Laboratorio #2

Amazon VPC - Redes Virtuales Privadas

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: 60-90 minutos
Costo: \$0.00 (100 % Gratuito)

Septiembre 2025
Elaborado: 28 de septiembre de 2025

Índice

Resumen

Este laboratorio introduce los conceptos fundamentales de Amazon Virtual Private Cloud (VPC), el servicio de red virtual de AWS que permite crear una red lógicamente aislada en la nube. A través de actividades prácticas completamente textuales, los estudiantes aprenderán a diseñar, configurar y gestionar redes virtuales privadas utilizando exclusivamente servicios del nivel gratuito de AWS.

El laboratorio cubre la arquitectura de VPC, incluyendo bloques CIDR (Classless Inter-Domain Routing), subredes públicas y privadas, tablas de enrutamiento, y la distribución de recursos en múltiples Zonas de Disponibilidad para alta disponibilidad. Los participantes comprenderán cómo VPC proporciona control total sobre el entorno de red virtual, permitiendo definir rangos de direcciones IP, crear subredes, y configurar rutas de red.

Se enfatiza la diferencia entre subredes públicas (con acceso a internet) y subredes privadas (sin acceso directo a internet), preparando el terreno para laboratorios posteriores donde se implementarán Internet Gateways, instancias EC2, y configuraciones de seguridad avanzadas. Este laboratorio es fundamental porque VPC es el componente base de casi cualquier arquitectura en AWS, y comprender su funcionamiento es esencial para diseñar soluciones escalables y seguras.

Los estudiantes aplicarán conocimientos de redes tradicionales (direccionamiento IP, subnetting, enrutamiento) en el contexto de infraestructura definida por software (SDN) en la nube. Al finalizar, habrán creado una VPC completamente funcional con subredes distribuidas geográficamente, tablas de enrutamiento configuradas, y comprenderán cómo esta infraestructura se integra con otros servicios de AWS.

Palabras clave: Amazon VPC, Virtual Private Cloud, CIDR, Subnetting, Subredes Públicas, Subredes Privadas, Tablas de Enrutamiento, Zonas de Disponibilidad, Redes Virtuales, Infraestructura como Código.

Duración estimada: 60-90 minutos.

Costo: $0.00 USD (Free Tier).

1 Objetivos

1.1 Objetivo General

Diseñar, crear y configurar una Amazon Virtual Private Cloud (VPC) con arquitectura multi-zona de disponibilidad, implementando subredes públicas y privadas con sus respectivas tablas de enrutamiento, aplicando principios de diseño de redes para construir una infraestructura de red escalable, segura y de alta disponibilidad en AWS, sentando las bases para el despliegue de aplicaciones y servicios en la nube.

1.2 Objetivos Específicos

- **Comprender los fundamentos de Amazon VPC:** Estudiar la arquitectura de redes virtuales en AWS, incluyendo el modelo de aislamiento lógico, la integración con la infraestructura global de AWS (regiones y zonas de disponibilidad), y las ventajas de VPC frente a modelos de red tradicionales.
- **Dominar el direccionamiento CIDR y subnetting:** Aplicar conocimientos de notación CIDR para definir rangos de direcciones IP privadas según RFC 1918, calcular máscaras de subred, determinar capacidad de hosts por subred, y planificar el crecimiento futuro de la red considerando la escalabilidad.
- **Crear una VPC personalizada en AWS:** Implementar una VPC desde cero utilizando la consola de AWS, especificando bloques CIDR primarios, configurando opciones de DNS, y entendiendo las diferencias entre VPC por defecto y VPC personalizadas.
- **Diseñar arquitectura de subredes multi-AZ:** Crear subredes distribuidas en al menos dos Zonas de Disponibilidad, diferenciando entre subredes públicas (con potencial acceso a internet) y subredes privadas (sin acceso directo a internet), aplicando principios de alta disponibilidad y tolerancia a fallos.
- **Configurar tablas de enrutamiento:** Crear y configurar tablas de enrutamiento personalizadas, entender rutas locales automáticas, asociar subredes a tablas de enrutamiento específicas, y comprender cómo el tráfico de red fluye dentro de una VPC.
- **Aplicar mejores prácticas de diseño de redes en la nube:** Implementar convenciones de nomenclatura consistentes, documentar decisiones de diseño, utilizar etiquetas (tags) para organizar recursos, y planificar arquitecturas de red escalables que soporten crecimiento futuro.
- **Verificar conectividad y configuración de red:** Validar que las subredes estén correctamente configuradas, verificar asociaciones de tablas de enrutamiento, confirmar distribución geográfica de recursos, y entender cómo diagnosticar problemas de configuración de red.
- **Preparar infraestructura para servicios futuros:** Construir la base de red sobre la cual se desplegarán instancias EC2, balanceadores de carga, bases de datos, y otros servicios en laboratorios posteriores, entendiendo cómo VPC es el fundamento de cualquier arquitectura en AWS.

1.3 Competencias a Desarrollar

Competencias Técnicas:

- Diseño y arquitectura de redes virtuales en entornos de nube pública
- Cálculo y aplicación de direccionamiento IP con notación CIDR
- Configuración de infraestructura de red definida por software (SDN)
- Implementación de arquitecturas de alta disponibilidad multi-zona
- Gestión de tablas de enrutamiento y flujos de tráfico de red
- Uso eficiente de la consola de administración de AWS para servicios de red
- Aplicación de etiquetado y organización de recursos en la nube

Competencias Profesionales:

- Planificación de infraestructura escalable considerando crecimiento futuro
- Documentación técnica de decisiones de diseño de arquitectura
- Aplicación de estándares de la industria (RFC 1918, mejores prácticas de AWS)
- Pensamiento sistémico para entender dependencias entre componentes de red
- Resolución de problemas de configuración de red en entornos de nube
- Toma de decisiones arquitectónicas balanceando simplicidad, costo y rendimiento

2 Marco Teórico

2.1 ¿Qué es Amazon VPC?

2.1.1. Definición y Concepto

Amazon Virtual Private Cloud (VPC) es un servicio de red virtual que te permite crear una red lógicamente aislada dentro de la nube de AWS. Es tu red privada.[en] AWS, donde tienes control total sobre la configuración de red, similar a operar una red tradicional en tu propio centro de datos, pero con los beneficios de escalabilidad y flexibilidad de la infraestructura de AWS.

Una VPC te permite:

- Definir tu propio rango de direcciones IP usando notación CIDR
- Crear subredes en diferentes Zonas de Disponibilidad
- Configurar tablas de enrutamiento para controlar el flujo de tráfico
- Conectar tu VPC a internet, a tu red corporativa, o a otras VPCs
- Aplicar múltiples capas de seguridad (Security Groups, Network ACLs)
- Alojar recursos de AWS (EC2, RDS, Lambda) en un entorno de red controlado

2.1.2. Analogía con Redes Tradicionales

Si tienes experiencia con redes tradicionales, puedes pensar en VPC de la siguiente manera:

- **VPC** ≡ Tu red empresarial completa con un rango IP privado
- **Subred** ≡ Segmentos de red (VLANs) dentro de tu red empresarial
- **Tabla de enrutamiento** ≡ Router que dirige tráfico entre subredes
- **Internet Gateway** ≡ Router de borde que conecta tu red a internet
- **Security Group** ≡ Firewall a nivel de instancia (stateful)
- **Network ACL** ≡ Firewall a nivel de subred (stateless)

La diferencia clave es que en VPC, toda esta infraestructura es **virtual** y se configura mediante software, no hardware físico.

2.1.3. VPC por Defecto vs VPC Personalizada

Cuando creas una cuenta de AWS, cada región viene con una **VPC por defecto (Default VPC)** preconfigurada:

Características de VPC por Defecto:

- Bloque CIDR: `172.31.0.0/16` (65,536 direcciones IP)
- Una subred pública por cada Zona de Disponibilidad en la región
- Internet Gateway adjunto (permite acceso a internet)
- Tablas de enrutamiento preconfiguradas
- Ideal para comenzar rápidamente sin configuración de red
- Todos los recursos tienen acceso a internet por defecto

Características de VPC Personalizada:

- Tú defines el bloque CIDR (por ejemplo: `10.0.0.0/16`)
- Tú creas las subredes según tus necesidades
- Control total sobre enrutamiento y conectividad
- Mayor seguridad (nada tiene acceso a internet hasta que lo configures)
- Recomendada para entornos de producción
- Permite implementar arquitecturas complejas

En este laboratorio crearemos una **VPC personalizada** para aprender todos los componentes desde cero.

