


BIENVENIDOS



Cloud Clubs aws Student Community Day — Medellín —



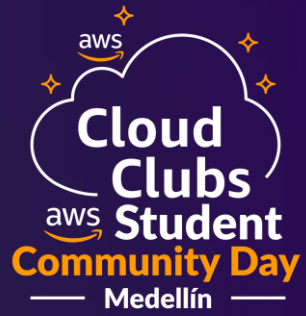


Fundamentos seguridad en AWS

Cristian Pavony

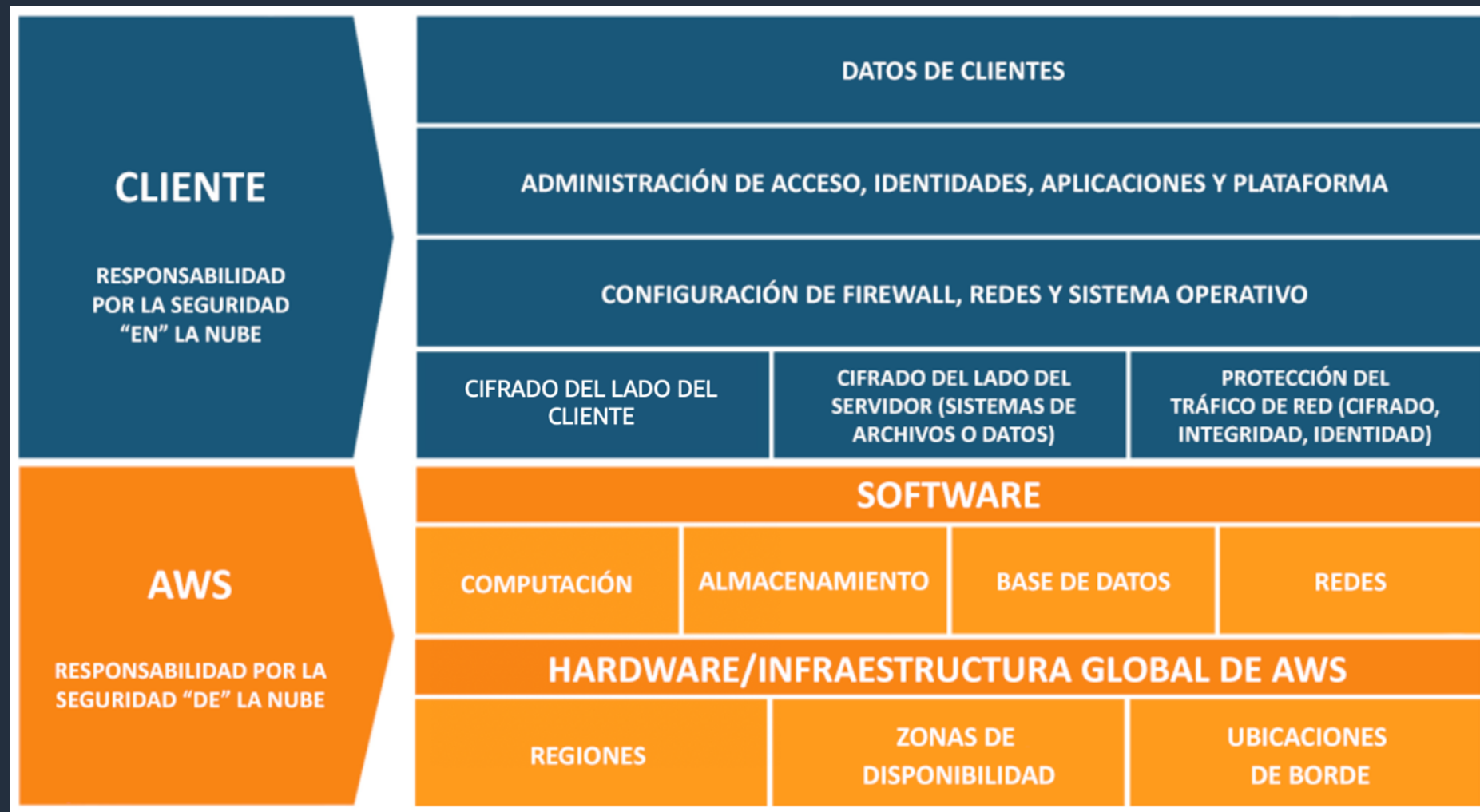
