

AWS USER GROUP MEDELLÍN

# Cloud Practitioner Challenge



O'REILLY®



rootstack

---

@awsugmed

# Identidad y seguridad en AWS

Cristian Pavony



# Agenda

Modelo de responsabilidad compartida

- 1      Modelo de responsabilidad compartida
- 2      AWS IAM (Identity and Access Management): usuarios, roles, políticas, permisos
- 3      Seguridad en la red: Security Groups y Network ACLs
- 4      Protección de datos en reposo y en tránsito
- 5      Otros servicios de seguridad en AWS
- 6      Seguridad en el examen de certificación CLF-C02





# 01

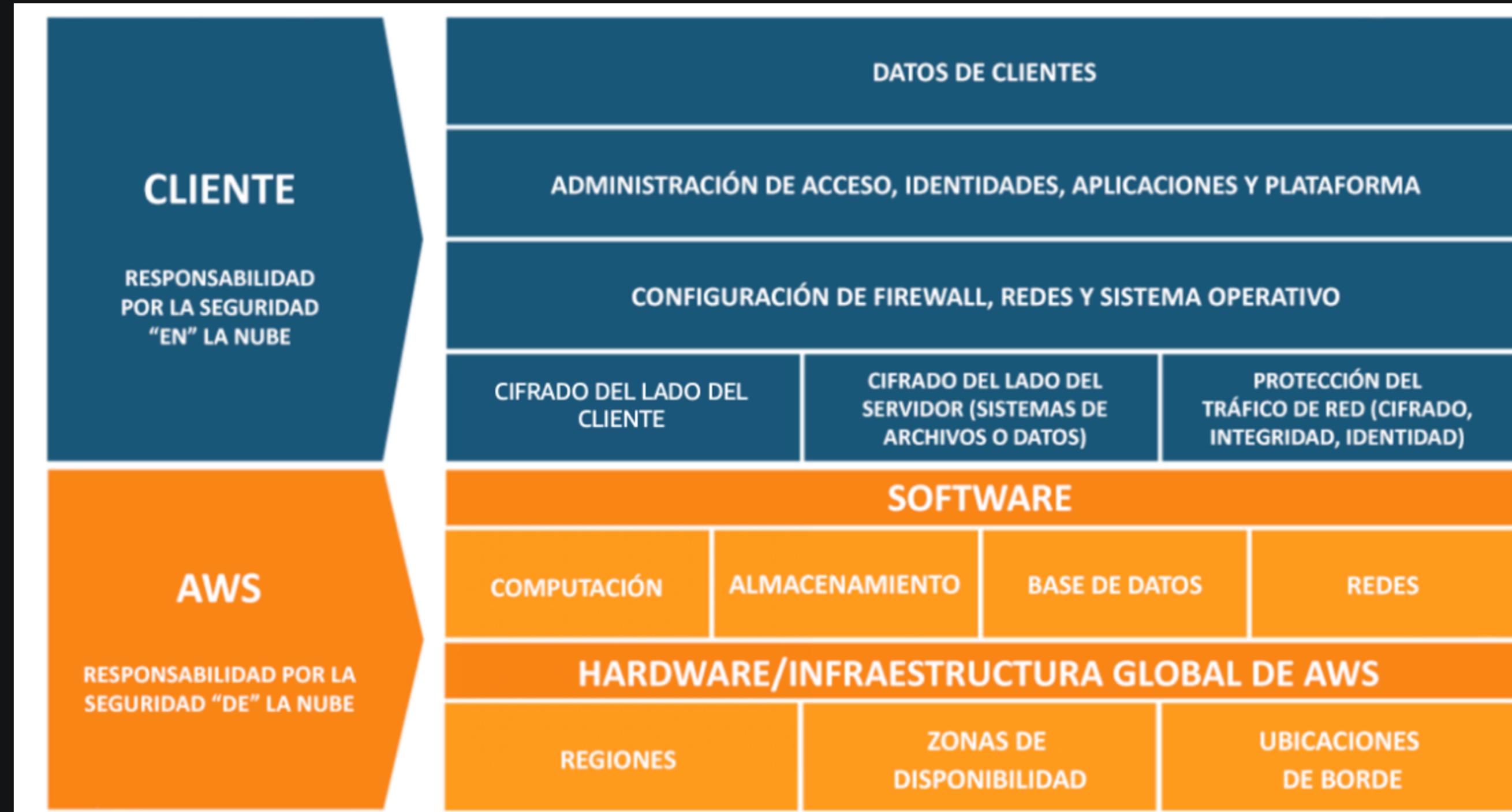
## Modelo de responsabilidad compartida (Shared Responsibility Model)

