

G



D



D

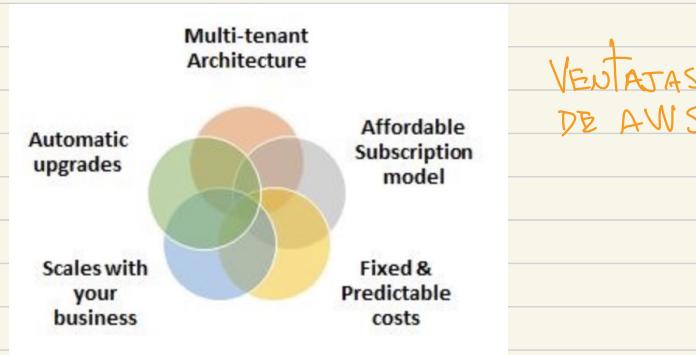
# Domain 1

## Cloud Concepts

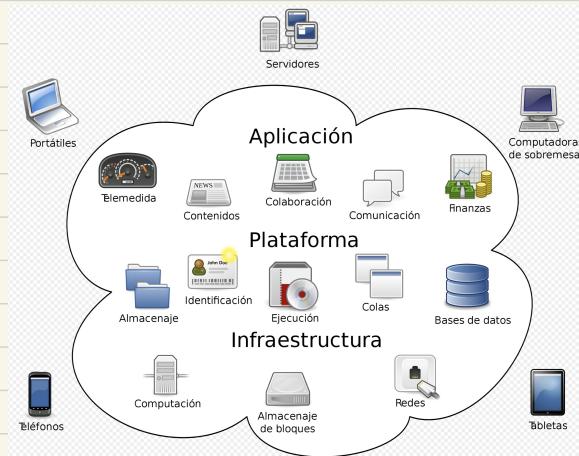
### AWS

{ QUE ES AWS ?

- Es una **plataforma de servicios segura**
- Ofrece **poder de computo**
- Ofrece **almacenamiento en base de datos**
- Ofrece **distribución de contenidos**.
- Ofrece **servicios adicionales para escalar negocios**.
- Plataforma más ampliamente usada en la nube
- Posee más de 200 servicios
- Posee millones de usuarios.



VENTAJAS  
DE AWS



Esquema General de  
Computación en la Nube

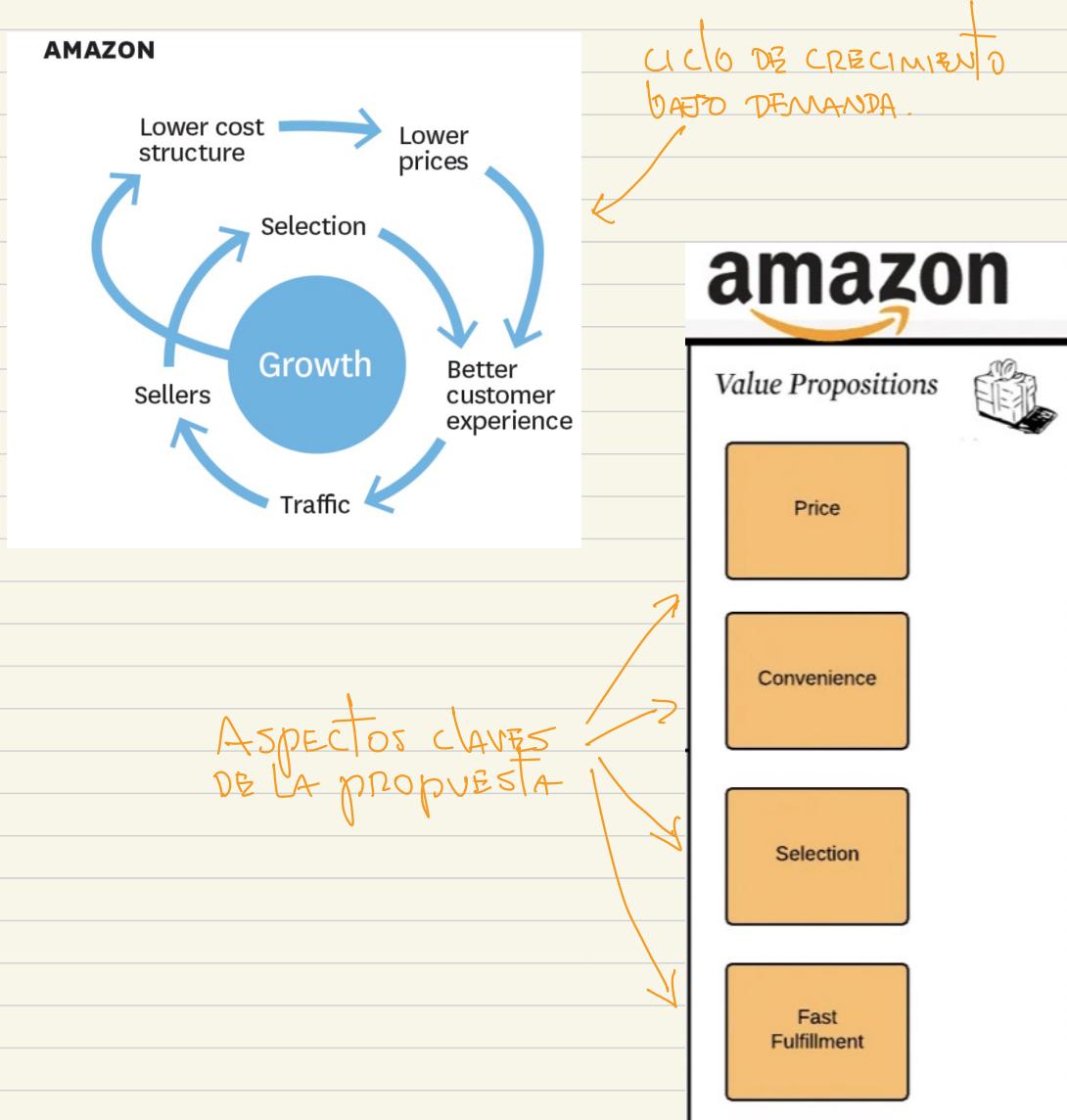
AWS es una **plataforma** dispuesta por Amazon para **negocios de todo tipo**, para ofrecer **servicios tecnológicos variados** (poder de computo, base de datos, distribución de contenido, etc) y dejar que las **compañías llenen sus necesidades tecnológicas** a los **servidores de la plataforma**, manteniendo la administración de los servicios mientras se bajan los costos (TCO).

DOMAIN 1  
Cloud Concepts

Propuesta de Valor de AWS

¿Cuáles son los principales atributos de la propuesta de valor de AWS?

- Seguridad (Data locality, protección de datos, confidencialidad)
- Agilidad (Velocidad de implementación)
- Elasticidad (Escalamiento bajo demanda, eliminación de capacidad ociosa)
- Flexibilidad (Amplia variedad de servicios, bajos costos de entrada)
- Barato (Corta costos de tenencia de equipos e instalaciones, solo pagas lo que consumes, varios servicios son gratis)
- Escalamiento (Beneficios por economía de escala, servicios disponibles globalmente en minutos, se crece en base a la demanda)



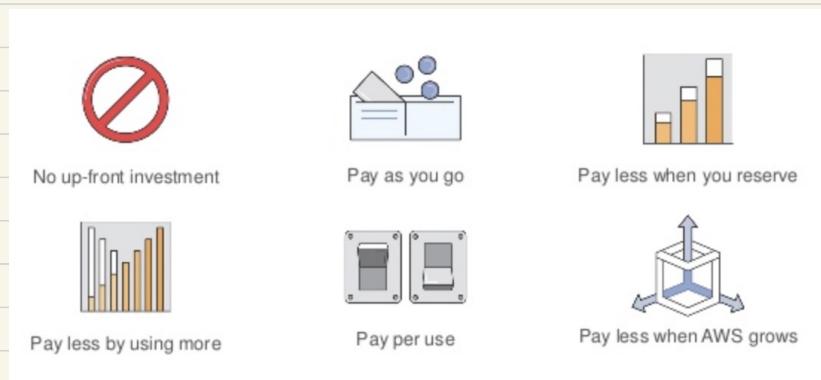
La propuesta de valor de AWS se basa en ofrecer una amplia selección de servicios en forma segura a clientes con todo tipo de tamaño, en forma rápida y confiable a nivel mundial, a bajo costo, pagando por lo que se consume, intercambiando el CAPEX por OPEX, mientras se tiene la flexibilidad de crecer bajo demanda.

¿CÓMO SE MANEJAN LOS COSTOS AL USAR AWS?

SE INTENTA REDUCIR EL TCO CON:

- Pay-as-you-go
  - PAGAS LO QUE CONSUMES
  - SIN COMPROMISO DE MÍNIMO USO
  - SIN CONTRATO DE LARGO TÉRMINO
  - SIN COMPLEJOS TÉRMINOS DE LICENCIAS.
- Modelo de Precios por Uso
  - APPLICA PARA ALMACENAMIENTO Y TRANSFERENCIAS DE DATOS
  - USAS MÁS, PAGAS MENOS
  - DESCUENTOS POR VOLUMEN
- Optimización de Costos
  - EVITAR COSTOS INNECESSARIOS
  - CONTROLAR DONDE EL DINERO SE GASTA
  - SELECCIONAR LOS TIPOS DE RECURSOS APROPIADOS
  - ANALIZAR LOS COSTOS EN EL TIEMPO
  - ESCALAR SIN SOBREPRECIOS.
  - USAR EL COST EXPLORER
- Trusted Advisor
  - ES UNA HERRAMIENTA ONLINE
  - GUÍA EN LA APLICACIÓN DE LAS MEJORES PRÁCTICAS PARA REDUCIR COSTOS
  - LOCALIZA OPORTUNIDADES DE REDUCCIÓN DE COSTOS MENSUALES SIN IMPACTAR EL RENDIMIENTO, MANTENIENDO LA PRODUCTIVIDAD.

### CARACTERÍSTICAS DEL MODELO DE PRECIOS



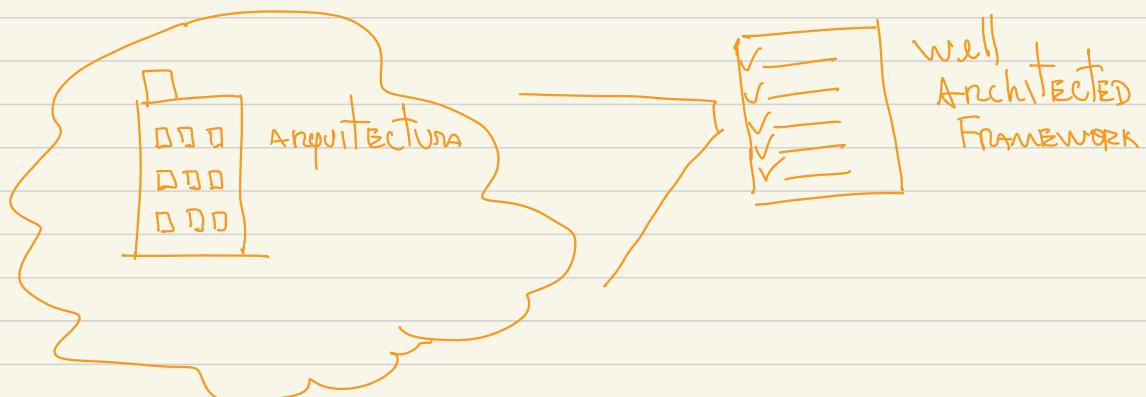
El modelo general de costos de AWS está orientado a la economía de escala, es decir que a mayor consumo menos es el costo a pagar, pero depende también de saber escoger las características más ajustadas al uso de recursos que necesitamos, para esto se puede hacer uso de la herramienta Trusted Advisor.

