Mitos de la seguridad en la nube ¡eliminados!

Dario Goldfarb

Security Architect, Amazon Web Services, LATAM

goldfarb@amazon.com

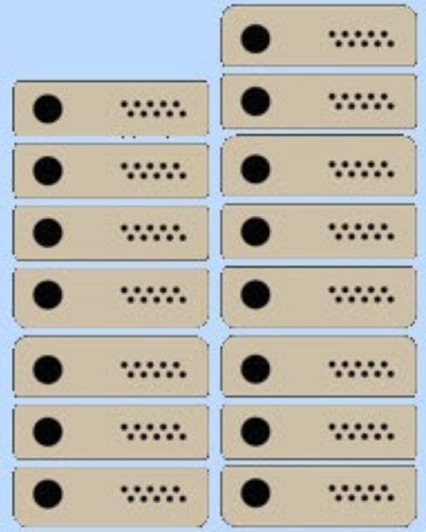
Mito Nro. 1

"Es lo mismo si está acá o en la nube, el trabajo de seguridad es el mismo"

Demitificado

aws

Hay mas transformación al moverse a la nube que esto …



Modelo de Responsabilidad Compartida

Seguridad EN la nube

El Cliente es responsable por la seguridad de las cargas de trabajo que despliega

Seguridad DE la nube

El Proveedor de Nube es responsable por proteger la infraestructura donde se ejecutan los servicios

En la nube no estás solo defendiendo la seguridad de tus datos y aplicaciones

aws

Modelo de responsabilidad compartida

Tipos de servicios

Servicios de infraestructura

Servicios encapsulados o gestionados

Servicios abstractos

aws

Modelo de responsabilidad compartida

Ejemplo: bases de datos

- Control de acceso
- Cifrado
- Crecimiento elástico
- Escalabilidad
- Alta disponibilidad
- Respaldos de BD
- Gestión de la BD (parches, hardening)
- Instalaciones para BD
- Gestión del SO (parches, hardening, antimalware*)
- Instalación del SO
- Mantenimiento de servidores
- Montaje en racks - red
- Electricidad, enfriamento
- Seguridad física – Procesos de seguridad

Servicios de infraestructura

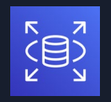
EC2

* Requerido Por PCI-DSS

Modelo de responsabilidad compartida

Ejemplo: bases de datos

Servicios encapsulados



RDS

Control de acceso

Crecimiento elástico

Operaciones

Cifrado

Escalabilidad

Alta disponibilidad

Respaldos de BD

Configuración

Gestión de la BD (parches, hardening)

Instalaciones para BD

Gestión del SO (parches, hardening, antimalware*)

Instalación del SO

Mantenimiento de servidores

Montaje en racks - red

Electricidad, enfriamento

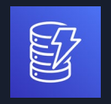
Seguridad física – Procesos de seguridad

* Requerido Por PCI-DSS

Modelo de responsabilidad compartida

Ejemplo: bases de datos

Servicios abstractos



DynamoDB

Control de acceso

Crecimiento elástico

Operaciones | Cifrado | Configuración

Escalabilidad

Alta disponibilidad

Respaldos de BD

Gestión de la BD (parches, hardening)

Instalaciones para BD

Gestión del SO (parches, hardening, antimalware*)

