Laboratorio #3

Internet Gateway - Conectando VPC a Internet

Proyecto:
Laboratorios Virtuales de Redes en AWS para el
Fortalecimiento de Competencias en Redes de Nueva Generación

Estudiantes:
Nicolás Carreño Tascón
Juan Manuel Canchala Jiménez

Director:
Carlos Olarte

Asignatura:
Redes de Nueva Generación

Duración Estimada: 45-60 minutos
Costo: $0.00 (100 % Gratuito)

Octubre 2025
Elaborado: 6 de octubre de 2025

Índice

Resumen **3**

1. Objetivos **4**
1.1. Objetivo General . . . 4
1.2. Objetivos Específicos . . . 4
1.3. Competencias a Desarrollar . . . 5

2. Marco Teórico **6**
2.1. ¿Qué es un Internet Gateway? . . . 6
2.1.1. Definición y Propósito . . . 6
2.1.2. ¿Cómo Funciona un Internet Gateway? . . . 6
2.1.3. Analogía con Redes Tradicionales . . . 7
2.2. Conceptos de Direccionamiento IP . . . 7
2.2.1. Direcciones IP Privadas (RFC 1918) . . . 7
2.2.2. Direcciones IP Públicas . . . 7
2.2.3. Network Address Translation (NAT) . . . 8
2.3. Componentes de Conectividad en AWS . . . 8
2.3.1. Internet Gateway vs NAT Gateway . . . 8
2.3.2. Flujo Completo de Tráfico . . . 9
2.4. Arquitectura de Subredes Públicas vs Privadas . . . 10
2.4.1. ¿Qué Hace a una Subred "Pública¿ . . . 10
2.4.2. ¿Qué Hace a una Subred "Privada¿ . . . 10
2.4.3. Patrón de Arquitectura Recomendado . . . 10
2.5. Costos y Consideraciones . . . 11
2.5.1. Costos de Internet Gateway . . . 11
2.5.2. Costos de Transferencia de Datos . . . 11
2.6. Mejores Prácticas de Seguridad . . . 12
2.6.1. Defensa en Profundidad . . . 12

3. Requisitos Previos **13**
3.1. Conocimientos Requeridos . . . 13
3.2. Recursos Técnicos . . . 13
3.3. Verificación de Infraestructura Existente . . . 13
3.4. Verificación de Costos . . . 14
3.5. Tiempo Estimado . . . 14

4. Procedimiento Paso a Paso **15**
4.1. Paso 1: Verificar Infraestructura Existente . . . 15
4.1.1. 1.1 Iniciar Sesión como Usuario IAM . . . 15
4.1.2. 1.2 Verificar Región . . . 15
4.1.3. 1.3 Navegar al Servicio VPC . . . 15
4.1.4. 1.4 Verificar VPC Existente . . . 15
4.1.5. 1.5 Verificar Subredes . . . 16
4.1.6. 1.6 Verificar Tablas de Enrutamiento . . . 16

4.2. Paso 2: Crear Internet Gateway . . . 16
4.2.1. 2.1 Navegar a Internet Gateways . . . 16
4.2.2. 2.2 Iniciar Creación de IGW . . . 17
4.2.3. 2.3 Confirmar Creación . . . 17
4.2.4. 2.4 Verificar Estado del IGW . . . 17
4.2.5. 2.5 Anotar Internet Gateway ID . . . 18
4.3. Paso 3: Adjuntar Internet Gateway a VPC . . . 18
4.3.1. 3.1 Iniciar Proceso de Adjunto . . . 18
4.3.2. 3.2 Seleccionar VPC . . . 19
4.3.3. 3.3 Confirmar Adjunto . . . 19
4.3.4. 3.4 Verificar Estado Después del Adjunto . . . 19
4.3.5. 3.5 Verificar desde la VPC . . . 20
4.3.6. 3.6 Entender el Estado Actual . . . 20
4.4. Paso 4: Configurar Ruta por Defecto en la Tabla de Enrutamiento Pública 21
4.4.1. 4.1 Identificar la Tabla de Enrutamiento Pública . . . 21
4.4.2. 4.2 Editar Rutas para Agregar la Ruta por Defecto . . . 21
4.4.3. 4.3 Guardar Cambios . . . 21
4.4.4. 4.4 Verificar Auto-asignación de IP Pública en Subredes . . . 22
4.5. Paso 5: Verificación de la Configuración . . . 22
4.5.1. 5.1 Verificar Rutas en la Tabla Pública . . . 22
4.5.2. 5.2 Verificar la Tabla Privada No Cambió . . . 22
4.5.3. 5.3 Verificar Adjunto del IGW . . . 22
4.5.4. 5.4 Verificaciones Adicionales Recomendadas . . . 23
4.6. Paso 6: Documentación y Limpieza (Opcional) . . . 23

5. Cuestionario **24**
5.1. Instrucciones . . . 24
5.2. Preguntas . . . 24
5.3. Respuestas . . . 27

6. Conclusiones **29**
6.1. Logros Alcanzados . . . 29
6.2. Competencias Desarrolladas . . . 29
6.3. Integración con el Ecosistema de Laboratorios . . . 30
6.4. Consideraciones de Seguridad y Mejores Prácticas . . . 30
6.5. Impacto en el Desarrollo Profesional . . . 31
6.6. Reflexión Final . . . 31

7. Referencias **32**
7.1. Documentación Oficial de AWS . . . 32
7.2. Estándares y RFCs de Red . . . 32
7.3. Libros y Recursos Académicos . . . 32
7.4. Artículos y Whitepapers Técnicos . . . 33
7.5. Herramientas y Recursos de Laboratorio . . . 33
7.6. Recursos de Certificación y Aprendizaje . . . 33
7.7. Recursos de Troubleshooting y Monitoreo . . . 34

Resumen

Este laboratorio se enfoca en la configuración de conectividad a internet para Amazon Virtual Private Cloud (VPC) mediante la implementación de un Internet Gateway (IGW). Los estudiantes aprenderán a transformar subredes privadas en subredes públicas funcionales, permitiendo comunicación bidireccional entre recursos en AWS e internet.

A través de actividades prácticas completamente textuales utilizando el nivel gratuito de AWS, se abordará la creación, adjunto y configuración de un Internet Gateway, la modificación de tablas de enrutamiento para agregar rutas hacia internet, y la comprensión del flujo de tráfico de red entre VPC e internet. Se explicará detalladamente la diferencia entre direcciones IP públicas y privadas, el papel del Network Address Translation (NAT) implícito en AWS, y cómo el Internet Gateway permite que instancias con direcciones IP públicas sean accesibles desde internet.

El laboratorio construye directamente sobre la infraestructura de VPC creada en el Laboratorio 2, agregando la capa de conectividad externa necesaria para que las aplicaciones web puedan servir tráfico público. Los estudiantes comprenderán conceptos críticos como el enrutamiento a nivel de VPC, la asimetría entre tráfico entrante y saliente, y las consideraciones de seguridad al exponer recursos a internet.

Al finalizar, los participantes habrán creado una arquitectura de red funcional donde las subredes públicas pueden comunicarse con internet mientras las subredes privadas permanecen aisladas, preparando el terreno para el despliegue de instancias EC2 y aplicaciones web en laboratorios posteriores.

Palabras clave: Internet Gateway, IGW, Conectividad Internet, Enrutamiento, Direcciones IP Públicas, NAT, Subredes Públicas, Tráfico Bidireccional, AWS Networking

1 Objetivos

1.1 Objetivo General

Implementar conectividad a internet en una Amazon VPC mediante la creación, configuración y adjunto de un Internet Gateway, modificando las tablas de enrutamiento apropiadas para permitir tráfico bidireccional entre subredes públicas e internet, y comprendiendo los fundamentos de direccionamiento IP público, enrutamiento de red, y las implicaciones de seguridad al exponer recursos de AWS a internet público.