¿Quién es responsable de mantener seguros los recursos en AWS:  
tú (el cliente de AWS) o AWS?



**La respuesta es: Sí  
¡ambos!**

# Modelo de responsabilidad compartida (Shared Responsibility Model)

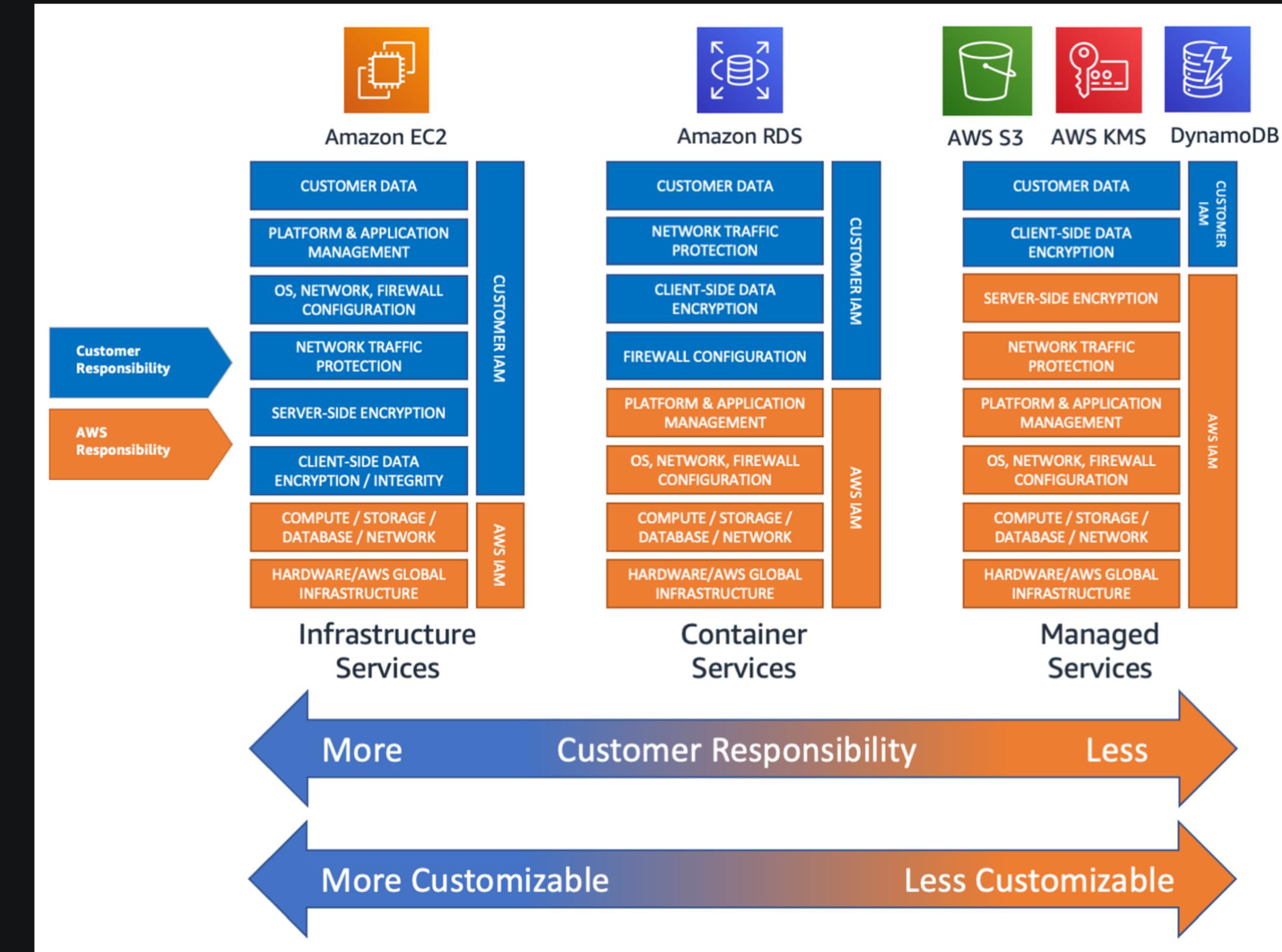


# Modelo de responsabilidad compartida (Shared Responsibility Model)



# Modelo de responsabilidad compartida (Shared Responsibility Model)

Las responsabilidades (y control) varían en función del servicio elegido por el cliente





# 02

## AWS IAM (Identity and Access Management)

Autenticación y autorización como servicio



**It's free!**

# AWS IAM (Identity and Access Management)

Autenticar



¿Quién soy en el sistema?

Autorizar



¿Qué puedo hacer en el sistema?



# AWS IAM (Identity and Access Management)

## Usuario



Identidad que representa una persona o app que interactúa con servicios y recursos de AWS.

## Política



Documento que permite o deniega permisos en servicios y recursos de AWS.

## Grupo



Identidad para agrupar usuarios de IAM

## Rol



Identidad que puedes asumir para tener temporalmente los permisos asociados a ella.



# AWS IAM (Identity and Access Management)

## Características

### Usuario



- Username + credenciales
- Passwd/Access Keys