Instalación del SO

Mantenimiento de servidores

Montaje en racks - red

Electricidad, enfriamento

Seguridad física – Procesos de seguridad

* Requerido Por PCI-DSS

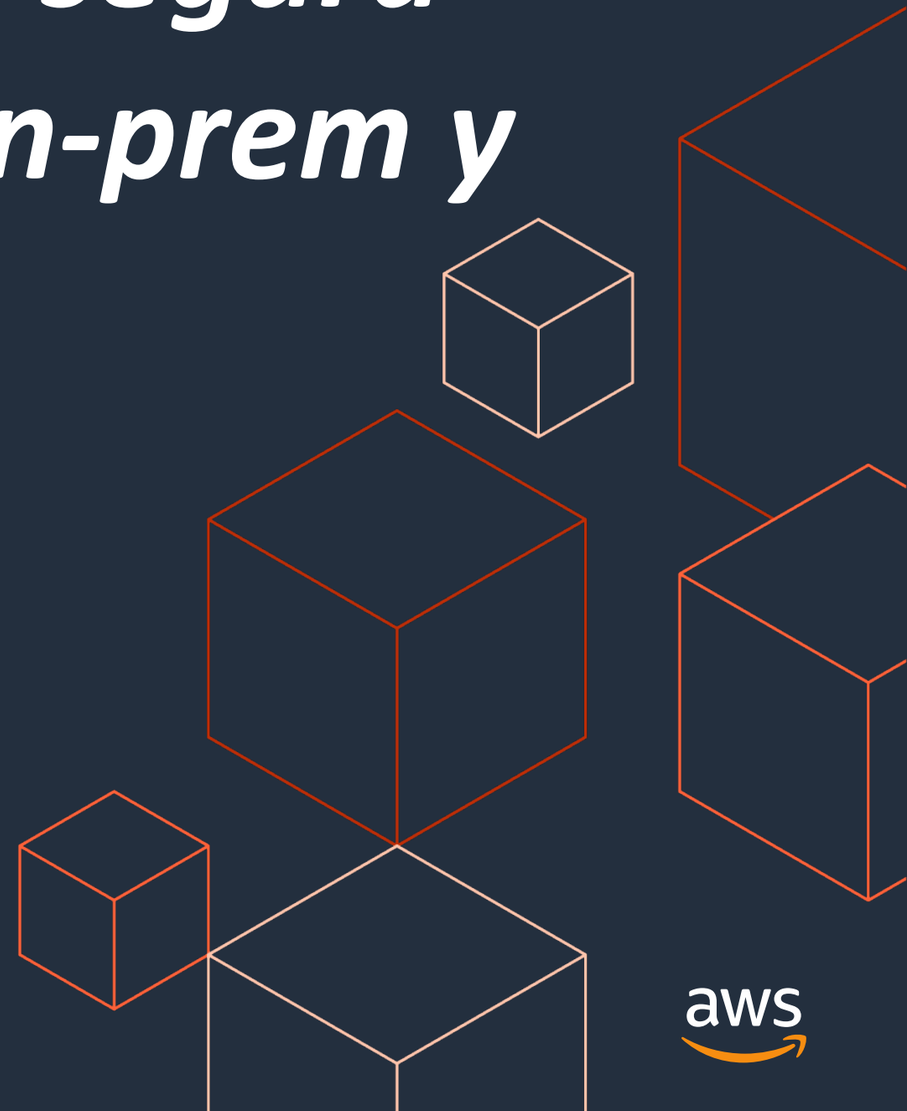
aws

aws

Mito Nro. 2

"La nube pública no es tan segura como mi infraestructura on-prem y nube privada"

Demitificado



aws

Seguridad de la nube

¿Cómo AWS hace su parte?