1.2 Objetivos Específicos

- **Comprender el funcionamiento del Internet Gateway:** Estudiar el papel del IGW como puerta de enlace entre VPC e internet, entender su arquitectura de alta disponibilidad, y conocer las diferencias entre IGW y otros componentes de conectividad como NAT Gateway.
- **Crear y adjuntar Internet Gateway a VPC:** Implementar un Internet Gateway desde la consola de AWS, adjuntarlo correctamente a la VPC existente, y verificar el estado de conexión del recurso.
- **Configurar enrutamiento para acceso a internet:** Modificar tablas de enrutamiento de subredes públicas agregando la ruta por defecto (0.0.0.0/0) apuntando al Internet Gateway, permitiendo que el tráfico destinado a internet sea correctamente enrutado.
- **Diferenciar entre subredes públicas y privadas operacionalmente:** Comprender cómo la presencia o ausencia de ruta a IGW determina la naturaleza pública o privada de una subred, y las implicaciones para recursos desplegados en cada tipo.
- **Comprender direccionamiento IP público vs privado:** Entender la diferencia entre direcciones IP privadas (RFC 1918) usadas dentro de VPC y direcciones IP públicas necesarias para comunicación con internet, incluyendo el papel del NAT implícito de AWS.
- **Analizar flujos de tráfico de red:** Trazar el camino que sigue el tráfico desde una instancia EC2 en subred pública hacia internet y viceversa, identificando cada salto de enrutamiento y transformación de direcciones.
- **Verificar conectividad sin instancias EC2:** Utilizar herramientas de la consola de AWS para confirmar que la configuración de red es correcta antes de desplegar recursos computacionales.
- **Aplicar principios de seguridad en conectividad internet:** Entender que exponer subredes a internet requiere configuración adicional de Security Groups y Network ACLs, preparando la arquitectura para despliegues seguros.

1.3 Competencias a Desarrollar

Competencias Técnicas:

- Configuración de componentes de conectividad en arquitecturas de nube
- Gestión de tablas de enrutamiento y rutas de red
- Comprensión de direccionamiento IP y Network Address Translation
- Diseño de arquitecturas de red con separación público/privado
- Verificación y troubleshooting de conectividad de red
- Implementación de mejores prácticas de seguridad en redes expuestas

Competencias Profesionales:

- Toma de decisiones sobre cuándo exponer recursos a internet
- Documentación de flujos de tráfico de red
- Comprensión de trade-offs entre accesibilidad y seguridad
- Aplicación de principios de defensa en profundidad
- Planificación de arquitecturas de conectividad escalables

2 Marco Teórico

2.1 ¿Qué es un Internet Gateway?

2.1.1. Definición y Propósito

Un **Internet Gateway (IGW)** es un componente de VPC horizontalmente escalado, redundante y de alta disponibilidad que permite la comunicación entre instancias en tu VPC e internet. Funciona como una "puerta de enlace"que conecta tu red privada virtual con la internet pública.

Características principales:

- **Administrado por AWS:** No requieres gestionar servidores ni preocuparte por disponibilidad
- **Alta disponibilidad:** Diseñado para no tener punto único de fallo
- **Escalabilidad automática:** Se adapta al ancho de banda requerido sin intervención
- **Sin costo:** El IGW en sí es gratuito, solo pagas por transferencia de datos
- **Funciones duales:** Permite tráfico saliente (de VPC a internet) y entrante (de internet a VPC)

2.1.2. ¿Cómo Funciona un Internet Gateway?

El Internet Gateway realiza dos funciones críticas:

1. Proporcionar un objetivo de ruta para tráfico a internet:

Cuando configuras una tabla de enrutamiento con una ruta `0.0.0.0/0` → `igw-xxxxx`, estás diciéndole a tu VPC: "Todo tráfico destinado a direcciones que no están en mi red local (10.0.0.0/16), envíalo al Internet Gateway".

2. Realizar traducción de direcciones de red (NAT) para instancias con IP pública:

- **Tráfico saliente:** IGW traduce la dirección IP privada de tu instancia (por ejemplo, 10.0.1.50) a su dirección IP pública (por ejemplo, 54.123.45.67) antes de enviar paquetes a internet
- **Tráfico entrante:** IGW traduce la dirección IP pública de destino de vuelta a la dirección IP privada de la instancia cuando llegan paquetes desde internet

Este proceso de NAT es completamente transparente y administrado por AWS. Tu instancia nunca "ve"su dirección IP pública en su interfaz de red; solo conoce su IP privada.

2.1.3. Analogía con Redes Tradicionales

En una red empresarial tradicional:

- **Internet Gateway** ≡ Router de borde + Firewall NAT
- Conecta tu red interna (LAN) con internet (WAN)
- Realiza NAT para permitir que múltiples dispositivos internos compartan una IP pública
- Proporciona punto de entrada/salida controlado

La diferencia es que en AWS, el IGW es completamente administrado, altamente disponible, y no requiere configuración de hardware.

2.2 Conceptos de Direccionamiento IP

2.2.1. Direcciones IP Privadas (RFC 1918)

Son direcciones IP usadas dentro de redes privadas que NO son enrutables en internet público:

Rango	**Uso en VPC**
10.0.0.0/8	Usamos 10.0.0.0/16 en nuestros labs
172.16.0.0/12	AWS Default VPC usa 172.31.0.0/16
192.168.0.0/16	Común en redes domésticas

Cuadro 1: Rangos de IP privadas según RFC 1918

Importante: Cada instancia EC2 en una VPC SIEMPRE tiene una dirección IP privada. Esta IP es persistente durante toda la vida de la instancia.

2.2.2. Direcciones IP Públicas

Son direcciones IP enrutables en internet que permiten comunicación directa con recursos fuera de tu VPC:

Tipos de IP públicas en AWS:

1. **Public IP (dinámica):**
   - Asignada automáticamente si .^Auto-assign Public IP.^está habilitado en subred
   - Cambia si detienes/inicias la instancia
   - Se libera cuando terminas la instancia
   - Gratuita
2. **Elastic IP (estática):**
   - Dirección IP pública que puedes reservar y asociar/desasociar libremente

- Persiste incluso si detienes la instancia
- Gratuita SOLO mientras está asociada a una instancia corriendo
- $0.005/hora si está reservada pero NO asociada (para prevenir acaparamiento)

En este laboratorio: Trabajaremos con Public IPs dinámicas (gratuitas).

2.2.3. Network Address Translation (NAT)

¿Qué es NAT?
Network Address Translation (NAT) es el proceso de modificar direcciones IP en paquetes de red mientras atraviesan un router o gateway. Permite que dispositivos en una red privada compartan una dirección IP pública para acceder a internet.
NAT en Internet Gateway:

1. Instancia EC2 con IP privada 10.0.1.50 e IP pública 54.123.45.67
2. Instancia envía solicitud HTTP a www.google.com (172.217.164.196)
3. Paquete sale con IP origen: 10.0.1.50
4. Internet Gateway intercepta el paquete
5. IGW cambia IP origen a: 54.123.45.67 (NAT)
6. Paquete llega a Google con origen 54.123.45.67
7. Google responde a 54.123.45.67
8. IGW recibe respuesta, traduce destino de vuelta a 10.0.1.50
9. Instancia recibe respuesta en su IP privada

Importante: La instancia EC2 nunca "sabe"que tiene IP pública. Si ejecutas `ifconfig` o `ip addr` en la instancia, solo verás la IP privada. La IP pública solo existe "fuera"de la instancia, gestionada por AWS.