¿Qué es el  
Well-Architected  
Framework?

AWS DEFINIO UN MARCO DE TRABAJO PARA GUIAR A SUS CLIENTES EN LA CREACION DE ARQUITECTURAS EN LA NUBE, SE CONOCE CON EL NOMBRE DE WELL-ARCHITECTED FRAMEWORK.

PILARES DEL WELL-ARCHITECTED  
FRAMEWORK

- Security: Proteger sistemas, información y activos.
- Reliability: Capacidad de recuperarse de fallos de infra o servicios.
- Performance Efficiency: Uso eficiente de los recursos computacionales.
- Cost Optimization: Evitar o eliminar costos innecesarios.
- Operational Excellence: Monitoreo para mejora continua de procesos.



El Well-Architected Framework es una iniciativa de AWS para crear una guía de diseño para arquitecturas en nube, priorizando las más valiosas características que deben poseer las soluciones desplegadas en AWS. Esto permite fijar un standard de calidad y buenas prácticas aplicables por todos los clientes.

## DOMAIN 2 SECURITY AND COMPLIANCE

### Modelo de Responsabilidad Compartida de AWS

¿Qué es el modelo de responsabilidad compartida de AWS?

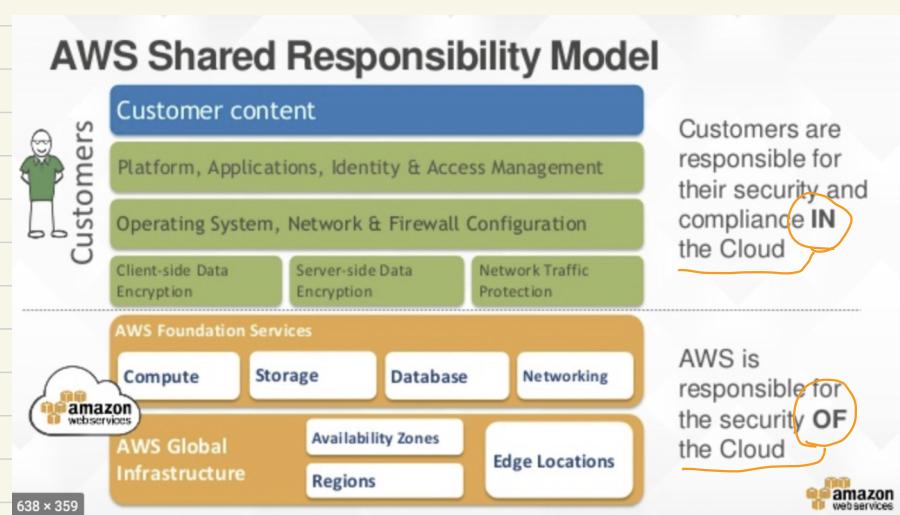
- Los clientes son responsables de la seguridad y cumplimiento **EN LA NUBE**.
- AWS es responsable de la seguridad **DE LA NUBE**.

La seguridad de los servicios funcionales y la infraestructura es **responsabilidad de AWS**, es decir:

- Computo
- Base de Datos
- Almacenamiento
- Red
- Availability Zones
- Regions
- Edge Locations

Los clientes se responsabilizan por todo lo que corren en la nube, es decir:

- Sistema Operativo
- Aplicaciones
- Accesos
- Configuración de Firewall
- Accesos y Permisos
- Encriptación de Datos
- Protección de Tráfico



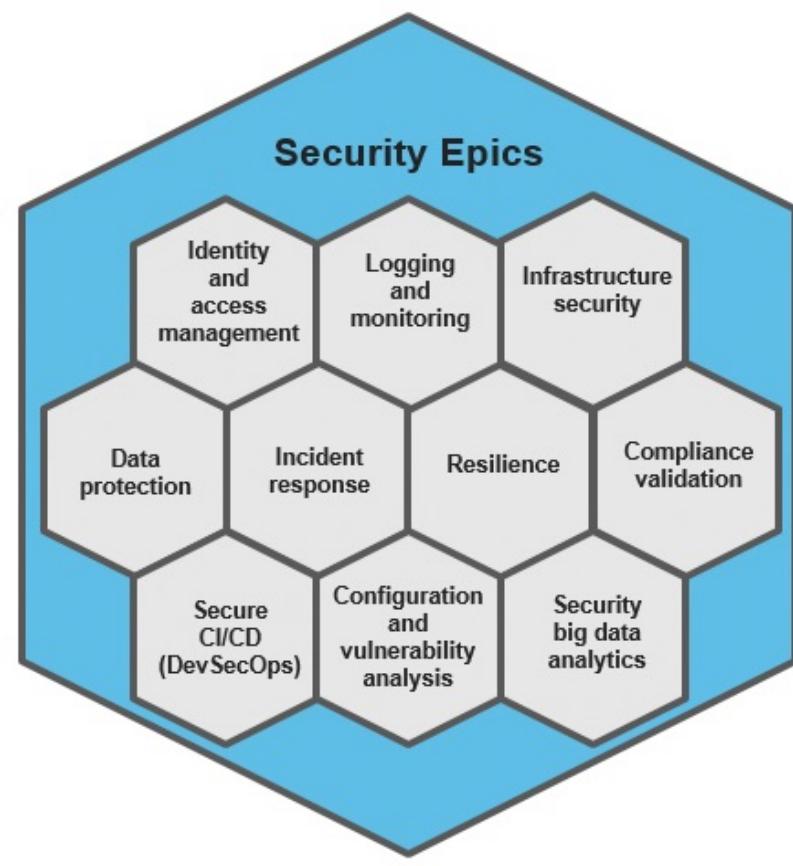
AWS divide muy bien las responsabilidades de clientes y de Amazon. Los clientes son responsables de usar correctamente y en forma segura los servicios que contiene y en cuanto a la infra y la disponibilidad de servicios, AWS tiene la responsabilidad, lo cual constituye un modelo de responsabilidad compartida

## DOMAIN 2 SECURITY AND COMPLIANCE CONCEPTS

### SEGURIDAD DE INFRAESTRUCTURA

¿COMO SE IMPLEMENTA LA SEGURIDAD DE LA INFRAESTRUCTURA DE AWS?

- FIREWALLS INTEGRADOS EN LA VPC
- ENCRYPTION BY DEFAULT EN TRANSITO ENTRE TODOS LOS SERVICIOS.
- SE PUEDE PROVER DE CONEXION DEDICADA PRIVADA ENTRE EL ON-PREMISE Y AWS.
- AWS PROVEE HERRAMIENTAS PARA AYUDAR A ALCANZAR LOS OBJETIVOS DE SEGURIDAD DE LOS CLIENTES (AMAZON INSPECTOR)



AWS PROVEE SU SEGURIDAD DIRECTAMENTE EN SU INFRAESTRUCTURA INCORPORANDO FIREWALLS, ENCRYPTION Y MONITORING, ADEMÁS DE PROPORCIONAR HERRAMIENTAS COMO AMAZON INSPECTOR PARA AYUDAR A ALCANZAR EL NIVEL DE SEGURIDAD DESEADO.

## DOMAIN 2 SECURITY AND COMPLIANCE CONCEPTS

### RESILIENCIA DE INFRAESTRUCTURA.

¿COMO SE IMPLEMENTA  
LA RESILIENCIA EN  
AWS?

- LOS SERVICIOS EN AWS ESTAN CONSTRUIDOS PENSANDO EN EVITAR LOS ATAQUES DDoS.
- LOS SERVICIOS AWS PUEDEN ESCALAR EN FUNCION DE SU DEMANDA.
- SE PUEDE USAR CLOUDFRONT Y ROUTE 53 PARA EVITAR ATAQUES DDoS.

LA RESILIENCIA EN AWS ES UN VALOR CLAVE PARA TODA LA PLATAFORMA, INCLUSO HAY HERRAMIENTAS DE USO GRATIS PARA MEJORAR LA CAPACIDAD DE TOLERANCIA DE LAS SOLUCIONES DESPLEGADAS EN AWS.

EN AWS SE ORIENTA A LOS CLIENTES A TENER UNA INFRAESTRUCTURA FUERTE A TRAVES DE UN DISEÑO DE SOLUCION SOLIDO AVANZADO A LA APLICACION DE LOS PRINCIPIOS DEL WELL-ArchITECTED Y EL USO DE HERRAMIENTAS PARA AUMENTAR LA RESILIENCIA COMO SON AWS CONFIG, TRUSTED ADVISOR Y AMAZON INSPECTOR.

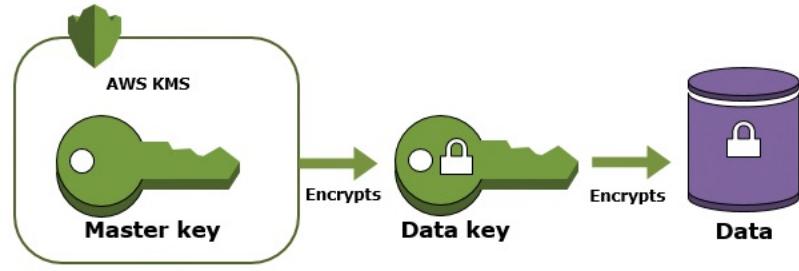
DOMAIN 2  
SECURITY AND COMPLIANCE  
CONCEPTS

¿Como AWS facilita la Encriptación de Datos?

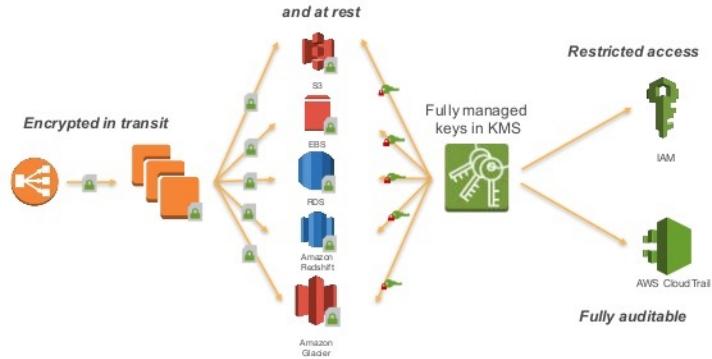
## ENCRIPCIÓN DE DATOS

- AWS INTEGRA EN SUS SERVICIOS CORE LA ENCRIPCIÓN (EBS, S3, GLACIER, RDS AND REDshift)
- AWS PROVEE EL SERVICIO KMS (KEY MANAGEMENT SERVICE) QUE PERMITE CREAR Y ADMINISTRAR LOS KEYS DE LOS SERVICIOS.
- LOS MENSAJES SQS TAMBÍEN INCLUYEN ENCRIPCIÓN.
- SE PUEDE USAR ENCRIPCIÓN POR HARDWARE, PARA ESTO SE USA EL SERVICIO CLOUDHSM LO CUAL PERMITE LA GENERACIÓN DE CLAVES (KEYS)
- ADICIONALMENTE AWS PROVEE UN API PARA INTEGRAR LA SEGURIDAD EN NUESTRAS APLICACIONES.

### AWS KMS



### Ubiquitous encryption



AWS ADOPTA LA ESTRATEGIA DE PROPORCIONAR ENCRIPCIÓN DE DATOS A VARIOS NIVELES, DIRECTAMENTE EN LOS SERVICIOS CORE DE UNA FORMA TRANSPARENTE, O ATRAVÉS DE KMS PARA GENERAR LAS LLAVES DE ENCRIPCIÓN, INCLUSO DANDO SOPORTE A CIFRADO POR HARDWARE CON CLOUDHSM.