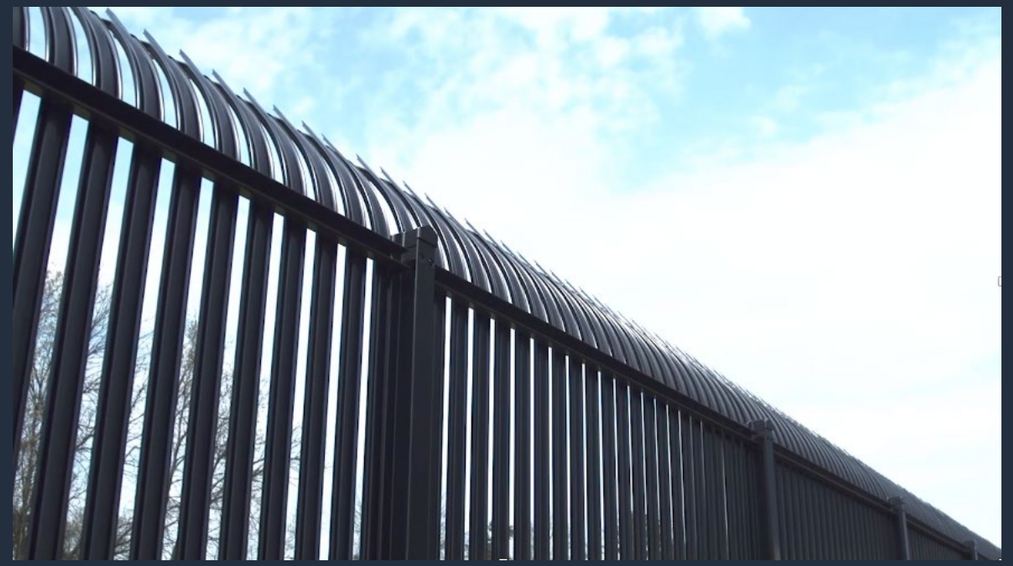
Seguridad DE la nube

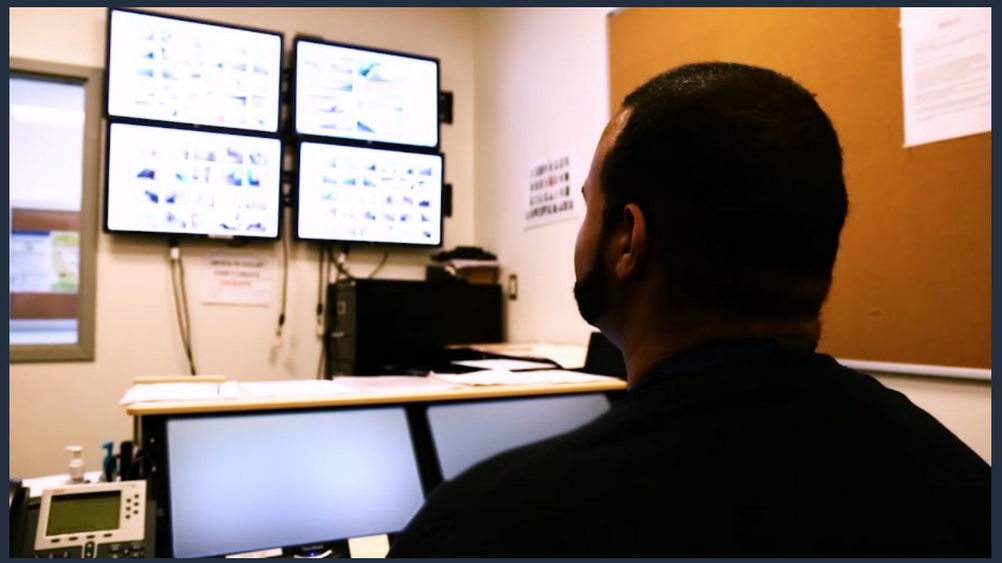
AWS es responsable por proteger la infraestructura donde se ejecutan los servicios