- Sin permisos por defecto, salvo Root
- No usar Root

### Política



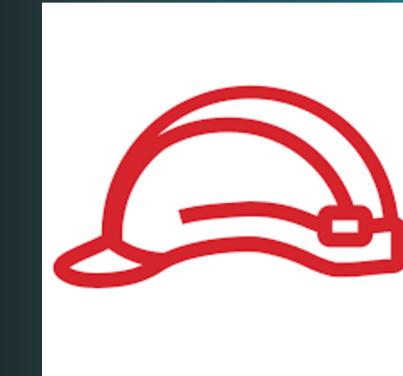
- JSON
- Basadas en identidad o recurso
- Principio de mínimo privilegio

### Grupo



- Permisos aplicados a un grupo se aplican a todos los miembros del grupo
- Facilita admon.

### Rol



- Política/relación de confianza (recurso)
- Política de permisos (identidad)
- ¡Credenciales temporales!



# AWS IAM (Identity and Access Management)

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "secretsmanager:GetSecretValue",  
            "Resource": "arn:aws:secretsmanager:us-east-1:5████████:secret:secreto"  
        }  
    ]  
}
```

1

Ejemplo: Política de permisos (Política basada en identidad)

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::123456789012:user/Juan"  
            },  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::mi-bucket-ejemplo/*"  
        }  
    ]  
}
```

2

Ejemplo: Política de bucket (Política basada en recurso)





# 03

## Seguridad en la red: Security Groups y Network ACLs



Protección esencial para tu VPC

# Seguridad en la red: Security Groups y Network ACLs

## Conceptos básicos de red en AWS

Amazon VPC permite aprovisionar una segmento de red aislado dentro de la nube de AWS.