2.3 Componentes de Conectividad en AWS

2.3.1. Internet Gateway vs NAT Gateway

Es importante no confundir estos dos componentes:
En este laboratorio: Solo usaremos Internet Gateway (gratuito).

Característica	Internet Gateway (IGW)	NAT Gateway
Propósito	Conectividad bidireccional entre VPC e internet	Solo salida: recursos privados acceden a internet
Tráfico entrante	Sí (si instancia tiene IP pública)	No
Tráfico saliente	Sí	Sí
Casos de uso	Servidores web, APIs públicas, bastion hosts	Actualizaciones de software, acceso APIs externas desde recursos privados
Costo	$0.00	$0.045/hora + $0.045/GB
Disponibilidad	Altamente disponible automáticamente	Alta disponibilidad (pero 1 por AZ)
Usado en	Subredes públicas	Subredes privadas

Cuadro 2: Comparación Internet Gateway vs NAT Gateway

2.3.2. Flujo Completo de Tráfico

Escenario: Usuario en internet accede a servidor web en subred pública.
Paso a paso del tráfico:

1. Usuario escribe en navegador: `http://54.123.45.67`
2. Navegador envía solicitud HTTP a 54.123.45.67:80
3. Paquete llega a Internet Gateway de AWS
4. IGW verifica tabla de enrutamiento de VPC
5. IGW traduce IP destino: 54.123.45.67 → 10.0.1.50
6. Paquete enrutado a subred pública (10.0.1.0/24)
7. Security Group de instancia evalúa: ¿permitir puerto 80? → Sí
8. Network ACL de subred evalúa: ¿permitir tráfico entrante? → Sí
9. Paquete llega a instancia EC2 (10.0.1.50)
10. Instancia procesa solicitud HTTP, genera respuesta
11. Respuesta sale con IP origen: 10.0.1.50
12. Tabla de enrutamiento: destino no es 10.0.0.0/16 → enviar a IGW
13. IGW traduce IP origen: 10.0.1.50 → 54.123.45.67
14. Respuesta llega al navegador del usuario

Este flujo demuestra la importancia de:

- Ruta correcta en tabla de enrutamiento (0.0.0.0/0 → IGW)
- Instancia con IP pública asignada
- Security Groups configurados para permitir tráfico deseado

2.4 Arquitectura de Subredes Públicas vs Privadas

2.4.1. ¿Qué Hace a una Subred "Pública¿

Una subred es "públicaçuando cumple TODAS estas condiciones:

1. **Tiene ruta a Internet Gateway:** Su tabla de enrutamiento incluye `0.0.0.0/0` → `igw-xxxxx`
2. **Auto-asignación de IP pública habilitada:** Configuración .Auto-assign public IPv4 address- Yes
3. **Internet Gateway adjunto a VPC:** El IGW está creado y asociado a la VPC

Si falta cualquiera de estos elementos, la subred NO funcionará como pública.

2.4.2. ¿Qué Hace a una Subred "Privada¿

Una subred es "privadaçuando:

1. **NO tiene ruta a Internet Gateway**
2. **Instancias NO tienen IP pública**
3. Opcionalmente: puede tener ruta a NAT Gateway para salida a internet (Lab futuro)

Importante: "Privada"no significa "sin conectividad". Subredes privadas pueden:

- Comunicarse con otras subredes en la VPC (ruta local)
- Acceder a internet vía NAT Gateway (solo salida)
- Conectarse a redes corporativas vía VPN/Direct Connect
- Alojar bases de datos, servidores de aplicación backend, etc.

2.4.3. Patrón de Arquitectura Recomendado

Mejores prácticas de AWS para arquitecturas de producción:

- **Capa pública (subredes públicas):**
  - Balanceadores de carga (ALB, NLB)
  - Bastion hosts / Jump boxes para administración
  - NAT Gateways (para dar salida a subredes privadas)
  - Servidores web que deben ser accesibles públicamente
- **Capa privada (subredes privadas):**
  - Servidores de aplicación backend

- Bases de datos (RDS, DynamoDB con endpoints VPC)
- Servicios internos de API
- Colas de mensajes, workers de procesamiento

Principio fundamental: Exponer a internet solo lo absolutamente necesario. Todo lo demás debe estar en subredes privadas.

2.5 Costos y Consideraciones

2.5.1. Costos de Internet Gateway

¡Buenas noticias! El Internet Gateway en sí es **completamente gratuito**. No hay cargo por:

- Crear un Internet Gateway
- Adjuntarlo a una VPC
- Mantenerlo activo 24/7
- Procesar paquetes a través de él

2.5.2. Costos de Transferencia de Datos

Lo que SÍ tiene costo es la transferencia de datos:

Tipo de Tráfico	Primeros 100 GB/mes	Después de 100 GB
Entrada a AWS (ingress)	$0.00	$0.00 (siempre gratis)
Salida de AWS (egress)	$0.00	$0.09/GB
Entre regiones AWS	-	$0.02/GB

Cuadro 3: Costos de transferencia de datos en AWS

En este laboratorio:

- No desplegaremos instancias EC2 que generen tráfico significativo
- Solo verificaremos configuración
- Costo esperado: **$0.00**

Para proyectos futuros: Los primeros 100 GB/mes de transferencia saliente son gratuitos, suficiente para aplicaciones pequeñas/medianas.

2.6 Mejores Prácticas de Seguridad

2.6.1. Defensa en Profundidad

Exponer recursos a internet requiere múltiples capas de seguridad:

1. **Capa 1 - Segregación de subredes:**
   - Solo subredes públicas tienen ruta a IGW
   - Recursos sensibles en subredes privadas sin acceso directo desde internet
2. **Capa 2 - Security Groups:**
   - Firewall stateful a nivel de instancia
   - Permitir solo puertos necesarios (80, 443 para web)
   - Denegar todo por defecto, permitir explícitamente
3. **Capa 3 - Network ACLs:**
   - Firewall stateless a nivel de subred
   - Reglas adicionales de entrada/salida
   - Útil para bloquear rangos IP maliciosos
4. **Capa 4 - IAM:**
   - Control de quién puede modificar IGW, tablas de enrutamiento
   - Auditoría con CloudTrail

En este lab: Configuramos la Capa 1 (segregación). Las demás capas se abordarán en laboratorios posteriores.

3 Requisitos Previos

3.1 Conocimientos Requeridos

- **Laboratorio 1 completado:**
  - Cuenta AWS activa con usuario IAM
  - Familiaridad con consola de AWS
  - Alertas de facturación configuradas
- **Laboratorio 2 completado (CRÍTICO):**
  - VPC creada: 10.0.0.0/16
  - 4 subredes: 2 públicas, 2 privadas
  - Tablas de enrutamiento: Public-Route-Table, Private-Route-Table
  - Subredes con auto-asignación de IP pública habilitada
- **Conceptos de redes:**
  - Enrutamiento y tablas de rutas
  - Direcciones IP públicas vs privadas
  - Concepto de gateway/puerta de enlace
  - NAT (Network Address Translation)

3.2 Recursos Técnicos

- **Cuenta AWS** con VPC del Lab 2 (NO eliminar)
- **Usuario IAM** con permisos de administrador
- **Conexión a internet** estable
- **Navegador web** moderno
- **Documentación del Lab 2** (IDs de VPC, subredes, route tables)

3.3 Verificación de Infraestructura Existente

Antes de comenzar, confirmar que tienes:
Si falta alguno de estos recursos, debes completar el Laboratorio 2 primero.