Protección del perímetro

https://aws.amazon.com/es/compliance/data-center/perimeter-layer

Protección del perímetro



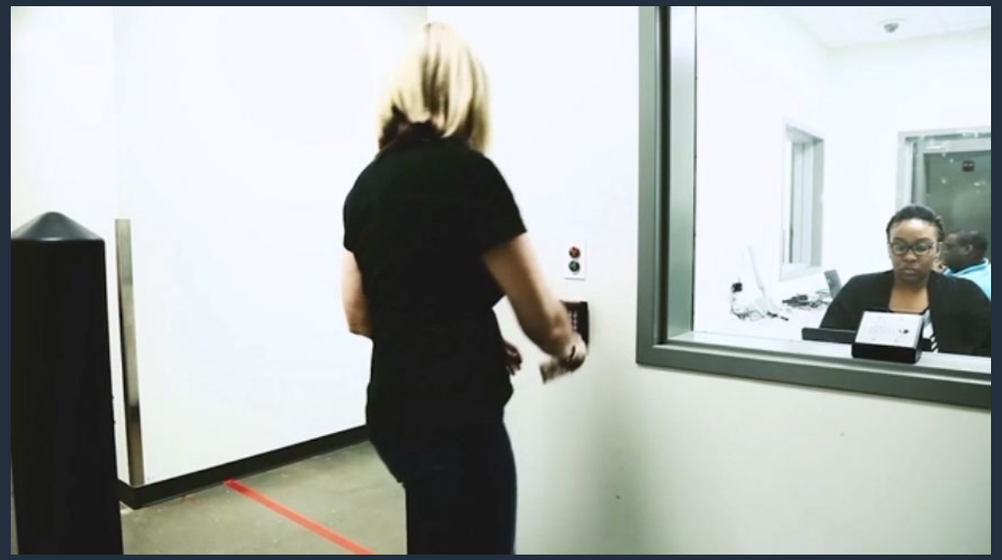


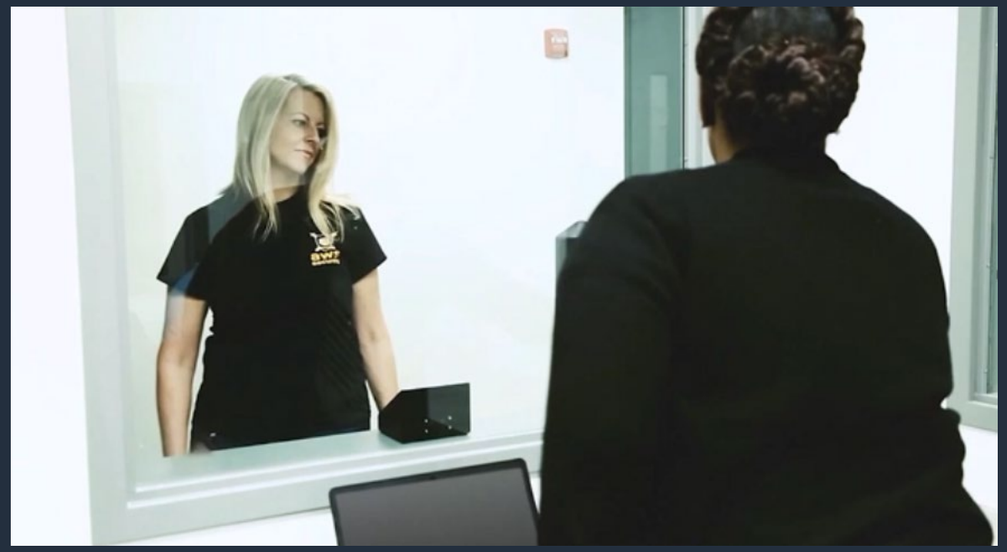
https://aws.amazon.com/es/compliance/data-center/perimeter-layer

Protección del acceso a las salas del datacenter

https://aws.amazon.com/es/compliance/data-center/data-layer

Protección del acceso a las salas del datacenter





https://aws.amazon.com/es/compliance/data-center/data-layer

aws

Ejemplo de políticas de seguridad de datos en AWS

Dispositivos de almacenamiento son destruidos EN el datacenter previo a ser decomisionados.

AWS Realiza su parte del modelo eficientemente con automatizaciones

- Pipelines de despliegue continuo
- Despliegue de parches
- Procesos probados a escala
- Mínima intervención humana enfocada en la supervisión de los procesos automatizados
- Los mas altos niveles en hardening
- Auditoría