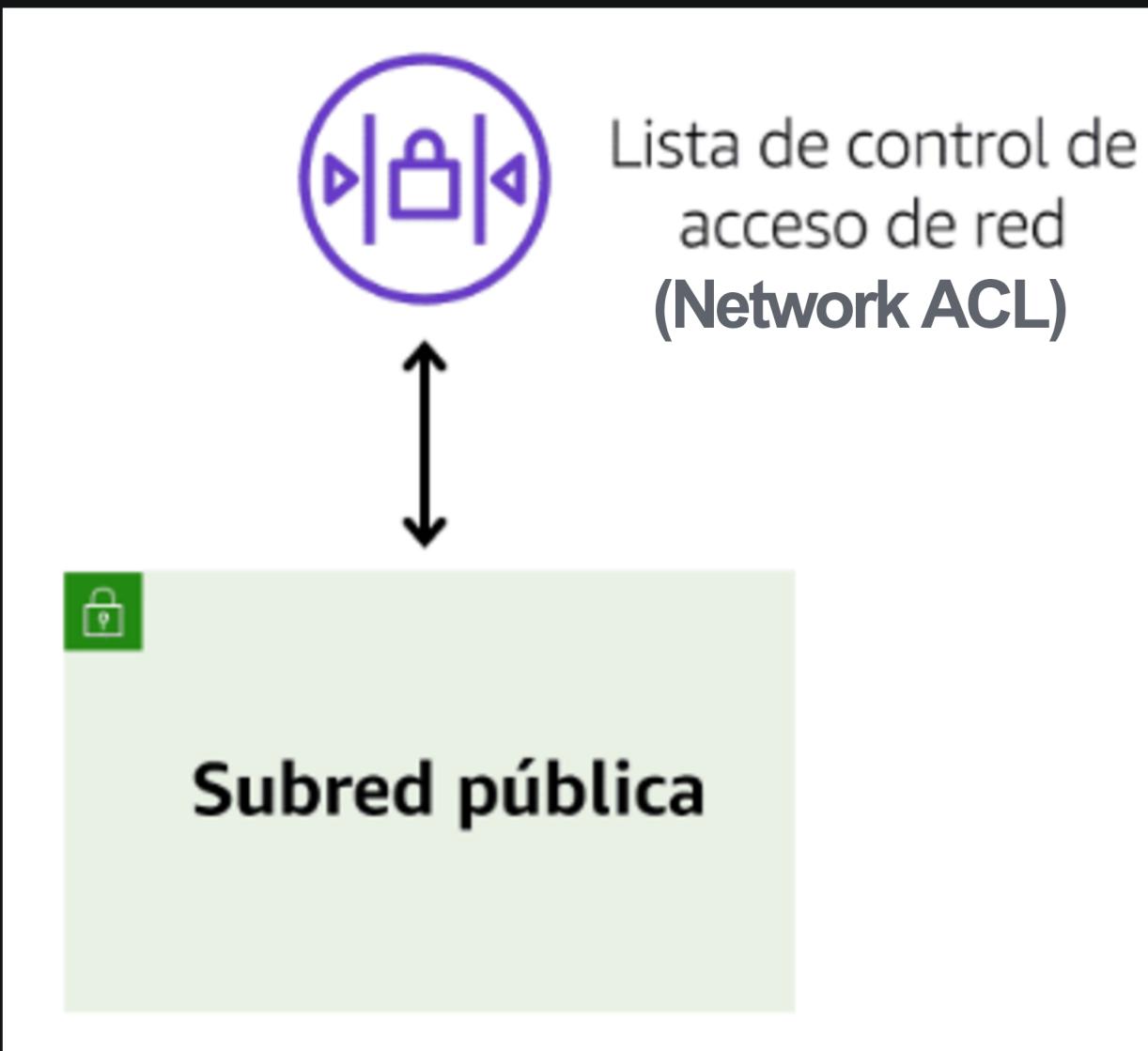
**Subredes (subnets):** segmentos de red de una VPC para desplegar recursos.

\***Públicas (public):** Pueden ser accedidas desde internet (ej. para mi frontend)

\***Privadas (private):** No pueden ser accedidas desde internet (ej. para BDs)



# Seguridad en la red: Security Groups y Network ACLs



Una ACL de red es un **firewall** virtual que controla el tráfico a **nivel de subred**.

