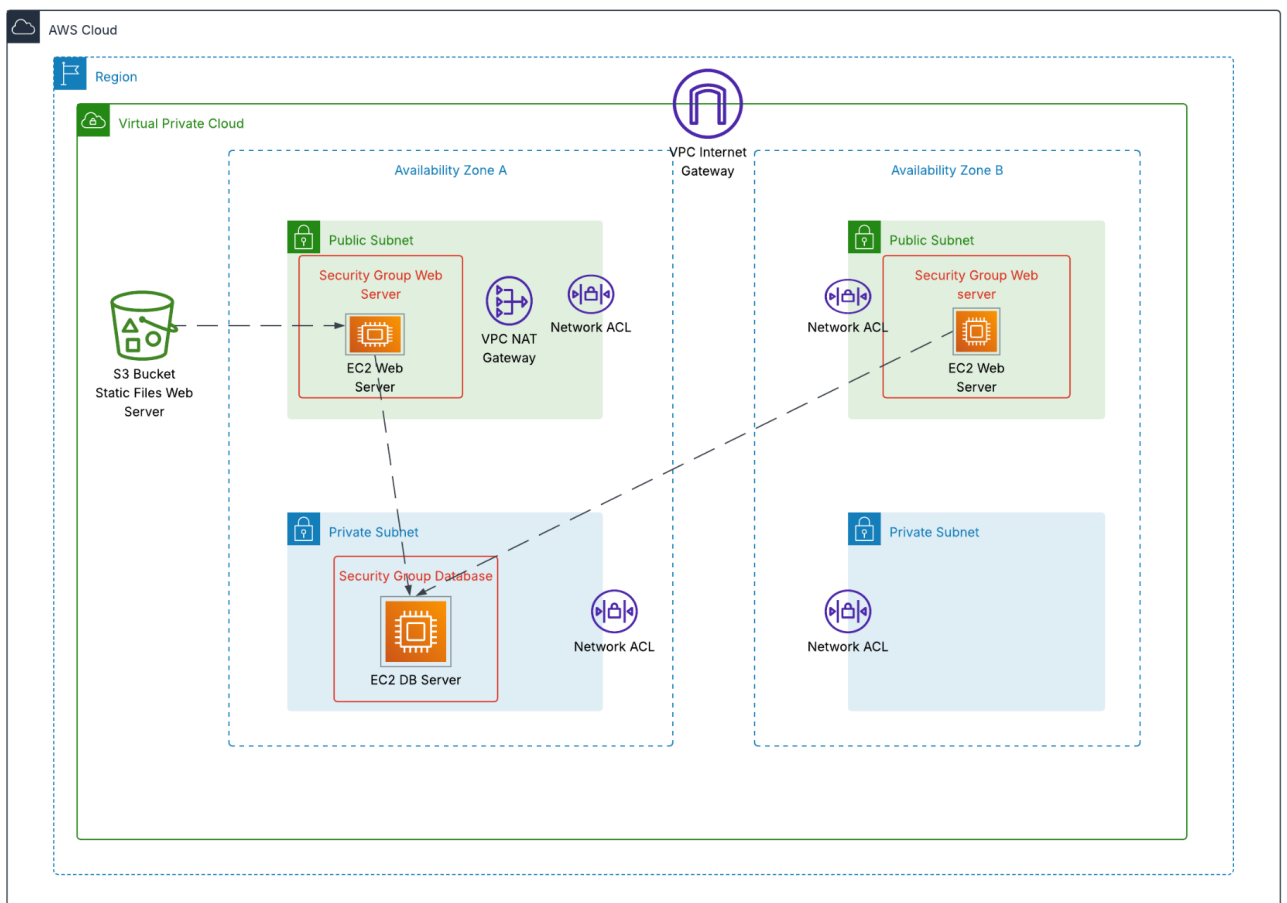


# Ciberseguridad en la Nube

## AWS Academy Learnerlab Aplicación Web de Comercio Electrónico

*Autor: Adrián Felipe Ibarra López*

**Objetivo:** Diseñar, implementar y documentar una arquitectura segura en AWS para una aplicación web de comercio electrónico, aplicando los principios y prácticas aprendidas en el curso Cloud Security Foundations.



Fase 1. Arquitectura de Red Segura (VPC y Subredes)

Diseño y creación de la VPC

Para garantizar una arquitectura segura y escalable, se creó una VPC personalizada denominada SecureVPC, utilizando el rango CIDR 10.0.0.0/16. Este rango proporciona más de 65.000 direcciones IP privadas, lo que permite una amplia capacidad de expansión, en concordancia con las recomendaciones de la RFC 1918. Ver figura 1.

Para lograr alta disponibilidad y tolerancia a fallos, se distribuyeron subredes entre dos Zonas de Disponibilidad (us-east-1a y us-east-1b). Se crearon un total de cuatro subredes. Ver la siguiente tabla:

NOMBRE	CIDR	ZONA DE DISPONIBILIDAD	TIPO	USO PRINCIPAL
Public-Subnet-1	10.0.0.0/24	(us-east-1a)	Pública	Instancia EC2 Web 1
Public-Subnet-2	10.0.1.0/24	(us-east-1b)	Pública	Instancia EC2 Web 2
Private-Subnet-1	10.0.10.0/24	(us-east-1a)	Privada	Base de datos 1
Private-Subnet-2	10.0.11.0/24	(us-east-1b)	Privada	Base de datos 2 / alta disponibilidad

Tabla 1. Subredes.