Recurso	Valor Esperado	
VPC	Lab2-VPC (10.0.0.0/16)	
Subred Pública 1	Public-Subnet-1A (10.0.1.0/24, us-east-1a)	
Subred Pública 2	Public-Subnet-1B (10.0.2.0/24, us-east-1b)	
Subred Privada 1	Private-Subnet-1A (10.0.11.0/24, us-east-1a)	
Subred Privada 2	Private-Subnet-1B (10.0.12.0/24, us-east-1b)	
Tabla Ruta Pública	Public-Route-Table (asociada a subredes públicas)	
Tabla Ruta Privada	Private-Route-Table (Main, asociada a privadas)	

Cuadro 4: Checklist de infraestructura requerida del Lab 2

Servicio	Costo	Nota
Internet Gateway	$0.00	Siempre gratuito
Modificación Route Tables	$0.00	Sin cargo
Transferencia datos (este lab)	$0.00	No habrá tráfico significativo
TOTAL	**$0.00**	100 % Free Tier

Cuadro 5: Costos del Laboratorio 3

3.4 Verificación de Costos

3.5 Tiempo Estimado

- **Lectura y comprensión de conceptos:** 15-20 minutos
- **Creación de Internet Gateway:** 5 minutos
- **Adjunto a VPC:** 3 minutos
- **Modificación de tablas de enrutamiento:** 10 minutos
- **Verificación de configuración:** 10 minutos
- **Cuestionario:** 5-10 minutos
- **TOTAL:** 45-60 minutos

4 Procedimiento Paso a Paso

4.1 Paso 1: Verificar Infraestructura Existente

Objetivo: Confirmar que la VPC del Lab 2 está lista para agregar Internet Gateway.

4.1.1. 1.1 Iniciar Sesión como Usuario IAM

1. Abrir navegador web
2. Ir a la URL de inicio de sesión IAM
3. Ingresar credenciales de usuario IAM administrador
4. Si tienes MFA habilitado, ingresar código de 6 dígitos
5. Hacer clic en "Sign in"

4.1.2. 1.2 Verificar Región

1. En barra superior derecha, verificar que estés en la región correcta
2. Debe decir "N. Virginia"(us-east-1) o la región que usaste en Lab 2
3. Si está en otra región, cambiarla ahora
4. **MUY IMPORTANTE:** Todos los recursos deben estar en la misma región

4.1.3. 1.3 Navegar al Servicio VPC

1. En consola de AWS, hacer clic en "Services"
2. Buscar y hacer clic en "VPC"
3. Se abrirá el dashboard de VPC

4.1.4. 1.4 Verificar VPC Existente

1. En panel izquierdo, hacer clic en "Your VPCs"
2. Buscar "Lab2-VPC.[en] la lista
3. Verificar:
   - State: Available (verde)
   - IPv4 CIDR: 10.0.0.0/16
   - Anotar el VPC ID (ejemplo: vpc-0a1b2c3d4e5f67890)
4. Si no encuentras la VPC, DETENTE y completa Lab 2 primero

4.1.5. 1.5 Verificar Subredes

1. En panel izquierdo, hacer clic en "Subnets"
2. Filtrar por VPC: seleccionar "Lab2-VPC"
3. Confirmar que existen 4 subredes:
   - Public-Subnet-1A (10.0.1.0/24, us-east-1a)
   - Public-Subnet-1B (10.0.2.0/24, us-east-1b)
   - Private-Subnet-1A (10.0.11.0/24, us-east-1a)
   - Private-Subnet-1B (10.0.12.0/24, us-east-1b)

4.1.6. 1.6 Verificar Tablas de Enrutamiento

1. En panel izquierdo, hacer clic en Route Tables"
2. Filtrar por VPC: "Lab2-VPC"
3. Confirmar que existen 2 tablas:
   - Public-Route-Table (asociada a 2 subredes públicas)
   - Private-Route-Table (Main = Yes, asociada a 2 subredes privadas)
4. Seleccionar "Public-Route-Table"
5. Hacer clic en pestaña Routes"
6. Verificar que SOLO existe ruta: 10.0.0.0/16 → local
7. NO debe haber ruta 0.0.0.0/0 (la agregaremos en este lab)

Si todo está correcto, estás listo para continuar. Si falta algo, revisar Lab 2.

4.2 Paso 2: Crear Internet Gateway

Objetivo: Crear un Internet Gateway que posteriormente adjuntaremos a nuestra VPC.

4.2.1. 2.1 Navegar a Internet Gateways

1. En el dashboard de VPC, buscar en panel izquierdo la sección "Virtual private cloud"
2. Hacer clic en Ïnternet Gateways"
3. Se abrirá la lista de Internet Gateways existentes
4. Probablemente no veas ninguno (a menos que hayas creado previamente)

4.2.2. 2.2 Iniciar Creación de IGW

1. En la parte superior, hacer clic en el botón naranja Çreate internet gateway"
2. Se abrirá el formulario de creación

Formulario de creación de Internet Gateway:

1. **Name tag:** Ingresar nombre descriptivo
   - Ejemplo: `Lab3-IGW`
   - O: `Internet-Gateway-Lab2-VPC`
   - El nombre debe ser claro para identificar su propósito
2. **Tags adicionales (opcional pero recomendado):**
   - Hacer clic en .Add new tag"
   - Key: `Environment`, Value: `development`
   - Hacer clic en .Add new tag"nuevamente
   - Key: `Project`, Value: `AWS-Labs`

Nota importante: A diferencia de otros recursos, NO seleccionas la VPC durante la creación del IGW. Primero creas el IGW ïndependientez luego lo adjuntas a una VPC.

4.2.3. 2.3 Confirmar Creación

1. Revisar la configuración
2. Verificar que el nombre sea correcto: "Lab3-IGW"
3. Hacer clic en el botón naranja Çreate internet gateway"(parte inferior)
4. AWS procesará la solicitud (tarda 1-2 segundos)
5. Verás banner verde de éxito: Çreated internet gateway igw-xxxxx"

4.2.4. 2.4 Verificar Estado del IGW

Después de la creación:

1. Serás redirigido automáticamente a la página de detalles del IGW
2. O puedes hacer clic en el IGW ID en el banner verde
3. Observar la información mostrada:
   - **Internet gateway ID:** igw-0123456789abcdef (ejemplo)
   - **State:** "detached"(en amarillo/naranja)
   - **VPC ID:** "(todavía no adjunto a ninguna VPC)

- **Owner ID:** Tu account ID

¿Por qué dice "detached¿

- El Internet Gateway se crea como recurso independiente
- Debe ser explícitamente "adjuntado"(attached) a una VPC
- Un IGW solo puede estar adjunto a 1 VPC a la vez
- Una VPC solo puede tener 1 IGW adjunto a la vez (relación 1:1)
- Estado "detached"significa: creado pero sin asociar

4.2.5. 2.5 Anotar Internet Gateway ID

Importante para siguientes pasos:

1. Copiar el Internet Gateway ID
2. Ejemplo: `igw-0123456789abcdef`
3. Guardarlo en documento temporal junto con VPC ID
4. Lo necesitarás para:
   - Adjuntarlo a la VPC (siguiente paso)
   - Agregar ruta en tabla de enrutamiento
   - Verificación final

4.3 Paso 3: Adjuntar Internet Gateway a VPC

Objetivo: Asociar el IGW creado con nuestra VPC del Lab 2.

