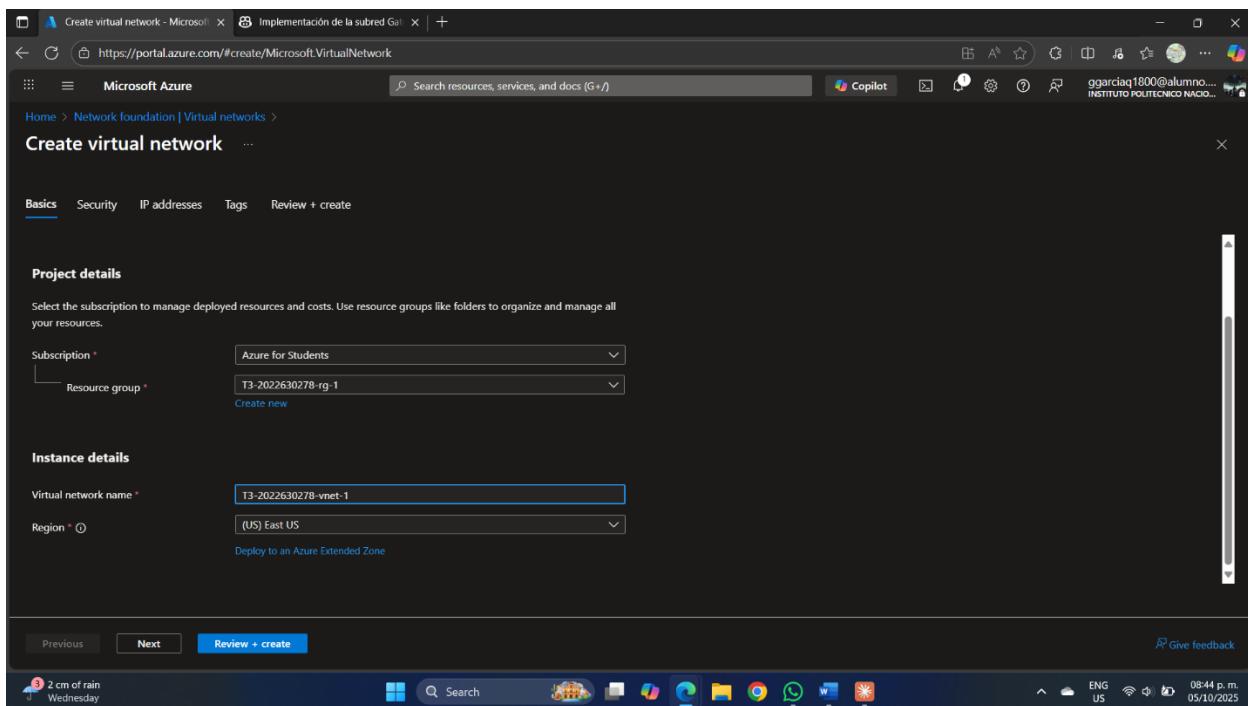
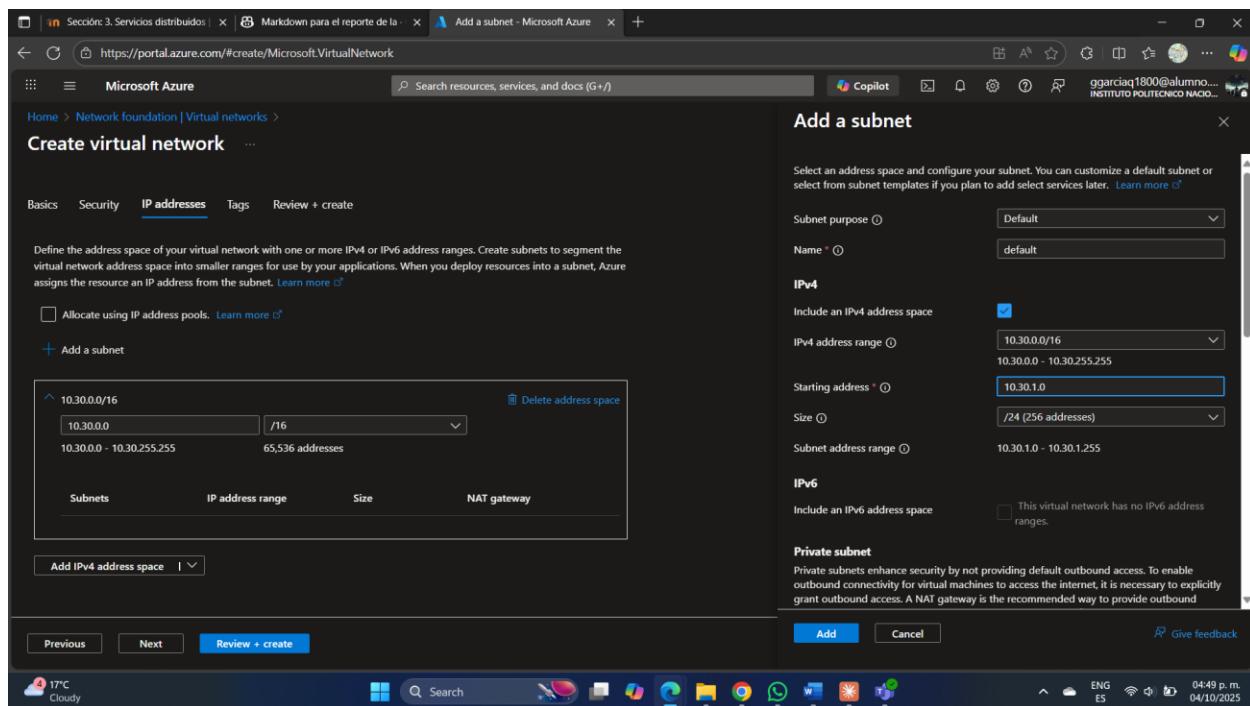


IMAGEN 4: Pestaña "Basics" de creación de Virtual Network

Esta captura debe mostrar la pestaña "Basics" del formulario de creación de Virtual Network. Se debe visualizar claramente el nombre T3-2022630278-vnet-1 en el campo "Name", el Resource Group T3-2022630278-rg-1 seleccionado, y la región.

Paso 3: Configuración del espacio de direcciones IP

1. En la pestaña "**IP Addresses**", configurar:
 - **IPv4 address space:** Eliminar cualquier espacio predeterminado y agregar 10.30.0.0/16
2. Configurar la subred predeterminada:
 - Si existe una subred "default" predeterminada, hacer clic en el ícono de lápiz (editar) o en el nombre de la subred
 - Si no existe, hacer clic en "**+ Add subnet**"
 - Subnet name: default
 - Subnet address range: 10.30.1.0/24
 - Dejar las demás opciones por defecto
 - Hacer clic en "**Add**" o "**Save**"



3. Verificar que el espacio de direcciones y la subred estén correctos

4. Hacer clic en "Next: Security"

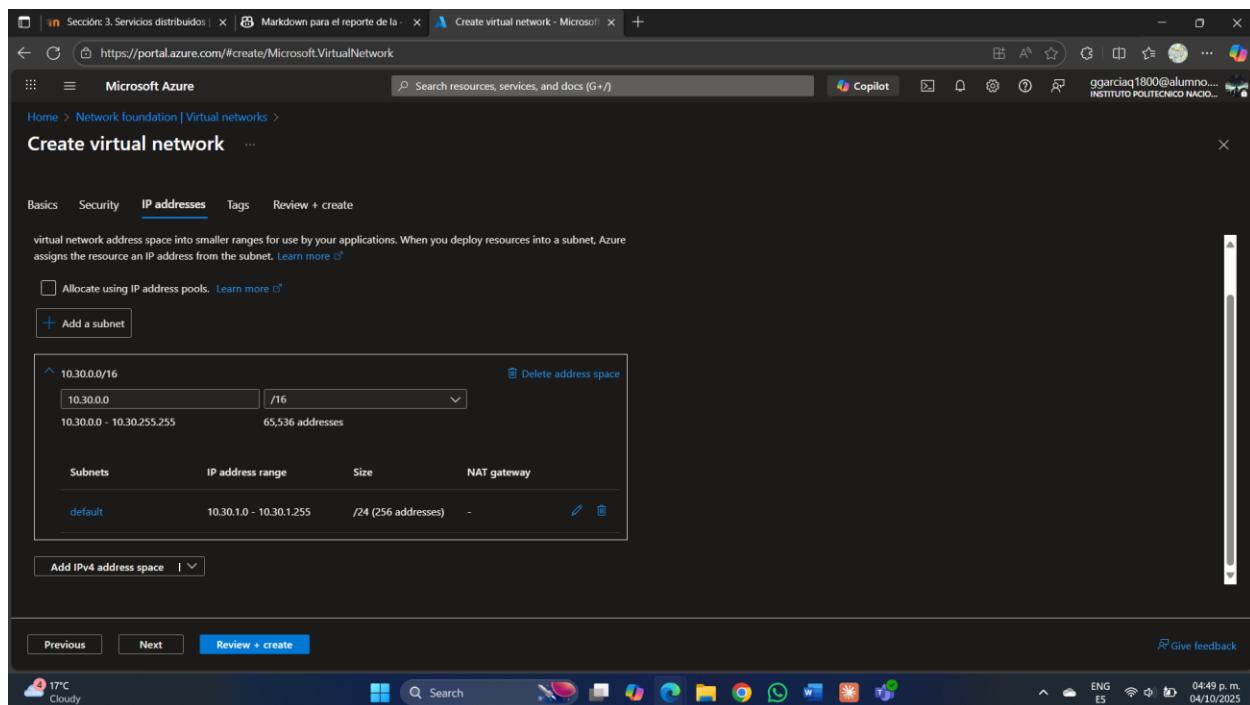


IMAGEN 5: Pestaña "IP Addresses" con address space y subnet configurados

Esta captura debe mostrar la pestaña "IP Addresses" con el espacio de direcciones IPv4 configurado como 10.30.0.0/16. Además, debe visualizarse la subred "default" con el rango 10.30.1.0/24 ya agregada. La imagen debe mostrar claramente la estructura jerárquica del address space y cómo la subred default está contenida dentro del espacio 10.30.0.0/16.

Paso 4: Configuración de seguridad (opcional)

1. En la pestaña "**Security**", dejar las opciones predeterminadas:
 - **BastionHost:** Disabled (no necesario para esta práctica)
 - **DDoS Protection Standard:** Disabled (no necesario, ahorra costos)
 - **Firewall:** Disabled (no necesario para esta práctica)
2. Hacer clic en "**Next: Tags**"

Enhance the security of your virtual network with these additional paid security services. [Learn more](#)

Virtual network encryption

Enable Virtual network encryption to encrypt traffic traveling within the virtual network. Virtual machines must have accelerated networking enabled. Traffic to public IP addresses is not encrypted. [Learn more](#)

Virtual network encryption

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. [Learn more](#)

Enable Azure Bastion

Azure Firewall

Previous Next Review + create Give feedback

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. [Learn more](#)

Enable Azure Firewall

Azure DDoS Network Protection

Azure DDoS Network Protection is a paid service that offers enhanced DDoS mitigation capabilities via adaptive tuning, attack notification, and telemetry to protect against the impacts of a DDoS attack for all protected resources within this virtual network. [Learn more](#)

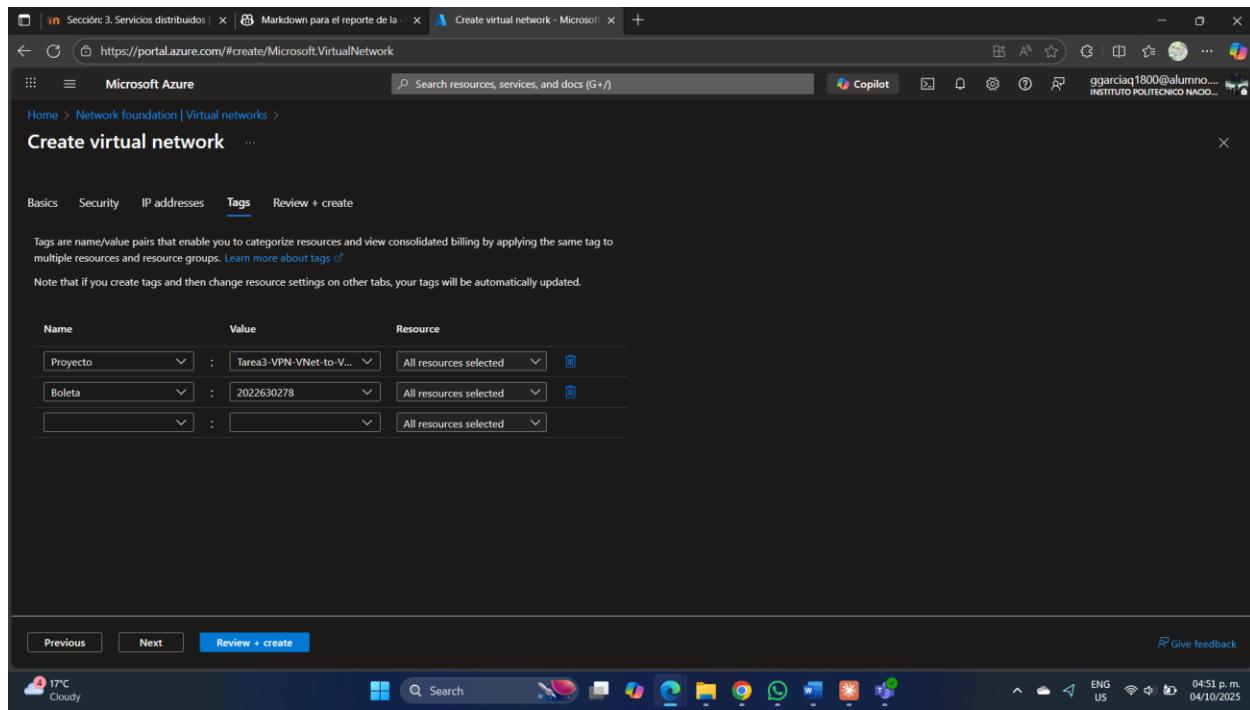
Enable Azure DDoS Network Protection

Previous Next Review + create Give feedback

Paso 5: Etiquetas (opcional)

1. En la pestaña "**Tags**", se pueden agregar etiquetas para organización (opcional):
 - **Name:** Proyecto | **Value:** Tarea3-VPN-VNet-to-VNet
 - **Name:** Boleta | **Value:** 2022630278

2. Hacer clic en "Next: Review + create"



Paso 6: Revisión y creación

1. En la pestaña "**Review + create**", verificar todos los parámetros:
 - Subscription: Azure for Students
 - Resource group: T3-2022630278-rg-1
 - Name: T3-2022630278-vnet-1
 - Region: East US
 - Address space: 10.30.0.0/16
 - Subnet default: 10.30.1.0/24
2. Esperar a que aparezca el mensaje "**Validation passed**" con marca verde
3. Hacer clic en "**Create**"
4. Esperar a que se complete el despliegue (generalmente toma menos de 1 minuto)

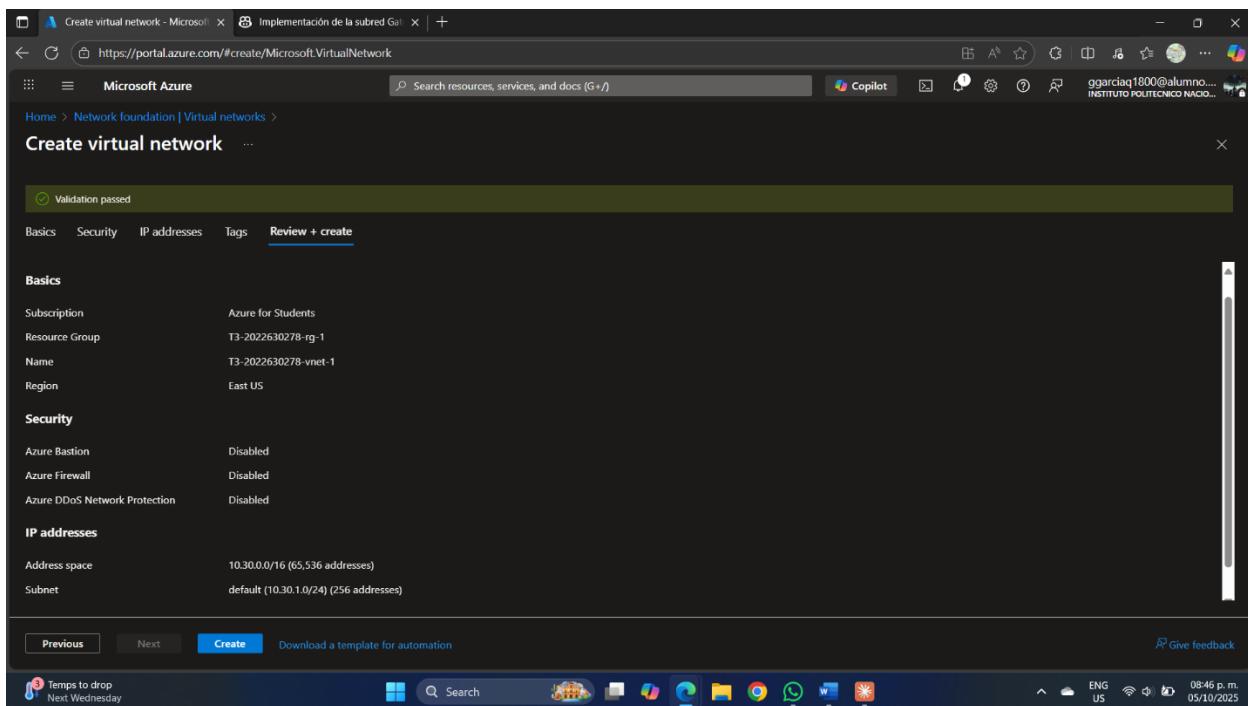


IMAGEN 6: Pestaña "Review + create" - Resumen de configuración de vnet-1

Esta captura debe mostrar el resumen completo de la configuración antes de crear la VNet. Debe incluir todos los detalles: nombre del recurso, grupo de recursos, región, espacio de direcciones IP, y la subred default. En la parte superior debe aparecer el mensaje verde "Validation passed". Esta imagen sirve como evidencia de que todos los parámetros fueron configurados correctamente antes de la creación.

Paso 7: Verificación de creación exitosa

1. Esperar el mensaje "Your deployment is complete"
2. Hacer clic en "**Go to resource**" para verificar la VNet creada
3. En el panel "**Overview**", verificar:
 - o Name: T3-2022630278-vnet-1
 - o Resource group: T3-2022630278-rg-1
 - o Location: East US
 - o Address space: 10.30.0.0/16

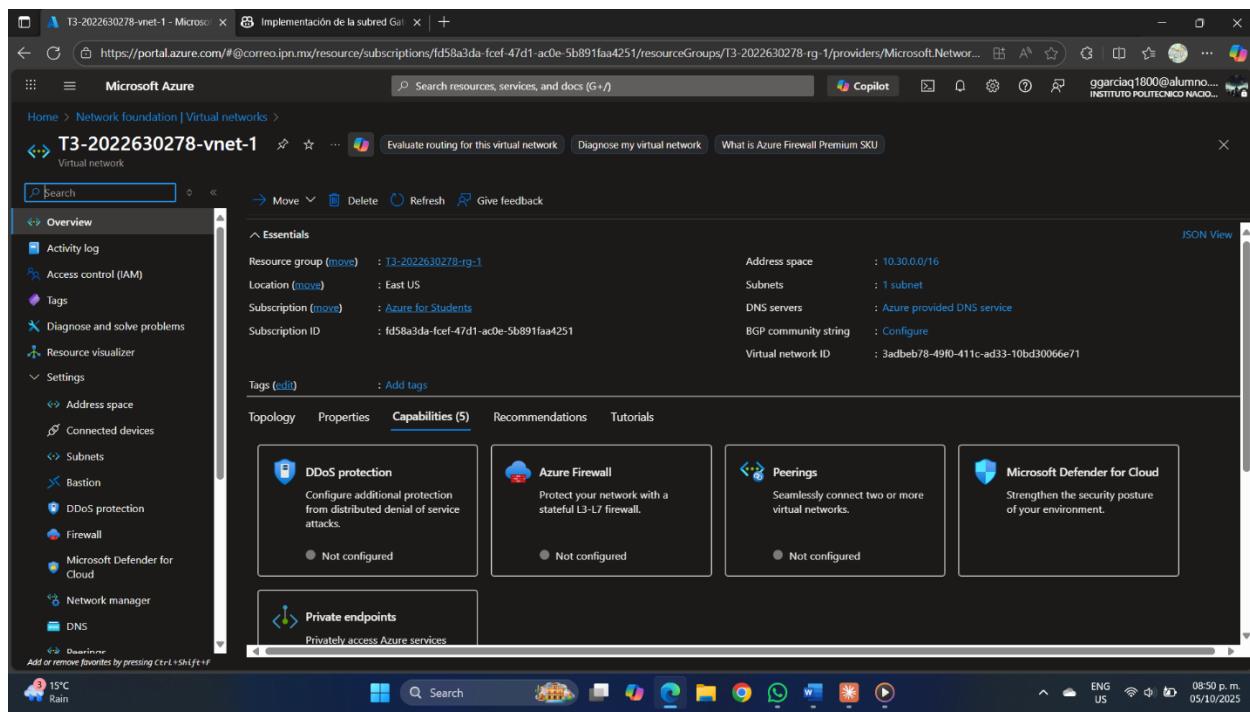


IMAGEN 6-A: Panel "Overview" de la VNet-1 creada

Esta captura debe mostrar el panel "Overview" (Información general) de la Virtual Network recién creada. Se deben visualizar claramente las propiedades principales: nombre, grupo de recursos, ubicación, espacio de direcciones (10.30.0.0/16), y el estado del recurso como "Succeeded" o activo. En el menú lateral izquierdo debe estar visible la opción "Subnets" para verificar posteriormente.

5.3 Creación de la Segunda Red Virtual (T3-2022630278-vnet-2)

Siguiendo el mismo procedimiento que para la primera VNet, crearemos la segunda red virtual en una región diferente con un espacio de direcciones que no traslape con la primera red. Es fundamental mantener espacios de direcciones IP completamente separados para evitar conflictos de enrutamiento en la VPN VNet-to-VNet.

Paso 1: Iniciar creación de la segunda Virtual Network

1. En el portal de Azure, hacer clic nuevamente en "**+ Create a resource**"
2. Buscar "Virtual Network"
3. Seleccionar "**Virtual Network**" y hacer clic en "**Create**"

Name	Resource group	Location	Subscription
T2-2022630278-vnet	T2-2022630278-group_09271755	Mexico Central	Azure for Students
T3-2022630278-rg-1	T3-2022630278-rg-1	East US	Azure for Students
T3-2022630278-rg-2	T3-2022630278-rg-2	West US 2	Azure for Students

Paso 2: Configuración básica de la VNet-2

1. En la pestaña "**Basics**", completar:
 - **Subscription:** Azure for Students
 - **Resource group:** Seleccionar T3-2022630278-rg-2 del dropdown (importante: usar RG-2, no RG-1)
 - **Name:** T3-2022630278-vnet-2
 - **Region:** West US (diferente a la primera VNet para simular conectividad inter-regional)
2. Hacer clic en "Next: IP Addresses"

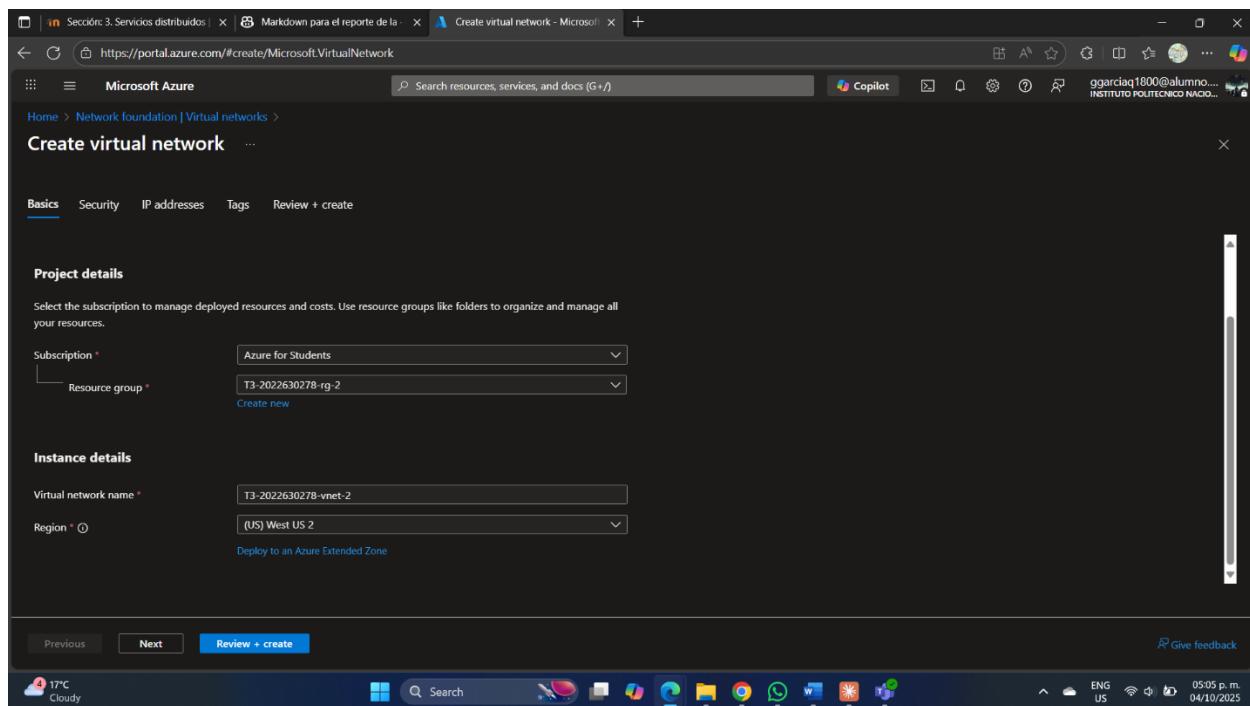


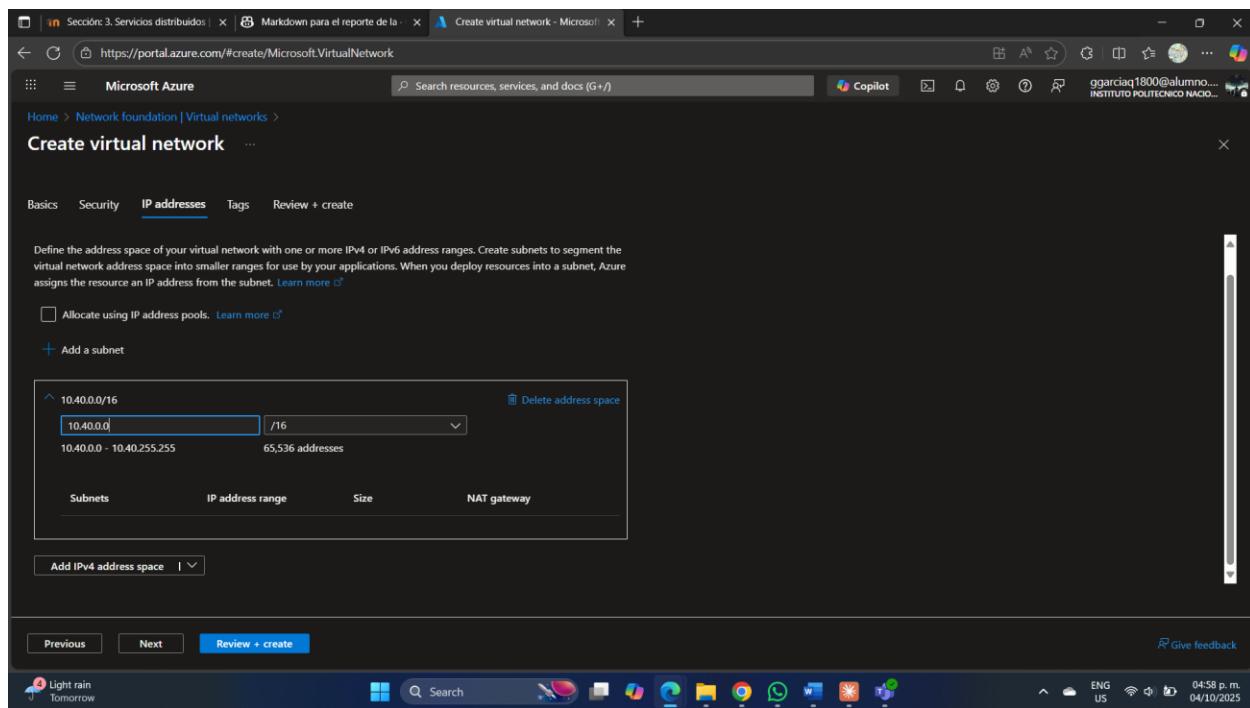
IMAGEN 7: Pestaña "Basics" de creación de la segunda Virtual Network

Esta captura debe mostrar el formulario de configuración básica de la segunda VNet. Verificar que sea visible el nombre T3-2022630278-vnet-2, el Resource Group T3-2022630278-rg-2 (diferente al primero), y la región "West US" (diferente a la primera VNet). Es importante que esta imagen demuestre claramente que se está creando un recurso separado en otra región.