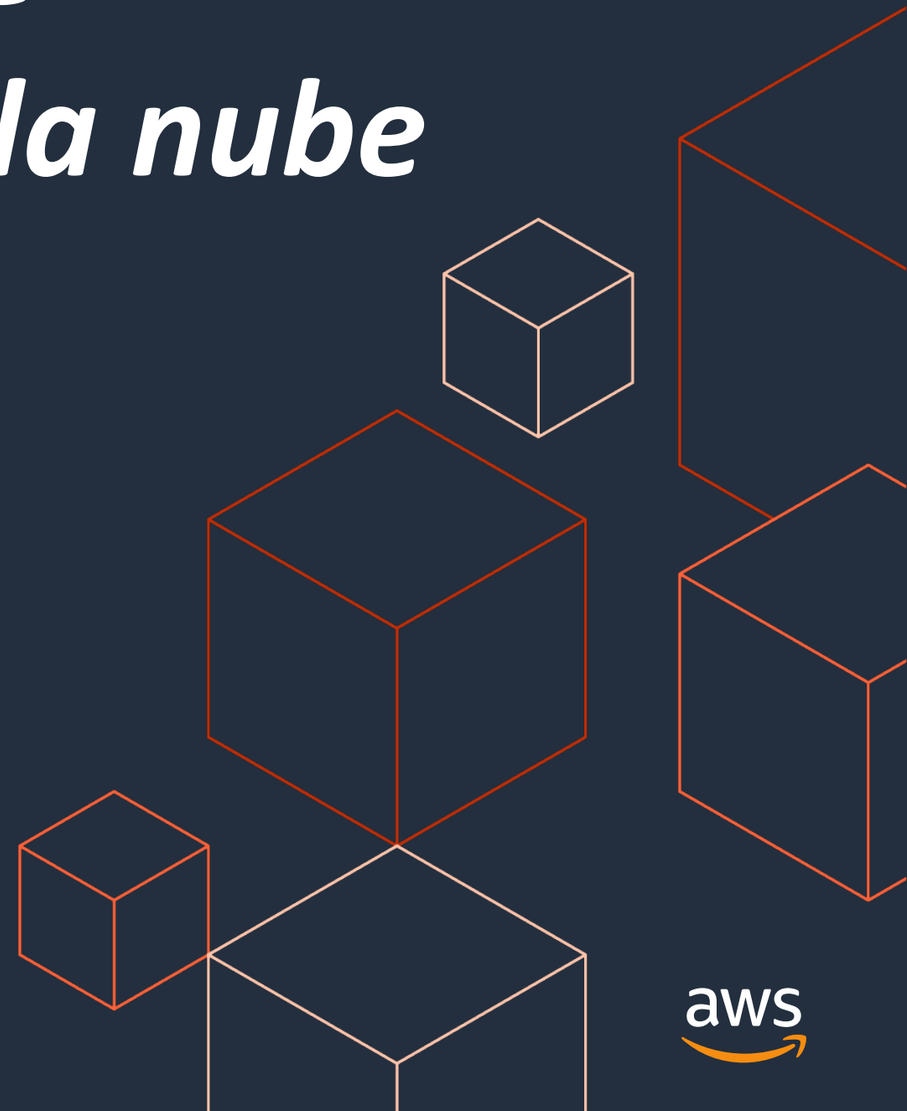
La inversión en seguridad de AWS es mucho más grande que lo que la mayoría de los clientes pueden hacer individualmente

aws

Mito Nro. 3

"Soy un negocio altamente regulado y no puedo usar la nube por mis requerimientos de cumplimiento"