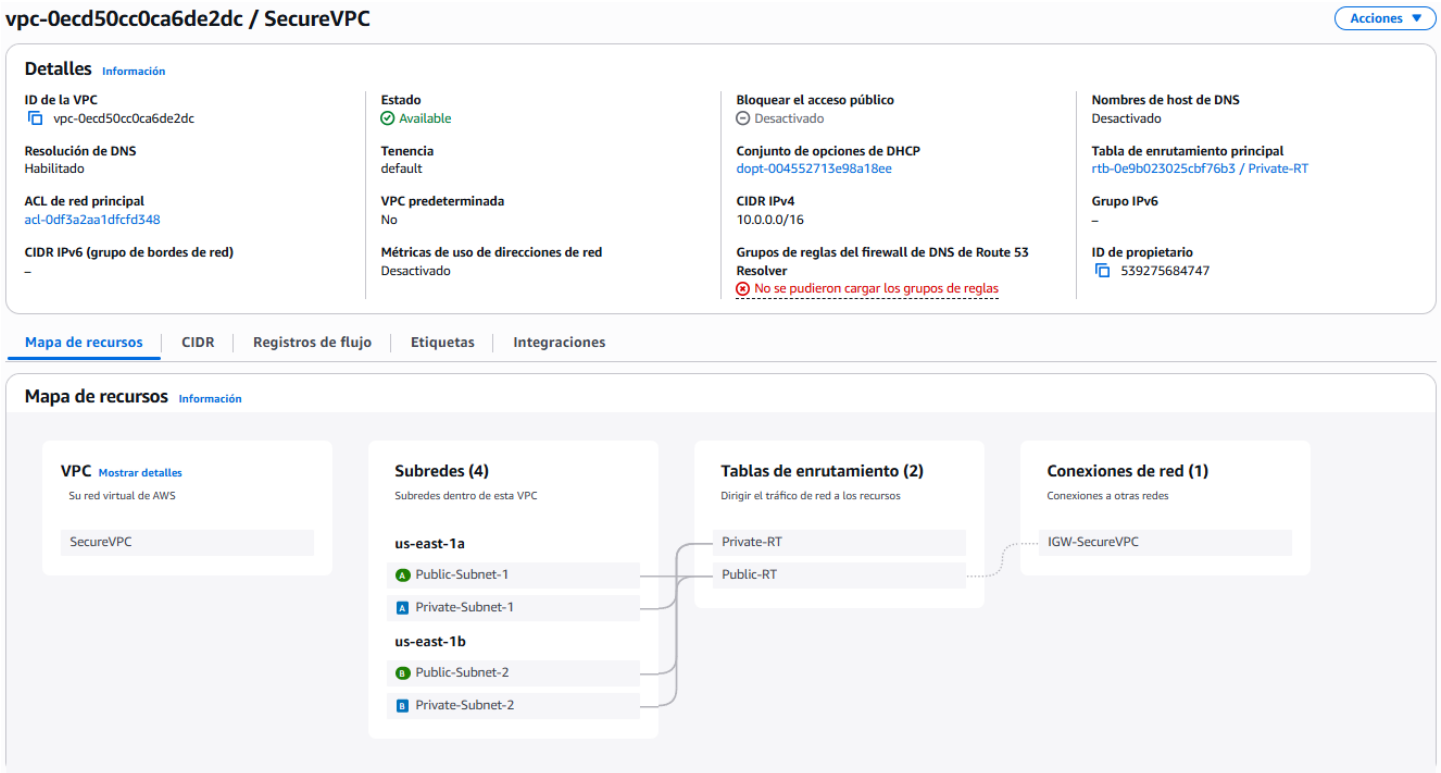


Figura 1. VPC - SecureVPC.

Este diseño garantiza un entorno organizado, seguro y preparado para el despliegue de una arquitectura web de alta disponibilidad y cumplimiento de las mejores prácticas de ciberseguridad en la nube.

### Configuración del acceso a Internet

Se creó un Internet Gateway denominado IGW-SecureVPC, el cual fue adjuntado a la VPC. Para permitir que las subredes públicas tengan acceso a Internet:

- 1. Se creó una tabla de ruteo personalizada llamada Public-RT.
- 2. Se añadió una ruta que direcciona todo el tráfico (0.0.0.0/0) hacia el Internet Gateway.
- 3. Esta tabla fue asociada explícitamente a las subredes públicas (Public-Subnet-1 y Public-Subnet-2).

igw-0d55f49e7a52b3061 / IGW-SecureVPC

Acciones

Detalles

Información

ID de gateway de Internet

igw-0d55f49e7a52b3061

Estado

Attached

ID de la VPC

vpc-0ecd50cc0ca6de2dc | SecureVPC

Propietario

539275684747

Etiquetas

Administrar etiquetas

Buscar etiquetas

Clave

Valor

Name

IGW-SecureVPC

Figura 2. Internet Gateway - IGW-SecureVPC.

rtb-0fcd1293a7a9964b0 / Public-RT

Acciones

Detalles

Información

ID de tabla de enrutamiento

rtb-0fcd1293a7a9964b0

Principal

No

Asociaciones de subredes explícitas

2 subredes

Asociaciones de borde

-

VPC

vpc-0ecd50cc0ca6de2dc | SecureVPC

ID de propietario

539275684747

Rutas

Asociaciones de subredes

Asociaciones de borde

Propagación de rutas

Etiquetas

Rutas (2)

Editar rutas

Filtrar rutas

Destino

Objetivo

Estado

Propagada

0.0.0.0/0

igw-0d55f49e7a52b3061

Activo

No

10.0.0.0/16

local

Activo

No

Figura 3. Tabla de enrutamiento – Public-RT.

rtb-0fcd1293a7a9964b0 / Public-RT

Acciones

Detalles

Información

ID de tabla de enrutamiento

rtb-0fcd1293a7a9964b0

VPC

vpc-0ecd50cc0ca6de2dc | SecureVPC

Principal

No

ID de propietario

539275684747

Asociaciones de subredes explícitas

2 subredes

Asociaciones de borde

-

Rutas

Asociaciones de subredes

Asociaciones de borde

Propagación de rutas

Etiquetas

Asociaciones de subredes explícitas (2)

Editar asociaciones de subredes

Buscar asociación de subredes

Nombre	ID de subred	CIDR IPv4	CIDR IPv6
Public-Subnet-1	subnet-0d3457ac24f108c50	10.0.0.0/24	-
Public-Subnet-2	subnet-02a6b396b87eee1bd	10.0.1.0/24	-

Subredes sin asociaciones explícitas (0)

Editar asociaciones de subredes

Las siguientes subredes no se han asociado explícitamente con ninguna tabla de enrutamiento y, por lo tanto, están asociadas a la tabla de enrutamiento principal:

Buscar asociación de subredes

Nombre	ID de subred	CIDR IPv4	CIDR IPv6
No hay subredes sin asociaciones explícitas			
Todas las subredes están asociadas a una tabla de enrutamiento.			

Figura 4. Tabla de enrutamiento – Public-RT.

Las subredes privadas no se asociaron a esta tabla, utilizando en su lugar la tabla de ruteo principal que no contiene rutas hacia Internet, garantizando así que los recursos en dichas subredes no sean accesibles desde el exterior, cumpliendo con los principios de segmentación y defensa en profundidad.

rtb-0e9b023025cbf76b3 / Private-RT

Acciones

Detalles

Información

ID de tabla de enrutamiento

rtb-0e9b023025cbf76b3

VPC

vpc-0ecd50cc0ca6de2dc | SecureVPC

Principal

Sí

ID de propietario

539275684747

Asociaciones de subredes explícitas

2 subredes

Asociaciones de borde

-

Rutas

Asociaciones de subredes

Asociaciones de borde

Propagación de rutas

Etiquetas

Asociaciones de subredes explícitas (2)

Editar asociaciones de subredes

Buscar asociación de subredes

Nombre	ID de subred	CIDR IPv4	CIDR IPv6
Private-Subnet-1	subnet-041de040349700ece	10.0.10.0/24	-
Private-Subnet-2	subnet-0a70a77d9fdc1d503	10.0.11.0/24	-

Subredes sin asociaciones explícitas (0)

Editar asociaciones de subredes

Las siguientes subredes no se han asociado explícitamente con ninguna tabla de enrutamiento y, por lo tanto, están asociadas a la tabla de enrutamiento principal:

Buscar asociación de subredes

Nombre	ID de subred	CIDR IPv4	CIDR IPv6
No hay subredes sin asociaciones explícitas			
Todas las subredes están asociadas a una tabla de enrutamiento.			

Figura 5. Tabla de enrutamiento – Private-RT.

## Fase 2: Recursos de Cómputo (EC2)

### Despliegue de instancias públicas para la aplicación web

Se implementaron dos instancias EC2 en las subredes públicas de la VPC SecureVPC, una en cada zona de disponibilidad (us-east-1a y us-east-1b), con el objetivo de alojar una aplicación web simple usando Apache. Ambas instancias fueron configuradas con el siguiente esquema:

- AMI: Amazon Linux 2023
- Tipo: t2.micro
- Nombre: Web-Server-1 y Web-Server-2
- Acceso público: habilitado con IP pública.
- Grupo de seguridad (SG-Web):
  - Permitir tráfico HTTP (puerto 80) desde cualquier IP (0.0.0.0/0)
  - Permitir tráfico SSH (puerto 22) desde IP específica para administración segura.