2.2 Componentes Fundamentales de VPC

2.2.1. Bloques CIDR (Classless Inter-Domain Routing)

CIDR es la notación moderna para representar rangos de direcciones IP. Usa el formato:

`dirección_IP/máscara_de_prefijo`

Ejemplos:

- `10.0.0.0/16` → 65,536 direcciones IP (10.0.0.0 a 10.0.255.255)
- `10.0.1.0/24` → 256 direcciones IP (10.0.1.0 a 10.0.1.255)
- `10.0.1.0/28` → 16 direcciones IP (10.0.1.0 a 10.0.1.15)

Rango CIDR	Direcciones IP	Uso Común
10.0.0.0/8	16,777,216	Redes empresariales grandes
172.16.0.0/12	1,048,576	Redes medianas (AWS Default VPC usa 172.31.0.0/16)
192.168.0.0/16	65,536	Redes pequeñas (hogares, oficinas)

Cuadro 1: Rangos de direcciones IP privadas según RFC 1918

Rangos IP Privados (RFC 1918):
Estos son los rangos que puedes usar libremente en tu VPC sin conflictos con internet público:

Cálculo de Direcciones Disponibles:
La máscara de prefijo determina cuántas direcciones IP tienes:

- $/16 \rightarrow 2^{32-16} = 2^{16} = 65,536$ direcciones
- $/20 \rightarrow 2^{32-20} = 2^{12} = 4,096$ direcciones
- $/24 \rightarrow 2^{32-24} = 2^{8} = 256$ direcciones
- $/28 \rightarrow 2^{32-28} = 2^{4} = 16$ direcciones

Importante: AWS reserva 5 direcciones IP en cada subred:

- Primera dirección: dirección de red (por ejemplo, 10.0.1.0)
- Segunda dirección: reservada para el router de VPC (10.0.1.1)
- Tercera dirección: reservada para DNS de AWS (10.0.1.2)
- Cuarta dirección: reservada para uso futuro (10.0.1.3)
- Última dirección: dirección de broadcast de red (10.0.1.255)

Por lo tanto, en una subred /24 (256 direcciones), solo tienes 251 direcciones IP utilizables para instancias EC2, bases de datos, etc.

2.2.2. Subredes (Subnets)

Una **subred** es un segmento del rango de direcciones IP de tu VPC. Cada subred:

- Debe residir completamente dentro de una Zona de Disponibilidad (AZ)
- No puede abarcar múltiples AZs
- Tiene su propio bloque CIDR (subconjunto del CIDR de la VPC)
- Puede ser pública o privada según su tabla de enrutamiento

Tipos de Subredes:

1. **Subred Pública:**

- Tiene una ruta a un Internet Gateway en su tabla de enrutamiento
- Los recursos pueden recibir direcciones IP públicas
- Ejemplo de uso: servidores web, balanceadores de carga
- Tráfico saliente puede llegar a internet

2. **Subred Privada:**

- NO tiene ruta directa a Internet Gateway
- Los recursos no tienen direcciones IP públicas
- Ejemplo de uso: bases de datos, servidores de aplicación backend
- Solo puede comunicarse dentro de la VPC (o mediante NAT Gateway)

Planificación de Subredes - Ejemplo Práctico:
Si tienes una VPC con CIDR `10.0.0.0/16`, podrías dividirla así:

Subred	**CIDR**	**Tipo**	**AZ**
Subred Pública 1	10.0.1.0/24	Pública	us-east-1a
Subred Pública 2	10.0.2.0/24	Pública	us-east-1b
Subred Privada 1	10.0.11.0/24	Privada	us-east-1a
Subred Privada 2	10.0.12.0/24	Privada	us-east-1b

Cuadro 2: Ejemplo de distribución de subredes multi-AZ

Este diseño proporciona:

- Alta disponibilidad (recursos en 2 AZs)
- Separación entre capa pública (web) y privada (base de datos)
- Espacio para crecer (muchos rangos /24 sin usar aún)

2.2.3. Tablas de Enrutamiento (Route Tables)

Una **tabla de enrutamiento** contiene un conjunto de reglas (rutas) que determinan hacia dónde se dirige el tráfico de red desde tu subred.

Componentes de una Ruta:

- **Destination (Destino):** Rango CIDR de destino (por ejemplo, `0.0.0.0/0` = cualquier dirección)
- **Target (Objetivo):** Hacia dónde enviar el tráfico (por ejemplo, Internet Gateway, NAT Gateway, local)

Ruta Local (Local Route):
Cada tabla de enrutamiento en una VPC incluye automáticamente una ruta "local":

- **Destination:** CIDR de la VPC (por ejemplo, `10.0.0.0/16`)
- **Target:** `local`

- **Significado:** Todo el tráfico dentro de la VPC se enruta localmente
- **Importante:** Esta ruta NO se puede modificar ni eliminar

Esto significa que todas las subredes dentro de una VPC pueden comunicarse entre sí por defecto.

Tabla de Enrutamiento Principal (Main Route Table):

- Cada VPC tiene una tabla de enrutamiento principal creada automáticamente
- Por defecto, cualquier subred nueva se asocia a esta tabla
- Recomendación: dejar la tabla principal sin ruta a internet (para seguridad)
- Crear tablas de enrutamiento personalizadas para subredes públicas

Ejemplo de Tablas de Enrutamiento:
Tabla de Enrutamiento Privada:

Destination	Target	Significado
10.0.0.0/16	local	Tráfico dentro de la VPC

Cuadro 3: Tabla de enrutamiento para subred privada

Tabla de Enrutamiento Pública (agregaremos Internet Gateway en Lab 3):

Destination	Target	Significado
10.0.0.0/16	local	Tráfico dentro de la VPC
0.0.0.0/0	igw-xxxx	Tráfico a internet (Lab 3)

Cuadro 4: Tabla de enrutamiento para subred pública (futuro)

2.3 Zonas de Disponibilidad y Alta Disponibilidad

2.3.1. ¿Qué son las Zonas de Disponibilidad (AZs)?

Una **Zona de Disponibilidad (Availability Zone - AZ)** es uno o más centros de datos discretos con energía, redes y conectividad redundantes dentro de una región de AWS.

Características de las AZs:

- Cada región de AWS tiene al menos 3 AZs (algunas tienen 6+)
- Las AZs están físicamente separadas (varios kilómetros de distancia)
- Conectadas con redes de baja latencia y alto rendimiento
- Aisladas entre sí para tolerancia a fallos
- Si una AZ falla, las otras continúan operando

Nomenclatura de AZs:
Ejemplos en región `us-east-1` (Norte de Virginia):

- `us-east-1a`
- `us-east-1b`
- `us-east-1c`
- `us-east-1d`
- `us-east-1e`
- `us-east-1f`

2.3.2. Diseño Multi-AZ para Alta Disponibilidad

Principio Fundamental: Distribuir recursos en múltiples AZs para que tu aplicación siga funcionando incluso si una AZ completa falla.

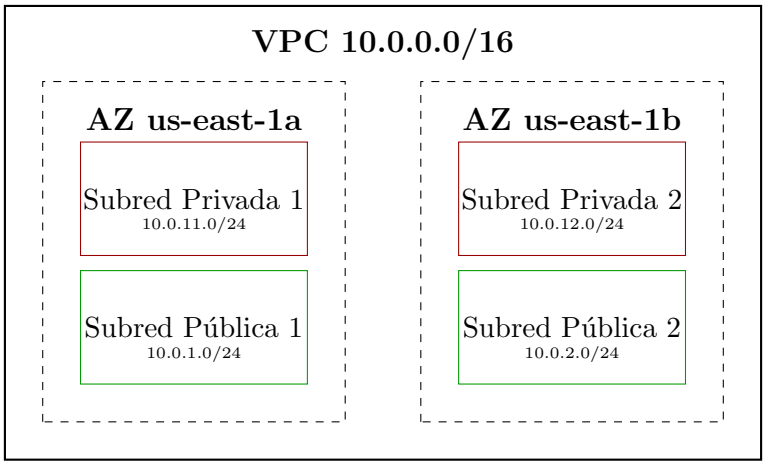
Arquitectura Recomendada:

1. **Mínimo 2 AZs:** Distribuir subredes en al menos 2 zonas de disponibilidad
2. **Simetría:** Crear subredes equivalentes en cada AZ
   - AZ-A: Subred pública + Subred privada
   - AZ-B: Subred pública + Subred privada
3. **Balanceo de carga:** Distribuir tráfico entre instancias en diferentes AZs
4. **Replicación de datos:** Bases de datos con réplicas en múltiples AZs

Beneficios del Diseño Multi-AZ:

- **Tolerancia a fallos:** Si AZ-A falla, AZ-B continúa sirviendo tráfico
- **Mantenimiento sin interrupciones:** Actualizar instancias en AZ-A mientras AZ-B atiende usuarios
- **Baja latencia:** Usuarios se conectan a la AZ más cercana
- **Cumplimiento normativo:** Algunas regulaciones exigen redundancia geográfica

Ejemplo Visual de Arquitectura Multi-AZ:



2.4 Características de VPC en AWS Free Tier

2.4.1. Costos de Amazon VPC

¡Excelente noticia! Amazon VPC es **completamente gratuito**. No hay cargos por:

- Crear VPCs
- Crear subredes
- Crear tablas de enrutamiento
- Asociar subredes a tablas de enrutamiento
- Usar direcciones IP privadas dentro de tu VPC
- Tráfico de red entre instancias en la misma VPC

Servicios relacionados que SÍ pueden generar costos:

- **NAT Gateway:** $0.045/hora + $0.045/GB procesado (NO lo usaremos en este lab)
- **VPN Connection:** $0.05/hora (NO lo usaremos)
- **Traffic Mirroring:** Tiene costo (NO lo usaremos)
- **Elastic IP no asociada:** $0.005/hora si no está en uso
- **Transferencia de datos a internet:** Primeros 100 GB/mes gratis, después $0.09/GB

En este laboratorio: Todo es `$0.00` porque solo crearemos la estructura de VPC sin servicios adicionales.

2.4.2. Límites de VPC en Free Tier

AWS tiene límites por defecto para proteger tu cuenta:
Para este laboratorio, estos límites son más que suficientes.