4.3.1. 3.1 Iniciar Proceso de Adjunto

Desde la página de detalles del IGW:

1. Si no estás ya en la página de detalles, ir a Ïnternet Gateways"
2. Seleccionar tu IGW "Lab3-IGW"(casilla izquierda)
3. En la parte superior, hacer clic en el menú desplegable "Actions"
4. Seleccionar "Attach to VPC"
5. Se abrirá una ventana modal / nueva página

Alternativa (desde la lista):

1. En la lista de Internet Gateways
2. Encontrar tu IGW con estado "detached"
3. Hacer clic derecho sobre él
4. Seleccionar "Attach to VPC"del menú contextual

4.3.2. 3.2 Seleccionar VPC

Formulario .Attach to VPC":

1. Verás el campo .Available VPCs"
2. Hacer clic en el campo desplegable
3. Buscar por nombre: "Lab2-VPC"
4. O buscar por VPC ID: vpc-0a1b2c3d4e5f67890
5. Seleccionar tu VPC
6. Verificar que el CIDR mostrado sea: 10.0.0.0/16

¿Qué VPCs aparecen en la lista?

- Solo VPCs que NO tienen IGW adjunto actualmente
- Si una VPC ya tiene IGW, NO aparecerá (límite 1 IGW por VPC)
- Si no ves tu Lab2-VPC, verifica:
  - ¿Estás en la región correcta?
  - ¿La VPC ya tiene un IGW? (revisar en detalles de VPC)
  - ¿La VPC fue eliminada por error?

4.3.3. 3.3 Confirmar Adjunto

1. Verificar que seleccionaste "Lab2-VPC (10.0.0.0/16)"
2. Hacer clic en el botón .Attach internet gateway"
3. AWS procesará la solicitud (tarda 2-3 segundos)
4. Verás banner verde: Ïnternet gateway igw-xxxxx attached to VPC vpc-xxxxx"

4.3.4. 3.4 Verificar Estado Después del Adjunto

Cambios visibles inmediatamente:

1. En la lista de Internet Gateways, el estado cambió:
   - **Antes:** State = "detached"(amarillo/naranja)
   - **Ahora:** State = .attached"(verde)
2. Hacer clic en tu IGW para ver detalles
3. Verificar:
   - **State:** .attached"
   - **VPC ID:** vpc-0a1b2c3d4e5f67890 (tu VPC)
   - Ahora muestra el nombre "Lab2-VPC.asociado

4.3.5. 3.5 Verificar desde la VPC

Vista desde el recurso VPC:

1. Navegar a "Your VPCs.en panel izquierdo
2. Seleccionar "Lab2-VPC"
3. En la parte inferior, buscar detalles de la VPC
4. NO hay una pestaña específica Ïnternet Gateway"
5. Pero puedes ver en la columna Ïnternet gateway"de la lista
6. Debería mostrar: igw-0123456789abcdef (tu IGW ID)

¿Por qué esta relación es 1:1?

- **1 VPC = 1 IGW máximo:** Simplifica enrutamiento y arquitectura
- **1 IGW = 1 VPC:** Un IGW no puede compartirse entre VPCs
- Si necesitas múltiples VPCs con internet, crea 1 IGW por VPC
- Esta restricción es por diseño de AWS para claridad y seguridad

4.3.6. 3.6 Entender el Estado Actual

¿Qué acabas de lograr?

- Internet Gateway creado
- IGW adjunto a Lab2-VPC
- AWS ahora tiene la "puerta de enlace"lista

¿Qué NO está funcionando todavía?

- Subredes NO pueden acceder a internet aún
- Razón: falta configurar RUTAS en tablas de enrutamiento
- Las tablas de enrutamiento no saben que deben enviar tráfico al IGW

Analogía:

- Instalaste una puerta (IGW) en tu casa (VPC)
- Pero no le dijiste a nadie (subredes) que usen esa puerta para salir
- Ahora debes actualizar las ïnstrucciones"(tablas de enrutamiento)

Siguiente paso crítico: Agregar ruta 0.0.0.0/0 → IGW en tabla pública.

4.4 Paso 4: Configurar Ruta por Defecto en la Tabla de Enrutamiento Pública

Objetivo: Enviar todo el tráfico destinado fuera de la VPC (IPv4) al Internet Gateway para las subredes públicas.

4.4.1. 4.1 Identificar la Tabla de Enrutamiento Pública

1. En el panel izquierdo, hacer clic en Route Tables"
2. Filtrar por VPC: seleccionar `Lab2-VPC`
3. Seleccionar **Public-Route-Table**
4. Ir a la pestaña **Subnet associations** y confirmar que están asociadas:
   - `Public-Subnet-1A` (10.0.1.0/24)
   - `Public-Subnet-1B` (10.0.2.0/24)

4.4.2. 4.2 Editar Rutas para Agregar la Ruta por Defecto

1. Con **Public-Route-Table** seleccionada, abrir la pestaña **Routes**
2. Hacer clic en **Edit routes**
3. Hacer clic en **Add route**
4. En **Destination**, escribir: `0.0.0.0/0`
5. En **Target**, desplegar y elegir: **Internet Gateway**
6. Seleccionar tu IGW: `igw-xxxxxxxxxxxxxxxx (Lab3-IGW)`

Notas:

- `0.0.0.0/0` es la **ruta por defecto** que coincide con cualquier destino IPv4 fuera del espacio local `10.0.0.0/16`
- Asegúrate de no eliminar la ruta local `10.0.0.0/16` $\rightarrow$ *local*
- `Si ves IPv6 habilitado en tu VPC, la ruta por defecto IPv6 sería ::/0 (no aplica en este lab)`

4.4.3. 4.3 Guardar Cambios

1. Verificar que ahora ves dos rutas:
   - `10.0.0.0/16` $\rightarrow$ *local*
   - `0.0.0.0/0` $\rightarrow$ $igw - xxxxxxxxxxxxxxxx$
2. Hacer clic en **Save changes**
3. Esperar confirmación (banner verde)

4.4.4. 4.4 Verificar Auto-asignación de IP Pública en Subredes

1. Ir a **Subnets** en el panel izquierdo
2. Abrir `Public-Subnet-1A` → *pestaña***Details**
2. Confirmar: **Auto-assign public IPv4 address** = `Yes`
3. Repetir para `Public-Subnet-1B`
4. Si alguna dice `No`:
   - Hacer clic en **Edit subnet settings**
   - Marcar **Enable auto-assign public IPv4 address**
   - Guardar cambios

Resultado esperado: Las subredes públicas ahora tienen una ruta por defecto a internet y asignarán IP pública a futuras instancias.

4.5 Paso 5: Verificación de la Configuración

Objetivo: Confirmar que la VPC, el IGW y las tablas de rutas quedaron correctamente configurados sin afectar las subredes privadas.