Septiembre 2025



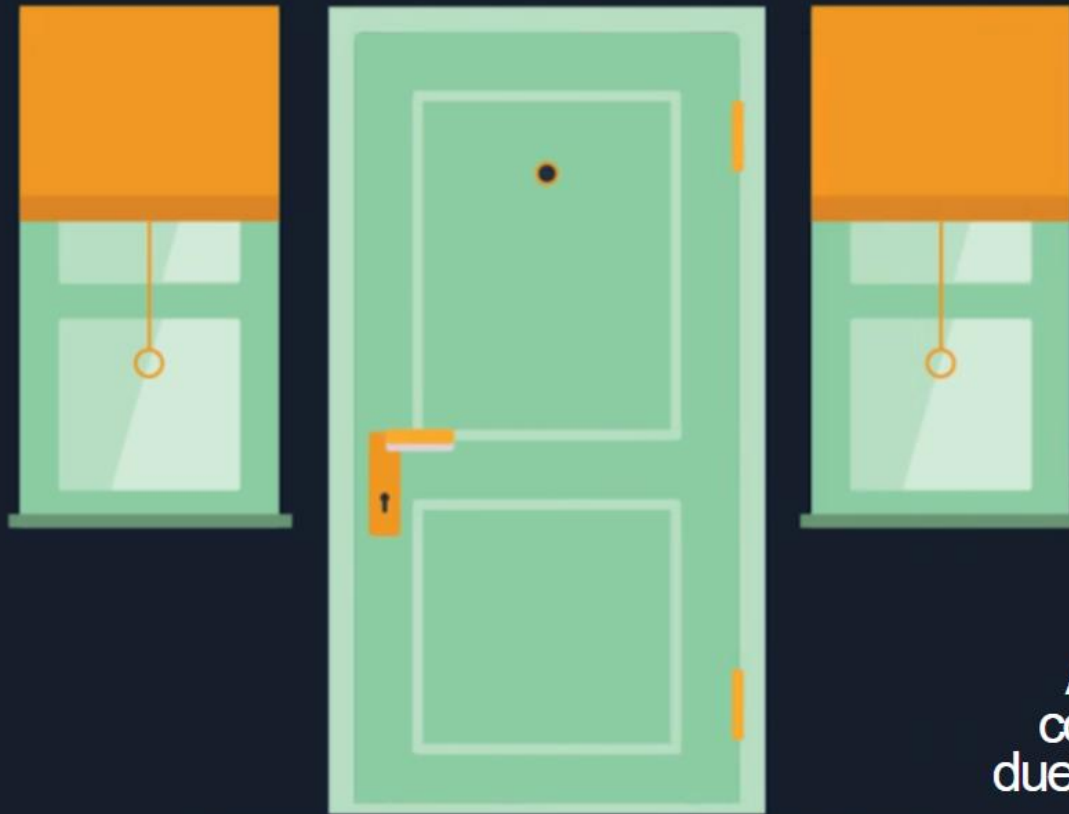


Modelo de responsabilidad compartida (Shared Responsibility Model)

Modelo de responsabilidad compartida (Shared Responsibility Model)