Paso 3: Configuración del espacio de direcciones IP (sin traslape)

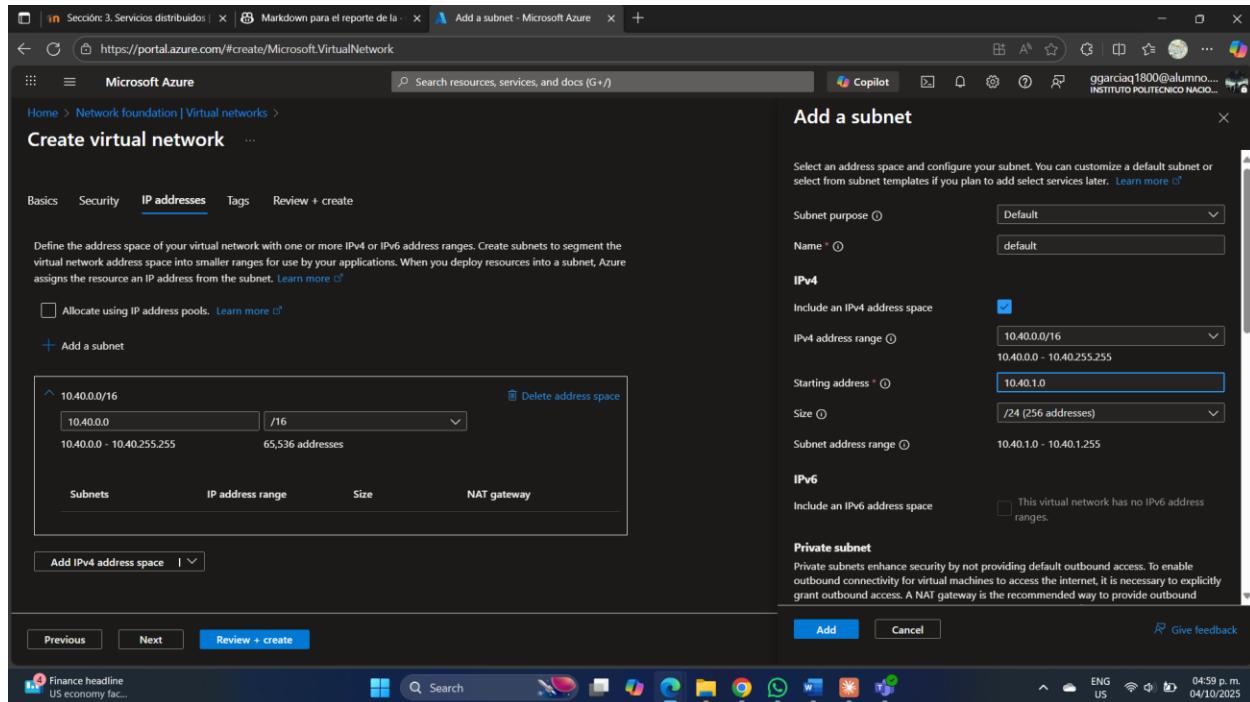
1. En la pestaña "IP Addresses", configurar:

- **IPv4 address space:** Eliminar cualquier espacio predeterminado y agregar 10.40.0.0/16
- **⚠ IMPORTANTE:** Este espacio NO debe traslapar con el de la primera VNet (10.30.0.0/16)



2. Configurar la subred predeterminada:

- Si existe una subred "default", editarla haciendo clic en el ícono de lápiz
- Si no existe, hacer clic en "**+ Add subnet**"
- Subnet name: default
- Subnet address range: 10.40.1.0/24
- Hacer clic en "**Add**" o "**Save**"



3. Verificar que el espacio de direcciones sea 10.40.0.0/16 y la subred 10.40.1.0/24
4. Hacer clic en "Next: Security"

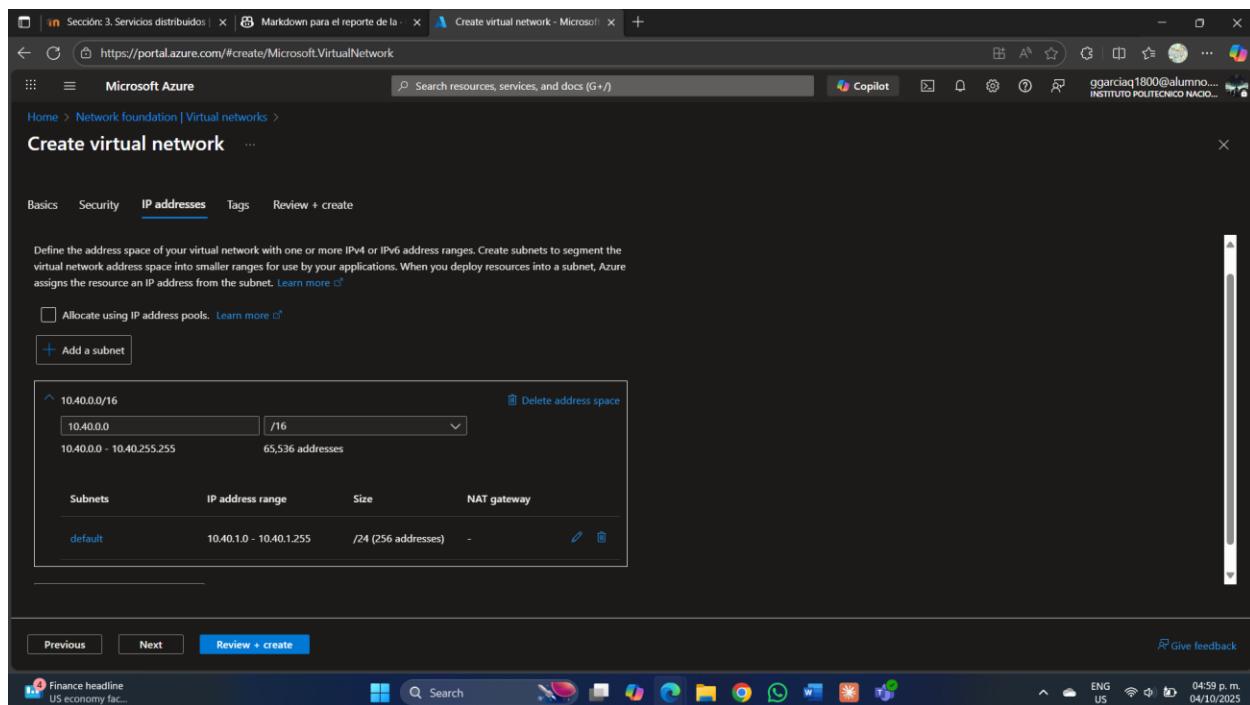


IMAGEN 8: Pestaña "IP Addresses" de vnet-2 con address space 10.40.0.0/16

Esta captura debe mostrar la pestaña "IP Addresses" de la segunda VNet con el espacio de direcciones IPv4 configurado como 10.40.0.0/16 (diferente al 10.30.0.0/16 de la primera VNet). Debe visualizarse la subred "default" con el rango 10.40.1.0/24. Esta imagen es crítica porque demuestra que se está utilizando un esquema de direccionamiento IP sin traslapes, requisito fundamental para la conectividad VPN VNet-to-VNet.

Paso 4: Configuración de seguridad y tags

1. En la pestaña "**Security**", dejar las opciones predeterminadas deshabilitadas:
 - BastionHost: Disabled
 - DDoS Protection Standard: Disabled
 - **Firewall:** Disabled

The screenshot shows the 'Create virtual network' wizard in Microsoft Azure. The 'Security' tab is selected. Under 'Virtual network encryption', there is a checked checkbox. Under 'Azure Bastion', there is an unchecked checkbox. Other sections like 'Azure Firewall' and 'Azure DDoS Network Protection' are also visible.

This screenshot shows the same 'Create virtual network' wizard as the previous one, but with different checkbox states. The 'Enable Azure Bastion' checkbox is now unchecked, while the 'Enable Azure Firewall' checkbox is checked. The other sections remain the same.

2. Hacer clic en "Next: Tags"

3. Hacer clic en "Next: Review + create"

Paso 5: Revisión y creación

1. En la pestaña "**Review + create**", verificar meticulosamente:

- Subscription: Azure for Students
 - Resource group: T3-2022630278-rg-2 ✓
 - Name: T3-2022630278-vnet-2 ✓
 - Region: West US ✓
 - Address space: 10.40.0.0/16 ✓ (diferente a 10.30.0.0/16)
 - Subnet default: 10.40.1.0/24 ✓
2. Esperar el mensaje "**Validation passed**"
 3. Hacer clic en "**Create**"
 4. Esperar a que se complete el despliegue

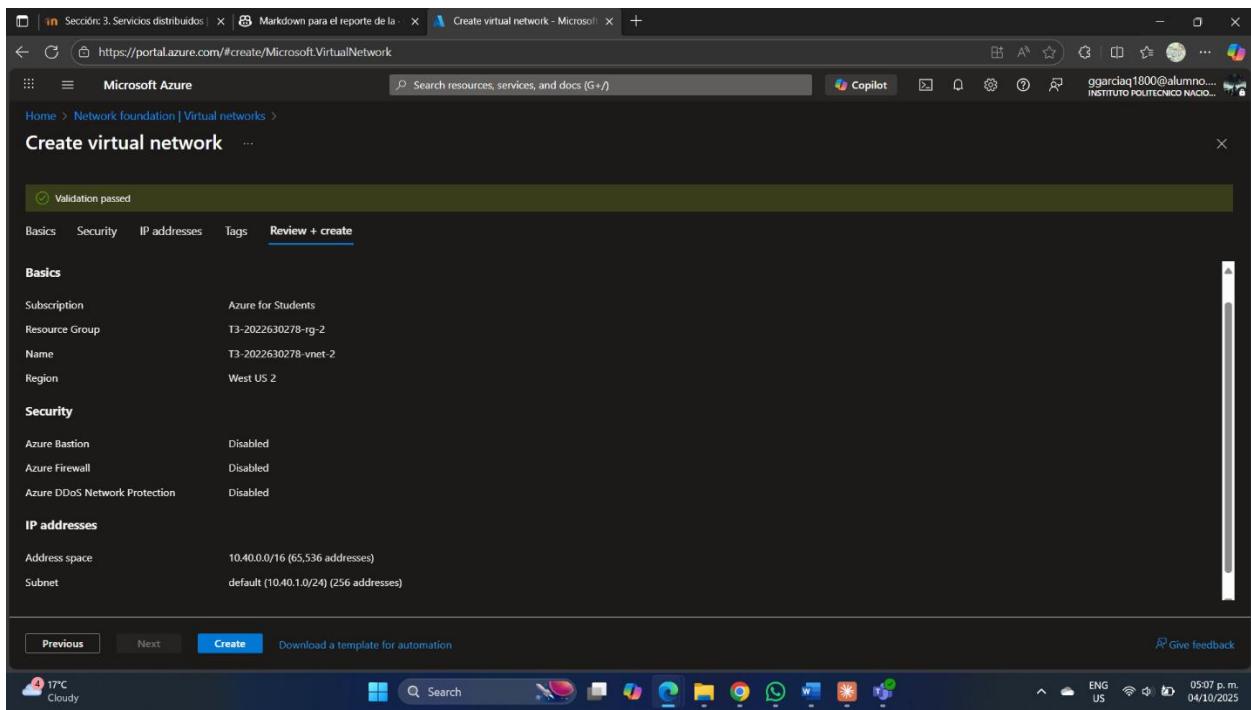


IMAGEN 9: Pestaña "Review + create" - Resumen completo de vnet-2

Esta captura debe mostrar el resumen de validación de la segunda VNet antes de crearla. Es crucial que se visualicen todos los parámetros correctamente: el nombre T3-2022630278-vnet-2, el Resource Group T3-2022630278-rg-2, la región "West US", el address space 10.40.0.0/16, y la subred default 10.40.1.0/24. El mensaje "Validation passed" debe estar visible en la parte superior con una marca de verificación verde.

Paso 6: Verificación de creación exitosa

1. Esperar el mensaje "Your deployment is complete"
2. Hacer clic en "Go to resource"
3. En el panel "**Overview**", verificar:
 - o Name: T3-2022630278-vnet-2
 - o Resource group: T3-2022630278-rg-2
 - o Location: West US
 - o Address space: 10.40.0.0/16

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#@correo.ipn.mx/resource/subscriptions/ld58a3da-fcef-47d1-ac0e-5b891faa4251/resourcegroups/T3-2022630278-rg-2/providers/Microsoft.Network/virtualNetworks/T3-2022630278-vnet-2>. The page title is "T3-2022630278-vnet-2 - Microsoft Azure". The left sidebar shows the navigation path: Home > T3-2022630278-vnet-2 > Virtual network. The main content area is titled "Overview" and includes sections for "Essentials" and "Capabilities (5)". In the "Essentials" section, it lists the following details:

	:	
Resource group	:	T3-2022630278-rg-2
Location	:	West US 2
Subscription	:	Azure for Students
Subscription ID	:	fd58a3da-fcef-47d1-ac0e-5b891faa4251
Address space	:	10.40.0.0/16
Subnets	:	1 subnet
DNS servers	:	Azure provided DNS service
BGP community string	:	Configure
Virtual network ID	:	ab0a094f-6d82-4aa6-86fe-760ffe313921

The "Capabilities" section shows five items, all marked as "Not configured":

- DDoS protection
- Azure Firewall
- Peering
- Microsoft Defender for Cloud
- Private endpoints

IMAGEN 9-A: Panel "Overview" de la VNet-2 creada

Esta captura debe mostrar el panel de información general de la segunda Virtual Network después de su creación exitosa. Debe incluir todos los detalles: nombre correcto, grupo de recursos RG-2, ubicación West US, y espacio de direcciones 10.40.0.0/16. Esta imagen confirma que ambas VNets están en regiones diferentes y con espacios IP separados, listos para la configuración de la VPN.

Paso 7: Verificación comparativa de ambas VNets

1. Navegar a "**Virtual networks**" desde el menú principal
2. Verificar que aparezcan ambas VNets en la lista:

- T3-2022630278-vnet-1 (Méjico Central, 10.30.0.0/16)
- T3-2022630278-vnet-2 (West US, 10.40.0.0/16)

Name	Resource group	Location	Subscription
T2-2022630278-vnet	T2-2022630278_group_09271755	Mexico Central	Azure for Students
T3-2022630278-vnet-1	T3-2022630278-rg-1	East US	Azure for Students
T3-2022630278-vnet-2	T3-2022630278-rg-2	West US 2	Azure for Students

IMAGEN 9-B: Lista de Virtual Networks mostrando ambas VNets creadas

Esta captura opcional pero muy útil debe mostrar la lista completa de Virtual Networks en el portal. Deben ser visibles ambas redes: T3-2022630278-vnet-1 en East US y T3-2022630278-vnet-2 en West US, con sus respectivos espacios de direcciones. Esta vista panorámica ayuda a confirmar que ambas redes están correctamente creadas y listas para los siguientes pasos de configuración de gateways.

Resumen de lo creado hasta ahora:

Recurso	Nombre	Región	Address	Subnet	Resource
			Space	Default	Group
VNet 1	T3-2022630278-vnet-1	Méjico Central	10.30.0.0/16	10.30.1.0/24	T3-2022630278-rg-1

VNet 2	T3-2022630278-vnet-2	West US	10.40.0.0/16	10.40.1.0/24	T3-2022630278-rg-2
--------	----------------------	---------	--------------	--------------	--------------------

5.4 Creación de las subredes GatewaySubnet

La subred GatewaySubnet es un componente obligatorio y crítico para el despliegue de Virtual Network Gateways en Azure. Esta subred debe tener exactamente ese nombre (sin variaciones) y proporciona el espacio de direcciones donde se desplegarán los componentes internos del gateway. Microsoft recomienda usar al menos una máscara /27 (32 direcciones IP) para garantizar suficiente espacio para futuras expansiones o configuraciones de alta disponibilidad.

5.4.1 Crear GatewaySubnet en la primera VNet (T3-2022630278-vnet-1)

Paso 1: En el Portal de Azure, navegar al menú lateral izquierdo y seleccionar "**Redes virtuales**" (Virtual networks).

Paso 2: En la lista de redes virtuales, localizar y hacer clic en T3-2022630278-vnet-1 para acceder a su panel de configuración.

Paso 3: En el menú lateral izquierdo de la VNet, localizar y hacer clic en la opción "**Subredes**" (Subnets) dentro de la sección "Settings".

La imagen debe mostrar el panel de subredes de T3-2022630278-vnet-1, con la lista de subredes existentes (típicamente solo "default" en este punto). El menú lateral izquierdo debe mostrar la opción "Subredes" seleccionada. La interfaz debe mostrar claramente el nombre de la VNet en la parte superior y el espacio de direcciones completo (10.30.0.0/16). En la barra de herramientas superior debe estar visible el botón "+ Subred" o "+ Subnet".

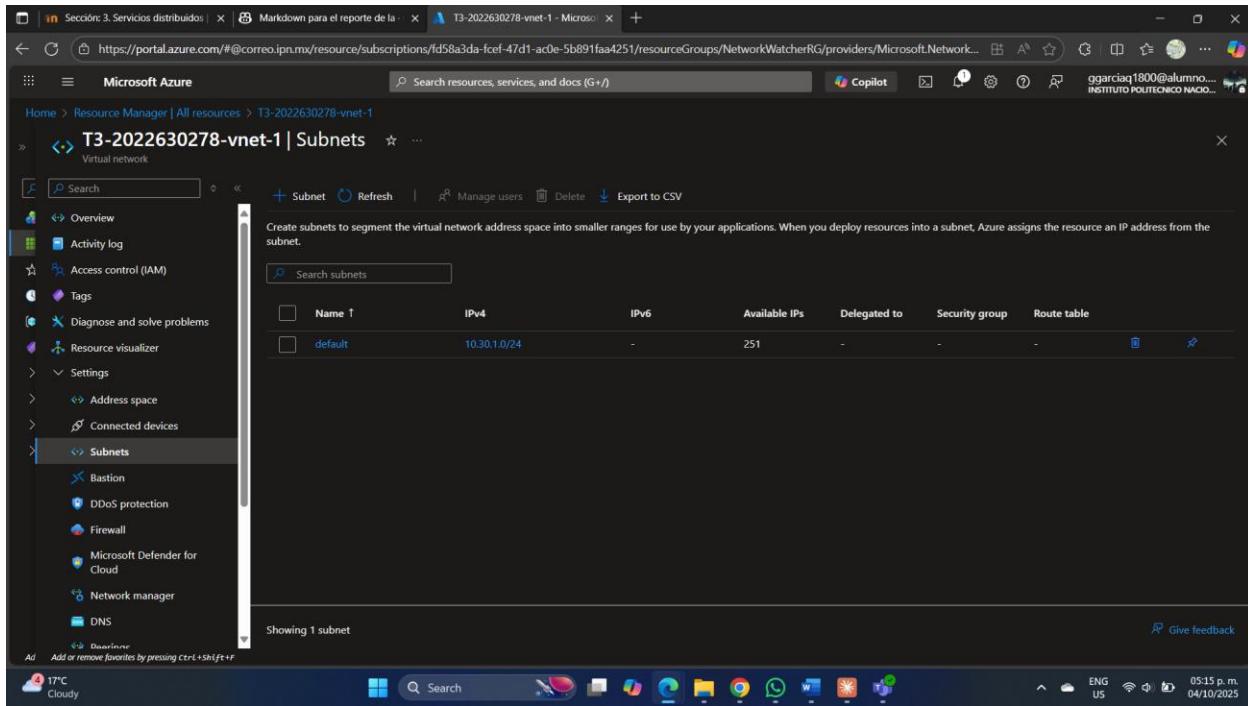


IMAGEN 10a: Panel de subredes de T3-2022630278-vnet-1 antes de crear GatewaySubnet

Paso 4: En la parte superior del panel de subredes, hacer clic en el botón "**+ Subred**" o "**+ Subnet**".

Paso 5: En el panel deslizante "Aregar subred" (Add subnet) que aparece a la derecha, configurar los siguientes campos:

- **Nombre de subred** (Subnet name): Escribir exactamente GatewaySubnet
- **Intervalo de direcciones de subred** (Subnet address range): 10.30.254.0/27
 - Este rango proporciona 32 direcciones IP (de 10.30.254.0 a 10.30.254.31)
 - La elección de la subred .254.0 es una práctica común que separa visualmente la infraestructura de gateway de las subredes de aplicaciones

Paso 6: Verificar que los campos opcionales queden en sus valores predeterminados:

- **Grupo de seguridad de red** (Network security group): None
- **Tabla de rutas** (Route table): None
- Puntos de conexión de servicio (Service endpoints): None
- **Delegación de subred** (Subnet delegation): None

Paso 7: Hacer clic en el botón "Guardar" (Save) en la parte inferior del panel.

La imagen debe mostrar el panel deslizante "Agregar subred" con los campos completados. Debe ser claramente visible:

- Campo "Nombre de subred" con el valor exacto: **GatewaySubnet**
- Campo "Intervalo de direcciones de subred" con el valor: **10.30.254.0/27**
- El nombre de la VNet padre (T3-2022630278-vnet-1) en el contexto superior
- El botón "Guardar" en la parte inferior

La captura debe tomarse justo antes de hacer clic en "Guardar" para documentar la configuración exacta.

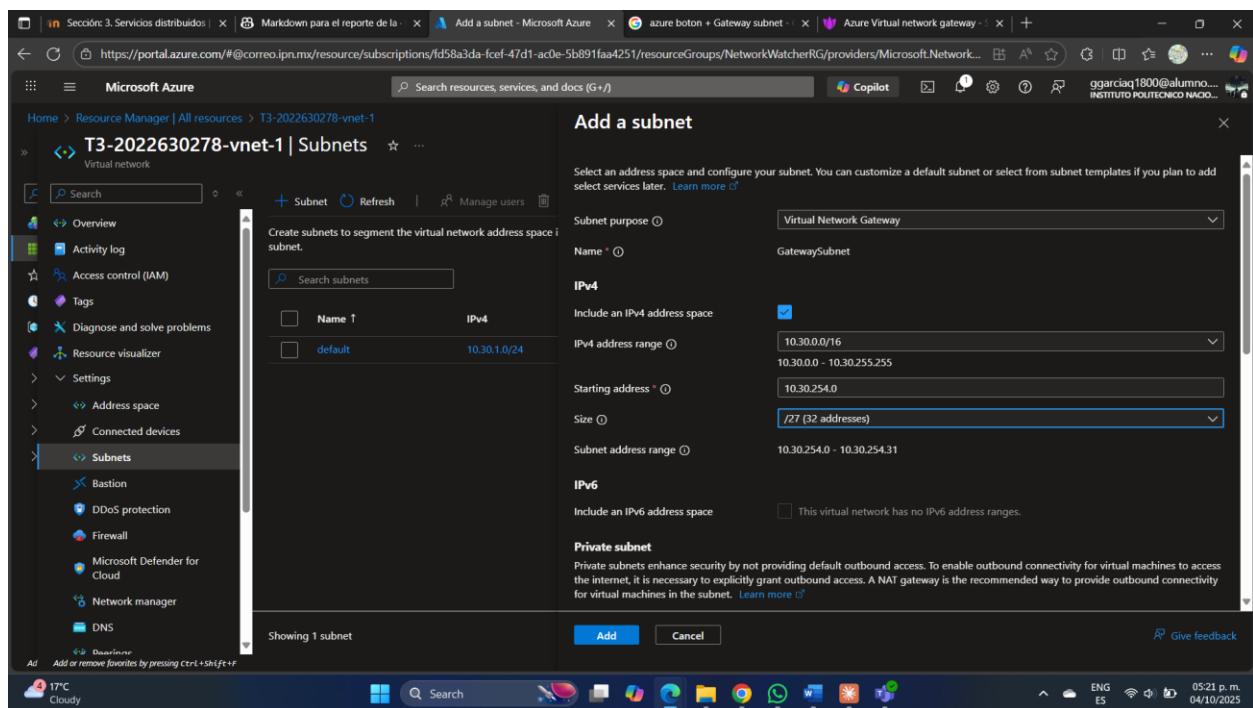


IMAGEN 10b: Configuración del rango de direcciones para GatewaySubnet en vnet-1 (10.30.254.0/27)

Paso 8: Esperar a que Azure complete la operación (generalmente toma 5-10 segundos). Una vez completada, el portal mostrará la nueva subred en la lista y cerrará automáticamente el panel deslizante.

La imagen debe mostrar el panel de subredes actualizado de T3-2022630278-vnet-1, donde ahora aparecen DOS subredes listadas en la tabla:

- **default** – 10.30.1.0/24
- **GatewaySubnet** – 10.30.254.0/27

La columna “Dirección” (Address) debe mostrar los rangos correctos. Esta captura confirma la creación exitosa de la GatewaySubnet y que ambas subredes coexisten sin conflictos de direccionamiento.

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
default	10.30.1.0/24	-	251	-	-	-
GatewaySubnet	10.30.254.0/27	-	available	dependent on ...	-	-

IMAGEN 10c: Lista de subredes actualizada mostrando GatewaySubnet creada en vnet-1

5.4.2 Crear GatewaySubnet en la segunda VNet (T3-2022630278-vnet-2)

Repetir el proceso anterior para la segunda red virtual, con los siguientes parámetros específicos:

Paso 1: En el Portal de Azure, navegar al menú lateral izquierdo y seleccionar "**Redes virtuales**" (Virtual networks).

Paso 2: En la lista de redes virtuales, localizar y hacer clic en T3-2022630278-vnet-2.

Name	Resource group	Location	Subscription
T2-2022630278-vnet	T2-2022630278_group_09271755	Mexico Central	Azure for Students
T3-2022630278-vnet-1	NetworkWatcherRG	Mexico Central	Azure for Students
T3-2022630278-vnet-2	T3-2022630278-rg-2	West US 2	Azure for Students

Paso 3: En el menú lateral izquierdo de la VNet, hacer clic en "**Subredes**" (Subnets).

Similar a la imagen 10a, pero mostrando el contexto de T3-2022630278-vnet-2 con su espacio de direcciones 10.40.0.0/16 y la subred "default" existente (10.40.1.0/24). El botón "+ Subred" debe estar visible en la barra de herramientas.