4.5.1. 5.1 Verificar Rutas en la Tabla Pública

1. En **Route Tables** → *seleccionar***Public-Route-Table**
1. Pestaña **Routes**: confirmar presencia de `0.0.0.0/0` → *igw* – ...
1. `Pestaña Subnet associations: confirmar subredes públicas asociadas`

4.5.2. 5.2 Verificar la Tabla Privada No Cambió

1. Seleccionar **Private-Route-Table**
2. Pestaña **Routes**: debe tener SOLO `10.0.0.0/16` → *local*

2. `No debe existir 0.0.0.0/0 en esta tabla`

3. `Pestaña Subnet associations: confirmar que están Private-Subnet-1A y Private-Subnet`

4.5.3. 5.3 Verificar Adjunto del IGW

1. Ir a **Internet Gateways**
2. Seleccionar `Lab3-IGW`
3. Confirmar: **State** = `attached` y **VPC** = `Lab2-VPC`

4.5.4. 5.4 Verificaciones Adicionales Recomendadas

- **Reachability Analyzer (opcional):** Puedes crear un análisis desde una IP pública hipotética hacia una instancia en subred pública (se usará en Lab 4)
- **Flujos esperados:** Tráfico desde subred pública hacia internet debe salir por IGW; desde internet hacia IP pública de una instancia regresará por IGW
- **Costos:** Sin instancias corriendo, el costo permanece $0,00

Estado actual:

- Subredes públicas listas para conectividad a internet
- Subredes privadas siguen aisladas (sin ruta por defecto)
- Preparado para lanzar EC2 en Lab 4 y probar conectividad real

4.6 Paso 6: Documentación y Limpieza (Opcional)

Recomendado:

- Registrar IDs: `VPC ID`, `IGW ID`, `Route Table IDs`
- Dibujar un pequeño diagrama del flujo: Subred pública → IGW → Internet
- Anotar decisiones: por qué solo las subredes públicas tienen ruta por defecto

NO eliminar: Este IGW y las rutas se utilizarán en el Laboratorio 4 para probar conectividad de instancias EC2.

5 Cuestionario

5.1 Instrucciones

Responde las siguientes preguntas basándote en los conceptos y procedimientos desarrollados en este laboratorio. Selecciona la opción correcta para cada pregunta de opción múltiple.

5.2 Preguntas

1. **¿Cuál es la función principal del Internet Gateway (IGW) en una VPC de AWS?**

   a) Solo permite tráfico saliente desde la VPC hacia internet
   b) Únicamente maneja la traducción de direcciones IP privadas
   c) Permite comunicación bidireccional entre instancias en VPC e internet
   d) Funciona como firewall entre subredes públicas y privadas

2. **¿Qué ocurre cuando AWS crea un Internet Gateway?**

   a) Se crea automáticamente adjunto a la VPC especificada
   b) Se crea en estado "detachedz debe adjuntarse manualmente a una VPC
   c) Se asocia automáticamente con todas las subredes de la región
   d) Requiere configuración de hardware específico

3. **¿Cuántos Internet Gateways puede tener una VPC simultáneamente?**

   a) Ilimitados
   b) Hasta 5 por región
   c) Solo 1 (relación 1:1)
   d) Depende del plan de AWS utilizado

4. **¿Qué significa la ruta "0.0.0.0/0.en una tabla de enrutamiento?**

   a) Ruta solo para direcciones IP locales
   b) Bloqueo de todo el tráfico externo
   c) Ruta por defecto que coincide con cualquier destino IPv4 no especificado
   d) Configuración exclusiva para IPv6

5. **Para que una subred sea funcionalmente "pública", ¿cuáles condiciones son OBLIGATORIAS?**

   a) Solo tener Internet Gateway adjunto a la VPC

b) IGW adjunto + ruta 0.0.0.0/0 al IGW + auto-asignación IP pública habilitada
c) Solo configurar auto-asignación de IP pública
d) Únicamente agregar la ruta por defecto

6. **¿Qué tipo de traducción de direcciones realiza automáticamente el Internet Gateway?**

a) Solo NAT para tráfico saliente
b) NAT bidireccional entre IP privadas de instancias e IP públicas
c) Únicamente enrutamiento sin traducción
d) Solo para protocolos HTTP/HTTPS

7. **¿Cuál es el costo de utilizar un Internet Gateway en AWS?**

a) $0.05 por hora de uso
b) $0.00 - El IGW es completamente gratuito
c) $0.10 por GB de datos procesados
d) Varía según la región

8. **¿Qué sucede si una instancia EC2 en subred pública ejecuta el comando ïfconfig¿**

a) Muestra tanto la IP privada como la IP pública
b) Solo muestra la IP privada; la IP pública es gestionada por AWS externamente
c) Solo muestra la IP pública
d) Muestra error porque no tiene conectividad

9. **¿Cuál es la diferencia principal entre Internet Gateway y NAT Gateway?**

a) No hay diferencia, son sinónimos
b) IGW permite tráfico bidireccional; NAT Gateway solo permite salida
c) NAT Gateway es más barato que IGW
d) IGW solo funciona con IPv6

10. **¿Qué debe hacer una subred privada para acceder a internet?**

a) Agregar ruta 0.0.0.0/0 apuntando al Internet Gateway
b) Usar NAT Gateway en subred pública (no implementado en este lab)
c) Habilitar auto-asignación de IP pública
d) Las subredes privadas nunca pueden acceder a internet

11. **¿En qué orden se debe realizar la configuración completa de conectividad internet?**

a) Rutas primero, luego crear IGW, finalmente adjuntar a VPC

b) Crear IGW, adjuntarlo a VPC, modificar tabla de rutas, verificar auto-assign IP

c) Solo crear el IGW es suficiente

d) Modificar rutas, crear subredes, luego IGW

12. **¿Qué arquitectura de seguridad recomienda AWS para aplicaciones en producción?**

a) Todas las instancias en subredes públicas para máximo rendimiento

b) Separación: load balancers/bastion en públicas, aplicaciones/DB en privadas

c) Solo usar subredes privadas sin conectividad externa

d) Colocar todo en una sola subred para simplificar

13. **¿Cuál es la configuración de la tabla de enrutamiento después de completar este laboratorio?**

a) Ambas tablas (pública y privada) tienen ruta 0.0.0.0/0

b) Solo tabla pública tiene 0.0.0.0/0 → IGW; privada solo tiene ruta local

c) Solo la tabla privada tiene ruta por defecto

d) No se modifican las rutas, solo se crea el IGW

14. **¿Qué verificaciones son esenciales al finalizar la configuración del Internet Gateway?**

a) Solo verificar que el IGW esté en estado .ªttached"

b) IGW attached, rutas correctas en tabla pública, tabla privada intacta, auto-assign IP habilitado

c) Únicamente verificar conectividad lanzando instancias EC2

d) Solo confirmar que no hay errores de facturación

15. **¿Por qué es importante mantener los recursos del Lab 3 para el Lab 4?**

a) Para evitar costos adicionales de recreación

b) Porque el Lab 4 utilizará esta conectividad para probar instancias EC2

c) Los recursos se eliminan automáticamente

d) No es necesario mantenerlos

5.3 Respuestas

1. **Respuesta: c)** Permite comunicación bidireccional entre instancias en VPC e internet

   Justificación: El Internet Gateway es un componente que permite tanto tráfico entrante (desde internet hacia instancias con IP pública) como saliente (desde instancias hacia internet). Realiza NAT automáticamente y proporciona conectividad completa, no solo en una dirección como los NAT Gateways.

2. **Respuesta: b)** Se crea en estado "detachedz debe adjuntarse manualmente a una VPC

   Justificación: El IGW se crea como recurso independiente en estado "detachedz debe ser explícitamente adjuntado a una VPC mediante la acción .ªttach to VPC". Esta separación permite flexibilidad en la gestión de recursos.

3. **Respuesta: c)** Solo 1 (relación 1:1)

   Justificación: AWS establece una relación 1:1 entre VPC e Internet Gateway. Una VPC solo puede tener un IGW adjunto, y un IGW solo puede estar asociado a una VPC. Esta restricción simplifica el enrutamiento y mejora la seguridad.

4. **Respuesta: c)** Ruta por defecto que coincide con cualquier destino IPv4 no especificado

   Justificación: La ruta "0.0.0.0/0.ᵉˢ la ruta por defecto que captura todo el tráfico destinado a direcciones IP que no coinciden con otras rutas más específicas en la tabla. Es esencial para enviar tráfico a internet.