Demitificado



aws

Programa de cumplimiento regulatorio global de AWS

CSA
Cloud
Security
Alliance Controls

ISO 9001
Global
Quality
Standard

ISO 27001
Security
Mgmt
Controls

ISO 27017
Cloud
Specific
Controls

ISO 27018
Personal
Data
Protection

PCS DSS
Level 1

+143

certificaciones y acreditaciones de seguridad y conformidad

SOC 1
Audit
Controls
Report

SOC 2
Security,
Availability &
Confidentiality
Report

SOC 3
General
Controls
Report

C5
(Germany)
Operational
Security
Attestation

Cyber
Essentials
Plus (UK)
Cyber Threat
Protection

ENS High (Spain)
Spanish
Gov
Standards

G-Cloud
UK
Gov
Standards

IT-Grundschutz
(Germany)
Baseline
Protection
Methodology

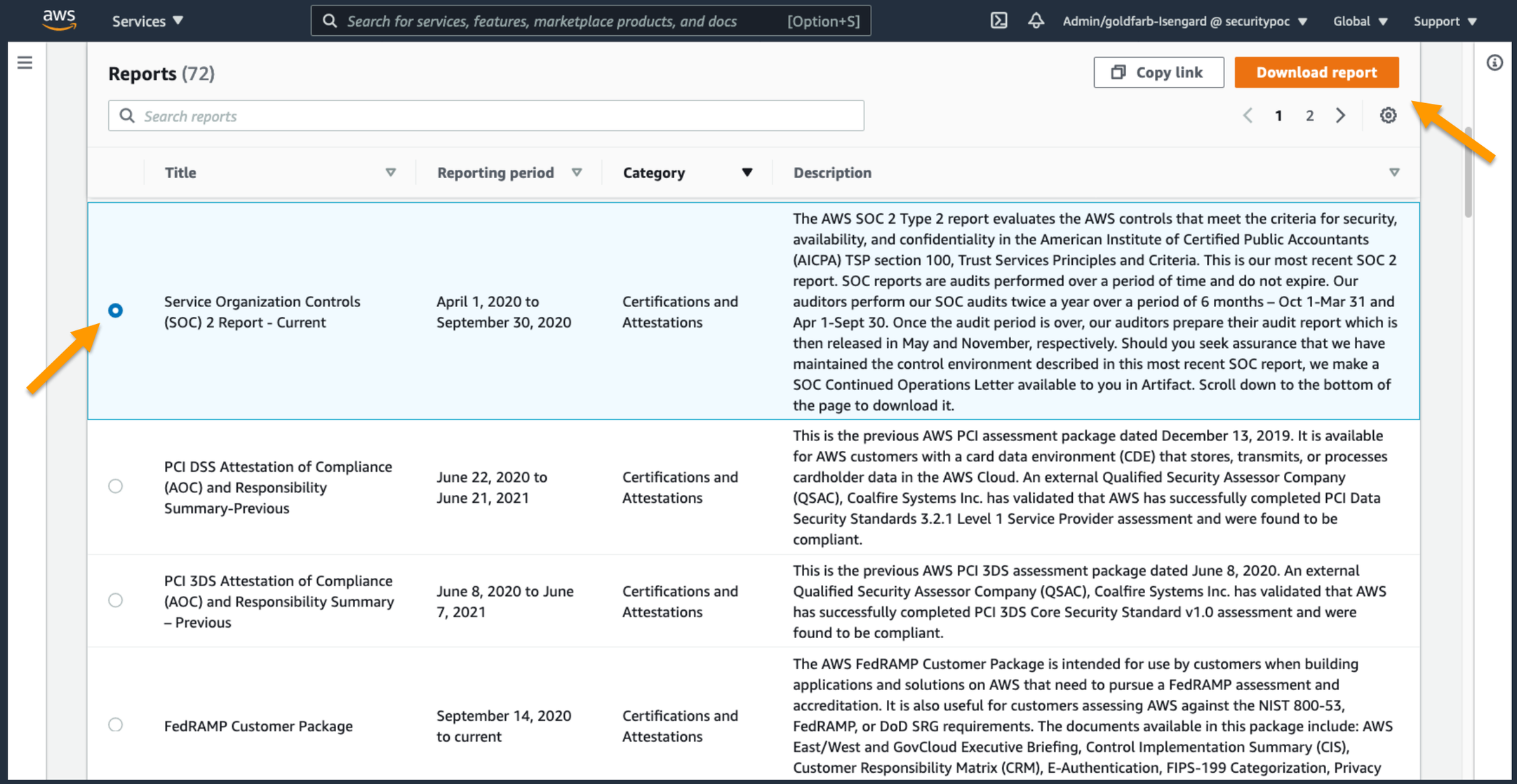
+2600

controles de seguridad auditados anualmente

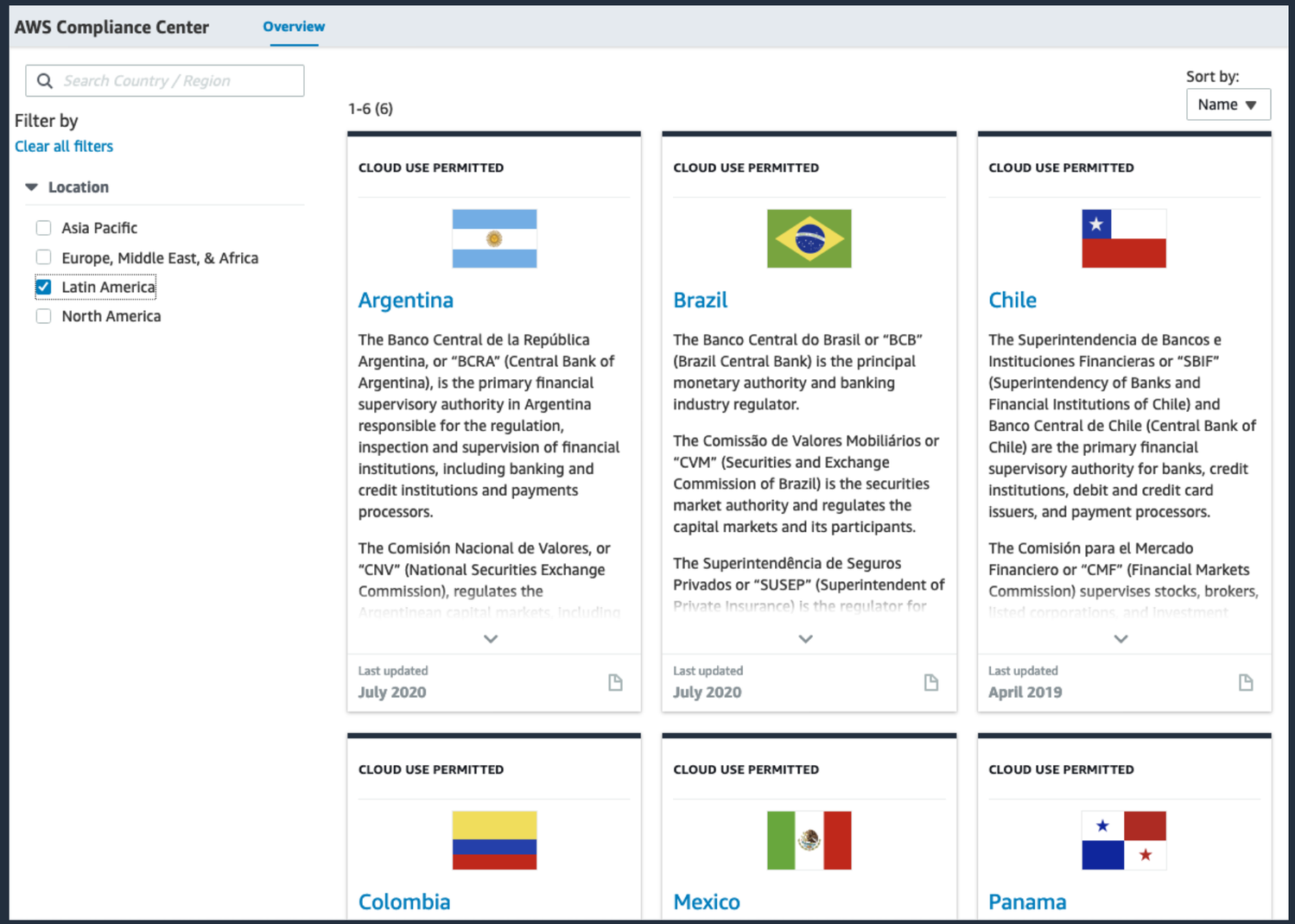
https://aws.amazon.com/es/compliance/programs/

Informes de auditoría y cumplimiento disponibles para los clientes en el portal de servicios en **AWS Artifact**