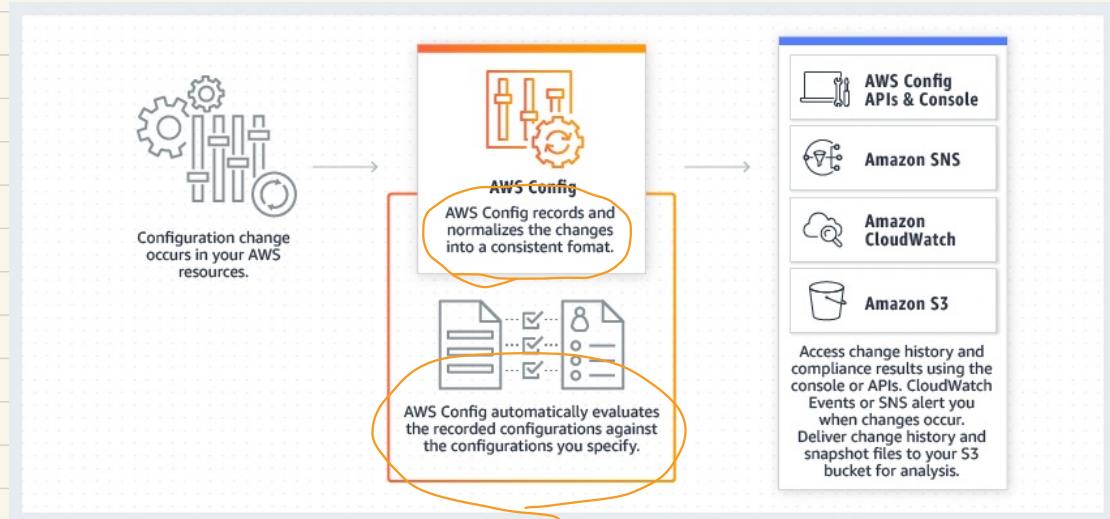
## DOMAIN 2 SECURITY AND COMPLIANCE CONCEPTS

## ESTÁNDARES Y BUENAS PRÁCTICAS

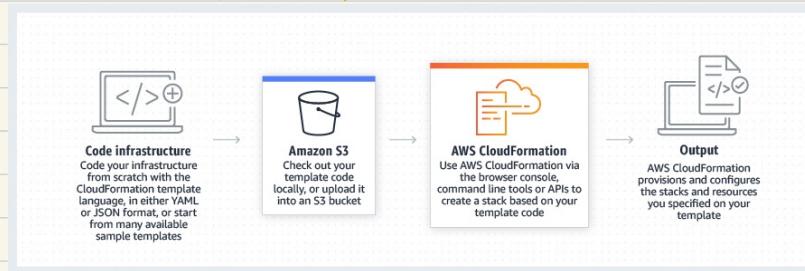
¿Cuáles estandares y buenas prácticas implementa AWS?

- Con Amazon Inspector se pueden supervisar automáticamente aplicaciones desplegadas en AWS para identificar vulnerabilidades, desviaciones de las mejores prácticas incluyendo red, sistema operativo y almacenamiento.
- AWS Config permite llevar un inventario de configuraciones, con lo cual se puede hacer un seguimiento en el tiempo de los cambios hechos sobre un recurso.
- Con la herramienta CloudFormation podemos crear plantillas estandarizadas para recrear ambientes predefinidos.

### AWS CONFIG



### AWS CLOUDFORMATION



SE PROMUEVE EN AWS LA ESTANDARIZACIÓN DE LOS DESPLIEGUES A TRAVÉS DEL USO DE HERRAMIENTAS COMO CloudFormation, AÑADIDO AL SEGUIMIENTO DE LOS CAMBIOS HECHOS A LOS SERVICIOS (TRAZA DE AUDITORÍA) CON AWS Config. ESTO ASEGURA LA APLICACIÓN SISTEMÁTICA DE LAS BUENAS PRÁCTICAS Y ESTÁNDARES, QUE A SU VÉZ PUEDEN SER VALIDADAS CON Amazon Inspector.

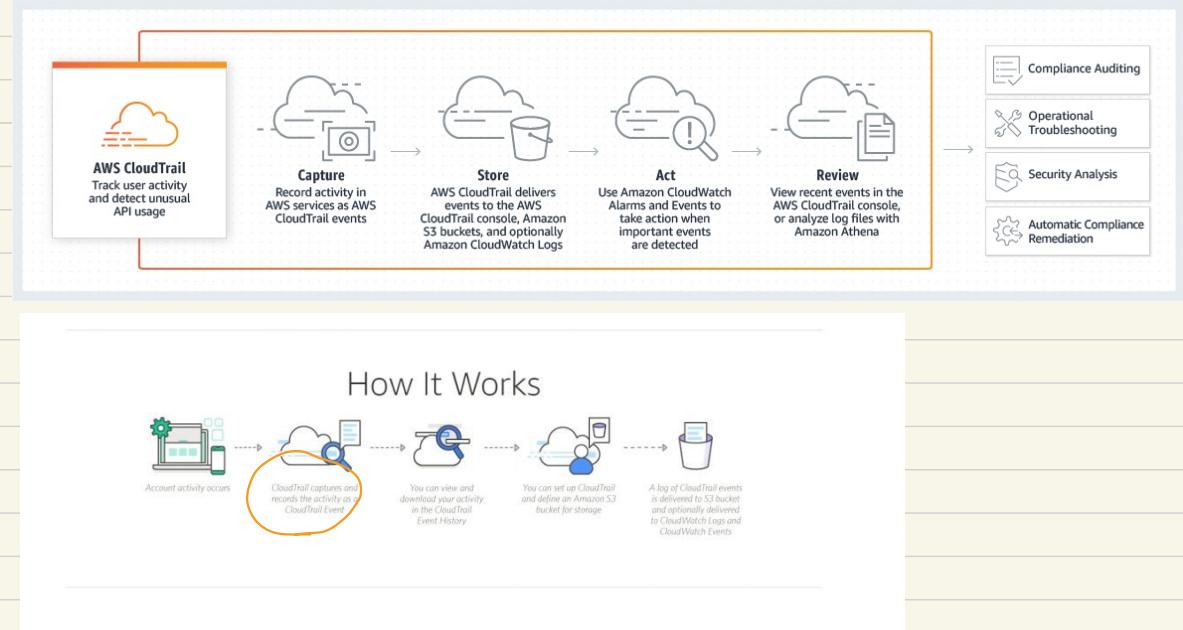
## DOMAIN 2 Cloud Security and Compliance Concepts

## MONITOREO y TRAZABILIDAD

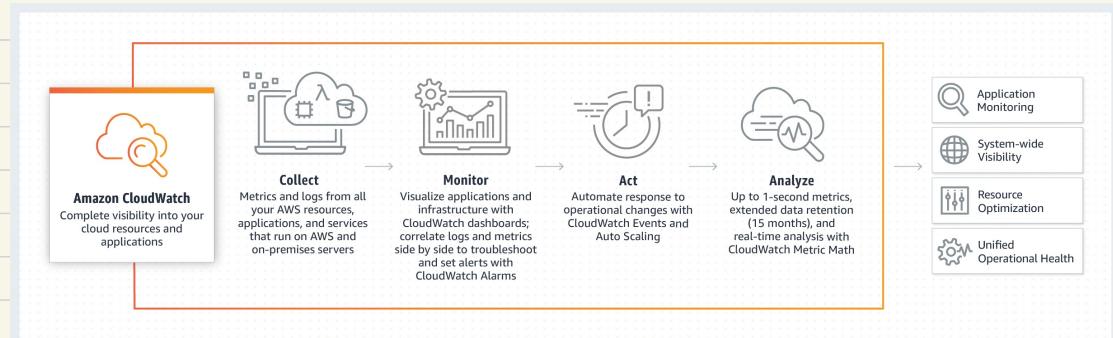
¿CUALES HERRAMIENTAS DE MONITOREO Y LOGGING POSEE AWS?

- AWS OFRECE LA POSIBILIDAD DE ACTIVAR EL LOGEO DE ACTIVIDADES PARA LOS DIFERENTES SERVICIOS EN LA PLATAFORMA.
- CloudTrail PERMITE OBSERVAR EL LOGEO DE LLAMADAS VIA API, INCLUYENDO QUIEN, QUE, CUANDO Y DE DONDE SE ORIGINAN LAS LLAMADAS A UN SERVICIO.
- CloudWatch SE PUEDE CONFIGURAR PARA LANZAR ALERTAS CUANDO SE PRESENTEN CIERTOS TIPOS DE EVENTOS O CUANDO CIERTOS PARAMETROS SON SOBREPASADOS.

### CLOUDTRAIL



### CLOUDWATCH



LAS DOS PRINCIPALES HERRAMIENTAS DE MONITOREO QUE POSEE AWS SON: CloudTrail y CloudWatch, CON LOS CUALES SE PROVEE UN SOPORTE COMPLETO A TAREAS DE AUDITORIA Y ANALISIS DE INCIDENTES, A LA VEZ QUE MEJORA LA SEGURIDAD DE LA PLATAFORMA.

## IDENTIDAD y CONTROL DE ACCESO

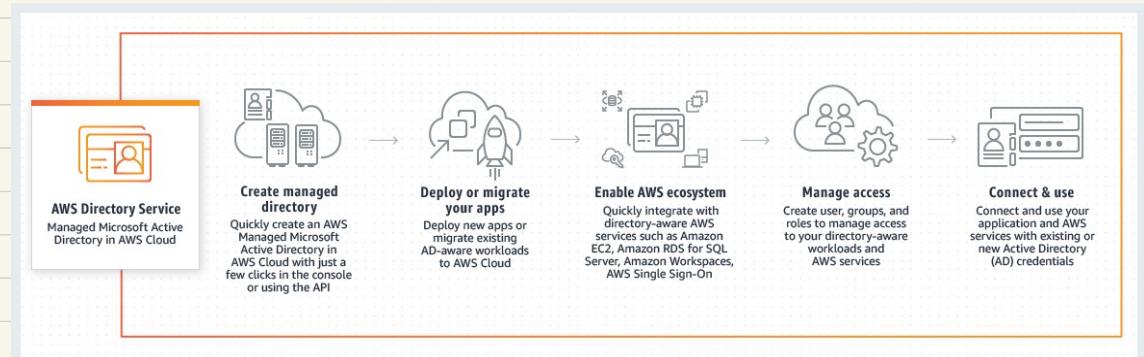
¿QUE FORMA DE ADMINISTRACION DE USUARIOS Y CUENTAS PUEDE OFRECER AWS?

- La piedra angular de la permisología y accesos en AWS es IAM (Identity and Access Management). Esta herramienta permite crear cuentas de usuario con permisos de acceso a servicios en diferentes granularidades.
- Para cuentas privilegiadas se puede incluir un segundo factor de autenticación, incluyendo autenticación por hardware.
- Cuando se requiere administrar cuentas y permisos usando directorios de usuarios que no están creados en AWS, se puede integrar y federar usuarios a través de AWS Directory Service.

### Como Funciona AWS IAM



### Como Funciona AWS Directory Service



AWS centraliza la administración de usuarios y permisos en un solo servicio IAM (Identity and Access Management) permitiendo un uso más lógico y seguro, ya que se puede ajustar la granularidad de permisos para cada cuenta y cada servicio. Además de lo anterior, AWS también se integra a directorios de usuarios con AWS Directory Service.

## DOMINIO 2 SECURITY AND COMPLIANCE CONCEPTS

### SOPORTE A LA SEGURIDAD

¿COMO AWS DA SOPORTE DE SEGURIDAD?

- El soporte en tiempo real de seguridad se obtiene a través del uso de la herramienta Trusted Advisor.
- El Trusted Advisor permite visualizar a través de un tablero de alertas de seguridad, parches y actualizaciones recomendadas sobre los servicios utilizados, permitiendo ver en tiempo real la evolución del nivel de seguridad de los aplicativos desplegados.
- Un enfoque proactivo de la seguridad puede ser ejecutado en conjunto con el TAM (Technical Account Manager) quien puede guiar y aconsejar desde el punto de vista técnico en las mejores prácticas y optimización de la seguridad.