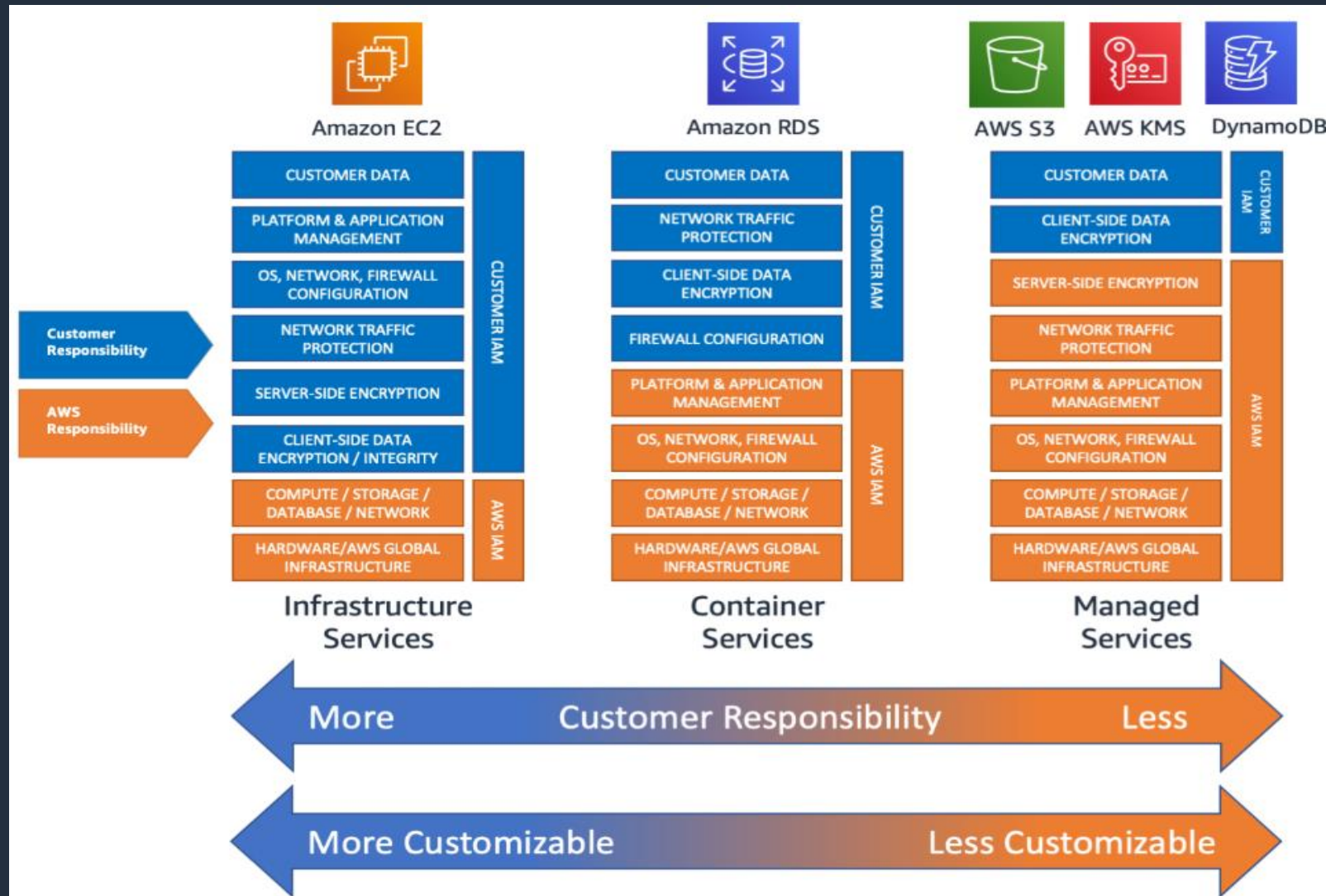


Modelo de responsabilidad compartida (Shared Responsibility Model)

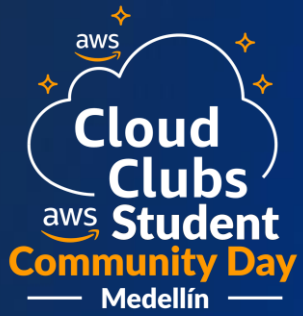


Analogía del
constructor y el
dueño de una casa

Modelo de responsabilidad compartida (Shared Responsibility Model)



En la nube, las responsabilidades (y control) varían en función del servicio elegido por el cliente



IAM (Identity and Access Management)

Servicio de autenticación y autorización en la nube de 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.

IAM (Identity and Access Management)



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!