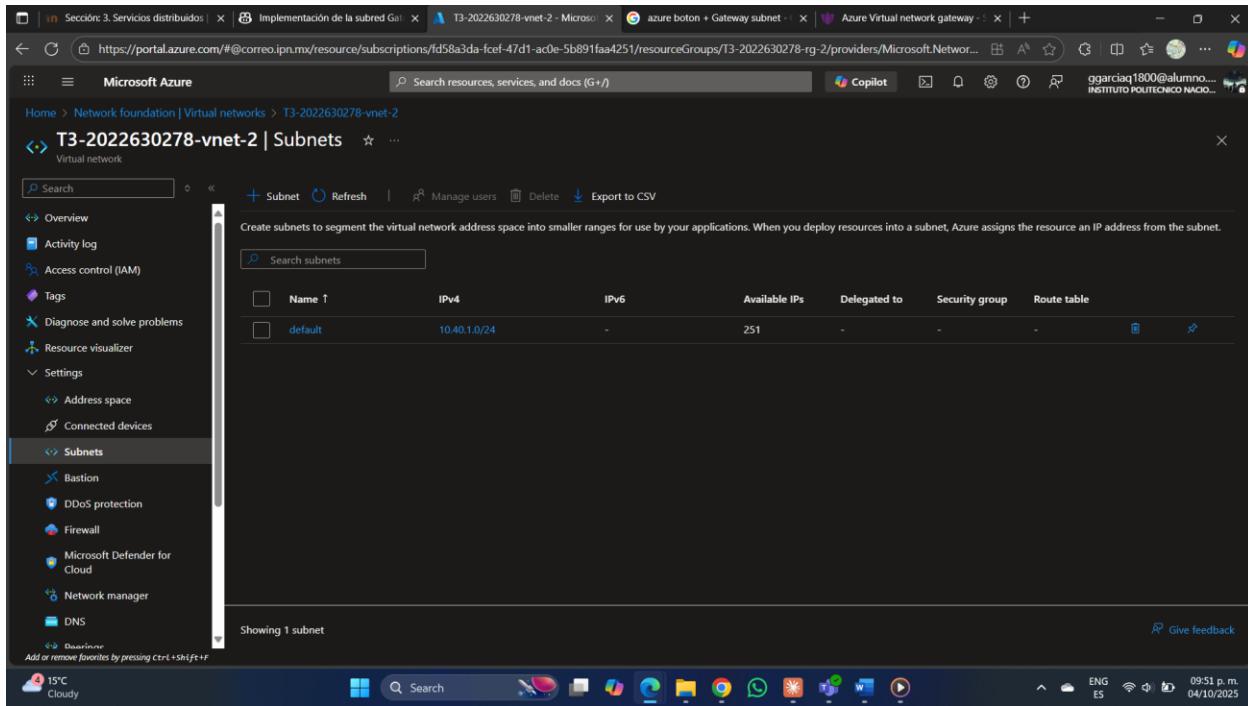


IMAGEN 11a: Panel de subredes de T3-2022630278-vnet-2 antes de crear GatewaySubnet

Paso 4: Hacer clic en el botón "+ Subred" o "+ Subnet".

Paso 5: En el panel deslizante "Agregar subred", configurar:

- **Nombre de subred:** GatewaySubnet (exactamente igual, sin variaciones)
- Intervalo de direcciones de subred: 10.40.254.0/27
 - Este rango corresponde al espacio de direcciones de vnet-2 (10.40.0.0/16)
 - Proporciona 32 direcciones IP (de 10.40.254.0 a 10.40.254.31)

Paso 6: Dejar los campos opcionales en sus valores predeterminados (None).

Paso 7: Hacer clic en "Guardar" (Save).

Panel de configuración "Agregar subred" mostrando:

- Campo "Nombre de subred" con el valor: **GatewaySubnet**
- Campo "Intervalo de direcciones de subred" con el valor: **10.40.254.0/27**
- El contexto debe mostrar claramente que se trata de vnet-2 (no vnet-1)
- El botón "Guardar" debe estar visible

Es importante que sea claramente distinguible de la captura 10b por el rango de direcciones diferente (10.40.x.x vs 10.30.x.x).

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a 'Subnets' section selected under 'Settings'. The main area is titled 'Add a subnet' for 'T3-2022630278-vnet-2'. It's set to 'Virtual Network Gateway' purpose. A table lists a single subnet named 'GatewaySubnet' with an IPv4 range of 10.40.0.0/16 and a size of /27 (32 addresses). The IPv6 section is collapsed. A note about private subnets is present. At the bottom are 'Add' and 'Cancel' buttons.

IMAGEN 11b: Configuración del rango de direcciones para GatewaySubnet en vnet-2 (10.40.254.0/27)

Paso 8: Verificar la creación exitosa esperando a que Azure complete la operación.

Panel de subredes de vnet-2 mostrando ambas subredes en la tabla:

- **default** - 10.40.1.0/24
- **GatewaySubnet** - 10.40.254.0/27

Esta captura confirma que ambas VNets ahora tienen la infraestructura de subred necesaria para los gateways. La diferencia en los rangos de direcciones (10.30.x.x vs 10.40.x.x) documenta que no hay traslape entre las redes virtuales.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes Home, Network foundation, Virtual networks, and a specific resource named 'T3-2022630278-vnet-2'. Under 'Virtual networks', the 'Subnets' section is selected. The main content area shows a table of subnets with columns: Name, IPv4, IPv6, Available IPs, Delegated to, Security group, and Route table. Two subnets are listed: 'default' (IPv4: 10.40.1.0/24) and 'GatewaySubnet' (IPv4: 10.40.254.0/27). A success message at the top right says 'Successfully added subnet'.

IMAGEN 11c: Lista de subredes actualizada mostrando GatewaySubnet creada en vnet-2

5.4.3 Verificación consolidada

Una vez creadas ambas GatewaySubnets, es recomendable verificar que la configuración sea consistente en ambas VNets.

Checklist de verificación:

- Ambas subredes se llaman exactamente "GatewaySubnet"
- Ambas tienen máscara /27 (32 direcciones IP disponibles)
- Los rangos no se traslanan (10.30.254.0/27 vs 10.40.254.0/27)
- Ambas están dentro del espacio de direcciones de su VNet respectiva
- No tienen NSG, Route Table, ni Service Endpoints asociados

Captura de pantalla mostrando una tabla comparativa o vista de "All resources" filtrada para mostrar ambas VNets con sus subredes expandidas. Esta vista panorámica puede ayudar a documentar que la configuración es simétrica y correcta antes de proceder con los gateways.

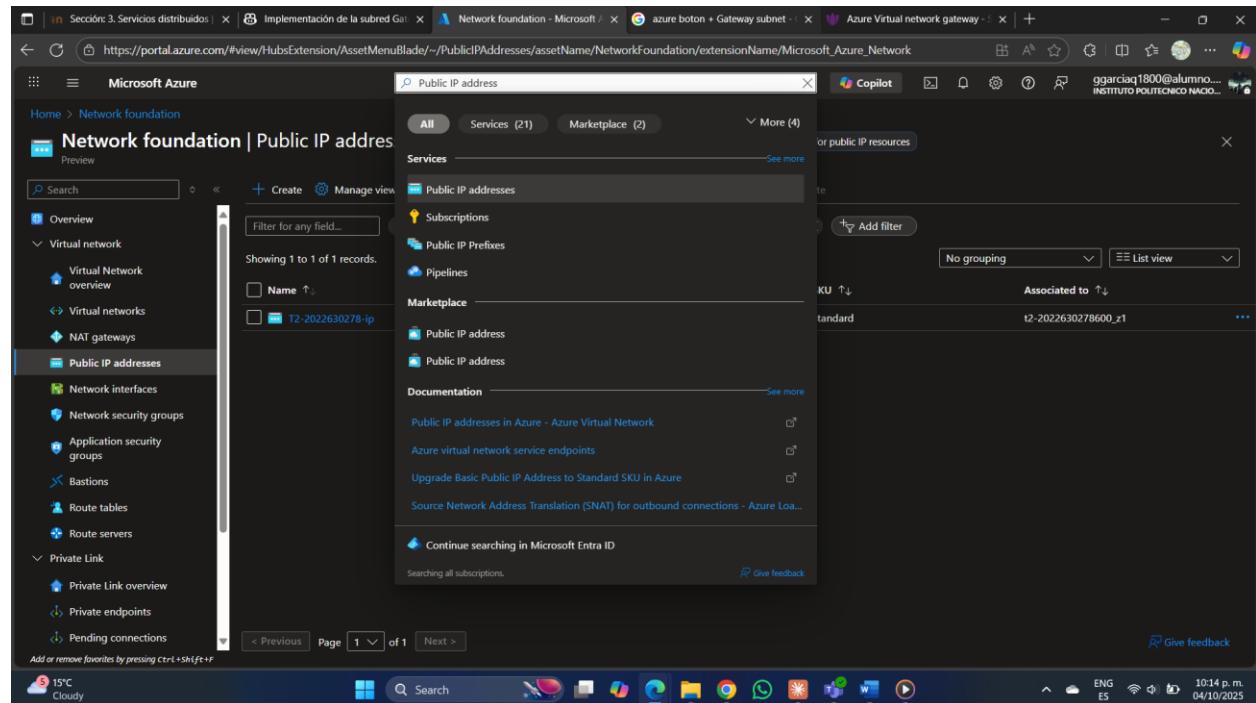
5.5 Creación de IPs públicas para los Gateways

Los Virtual Network Gateways requieren direcciones IP públicas para establecer los túneles VPN. Estas IPs públicas actúan como los endpoints externos que permiten la comunicación entre gateways ubicados en diferentes regiones. Azure asigna estas direcciones desde su pool global y se mantienen asociadas al gateway durante su ciclo de vida.

Para esta implementación, se utilizará el SKU **Standard** con asignación **Static**, lo cual es un requisito para gateways VPN de tipo VpnGw1 o superior. Las IPs estáticas garantizan que la dirección no cambie, manteniendo la estabilidad de las conexiones VPN.

5.5.1 Crear la primera IP pública (T3-2022630278-ip-1)

Paso 1: En la barra de búsqueda, escribir Public IP address y presionar Enter.



Paso 2: Seleccionar **Public IP address** de los resultados (publicado por Microsoft) y hacer clic en el botón **Create**.

La imagen debe mostrar el Marketplace de Azure con "Public IP address" en la barra de búsqueda. El resultado relevante debe estar visible con su icono característico de Microsoft Azure y el botón "Create" debe ser claramente visible.

The screenshot shows a Microsoft Edge browser window with several tabs open. The active tab is titled 'Network foundation - Microsoft / azure botón + Gateway subnet -'. The search bar at the top contains the query 'azul botón + Gateway subnet'. Below the search bar, the page title is 'Network foundation | Public IP addresses'. On the left, there's a navigation sidebar with categories like 'Overview', 'Virtual network', 'Public IP addresses' (which is selected), 'Network interfaces', etc. The main content area displays a table with one record: 'T2-2022630278-ip' (IP address: 158.23.160.73, IP version: IPv4, SKU: Standard). At the bottom of the table, it says 'Associated to t2-2022630278600_z1'. The status bar at the bottom of the screen shows the date '04/10/2025' and time '10:15 p.m.'

IMAGEN 12a: Búsqueda de Public IP address en el Azure Marketplace

Paso 4: En la pestaña **Basics** del formulario de creación, configurar los siguientes campos:

- **Subscription:** Seleccionar la suscripción de Azure for Students activa
- **Resource group:** Seleccionar T3-2022630278-rg-1 (correspondiente a la primera región)
- **Region:** Seleccionar la misma región donde se desplegó vnet-1
- **Name:** T3-2022630278-ip-1
- **IP Version:** IPv4
- **SKU: Standard** (requerido para VPN Gateways de nueva generación)
- **Availability zone:** Zone-redundant (si está disponible en la región, mejora la resiliencia)
- **Tier:** Regional
- **Assignment:** Static (obligatorio para SKU Standard)

- **Routing preference:** Microsoft network (recomendado para menor latencia)

Create public IP address

Basics

Create a public IP address. Associate it with a virtual machine or other Azure resources. Internet resources communicate to Azure resources through a public IP address. [Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription: Azure for Students

Resource group: T3-2022630278-rg-1

Region: (US) East US

Instance details

Region: (US) East US

Deploy to an Azure Extended Zone

Review + create

The limit for global public IP addresses with the selected IP version in the selected subscription and region has been reached.

The limit for public IP addresses with 'Internet' routing preference in the selected subscription and region has been reached.

Paso 6: Hacer clic en **Review + create** para validar la configuración.

La imagen debe mostrar el formulario de creación de Public IP address con todos los campos completados según lo especificado. Debe ser claramente visible: el nombre T3-

2022630278-ip-1, el Resource Group T3-2022630278-rg-1, SKU Standard, Assignment Static, y la región seleccionada. La captura debe incluir la parte superior del formulario mostrando el título "Create public IP address".

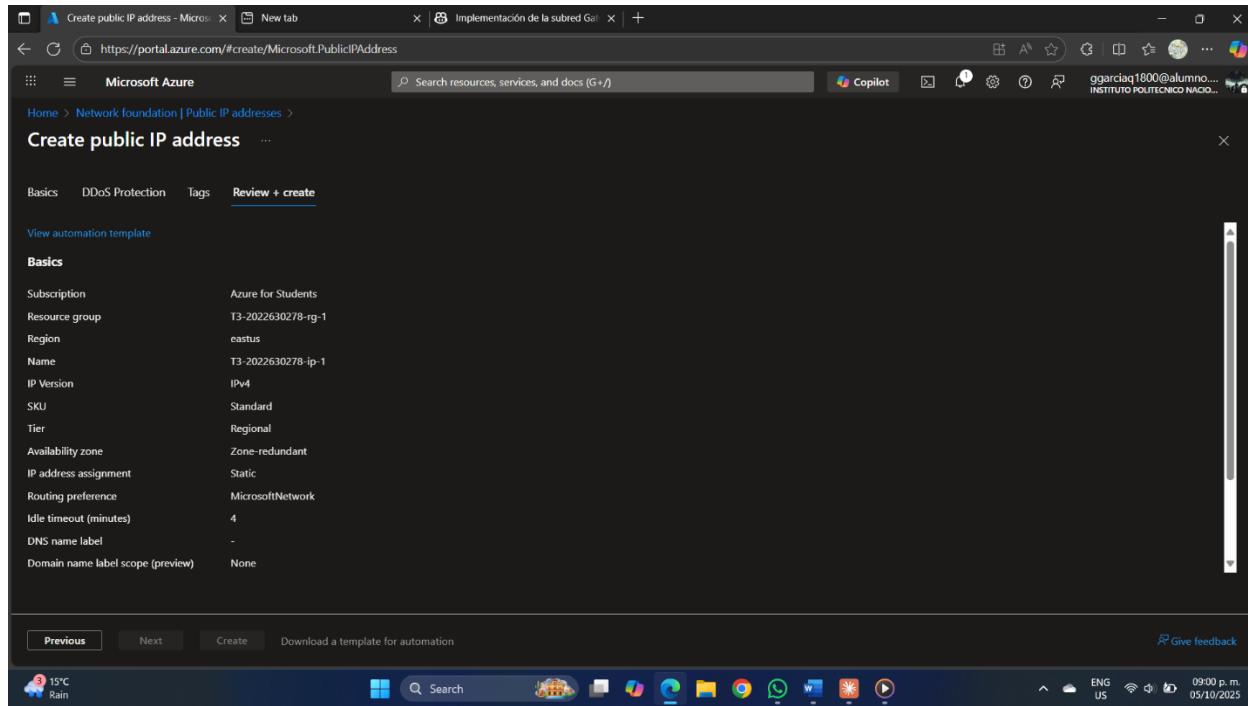


IMAGEN 12b: Configuración completa para la creación de T3-2022630278-ip-1

Paso 7: Revisar el resumen de validación y hacer clic en **Create**.

Paso 8: Esperar a que se complete el despliegue (generalmente 10-20 segundos). Azure mostrará una notificación de "Deployment succeeded".

Paso 9: Hacer clic en **Go to resource** para ver los detalles de la IP pública creada.

La imagen debe mostrar el panel "Overview" de la IP pública recién creada (T3-2022630278-ip-1). Debe ser visible: el nombre del recurso, la dirección IP pública asignada por Azure (ejemplo: 20.x.x.x), el estado "Succeeded", SKU Standard, Assignment type Static, y la región. También debe mostrarse que actualmente está "Not associated" (sin asociar a ningún recurso aún).

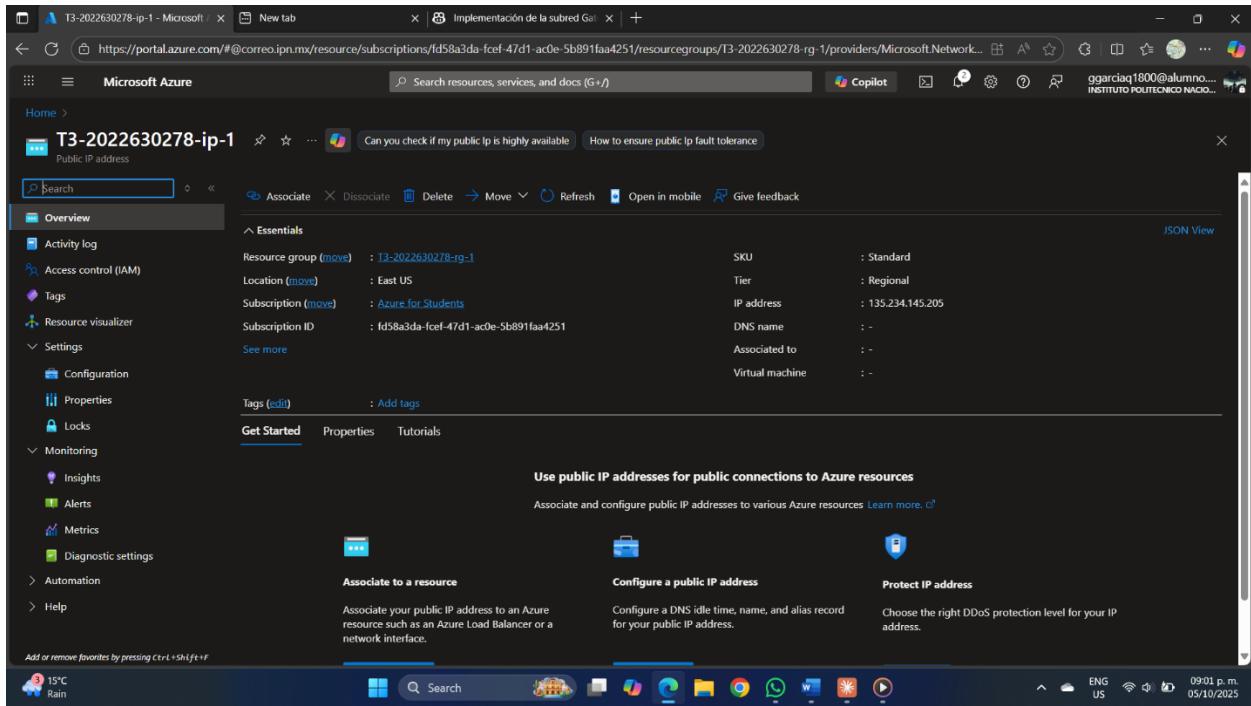


IMAGEN 12c: Panel Overview de T3-2022630278-ip-1 mostrando la IP pública asignada

5.5.2 Crear la segunda IP pública (T3-2022630278-ip-2)

Repetir el proceso anterior con los siguientes parámetros específicos para la segunda región:

Paso 1-3: Navegar nuevamente a Create a resource > Public IP address > Create

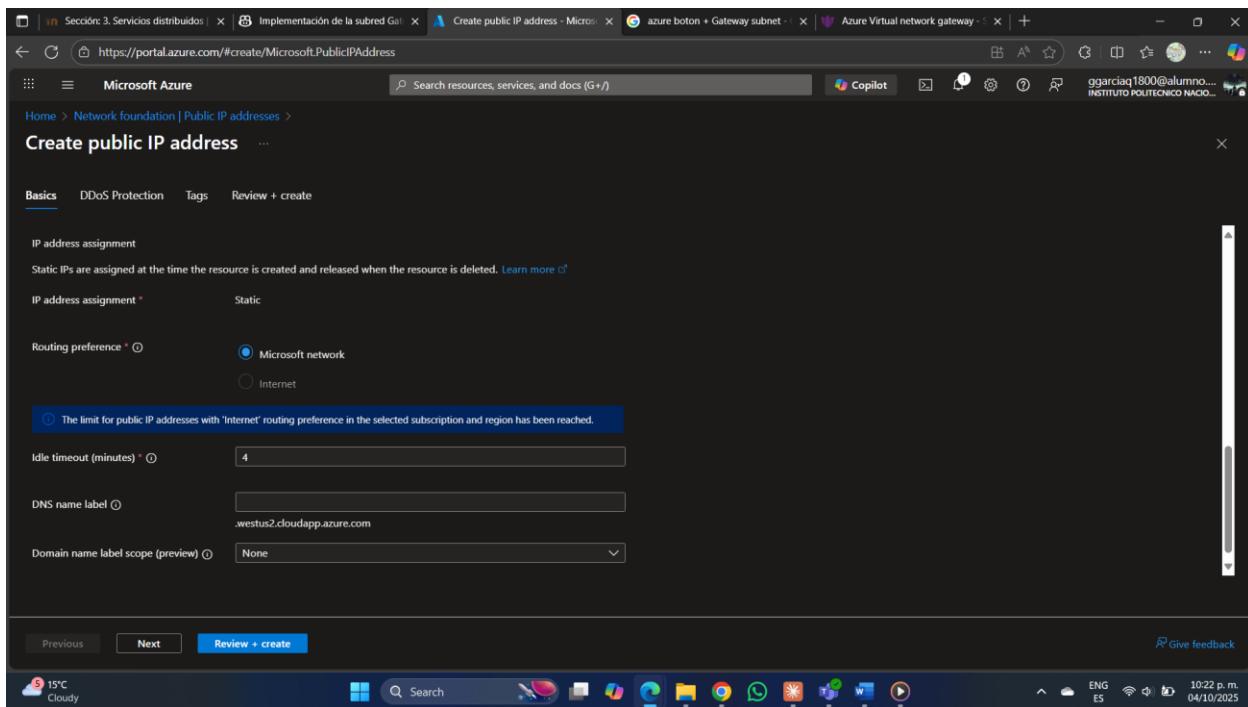
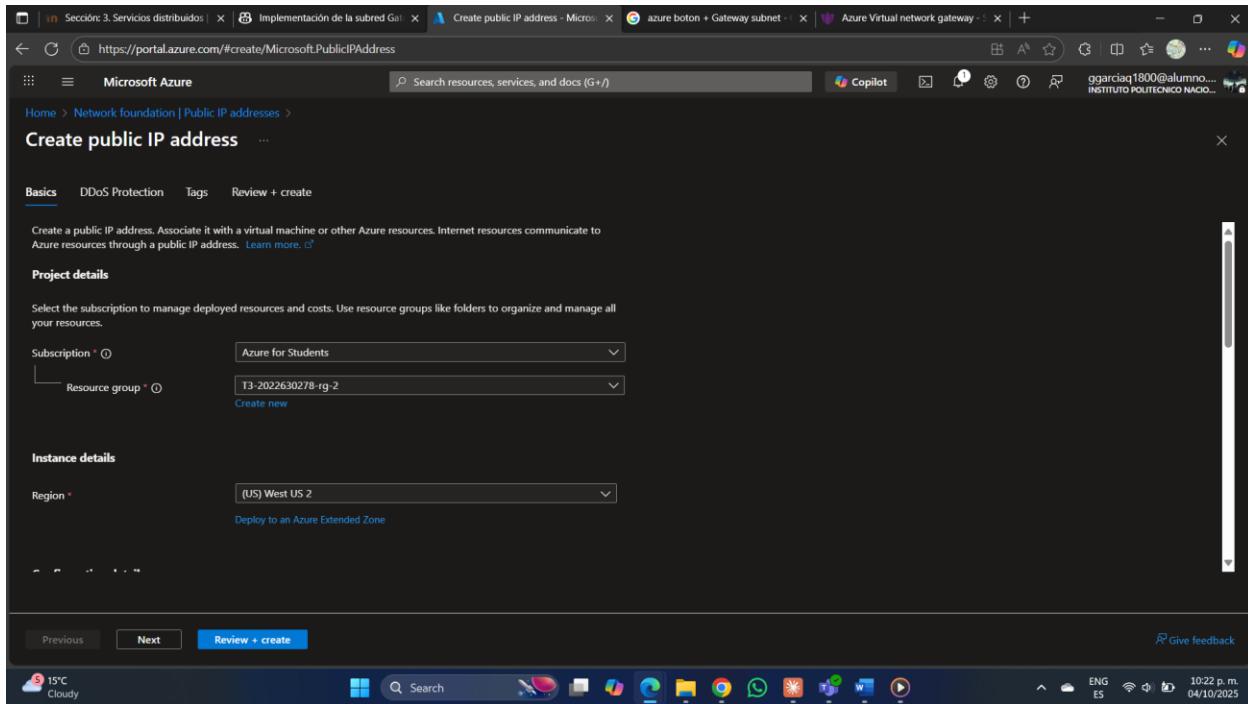
The screenshot shows the Microsoft Azure portal interface. The main title is "Network foundation | Public IP addresses". On the left, there's a sidebar with a tree view of network resources, including "Virtual network", "Public IP addresses" (which is currently selected), and other options like "Network interfaces" and "Bastions". The main content area shows a table with two rows of data:

Name	IP address	IP version	SKU	Associated to
T2-2022630278-ip-1	158.23.160.73	IPv4	Standard	t2-2022630278600_z1
T3-2022630278-ip-1	158.23.240.237	IPv4	Standard	-

At the bottom of the portal window, there are standard Windows taskbar icons and system status indicators.

Paso 4: Configurar el formulario Basics:

- **Subscription:** Azure for Students
- **Resource group:** T3-2022630278-rg-2 (correspondiente a la segunda región)
- Region: Seleccionar la misma región donde se desplegó vnet-2
- **Name:** T3-2022630278-ip-2
- IP Version: IPv4
- SKU: Standard
- Availability zone: Zone-redundant
- **Tier:** Regional
- Assignment: Static
- **Routing preference:** Microsoft network



Paso 6: Hacer clic en Review + create

Formulario de creación mostrando la configuración para T3-2022630278-ip-2, con el Resource Group T3-2022630278-rg-2 y la región correspondiente a vnet-2 (diferente de la primera IP). Todos los demás parámetros deben coincidir con la primera IP pública.