Recurso	Límite por Región
VPCs	5 (puede aumentarse)
Subredes por VPC	200
Tablas de enrutamiento por VPC	200
Rutas por tabla de enrutamiento	50
Internet Gateways por región	5
Elastic IPs	5
Security Groups por VPC	2,500
Reglas por Security Group	60 (entrada) + 60 (salida)
Network ACLs por VPC	200

Cuadro 5: Límites de recursos de VPC por región

2.5 Mejores Prácticas de Diseño de VPC

2.5.1. Planificación de Direccionamiento IP

1. Elegir el tamaño correcto de CIDR:

- **Demasiado pequeño** (/24, /28): Te quedarás sin IPs rápidamente
- **Demasiado grande** (/8): Desperdicia espacio, complica enrutamiento
- **Recomendado para producción:** /16 (65,536 IPs) - Balance ideal
- **Para este lab:** /16 es perfecto para aprendizaje

2. Evitar conflictos con redes existentes:
Si planeas conectar tu VPC con redes corporativas o VPNs:

- Verifica que el rango CIDR no se solape con redes existentes
- Documenta qué rangos IP usas en cada VPC
- Usa herramientas de gestión de direcciones IP (IPAM)

3. Reservar espacio para crecimiento:
No uses todos los rangos inmediatamente:

- Ejemplo: Si tienes VPC `10.0.0.0/16`, usa solo `10.0.0.0/20` inicialmente
- Deja rangos `10.0.16.0/20`, `10.0.32.0/20`, etc., para expansión futura
- Así puedes añadir nuevas subredes sin reconfigurar la arquitectura completa

2.5.2. Nomenclatura y Etiquetado

Convenciones de nombres claras:

- **VPC:** `proyecto-entorno-vpc` (ejemplo: `laboratorio-dev-vpc`)
- **Subredes públicas:** `public-subnet-az` (ejemplo: `public-subnet-1a`)
- **Subredes privadas:** `private-subnet-az` (ejemplo: `private-subnet-1a`)
- **Tablas de enrutamiento:** `tipo-rtb` (ejemplo: `public-rtb`, `private-rtb`)

Etiquetas (Tags) obligatorias:

- `Name`: Nombre descriptivo del recurso
- `Environment`: dev / staging / production
- `Project`: Nombre del proyecto
- `ManagedBy`: Terraform / CloudFormation / Manual
- `CostCenter`: Para rastreo de costos en organizaciones

2.5.3. Seguridad desde el Diseño

Principio de defensa en profundidad:

1. **Capa 1 - Subredes:** Separar recursos públicos de privados
2. **Capa 2 - Security Groups:** Firewall a nivel de instancia (stateful)
3. **Capa 3 - Network ACLs:** Firewall a nivel de subred (stateless)
4. **Capa 4 - IAM:** Control de quién puede modificar recursos de red
5. **Capa 5 - VPC Flow Logs:** Auditoría de tráfico de red

Regla de oro: Por defecto, denegar todo. Luego, permitir explícitamente solo lo necesario.

3 Requisitos Previos

3.1 Conocimientos Requeridos

Para aprovechar al máximo este laboratorio, deberías tener conocimientos básicos en:

1. **Laboratorio 1 completado:**
   - Cuenta de AWS creada y activa
   - Usuario IAM configurado con permisos de administrador
   - MFA habilitado en cuenta root y usuario IAM
   - Alertas de facturación configuradas
   - Familiaridad con la consola de AWS
2. **Fundamentos de redes TCP/IP:**
   - Direcciones IP (IPv4)
   - Máscaras de subred y notación CIDR
   - Concepto de gateway y enrutamiento
   - Diferencia entre direcciones IP públicas y privadas
   - Modelo OSI (especialmente capas 2-4)
3. **Conceptos básicos de seguridad:**
   - Firewalls y reglas de acceso
   - Principio de mínimo privilegio
   - Aislamiento de redes

3.2 Recursos Técnicos

- **Cuenta de AWS activa** con acceso al Free Tier
- **Conexión a internet** estable
- **Navegador web moderno** (Chrome, Firefox, Edge, Safari)
- **Usuario IAM** con permisos de administrador (creado en Lab 1)
- **Calculadora de subnetting** (opcional): https://www.subnet-calculator.com/
- **Papel y lápiz** (recomendado) para dibujar tu arquitectura

3.3 Verificación de Costos

Antes de comenzar, verificar:
¡Garantizado $0.00! Este laboratorio no generará ningún cargo en tu cuenta de AWS.

Servicio	Costo	Nota
Amazon VPC	$0.00	Siempre gratuito
Subredes	$0.00	Sin límite
Tablas de enrutamiento	$0.00	Sin límite
Etiquetas (Tags)	$0.00	Sin límite
TOTAL	**$0.00**	100 % Free Tier

Cuadro 6: Costos del Laboratorio 2

3.4 Tiempo Estimado

- **Lectura y comprensión de conceptos:** 20-30 minutos
- **Creación de VPC y subredes:** 15-20 minutos
- **Configuración de tablas de enrutamiento:** 10-15 minutos
- **Verificación y documentación:** 10-15 minutos
- **Cuestionario:** 10 minutos
- **TOTAL:** 60-90 minutos

3.5 Región de AWS Recomendada

Para este laboratorio, recomendamos usar:

- **Región primaria:** `us-east-1` (Norte de Virginia)
- **Razón:** Mayor cantidad de AZs disponibles (6 zonas)
- **Alternativas:** `us-west-2` (Oregón), `eu-west-1` (Irlanda)

Importante: Asegúrate de trabajar siempre en la misma región durante todo el laboratorio.

4 Procedimiento Paso a Paso

4.1 Paso 1: Planificación de la Arquitectura de Red

Objetivo: Diseñar la arquitectura de red antes de crearla en AWS.

4.1.1. 1.1 Definir Especificaciones de la VPC

Antes de crear recursos, definiremos exactamente qué vamos a construir:
Especificaciones de nuestro diseño:

1. **VPC CIDR:** `10.0.0.0/16`
   - Capacidad: 65,536 direcciones IP
   - Rango: 10.0.0.0 hasta 10.0.255.255
   - Razón: Suficientemente grande para escalar, estándar RFC 1918
2. **Cantidad de AZs:** 2 (us-east-1a y us-east-1b)
   - Proporciona alta disponibilidad
   - Cumple mejores prácticas de AWS
   - Permite balanceo de carga en futuros laboratorios
3. **Cantidad de subredes:** 4 subredes totales
   - 2 subredes públicas (una por AZ)
   - 2 subredes privadas (una por AZ)

Tabla de diseño de subredes:

Nombre	CIDR	Tipo	AZ	IPs útiles
Public Subnet 1A	10.0.1.0/24	Pública	us-east-1a	251
Public Subnet 1B	10.0.2.0/24	Pública	us-east-1b	251
Private Subnet 1A	10.0.11.0/24	Privada	us-east-1a	251
Private Subnet 1B	10.0.12.0/24	Privada	us-east-1b	251

Cuadro 7: Plan de subredes para el laboratorio

Notas sobre el diseño:

- Usamos /24 (256 IPs) para cada subred, de las cuales 251 son utilizables
- Las subredes públicas usan rangos 10.0.1.x y 10.0.2.x
- Las subredes privadas usan rangos 10.0.11.x y 10.0.12.x (separación clara)
- Quedan disponibles rangos 10.0.3-10, 10.0.13-255 para expansión futura

4.1.2. 1.2 Dibujar Diagrama de Arquitectura (Opcional pero Recomendado)

En papel o usando una herramienta digital, dibuja tu arquitectura:

1. Dibuja un rectángulo grande etiquetado "VPC 10.0.0.0/16"
2. Dentro, dibuja dos columnas verticales para las dos AZs
3. En cada AZ, dibuja dos rectángulos: uno para subred pública, otro para privada
4. Etiqueta cada subred con su CIDR
5. Añade una nota: "Internet Gateway"(lo crearemos en Lab 3)

Este diagrama te ayudará a visualizar tu red y será útil en laboratorios futuros.

4.2 Paso 2: Crear la VPC

Objetivo: Crear una VPC personalizada con el bloque CIDR planificado.

4.2.1. 2.1 Iniciar Sesión como Usuario IAM

Importante: NO uses la cuenta root. Usa tu usuario IAM administrador del Lab 1.

1. Abrir navegador web
2. Ir a la URL de inicio de sesión de IAM que guardaste en Lab 1
3. Ejemplo: `https://tu-alias.signin.aws.amazon.com/console`
4. O: `https://123456789012.signin.aws.amazon.com/console`
5. Ingresar nombre de usuario IAM (ejemplo: `admin-usuario`)
6. Ingresar contraseña
7. Si configuraste MFA, ingresar código de 6 dígitos de tu aplicación
8. Hacer clic en "Sign in"

Verificar que estás usando usuario IAM:

- En esquina superior derecha, deberías ver tu nombre de usuario
- Ejemplo: "admin-usuario @ tu-alias"
- NO debería aparecer tu correo electrónico (eso indicaría cuenta root)

4.2.2. 2.2 Verificar Región

Crucial: Asegurarte de estar en la región correcta.

1. En la barra superior derecha, ver el selector de región
2. Debería decir "N. Virginia.º el nombre de tu región elegida
3. Si está en otra región, hacer clic en el selector
4. Seleccionar ÜS East (N. Virginia) us-east-1"
5. Todas las operaciones de este lab deben ser en esta región

¿Por qué es importante la región?