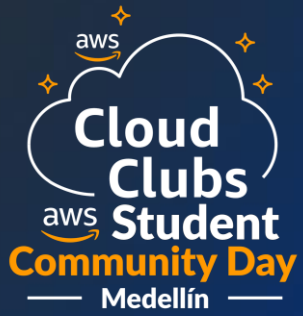
IAM (Identity and Access Management)

Ejemplo: Política de permisos
(Política basada en identidad)

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

Ejemplo: Política de bucket
(Política basada en recurso)

```
{
  "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/*"
    }
  ]
}
```



Seguridad de red en la nube: Security Groups y Network ACLs

Seguridad de red en la nube: SGs y NACLs

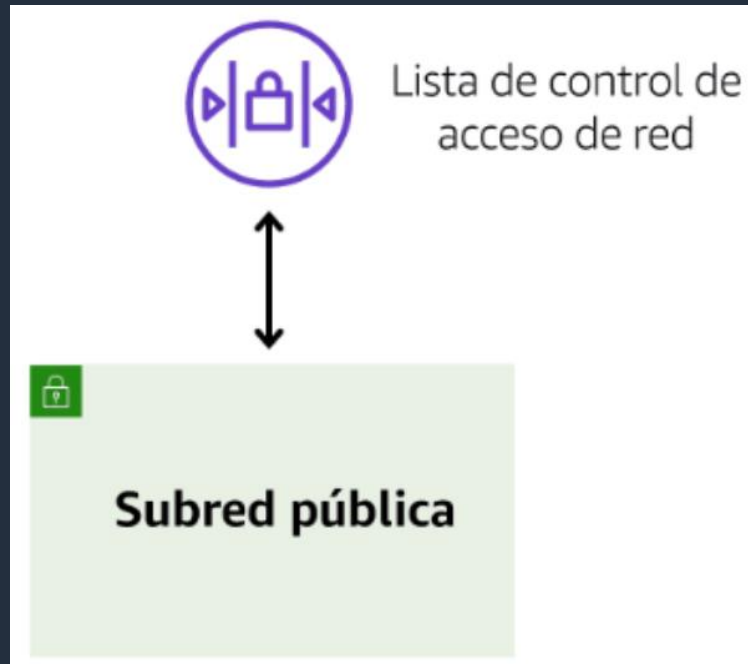


Amazon VPC permite aprovisionar un segmento de red aislado dentro de la nube de AWS.

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 de red en la nube: SGs y NACLs

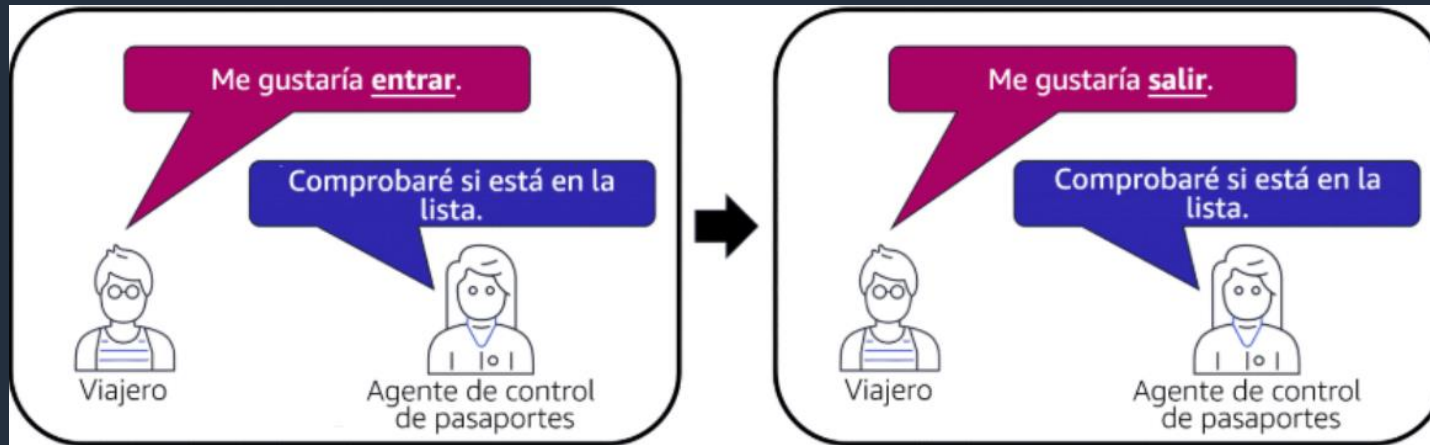


Una **ACL** de red es un **firewall** virtual que controla el tráfico **a nivel de subred**.