**CHEQUEO DE SEGURIDAD CON TRUSTED ADVISOR**

The screenshot shows the AWS Trusted Advisor interface under the 'Security' tab. It displays a summary of security checks with 1 green checkmark, 1 yellow warning, and 1 red error. Below this, two specific checks are detailed:

- Security Groups - Specific Ports Unrestricted** (Red Error): Checks for rules that allow unrestricted access to specific ports. It states that security group rules allow unrestricted access to a specific port. Recommended action: Log in to your root account and activate an MFA device.
- MFA on Root Account** (Yellow Warning): Checks if multi-factor authentication (MFA) is not enabled. It recommends protecting the account by using MFA, which requires a user to enter a unique authentication code from their MFA hardware or virtual device. Alert Criteria: Yellow: MFA is not enabled on the root account. Recommended Action: Log in to your root account and activate an MFA device.

**ROL DEL TAM**

### Technical Account Manager (TAM) Role

- **Technical Account Manager (TAM)**
  - Provides access to technical expertise for the full range of AWS services.
  - Work with AWS Solution Architects to help you launch new projects and give best practices recommendations throughout the implementation life cycle.
  - Acts as the primary point of contact for ongoing support needs - you have a direct communications channel with your TAM.
- **Core values of TAM**
  - Orchestrate resources within AWS to help Enterprise customers in the best possible way.
  - Develop a detailed understanding of your technology architecture and use case.
  - Be your advocate inside Amazon Web Services.

Amazon Confidential

EXISTEN DOS MANERAS DE ABONDAR EL SOPORTE DE SEGURIDAD EN AWS, DESDE UN PUNTO DE VISTA REACTIVO (TRUSTED ADVISOR) Y PROACTIVAMENTE CON EL TAM, IGUALMENTE ES ACONSEJABLE USAR AMBOS ESCENARIOS, PARA CONFIGURAR SOLUCIONES SÓLIDAS A NIVEL DE SEGURIDAD.

¿Qué programas de cumplimiento reporta AWS?

- AWS ha cubierto varios programas de cumplimiento, certificaciones, regulaciones y marcos de trabajo de nivel internacional, a saber:
  - Cyber Essentials Plus (UK)
  - DoD SRG (US)
  - FIPS (US)
  - ISO 9001
  - CISPE
  - GLBA
  - UK Data Protection Act
  - EU Data Protection Directive
  - FFIEC
  - G-CLOUD (UK)
  - NIST
  - UK Cloud Security Principles

### Otras Certificaciones



Con la idea de dar soporte a los clientes que requieren hacer cumplimiento de estandares en sus aplicaciones, la plataforma a incorporado varias certificaciones y programas de cumplimiento a sus servicios, así alcanzando altos estandares internacionales de seguridad.

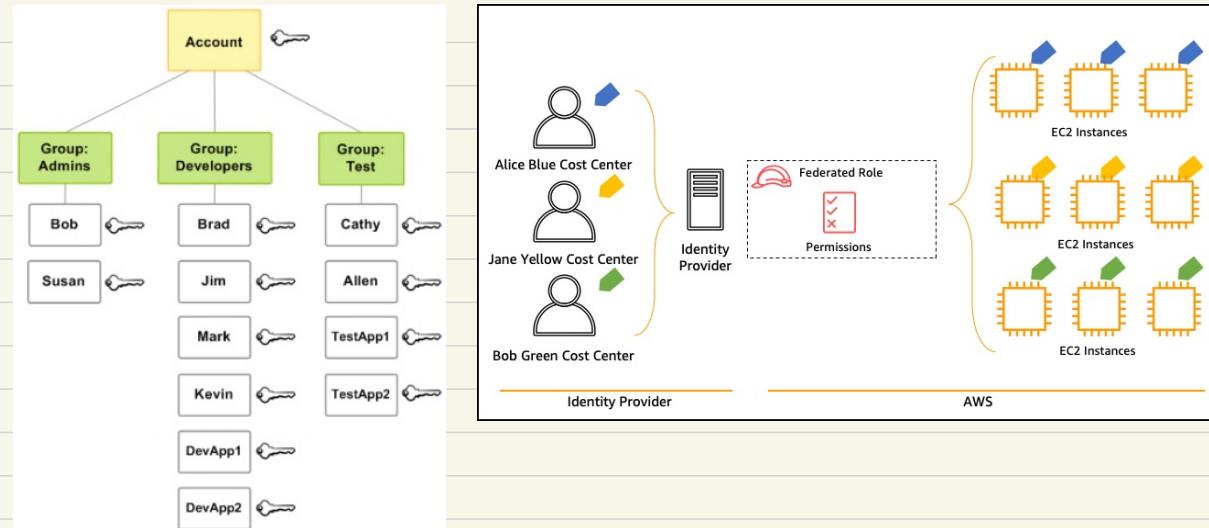
## DOMAIN 2

### Security and Compliance Access Management Capabilities

### IAM - Identity and Access Management

¿Qué es AWS IAM?

- IAM permite el control de acceso a los servicios y recursos de AWS para todos los usuarios.
- IAM NO SE CARGA EN LOS PAGOS DE AWS.
- IAM permite
  - CREAR USUARIOS
  - ASIGNAR CREDENCIALES DE SEGURIDAD INDIVIDUALES
  - CREAR CREDENCIALES DE SEGURIDAD TEMPORALES
  - CREAR roles
  - CREAR PERMISOS A NIVEL DE OPERACIONES, SERVICIOS O ENTIDADES.
  - ADMINISTRAR USUARIOS FEDERADOS y sus permisos.



El AWS IAM es un servicio que ayuda a la administración de autenticación y autorización de usuarios, con diferentes granularidades con capacidades de roles, segregación de permisos y federación de usuarios.

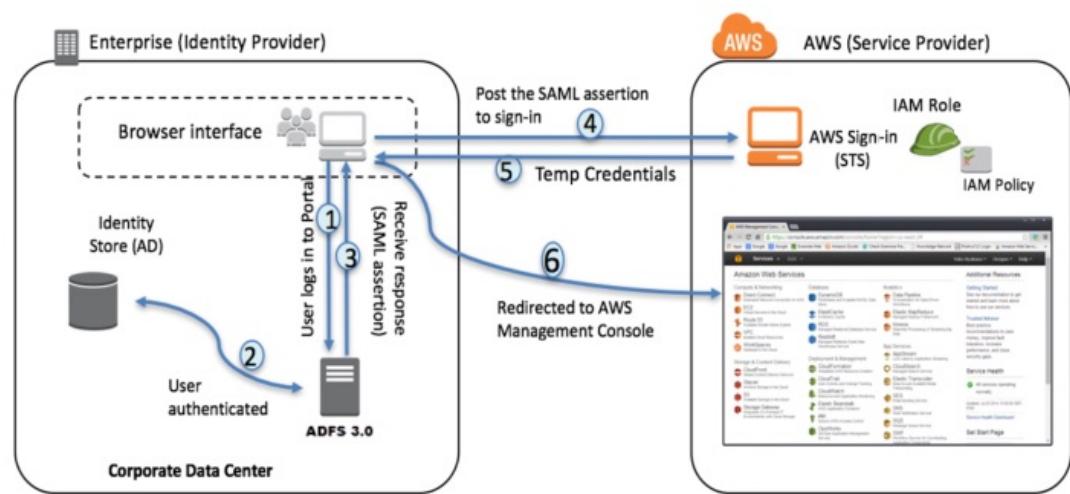
DOMAIN 2

Security and Compliance  
Access Management Capabilities

Accesos y Federación

- En AWS se pueden asignar permisos para administrar y usar recursos de tu cuenta AWS, sin compartir la clave de la misma.
- Se puede permitir el acceso a usuarios que ya tienen password en servicios de directorios a tu cuenta AWS. (federar usuario)
- AWS tiene soporte para administración de identidades que cumplen el estandar SAML 2.0

## AWS Federation



En AWS esta soportada la federación de usuarios, para facilitar a clientes que tengan ya implantados on-premises servicios de directorios de usuarios integrarlos con AWS, siempre que soporten estandar SAML 2.0. Por otra parte tambien soporta delegación de permisos y accesos, ademas de la creacion de roles, permitiendo el acceso basado en perfilamiento.

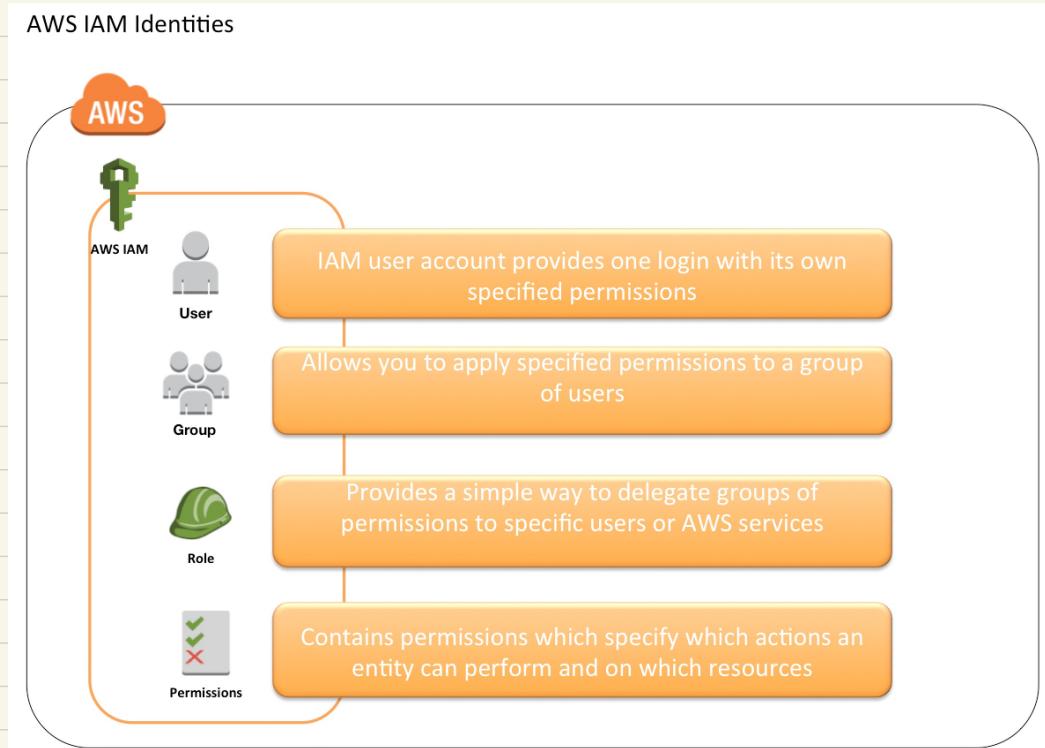
DOMAIN 2

Security And Compliance  
Access Management Capabilities

GRANULARIDAD DE PERMISOS

¿Cómo implementa AWS la granularidad de permisos?

- SE PUEDEN CONCEDER DIFERENTES PERMISOS PARA DIFERENTES PERSONAS PARA DIFERENTES RECURSOS.
- SE PUEDE CONCEDER PERMISOS DE READ-only HASTA ADMINISTRADOR PARA CADA RECURSO.
- ADICIONALMENTE SE PUEDEN ESPECIFICAR CONDICIONES PARTICULARES PARA EL USO DE UN RECURSO, POR EJEMPLO: TIPO DE AUTENTICACION, SSL, ETC.



La granularidad de los permisos se administran en AWS IAM (Identity Access Management) y pueden ser de varios niveles, incluso a nivel de método de login y capacidades de uso de los recursos.