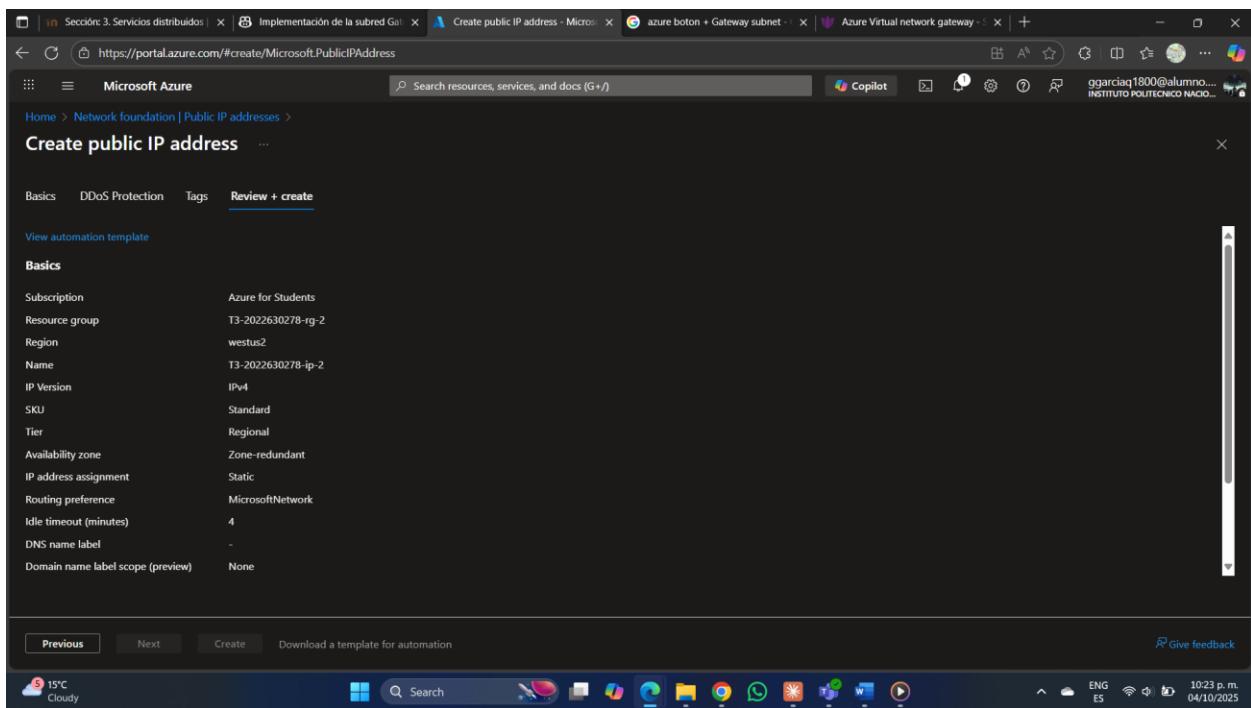


IMAGEN 13a: Configuración completa para la creación de T3-2022630278-ip-2

Paso 7: Hacer clic en **Create** y esperar el despliegue

Paso 8: Acceder al recurso creado mediante **Go to resource**

Panel Overview de T3-2022630278-ip-2 mostrando la dirección IP pública asignada (diferente de ip-1), estado Succeeded, y configuración Static/Standard. La región debe ser claramente diferente de la primera IP pública, confirmando el despliegue multi-región.

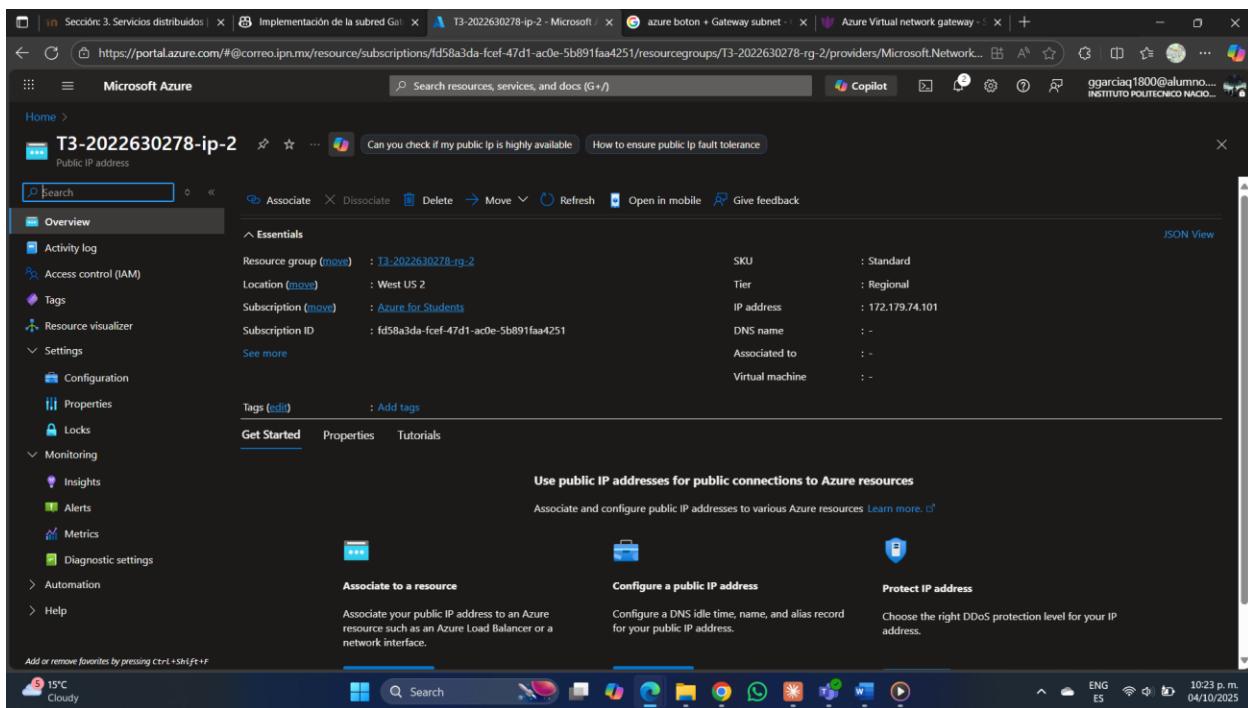


IMAGEN 13b: Panel Overview de T3-2022630278-ip-2 mostrando la IP pública asignada

Verificación final: En este punto, se deben tener dos IPs públicas creadas:

- T3-2022630278-ip-1 en la región de vnet-1 (ejemplo: East US)
- T3-2022630278-ip-2 en la región de vnet-2 (ejemplo: West US)

Ambas IPs deben tener SKU Standard, asignación Static, y estar en estado "Not associated".

5.6 Creación de los Virtual Network Gateways

Los Virtual Network Gateways son la pieza central de la arquitectura VPN VNet-to-VNet. Estos componentes administrados de Azure establecen y mantienen los túneles IPsec/IKE cifrados entre las redes virtuales. El proceso de creación es uno de los más lentos en Azure, típicamente requiriendo entre 30 y 45 minutos por gateway debido a la complejidad del aprovisionamiento de infraestructura dedicada.

5.6.1 Crear el primer Virtual Network Gateway (T3-2022630278-gateway-1)

Paso 1: En el Portal de Azure, hacer clic en **+ Create a resource**

Paso 2: Buscar Virtual Network Gateway en el Marketplace y seleccionar el resultado publicado por Microsoft

Paso 3: Hacer clic en **Create**

Página del Marketplace mostrando "Virtual Network Gateway" seleccionado, con su descripción y el botón "Create" visible. La imagen debe mostrar el ícono oficial de Virtual Network Gateway de Azure.

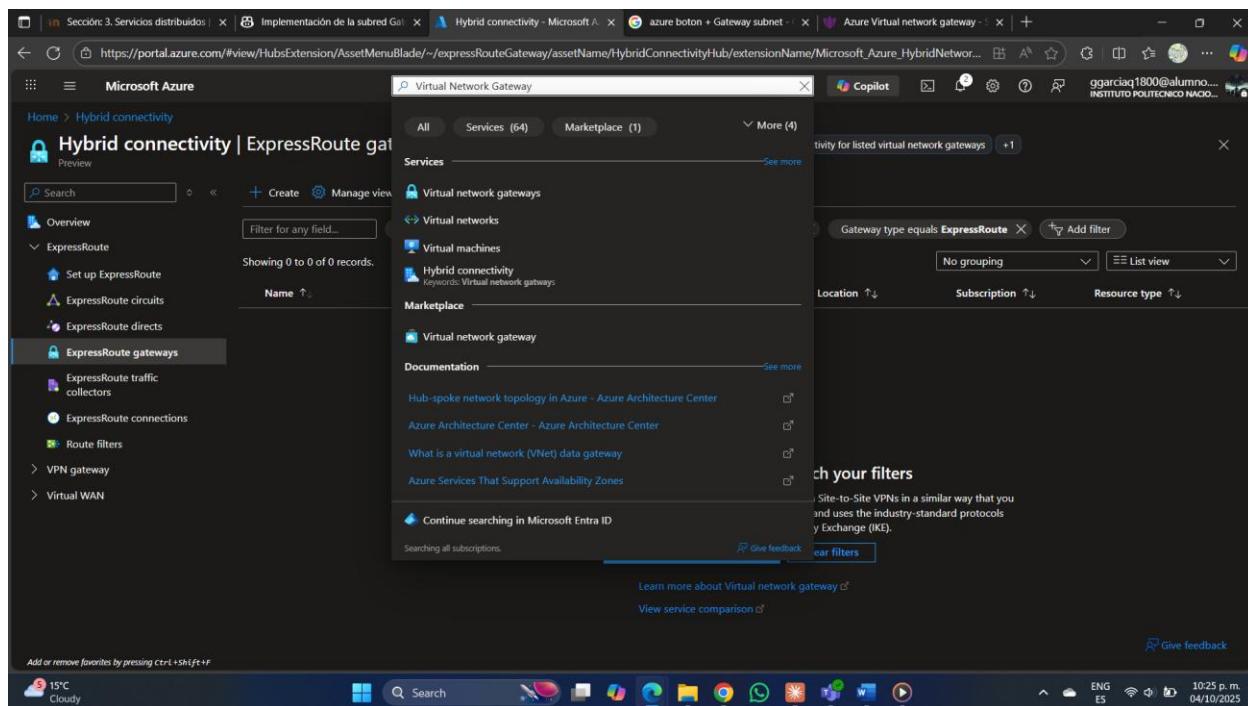


IMAGEN 14a: Selección de Virtual Network Gateway en el Marketplace

Paso 4: En la pestaña **Basics**, configurar los siguientes campos:

Project details:

- **Subscription:** Azure for Students
- **Resource group:** Hacer clic en "Create new" y crear T3-2022630278-rg-gateway-1 O seleccionar T3-2022630278-rg-1 (reutilizar el RG existente)

Instance details:

- **Name:** T3-2022630278-gateway-1
- **Region:** Seleccionar la misma región de vnet-1

- **Gateway type:** **VPN** (no ExpressRoute)
- **VPN type:** **Route-based** (requerido para VNet-to-VNet y configuraciones flexibles)
- **SKU:**
 - Para ambiente de producción: **VpnGw1** (throughput hasta 650 Mbps, 30 túneles)
 - Para laboratorio académico: **Basic** (throughput hasta 100 Mbps, 10 túneles, menor costo)
 - **Nota:** El SKU no puede cambiarse posteriormente sin eliminar y recrear el gateway
- Generation: Generation1
- **Virtual network:** Hacer clic en el selector y elegir T3-2022630278-vnet-1

Public IP address:

- **Public IP address:** Create new (dejar marcado)
- **Public IP address name:** Cambiar a T3-2022630278-ip-1
- **Public IP address SKU:** **Standard** (auto-seleccionado si el gateway SKU es VpnGw1+)
- **Assignment:** **Static** (no modificable con SKU Standard)
- **Enable active-active mode:** **Disabled** (para topología simple sin redundancia)
- **Configure BGP:** **Disabled** (no necesario para VNet-to-VNet básico)

Paso 5: Hacer clic en Review + créate

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#create/Microsoft.VirtualNetworkGateway>. The page title is "Create virtual network gateway". The "Basics" tab is selected. The "Project details" section shows a subscription "Azure for Students" and a resource group "T3-2022630278-rg-1". The "Instance details" section includes fields for "Name" (T3-2022630278-gateway-1), "Region" (East US), "Gateway type" (VPN), "SKU" (VpnGw2AZ), and "Generation" (Generation2). The "Enable Advanced Connectivity" option is set to "Enabled". At the bottom, there are "Review + create", "Previous", "Next : Tags >", and "Download a template for automation" buttons.

This screenshot is identical to the one above, showing the "Create virtual network gateway" wizard in the Microsoft Azure portal. The "Basics" tab is selected, and the configuration for the virtual network gateway is the same as in the first screenshot.

IMAGEN 14b: Configuración completa del primer Virtual Network Gateway (parte 1 - Basics)

Continuación del formulario mostrando las opciones de active-active mode y BGP (ambas disabled). Esta captura complementa la anterior para documentar todas las configuraciones.

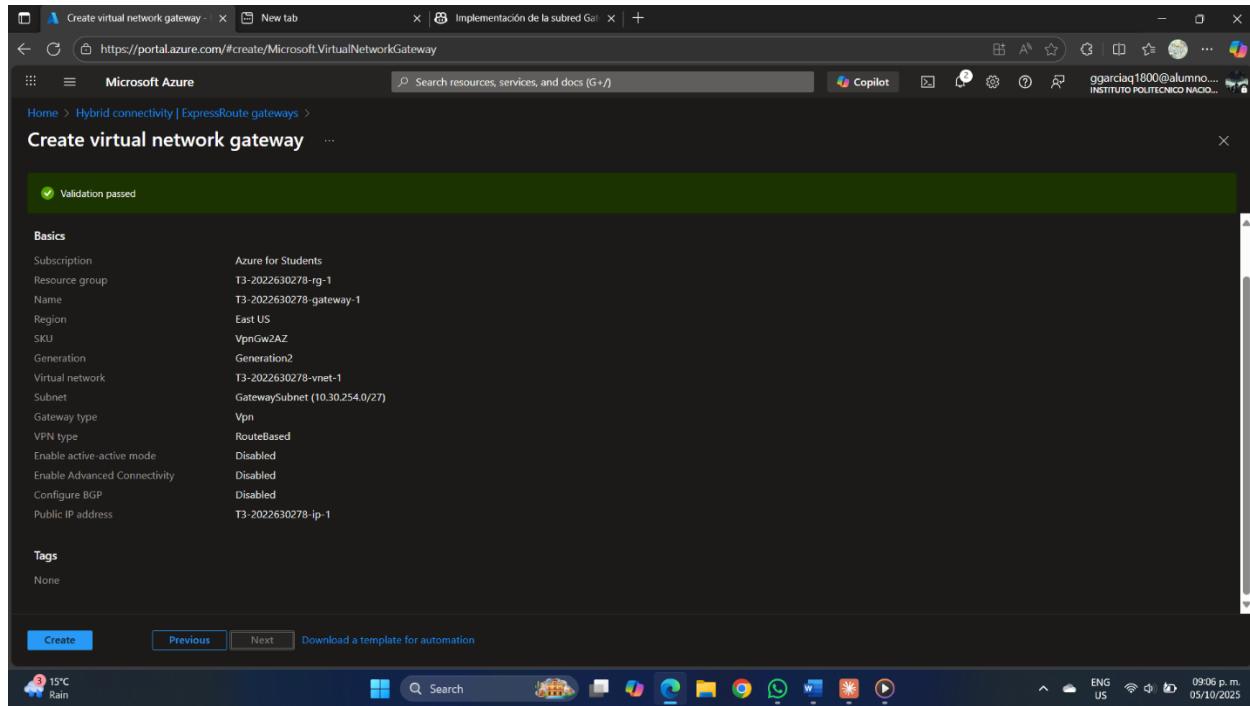


IMAGEN 14c: Configuración completa del primer Virtual Network Gateway (parte 2 - Opciones avanzadas)

Paso 7: Hacer clic en **Create** para iniciar el despliegue

Página de validación "Review + create" mostrando el resumen de la configuración con el mensaje "Validation passed" en la parte superior. Debe incluir el costo estimado mensual del gateway según el SKU seleccionado. El botón "Create" debe estar visible en la parte inferior.

Paso 8: Azure iniciará el despliegue y mostrará la página "Deployment is in progress".
Este proceso tomará entre 30-45 minutos.

Durante este tiempo, Azure está:

- Aprovisionando infraestructura de red dedicada
- Configurando el plano de control del gateway
- Estableciendo la conectividad con la GatewaySubnet

- Asociando la IP pública
- Configurando tablas de enrutamiento internas

Página "Deployment is in progress" mostrando el progreso del despliegue. Debe incluir: el nombre del despliegue, el timestamp de inicio, una barra de progreso o spinner, y la lista de recursos siendo desplegados (debe aparecer "Microsoft.Network/virtualNetworkGateways" con estado "Running" o similar). Esta captura documenta que el proceso inició correctamente.

IMAGEN 15a: Despliegue de T3-2022630278-gateway-1 en progreso (iniciando)

Después verificar el panel Overview del gateway creado

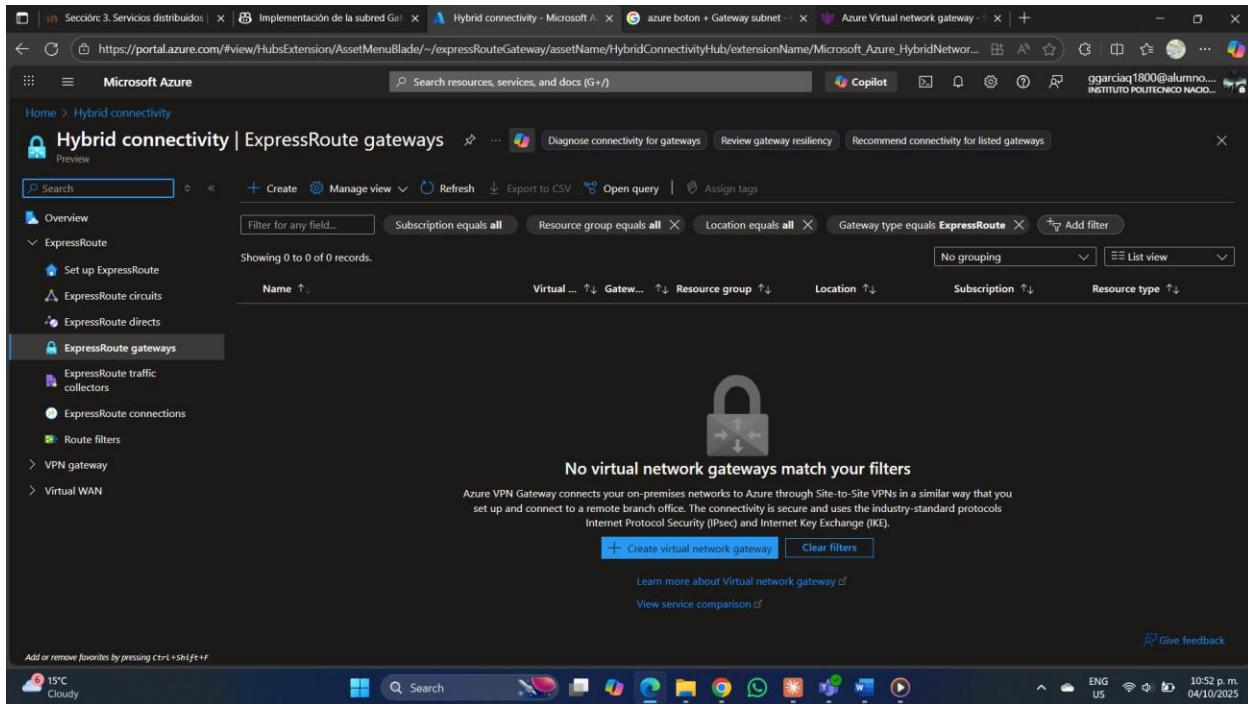
- Status: **Succeeded** (indicador verde)
- Provisioning state: **Succeeded**
- Gateway type: VPN
- VPN type: Route-based
- Virtual network: T3-2022630278-vnet-1
- Public IP address: La dirección IP pública asignada (ejemplo: 20.x.x.x)
- SKU: El SKU seleccionado (Basic o VpnGw1)
- Location: La región del gateway

La sección "Connections" debe mostrar "0" ya que aún no se han configurado conexiones. Esta captura confirma que el gateway está operacional y listo para configurar conexiones.

5.6.2 Crear el segundo Virtual Network Gateway (T3-2022630278-gateway-2)

Repetir el proceso anterior con los siguientes parámetros específicos:

Paso 1-3: Navegar a Create a resource > Virtual Network Gateway > Create



Paso 4: Configurar el formulario Basics:

Project details:

- **Subscription:** Azure for Students
- **Resource group:** T3-2022630278-rg-2 (o el RG correspondiente a la segunda región)

Instance details:

- **Name:** T3-2022630278-gateway-2
- **Region:** Seleccionar la **misma región de vnet-2** (ejemplo: West US)
- Gateway type: VPN
- VPN type: Route-based
- **SKU: El mismo SKU usado para gateway-1** (consistencia en la configuración)
- Generation: Generation1
- **Virtual network:** T3-2022630278-vnet-2

Public IP address:

- Public IP address name: T3-2022630278-ip-2

- Enable active-active mode: Disabled
- Configure BGP: Disabled

Create virtual network gateway

Enable Advanced Connectivity Enabled Disabled

Virtual network T3-2022630278-vnet-2

Subnet GatewaySubnet (10.40.254.0/27)

Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address Create new Use existing T3-2022630278-ip-2 (172.179.74.101)

Choose public IP address Enabled Disabled

Enable active-active mode Enabled Disabled

Configure BGP Enabled Disabled

Authentication Information (Preview)

Enable Key Vault Access Enabled Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription Azure for Students Azure Government Microsoft Cloud for US Government Microsoft Cloud for Healthcare

Resource group T3-2022630278-rg-2 (derived from virtual network's resource group)

Instance details

Name

Region West US 2 Deploy to an Azure Extended Zone

Gateway type VPN ExpressRoute

SKU VpnGw2AZ VpnGw2BZ

Generation Generation2 Generation3

Enable Advanced Connectivity Enabled Disabled

[Review + create](#) [Previous](#) [Next : Tags >](#) [Download a template for automation](#)

IMAGEN 17a: Configuración completa del segundo Virtual Network Gateway (T3-2022630278-gateway-2)

Paso 5: Hacer clic en **Review + create** y verificar el resumen

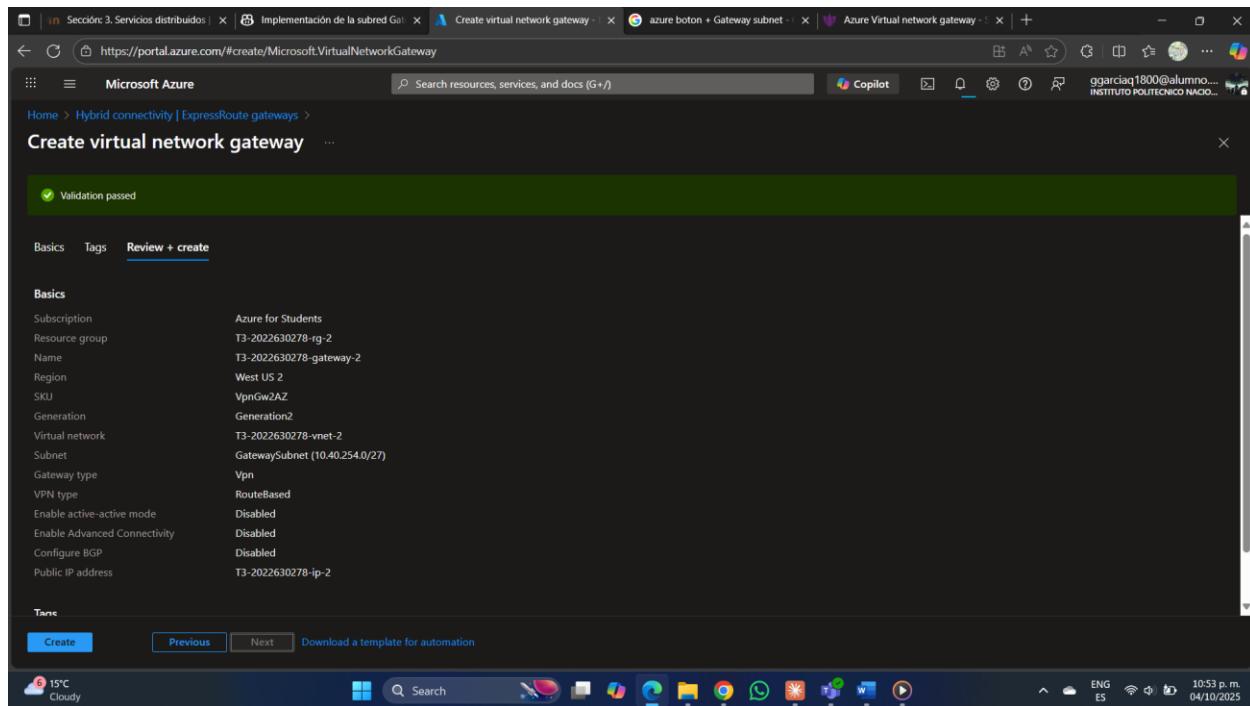


IMAGEN 17b: Resumen de validación antes de crear T3-2022630278-gateway-2

Paso 6: Hacer clic en **Create** e iniciar el despliegue (otros 30-45 minutos de espera)

Paso 7: Esperar la completación del despliegue

Paso 8: Acceder al recurso y verificar el estado

Panel Overview de T3-2022630278-gateway-2 mostrando estado Succeeded, la configuración VPN/Route-based, la VNet asociada (vnet-2), la IP pública asignada, y el SKU. Al igual que gateway-1, las "Connections" deben mostrar "0" en este momento.

5.6.3 Verificación consolidada de ambos gateways

Una vez que ambos gateways estén en estado "Succeeded", es útil documentar una vista consolidada para confirmar que la infraestructura base está lista para configurar las conexiones.

Vista de "All resources" filtrada para mostrar solo los dos Virtual Network Gateways creados. La tabla debe incluir columnas: Name, Type, Resource group, Location, y Status. Ambos gateways deben mostrar:

- T3-2022630278-gateway-1 | Virtual network gateway | rg-1 | East US | Succeeded
- T3-2022630278-gateway-2 | Virtual network gateway | rg-2 | West US | Succeeded

Esta vista panorámica confirma que la infraestructura multi-región está completamente aprovisionada.