#### sg-09264a42267cae55e - SG-Web

Acciones ▾

##### Detalles

Nombre del grupo de seguridad SG-Web	ID del grupo de seguridad sg-09264a42267cae55e	Descripción Grupo de seguridad	ID de la VPC vpc-0ecd50cc0ca6de2dc
Propietario 539275684747	Número de reglas de entrada 2 Entradas de permisos	Número de reglas de salida 1 Entrada de permiso	

Reglas de entrada | Reglas de salida | Compartiendo : *novedad* | Asociaciones de VPC : *novedad* | Etiquetas

##### Reglas de entrada (2)

Administrar etiquetas Editar reglas de entrada

<input type="checkbox"/>	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen
<input type="checkbox"/>	-	sgr-02a4a231397d09ea3	IPv4	SSH	TCP	22	201.236.221.29/32
<input type="checkbox"/>	-	sgr-0a4a971706e0e20c8	IPv4	HTTP	TCP	80	0.0.0.0/0

Figura 6. Grupo de seguridad SG-Web

Resumen de instancia de i-00755a3660c5d5bcc (Web-Server-1)

Información

Se ha actualizado hace less than a minute

ID de la instancia

i-00755a3660c5d5bcc

Dirección IPv6

-

Tipo de nombre de anfitrión

Nombre de IP: ip-10-0-0-184.ec2.internal

Responder al nombre DNS de recurso privado

-

Dirección IP asignada automáticamente

13.219.75.200 [IP pública]

Rol de IAM

-

IMDSv2

Required

Operador

-

Dirección IPv4 pública

13.219.75.200 | dirección abierta

Estado de la instancia

En ejecución

Nombre DNS de IP privada (solo IPv4)

ip-10-0-0-184.ec2.internal

Tipo de instancia

t2.micro

ID de VPC

vpc-0ecd50cc0ca6de2dc (SecureVPC)

ID de subred

subnet-0d3457ac24f108c50 (Public-Subnet-1)

ARN de instancia

arn:aws:ec2:us-east-1:539275684747:instance/i-00755a3660c5d5bcc

Direcciones IPv4 privadas

10.0.0.184

DNS público

-

Direcciones IP elásticas

-

Hallazgo de AWS Compute Optimizer

Suscribirse a AWS Compute Optimizer para recibir recomendaciones. | Más información

Nombre del grupo de Auto Scaling

-

Administradas

falso

Detalles

Estado y alarmas

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

▼ Detalles de la instancia

Información

ID de AMI

ami-0953476d60561c955

Nombre de AMI

al2023-ami-2023.7.20250512.0-kernel-6.1-x86\_64

Detener la protección

desactivado

Recuperación automática de instancias

Predeterminada

Índice de lanzamiento de AMI

0

Especificación de crédito

standard

Operación de uso

RunInstances

Compatibilidad con enclaves

-

Permitir etiquetas en los metadatos de la instancia

desactivado

► Host y grupo de ubicación

Información

▼ Reserva de capacidad

Información

ID de reserva de capacidad

-

Monitoreo

desactivado

Imagen permitida

-

Hora de lanzamiento

Fri May 23 2025 09:07:43 GMT-0500 (hora estándar de Colombia) (about 1 hour)

Ciclo de vida

normal

Par de claves asignado en el lanzamiento

key\_EC2

ID de kernel

-

ID de disco RAM

-

Modo de arranque

uefi-preferred

Utilizar RBN como nombre de host del SO invitado

desactivado

Detalles de la plataforma

Linux/UNIX

Protección de terminación

desactivado

Ubicación de AMI

amazon/al2023-ami-2023.7.20250512.0-kernel-6.1-x86\_64

Comportamiento de detención de hibernación

desactivado

Motivo de transición de estado

-

Mensaje de transición de estado

-

Propietario

539275684747

Modo de arranque de instancia actual

legacy-bios

Responder a RBN de DNS de nombre de host IPv4

desactivado

Figura 7. EC2 Web-Server-1

Resumen de instancia de i-0b8ccc82e441c84c5 (Web-Server-2)Información

Se ha actualizado hace less than a minute

ID de la instancia

i-0b8ccc82e441c84c5

Dirección IPv6

—

Tipo de nombre de anfitrión

Nombre de IP: ip-10-0-1-4.ec2.internal

Responder al nombre DNS de recurso privado

—

Dirección IP asignada automáticamente

34.224.60.6 [IP pública]

Rol de IAM

—

IMDSv2

Required

Operador

—

Dirección IPv4 pública

34.224.60.6 | dirección abierta

Estado de la instancia

En ejecución

Nombre DNS de IP privada (solo IPv4)

ip-10-0-1-4.ec2.internal

Tipo de instancia

t2.micro

ID de VPC

vpc-0ecd50cc0ca6de2dc (SecureVPC)

ID de subred

subnet-02a6b396b87eee1bd (Public-Subnet-2)

ARN de instancia

arn:aws:ec2:us-east-1:539275684747:instance/i-0b8ccc82e441c84c5

Direcciones IPv4 privadas

10.0.1.4

DNS público

—

Direcciones IP elásticas

—

Hallazgo de AWS Compute Optimizer

Suscribirse a AWS Compute Optimizer para recibir recomendaciones. | Más información

Nombre del grupo de Auto Scaling

—

Administradas

falso

DetallesEstado y alarmasMonitoreoSeguridadRedesAlmacenamientoEtiquetas

▼ Detalles de la instanciaInformación

ID de AMI

ami-0953476d60561c955

Nombre de AMI

al2023-ami-2023.7.20250512.0-kernel-6.1-x86\_64

Detener la protección

desactivado

Recuperación automática de instancias

Predeterminada

Índice de lanzamiento de AMI

0

Especificación de crédito

standard

Operación de uso

RunInstances

Compatibilidad con enclaves

—

Permitir etiquetas en los metadatos de la instancia

desactivado

► Host y grupo de ubicaciónInformación

▼ Reserva de capacidadInformación

ID de reserva de capacidad

—

Monitoreo

desactivado

Imagen permitida

—

Hora de lanzamiento

Fri May 23 2025 09:09:45 GMT-0500 (hora estándar de Colombia) (about 1 h our)

Ciclo de vida

normal

Par de claves asignado en el lanzamiento

key\_EC2

ID de kernel

—

ID de disco RAM

—

Modo de arranque

uefi-preferred

Utilizar RBN como nombre de host del SO invitado

desactivado

Configuración de reserva de capacidad

open

Detalles de la plataforma

Linux/UNIX

Protección de terminación

desactivado

Ubicación de AMI

amazon/al2023-ami-2023.7.20250512.0-kernel-6.1-x86\_64

Comportamiento de detención de hibernación

desactivado

Motivo de transición de estado

—

Mensaje de transición de estado

—

Propietario

539275684747

Modo de arranque de instancia actual

legacy-bios

Responder a RBN de DNS de nombre de host IPv4

desactivado

Figura 8. EC2 Web-Server-2

Una vez creadas, se instalaron los paquetes Apache y se configuraron páginas HTML de prueba para validar la conectividad externa.