DOMAIN 2

SECURITY AND COMPLIANCE  
ACCESS MANAGEMENT Capabilities

Segurizando el acceso de  
Aplicaciones

¿Como se puede segurar el acceso de las aplicaciones en AWS?

- Haciendo uso de IAM se puede crear credenciales para autorizar a una aplicación el acceso a ciertos recursos de AWS, incluyendo S3, RDS y otros. Esto permite configurar accesos desde instancias EC2 a otros servicios.

Como medida adicional de seguridad se pueden establecer el acceso entre una aplicación ejecutándose en una instancia EC2 haciendo uso de credenciales administradas en IAM, con esto podemos segurar ese acceso.

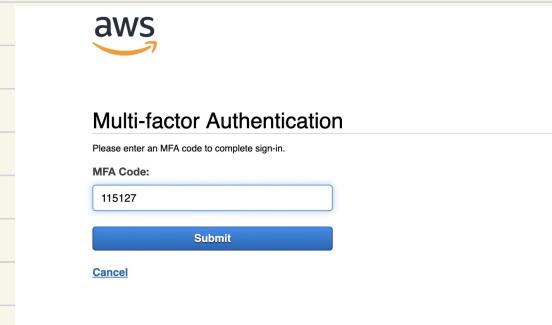
## DOMAIN 2

### SECURITY AND COMPLIANCE ACCESS MANAGEMENT CAPABILITIES

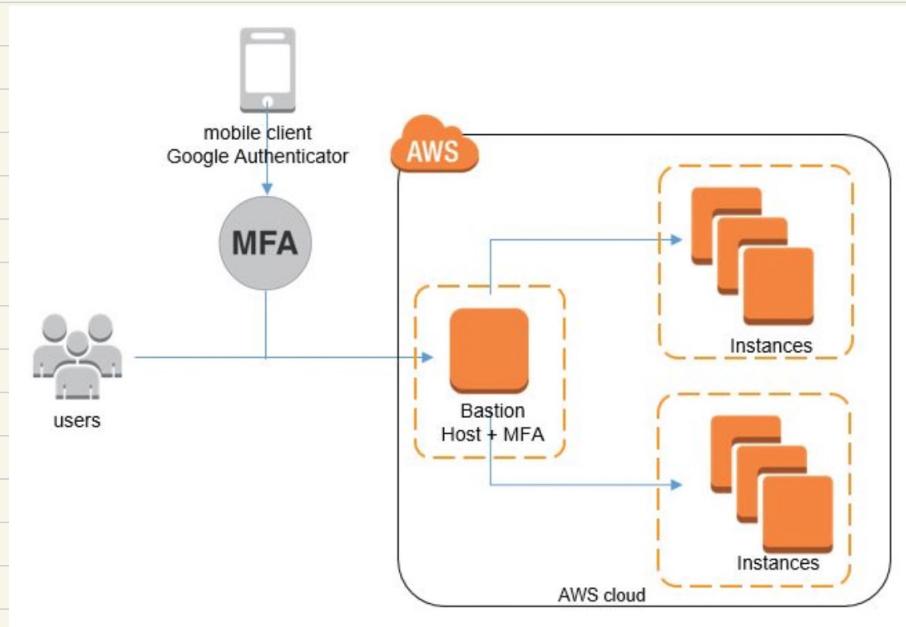
#### AUTENTIFICACIÓN MULTI-FACTOR

¿Cómo trabaja el MFA de AWS IAM?

- AWS PERMITE AGREGAR MAS SEGURIDAD AL MOMENTO DE HACER LOGGING CON ALGUNA CUENTA DE USUARIO, ESTO SE LOGRA MEDIANTE LA OBLIGACIÓN DE PROPORCIONAR UN CÓDIGO ADICIONAL AL PASSWORD DE LA CUENTA, ESTO ES LO QUE LLAMAREMOS AUTENTIFICACIÓN MULTI-FACTOR o MFA.
- LA MFA PUEDE SER UN CÓDIGO ADICIONAL FIJO O UN CÓDIGO GENERADO POR UN DISPOSITIVO DE HARDWARE ASOCIADO A LA CUENTA DE USUARIO.



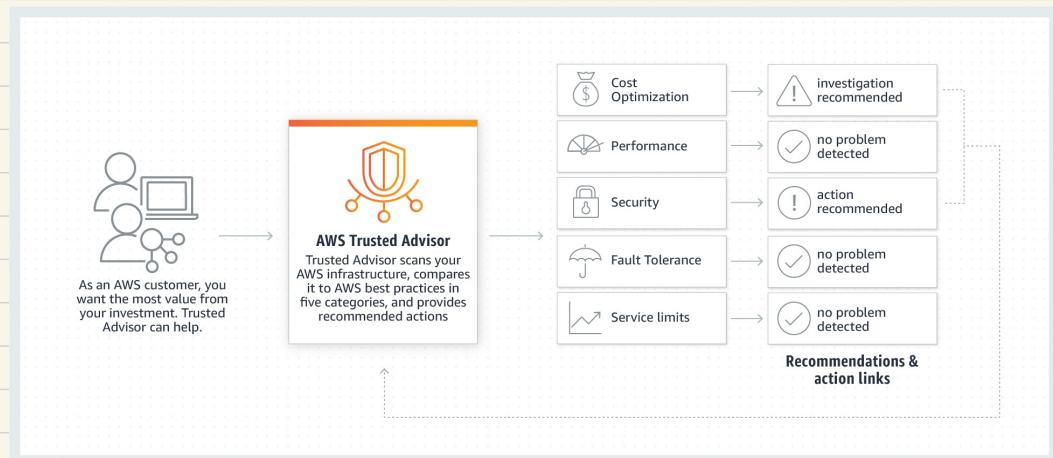
Esquema cómo trabaja el MFA



La herramienta IAM permite activar la solicitud de un factor de autenticación adicional para las cuentas de usuario, esto haría obligatorio en el momento del logging de esa cuenta introducir adicionalmente un código para validar la identidad del usuario, este puede ser un valor fijo conocido o un código generado por un dispositivo de hardware.

¿Qué es el soporte AWS?

- CON FOCO EN LA EFICIENCIA, COSTO EFECTIVO, SEGURIDAD Y SALUD OPERACIONAL, AWS PROVEE LOS PRINCIPALES HERRAMIENTAS DE SOPORTE:
  - + Trusted Advisor: Herramienta online que ayuda en el aprovisionamiento de recursos siguiendo las mejores prácticas.
  - + Technical Account Manager (TAM): Es un punto de contacto con AWS para obtener mentoría técnica y resolución de problemas técnicos.
- El nuevo completo del Trusted Advisor se obtiene sólo para todos los clientes con Nivel de Soporte BUSINESS y ENTERPRISE.
- EL TAM se puede solicitar cuando se tiene el NIVEL DE SOPORTE Enterprise.



	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
<b>Cost</b>	Free	\$29/mo	\$100/mo	\$15,000/mo
<b>Use Case</b>		Experimenting	Production use	Mission-critical use
<b>Tech Support</b>	NO	Business hour via e-mail	24x7 via email, chat & phone	24x7 via email, chat & phone
<b>SLA</b>		12-24 hrs at local business hours	1 hr response to urgent support cases	15 min to critical support cases w/ priority
<b>TAM &amp; Support Concierge</b>	NO	NO	NO	YES
<b>Support Cases</b>	None	1 Person, Unlimited Cases	Unlimited contacts/cases	Unlimited contacts/cases

Las dos principales maneras de obtener soporte por parte de AWS en temas de buenas prácticas y seguridad, es a través de la herramienta Trusted Advisor y poniéndose en contacto con el TAM, en ambos casos están sujetos al nivel de soporte que posea la cuenta principal AWS.

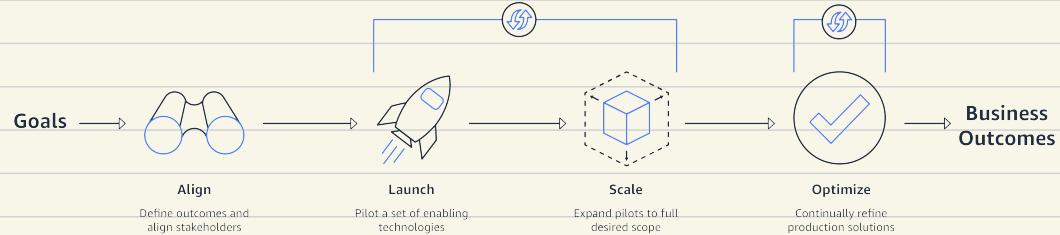
## DOMAIN 2

### SECURITY AND COMPLIANCE RESOURCES FOR SECURITY SUPPORT

### SERVICIOS PROFESIONALES

EN QUE CONSISTEN LOS SERVICIOS PROFESIONALES DE AWS?

- LOS SERVICIOS PROFESIONALES Y LA AWS PARTNER NETWORK PUEDEN AYUDAR A LOS CLIENTES A CREAR SOLUCIONES MÁS SEGURAS, AL IGUAL QUE COOPERAR EN LA REINGENIERÍA DE SOLUCIONES YA DESPLEGADAS, POR EJEMPLO:
  - **SEGURIDAD DE ARQUITECTURAS EMPRESARIALES:** EVALUA LA NATURALEZA DE LAS CARGAS DE TRABAJO JUNTO CON LA SEGURIDAD, PARA DEFINIR UNA ARQUITECTURA Y UN CONJUNTO DE CONTROLES DE SEGURIDAD PARA PROTEGER LA DATA, TODO ALINEADO CON LAS MEJORES PRÁCTICAS.
  - **POLÍTICAS Y CONTROL DE MAPES:** EXAMINA TUS REQUERIMIENTOS BASADO EN TUS POLÍTICAS DE SEGURIDAD O MANDADOS REGULATORIOS, PROPORCIONANDO RECOMENDACIONES DETALLADAS SOBRE CÓMO SATISFACER ESTOS REQUERIMIENTOS Y DEMOSTRAR CUMPLIMIENTO.
  - **MANUAL DE OPERACIONES DE SEGURIDAD:** DEFINE LOS PROCESOS Y ESTRUCTURAS CORRECTAS PARA ASSEGURAR QUE CONTROLES DE SEGURIDAD ESTÉN TRABAJANDO CORRECTAMENTE CUANDO SE DETECTE UN PROBLEMA DE SEGURIDAD, ASÍ COMO LA RESPUESTA AL MISMO.
  - **TALLERES CON UNIDADES DE NEGOCIO:** TRABAJANDO EN CONJUNTO CON LÍDERES DEL NEGOCIO Y EL DEPARTAMENTO DE TI PARA ENTENDER SUS PLANES Y ESTRATEGIAS, EDUCANDOLOS DE LA MEJOR MANERA EN LA ADOPCIÓN DE LA NUBE, MIENTRAS SE MINIMIZAN LOS PRESUPUESTOS.



LA RED DE SERVICIOS PROFESIONALES DE AWS, IMPLEMENTADA EN CONJUNTO CON LA PARTNER NETWORK, ENTREGA CAPACITACIÓN, SOPORTE Y GUÍA EN LA IMPLANTACIÓN SEGURA DE ARQUITECTURA DE SOLUCIONES PARA LA NUBE, ASÍ COMO SU ADOPCIÓN DE UNA FORMA MÁS PERSONALIZADA Y CERCANA A LOS CLIENTES Y SUS NECESIDADES.