Name	IP address	IP version	SKU	Associated to
T2-2022630278-ip	158.23.160.73	IPv4	Standard	t2-2022630278600_x1
T3-2022630278-ip-1	135.234.145.205	IPv4	Standard	T3-2022630278-gateway-1
T3-2022630278-ip-2	172.179.74.101	IPv4	Standard	T3-2022630278-gateway-2

IMAGEN 18b: Vista consolidada de ambos Virtual Network Gateways en estado Succeeded

5.7 Creación de las Conexiones VNet-to-VNet

5.7.1 Conexión 1: Desde Gateway 1 hacia Gateway 2

Pasos detallados:

1. En el Portal de Azure, navega a **Virtual Network Gateways**
2. Selecciona el gateway T3-2022630278-gateway-1
3. En el menú lateral izquierdo, busca la sección **Settings** y haz clic en **Connections**
4. En la parte superior, haz clic en el botón **+ Add o + Create**

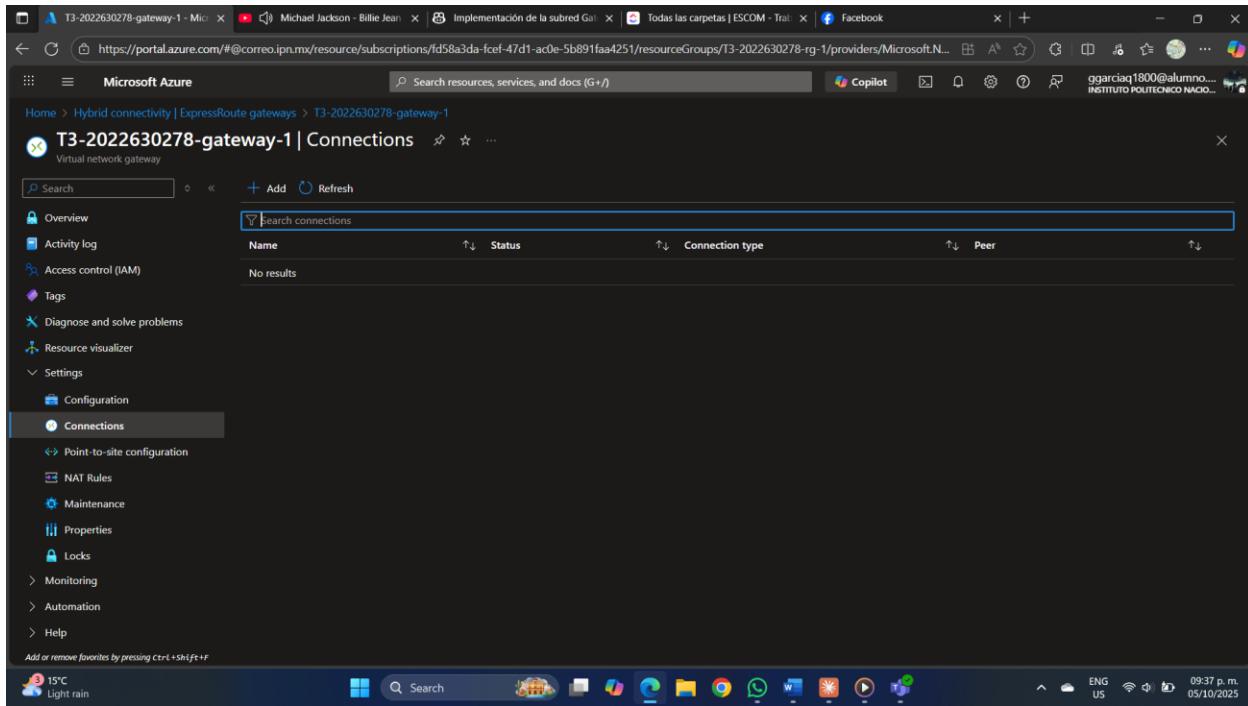


IMAGEN 19: Captura del panel de Connections vacío con el botón "+ Add" visible

5. En la pantalla de configuración de la nueva conexión, completa los siguientes campos:

- Basics:
 - **Name:** T3-2022630278-conexion-1
 - **Connection type:** Selecciona **VNet-to-VNet** del menú desplegable
 - **Region:** Se selecciona automáticamente (debe coincidir con gateway-1)
 - **First virtual network gateway:** T3-2022630278-gateway-1 (ya seleccionado)
 - **Second virtual network gateway:** Haz clic en Choose a virtual network gateway y selecciona T3-2022630278-gateway-2

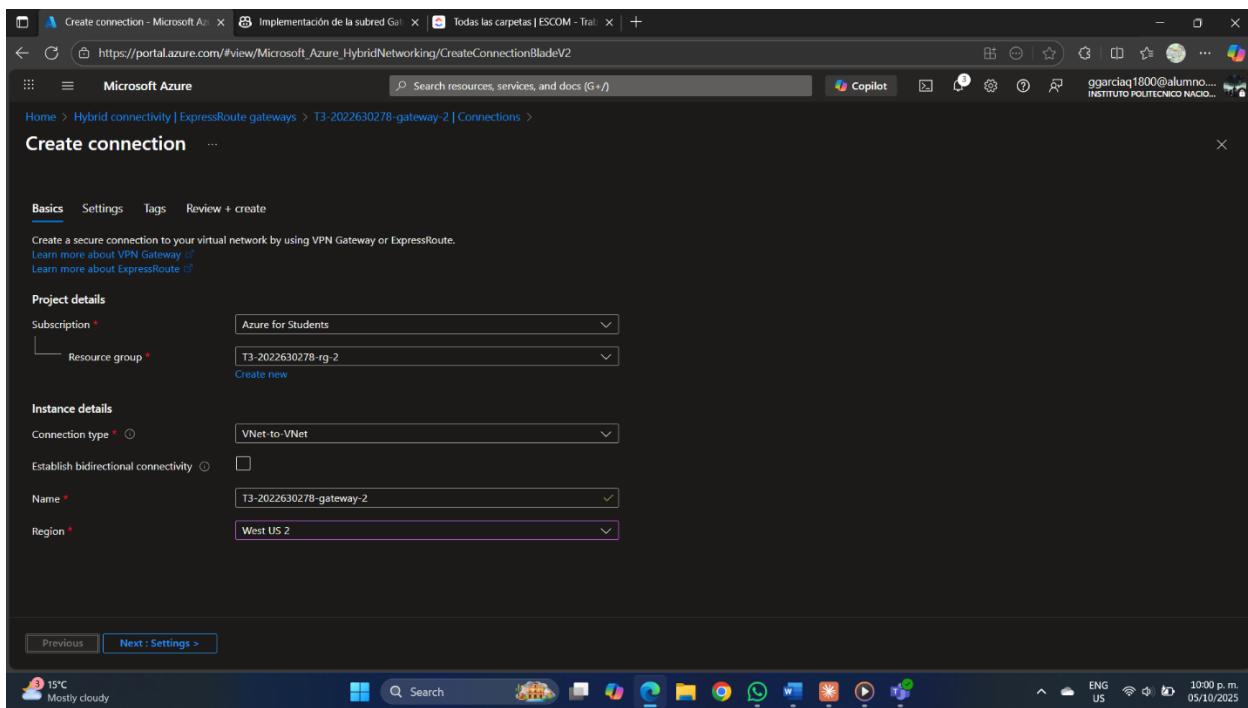


IMAGEN 20: Captura de la pestaña "Basics" con todos los campos completados, mostrando ambos gateways seleccionados

6. Haz clic en Next: Settings >
7. En la pestaña **Settings**:
 - o **Shared key (PSK)**: Ingresa una clave segura, por ejemplo: ClavePSK2022630278!
 - **Importante:** Esta clave debe ser exactamente la misma para ambas conexiones
 - o **IKE Protocol**: Déjalo en **IKEv2** (por defecto)
 - o **Use policy based traffic selectors**: Deshabilitado (por defecto)
 - o **Enable BGP**: Deshabilitado (por defecto para esta práctica)

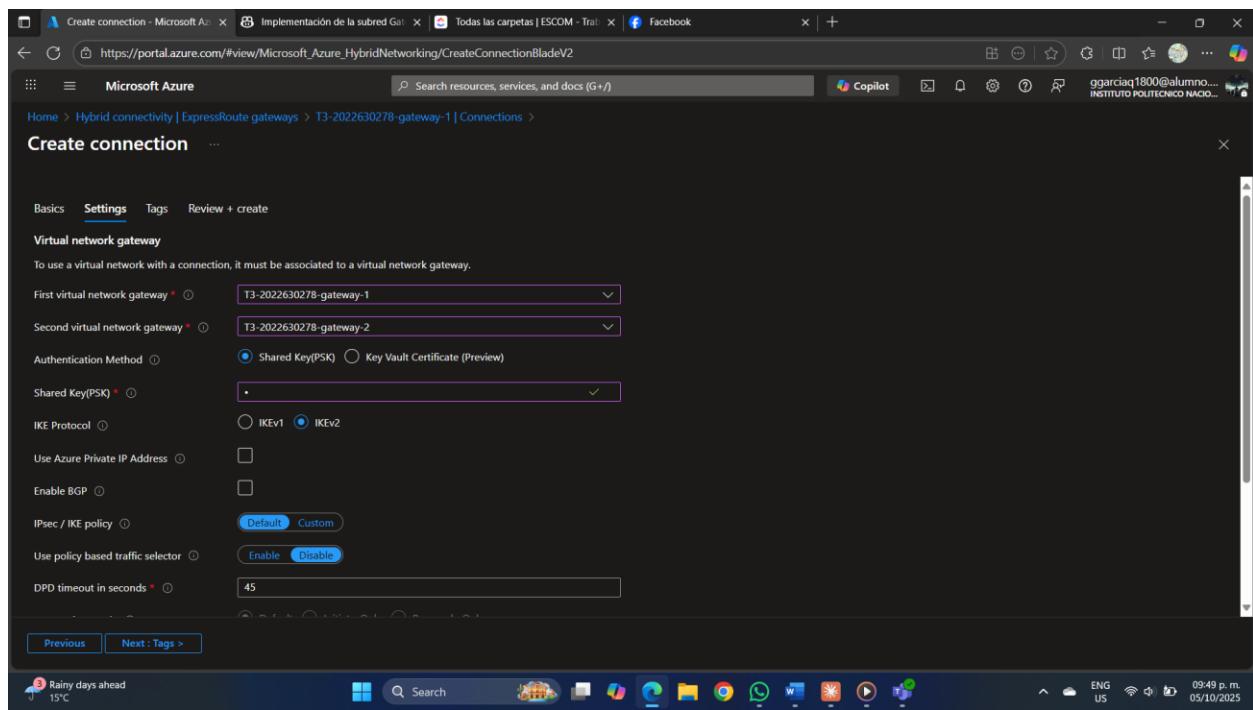


IMAGEN 21: Captura de la pestaña "Settings" mostrando el campo Shared Key completado (puede pixelar parcialmente la clave por seguridad, pero debe ser visible que está completada)

8. Haz clic en **Next: Tags >**
9. Haz clic en **Review + create**
10. Revisa que toda la configuración sea correcta y haz clic en **Create**

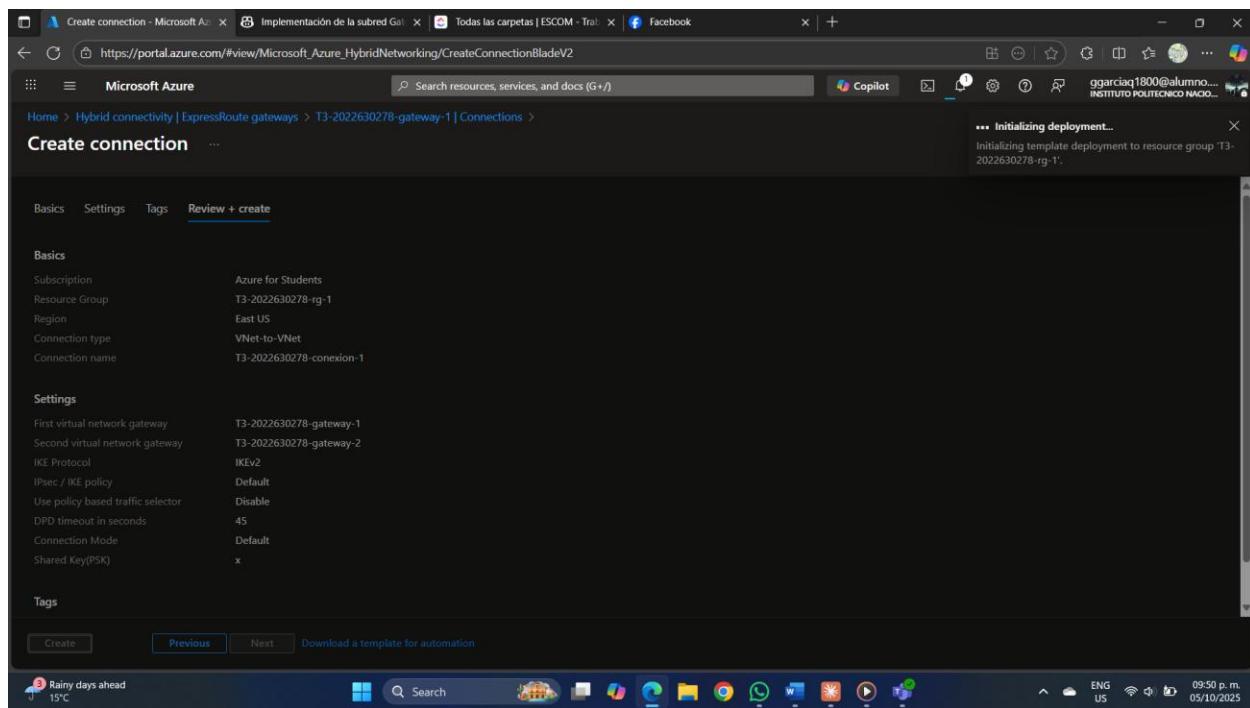


IMAGEN 22: Captura de la pantalla "Review + create" mostrando el resumen de la configuración antes de crear

11. Espera a que se complete el despliegue (puede tardar 1-2 minutos)

5.7.2 Conexión 2: Desde Gateway 2 hacia Gateway 1

Pasos detallados:

12. Ahora navega al segundo gateway: T3-2022630278-gateway-2

13. Repite los pasos del 3 al 10, pero con los siguientes valores:

- **Name:** T3-2022630278-conexion-2
- Connection type: VNet-to-VNet
- **First virtual network gateway:** T3-2022630278-gateway-2 (ya seleccionado)
- Second virtual network gateway: T3-2022630278-gateway-1
- **Shared key (PSK):** ClavePSK2022630278! (LA MISMA CLAVE exacta)

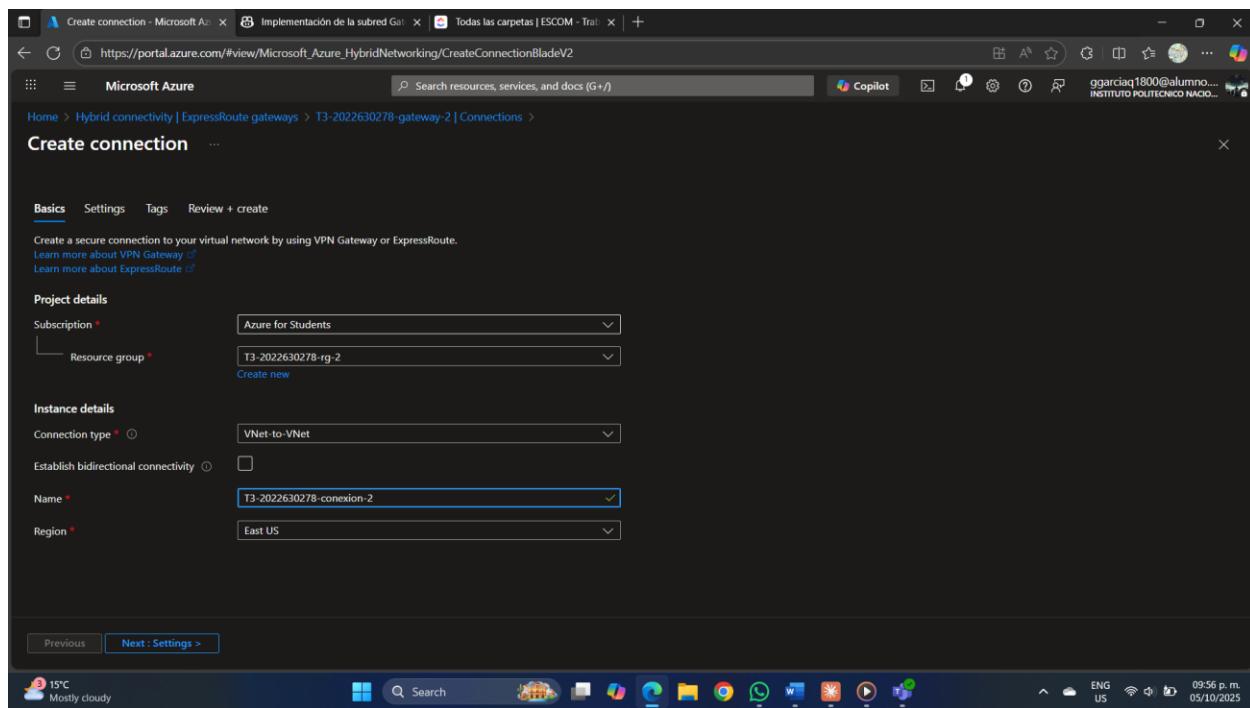


IMAGEN 23: Captura de la configuración de T3-2022630278-conexion-2 en la pestaña "Basics"

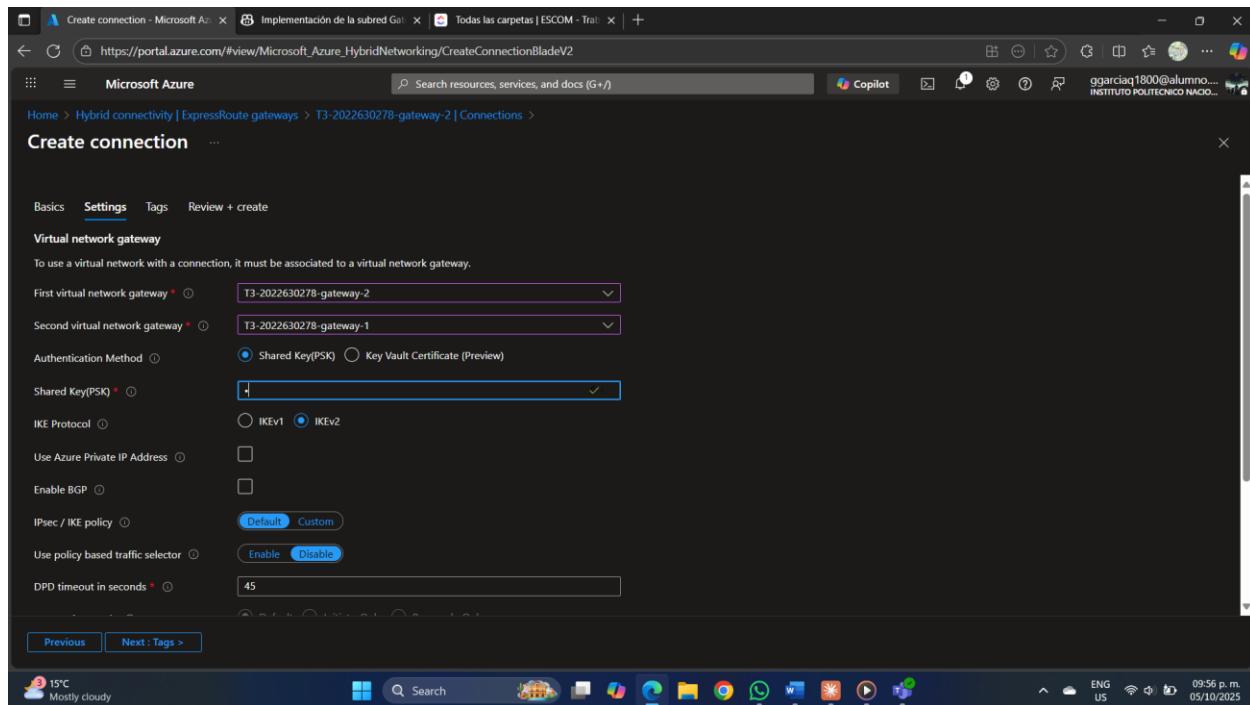


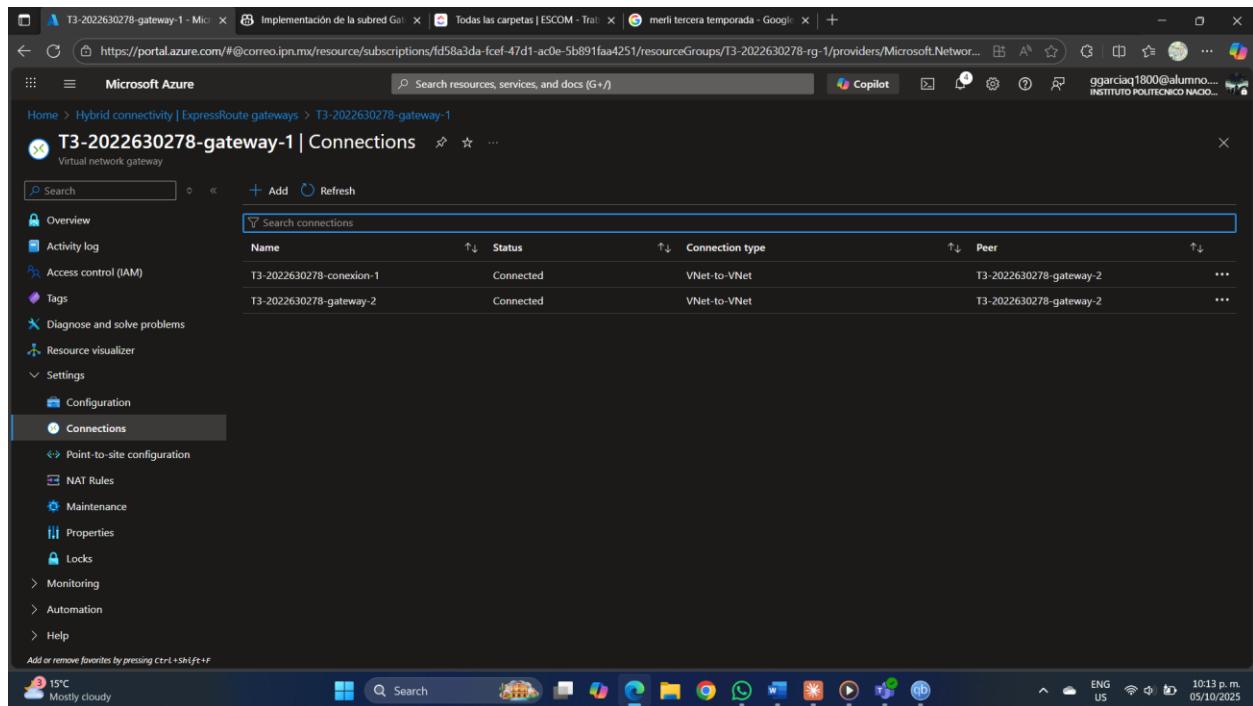
IMAGEN 24: Captura de la configuración de T3-2022630278-conexion-2 en la pestaña "Settings" con la misma PSK

Verificación del Estado de las Conexiones

14. Una vez creadas ambas conexiones, espera aproximadamente **5-10 minutos** para que el túnel IPsec se establezca completamente

15. Verifica el estado de la conexión 1:

- Ve a T3-2022630278-gateway-1 > **Connections**
- Observa que T3-2022630278-conexion-1 debe mostrar **Status: Connected**



Name	Status	Connection type	Peer
T3-2022630278-conexion-1	Connected	VNet-to-VNet	T3-2022630278-gateway-2
T3-2022630278-gateway-2	Connected	VNet-to-VNet	T3-2022630278-gateway-2

IMAGEN 25: Captura del panel de Connections del gateway-1 mostrando la conexión-1 en estado "Connected" (fondo verde)

16. Verifica el estado de la conexión 2:

- Ve a T3-2022630278-gateway-2 > **Connections**
- Observa que T3-2022630278-conexion-2 debe mostrar **Status: Connected**

The screenshot shows the Microsoft Azure portal interface. The main title is "T3-2022630278-gateway-2 | Connections". The left sidebar has a tree view with "Virtual network gateway" selected, followed by "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Resource visualizer", "Settings", "Configuration", and "Connections" (which is currently selected). Under "Connections", there are links for "Point-to-site configuration", "NAT Rules", "Maintenance", "Properties", "Locks", "Monitoring", "Automation", and "Help". The status bar at the bottom shows the weather as "15°C Mostly cloudy", the system tray with icons like battery, signal, and volume, and the date and time as "10:13 p.m. 05/10/2025".

Name	Status	Connection type	Peer
T3-2022630278-conexion-1	Connected	VNet-to-VNet	T3-2022630278-gateway-1
T3-2022630278-gateway-2	Connected	VNet-to-VNet	T3-2022630278-gateway-1

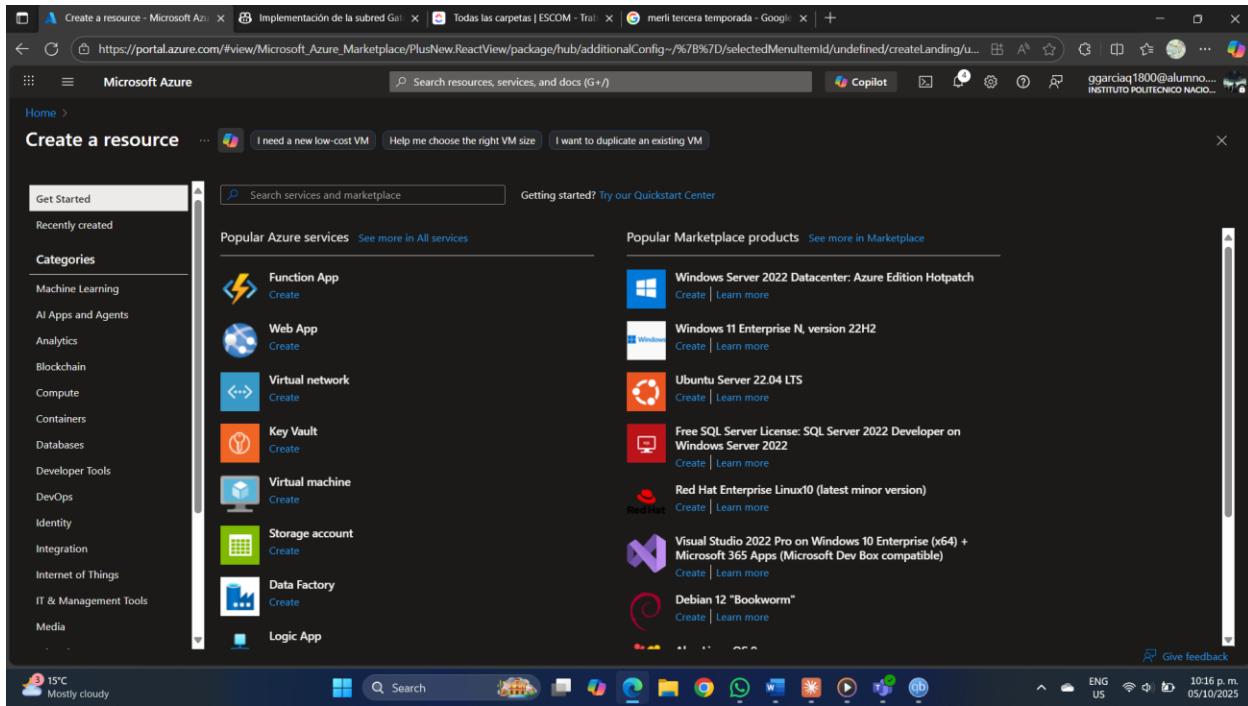
IMAGEN 26: Captura del panel de Connections del gateway-2 mostrando la conexión-2 en estado "Connected"

5.8 Creación de las Máquinas Virtuales Ubuntu

5.8.1 Máquina Virtual 1 (VM1)

Pasos detallados:

1. En el Portal de Azure, haz clic en **+ Create a resource**
2. Busca **Ubuntu Server 20.04 LTS** y selecciónalo



3. Haz clic en **Create**

Pestaña Basics:

4. Completa los siguientes campos:

- **Subscription:** Azure for Students
- **Resource group:** T3-2022630278-rg-1 (el mismo del primer VNet)
- **Virtual machine name:** T3-2022630278-1
- **Region:** La misma región que tu VNet-1 (ej. East US)
- **Availability options:** No infrastructure redundancy required
- **Security type:** Standard
- **Image:** Ubuntu Server 20.04 LTS - x64 Gen2
- **Size:** Haz clic en "See all sizes" y selecciona **Standard_B1s** (1 vCPU, 1 GiB RAM)