5. **Respuesta: b)** IGW adjunto + ruta 0.0.0.0/0 al IGW + auto-asignación IP pública habilitada

   Justificación: Una subred pública requiere TODAS estas condiciones: (1) IGW adjunto a la VPC, (2) tabla de enrutamiento con ruta 0.0.0.0/0 apuntando al IGW, y (3) auto-asignación de IP pública habilitada. Sin cualquiera de estos elementos, no funcionará como pública.

6. **Respuesta: b)** NAT bidireccional entre IP privadas de instancias e IP públicas

   Justificación: El IGW realiza NAT automático en ambas direcciones: traduce IP privada a pública para tráfico saliente, y IP pública a privada para tráfico entrante. Este proceso es transparente para las instancias.

7. **Respuesta: b)** $0.00 - El IGW es completamente gratuito

   Justificación: El Internet Gateway no tiene costo alguno. AWS solo cobra por transferencia de datos (primeros 100 GB/mes gratuitos, luego $0.09/GB para datos salientes). El IGW en sí, su creación y mantenimiento son gratuitos.

8. **Respuesta: b)** Solo muestra la IP privada; la IP pública es gestionada por AWS externamente

   Justificación: La instancia EC2 solo çonoce"su IP privada. La IP pública existe solo en la infraestructura de AWS y es utilizada por el IGW para realizar NAT. La instancia nunca ve su IP pública en sus interfaces de red.

9. **Respuesta: b)** IGW permite tráfico bidireccional; NAT Gateway solo permite salida

   Justificación: Internet Gateway permite tráfico entrante y saliente (bidireccional), mientras NAT Gateway solo permite tráfico saliente desde subredes privadas. IGW es gratuito, NAT Gateway cuesta $0.045/hora + $0.045/GB.

10. **Respuesta: b)** Usar NAT Gateway en subred pública (no implementado en este lab)

    Justificación: Las subredes privadas mantienen su privacidad usando NAT Gateway ubicado en una subred pública. Esto permite salida a internet sin exposición de retorno. Agregar ruta directa al IGW las convertiría en públicas.

11. **Respuesta: b)** Crear IGW, adjuntarlo a VPC, modificar tabla de rutas, verificar auto-assign IP

    Justificación: El orden correcto es: (1) crear IGW independiente, (2) adjuntarlo a VPC específica, (3) agregar ruta 0.0.0.0/0 en tabla pública, (4) verificar auto-asignación IP en subredes públicas. Seguir este orden evita errores de dependencias.

12. **Respuesta: b)** Separación: load balancers/bastion en públicas, aplicaciones/DB en privadas

    Justificación: AWS recomienda arquitectura de defensa en profundidad: exponer solo lo necesario (load balancers, bastion hosts) en subredes públicas, mantener aplicaciones y bases de datos en subredes privadas para minimizar superficie de ataque.

13. **Respuesta: b)** Solo tabla pública tiene 0.0.0.0/0 → IGW; privada solo tiene ruta local

    Justificación: Public-Route-Table queda con dos rutas: 10.0.0.0/16 → local y 0.0.0.0/0 → IGW. Private-Route-Table mantiene solo 10.0.0.0/16 → local, preservando la privacidad de las subredes asociadas.

14. **Respuesta: b)** IGW attached, rutas correctas en tabla pública, tabla privada intacta, auto-assign IP habilitado

    Justificación: Una verificación completa incluye: (1) IGW en estado .ªttached", (2) ruta 0.0.0.0/0 presente solo en tabla pública, (3) tabla privada sin cambios, (4) auto-asignación IP habilitada en subredes públicas, (5) costo mantenido en $0.00.

15. **Respuesta: b)** Porque el Lab 4 utilizará esta conectividad para probar instancias EC2

    Justificación: La infraestructura creada (IGW + rutas configuradas) será la base para el Lab 4, donde se lanzarán instancias EC2 en subredes públicas y privadas para probar la conectividad real a internet. Eliminar estos recursos requeriría reconfigurarlos.

6 Conclusiones

6.1 Logros Alcanzados

Al completar este laboratorio, hemos logrado implementar exitosamente la conectividad a internet para una Amazon VPC, transformando subredes aisladas en infraestructura de red funcional capaz de soportar aplicaciones web y servicios accesibles públicamente. Los principales logros incluyen:

- **Configuración completa de Internet Gateway:** Creación, adjunto y verificación de un IGW funcional asociado a la VPC del Lab 2, estableciendo la puerta de enlace necesaria para comunicación bidireccional con internet.
- **Implementación de enrutamiento diferenciado:** Configuración exitosa de tablas de enrutamiento que distinguen claramente entre subredes públicas (con ruta 0.0.0.0/0 hacia IGW) y privadas (solo ruta local), manteniendo la segregación de red apropiada.
- **Comprensión de NAT automático:** Dominio del concepto de traducción de direcciones de red implementado transparentemente por AWS, donde las instancias mantienen IPs privadas mientras el IGW gestiona la comunicación externa.
- **Verificación de configuración sin costos:** Completación de todas las verificaciones necesarias mantieniendo el laboratorio en $0.00, demostrando eficiencia en el uso de recursos del nivel gratuito.

6.2 Competencias Desarrolladas

Competencias Técnicas Adquiridas:

- **Gestión de componentes de conectividad:** Capacidad para crear, configurar y gestionar Internet Gateways como componentes críticos de arquitecturas de nube escalables y seguras.
- **Administración avanzada de enrutamiento:** Habilidad para diseñar, implementar y verificar tablas de enrutamiento complejas que soporten arquitecturas multi-tier con separación público/privado.
- **Comprensión de direccionamiento IP:** Dominio profundo de la diferencia entre direcciones IP públicas y privadas, incluyendo su gestión automática por parte de AWS y las implicaciones para el diseño de aplicaciones.
- **Análisis de flujos de tráfico:** Capacidad para trazar y entender el camino completo que sigue el tráfico de red desde instancias hacia internet y viceversa, identificando cada punto de traducción y enrutamiento.
- **Verificación de conectividad:** Desarrollo de metodologías sistemáticas para verificar configuraciones de red antes del despliegue de recursos computacionales, reduciendo errores y troubleshooting posterior.

Competencias Profesionales Fortalecidas:

- **Toma de decisiones arquitectónicas:** Capacidad para determinar cuándo y cómo exponer recursos a internet, balanceando accesibilidad con requisitos de seguridad organizacional.
- **Implementación de mejores prácticas:** Aplicación consistente de principios de defensa en profundidad, manteniendo recursos sensibles en capas privadas mientras se habilita conectividad necesaria.
- **Documentación técnica:** Desarrollo de habilidades para documentar configuraciones de red complejas, incluyendo IDs de recursos, flujos de tráfico y decisiones de diseño.
- **Gestión de costos:** Comprensión profunda del modelo de costos de AWS para componentes de red, optimizando configuraciones para minimizar gastos sin comprometer funcionalidad.