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

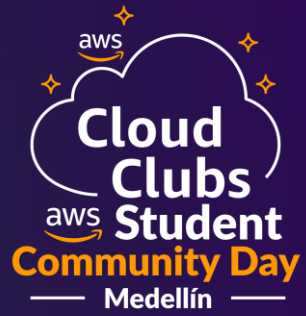
Seguridad de red en la nube: SGs y NACLs



Las **NACLs** son sin estado (**stateless**): Debo definir reglas en cada sentido



Los **SGs** son con estado (**stateful**): Debo definir reglas en el sentido que inicia la conex.



Protección de datos en reposo y en tránsito

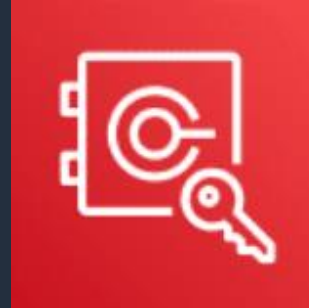
Protección de datos en reposo

-> Guardamos datos **cifrados**



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

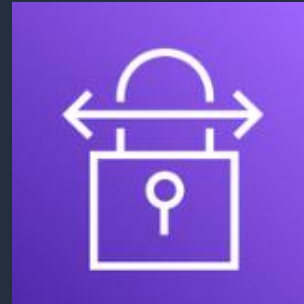
Protección de datos en tránsito

-> Transmitimos datos **cifrados**



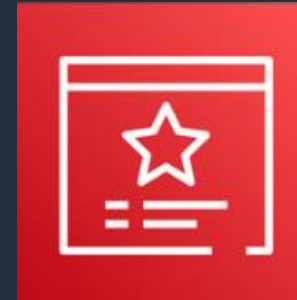
TLS, SSH

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



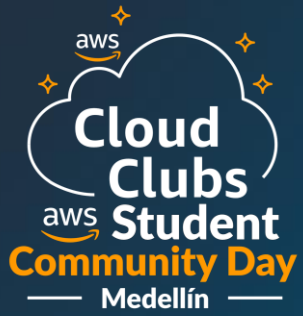
Site-to-site VPN

conexión cifrada entre tu red on-prem y AWS



ACM

AWS Certificate Manager: Generar y administrar **certificados digitales**



Otros servicios de seguridad en AWS

Otros servicios de seguridad en AWS



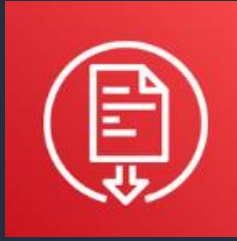
WAF

Protección
contra
ataques a
aplicaciones
web



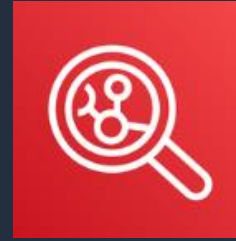
Shield

Protección
contra
ataques
DDoS



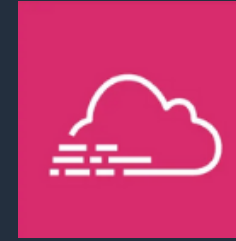
Artifact

Descarga de
informes de
auditoría y
acuerdos de
servicio



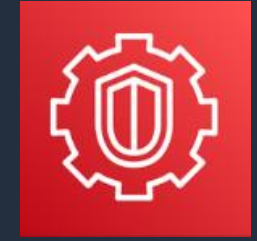
Inspector

Automática/e
evalúa
desviaciones
de seguridad
y detecta
vulnerabilida
des



CloudTrail

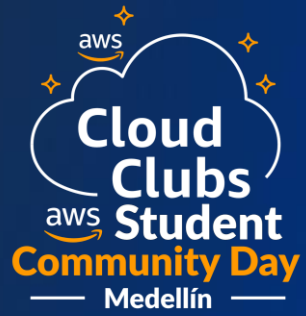
Registro de
eventos en
tu cuenta de
AWS



GuardDuty

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

(y no son todos 😊)
[+ info](#)



Demo time!

(si hay time)

(sino, revisa el readme que te compartiremos con el paso a paso para repetir el demo en tu cuenta AWS)