- Los recursos de VPC son específicos de región
- Si cambias de región, no verás los recursos creados en otra región
- Las VPCs no se comparten entre regiones

4.2.3. 2.3 Navegar al Servicio VPC

1. En la consola de AWS, hacer clic en "Services"(esquina superior izquierda)
2. En el cuadro de búsqueda, escribir: `VPC`
3. En los resultados, hacer clic en "VPC"
4. Categoría: "Networking & Content Delivery"
5. Se abrirá el dashboard del servicio VPC

Alternativa rápida:

- Usar la barra de búsqueda global (parte superior central)
- Escribir "VPCz presionar Enter
- Hacer clic en el primer resultado

4.2.4. 2.4 Explorar el Dashboard de VPC

Vista inicial del dashboard de VPC:
Al abrir VPC por primera vez, verás:

1. **Panel izquierdo:** Menú de navegación con opciones:
   - Your VPCs
   - Subnets
   - Route Tables

- Internet Gateways
- NAT Gateways
- Security Groups
- Network ACLs
- Y más...

2. **Panel central:** Dashboard con resumen de recursos
   - Cantidad de VPCs (probablemente verás 1: la VPC por defecto)
   - Cantidad de subredes
   - Cantidad de tablas de enrutamiento
   - Gráficos de uso
3. **Botones de acción:** Çreate VPC", "Launch VPC Wizard"

Nota sobre VPC por defecto:

- Verás una VPC ya existente (Default VPC)
- CIDR: `172.31.0.0/16`
- NO la borraremos (puede ser útil para pruebas rápidas)
- Crearemos nuestra propia VPC personalizada

4.2.5. 2.5 Crear VPC Personalizada

Opción 1: Crear VPC manualmente (Recomendado para aprendizaje)
Usaremos esta opción porque nos enseña cada componente:

1. En el panel izquierdo, hacer clic en "Your VPCs"
2. En la parte superior, hacer clic en el botón naranja Çreate VPC"
3. Se abrirá el formulario de creación

Formulario de creación de VPC:

1. **Resources to create:** Seleccionar "VPC only"
   - NO seleccionar "VPC and more"(eso usa un wizard)
   - Queremos crear cada componente manualmente para aprender
2. **Name tag:** Ingresar nombre descriptivo
   - Ejemplo: `Lab2-VPC`
   - O: `Laboratorio-Redes-VPC`
   - Este nombre aparecerá en la consola para identificar tu VPC

3. **IPv4 CIDR block:** Especificar el rango de direcciones IP
   - Seleccionar ÏPv4 CIDR manual input"
   - En el campo de texto, ingresar: `10.0.0.0/16`
   - Verificar que no aparezca ningún error rojo
   - Deberías ver un mensaje indicando: "65,536 IPs available"
4. **IPv6 CIDR block:** Dejar en "No IPv6 CIDR block"
   - No usaremos IPv6 en este laboratorio
   - IPv4 es suficiente para nuestros propósitos
5. **Tenancy:** Dejar en "Default"
   - "Default- instancias comparten hardware físico (normal)
   - "Dedicated- hardware dedicado (caro, no necesario)
6. **Tags:** Agregar etiquetas 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`
   - Las etiquetas ayudan a organizar recursos en cuentas grandes

Revisar configuración antes de crear:
Verificar que los valores sean exactamente:

- Name: Lab2-VPC (o tu nombre elegido)
- IPv4 CIDR: 10.0.0.0/16
- IPv6: No IPv6 CIDR block
- Tenancy: Default
- Tags: Name, Environment, Project (al menos)

4.2.6. 2.6 Confirmar Creación de VPC

1. Hacer clic en el botón naranja Çreate VPC"(parte inferior derecha)
2. AWS procesará la solicitud (tarda 2-5 segundos)
3. Verás un banner verde de éxito: "Successfully created VPC"
4. El banner mostrará el VPC ID (ejemplo: `vpc-0a1b2c3d4e5f67890`)
5. Hacer clic en el VPC ID en el banner (es un enlace)

Vista de detalles de tu nueva VPC:
Serás redirigido a la página de detalles de tu VPC, donde verás:

- **VPC ID:** Identificador único (ejemplo: vpc-0a1b2c3d4e5f67890)
- **State:** .ªvailable"(en verde)
- **IPv4 CIDR:** 10.0.0.0/16
- **DHCP options set:** (asignado automáticamente)
- **Main route table:** (creada automáticamente)
- **Main network ACL:** (creada automáticamente)
- **DNS resolution:** Enabled (permite que instancias resuelvan nombres DNS)
- **DNS hostnames:** Disabled (podemos habilitarlo si es necesario)

¿Qué creó AWS automáticamente?
Al crear una VPC, AWS automáticamente crea:

1. **Tabla de enrutamiento principal (Main Route Table):**
   - Con una ruta local: 10.0.0.0/16 → local
   - Permite comunicación entre recursos dentro de la VPC
2. **Network ACL principal (Main Network ACL):**
   - Por defecto, permite todo el tráfico entrante y saliente
   - Es un firewall a nivel de subred (stateless)
3. **Security Group por defecto (Default Security Group):**
   - Permite tráfico entre recursos que usen este security group
   - Permite todo el tráfico saliente

Importante: NO se crean subredes automáticamente. Tendremos que crearlas manualmente.

4.2.7. 2.7 Anotar VPC ID

Muy importante para siguientes pasos:

1. Copiar el VPC ID de tu nueva VPC
2. Ejemplo: `vpc-0a1b2c3d4e5f67890`
3. Guardarlo en un documento de texto temporal
4. Lo necesitarás para crear subredes y verificar configuraciones

¿Dónde encontrar el VPC ID?

- En la página de detalles de la VPC (donde estás ahora)
- En la lista de VPCs (panel "Your VPCs")
- En la columna "VPC ID"

4.3 Paso 3: Crear Subredes

Objetivo: Crear 4 subredes (2 públicas, 2 privadas) distribuidas en 2 AZs.

4.3.1. 3.1 Navegar a la Sección de Subredes

1. En el panel izquierdo del dashboard de VPC, hacer clic en "Subnets"
2. Verás una lista de subredes existentes (probablemente de la VPC por defecto)
3. En la parte superior, hacer clic en el botón naranja Çreate subnet"

4.3.2. 3.2 Crear Primera Subred Pública (Public Subnet 1A)

Formulario de creación de subred:

1. **VPC ID:** Seleccionar tu VPC recién creada
   - Hacer clic en el campo desplegable
   - Buscar por nombre: "Lab2-VPC"
   - O buscar por VPC ID: vpc-0a1b2c3d4e5f67890
   - Seleccionar tu VPC (NO la Default VPC)
   - Verificar que muestre: "Lab2-VPC — 10.0.0.0/16"

Configuración de la subred:

1. **Subnet name:** Ingresar nombre descriptivo
   - Escribir: `Public-Subnet-1A`
   - Este nombre indica que es pública y está en AZ .ª"
2. **Availability Zone:** Seleccionar primera AZ
   - Hacer clic en el desplegable
   - Seleccionar: `us-east-1a`
   - NO seleccionar "No preference"(queremos control específico)
3. **IPv4 CIDR block:** Definir rango de direcciones
   - Ingresar: `10.0.1.0/24`
   - AWS mostrará: "256 IPs available"

- Recordar: solo 251 son realmente utilizables (AWS reserva 5)
- Verificar que el rango esté dentro de 10.0.0.0/16

4. **IPv6 CIDR block:** Dejar en "No IPv6 CIDR block"
5. **Tags:** Agregar etiquetas adicionales
   - Ya tiene tag "Nameçon valor "Public-Subnet-1A"
   - Clic en .^dd new tag"
   - Key: `Type`, Value: `Public`
   - Clic en .^dd new tag"
   - Key: `AZ`, Value: `us-east-1a`

Crear la subred:

1. Revisar todos los valores:
   - VPC: Lab2-VPC (10.0.0.0/16)
   - Name: Public-Subnet-1A
   - AZ: us-east-1a
   - CIDR: 10.0.1.0/24
2. Hacer clic en Çreate subnet"(botón naranja, parte inferior)
3. Verás banner verde: "Successfully created subnet"
4. Anotar el Subnet ID (ejemplo: subnet-0123456789abcdef0)

4.3.3. 3.3 Crear Segunda Subred Pública (Public Subnet 1B)

Repetir el proceso para la segunda AZ:

1. En la lista de subredes, hacer clic nuevamente en Çreate subnet"
2. **VPC ID:** Seleccionar la misma VPC: "Lab2-VPC"
3. **Subnet name:** `Public-Subnet-1B`
4. **Availability Zone:** `us-east-1b` (nota la "b")
5. **IPv4 CIDR block:** `10.0.2.0/24` (nota el "2")
6. **Tags adicionales:**
   - Key: `Type`, Value: `Public`
   - Key: `AZ`, Value: `us-east-1b`
7. Hacer clic en Çreate subnet"
8. Anotar el Subnet ID

¡Ya tienes 2 subredes públicas en 2 AZs diferentes!