# DOMAIN 3

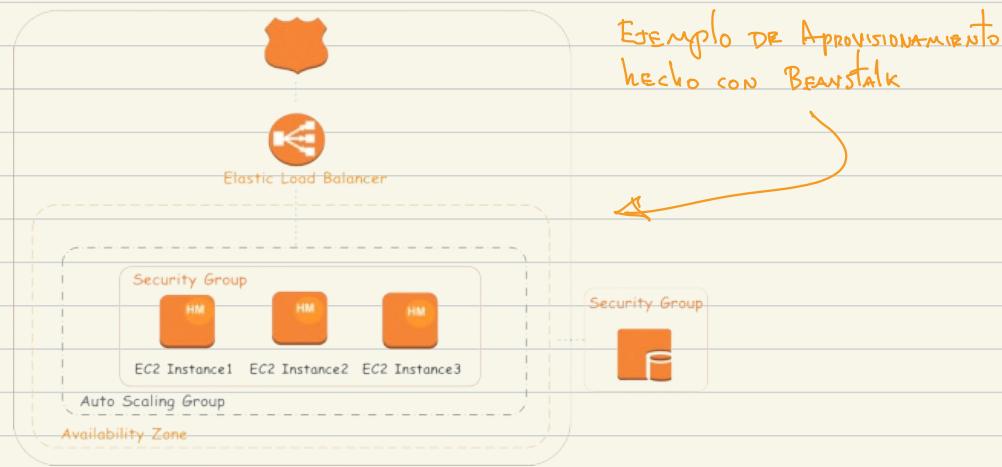
## Technology

### Methods of deploying and operating

#### Elastic Beanstalk

¿Qué es Elastic Beanstalk?

- Elastic Beanstalk es una herramienta online que toma una aplicación completa y la despliega en AWS, sin tener que preocuparse por la administración de la infraestructura a usar.
- Elastic Beanstalk maneja los detalles de aprovisionamiento como son:
  - Capacity
  - Balanceo de Carga
  - Escalamiento
  - Monitoreo & Alarms
  - Seguridad



Elastic Beanstalk es la manera más fácil y rápida de llevar un aplicativo a AWS, dado que el aprovisionamiento es automático, lo importante es tener bien definido el stack tecnológico de la aplicación. Los casos más comunes de aplicación de Beanstalk son aplicaciones web, CMS (Content System Management) y APIs.

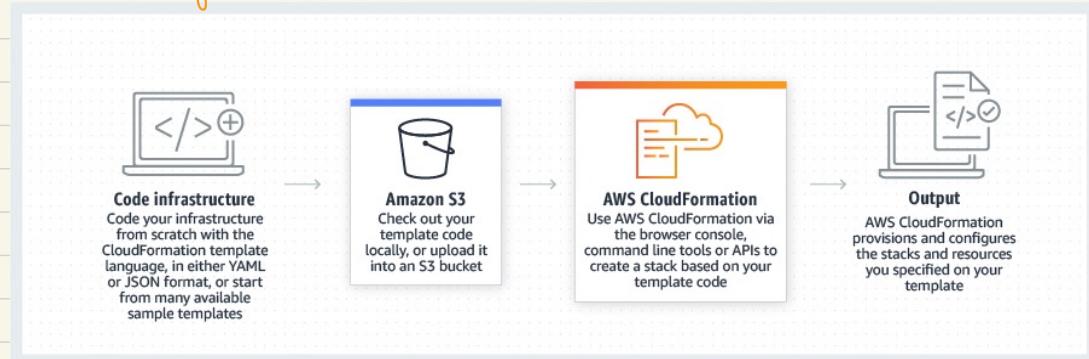
Domain 3  
Technology  
Methods of deploying and operating

CloudFormation

¿Qué es CloudFormation?

- CloudFormation es una herramienta para despliegues en AWS, que se basa en usar templates para crear y administrar recursos.
- Permite aplicar un modelo de infraestructura como código a través de plantillas.
- Facilita el control de versiones de nuestro aprovisionamiento.
- Permite replicar la infraestructura repetidamente y en forma rápida.
- Permite ahorrar tiempo.

Modelo de implementación de CloudFormation



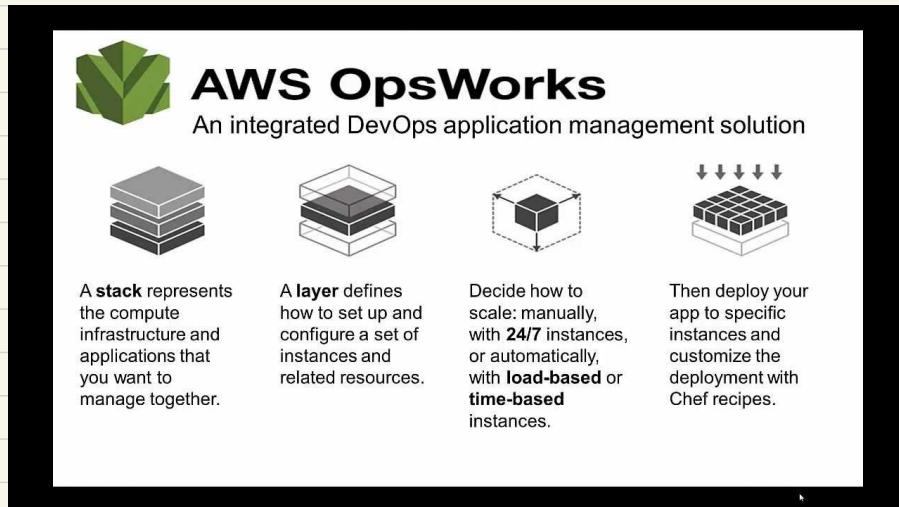
CloudFormation permite usar repositorios de templates para administrar las versiones de nuestra infraestructura en forma más eficiente, además de poder replicar arquitectura en forma segura y ordenada, manteniendo control sobre la granularidad.

DOMAIN 3  
Technology  
Method of Deploying and operating

## OpsWorks

¿Qué es AWS OpsWorks?

- Es una herramienta que permite administrar la configuración de despliegues con Chef.
- Permite personalizar aún más los despliegues y el aprovisionamiento de un stack.
- Existen dos variantes:
  - OpsWorks stacks: Permite organizar los despliegues en stacks configurables, sin necesidad de tener un chef server, ya que AWS lo maneja automáticamente.
  - OpsWorks for Chef Automate: La idea es la misma, sólo que los servidores Chef necesarios los administra AWS como Chef Server Premium, permitiendo usar herramientas como Chef DK y otras herramientas adicionales de Chef.



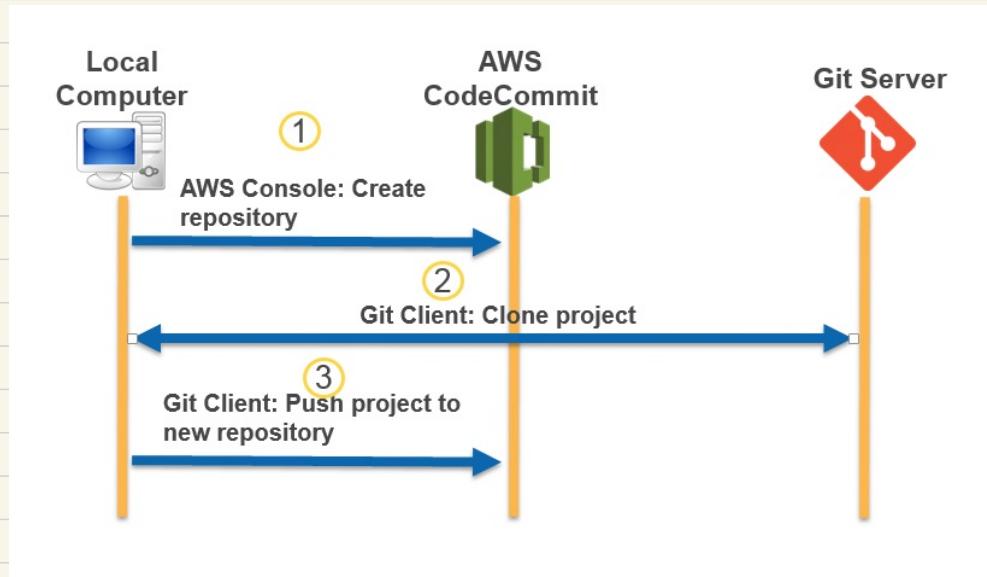
OpsWork nos permite usar Chef como sistema de administración de despliegues así podemos hacer despliegues programáticos.

Dom 4W 3  
Technology  
Methods of Deploying and Operating

Code Commit

¿Qué es Code Commit?

- Es un servicio de control de código (repositorio) de alta disponibilidad y escalabilidad, para almacenar desde código hasta binarios.
- Implementa Git
- Es compatible con CodePipeline and CodeDeploy



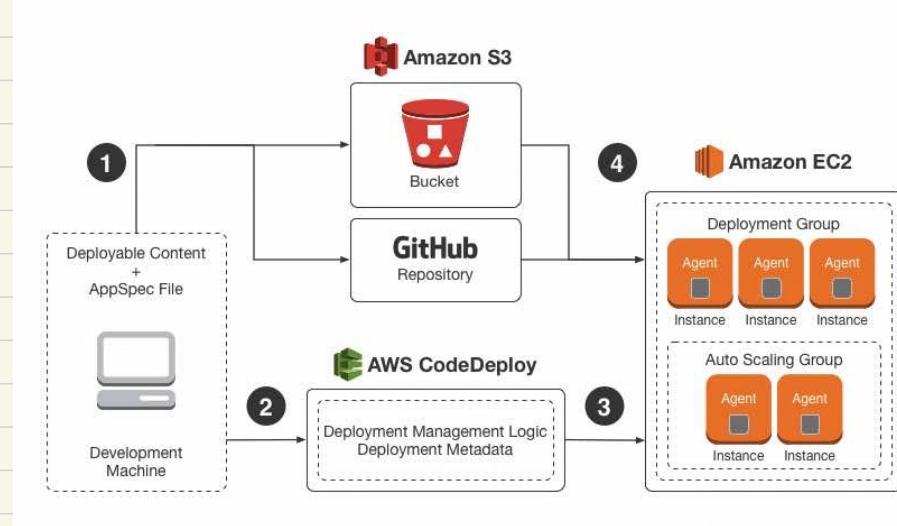
Es un repositorio git disponible en AWS compatible con CodeDeploy y CodePipeline.

DOMAIN 3  
Technology  
Methods of deploying and operate

CODE DEPLOY

¿QUE ES CODE Deploy?

- Es un servicio que coordina despliegues de aplicaciones automáticamente.
- Agiliza los despliegues y evita el downtime.
- Maneja la complejidad de los despliegues.
- Es una buena elección para delegar tareas de despliegue o para instrumentar CI/CD



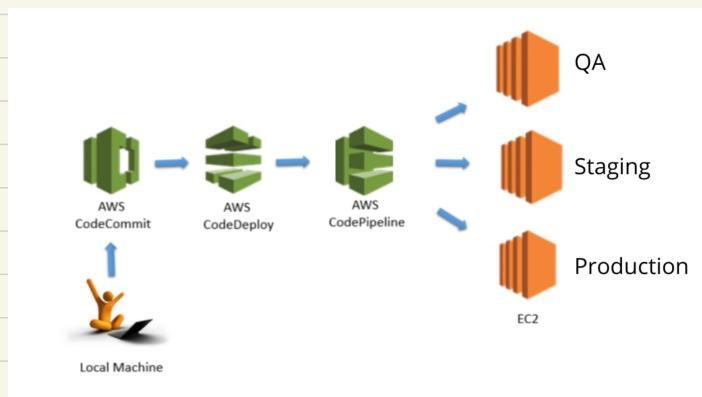
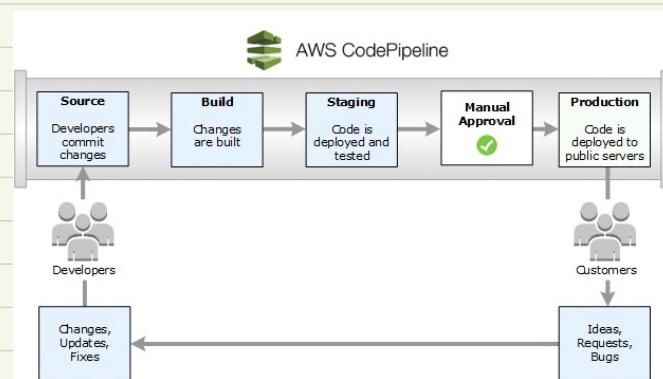
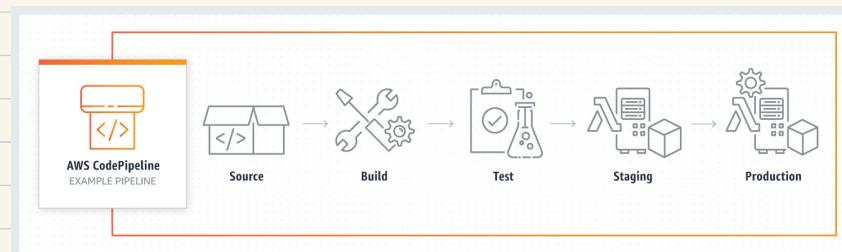
CodeDeploy permite crear scripts para despliegues automáticos, facilitando la tarea compleja de despliegues. Es compatible con CloudFormation, permitiendo desplegar infraestructura también.