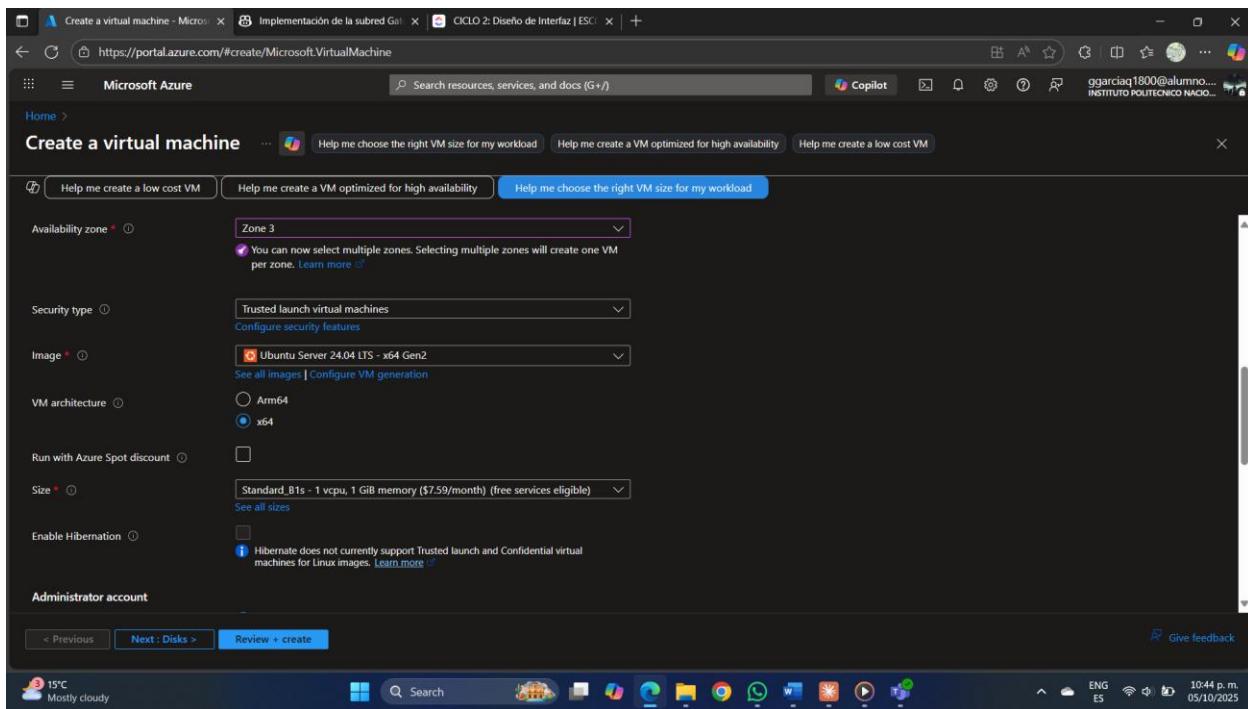
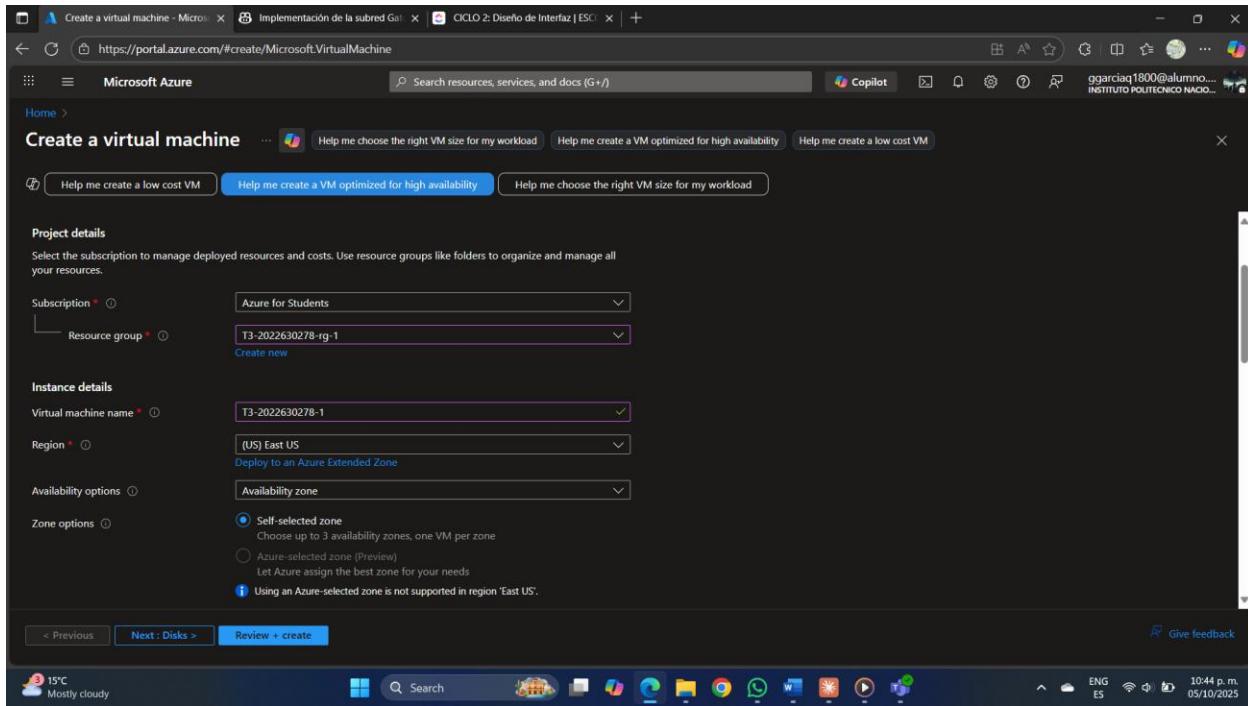


IMAGEN 28: Captura de la sección "Project details" e "Instance details" completada

Administrator account:

- **Authentication type:** SSH public key (recomendado) o Password
- **Username:** azureuser (o el que prefieras)

- Eligimos Password:
 - **Password:** (ingresa una contraseña segura)
 - **Confirm password:** (repite la contraseña)

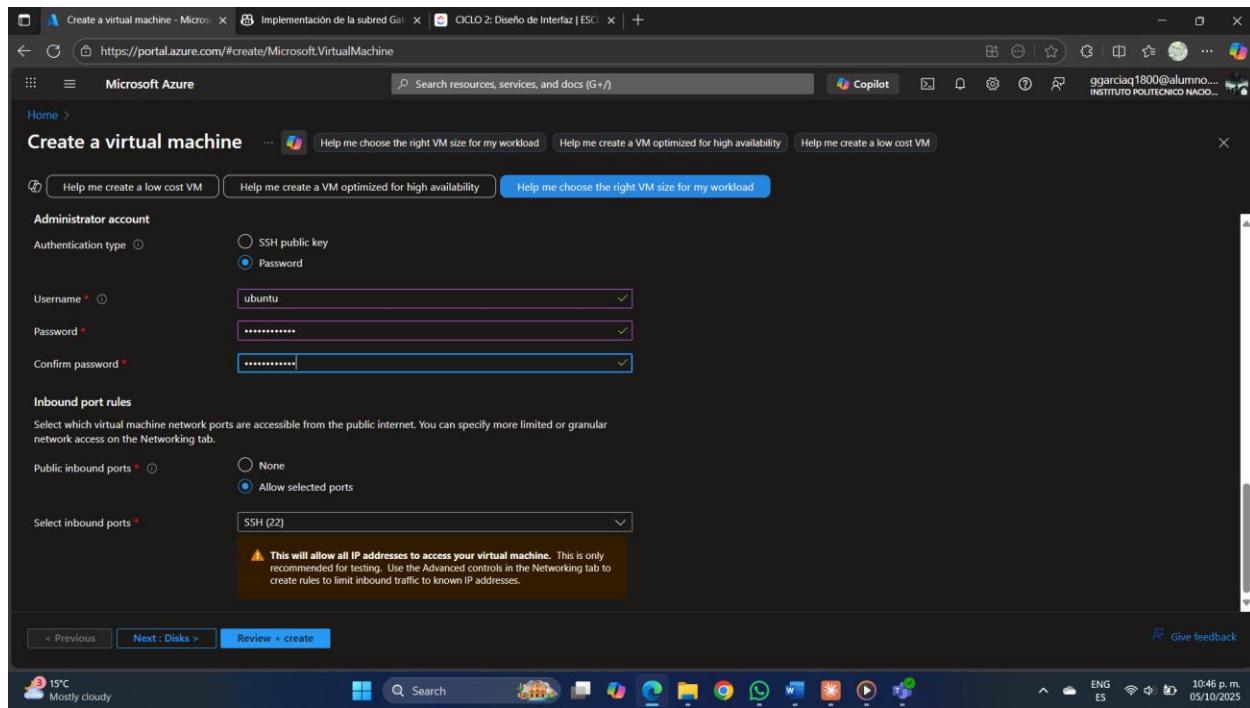


IMAGEN 29: Captura de la sección "Administrator account" completada

Inbound port rules:

- **Public inbound ports:** Allow selected ports
- Select inbound ports: Marca SSH (22)
- 5. Haz clic en Next: Disks >

Pestaña Disks:

6. Configura el disco:
 - **OS disk type:** Standard SSD (o Standard HDD para ahorrar costos)
 - **OS disk size:** 30 GiB (por defecto)
 - **Delete with VM:** Marcado (recomendado)
 - **Encryption type:** (Default) Encryption at-rest with a platform-managed key

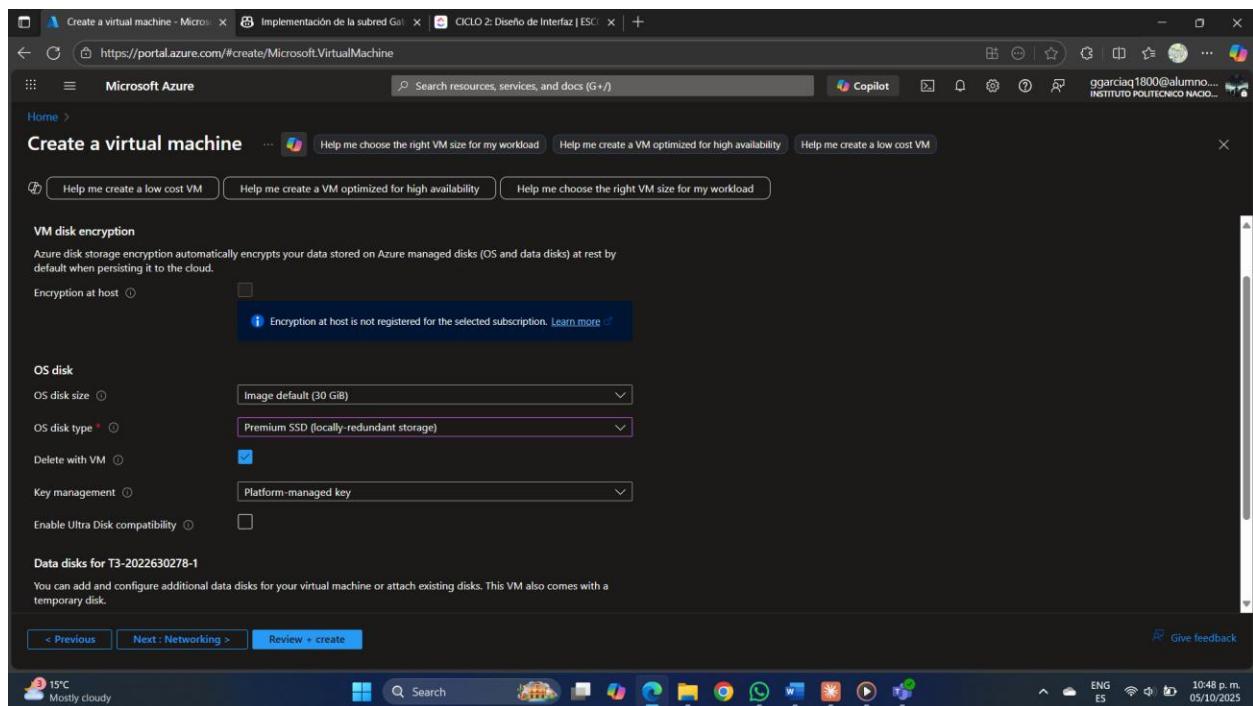


IMAGEN 31: Captura de la pestaña "Disks" con la configuración del disco

7. Haz clic en Next: Networking >

Pestaña Networking:

8. Configura la red:

- **Virtual network:** Selecciona T3-2022630278-vnet-1
- **Subnet:** default (10.30.1.0/24)
- **Public IP:** (new) T3-2022630278-1-ip (se crea automáticamente)
- NIC network security group: Basic
- **Public inbound ports:** Allow selected ports
- Select inbound ports: SSH (22)
- Delete public IP and NIC when VM is deleted: Marcado (recomendado)

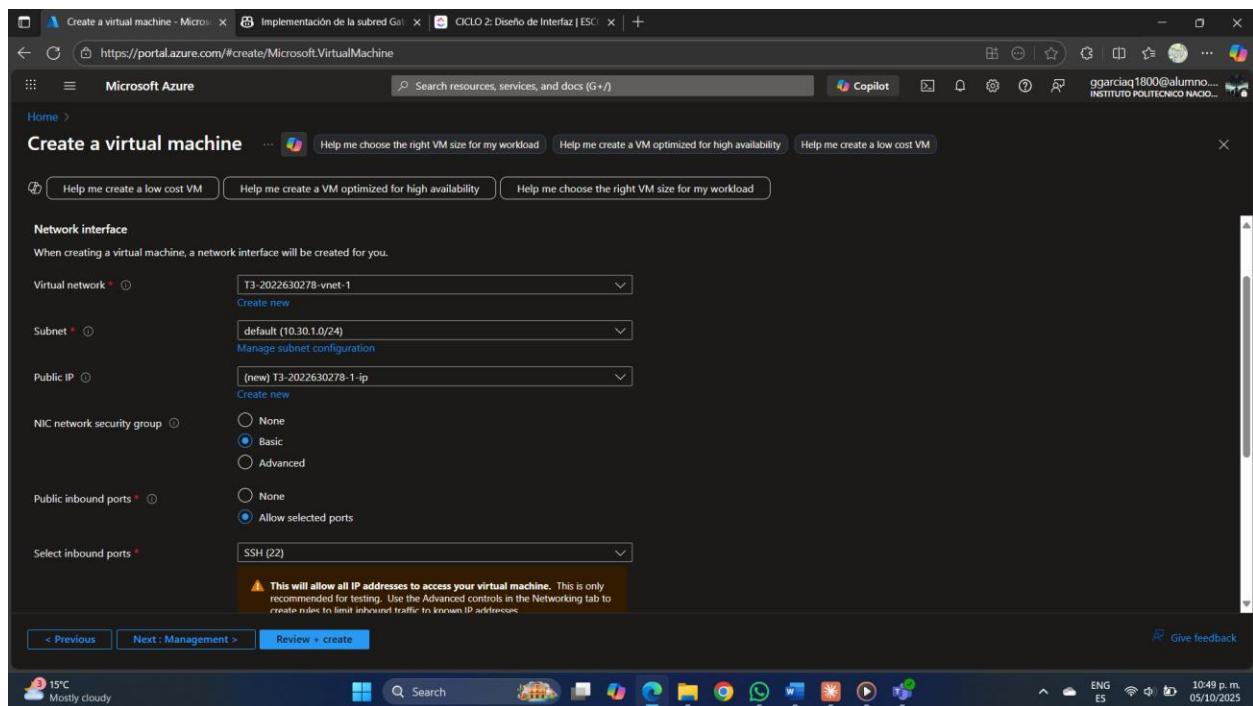


IMAGEN 32: Captura de la pestaña "Networking" mostrando la VNet y subnet correctas

9. Haz clic en **Next: Management >** (puedes dejar los valores por defecto)
10. Haz clic en **Next: Monitoring >** (puedes dejar los valores por defecto)
11. Haz clic en **Next: Advanced >** (puedes omitir esta sección)
12. Haz clic en **Review + create**

Review + create:

14. Revisa que toda la configuración sea correcta:

- Nombre: T3-2022630278-1
- Size: Standard_B1s
- VNet: T3-2022630278-vnet-1
- Subnet: default

Price

1 X Standard B1s by Microsoft **0.0104 USD/hr** Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name: GUSTAVO IVAN GARCIA QUIROZ
Preferred e-mail address: ggarciaq1800@alumno.ipn.mx

< Previous Next > Create Download a template for automation Give feedback

Validation passed

Basics

Setting	Value
Subscription	Azure for Students
Resource group	T3-2022630278-rg-1
Virtual machine name	T3-2022630278-1
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	3
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Ubuntu Server 24.04 LTS - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Authentication type	Password
Username	ubuntu

< Previous Next > Create Download a template for automation Give feedback

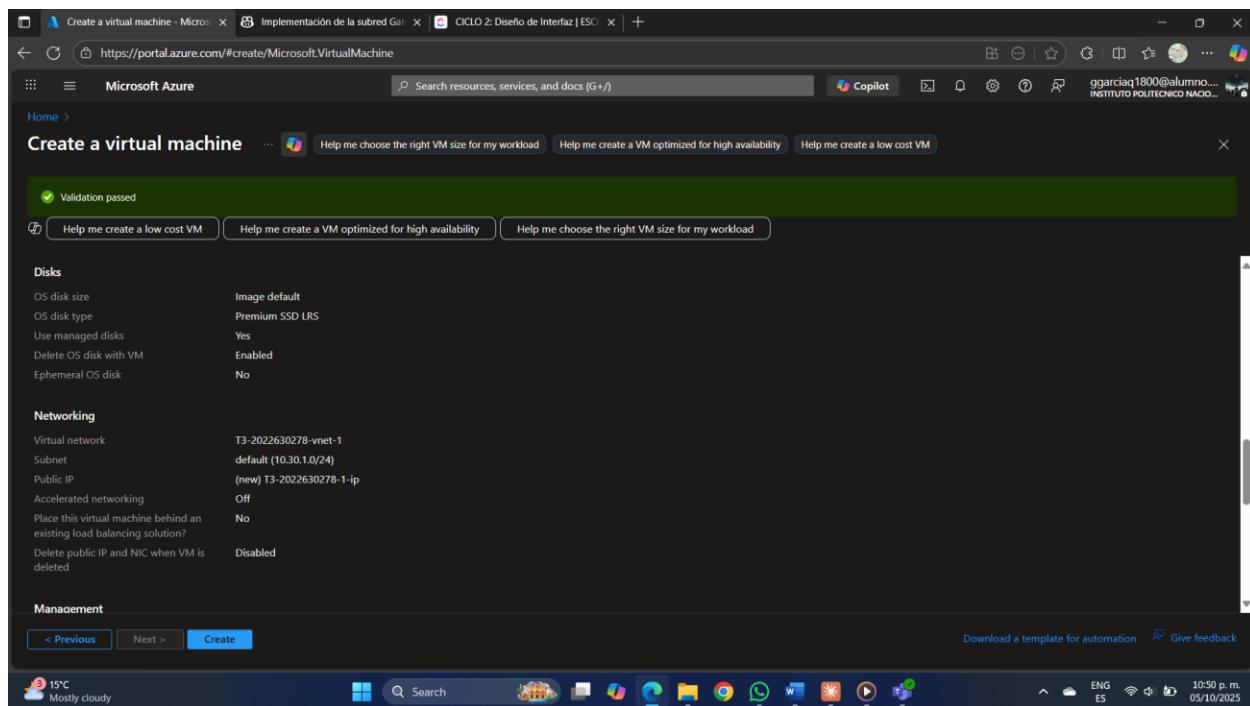


IMAGEN 33: Captura de la pantalla "Review + create" mostrando el resumen completo de la VM1

15. Haz clic en **Create**

17. Espera a que se complete el despliegue (2-3 minutos)

5.8.2 Máquina Virtual 2 (VM2)

Pasos detallados:

20. Repite todos los pasos del 1 al 19, pero con los siguientes valores diferentes:

En Basics:

- **Resource group:** T3-2022630278-rg-2
- **Virtual machine name:** T3-2022630278-2
- **Region:** La misma región que tu VNet-2 (ej. West US)
- **Username:** ubuntu

En Networking:

- **Virtual network:** T3-2022630278-vnet-2

- **Subnet:** default (10.40.1.0/24)
- **Public IP:** (new) T3-2022630278-2-ip

Price

1 X Standard B1s
by Microsoft
[Terms of use](#) [Privacy policy](#)

Subscription credits apply ⓘ
0.0104 USD/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name: GUSTAVO IVAN GARCIA QUIROZ
Preferred e-mail address: ggarciaq1800@alumno.ipn.mx

< Previous Next > Create Download a template for automation Give feedback

6 cm of rain In 2 hours 06:17 p.m. 06/10/2025

IMAGEN 36 Captura de la pestaña "Basics" de VM2 con el nombre y región correctos

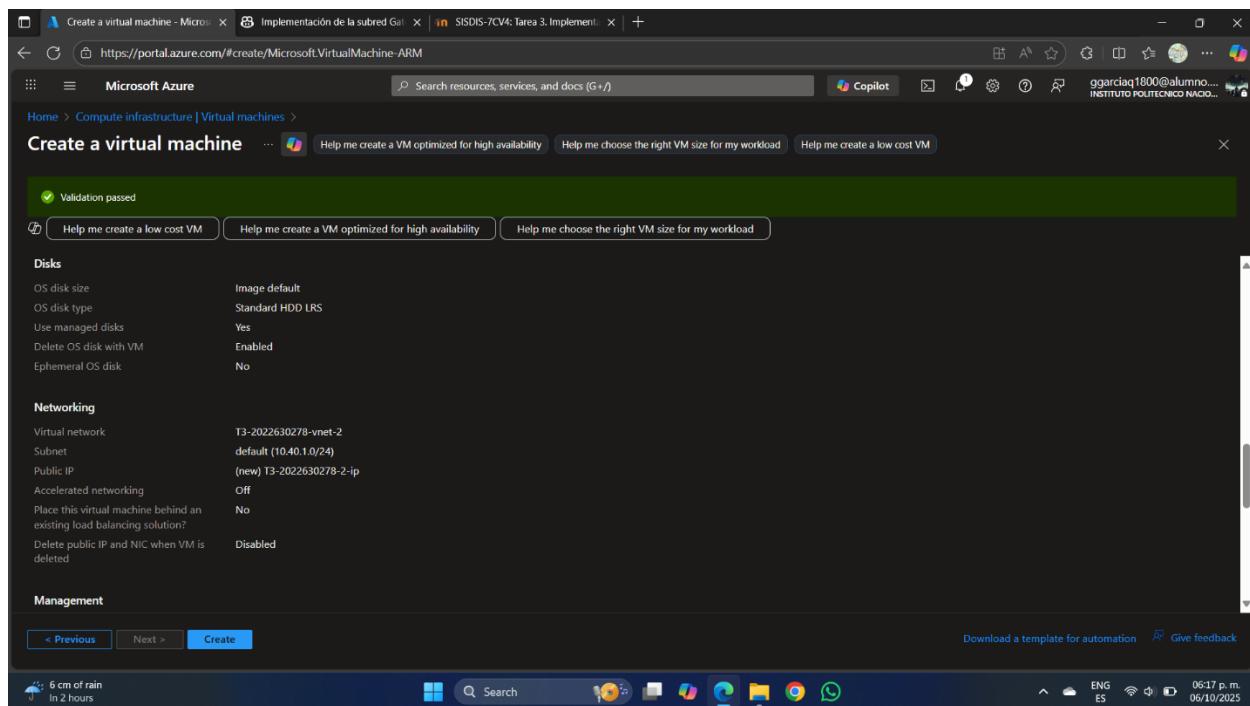


IMAGEN 37 Captura de la pestaña "Networking" de VM2 mostrando la VNet-2 y subnet correctas

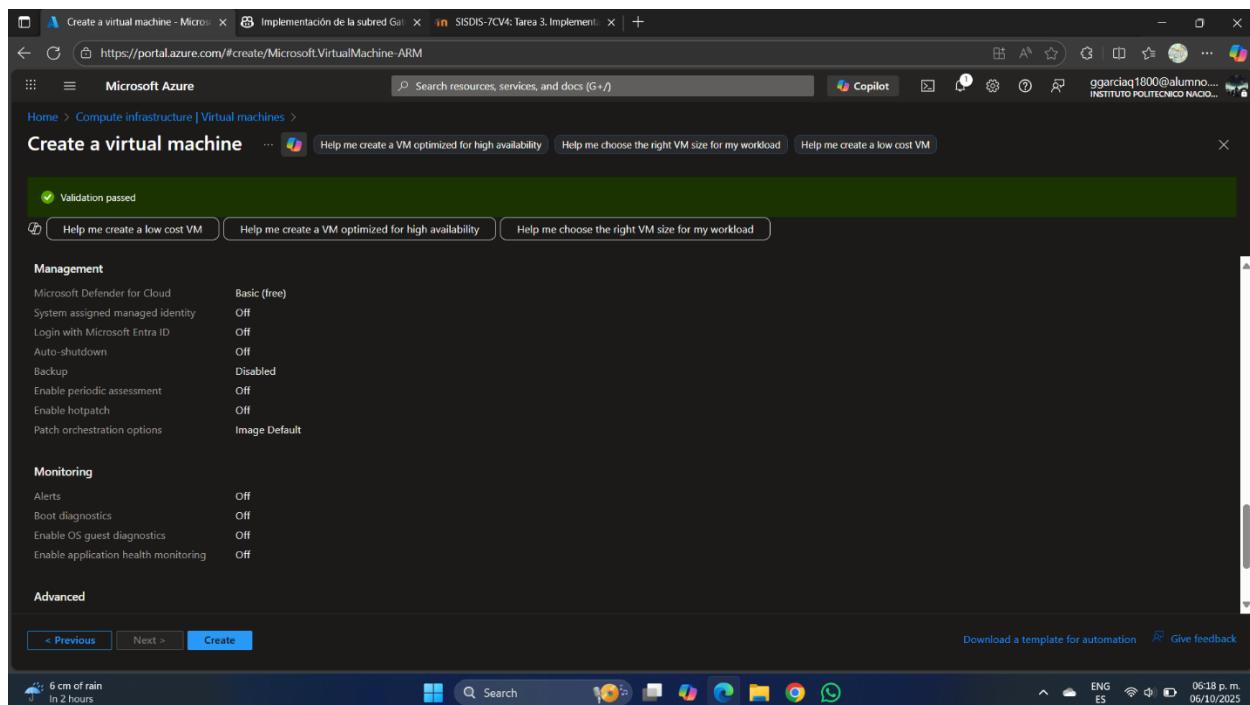


IMAGEN 38 Captura del "Review + create" de VM2

En resumen, la siguiente tabla muestra las direcciones IP que vamos a usar para realizar la comunicación entre las máquinas virtuales.

Recurso	IP Privada	VNet
T3-2022630278-1	10.30.1.4	vnet-1
T3-2022630278-2	10.40.1.4	vnet-2

Tabla 2 tabla de direcciones ip

5.9 Configuración de reglas ICMP (NSG)

Por defecto, Azure bloquea el tráfico ICMP (ping) en los Network Security Groups. Necesitamos crear reglas explícitas para permitir ICMP en ambas VMs.