13.219.75.200 x +  
No es seguro 13.219.75.200  
Servidor Web desde Web-Server-1 (us-east-1a)

34.224.60.6 x +  
No es seguro 34.224.60.6  
Servidor Web desde Web-Server-2 (us-east-1a)

Figura 9. Servidor web de las instancias Web-Server-1 y Web-Server-2

## Despliegue de instancia privada para base de datos

Se creó una tercera instancia EC2 en la subred privada Private-Subnet-1, sin dirección IP pública, destinada exclusivamente a alojar el servicio de base de datos MariaDB.

- Nombre: DB-Server
- AMI: Amazon Linux 2023
- Grupo de seguridad (SG-DB):

- Permitir conexiones al puerto 3306 únicamente desde el grupo de seguridad SG-Web (tráfico interno desde las instancias web).
- Permitir SSH únicamente desde las instancias públicas (para administración desde Web-Server-1 como jump host).

#### sg-0d7b39a9a0b8b6bcc - SG-DB

Acciones

Detalles

Nombre del grupo de seguridad

SG-DB

ID del grupo de seguridad

sg-0d7b39a9a0b8b6bcc

Descripción

Grupo de seguridad privado

ID de la VPC

vpc-0ecd50cc0ca6de2dc

Propietario

539275684747

Número de reglas de entrada

2 Entradas de permisos

Número de reglas de salida

1 Entrada de permiso

Reglas de entrada

Reglas de salida

Compartiendo : *novedad*

Asociaciones de VPC : *novedad*

Etiquetas

Reglas de entrada (2)

Administrar etiquetas

Editar reglas de entrada

Buscar

<input type="checkbox"/>	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen
<input type="checkbox"/>	-	sgr-0bc6119f85b3a4e7a	-	MySQL/Aurora	TCP	3306	sg-09264a42267cae55e / SG-Web
<input type="checkbox"/>	-	sgr-042d3803bc7af373d	-	SSH	TCP	22	sg-09264a42267cae55e / SG-Web

Figura 10. Grupo de seguridad SG-DB

Resumen de instancia de i-08dcf3a6cd6e839fb (DB-Server)

Información

Conectar

Estado de la instancia

Acciones

Se ha actualizado hace less than a minute

ID de la instancia

i-08dcf3a6cd6e839fb

Dirección IPv6

-

Tipo de nombre de anfitrión

Nombre de IP: ip-10-0-10-186.ec2.internal

Responder al nombre DNS de recurso privado

-

Dirección IP asignada automáticamente

-

Rol de IAM

-

IMDSv2

Required

Operador

-

Dirección IPv4 pública

-

Estado de la instancia

En ejecución

Nombre DNS de IP privada (solo IPv4)

ip-10-0-10-186.ec2.internal

Tipo de instancia

t2.micro

ID de VPC

vpc-0ecd50cc0ca6de2dc (SecureVPC)

ID de subred

subnet-041de040349700ece (Private-Subnet-1)

ARN de instancia

arn:aws:ec2:us-east-1:539275684747:instance/i-08dcf3a6cd6e839fb

Direcciones IPv4 privadas

10.0.10.186

DNS público

-

Direcciones IP elásticas

-

Hallazgo de AWS Compute Optimizer

Suscribirse a AWS Compute Optimizer para recibir recomendaciones. | Más información

Nombre del grupo de Auto Scaling

-

Administradas

falso

Detalles

Estado y alarmas

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

▼ Detalles de la instancia

Información

ID de AMI

ami-0953476d60561c955

Nombre de AMI

al2023-ami-2023.7.20250512.0-kernel-6.1-x86\_64

Detener la protección

desactivado

Recuperación automática de instancias

Predefinida

Índice de lanzamiento de AMI

0

Especificación de crédito

standard

Operación de uso

RunInstances

Compatibilidad con enclaves

-

Permitir etiquetas en los metadatos de la instancia

desactivado

► Host y grupo de ubicación

Información

▼ Reserva de capacidad

Información

ID de reserva de capacidad

-

Monitoreo

desactivado

Imagen permitida

-

Hora de lanzamiento

Fri May 23 2025 09:25:36 GMT-0500 (hora estándar de Colombia) (about 1 h our)

Ciclo de vida

normal

Par de claves asignado en el lanzamiento

key\_EC2

ID de kernel

-

ID de disco RAM

-

Modo de arranque

uefi-preferred

Utilizar RBN como nombre de host del SO invitado

desactivado

Configuración de reserva de capacidad

open

Detalles de la plataforma

Linux/UNIX

Protección de terminación

desactivado

Ubicación de AMI

amazon/al2023-ami-2023.7.20250512.0-kernel-6.1-x86\_64

Comportamiento de detención de hibernación

desactivado

Motivo de transición de estado

-

Mensaje de transición de estado

-

Propietario

539275684747

Modo de arranque de instancia actual

legacy-bios

Responder a RBN de DNS de nombre de host IPv4

desactivado

Figura 11. EC2 DB-Server



Dado que la instancia se encuentra en una subred privada, se configuró un NAT Gateway en la subred pública Public-Subnet-1, asociado a una IP elástica, y se editó la tabla de ruteo privada para permitir tráfico de salida hacia Internet exclusivamente mediante dicho NAT.

52.54.68.218

Acciones

Dirección IP elástica asociada

Resumen

Dirección IPv4 asignada

52.54.68.218

ID de asociación

eipassoc-0804d4c9905fcd378

ID de interfaz de red

eni-0e5307a92f3b5dd38

Grupo de direcciones

Amazon

Tipo

IP pública

Ámbito

VPC

ID de la cuenta del propietario de la interfaz de red

539275684747

Grupo fronterizo de red

us-east-1

ID de asignación

eipalloc-0b54bbcedcfad934a

ID de instancia asociada

-

DNS público

-

Registro DNS inverso

-

Dirección IP privada

10.0.0.197

ID de puerta de enlace de NAT

nat-0a492e6a26cf8bd46 (NAT-Gateway)

Etiquetas(1)

Administrar etiquetas

Figura 12. IP elástica

nat-0a492e6a26cf8bd46 / NAT-Gateway

Acciones

Detalles

ID de gateway NAT

nat-0a492e6a26cf8bd46

ARN de puerta de enlace NAT

arn:aws:ec2:us-east-1:539275684747:natgateway/nat-0a492e6a26cf8bd46

VPC

vpc-0ecd50cc0ca6de2dc / SecureVPC

Tipo de conectividad

Public

Dirección IPv4 principal

52.54.68.218

Subred

subnet-0d3457ac24f108c50 / Public-Subnet-1

Estado

Available

Dirección IPv4 privada principal

10.0.0.197

Creado

viernes, 23 de mayo de 2025, 10:01:31 GMT-5

Mensaje de estado

Información

-

ID de interfaz de red principal

eni-0e5307a92f3b5dd38

Eliminado

-

Direcciones IPv4 secundarias

Monitoreo

Etiquetas

Direcciones IPv4 secundarias

Editar asociaciones de direcciones IPv4 secundarias

Buscar

Figura 13. NAT-Gateway

rtb-0e9b023025cbf76b3 / Private-RT

Acciones

Detalles

ID de tabla de enrutamiento

rtb-0e9b023025cbf76b3

VPC

vpc-0ecd50cc0ca6de2dc | SecureVPC

Principal

Sí

ID de propietario

539275684747

Asociaciones de subredes explícitas

2 subredes

Asociaciones de borde

-

Rutas

Asociaciones de subredes

Asociaciones de borde

Propagación de rutas

Etiquetas

Rutas (2)

Ambos

Editar rutas

Filtrar rutas

Figura 14. Tabla de enrutamiento Private-RT

Esto permitió instalar correctamente MariaDB 10.5 mediante dnf y habilitar su servicio con los siguientes comandos:

- sudo systemctl start mariadb
- sudo systemctl enable mariadb

```
[ec2-user@ip-10-0-10-186 ~]$ sudo systemctl start mariadb
[ec2-user@ip-10-0-10-186 ~]$ sudo systemctl enable mariadb
Created symlink /etc/systemd/system/mysql.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/mysqld.service → /usr/lib/systemd/system/mariadb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/mariadb.service → /usr/lib/systemd/system/mariadb.service.
[ec2-user@ip-10-0-10-186 ~]$ sudo systemctl status mariadb
● mariadb.service - MariaDB 10.5 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-05-23 15:06:49 UTC; 12s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
  Main PID: 28250 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 10 (limit: 1111)
  Memory: 66.1M
       CPU: 407ms
    CGroup: /system.slice/mariadb.service
            └─28250 /usr/libexec/mariabdd --basedir=/usr

May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: The second is mysql@localhost, it has no password either, but
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: you need to be the system 'mysql' user to connect.
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: After connecting you can set the password, if you would need to be
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: able to connect as any of these users with a password and without sudo
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: See the MariaDB Knowledgebase at https://mariadb.com/kb
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: Please report any problems at https://mariadb.org/jira
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: The latest information about MariaDB is available at https://mariadb.org/.
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: Consider joining MariaDB's strong and vibrant community:
May 23 15:06:49 ip-10-0-10-186.ec2.internal mariadb-prepare-db-dir[28207]: https://mariadb.org/get-involved/
May 23 15:06:49 ip-10-0-10-186.ec2.internal systemd[1]: Started mariadb.service - MariaDB 10.5 database server.
[ec2-user@ip-10-0-10-186 ~]$
```

*Figura 15. Instalación de MariaDB en la base de datos*

Luego, se procedió a crear una base de datos, con un usuario remoto y se configuró el archivo /etc/my.cnf para permitir conexiones remotas desde las instancias web:

- Usuario: user
- Contraseña: student12

```
ec2-user@ip-10-0-10-186:~$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 10.5.25-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE tienda;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'user'@'%' IDENTIFIED BY 'student12';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON tienda.* TO 'user'@'%';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> exit
Bye
[ec2-user@ip-10-0-10-186 ~]$
```

*Figura 16. Base de datos.*

Con estas acciones, se completó exitosamente la arquitectura de cómputo segura en AWS, con separación lógica entre los servidores web públicos y el servidor de base de datos privado, respetando principios de mínima exposición y segmentación de red.

Para probar la conexión a la base de datos, se ingresa a instancia Web-Server-1 y mediante mysql se conecta a la instancia de la base de datos con la IP privada, de la siguiente forma:

```
[ec2-user@ip-10-0-0-184 ~]$ mysql -h 10.0.10.186 -u user -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 4
Server version: 10.5.25-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tienda |
+-----+
2 rows in set (0.001 sec)
```

*Figura 17. Conexión a la base de datos desde Web-Server-1*

### ***Fase 3. Seguridad de Red***

En esta fase se aplicaron mecanismos de control de tráfico a nivel de red para proteger los recursos desplegados en la VPC SecureVPC, cumpliendo con principios de defensa en profundidad, mínimo privilegio y segmentación lógica. Se utilizaron grupos de seguridad (SG) y listas de control de acceso a la red (NACLs), de forma complementaria.

#### ***Grupos de seguridad***

Los grupos de seguridad fueron diseñados para restringir el acceso de manera específica a cada tipo de instancia:

- SG-Web (Instancias públicas):
  - Permitir acceso HTTP (puerto 80) desde cualquier origen (0.0.0.0/0).
  - Permitir acceso SSH (puerto 22) exclusivamente desde la IP pública del administrador.
  - No permite acceso a MySQL ni a otros puertos.
- SG-DB (Instancia privada):
  - Permitir acceso MySQL (puerto 3306) solo desde instancias que usen SG-Web.
  - Permitir SSH (puerto 22) solo desde SG-Web, para administración por salto.
  - No permite accesos desde el exterior.

Esta segmentación garantiza que la base de datos solo es accesible desde la capa de aplicación, y nunca directamente desde Internet.

#### ***Listas de control de acceso ACL***

Se crearon NACLs personalizadas para las subredes públicas y privadas, reforzando el control de tráfico.

- ACL Pública (Public-ACL):  
Aplicada a Public-Subnet-1 y Public-Subnet-2. Las reglas permiten:
  - Entrada:
    1. HTTP (80) desde 0.0.0.0/0
    2. SSH (22) solo desde la IP pública del administrador
    3. Rango efímero (1024–65535) para retorno de tráfico
  - Salida:
    1. Permitir puertos efímeros, HTTP y SSH hacia 0.0.0.0/0
  - Denegación por defecto para todo tráfico no autorizado.

#### acl-045ca0485d3d59a66 / Public-ACL

Acciones ▾

##### Detalles Información

ID de ACL de red  
acl-045ca0485d3d59a66

Asociada a  
2 Subredes

Predeterminada  
No

ID de la VPC  
vpc-0ecd50cc0ca6de2dc / SecureVPC

Propietario  
539275684747

Reglas de entrada | Reglas de salida | Asociaciones de subredes | Etiquetas

##### Reglas de entrada (4)

Editar reglas de entrada

Número de regla	Tipo	Protocolo	Rango de puertos	Origen	Permitir/denegar
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
110	SSH (22)	TCP (6)	22	201.236.221.29/32	Allow
120	TCP personalizado	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

#### acl-045ca0485d3d59a66 / Public-ACL

Acciones ▾

##### Detalles Información

ID de ACL de red  
acl-045ca0485d3d59a66

Asociada a  
2 Subredes

Predeterminada  
No

ID de la VPC  
vpc-0ecd50cc0ca6de2dc / SecureVPC

Propietario  
539275684747

Reglas de entrada | Reglas de salida | Asociaciones de subredes | Etiquetas

##### Reglas de salida (4)

Editar reglas de salida

Número de regla	Tipo	Protocolo	Rango de puertos	Destino	Permitir/denegar
100	TCP personalizado	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
110	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
120	SSH (22)	TCP (6)	22	201.236.221.29/32	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

#### acl-045ca0485d3d59a66 / Public-ACL

Acciones ▾

##### Detalles Información

ID de ACL de red  
acl-045ca0485d3d59a66

Asociada a  
2 Subredes

Predeterminada  
No

ID de la VPC  
vpc-0ecd50cc0ca6de2dc / SecureVPC

Propietario  
539275684747

Reglas de entrada | Reglas de salida | Asociaciones de subredes | Etiquetas

##### Asociaciones de subredes (2)

Editar asociaciones de subredes

Nombre	ID de subred	Asociada a	Zona de disponibilidad	CIDR IPv4	CIDR IPv6
Public-Subnet-2	subnet-02a6b396b87eee1bd	acl-045ca0485d3d59a66 / Public-ACL	us-east-1b	10.0.1.0/24	-
Public-Subnet-1	subnet-0d3457ac24f108c50	acl-045ca0485d3d59a66 / Public-ACL	us-east-1a	10.0.0.0/24	-