6.3 Integración con el Ecosistema de Laboratorios

Este laboratorio constituye un eslabón crítico en la secuencia de aprendizaje diseñada:
Consolidación de conocimientos previos:

- Utilización efectiva de la infraestructura IAM establecida en el Lab 1 para gestión segura de recursos
- Aprovechamiento completo de la arquitectura VPC multi-AZ creada en el Lab 2 como base para conectividad externa
- Aplicación práctica de conceptos de redes aprendidos en laboratorios anteriores

Preparación para laboratorios futuros:

- **Lab 4 - Instancias EC2:** La conectividad establecida permitirá desplegar y probar servidores web accesibles desde internet
- **Lab 5 - Seguridad Avanzada:** La separación público/privada configurada será base para implementar Security Groups y NACLs
- **Labs 6-8:** La arquitectura de conectividad soportará patrones avanzados como VPC Peering, monitoreo con CloudWatch, y proyectos de integración

6.4 Consideraciones de Seguridad y Mejores Prácticas

La implementación realizada incorpora principios fundamentales de seguridad de redes:

- **Principio de menor privilegio:** Solo las subredes que requieren acceso público tienen ruta al IGW, manteniendo recursos sensibles aislados
- **Segregación de capas:** Separación clara entre capa de presentación (subredes públicas) y capas de aplicación/datos (subredes privadas)
- **Preparación para defensa en profundidad:** Arquitectura lista para implementar múltiples capas de seguridad en laboratorios posteriores
- **Auditoría y trazabilidad:** Configuración documentada que permite auditoría de cambios y troubleshooting sistemático

6.5 Impacto en el Desarrollo Profesional

La completación de este laboratorio contribuye significativamente al perfil profesional en tecnologías de nube:

- **Competencias en demanda:** Las habilidades de configuración de conectividad AWS son altamente valoradas en el mercado laboral actual
- **Fundamentos sólidos:** Comprensión profunda de conceptos que trascienden AWS y se aplican a otras plataformas de nube
- **Experiencia práctica:** Experiencia hands-on con herramientas y procesos utilizados en entornos empresariales reales
- **Preparación para certificaciones:** Conocimientos directamente aplicables a exámenes de certificación AWS como Solutions Architect Associate

6.6 Reflexión Final

Este laboratorio demuestra cómo la correcta implementación de componentes de conectividad fundamenta arquitecturas de nube robustas y escalables. La transformación de una VPC aislada en infraestructura con conectividad internet controlada ilustra la potencia de AWS para soportar aplicaciones empresariales complejas.

La experiencia adquirida en la gestión de Internet Gateways, tablas de enrutamiento y arquitecturas de red diferenciadas proporciona una base sólida para el desarrollo de soluciones de nube más sofisticadas. La metodología sistemática aplicada - desde la planificación inicial hasta la verificación final - establece patrones de trabajo que serán invaluables en proyectos profesionales futuros.

La preparación cuidadosa para laboratorios subsecuentes asegura una progresión de aprendizaje coherente, donde cada componente construye sobre conocimientos anteriores mientras introduce nuevas capacidades técnicas. Esta aproximación holística al aprendizaje de tecnologías de nube refleja las mejores prácticas de la industria y prepara para desafíos del mundo real en arquitectura y administración de sistemas distribuidos.

7 Referencias

7.1 Documentación Oficial de AWS

- Amazon Web Services. (2024). *Internet Gateways - Amazon VPC User Guide.* Documentación oficial de AWS. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html
- Amazon Web Services. (2024). *Route Tables - Amazon VPC User Guide.* Documentación oficial de AWS. https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html
- Amazon Web Services. (2024). *Subnets for your VPC - Amazon VPC User Guide.* https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html
- Amazon Web Services. (2024). *Security Groups for your VPC - Amazon VPC User Guide.* https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html
- Amazon Web Services. (2024). *AWS Free Tier - VPC Pricing.* https://aws.amazon.com/vpc/pricing/
- Amazon Web Services. (2024). *AWS Well-Architected Framework - Security Pillar.* https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/
- Amazon Web Services. (2024). *VPC Flow Logs - Amazon VPC User Guide.* https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

7.2 Estándares y RFCs de Red

- Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). *RFC 1918 - Address Allocation for Private Internets.* Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc1918
- Postel, J. (1981). *RFC 791 - Internet Protocol - DARPA Internet Program Protocol Specification.* Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc791
- Srisuresh, P., & Holdrege, M. (1999). *RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations.* Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc2663
- Fuller, V., Li, T., Yu, J., & Varadhan, K. (1993). *RFC 1519 - Classless Inter-Domain Routing (CIDR).* Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc1519

7.3 Libros y Recursos Académicos

- Wittig, A., & Wittig, M. (2022). *Amazon Web Services in Action, Third Edition.* Manning Publications. Capítulos 6-8: VPC, Subredes, y Conectividad.

- Piper, B., & Clinton, D. (2020). *AWS Certified Solutions Architect Study Guide: Associate (SAA-C02) Exam.* Sybex. Capítulo 4: VPC y Redes.
- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach, 8th Edition.* Pearson. Capítulos 4-5: Capa de Red y Enrutamiento.
- Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks, 6th Edition.* Pearson. Capítulo 5: La Capa de Red.
- García-Martínez, A., & Burriel, V. (2019). *Redes de Computadoras y Arquitecturas de Comunicación.* Editorial Paraninfo. Capítulo 8: Interconexión de Redes.

7.4 Artículos y Whitepapers Técnicos

- Amazon Web Services. (2023). *AWS Architecture Center - VPC Connectivity Options Whitepaper.* https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-optio
- Amazon Web Services. (2023). *Security Best Practices for Amazon VPC.* AWS Security Blog. https://aws.amazon.com/blogs/security/
- Varia, J., & Mathew, S. (2014). *Overview of Amazon Web Services - AWS Whitepaper.* Amazon Web Services. Sección: Redes y Entrega de Contenido.
- NIST. (2020). *SP 800-145 - The NIST Definition of Cloud Computing.* National Institute of Standards and Technology. Consideraciones de Seguridad de Red.

7.5 Herramientas y Recursos de Laboratorio

- AWS CLI Documentation. (2024). *VPC Commands Reference.* https://docs.aws.amazon.com/cli/latest/reference/ec2/
- AWS CloudFormation. (2024). *VPC Resource Templates.* https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-vpc.html
- Terraform AWS Provider. (2024). *VPC Resources Documentation.* HashiCorp. https://registry.terraform.io/providers/hashicorp/aws/latest/docs/resources/vpc
- AWS Cost Calculator. (2024). *VPC and Data Transfer Pricing Calculator.* https://calculator.aws/

7.6 Recursos de Certificación y Aprendizaje

- AWS Training and Certification. (2024). *AWS Certified Solutions Architect - Associate Exam Guide.* Dominio 3: Diseño de Arquitecturas Seguras.
- AWS Training and Certification. (2024). *AWS Certified Advanced Networking - Specialty Exam Guide.* Dominios de Conectividad Híbrida.
- Linux Academy / A Cloud Guru. (2024). *AWS Networking Deep Dive Course.* Módulos de VPC y Conectividad.

- AWS re:Invent Sessions. (2023). *Advanced VPC Design and Implementation.* Sesiones técnicas de conferencia anual.

7.7 Recursos de Troubleshooting y Monitoreo

- AWS Support. (2024). *VPC Connectivity Troubleshooting Guide.* https://aws.amazon.com/premiumsupport/knowledge-center/
- AWS CloudWatch. (2024). *VPC Flow Logs Analysis and Monitoring.* https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/
- AWS X-Ray. (2024). *Distributed Network Tracing for VPC Applications.* https://docs.aws.amazon.com/xray/
- AWS Config. (2024). *VPC Configuration Compliance and Auditing.* https://docs.aws.amazon.com/config/

Nota: Todas las URLs fueron verificadas como activas al momento de la elaboración de este laboratorio (octubre 2025). La documentación oficial de AWS se actualiza regularmente; se recomienda consultar las versiones más recientes para obtener información actualizada sobre nuevas funcionalidades y mejores prácticas.