DOMAIN 3  
Technology  
Methods of Deployment and operating

## CODE Pipeline

### ¿Qué es CodePipeline?

- Es una herramienta de CI y CD usada para aplicaciones como para infraestructura.
- Facilmente se integra con herramientas de terceros.
- Se puede usar en conjunto con CodeCommit y CodeDeploy.
- Construye, Prueba y Despliega el aplicativo cada vez que se presentan cambios.
- Se pueden definir modelos de release.



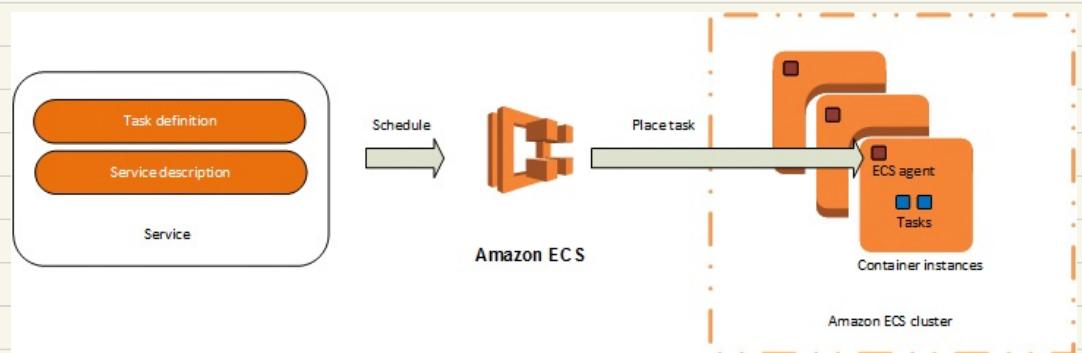
CodePipeline es la herramienta en AWS que permite diseñar modelos de despliegue, permitiendo instrumentar un ambiente de Integración Continua y Delivery Continuo. Es el equivalente a Jenkins en AWS.

DOMAIN 3  
Technology  
METHODS OF DEPLOYMENT AND OPERATING

## ELASTIC CONTAINER SERVICE (ECS)

¿QUÉ ES AWS ECS?

- Es un servicio de administración de contenedores basado en Docker.
- Permite ejecutar, pausar y parar contenedores Docker en AWS.
- Elimina la necesidad de instalar, operar y escalar tu propia infraestructura de clusters.
- Posee una API para manejar los contenedores.



ECS simplifica la administración de contenedores Docker proveiendo un servicio en AWS que simplifica la tarea de correr aplicaciones en Docker.

DOMAIN 3  
Technology  
Methods for Deployment and Operating

SOLUCIONES NO AWS

¿Cuáles son las soluciones no AWS?

- SON TODAS LAS SOLUCIONES COMPATIBLES CON LA PLATAFORMA AWS PERO QUE NO SON PARTE DE ELLA, TALES COMO:
  - INFRAESTRUCTURA COMO CÓDIGO: Es el proceso de administrar y aprovisionar data centers a través de archivos de configuración que pueden ser leídos por la máquina.
    - \* TERRAFORM
    - \* SALT STACK
    - \* ANSIBLE
  - ADMINISTRACIÓN DE CONFIGURACIONES: Es un sistema de manejo de configuraciones que permite mantener la estabilidad, el rendimiento y atributos físicos de una aplicación.
    - \* CHEF
    - \* PUPPET
    - \* ANSIBLE
  - INTEGRACIÓN CONTINUA: Es la práctica de la integración de cambios en el código desde múltiples contribuyentes en un único proyecto de software.
    - \* JENKINS
    - \* TEAM CITY
  - REPOSITORIOS DE CONTROL DE VERSIONES: Son productos que permiten a los desarrolladores colaborar en un código fuente único, manteniendo el versionamiento.
    - \* GITHUB
    - \* GITLAB
    - \* BITBUCKET

EXISTEN VARIAS SOLUCIONES DE SOFTWARE FUERA DEL ESPECTRO DE AWS, LAS MAS IMPORTANTES SON:

- Terraform	- CHEF	- TEAMCITY	- Bitbucket
- Ansible	- Puppet	- GitHub	
- Salt Stack	- JENKINS	- GitHub	

Domain 3  
Technology  
Method for Deploying and Operation

Principios Generales

¿Cuáles son los principios generales de AWS?

- BUENAS PRÁCTICAS:
  - \* APROVISIONAR INFRAESTRUCTURA DESDE CÓDIGO
  - \* DESPLEGAR ARTEFACTOS AUTOMÁTICAMENTE DESDE EL CONTROL DE VERSIONES.
  - \* ADMINISTRAR CONFIGURACIONES DESDE CÓDIGO
  - \* ESCALAR LA INFRAESTRUCTURA AUTOMÁTICAMENTE.
  - \* MONITOREAR USANDO CLOUDWATCH
  - \* HACER LOGGING DE CADA OPERACIÓN, USAR CLOUDWATCH Y CLOUDTRAIL
  - \* ASIGNAR ROLES IAM A CADA PERFIL.
  - \* USAR VARIABLES, NO QUÉMAR VALORES
  - \* TAGEAR LOS RECURSOS APROVISIONADOS.
- ACTUALIZACIONES DE STACK TECNOLÓGICO:
  - \* MANTENER ACTUALIZADA EL IAM
  - \* HACER USO DE INTEGRACIÓN CONTINUA
  - \* USAR EL MÉTODO BLUE/GREEN, TENIENDO UN AMBIENTE DE PRODUCCIÓN AZUL (BLUE) Y OTRO AMBIENTE VERDE (GREEN) PARA NUEVAS VERSIONES.

AWS DEFINE UNOS PRINCIPIOS GENERALES COMO UN CONJUNTO DE NORMAS GENERALMENTE ACEPTADAS COMO BUENAS PRÁCTICAS PARA LA GOBERNANZA DE RECURSOS EN AWS.

## Regions y Availability Zones

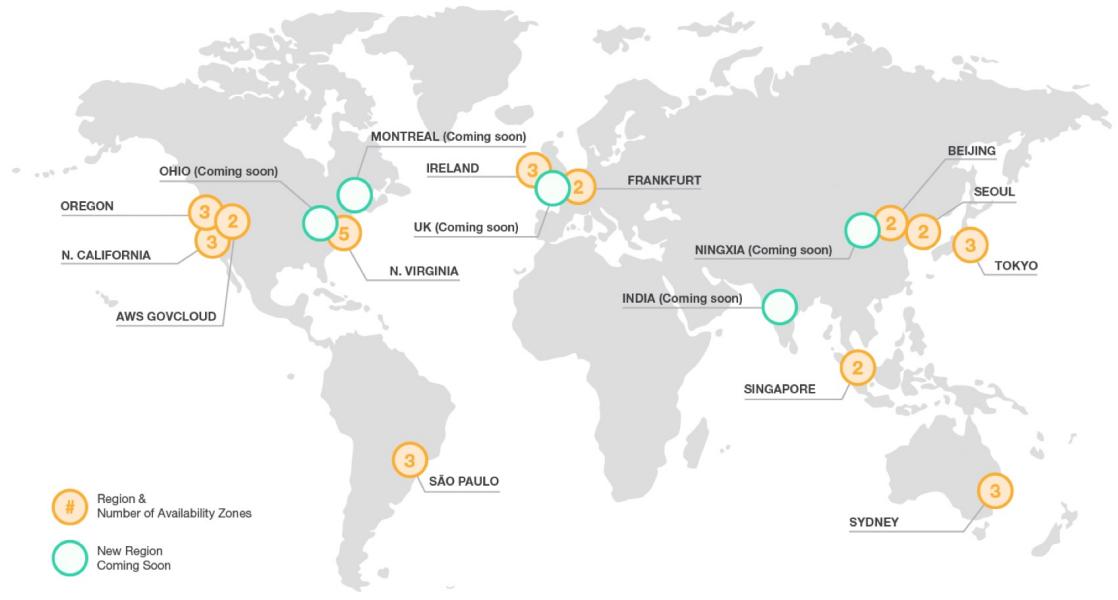
¿Cómo está construida la Infraestructura de AWS?

- TODA LA INFRAESTRUCTURA DE AWS ESTÁ CONSTRUIDA SOBRE DOS TIPOS DE RECURSOS:

\* Region: Es una localización física en el mundo con múltiples Availability Zones

\* Availability Zone: Consiste en uno o más datacenters discretos con sus propias red, fuentes de poder y espacio.

## Global Infrastructure



Los servicios de AWS se encuentran disponibles a través de las regiones y sus diferentes Availability Zones a nivel mundial.

DOMAIN 3  
Technology  
AWS Global Infrastructure

Regiones y Número de AZs

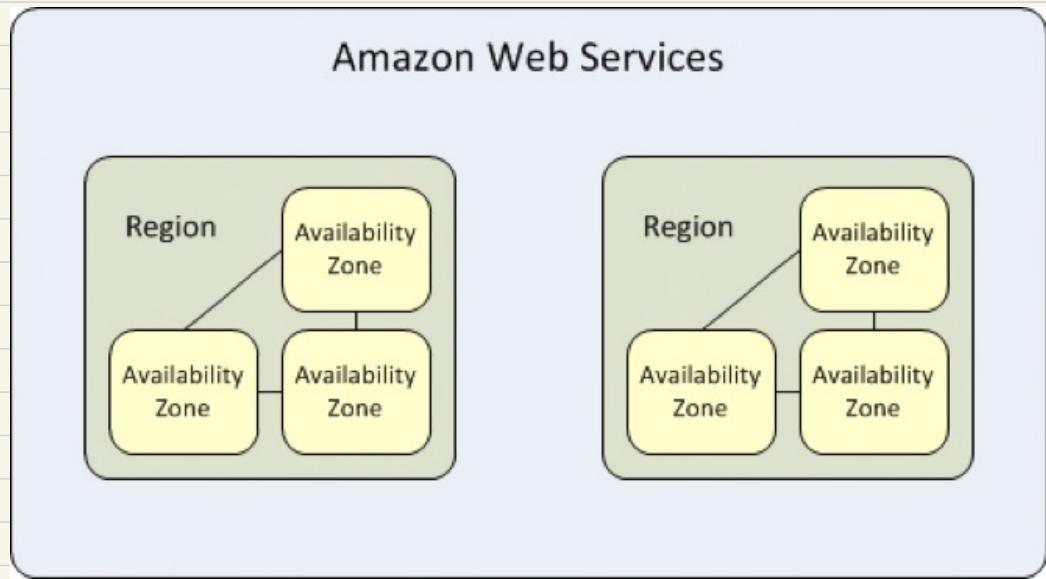
¿Cuántas Regiones y AZ tiene AWS?