Configuración en VM1:

Pasos detallados:

1. En el Portal de Azure, navega a la VM T3-2022630278-1
2. En el menú lateral izquierdo, busca la sección **Networking** y haz clic en **Network settings** o **Networking**
3. Verás la interfaz de red (NIC) y el Network Security Group (NSG) asociado
4. Haz clic en la pestaña Inbound port rules o Inbound security rules

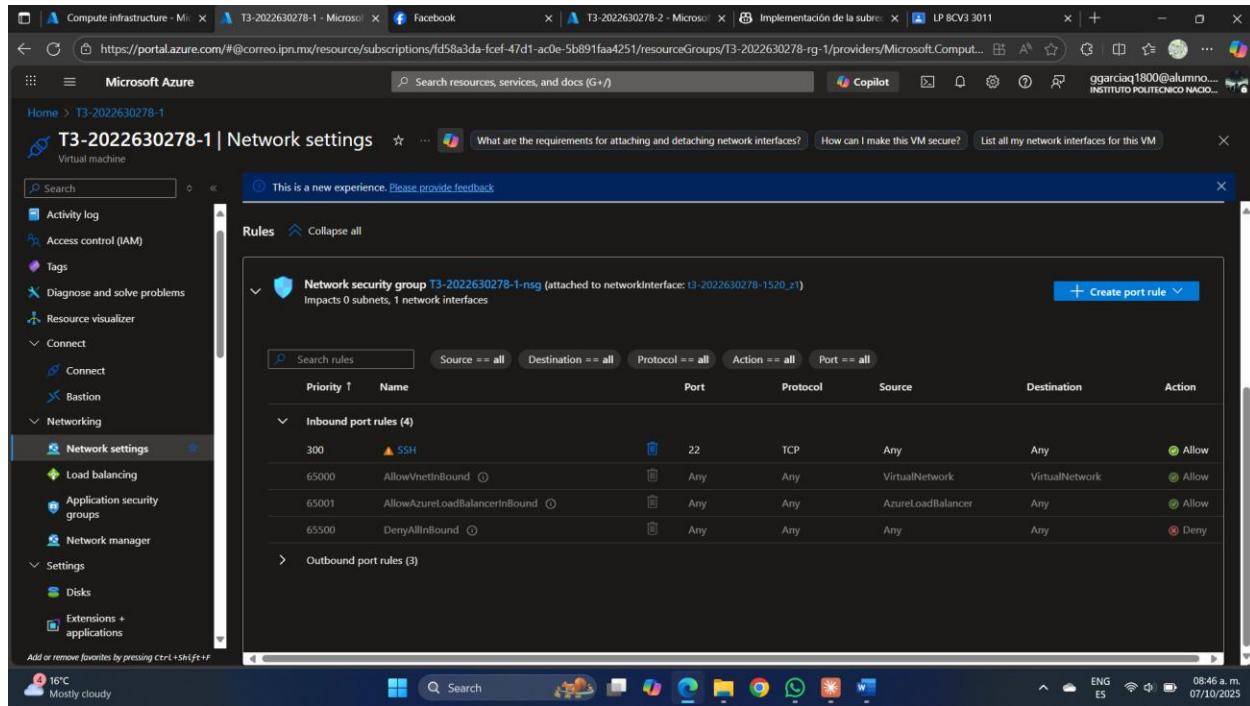


IMAGEN 40: Captura del panel de "Network settings" mostrando las reglas existentes

5. Haz clic en el botón + Add inbound port rule o + Add inbound security rule
6. En el panel lateral que se abre, configura la nueva regla:
 - Source: Any
 - Source port ranges: * (asterisco)
 - Destination: Any
 - Service: Custom
 - Destination port ranges: * (asterisco)
 - Protocol: ICMP
 - Action: Allow
 - **Priority:** 350 (debe ser menor que 65000 y no conflictuar con reglas existentes)
 - **Name:** allow-icmp
 - **Description:** (opcional) "Permitir tráfico ICMP para pruebas de conectividad"

IMAGEN 41: Captura del panel de configuración de la regla "allow-icmp" con todos los campos completados

7. Haz clic en **Add**
8. Espera unos segundos a que la regla se aplique

9. Verifica que la nueva regla allow-icmp aparezca en la lista de reglas con:

- Priority: 350
- Port: *
- Protocol: ICMP
- **Action: Allow ✓**

The screenshot shows the Azure portal interface for a virtual machine named T3-2022630278-1. The left sidebar navigation is expanded to show 'Compute infrastructure' and 'Virtual machines'. Under 'Virtual machines', the specific VM is selected. The main content area is titled 'Network settings'. On the left, there's a 'Rules' section with a 'Collapse all' button. Below it, a shield icon indicates a 'Network security group T3-2022630278-1-nsg' attached to the network interface. A 'Create port rule' button is available. The 'Inbound port rules' table lists five entries:

Priority ↑	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	allow-icmp	Any	ICMP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

IMAGEN 42: Captura de la lista de "Inbound security rules" mostrando la nueva regla "allow-icmp" aplicada y activa

Configuración en VM2:

Pasos detallados:

10. Repite exactamente los pasos del 1 al 9 para la VM T3-2022630278-2

11. Asegúrate de usar los mismos valores:

- Protocol: ICMP
- Action: Allow
- Priority: 350
- **Name: allow-icmp**

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
310	allow-icmp	Any	ICMP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

IMAGEN 43: Captura del panel de configuración de la regla "allow-icmp" en VM2

5.10 Verificación de conectividad (ping)

Ahora probaremos la conectividad entre las dos VMs a través del túnel VPN VNet-to-VNet usando sus IPs privadas.

Prueba 1: Ping desde VM1 hacia VM2

Pasos detallados:

1. Obtén las IPs necesarias:
 - IP pública de VM1: (de la sección 5.8, ej. 20.x.x.x)
 - IP privada de VM2: (de la sección 5.8, ej. 10.40.1.4)
2. Conexión SSH a VM1:

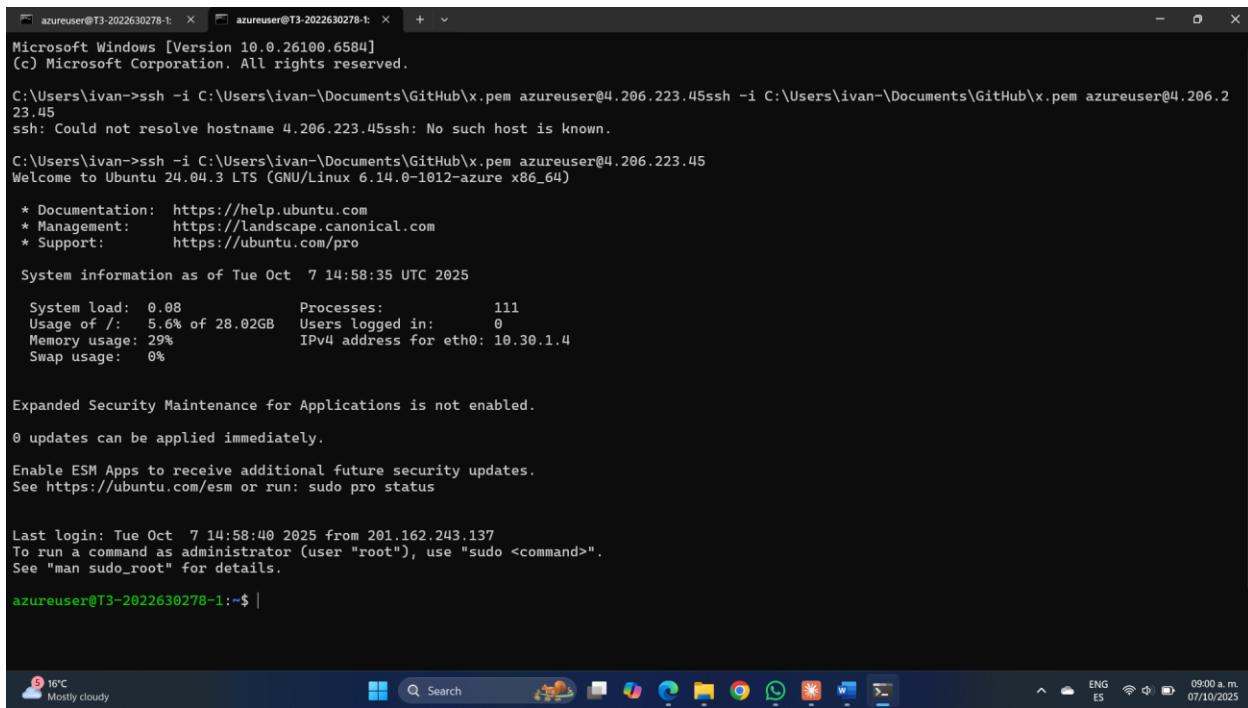
Desde Windows (PowerShell o CMD):

```
ssh -i C:\Users\ivan-\Documents\GitHub\x.pem azureuser@4.206.223.45
```

Desde Azure Cloud Shell:

- Haz clic en el ícono de Cloud Shell en la parte superior del portal

- Sube tu clave privada si es necesario
- Ejecuta el comando ssh



```

azureuser@T3-2022630278-1: ~ azureuser@T3-2022630278-1: ~ + -
Microsoft Windows [Version 10.0.26100.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ivan->ssh -i C:\Users\ivan\Documents\GitHub\x.pem azureuser@4.206.223.45ssh -i C:\Users\ivan\Documents\GitHub\x.pem azureuser@4.206.23.45
ssh: Could not resolve hostname 4.206.223.45ssh: No such host is known.

C:\Users\ivan->ssh -i C:\Users\ivan\Documents\GitHub\x.pem azureuser@4.206.223.45
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1012-azure x86_64)

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

System information as of Tue Oct 7 14:58:35 UTC 2025

System load: 0.08      Processes:           111
Usage of /: 5.6% of 28.02GB  Users logged in:     0
Memory usage: 29%          IPv4 address for eth0: 10.30.1.4
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

Last login: Tue Oct 7 14:58:40 2025 from 201.162.243.137
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@T3-2022630278-1:~$ |
```

IMAGEN 45: Captura de la terminal mostrando la conexión SSH exitosa a VM1

Ejecuta el comando ping desde VM1:

3. ping -c 4 10.40.1.4

Parámetros del comando:

- -c 4: Envía solo 4 paquetes (en lugar de infinitos)
- 10.40.1.4: IP privada de VM2

4. Observa los resultados:

Deberías ver una salida similar a:

PING 10.40.1.4 (10.40.1.4) 56(84) bytes of data.

64 bytes from 10.40.1.4: icmp_seq=1 ttl=64 time=15.2 ms

64 bytes from 10.40.1.4: icmp_seq=2 ttl=64 time=14.8 ms

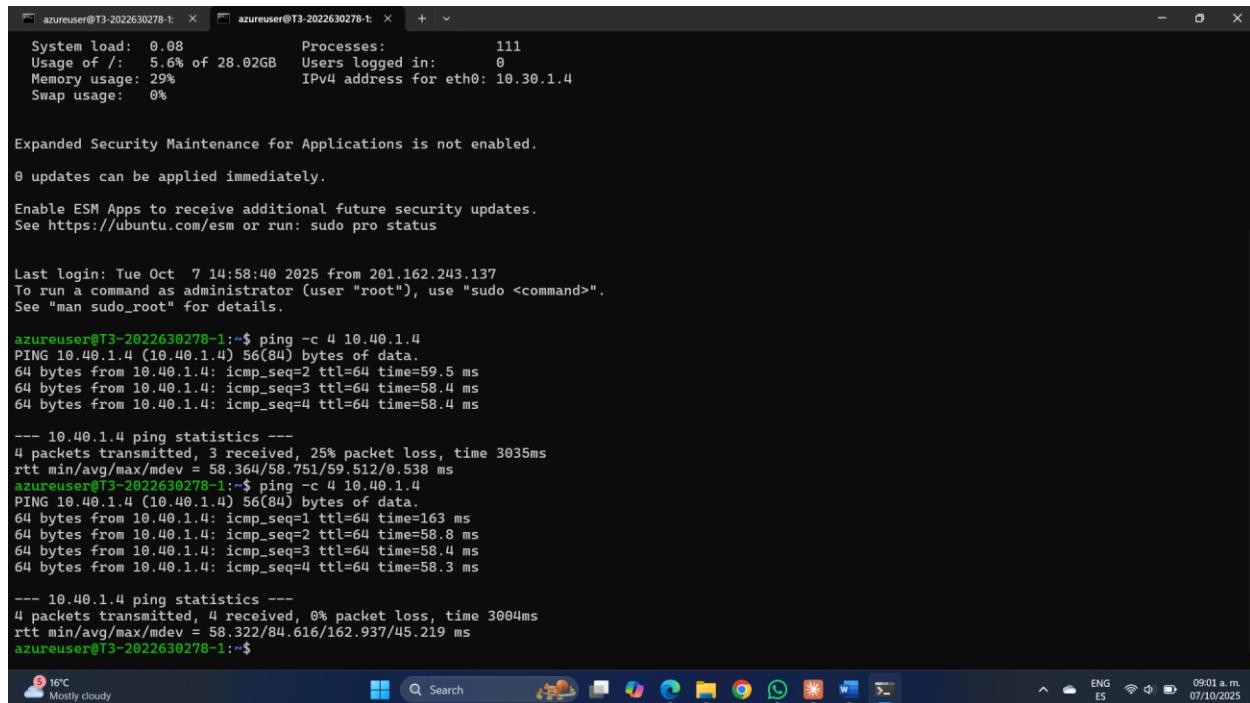
64 bytes from 10.40.1.4: icmp_seq=3 ttl=64 time=15.1 ms

64 bytes from 10.40.1.4: icmp_seq=4 ttl=64 time=14.9 ms

--- 10.40.1.4 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3005ms

rtt min/avg/max/mdev = 14.800/15.000/15.200/0.163 ms



The screenshot shows a Windows desktop environment with a terminal window open. The terminal window displays system load (0.08), usage (5.6% of 28.02GB), memory (29%), swap (0%), and network information (IPv4 address for eth0: 10.30.1.4). It also shows expanded security maintenance information, last login details (Tue Oct 7 14:58:40 2025), and a ping command to 10.40.1.4. The ping results show 4 packets transmitted, 4 received, 0% packet loss, and an average round-trip time (rtt) of 14.800/15.000/15.200/0.163 ms. The desktop taskbar at the bottom includes icons for search, file explorer, and various applications.

```
System load: 0.08      Processes: 111
Usage of /: 5.6% of 28.02GB  Users logged in: 0
Memory usage: 29%          IPv4 address for eth0: 10.30.1.4
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

Last login: Tue Oct 7 14:58:40 2025 from 201.162.243.13"
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@T3-2022630278-1:~$ ping -c 4 10.40.1.4
PING 10.40.1.4 (10.40.1.4) 56(84) bytes of data.
64 bytes from 10.40.1.4: icmp_seq=1 ttl=64 time=59.5 ms
64 bytes from 10.40.1.4: icmp_seq=2 ttl=64 time=58.4 ms
64 bytes from 10.40.1.4: icmp_seq=3 ttl=64 time=58.4 ms
64 bytes from 10.40.1.4: icmp_seq=4 ttl=64 time=58.4 ms

--- 10.40.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 58.364/58.751/59.512/0.538 ms
azureuser@T3-2022630278-1:~$ ping -c 4 10.40.1.4
PING 10.40.1.4 (10.40.1.4) 56(84) bytes of data.
64 bytes from 10.40.1.4: icmp_seq=1 ttl=64 time=163 ms
64 bytes from 10.40.1.4: icmp_seq=2 ttl=64 time=58.8 ms
64 bytes from 10.40.1.4: icmp_seq=3 ttl=64 time=58.4 ms
64 bytes from 10.40.1.4: icmp_seq=4 ttl=64 time=58.3 ms

--- 10.40.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 58.322/84.616/162.937/45.219 ms
azureuser@T3-2022630278-1:~$
```

IMAGEN 46: Captura de pantalla completa mostrando el comando ping -c 4 10.40.1.4 y su salida exitosa con 0% packet loss

5. Anota los valores para tu reporte:

- Paquetes transmitidos: 4
- Paquetes recibidos: 4
- % de pérdida: 0%
- Latencia promedio (avg): (anotar el valor en ms)

Prueba 2: Ping desde VM2 hacia VM1

Pasos detallados:

6. Abre una nueva terminal o pestaña (mantén la conexión a VM1 abierta siquieres)
7. Obtén las IPs necesarias:
 - o IP pública de VM2: (de la sección 5.8)
 - o IP privada de VM1: (de la sección 5.8, ej. 10.30.1.4)
8. Conexión SSH a VM2:

```
ssh -i C:\Users\ivan-\Documents\GitHub\x(1).pem azureuser@20.3.251.126
```



The screenshot shows a Windows desktop environment with a taskbar at the bottom. On the taskbar, there are several icons: a weather icon (Rainy days ahead, 16°C), a search bar, and pinned application icons for File Explorer, Edge, and others. Two terminal windows are open in the background. The active window is titled "azureuser@T3-2022630278-2" and displays a successful SSH session to an Ubuntu 24.04.3 LTS server. The session output includes system status, security information, and a prompt for further action.

```
Reading state information... Done
All packages are up to date.
azureuser@T3-2022630278-1:~$ exit
logout
Connection to 4.206.223.45 closed.

C:\Users\ivan->ssh -i C:\Users\ivan-\Documents\GitHub\x(1).pem azureuser@20.3.251.126
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1012-azure x86_64)

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

System information as of Tue Oct  7 15:06:46 UTC 2025

System load:  0.0          Processes:           114
Usage of /:   5.7% of 28.02GB  Users logged in:     0
Memory usage: 32%          IPv4 address for eth0: 10.40.1.4
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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

Last login: Tue Oct  7 00:32:45 2025 from 148.204.1.148
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@T3-2022630278-2:~$
```

IMAGEN 47: Captura de la terminal mostrando la conexión SSH exitosa a VM2

Ejecuta el comando ping desde VM2:

```
ping -c 4 10.30.1.4
```

The screenshot shows a terminal window with two tabs open. The left tab displays system information as of Tuesday, October 7, 15:06:46 UTC 2025. It includes metrics like system load (0.0), memory usage (32%), swap usage (0%), and network details (IPv4 address 10.40.1.4). The right tab shows a successful ping command to 10.30.1.4, with four packets transmitted and no loss.

```
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

System information as of Tue Oct 7 15:06:46 UTC 2025

System load: 0.0      Processes: 114
Usage of /: 5.7% of 28.02GB  Users logged in: 0
Memory usage: 32%     IPv4 address for eth0: 10.40.1.4
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

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

Last login: Tue Oct 7 00:32:45 2025 from 148.204.1.148
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@T3-2022630278-2:~$ ping -c 4 10.30.1.4
PING 10.30.1.4 (10.30.1.4) 56(84) bytes of data.
64 bytes from 10.30.1.4: icmp_seq=1 ttl=64 time=60.5 ms
64 bytes from 10.30.1.4: icmp_seq=2 ttl=64 time=63.3 ms
64 bytes from 10.30.1.4: icmp_seq=3 ttl=64 time=58.8 ms
64 bytes from 10.30.1.4: icmp_seq=4 ttl=64 time=58.5 ms

--- 10.30.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 58.466/60.254/63.298/1.921 ms
azureuser@T3-2022630278-2:~$ |
```

IMAGEN 48: Captura de pantalla completa mostrando el comando ping -c 4 10.30.1.4 y su salida exitosa desde VM2

10. Anota los valores para tu reporte

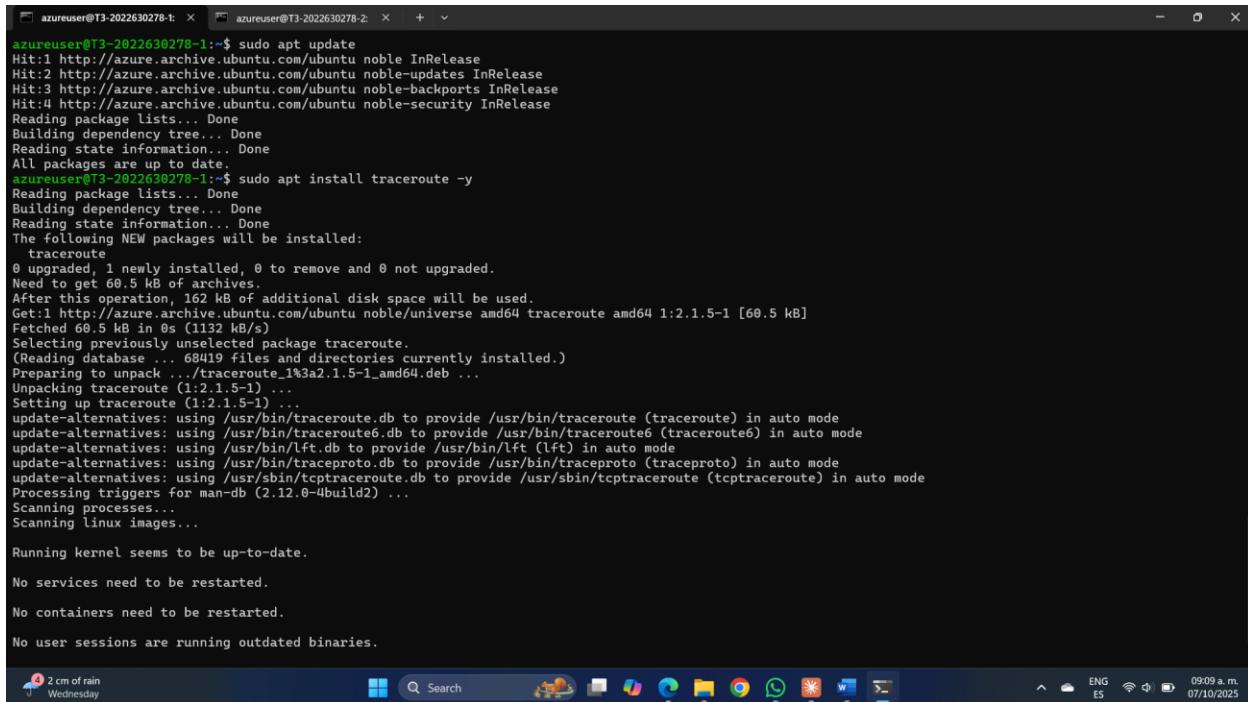
Prueba 3 (Opcional): Traceroute para visualizar el túnel

Pasos detallados:

11. Desde cualquiera de las VMs, instala traceroute:

sudo apt update

sudo apt install traceroute -y



```
azureuser@T3-2022630278-1:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
azureuser@T3-2022630278-1:~$ sudo apt install traceroute -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 60.5 kB of archives.
After this operation, 162 kB of additional disk space will be used.
Get:1 http://azure.archive.ubuntu.com/ubuntu/noble/universe amd64 traceroute amd64 1:2.1.5-1 [60.5 kB]
Fetched 60.5 kB in 0s (1132 kB/s)
Selecting previously unselected package traceroute.
(Reading database ... 68419 files and directories currently installed.)
Preparing to unpack .../traceroute_1%3a2.1.5-1_amd64.deb ...
Unpacking traceroute (1:2.1.5-1) ...
Setting up traceroute (1:2.1.5-1) ...
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute (traceroute) in auto mode
update-alternatives: using /usr/bin/traceroute6.db to provide /usr/bin/traceroute6 (traceroute6) in auto mode
update-alternatives: using /usr/bin/lft.db to provide /usr/bin/lft (lft) in auto mode
update-alternatives: using /usr/bin/traceproto.db to provide /usr/bin/traceproto (traceproto) in auto mode
update-alternatives: using /usr/sbin/tcptraceroute.db to provide /usr/sbin/tcptraceroute (tcptraceroute) in auto mode
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
```

IMAGEN 49: Captura de la instalación de traceroute

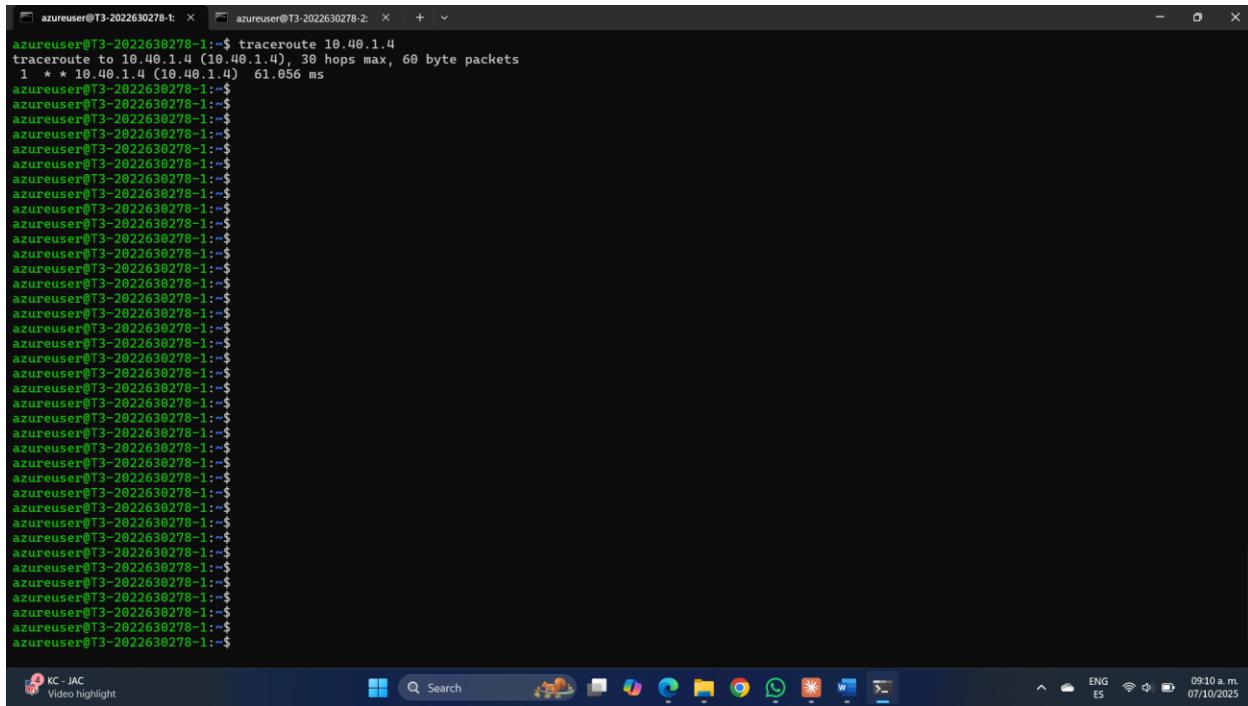
12. Ejecuta traceroute hacia la otra VM:

13. traceroute 10.40.1.4

desde VM1 hacia VM2, o viceversa

Interpretación:

- Deberías ver muy pocos saltos (1-2)
- El tráfico va directamente a través del túnel VPN
- Puede mostrar asteriscos (*) en algunos saltos debido a ICMP time-exceeded



A screenshot of a Windows desktop environment showing a terminal window titled "azureuser@T3-2022630278-1" with the command "traceroute 10.40.1.4" running. The terminal output shows the traceroute path from the VM to the destination IP 10.40.1.4, which is located at hop 1. The terminal window is part of a taskbar that includes other icons like File Explorer, Edge, and Task View. The system tray shows the date and time as 09:10 a.m. on 07/10/2025.

```
azureuser@T3-2022630278-1:~$ traceroute 10.40.1.4
traceroute to 10.40.1.4 (10.40.1.4), 30 hops max, 60 byte packets
 1 * * 10.40.1.4 (10.40.1.4)  61.056 ms
```

IMAGEN 50 Captura del comando traceroute mostrando la ruta entre las VMs

Prueba 4 (Opcional): Verificar rutas en la VM

13. Desde cualquiera de las VMs, verifica las rutas:

14. ip route

Deberías ver una ruta hacia la red remota a través del gateway local

```
azurereuser@T3-2022630278-1: ~$ ip route
default via 10.30.1.1 dev eth0 proto dhcp src 10.30.1.4 metric 100
10.30.1.0/24 dev eth0 proto kernel scope link src 10.30.1.4 metric 100
10.30.1.1 dev eth0 proto dhcp scope link src 10.30.1.4 metric 100
168.63.129.16 via 10.30.1.1 dev eth0 proto dhcp src 10.30.1.4 metric 100
169.254.169.254 via 10.30.1.1 dev eth0 proto dhcp src 10.30.1.4 metric 100
azurereuser@T3-2022630278-1: ~$
```

IMAGEN 51: (OPCIONAL) Captura del comando ip route mostrando las rutas configuradas

Origen	IP Origen	Destino	IP Destino	Paquetes enviados	Paquetes recibidos	% Pérdida
VM1	10.30.1.4	VM2	10.40.1.4	4	4	0%
VM2	10.40.1.4	VM1	10.30.1.4	4	4	0%

5.11 Visualización de topología de red

Azure Network Watcher proporciona una herramienta de visualización de topología que muestra gráficamente cómo están conectados los recursos de red.