Figura 18. Configuración de ACL Public-ACL

- ACL Privada (Private-ACL):  
Aplicada a Private-Subnet-1 y Private-Subnet-2. Las reglas permiten:
  - Entrada: MySQL (3306), SSH (22) y puertos efimeros desde la red interna 10.0.0.0/16
  - Salida: Puertos efimeros, MySQL y SSH hacia la red interna y a través del NAT Gateway
  - Denegación explícita para todo lo no definido.

acl-0901d36745f077a92 / Private-ACL

Detalles

ID de ACL de red

acl-0901d36745f077a92

Asociada a

2 Subredes

Predeterminada

No

ID de la VPC

vpc-0ecd50cc0ca6de2dc / SecureVPC

Propietario

539275684747

Reglas de entrada

Reglas de salida

Asociaciones de subredes

Etiquetas

Reglas de entrada (4)

Filter inbound rules

1

<

>

⚙

Número de regla	Tipo	Protocolo	Rango de puertos	Origen	Permitir/denegar
100	MySQL/Aurora (3306)	TCP (6)	3306	10.0.0.0/16	Allow
110	SSH (22)	TCP (6)	22	10.0.0.0/16	Allow
120	TCP personalizado	TCP (6)	1024 - 65535	10.0.0.0/16	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

acl-0901d36745f077a92 / Private-ACL

Detalles

ID de ACL de red

acl-0901d36745f077a92

Asociada a

2 Subredes

Predeterminada

No

ID de la VPC

vpc-0ecd50cc0ca6de2dc / SecureVPC

Propietario

539275684747

Reglas de entrada

Reglas de salida

Asociaciones de subredes

Etiquetas

Reglas de salida (4)

Filter outbound rules

1

<

>

⚙

Número de regla	Tipo	Protocolo	Rango de puertos	Destino	Permitir/denegar
100	TCP personalizado	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
110	MySQL/Aurora (3306)	TCP (6)	3306	10.0.0.0/16	Allow
120	SSH (22)	TCP (6)	22	10.0.0.0/16	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

acl-0901d36745f077a92 / Private-ACL

Detalles

ID de ACL de red

acl-0901d36745f077a92

Asociada a

2 Subredes

Predeterminada

No

ID de la VPC

vpc-0ecd50cc0ca6de2dc / SecureVPC

Propietario

539275684747

Reglas de entrada

Reglas de salida

Asociaciones de subredes

Etiquetas

Asociaciones de subredes (2)

Filter subnet associations

1

<

>

⚙

Nombre	ID de subred	Asociada a	Zona de disponibilidad	CIDR IPv4	CIDR IPv6
Private-Subnet-1	subnet-041de040349700ece	acl-0901d36745f077a92 / Private-ACL	us-east-1a	10.0.10.0/24	-
Private-Subnet-2	subnet-0a70a77d9fdc1d503	acl-0901d36745f077a92 / Private-ACL	us-east-1b	10.0.11.0/24	-

Figura 19. Configuración de ACL Private-ACL

Esta configuración asegura que el tráfico entre subredes está restringido y auditado, mientras que el acceso público a las instancias está controlado con reglas precisas.

Fase 4: Gestión de Identidades (IAM)

Durante el desarrollo de esta fase, se intentó crear usuarios IAM con diferentes niveles de acceso para aplicar control de identidades siguiendo las buenas prácticas de seguridad. Sin embargo, el entorno proporcionado por AWS Academy Learner Lab restringe ciertas operaciones administrativas, como iam:CreateUser, impidiendo completar esta etapa.

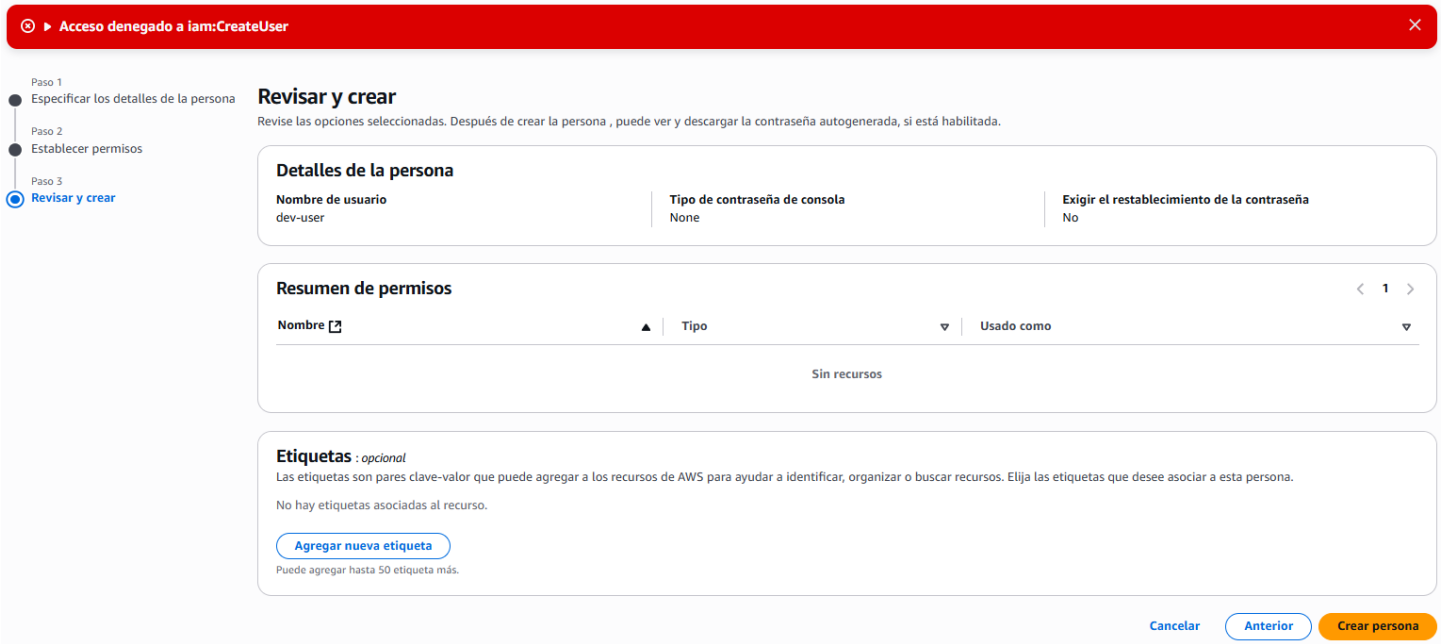


Figura 20. Error al crear usuarios en IAM

Fase 5. Almacenamiento Seguro (S3)

Con el objetivo de aplicar buenas prácticas de seguridad y almacenamiento en la nube, se configuraron dos buckets en Amazon S3:

- 1. webapp-static-files-v1: destinado a almacenar archivos estáticos de la aplicación web, como el archivo index.html.