- En total AWS opera con 77 AZs dentro de 24 Regiones:
  - US EAST
    - + Virginia (6)
    - + Ohio (3)
  - US WEST
    - + North California (3)
    - + Oregon (3)
  - ASIA PACIFIC
    - + Mumbai (2)
    - + Seoul (2)
    - + Singapore (2)
    - + Sydney (3)
    - + Tokyo (4)
    - + Bahrain (1)
  - CANADA
    - + Central (2)
  - CHINA
    - + Beijing (2)
  - EUROPE
    - + Frankfurt (3)
    - + Ireland (3)
    - + London (2)
  - South AMERICA
    - + São Paulo (3)
  - AWS GovCloud (US-West) (2)

AWS TIENE 77 AZs EN 24 REGIONES.

? Como se logra la alta disponibilidad en AWS?

- AWS implementa la alta disponibilidad a través de la conexión de AZs con otras en una red de fibra óptica permitiendo el failover al migrar de AZ.



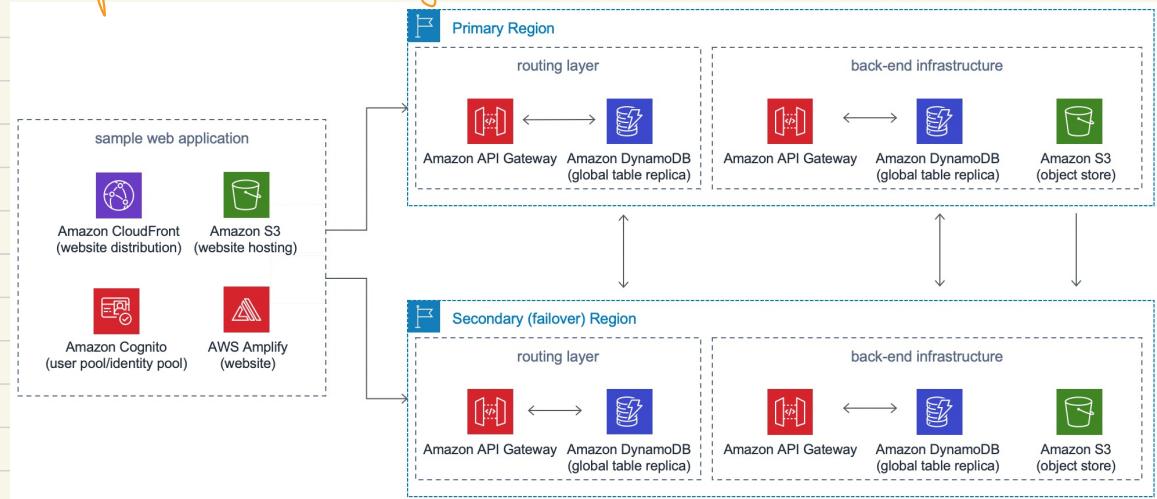
Los AZs son las piezas clave que al mantenerlas conectadas entre sí permite mantener la alta disponibilidad.

## MIGRACIÓN A ALTA DISPONIBILIDAD AL DESPLEGAR EN MÚLTIPLES REGIONES

¿Qué se logra al desplegar en múltiples regiones?

- Si se despliegan aplicaciones en múltiples AZs y múltiples regiones, se logra aumentar la tolerancia a fallos e incrementar la redundancia.
- Adicionalmente se puede hacer uso de redes privadas y redes públicas para agregar una capa adicional de continuidad del negocio o proveer baja latencia a nivel mundial.

### Ejemplo solución multi-region



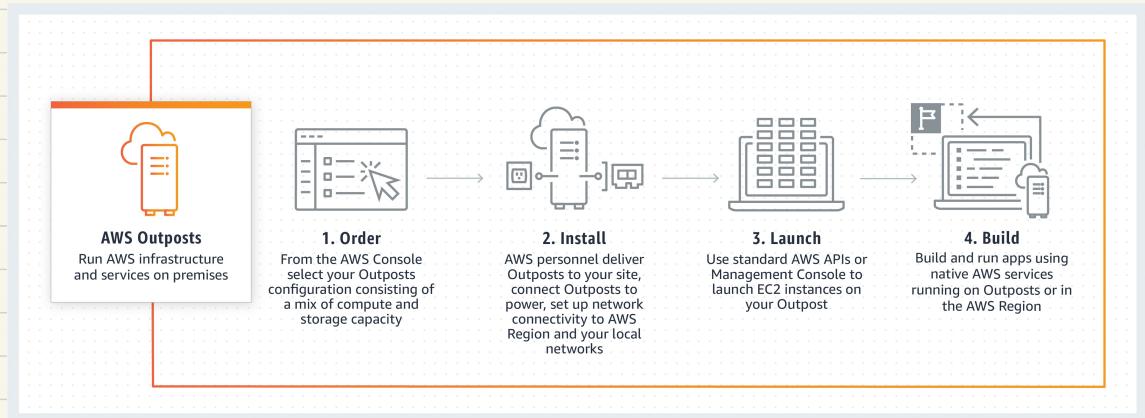
El objetivo fundamental al desplegar multi-region es contar con una redundancia mayor y aumentar la alta disponibilidad. En el momento de un incidente en una región se puede seguir prestando servicio con las regiones restantes, siempre que esté activa la replicación de los datos de los aplicativos también multi-region.

# DOMAIN 3 Technology AWS Global Infrastructure

Compliance y Data con Requerimientos Residenciales

¿Cómo AWS para soporte a los requerimientos residenciales de datos?

- Por temas legales, regulatorios, contractuales o de políticas, muchas organizaciones deben mantener su data en una cierta localización. Esos son requerimientos residenciales.
- AWS Outpost es el servicio para implementar requerimientos residenciales, extiende los servicios de AWS, tales como: Infraestructura, servicios y APIs desplegandolos en tu propio datacenter.



AWS asesora a sus clientes para dar cumplimiento a requerimientos que afecta el lugar de almacenamiento y procesamiento de la data, permitiendo incluso tener servicios de AWS corriendo On-Premise

DOMAIN 3  
Technology  
AWS Global Infrastructure

EXPANSIÓN GEOGRÁFICA.

¿Qué planes de  
expansión geográfica  
tiene AWS?

- AWS tiene planes de agregar 9 AZ nuevos en 3 regiones en CAPE TOWN, JAKARTA y MILAN.



AWS TIENE COMO NUEVOS AZ ADICIONALES 9 AZ Y 3 REGIONES ADICIONALES: CAPE TOWN, MILAN  
y JAKARTA

## Edge Locations

¿Dónde son los AWS Edge Locations?

- Un Edge Location es un cache de contenido usado por CloudFront para despachar los contenidos más rápido al estar estos Edge Location más cerca geográficamente de los clientes.
- Edge Location permite bajar la latencia al despachar contenido.



## Amazon CloudFront Edge Locations

Global Network Infrastructure



Los Edge Locations son usados cuando un cliente accede a un contenido que su fuente se encuentra en otra región alejada del cliente, entonces AWS reenruta y sirve el contenido del Edge Location más cerca geográficamente, bajando la latencia.

¿QUÉ ES EC2?

- Es un servicio de AWS que permite aprovisionar capacidad de cómputo escalable.
- Existen mucho tipos de instancias de EC2 dependiendo del trabajo a realizar
  - EC2 de propósito general { - T2  
- M4 }
  - EC2 de Computación Optimizada { - C4 }
  - EC2 de Memoria Optimizada { - X1  
- R4 }
  - EC2 de Computación Acelerada { - P2  
- G3  
- M1 }
  - EC2 de Almacenamiento Optimizado { - I3  
- D2 }
- Las instancias de EC2 están gobernadas por Security Groups.
- El modelo de precio de EC2 son 4, a saber:
  - On-Demand: Tu pagas la capacidad de cómputo contratada por hora o por segundo dependiendo de las instancias que se ejecuten.
  - Instancias Spot: Son instancias que no están en uso por la plataforma, por lo que su costo es 90% menor.
  - Instancias Reservadas: Son instancias que se reservan anticipadamente en periodo de 1 a 3 años, su costo es 75% menor.
  - Facturada por segundo: Solo pagues por lo que usas, facturado por segundos mensuales.
- Se usa AWS AMI (Amazon Machine Images) para aprovisionar EC2 desde Templates.
- Se usan Keys para su acceso
- Se usa EBS (Elastic Block Storage) para proveer almacenamiento a instancias EC2

EC2 es el servicio de AWS que permite aprovisionar poder de cómputo a través de la creación de instancias de diferentes tipos, dependiendo de las necesidades de procesador, memoria y uso.

¿Qué es S3?

- Es un servicio de almacenamiento de objetos, creado para guardar y extraer cualquier cantidad de datos, con 99.9999999999 de durabilidad.
- Es el único servicio en la nube de almacenamiento con funcionalidad query-in-place, permitiendo hacer analítica directo al almacenamiento.
- Existe clases de almacenamiento en S3:
  - S3 Standard: Diseñada para almacenamiento de propósito general y acceso frecuente.
  - S3 Standard Acceso Infrecuente: Diseñado como un almacenamiento de largo plazo, pero de acceso menos frecuente, pero de rápido acceso cuando se necesita.
  - Glacier: Diseñado para almacenar datos tipo archive, es decir a largo plazo pero de muy poco acceso, hay tres opciones de accesos de minutos a varias horas.
- En S3 la pieza fundamental para repositorio son los buckets.



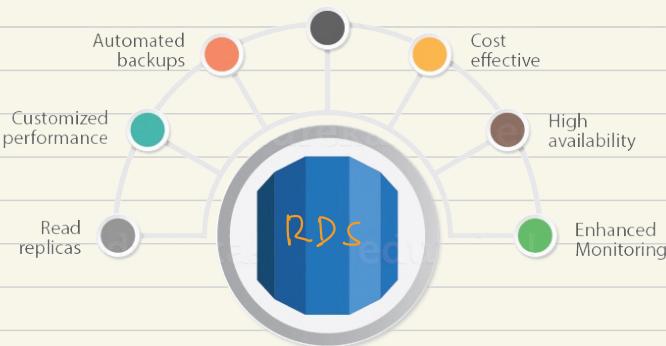
S3 es el servicio de almacenamiento en AWS, permitiendo almacenar objetos y retornarlos con 99.9999999999 de durabilidad, posee tres tipos de tipos: Standard, Acceso Infrecuente y Glacier.

¿Qué es RDS?

- RDS (Relational Database Service): Es el servicio de aprovisionamiento de bases de datos relacionales en la nube de AWS.
- Hay dos tipos de instancias de RDS:
  - Instancia de Propósito General
    - T3
    - T2
    - M6g
    - M5
    - M5
    - M4
  - Instancia de Memoria Optimizada
    - R6g
    - R5
    - R5b
    - R5d
    - R4
    - X1c
    - X1
    - Z1d
- RDS soporta varios motores de base de datos:
  - Amazon Aurora
  - PostgreSQL
  - MySQL
  - MariaDB
  - Oracle Database
  - Microsoft SQL Server
- RDS soporta encriptación en el almacenamiento y en tránsito usando keys administradas con KMS.
- Los backups son automáticos, se pueden hacer snapshot bajo demanda y el software de base de datos es actualizado automáticamente.

IAM integration

edureka!



RDS es el servicio en AWS que permite aprovisionar motores de Base de Datos Relacionales, como: Aurora, MySQL, MariaDB, SQL Server, Oracle PostgreSQL, de esta forma se facilita la administración y mantenimiento, a la vez que se mantienen los backups, actualizaciones y la seguridad.