4.3.4. 3.4 Crear Primera Subred Privada (Private Subnet 1A)

1. Hacer clic nuevamente en Çreate subnet"
2. **VPC ID:** Seleccionar "Lab2-VPC"
3. **Subnet name:** `Private-Subnet-1A`
4. **Availability Zone:** `us-east-1a`
   - Misma AZ que Public-Subnet-1A
   - Esto permite arquitecturas donde frontend (público) y backend (privado) están en la misma AZ
5. **IPv4 CIDR block:** `10.0.11.0/24`
   - Nota el "11.$^{\text{en}}$ vez de "1"
   - Esto separa claramente subredes públicas (10.0.1-10) de privadas (10.0.11-20)
6. **Tags adicionales:**
   - Key: `Type`, Value: `Private`
   - Key: `AZ`, Value: `us-east-1a`
7. Hacer clic en Çreate subnet"
8. Anotar el Subnet ID

4.3.5. 3.5 Crear Segunda Subred Privada (Private Subnet 1B)

1. Hacer clic nuevamente en Çreate subnet"
2. **VPC ID:** Seleccionar "Lab2-VPC"
3. **Subnet name:** `Private-Subnet-1B`
4. **Availability Zone:** `us-east-1b`
5. **IPv4 CIDR block:** `10.0.12.0/24`
6. **Tags adicionales:**
   - Key: `Type`, Value: `Private`
   - Key: `AZ`, Value: `us-east-1b`
7. Hacer clic en Çreate subnet"
8. Anotar el Subnet ID

¡Felicidades! Ya creaste las 4 subredes.

Nombre	CIDR	AZ	VPC
Public-Subnet-1A	10.0.1.0/24	us-east-1a	Lab2-VPC
Public-Subnet-1B	10.0.2.0/24	us-east-1b	Lab2-VPC
Private-Subnet-1A	10.0.11.0/24	us-east-1a	Lab2-VPC
Private-Subnet-1B	10.0.12.0/24	us-east-1b	Lab2-VPC

Cuadro 8: Verificación de subredes creadas

4.3.6. 3.6 Verificar Todas las Subredes Creadas

En la lista de subredes:
Deberías ver ahora tus 4 subredes listadas. Verificar:
Filtrar por VPC (opcional pero útil):
Para ver solo tus subredes (sin las de la VPC por defecto):

1. En la lista de subredes, buscar el campo de filtro (parte superior)
2. Hacer clic en el ícono de filtro
3. Seleccionar "VPC ID"
4. Elegir tu VPC: "Lab2-VPC"
5. Ahora solo verás las 4 subredes de tu VPC

4.3.7. 3.7 Entender el Estado de las Subredes

Inspeccionar detalles de una subred:

1. Seleccionar una subred (hacer clic en la casilla izquierda)
2. Ejemplo: seleccionar "Public-Subnet-1A"
3. En la parte inferior, ver las pestañas de detalles

Pestaña "Details":

- **Subnet ID:** Identificador único
- **State:** ."Available"(en verde)
- **VPC:** Lab2-VPC
- **IPv4 CIDR:** 10.0.1.0/24
- **Available IPv4 addresses:** 251
- **Availability Zone:** us-east-1a
- **Availability Zone ID:** (ID interno de AWS)
- **Route table:** (tabla principal por defecto)

- **Network ACL:** (ACL principal por defecto)
- **Auto-assign public IPv4 address:** No (para públicas, cambiaremos esto)

Nota importante sobre .Auto-assign public IPv4 address":

- Por defecto está en "No"para todas las subredes nuevas
- Significa que instancias EC2 NO recibirán IP pública automáticamente
- Para subredes públicas, queremos habilitarlo
- Lo haremos en el siguiente paso

4.3.8. 3.8 Habilitar Asignación Automática de IP Pública (Subredes Públicas)

Para Public-Subnet-1A:

1. Seleccionar "Public-Subnet-1A"(casilla izquierda)
2. Hacer clic en el menú .Actions"(parte superior derecha)
3. Seleccionar .Edit subnet settings"
4. Se abrirá una página de configuración
5. Buscar la sección .Auto-assign IP settings"
6. Marcar la casilla: **.Enable auto-assign public IPv4 address"**
7. Hacer clic en "Save"(guardar)
8. Verás banner verde: "Subnet settings updated"

Para Public-Subnet-1B:

1. Repetir el mismo proceso para "Public-Subnet-1B"
2. Seleccionar la subred
3. Actions → Edit subnet settings
4. Marcar .Enable auto-assign public IPv4 address"
5. Save

NO habilitar para subredes privadas:

- Private-Subnet-1A y Private-Subnet-1B deben permanecer con "No"
- Los recursos en subredes privadas NO deben tener IPs públicas
- Esto es una característica de seguridad, no un bug

¿Qué logramos con esto?

- Cuando lances instancias EC2 en subredes públicas (Lab 4), recibirán IP pública automáticamente
- Podrán acceder a internet (una vez que agreguemos Internet Gateway en Lab 3)
- Usuarios externos podrán conectarse a esas instancias (con security groups apropiados)

Tabla actualizada de configuración:

Nombre	**CIDR**	**AZ**	**Auto-assign Public IP**
Public-Subnet-1A	10.0.1.0/24	us-east-1a	Yes
Public-Subnet-1B	10.0.2.0/24	us-east-1b	Yes
Private-Subnet-1A	10.0.11.0/24	us-east-1a	No
Private-Subnet-1B	10.0.12.0/24	us-east-1b	No

Cuadro 9: Configuración de asignación de IP pública por subred

4.4 Paso 4: Configurar Tablas de Enrutamiento

Objetivo: Crear y configurar tablas de enrutamiento para subredes públicas y privadas.

4.4.1. 4.1 Entender las Tablas de Enrutamiento Actuales

Navegar a Route Tables:

1. En el panel izquierdo del dashboard de VPC, hacer clic en Route Tables"
2. Verás una lista de tablas de enrutamiento
3. Buscar las que pertenecen a tu VPC (Lab2-VPC)

Tabla de enrutamiento principal (Main Route Table):

1. Filtrar por VPC: hacer clic en el filtro, seleccionar "Lab2-VPC"
2. Verás una tabla con columna "Main- "Yes"
3. Esta es la tabla de enrutamiento principal creada automáticamente
4. Seleccionarla (casilla izquierda) para ver detalles

Inspeccionar rutas de la tabla principal:

1. Con la tabla principal seleccionada, hacer clic en la pestaña Routes"(parte inferior)
2. Verás una ruta:
   - **Destination:** 10.0.0.0/16
   - **Target:** local
   - **Status:** Active
3. Esta ruta permite comunicación entre todas las subredes dentro de la VPC
4. NO se puede eliminar ni modificar

Ver asociaciones de subredes:

1. Hacer clic en la pestaña "Subnet associations"(junto a Routes)
2. Verás dos secciones:
   - **Explicit subnet associations:** Ninguna (inicialmente)
   - **Subnets without explicit associations:** Las 4 subredes
3. Esto significa que tus 4 subredes usan la tabla principal por defecto
4. Vamos a cambiar esto

4.4.2. 4.2 Estrategia de Tablas de Enrutamiento

Mejor práctica recomendada por AWS:

1. **Tabla Principal (Main Route Table):**
   - Dejarla sin ruta a internet
   - Así, si alguien crea una subred y olvida especificar tabla, será privada por defecto
   - Principio de seguridad: "seguro por defecto"
2. **Tabla Pública (nueva):**
   - Crear una tabla nueva para subredes públicas
   - Asociar subredes públicas a esta tabla
   - En Lab 3, agregaremos ruta a Internet Gateway
3. **Tabla Privada (opcional):**
   - Podemos usar la tabla principal para subredes privadas
   - O crear una tabla explícita para mayor claridad
   - En este lab, usaremos la tabla principal

4.4.3. 4.3 Renombrar la Tabla Principal

Para claridad, darle nombre a la tabla principal:

1. Seleccionar la tabla principal (Main = Yes)
2. Hacer clic en el ícono de lápiz junto a la columna "Name"(o hacer clic en la celda)
3. Ingresar nombre: `Private-Route-Table`
4. Presionar Enter o hacer clic en el check verde
5. Ahora la tabla tiene un nombre descriptivo

Agregar etiquetas a la tabla principal:

1. Con la tabla seleccionada, hacer clic en la pestaña "Tags"
2. Hacer clic en "Manage tags"
3. Agregar etiqueta:
   - Key: `Type`, Value: `Private`
4. Hacer clic en "Save"

4.4.4. 4.4 Crear Tabla de Enrutamiento Pública

1. En la lista de Route Tables, hacer clic en Çreate route table"(botón naranja)
2. Se abrirá el formulario de creación

Formulario de creación:

1. **Name:** Ingresar `Public-Route-Table`
2. **VPC:** Seleccionar "Lab2-VPC"(tu VPC)
3. Verificar que el VPC ID sea correcto
4. **Tags:** Agregar etiquetas
   - Ya tiene tag "Nameçon valor "Public-Route-Table"
   - Agregar: Key: `Type`, Value: `Public`
5. Hacer clic en Çreate route table"
6. Verás banner verde: "Successfully created route table"

Verificar rutas de la nueva tabla:

1. La nueva tabla aparecerá seleccionada automáticamente
2. Hacer clic en la pestaña Routes"
3. Verás solo una ruta:
   - Destination: 10.0.0.0/16, Target: local
4. En Lab 3, agregaremos ruta 0.0.0.0/0 → Internet Gateway
5. Por ahora, déjala con solo la ruta local

4.4.5. 4.5 Asociar Subredes Públicas a la Tabla Pública

Asociar Public-Subnet-1A:

1. Con "Public-Route-Table"seleccionada, hacer clic en la pestaña "Subnet associations"
2. Verás "Subnets without explicit associations": todas tus subredes
3. Hacer clic en .Editit subnet associations"
4. Se abrirá una página con lista de checkboxes
5. Marcar las casillas de:
   - **Public-Subnet-1A** (10.0.1.0/24)
   - **Public-Subnet-1B** (10.0.2.0/24)

6. **NO** marcar las subredes privadas
7. Hacer clic en "Save associations"
8. Verás banner verde: "Successfully updated subnet associations"

Verificar asociaciones:

1. En la pestaña "Subnet associations", ahora deberías ver:
2. **Explicit subnet associations:** 2 subredes
   - Public-Subnet-1A (10.0.1.0/24, us-east-1a)
   - Public-Subnet-1B (10.0.2.0/24, us-east-1b)

4.4.6. 4.6 Verificar Asociaciones de Subredes Privadas

Las subredes privadas deben usar la tabla principal:

1. En la lista de Route Tables, seleccionar "Private-Route-Table"(Main = Yes)
2. Hacer clic en la pestaña "Subnet associations"
3. En "Subnets without explicit associations", deberías ver:
   - Private-Subnet-1A (10.0.11.0/24, us-east-1a)
   - Private-Subnet-1B (10.0.12.0/24, us-east-1b)
4. Esto significa que estas subredes usan la tabla principal automáticamente
5. NO necesitamos hacer asociación explícita

¿Por qué "Subnets without explicit associations¿

- AWS usa el término ïmplicit association"para subredes que usan la tabla principal
- Cualquier subred sin asociación explícita usa la tabla principal (Main)
- Esto es conveniente: nuevas subredes serán privadas por defecto

4.4.7. 4.7 Verificar Configuración Completa de Enrutamiento

Estado final de tablas de enrutamiento:

Tabla	Rutas	Subredes Asociadas
Private-Route-Table (Main)	10.0.0.0/16 → local	Private-Subnet-1A, Private-Subnet-1B
Public-Route-Table	10.0.0.0/16 → local	Public-Subnet-1A, Public-Subnet-1B

Cuadro 10: Configuración de tablas de enrutamiento

Verificar desde la vista de Subnets:

1. Navegar a "Subnets.[en] el panel izquierdo
2. Filtrar por tu VPC: Lab2-VPC
3. Ver la columna Route table"
4. Verificar:
   - Public-Subnet-1A → Public-Route-Table
   - Public-Subnet-1B → Public-Route-Table
   - Private-Subnet-1A → Private-Route-Table
   - Private-Subnet-1B → Private-Route-Table

¡Perfecto! Enrutamiento configurado correctamente.

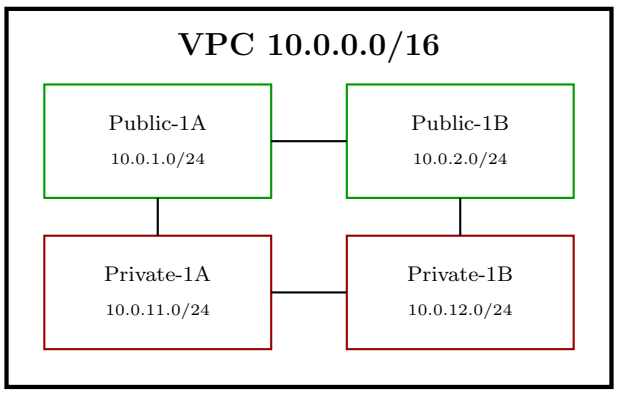
4.4.8. 4.8 Entender el Flujo de Tráfico Actual

¿Qué puede hacer el tráfico AHORA con esta configuración?

1. **Comunicación dentro de la VPC:**
   - Una instancia en Public-Subnet-1A puede comunicarse con instancia en Private-Subnet-1B
   - Razón: ambas tienen ruta 10.0.0.0/16 → local
   - El tráfico fluye dentro de la VPC sin salir a internet
2. **Comunicación entre AZs:**
   - Instancias en us-east-1a pueden comunicarse con instancias en us-east-1b
   - AWS enruta el tráfico internamente entre AZs de forma segura y rápida
3. **Acceso a internet:**
   - NINGUNA subred puede acceder a internet todavía
   - Razón: no hay ruta 0.0.0.0/0 → Internet Gateway
   - Lo agregaremos en Lab 3
4. **Acceso DESDE internet:**
   - Nadie desde internet puede llegar a tus subredes
   - Razón: no hay Internet Gateway adjunto
   - También lo haremos en Lab 3

Resumen visual del estado actual:

Comunicación interna funcionando



Sin acceso a internet (aún)

4.5 Paso 5: Verificación de la Configuración

Objetivo: Confirmar que toda la infraestructura de red está correctamente configurada.

4.5.1. 5.1 Verificar VPC

1. Navegar a "Your VPCs.[en] el panel izquierdo
2. Filtrar por región us-east-1 (si no lo hiciste antes)
3. Verificar que existe "Lab2-VPCçon:
   - IPv4 CIDR: 10.0.0.0/16
   - State: Available (verde)
   - DNS resolution: Enabled
   - DNS hostnames: Enabled o Disabled (ambos OK por ahora)

4.5.2. 5.2 Verificar Subredes

1. Navegar a "Subnets"
2. Filtrar por VPC: Lab2-VPC
3. Contar: deben aparecer exactamente 4 subredes
4. Verificar cada subred:

Checklist de verificación:

Nombre	CIDR	AZ	Auto IP	Route Table	
Public-Subnet-1A	10.0.1.0/24	us-east-1a	Yes	Public-Route-Table	
Public-Subnet-1B	10.0.2.0/24	us-east-1b	Yes	Public-Route-Table	
Private-Subnet-1A	10.0.11.0/24	us-east-1a	No	Private-Route-Table	
Private-Subnet-1B	10.0.12.0/24	us-east-1b	No	Private-Route-Table	

Cuadro 11: Checklist de verificación de subredes

4.5.3. 5.3 Verificar Tablas de Enrutamiento

1. Navegar a Route Tables"
2. Filtrar por VPC: Lab2-VPC
3. Deben aparecer 2 tablas:
   - Private-Route-Table (Main = Yes)
   - Public-Route-Table (Main = No)

Verificar Public-Route-Table:

1. Seleccionar "Public-Route-Table"
2. Pestaña Routes": debe tener solo ruta 10.0.0.0/16 → local
3. Pestaña "Subnet associations": debe mostrar 2 subredes públicas
4. Si todo correcto:

Verificar Private-Route-Table:

1. Seleccionar "Private-Route-Table"
2. Pestaña Routes": debe tener solo ruta 10.0.0.0/16 → local
3. Pestaña "Subnet associations": debe mostrar 2 subredes privadas (implícitas)
4. Si todo correcto:

4.5.4. 5.4 Verificar Costos

Confirmar que no hay cargos:

1. Hacer clic en tu nombre (esquina superior derecha)
2. Seleccionar "Billing and Cost Management"
3. Ver "Month-to-date costs"
4. Debe seguir en $0.00
5. Si hay algún cargo, verificar qué servicio lo generó (no debería ser VPC)

4.6 Paso 6: Documentación y Limpieza

4.6.1. 6.1 Documentar tu Infraestructura

Crear documento de referencia (opcional pero muy recomendado):
En un documento de texto o hoja de cálculo, anotar:

1. **VPC ID:** vpc-0a1b2c3d4e5f67890
2. **VPC CIDR:** 10.0.0.0/16
3. **Región:** us-east-1
4. **Subredes:**
   - Public-Subnet-1A: subnet-xxx (10.0.1.0/24, us-east-1a)
   - Public-Subnet-1B: subnet-yyy (10.0.2.0/24, us-east-1b)
   - Private-Subnet-1A: subnet-zzz (10.0.11.0/24, us-east-1a)
   - Private-Subnet-1B: subnet-www (10.0.12.0/24, us-east-1b)

5. **Route Tables:**
   - Public-Route-Table: rtb-aaa
   - Private-Route-Table: rtb-bbb (Main)

Esta documentación será útil en laboratorios futuros cuando necesites recordar IDs de recursos.

4.6.2. 6.2 ¿Limpiar Recursos?

Pregunta importante: ¿Debemos eliminar la VPC ahora?
Respuesta: NO

- La VPC y subredes NO generan costos ($0.00)
- Las necesitaremos para Lab 3 (Internet Gateway)
- Y para Lab 4 (instancias EC2)
- Y para todos los laboratorios siguientes

Cuándo SÍ deberías eliminar recursos:

- Al finalizar TODOS los laboratorios del curso
- Si decides pausar el curso por más de 1 mes
- Si vas a crear una nueva arquitectura desde cero

Cómo eliminar VPC (para referencia futura):
Si en el futuro necesitas eliminar la VPC:

1. PRIMERO: Eliminar todos los recursos dentro de la VPC
   - Instancias EC2 (si existen)
   - Internet Gateways adjuntos
   - NAT Gateways (si existen)
   - Elastic IPs asociados
   - Load Balancers
   - Endpoints de VPC
2. LUEGO: Eliminar la VPC
   - Ir a "Your VPCs"
   - Seleccionar tu VPC
   - Actions → Delete VPC
   - AWS eliminará automáticamente subredes, tablas de enrutamiento, NACLs

Por ahora: NO eliminar nada. Mantener la VPC para siguientes laboratorios.