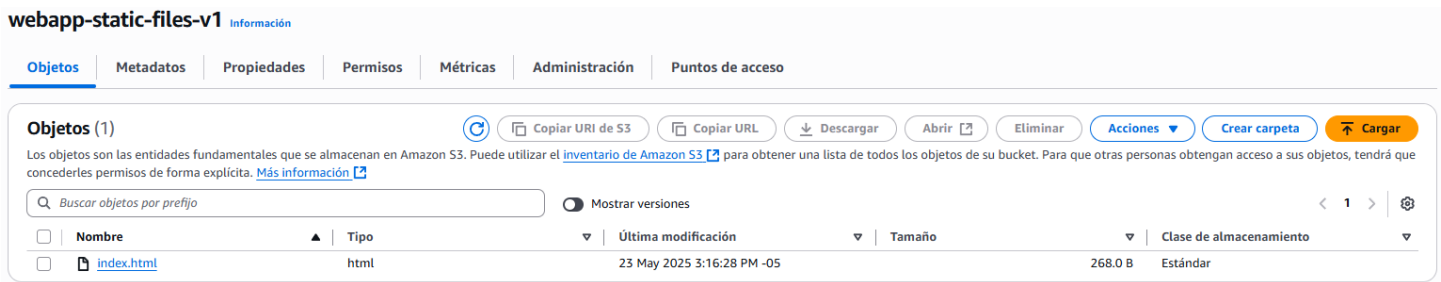


Figura 21. Bucket S3 webapp-static-files-v1

- 2. webapp-audit-logs-v2: utilizado como destino para almacenar los logs de acceso generados por el bucket anterior, activando el registro del servidor desde sus propiedades.

**Objetos (0)** [Copiar URI de S3](#) [Copiar URL](#) [Descargar](#) [Abrir](#) [Eliminar](#) [Acciones](#) [Crear carpeta](#) [Cargar](#)

Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

☐ Mostrar versiones < 1 > [Configuración](#)

<input type="checkbox"/>	Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
No hay objetos No tiene objetos en este bucket.					
<a href="#">Cargar</a>					

Figura 21. Bucket S3 webapp-audit-logs-v2

Ambos buckets fueron configurados con:

- Versionado habilitado, permitiendo mantener un historial de cambios de los objetos.
- Cifrado del lado del servidor (SSE-S3), activado por defecto para proteger los datos en reposo.
- Bloqueo de acceso público desactivado únicamente en el bucket de archivos estáticos, con intención de permitir el acceso público al archivo index.html.

Se intentó aplicar una política de bucket pública para habilitar el acceso anónimo a los archivos del bucket webapp-static-files-v1, con la siguiente política:

**Política de bucket** [Ejemplos de políticas](#) [Generador de políticas](#)

La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

**ARN del bucket**  
[arn:aws:s3::webapp-static-files-v1](#)

**Política**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3::webapp-static-files-v1/*"
10    }
11  ]
12 }
13
```

**Editar instrucción**

**Seleccionar una instrucción**  
Seleccione una instrucción existente en la política o agregue una nueva instrucción.  
[+ Agregar nueva instrucción](#)

[+ Agregar nueva instrucción](#)

JSON Ln 13, Col 0

Seguridad: 0 Errores: 0 Advertencias: 0 Sugerencias: 0 [Vista previa del acceso externo](#)

**Necesita permisos**  
User: arn:aws:sts:539275684747:assumed-role/voclabs/user3843070-felipe.ibarra1@utp.edu.co is not authorized to perform: access-analyzer:ValidatePolicy on resource: arn:aws:access-analyzer:us-east-1:539275684747:\* [Diagnose with Amazon Q](#)

Figura 22. Error access-analyzer:ValidatePolicy AccessDenied

Sin embargo, el entorno AWS Academy Learner Lab restringe ciertas acciones administrativas, y se recibió un error al intentar aplicar esta política: access-analyzer:ValidatePolicy AccessDenied, lo cual impidió que los objetos fueran accesibles públicamente como parte de un sitio web estático.

A pesar de esto, se logró:

- Subir correctamente el archivo index.html.
- Confirmar que el archivo fue versionado y cifrado automáticamente.
- Redirigir correctamente los logs del bucket estático hacia el bucket de auditoría (webapp-audit-logs-v2), cumpliendo con los principios de trazabilidad y supervisión.

index.html

Información

Copiar URI de S3

Descargar

Abrir

Acciones de objetos

Propiedades

Permisos

Versiones

Versiones (2)

Descargar

Abrir

Eliminar

Acciones

<input type="checkbox"/>	ID de versión	Tipo	Última modificación	Tamaño	Clase de almacenamiento
<input type="checkbox"/>	XE09hEByn6WckRrm5NWv3MbH0GV... (Versión actual)	html	23 May 2025 3:24:28 PM -05	292.0 B	Estándar
<input type="checkbox"/>	Qvau6_vlvOAAI58a36XBLMBkxibh...	html	23 May 2025 3:16:28 PM -05	268.0 B	Estándar

Figura 23. Control de versiones de webapp-static-files-v1

webapp-audit-logs-v2

Información

Objetos

Metadatos

Propiedades

Permisos

Métricas

Administración

Puntos de acceso

Objetos (25)

Buscar objetos por prefijo

Mostrar versiones

Copiar URI de S3

Copiar URL

Descargar

Abrir

Eliminar

Acciones

Crear carpeta

Cargar

Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

<input type="checkbox"/>	Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
<input type="checkbox"/>	2025-05-23-21-14-36-39DEF457B8E991A1	-	23 May 2025 4:14:37 PM -05	1.3 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-15-22-4FE1DF009D4BDDE3	-	23 May 2025 4:15:23 PM -05	1.3 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-15-24-ED987F19448CC5D8	-	23 May 2025 4:15:25 PM -05	4.3 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-15-25-3EA4DCEA36877024	-	23 May 2025 4:15:26 PM -05	658.0 B	Estándar
<input type="checkbox"/>	2025-05-23-21-15-38-933C2CB682F32C3F	-	23 May 2025 4:15:39 PM -05	6.9 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-16-32-8794F9EDA34C0122	-	23 May 2025 4:16:33 PM -05	2.6 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-16-46-C3912D438BD2C1B9	-	23 May 2025 4:16:47 PM -05	1.0 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-17-44-F6C49624B8369296	-	23 May 2025 4:17:45 PM -05	1.4 KB	Estándar
<input type="checkbox"/>	2025-05-23-21-19-44-F6C4CAFF1B977543	-	23 May 2025 4:19:45 PM -05	1.3 KB	Estándar

Figura 24. Registro de logs

Fase 6. Diagrama de Arquitectura

La siguiente figura representa la arquitectura implementada en AWS durante el desarrollo del laboratorio. Esta solución fue diseñada siguiendo las buenas prácticas de seguridad, alta disponibilidad y segmentación por capas.



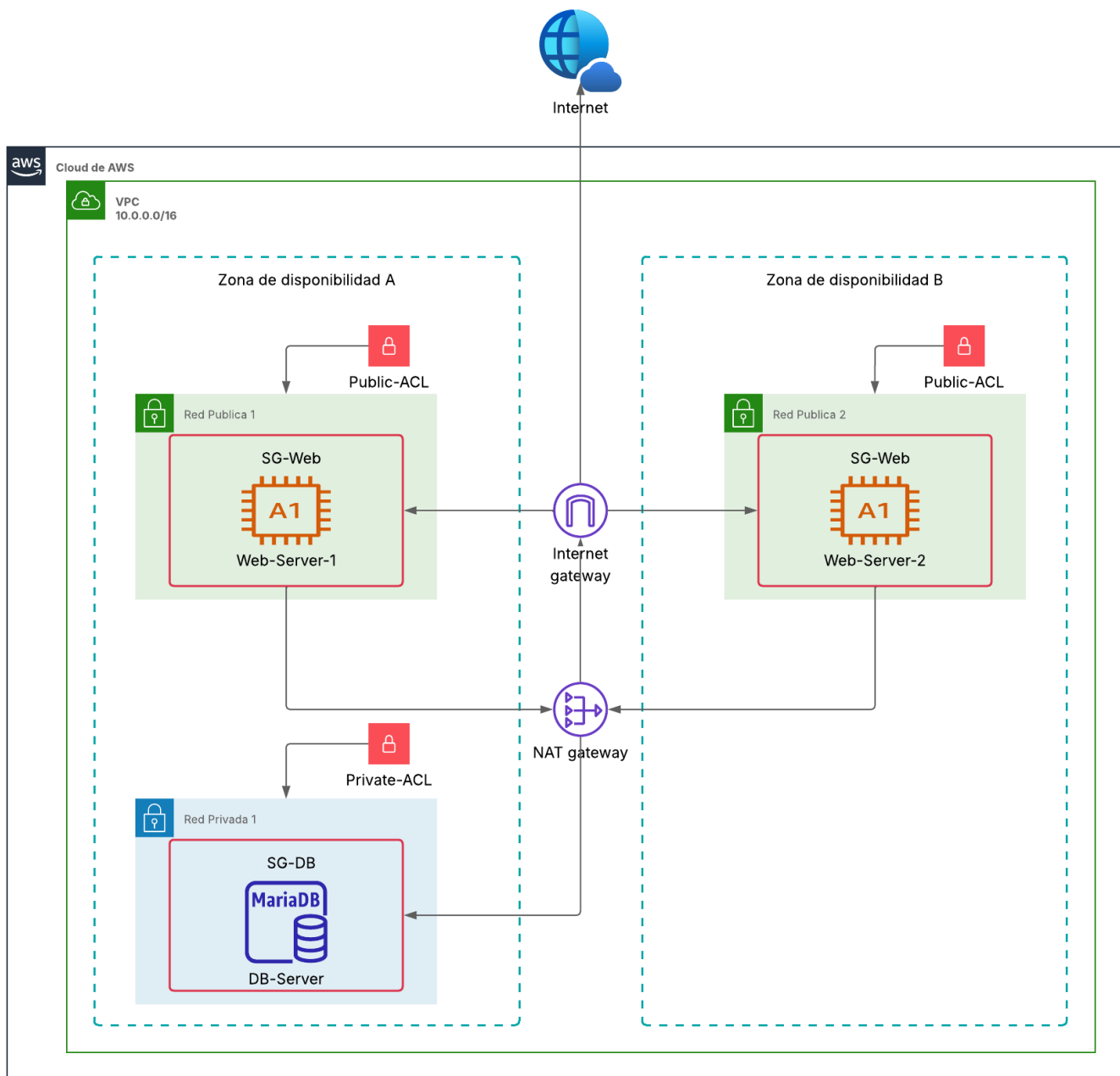


Figura 25. Diagrama de arquitectura

### Pruebas de conectividad y acceso

#### Conexión a la Base de Datos Privada (DB-Server)

Dado que la instancia DB-Server se encuentra en una subred privada, sin dirección IP pública, no es posible conectarse directamente a ella desde Internet. Por seguridad y siguiendo buenas prácticas de arquitectura en AWS, se utilizó un modelo de salto (jump host) para acceder a la base de datos desde una instancia pública (Web-Server-1).

Desde la máquina local (o mediante EC2 Instance Connect), se conecta primero a la instancia Web-Server-1 que está en la subred pública:

```

ec2-user@ip-10-0-10-186:~$ cd C:\Users\Felipe Ibarra\OneDrive - Universidad Tecnológica de Pereira\Desktop\esp_TIC\ciberseguridad_cloud\actividad_final>dir
C:\Users\Felipe Ibarra\OneDrive - Universidad Tecnológica de Pereira\Desktop\esp_TIC\ciberseguridad_cloud\actividad_final>dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 54BC-09F4

Directorio de C:\Users\Felipe Ibarra\OneDrive - Universidad Tecnológica de Pereira\Desktop\esp_TIC\ciberseguridad_cloud\actividad_final

29/05/2025 09:11 p. m. <DIR> .
22/05/2025 08:01 p. m. <DIR> ..
29/05/2025 07:20 p. m. 2.869.484 actividad_final.docx
23/05/2025 03:23 p. m. 292 index.html
23/05/2025 09:03 a. m. 1.674 key_EC2.pem
22/05/2025 07:55 p. m. 409.796 Trabajo final.pdf
4 archivos 3.281.246 bytes
2 dirs 258.833.027.072 bytes libres

C:\Users\Felipe Ibarra\OneDrive - Universidad Tecnológica de Pereira\Desktop\esp_TIC\ciberseguridad_cloud\actividad_final>ssh -i key_EC2.pem ec2-user@54.163.145.129
#
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Fri May 30 02:54:53 2025 from 186.86.14.77
[ec2-user@ip-10-0-0-184 ~]$ ls
key_EC2.pem
[ec2-user@ip-10-0-0-184 ~]$ ssh -i key_EC2.pem ec2-user@10.0.10.186
#
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Fri May 30 02:55:30 2025 from 10.0.0.184
[ec2-user@ip-10-0-10-186 ~]$ ls
[ec2-user@ip-10-0-10-186 ~]$

```

Figura 26. Conexión a DB-Server desde Web-Server-1 mediante SSH

[illegible]

Figura 27. Conexión a DB-Server desde Web-Server-2 mediante SSH

```
ec2-user@ip-10-0-1-4:~$ mysql -h 10.0.10.186 -u user -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 10.5.25-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tienda    |
+-----+
2 rows in set (0.001 sec)

MariaDB [(none)]> use tienda;
Database changed
MariaDB [tienda]> show tables;
Empty set (0.001 sec)

MariaDB [tienda]> |
```

*Figura 28. Conexión a DB-Server desde Web-Server-2 mediante MYSQL*

## Conclusiones

A lo largo del desarrollo de este laboratorio se implementó una arquitectura completa y segura en AWS, utilizando servicios fundamentales como VPC, subredes públicas y privadas, instancias EC2, buckets S3, grupos de seguridad, ACLs y NAT Gateway. La solución fue diseñada siguiendo buenas prácticas de segmentación, aislamiento de capas y control de accesos, permitiendo el despliegue de una aplicación distribuida con separación entre la capa web y la capa de datos, junto con almacenamiento externo en S3 para archivos estáticos y logs de auditoría. A pesar de las restricciones del entorno AWS Academy Learner Lab, que limitaron el uso de roles y usuarios IAM o la aplicación de ciertas políticas públicas, se documentó adecuadamente cómo se habría resuelto cada caso en un entorno productivo real.

Durante el proceso, se comprobó la importancia de un diseño planificado en la configuración de reglas de red, flujos de tráfico y acceso a recursos. La creación de buckets con cifrado, versionado y trazabilidad, el uso de Security Groups precisos, y la implementación de ACLs para reforzar el control a nivel de subred, permitieron aplicar los principios de seguridad desde la arquitectura. La validación de cada fase, incluyendo pruebas de conectividad, acceso restringido, y la interacción controlada entre servicios, reforzó la comprensión de cómo funciona la infraestructura en la nube y la responsabilidad compartida en la gestión de la misma.

En general, este laboratorio no solo permitió aplicar conocimientos técnicos sobre los servicios de AWS, sino que fortaleció habilidades clave como el razonamiento lógico, la documentación técnica, y la capacidad de solucionar problemas en entornos reales con limitaciones. El trabajo realizado evidencia la capacidad para diseñar soluciones sólidas, seguras y escalables en la nube, y marca una base sólida para enfrentar desafíos más complejos en entornos empresariales o profesionales.