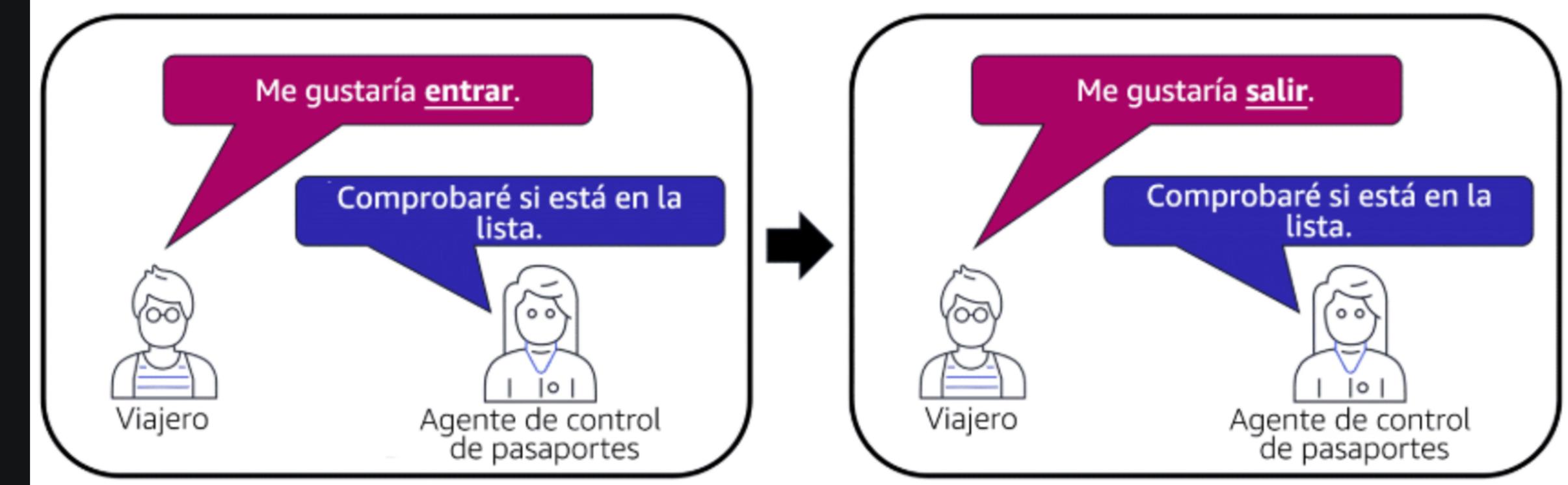


Un grupo de seguridad es un **firewall** virtual que controla el tráfico de **una o varias instancias\***.

# Seguridad en la red: Security Groups y Network ACLs

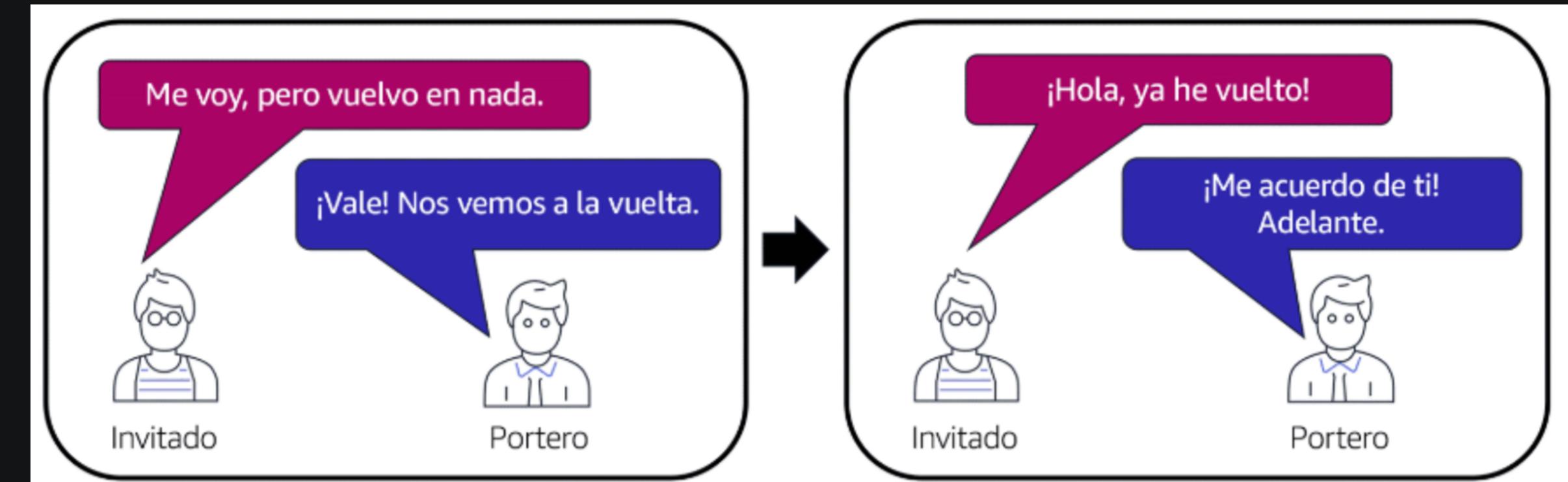
**Las NACL  
son sin  
estado  
(stateless)**