5 Cuestionario de Evaluación

Instrucciones: Selecciona la respuesta correcta para cada pregunta.

5.1 Preguntas de Selección Múltiple

1. **¿Qué significa CIDR en el contexto de redes?**

   a) Central Internet Data Routing

   b) Classless Inter-Domain Routing

   c) Cloud Infrastructure Data Repository

   d) Centralized IP Distribution Range

2. **¿Cuántas direcciones IP proporciona un bloque CIDR /16?**

   a) 256 direcciones

   b) 4,096 direcciones

   c) 65,536 direcciones

   d) 16,777,216 direcciones

3. **¿Cuántas direcciones IP reserva AWS en cada subred y para qué?**

   a) 3 direcciones: red, router, broadcast

   b) 5 direcciones: red, router VPC, DNS, uso futuro, broadcast

   c) 2 direcciones: red y broadcast

   d) 10 direcciones para uso interno de AWS

4. **¿Cuál es la principal diferencia entre una subred pública y una privada en VPC?**

   a) El tamaño del bloque CIDR

   b) La tabla de enrutamiento: públicas tienen ruta a Internet Gateway, privadas no

   c) Las subredes públicas están en múltiples AZs, las privadas en una sola

   d) Las subredes públicas son más caras que las privadas

5. **¿Puede una subred de VPC abarcar múltiples Zonas de Disponibilidad?**

   a) Sí, para mayor disponibilidad

   b) Sí, pero solo si es subred pública

   c) No, cada subred debe residir completamente en una sola AZ

   d) Depende del tamaño del bloque CIDR

6. **¿Cuál es el rango de direcciones IP privadas más grande según RFC 1918?**

a) 192.168.0.0/16
b) 172.16.0.0/12
c) 10.0.0.0/8
d) 100.64.0.0/10

7. **¿Qué ruta se crea automáticamente en toda tabla de enrutamiento de VPC?**

a) 0.0.0.0/0 → Internet Gateway
b) CIDR de la VPC → local
c) 169.254.169.254/32 → metadata service
d) 8.8.8.8/32 → DNS de Google

8. **¿Tiene costo crear y mantener una VPC en AWS?**

a) Sí, $0.05 por hora por VPC
b) Sí, pero solo las primeras 5 VPCs son gratis
c) No, Amazon VPC es siempre gratuito
d) Depende del tamaño del bloque CIDR

9. **Si una subred NO tiene asociación explícita a una tabla de enrutamiento, ¿cuál usa?**

a) No puede funcionar sin asociación explícita
b) Usa la tabla de enrutamiento principal (Main Route Table)
c) Crea una tabla de enrutamiento temporal
d) Usa la tabla de enrutamiento de la VPC por defecto

10. **¿Cuál es la mejor práctica para la tabla de enrutamiento principal (Main)?**

a) Agregarle ruta a Internet Gateway para que todas las subredes tengan internet
b) Dejarla sin ruta a internet, así nuevas subredes son privadas por defecto
c) Eliminarla y crear solo tablas personalizadas
d) Asociarle explícitamente todas las subredes

11. **¿Qué configuración permite que instancias EC2 en una subred reciban IP pública automáticamente?**

a) Habilitar .Auto-assign public IPv4 address.en la configuración de la subred
b) Agregar ruta 0.0.0.0/0 a la tabla de enrutamiento
c) Adjuntar un Internet Gateway a la VPC
d) Configurar DHCP options set

12. **¿Cuántas VPCs puedes crear por región en AWS Free Tier por defecto?**

a) 1 VPC

b) 5 VPCs (límite puede aumentarse)

c) 10 VPCs

d) Ilimitadas

13. **Si tienes VPC con CIDR 10.0.0.0/16 y creas subred 10.0.1.0/24, ¿cuántas IPs utilizables tiene esa subred?**

a) 256 IPs

b) 254 IPs

c) 251 IPs (AWS reserva 5)

d) 250 IPs

14. **¿Por qué se recomienda distribuir subredes en al menos 2 Zonas de Disponibilidad?**

a) Para aumentar el ancho de banda disponible

b) Para alta disponibilidad y tolerancia a fallos

c) Para reducir costos de transferencia de datos

d) Para cumplir requisitos mínimos de AWS Free Tier

15. **Con la configuración de este laboratorio (sin Internet Gateway), ¿pueden las instancias en subredes públicas comunicarse con instancias en subredes privadas dentro de la misma VPC?**

a) No, necesitan Internet Gateway para comunicarse

b) No, subredes públicas y privadas están aisladas

c) Sí, gracias a la ruta local 10.0.0.0/16 → local

d) Solo si están en la misma AZ

5.2 Respuestas del Cuestionario

1. **Respuesta correcta: b)** CIDR significa Classless Inter-Domain Routing. Es un método para asignar direcciones IP y enrutar paquetes que reemplazó al antiguo sistema de clases (A, B, C). Usa notación slash (/) para indicar la máscara de red.

2. **Respuesta correcta: c)** Un bloque /16 proporciona $2^{32-16} = 2^{16} = 65,536$ direcciones IP. Por ejemplo, 10.0.0.0/16 va desde 10.0.0.0 hasta 10.0.255.255.

3. **Respuesta correcta: b)** AWS reserva 5 direcciones en cada subred: primera (dirección de red), segunda (router de VPC), tercera (servidor DNS de AWS), cuarta (uso futuro), y última (broadcast de red). Por eso una subred /24 con 256 IPs solo tiene 251 utilizables.

4. **Respuesta correcta: b)** La diferencia está en la tabla de enrutamiento. Subredes públicas tienen una ruta 0.0.0.0/0 apuntando a un Internet Gateway, permitiendo tráfico hacia/desde internet. Subredes privadas no tienen esta ruta y por tanto no pueden acceder directamente a internet.

5. **Respuesta correcta: c)** No, cada subred debe residir completamente dentro de una sola Zona de Disponibilidad. No puede abarcar múltiples AZs. Para alta disponibilidad, debes crear múltiples subredes, una en cada AZ.

6. **Respuesta correcta: c)** El rango 10.0.0.0/8 es el más grande según RFC 1918, proporcionando 16,777,216 direcciones IP (desde 10.0.0.0 hasta 10.255.255.255). Los otros rangos privados son 172.16.0.0/12 (1,048,576 IPs) y 192.168.0.0/16 (65,536 IPs).

7. **Respuesta correcta: b)** Automáticamente se crea una ruta con destino al CIDR completo de la VPC y target "local". Por ejemplo, si tu VPC es 10.0.0.0/16, la ruta será 10.0.0.0/16 → local. Esta ruta permite comunicación entre todas las subredes dentro de la VPC y no se puede eliminar.

8. **Respuesta correcta: c)** Amazon VPC es completamente gratuito. No hay cargos por crear VPCs, subredes, tablas de enrutamiento, o usar direcciones IP privadas. Solo algunos servicios relacionados como NAT Gateway o VPN Connection tienen costo.

9. **Respuesta correcta: b)** Usa la tabla de enrutamiento principal (Main Route Table) automáticamente. Por eso es una mejor práctica mantener la tabla principal sin ruta a internet: así, cualquier subred creada sin asociación explícita será privada por defecto (principio de seguridad).

10. **Respuesta correcta: b)** La mejor práctica es dejar la tabla principal SIN ruta a Internet Gateway. Así, si alguien crea una subred y olvida especificar tabla de enrutamiento, será privada por defecto. Crear tablas separadas para subredes públicas garantiza que el acceso a internet sea explícito e intencional.

11. **Respuesta correcta: a)** Debes habilitar .Auto-assign public IPv4 address.en la configuración de la subred. Esto hace que instancias lanzadas en esa subred reciban automáticamente una IP pública además de su IP privada. Las subredes privadas deben tener esta opción deshabilitada.

12. **Respuesta correcta: b)** Por defecto puedes crear 5 VPCs por región. Este límite puede aumentarse contactando a AWS Support. En Free Tier, las 5 VPCs son gratuitas (VPC es siempre gratis, independientemente del plan).

13. **Respuesta correcta: c)** Una subred /24 tiene 256 direcciones, pero AWS reserva 5, dejando 251 utilizables para instancias EC2, bases de datos, y otros recursos. Las 5 reservadas son: .0 (red), .1 (router), .2 (DNS), .3 (futuro), .255 (broadcast).

14. **Respuesta correcta: b)** Distribuir en múltiples AZs proporciona alta disponibilidad y tolerancia a fallos. Si una AZ completa falla (evento raro pero posible), tus

recursos en otras AZs continúan funcionando. Es una práctica fundamental para arquitecturas de producción.

15. **Respuesta correcta: c)** Sí, pueden comunicarse gracias a la ruta local. Todas las subredes dentro de una VPC tienen automáticamente una ruta al CIDR completo de la VPC con target "local", permitiendo comunicación interna sin necesidad de Internet Gateway. El concepto de "pública"vs "privada"solo afecta el acceso a/desde internet, no la comunicación interna.

6 Conclusiones

Al finalizar este laboratorio, has construido los cimientos de una infraestructura de red robusta en AWS, dominando conceptos fundamentales de redes virtuales que son aplicables no solo a AWS, sino a cualquier plataforma de computación en nube. La VPC que creaste es el componente base sobre el cual se construirán todas las arquitecturas futuras en este curso.