Visualización desde VM1:

Pasos detallados:

1. En el Portal de Azure, navega a la VM T3-2022630278-1
 2. En el menú lateral izquierdo, busca la sección **Help** o **Monitoring**
 3. Haz clic en Connection troubleshoot o busca Network Watcher

4. Alternativamente, puedes ir directamente a **Network Watcher** desde el menú principal de Azure

Método más directo:

5. En el Portal de Azure, busca **Network Watcher** en la barra de búsqueda superior
6. Haz clic en **Network Watcher** en los resultados

[IMAGEN 52 - AQUÍ]: Captura del servicio Network Watcher en el portal de Azure

7. En el menú lateral de Network Watcher, en la sección **Monitoring**, haz clic en **Topology**
8. Configura los filtros:
 - **Subscription:** Tu suscripción Azure for Students
 - **Resource Group:** Selecciona T3-2022630278-rg-1
 - **Virtual Network:** Selecciona T3-2022630278-vnet-1

[IMAGEN 53 - AQUÍ]: Captura de los filtros de topología configurados para VNet-1

9. Haz clic en el ícono de actualizar o espera a que se genere la topología
10. La topología mostrará:

- La VNet T3-2022630278-vnet-1
- Las subredes (default y GatewaySubnet)
- La VM T3-2022630278-1
- El Virtual Network Gateway T3-2022630278-gateway-1
- La interfaz de red (NIC) de la VM
- El Network Security Group (NSG)
- Las conexiones entre componentes

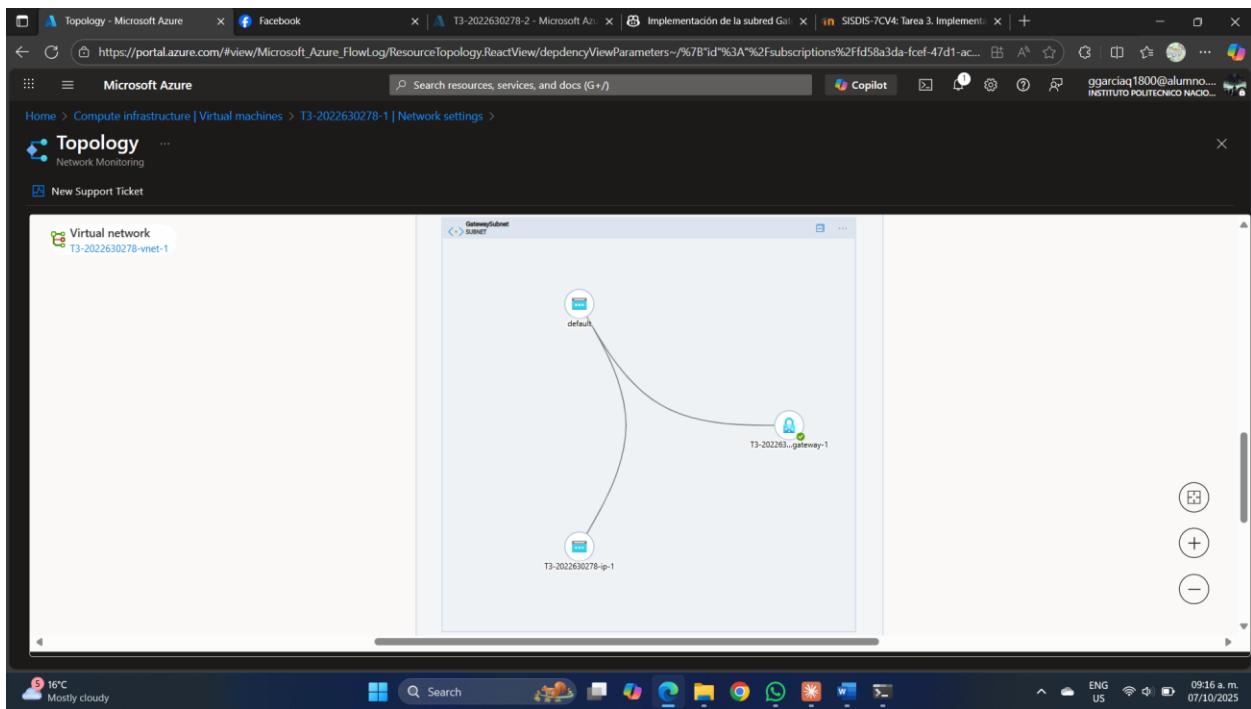
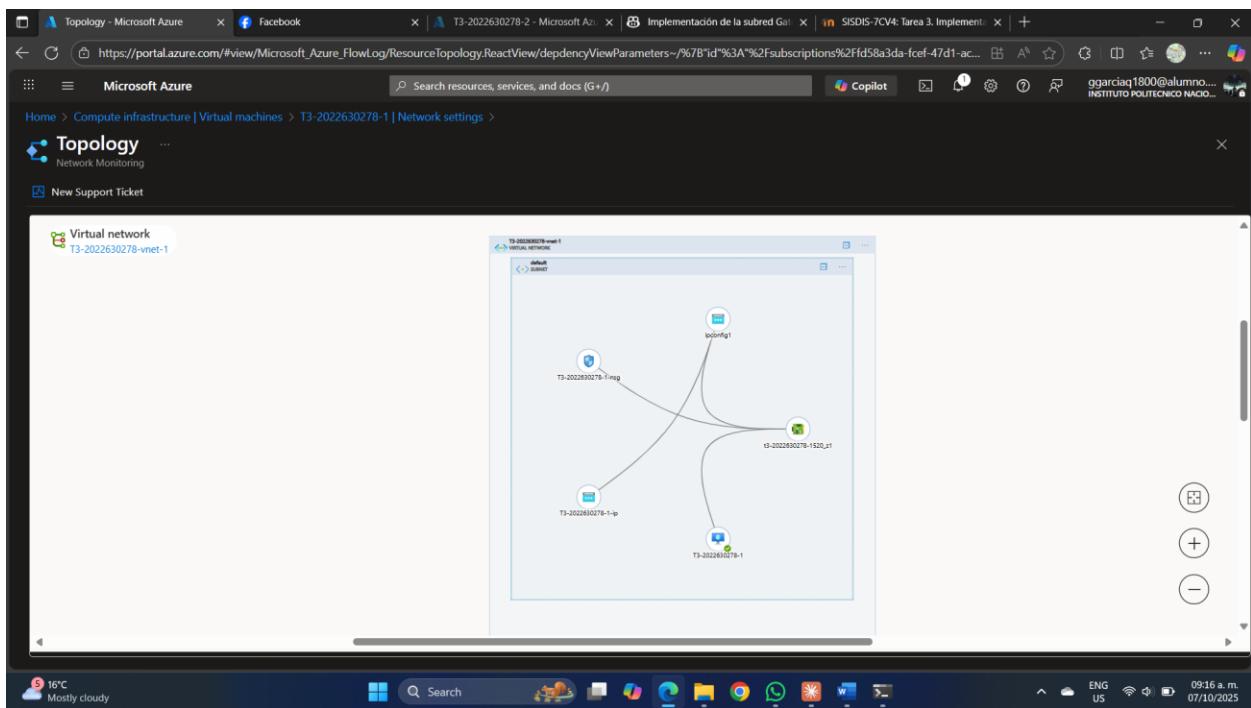


IMAGEN 54 Captura de pantalla COMPLETA de la topología de red de VNet-1, mostrando todos los componentes conectados (VNet, subnets, VM, gateway, NIC, NSG)

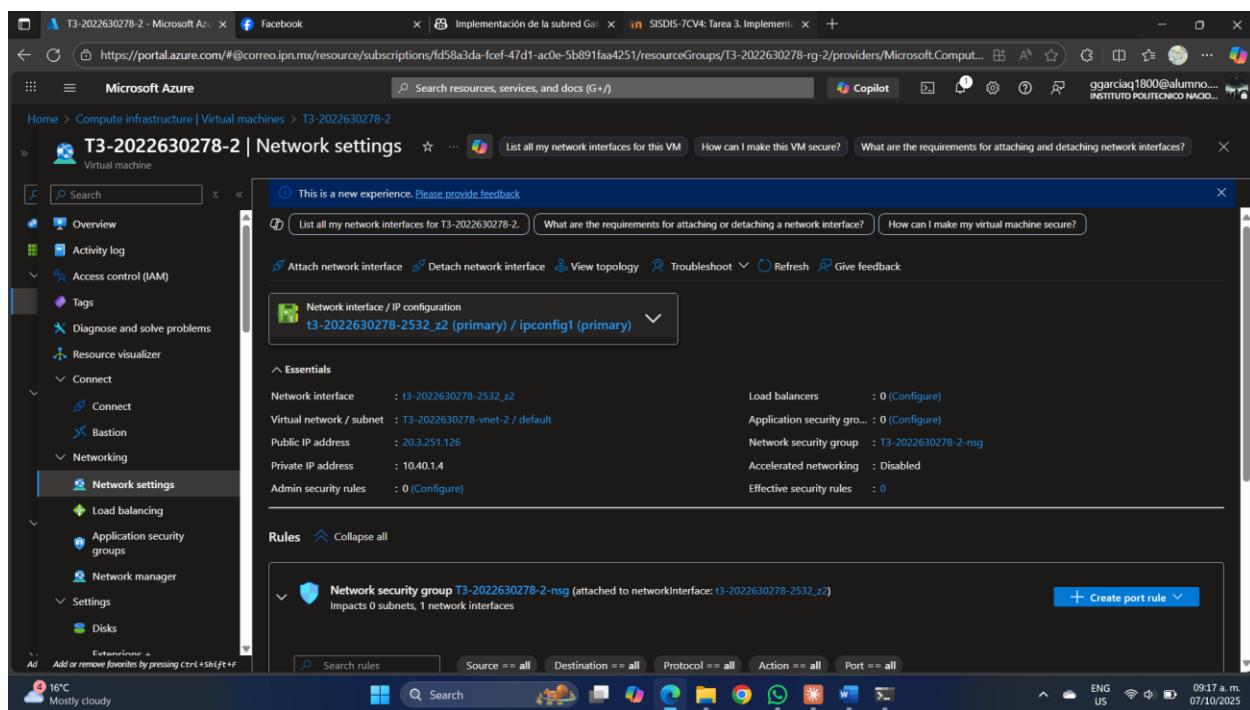
11. (Opcional) Puedes hacer clic en cada componente para ver sus propiedades

12.(Opcional) Usa el botón **Download topology** para guardar la topología como imagen SVG

18.Visualización desde VM2:

19.Pasos detallados:

13.Regresa a Network Watcher > Topology



14.Cambia los filtros:

- **Resource Group:** Selecciona T3-2022630278-rg-2
- **Virtual Network:** Selecciona T3-2022630278-vnet-2

IMAGEN 55 Captura de los filtros de topología configurados para VNet-2

15.La topología mostrará los componentes de la segunda VNet:

- La VNet T3-2022630278-vnet-2
- Las subredes (default y GatewaySubnet)
- La VM T3-2022630278-2
- El Virtual Network Gateway T3-2022630278-gateway-2
- NIC y NSG de VM2

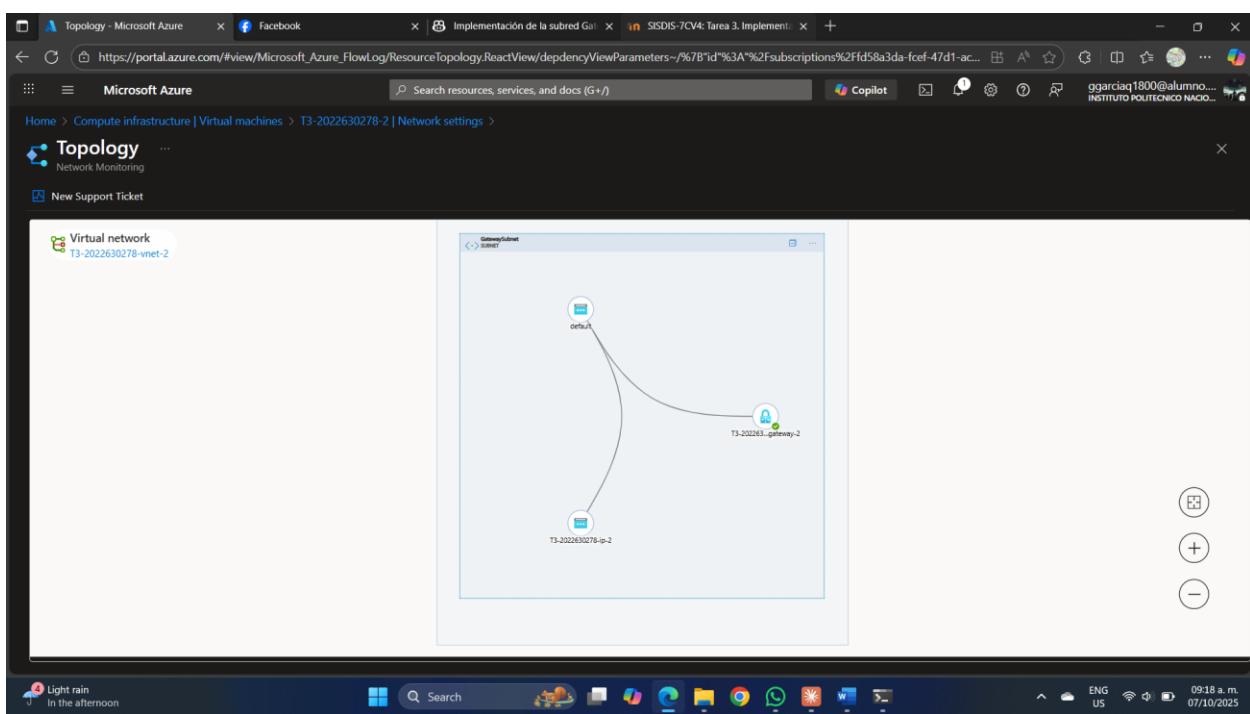
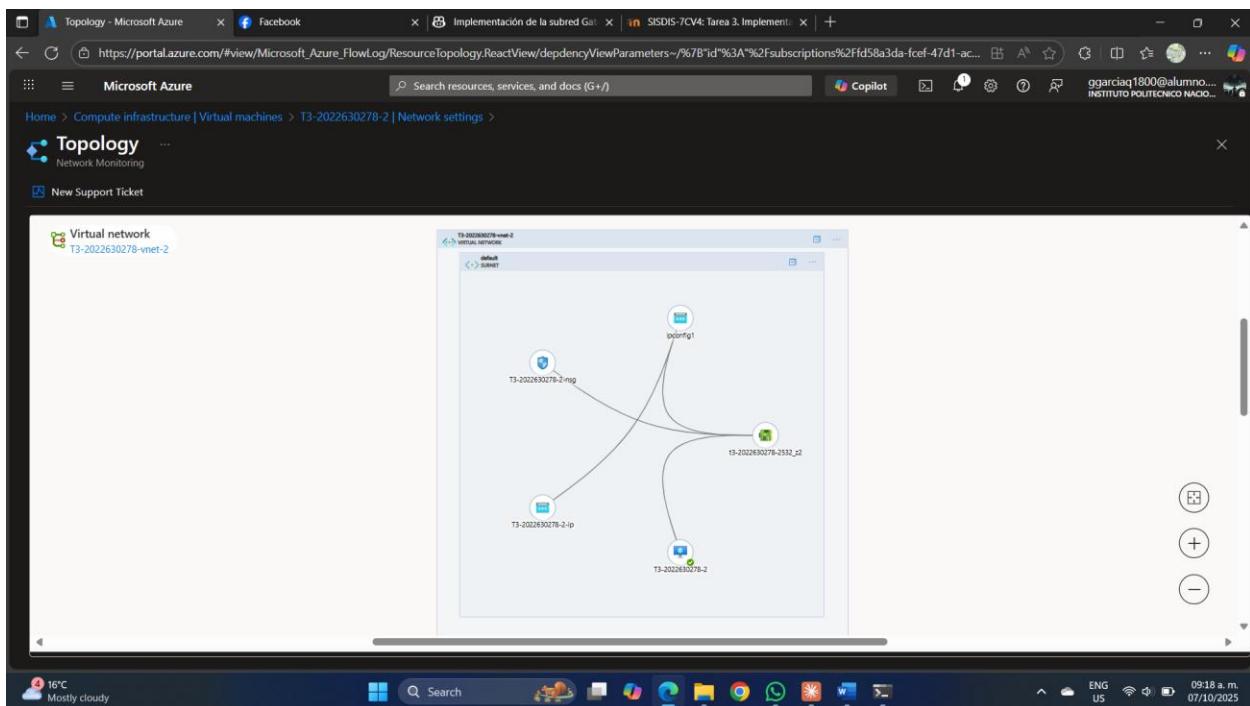


IMAGEN 56 Captura de pantalla COMPLETA de la topología de red de VNet-2, mostrando todos los componentes conectados

6 Eliminación (limpieza) de recursos

La forma más rápida y eficiente de eliminar todos los recursos creados en esta práctica es **eliminar directamente los Resource Groups**, ya que esto elimina automáticamente todos los recursos contenidos dentro de ellos.

6.1 Procedimiento de eliminación

Paso 1: Eliminar Resource Group 1

1. Ir a "Resource groups" en el portal de Azure

Name	Subscription	Location
NetworkWatcherRG	Azure for Students	Mexico Central
T2-2022630278_group_09271755	Azure for Students	Mexico Central
T3-2022630278-rg-1	Azure for Students	Canada Central
T3-2022630278-rg-2	Azure for Students	West US 2

2. Seleccionar T3-2022630278-rg-1
3. Clic en "Delete resource group"
4. Escribir el nombre del resource group para confirmar: T3-2022630278-rg-1
5. Clic en "Delete"

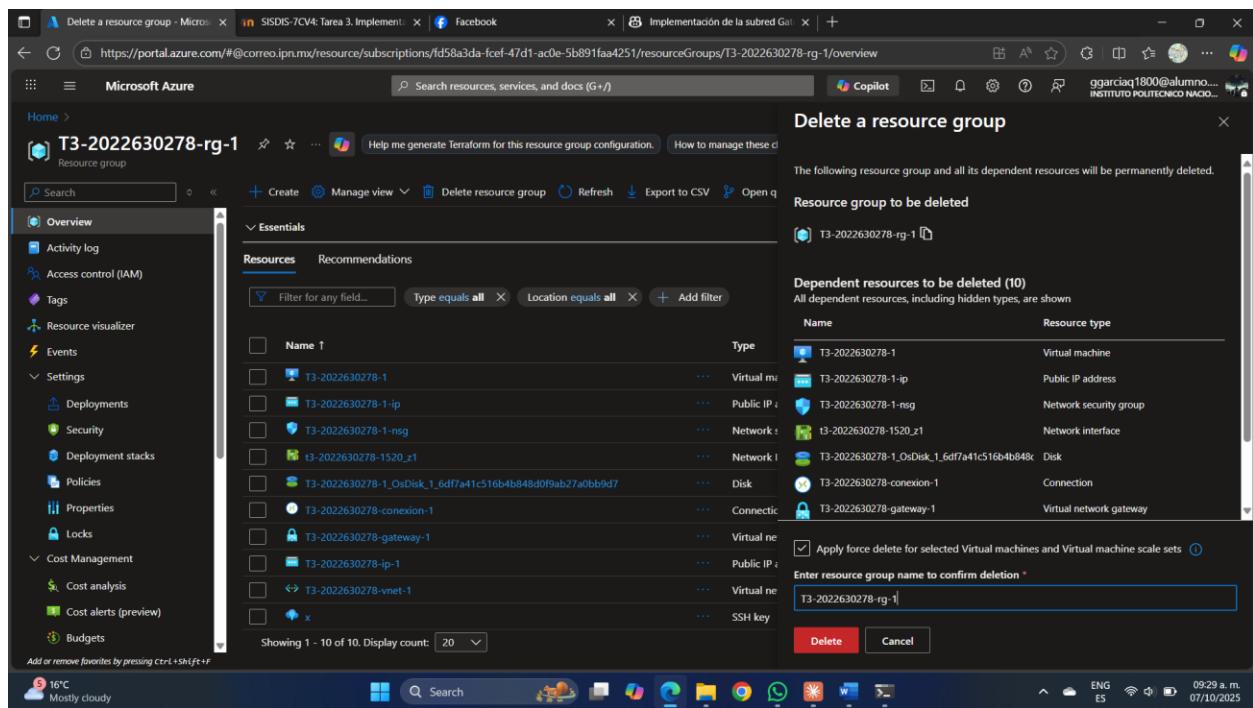


IMAGEN 46: Confirmación de eliminación de T3-2022630278-rg-1

Paso 2: Eliminar Resource Group 2

1. Seleccionar T3-2022630278-rg-2
2. Clic en "Delete resource group"
3. Escribir el nombre del resource group para confirmar: T3-2022630278-rg-2
4. Clic en "Delete"

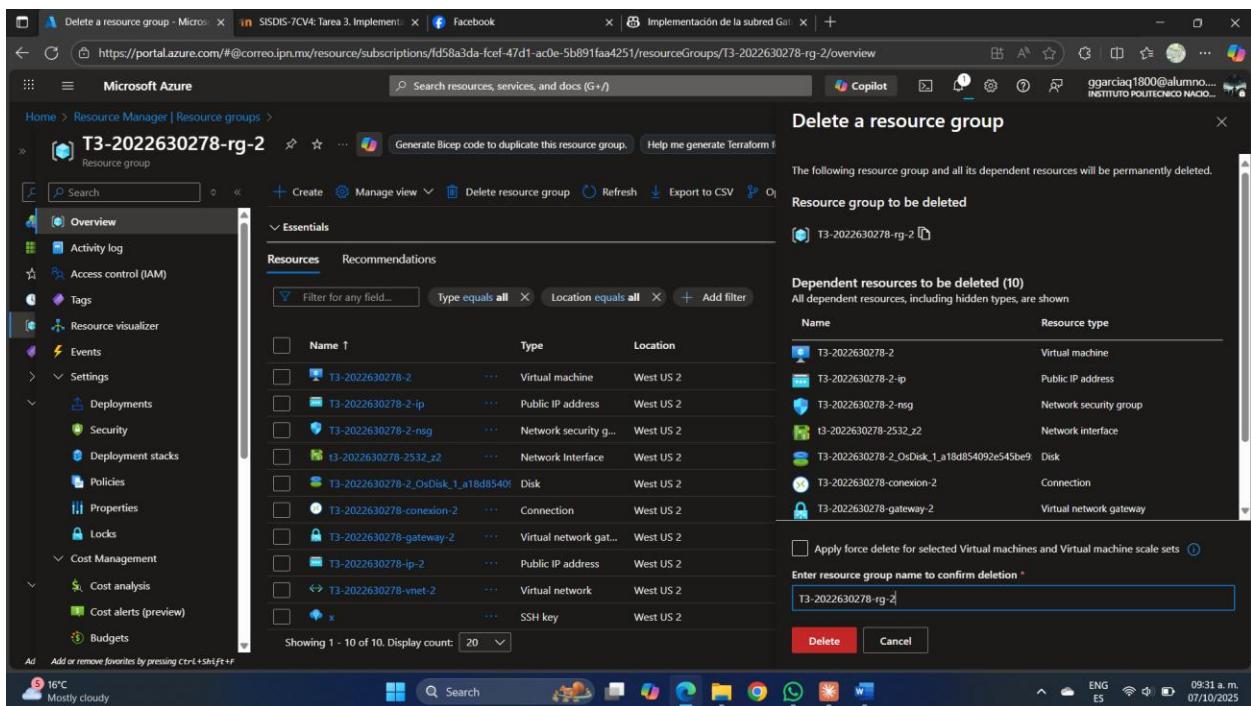


IMAGEN 47: Confirmación de eliminación de T3-2022630278-rg-2

7 Enlace al chat de la IA GitHub Copilot

El enlace al chat de la IA GitHub Copilot que usamos para el desarrollo de esta práctica es el siguiente:

- <https://github.com/copilot/share/c03d5094-0b64-8005-8912-a00f04f029d2>

8 REFERENCIAS

- [1] Microsoft Azure, "Azure Virtual Network documentation," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/virtual-network/> [Accedido: 08-Oct-2025].
- [2] Microsoft Azure, "What is VPN Gateway?," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>. [Accedido: 08-Oct-2025].
- [3] Microsoft Azure, "Configure a VNet-to-VNet VPN gateway connection by using the Azure portal," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>. [Accedido: 08-Oct-2025].
- [4] Microsoft Azure, "About VPN Gateway configuration settings," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings>. [Accedido: 08-Oct-2025].
- [5] Microsoft Azure, "Virtual network peering," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>. [Accedido: 08-Oct-2025].
- [6] Microsoft Azure, "Plan and design Azure Virtual Networks," Microsoft Learn, 2024. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm>. [Accedido: 08-Oct-2025].
- [7] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey, y S. R. Sharma, "Guide to IPsec VPNs," NIST Special Publication 800-77, National Institute of Standards and Technology, Gaithersburg, MD, EE.UU., 2005.
- [8] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, y T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, Internet Engineering Task Force (IETF), 2014. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc7296>.

- [9] S. Kent y K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, Internet Engineering Task Force (IETF), 2005. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4301>.
- [10] Microsoft Azure, "Azure VPN Gateway SKUs," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsku>. [Accedido: 08-Oct-2025].
- [11] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, y E. Lear, "Address Allocation for Private Internets," RFC 1918, Internet Engineering Task Force (IETF), 1996. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc1918>.
- [12] Microsoft Azure, "Create a gateway subnet," Microsoft Learn, 2024. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsub>. [Accedido: 08-Oct-2025].
- [13] J. Postel, "Internet Control Message Protocol," RFC 792, Internet Engineering Task Force (IETF), 1981. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc792>.
- [14] Microsoft Azure, "Network security groups," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>. [Accedido: 08-Oct-2025].
- [15] T. Ylonen y C. Lonvick, "The Secure Shell (SSH) Protocol Architecture," RFC 4251, Internet Engineering Task Force (IETF), 2006. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4251>.
- [16] Microsoft Azure, "Azure for Students," Microsoft Azure Education, 2025. [En línea]. Disponible en: <https://azure.microsoft.com/en-us/free/students/>. [Accedido: 08-Oct-2025].
- [17] Microsoft Azure, "Troubleshoot Azure VPN Gateway," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-troubleshoot>. [Accedido: 08-Oct-2025].
- [18] R. Perlman, Interconnections: Bridges, Routers, Switches, and Internetworking Protocols, 2^a ed. Boston, MA, EE.UU.: Addison-Wesley Professional, 1999.

- [19] A. S. Tanenbaum y D. J. Wetherall, Computer Networks, 5^a ed. Upper Saddle River, NJ, EE.UU.: Prentice Hall, 2011.
- [20] C. Hagen, Mastering Azure Virtual Networks: Design, Implement, and Manage Complex Azure Virtual Network Solutions. Birmingham, Reino Unido: Packt Publishing, 2023.
- [21] Microsoft Azure, "Azure Network Watcher," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-overview>. [Accedido: 08-Oct-2025].
- [22] S. Kent, "IP Encapsulating Security Payload (ESP)," RFC 4303, Internet Engineering Task Force (IETF), 2005. [En línea]. Disponible en: <https://www.rfc-editor.org/rfc/rfc4303>.
- [23] Microsoft Copilot, "Asistencia técnica para configuración de VPN Gateway en Azure," Microsoft AI, 2025. [En línea]. Disponible en: <https://copilot.microsoft.com/>. [Accedido: 08-Oct-2025].
- [24] Microsoft Azure, "Azure regions and availability zones," Microsoft Learn, 2025. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/reliability/availability-zones-overview>. [Accedido: 08-Oct-2025].
- [25] W. R. Stevens, TCP/IP Illustrated, Volume 1: The Protocols, 2^a ed. Upper Saddle River, NJ, EE.UU.: Addison-Wesley Professional, 2011.