Debo definir  
reglas en cada  
sentido



**Los SG son  
con estado  
(stateful)**

Debo definir  
reglas en un  
sólo sentido





# 04

## Protección de datos en reposo y en tránsito



Cifrado  
Djgsbep

# Protección de datos en reposo

Guardamos los datos cifrados (en S3, BDs, etc.)

Cifrado del lado del cliente

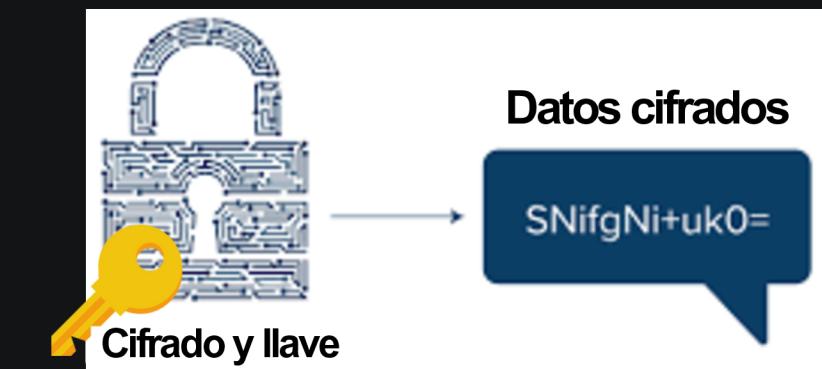


Ambiente del cliente

Cifrado del lado del servidor



Ambiente del cliente



# Protección de datos en reposo

## AWS KMS



Crear, almacenar,  
administrar y usar  
**llaves**  
**criptográficas**  
utilizadas para cifrar  
datos

## AWS CloudHSM



Similar a KMS pero  
con **hardware**  
**dedicado** y admin.  
del servicio por el  
cliente

## Macie



**Descubrir y**  
**clasificar info.**  
**confidencial** en  
AWS de manera  
automática



# Protección de datos en tránsito

Datos cifrados mientras se transmiten por las redes

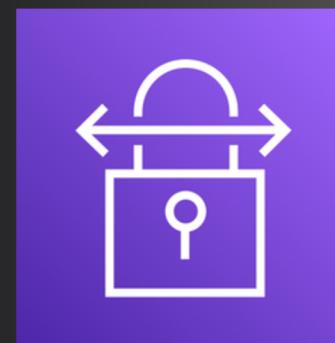


TLS, SSH



Conexión segura a APIs y recursos AWS con estos protocolos (ej HTTPS, SMTPS, WSS)

IPSEC



AWS Site-to-site VPN: conexión cifrada entre tu red on-prem y AWS

ACM



AWS Certificate Manager: Generar y administrar certificados digitales



# 05

## Otros servicios de seguridad en AWS



¡Espera, hay más!  
(y no son todos 😊)