6.1 Logros Técnicos Principales

1. Dominio de Direccionamiento IP y CIDR

Has aplicado conocimientos de redes tradicionales al contexto de infraestructura definida por software. Comprendes cómo calcular rangos CIDR, determinar capacidad de hosts, y planificar subredes considerando las 5 direcciones reservadas por AWS. Esta habilidad es fundamental para cualquier arquitecto de soluciones en la nube.

2. Creación de Arquitectura Multi-AZ

Has diseñado e implementado una arquitectura distribuida geográficamente en dos Zonas de Disponibilidad, aplicando principios de alta disponibilidad y tolerancia a fallos. Esta arquitectura simétrica (2 subredes públicas + 2 privadas) es un patrón estándar de la industria utilizado en entornos de producción.

3. Segmentación de Red con Subredes Públicas y Privadas

Has implementado separación de responsabilidades mediante subredes públicas (para recursos orientados a internet) y privadas (para recursos backend). Esta arquitectura de múltiples capas es una práctica de seguridad fundamental que reduce la superficie de ataque y aísla componentes críticos.

4. Gestión de Tablas de Enrutamiento

Has configurado enrutamiento diferenciado para subredes públicas y privadas, entendiendo cómo controlar flujos de tráfico mediante tablas de enrutamiento. Comprendes la importancia de la ruta local automática y has preparado la infraestructura para futuros Internet Gateways.

6.2 Competencias Desarrolladas

Competencias de Diseño:

- Planificación de arquitecturas de red escalables
- Aplicación de convenciones de nomenclatura consistentes
- Uso de etiquetado (tagging) para organización de recursos
- Documentación de decisiones de arquitectura
- Previsión de crecimiento futuro en diseño de direccionamiento

Competencias Operacionales:

- Navegación eficiente en consola de AWS para servicios de red

- Creación y configuración de recursos de VPC
- Verificación sistemática de configuraciones de red
- Interpretación de flujos de tráfico en arquitecturas de nube
- Resolución de problemas de configuración de red

Competencias de Seguridad:

- Aplicación de principio de "seguro por defecto"(tabla principal sin internet)
- Diseño de arquitectura de defensa en profundidad
- Aislamiento de recursos mediante subredes privadas
- Control de acceso a nivel de red

6.3 Comprensión de Conceptos Clave

VPC como Fundamento:
Has comprendido que VPC es el primer paso obligatorio en casi cualquier arquitectura de AWS. Sin una VPC adecuadamente diseñada, no puedes desplegar instancias EC2, bases de datos RDS, clústeres EKS, o la mayoría de servicios de AWS de manera controlada y segura.

Infraestructura como Código Conceptual:
Aunque has creado recursos mediante la consola, has seguido un proceso sistemático y documentado que podría traducirse fácilmente a Infrastructure as Code (IaC) usando Terraform o CloudFormation. Comprendes qué recursos dependen de otros y el orden de creación necesario.

Costo Cero, Valor Infinito:
Has aprendido que una de las fortalezas de AWS es que puedes diseñar y construir arquitecturas de red completas sin costo alguno. La VPC, subredes, tablas de enrutamiento, y la mayoría de componentes de red son gratuitos, permitiendo experimentación y aprendizaje sin riesgo financiero.

6.4 Preparación para Laboratorios Futuros

Esta VPC que construiste será la base para:

- **Lab 3 - Internet Gateway:** Conectarás las subredes públicas a internet, permitiendo acceso bidireccional
- **Lab 4 - EC2 y Security Groups:** Lanzarás instancias EC2 en tus subredes, aplicando seguridad a nivel de instancia
- **Lab 5 - Seguridad Avanzada:** Implementarás Network ACLs, VPC Flow Logs, y análisis de tráfico
- **Lab 6 - VPC Peering:** Conectarás múltiples VPCs para arquitecturas complejas

- **Lab 7 - CloudWatch:** Monitorearás el rendimiento de tu red y recursos
- **Lab 8 - Proyecto Integrador:** Desplegarás una aplicación completa sobre esta infraestructura

Cada laboratorio agregará capas adicionales de funcionalidad y seguridad sobre la base sólida que construiste hoy.

6.5 Mejores Prácticas Aprendidas

1. **Planificar antes de implementar:** El tiempo invertido en diseño previene problemas futuros
2. **Convenciones de nomenclatura:** Nombres descriptivos facilitan gestión en entornos grandes
3. **Etiquetado consistente:** Tags permiten organización, facturación, y automatización
4. **Arquitectura multi-AZ:** Siempre considerar alta disponibilidad desde el inicio
5. **Seguridad por defecto:** Diseñar redes privadas por defecto, público solo cuando necesario
6. **Documentación continua:** Anotar IDs de recursos facilita troubleshooting futuro
7. **Escalabilidad:** Dejar espacio de direccionamiento para crecimiento

6.6 Reflexión Final

La habilidad de diseñar y construir redes virtuales en la nube es fundamental para cualquier profesional de tecnología moderna. No es solo sobre AWS: los conceptos de direccionamiento IP, subnetting, enrutamiento, y segmentación de red son universales y aplicables a Azure, Google Cloud, entornos on-premise, y cualquier infraestructura de red.

Has demostrado que comprendes no solo cómo crear recursos en AWS, sino *por qué* se crean de cierta manera. Entiendes las decisiones de arquitectura detrás de subredes públicas vs privadas, la importancia de distribución multi-AZ, y cómo las tablas de enrutamiento controlan flujos de tráfico.

Esta infraestructura de red que construiste en menos de 90 minutos, sin costo alguno, equivale a diseños de red empresarial que en entornos tradicionales requerirían hardware físico, configuración compleja, y semanas de implementación. Esta es la potencia de la nube: infraestructura definida por software, escalable, flexible, y accesible.

¡Felicidades por completar el Laboratorio 2 exitosamente!

Ahora tienes una VPC robusta, lista para el siguiente paso: conectarla a internet mediante Internet Gateway en el Laboratorio 3.

7 Referencias

7.1 Documentación Oficial de AWS

1. **Amazon VPC**
   - Amazon VPC Documentation
     https://docs.aws.amazon.com/vpc/
   - What is Amazon VPC?
     https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
   - VPC Examples and Scenarios
     https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenarios.html
   - Amazon VPC Best Practices
     https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-best-practices.html
2. **VPC Subnets**
   - VPC and Subnets
     https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html
   - Create a Subnet
     https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html
3. **Route Tables**
   - Route Tables for Your VPC
     https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html
   - Work with Route Tables
     https://docs.aws.amazon.com/vpc/latest/userguide/WorkWithRouteTables.html
4. **Availability Zones**
   - Regions and Availability Zones
     https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zo
     html
   - AWS Global Infrastructure
     https://aws.amazon.com/about-aws/global-infrastructure/

7.2 Recursos sobre Redes y CIDR

1. **RFC 1918 - Address Allocation for Private Internets**
   https://tools.ietf.org/html/rfc1918
   Especificación estándar de rangos de direcciones IP privadas.
2. **RFC 4632 - Classless Inter-domain Routing (CIDR)**
   https://tools.ietf.org/html/rfc4632
   Definición técnica de notación CIDR.

3. **CIDR Calculator**
   https://www.subnet-calculator.com/cidr.php
   Herramienta online para cálculos de CIDR y subnetting.

4. **IP Address Guide**
   https://www.ipaddressguide.com/cidr
   Guía interactiva sobre direccionamiento IP y CIDR.

7.3 Tutoriales y Guías de AWS

1. **Getting Started with Amazon VPC**
   https://aws.amazon.com/vpc/getting-started/

2. **AWS VPC Workshop**
   https://catalog.workshops.aws/networking/en-US

3. **AWS re:Invent Videos sobre VPC**
   https://www.youtube.com/c/AWSEventsChannel
   Buscar .ªmazon VPC.en el canal oficial de AWS.

4. **AWS Skill Builder - VPC Courses**
   https://skillbuilder.aws/
   Cursos gratuitos sobre networking en AWS.

7.4 Libros y Publicaciones

1. Wittig, A., & Wittig, M. (2018). *Amazon Web Services in Action* (2nd ed.). Manning Publications.
   Capítulo 6: "Securing your system: IAM, security groups, and VPC Explicación detallada de VPC.

2. Varia, J., & Mathew, S. (2014). *Overview of Amazon Web Services*. Amazon Web Services.
   https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html

3. AWS Well-Architected Framework - Security Pillar.
   https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html
   Sección sobre diseño de redes seguras.

4. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson.
   Referencia fundamental sobre conceptos de redes, incluyendo subnetting e IP routing.

7.5 Herramientas Útiles

1. **AWS VPC Visual Subnet Calculator**
   https://network00.com/NetworkTools/IPv4VisualSubnetCalculator/
   Calculadora visual para planificar subredes.

2. **draw.io (diagrams.net)**
   https://app.diagrams.net/
   Herramienta gratuita para dibujar arquitecturas de AWS, incluye íconos oficiales.

3. **AWS Architecture Icons**
   https://aws.amazon.com/architecture/icons/
   Íconos oficiales para documentar arquitecturas.

4. **CloudCraft**
   https://www.cloudcraft.co/
   Herramienta de diagramación de arquitecturas AWS con estimación de costos.

Nota: Todas las URLs fueron verificadas al momento de creación de este documento. AWS actualiza constantemente su documentación; si algún enlace cambia, buscar el tema en https://docs.aws.amazon.com/.