# Otros servicios de seguridad en AWS

## WAF



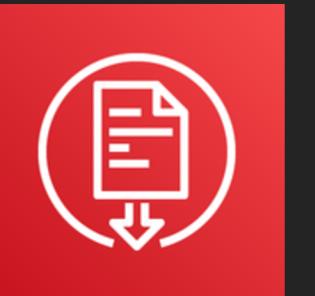
Protección contra ataques a aplicaciones web

## Shield



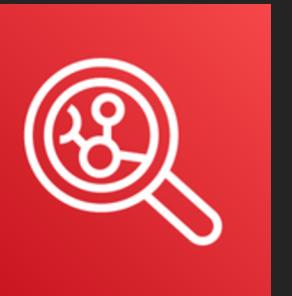
Protección contra ataques DDoS

## Artifact



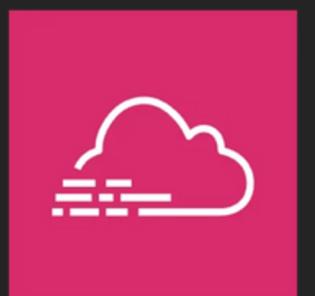
Descarga de informes de auditoría y acuerdos de servicio

## Inspector



Automáticamente evalúa desviaciones de seguridad y detecta vulnerabilidades

## CloudTrail



Registro de eventos en tu cuenta de AWS

## GuardDuty



Detección inteligente de amenazas para tu infra. y recursos de AWS



**+ info**



# 06

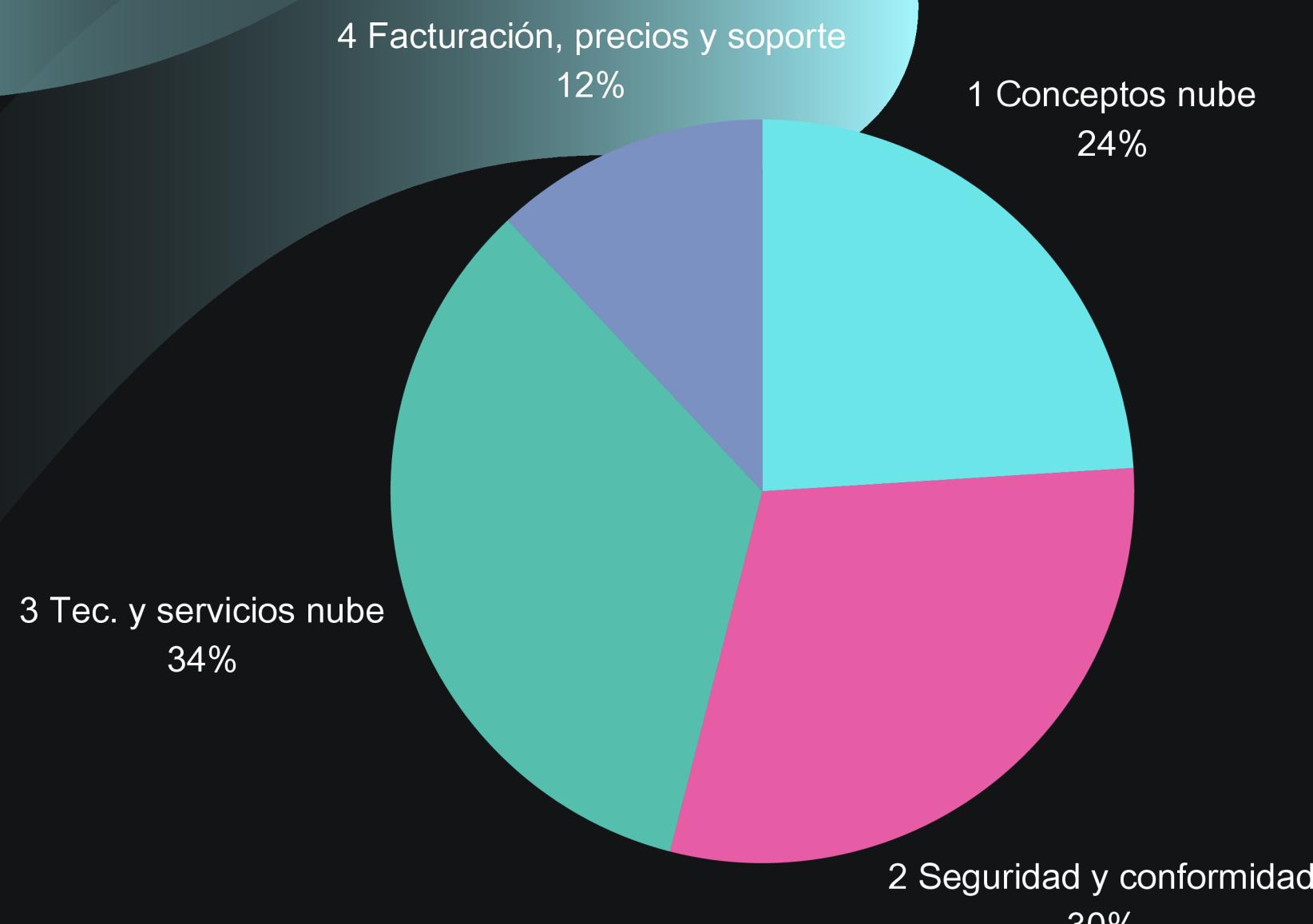
## Seguridad en el examen de certificación CLF-C02

Recursos que te servirán

Para que  
aprendas más 😎



# Seguridad en el examen de certificación CLF-C02



**Porcentaje de preguntas con puntaje por dominio (tema) del examen**

## + Recursos de estudio

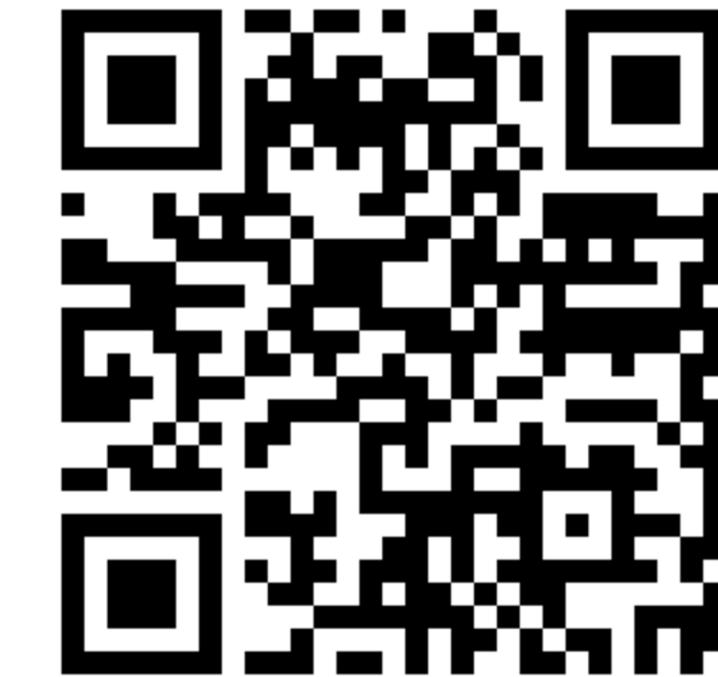
- [Guía del exámen](#)
- [Web oficial del examen con links a los cursos de preparación](#)
- [Examen de práctica \(multiidioma\)](#)



# Nuestras redes



Conecta con  
nosotros



Actualízate sobre  
el Challenge



# Patrocinadores



rootstack

O'REILLY®



# Muchas gracias



🌟 ¡Gracias por ser parte del AWS Cloud Practitioner Challenge! 🌟

¡Mucho éxito y vamos a explorar el mundo de AWS! 💡🔥