Informes de cumplimiento regulatorio: AWS Artifact



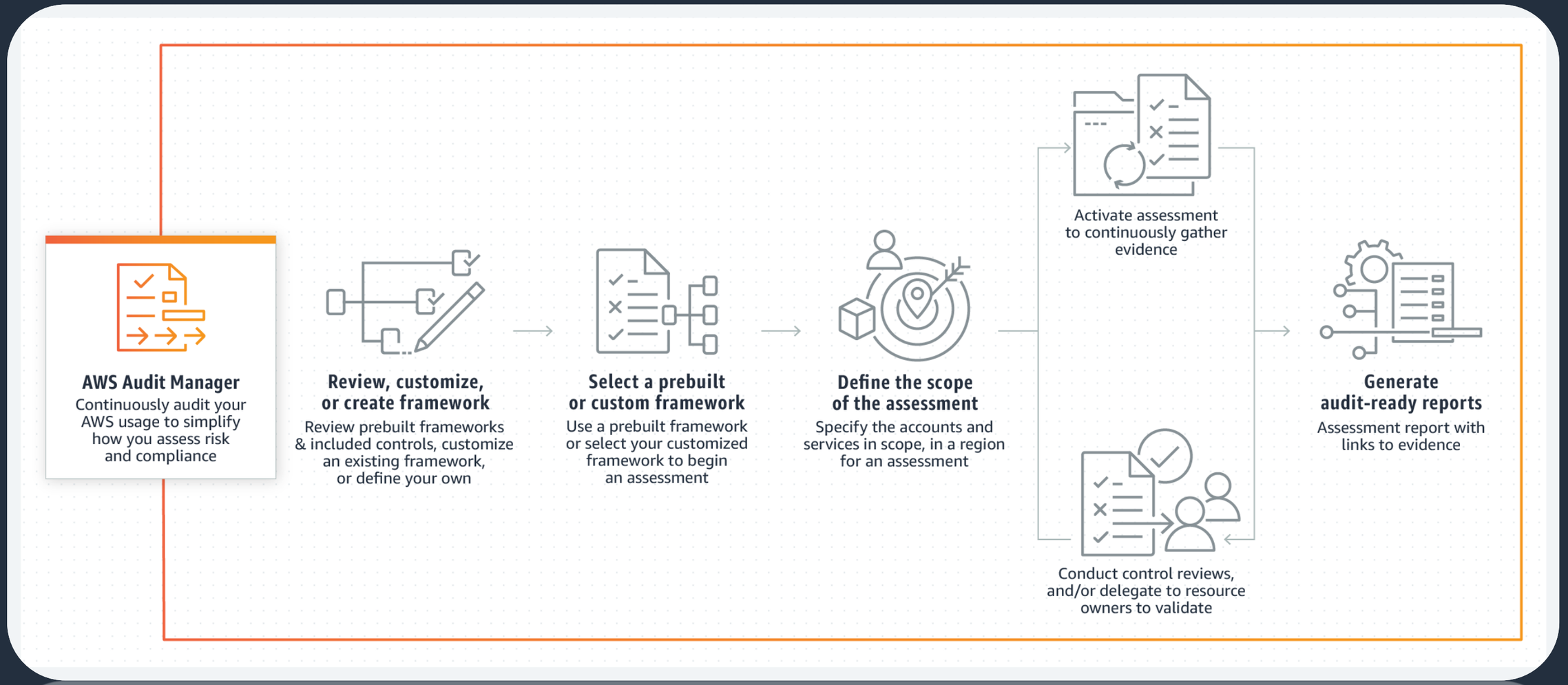
AWS Compliance Center



Información especifica de cada país para cumplimiento regulatorio en servicios financieros

https://aws.amazon.com/financial-services/security-compliance/compliance-center/

AWS Audit Manager



Frameworks de AWS Audit Manager

Incluye marcos de evaluación preconstruidos de AWS y AWS Partners

- **CIS** (Center for Internet Security) Foundations Benchmark
- **PCI DSS** (Payment Card Industry Data Security Standard)
- **GDPR** (General Data Protection Regulation)
- **GxP** (Good Practice Quality guidelines)
- **HITRUST** (Health Information Trust Alliance)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- **FedRAMP** (Federal Risk and Authorization Management Program)
- Mejores prácticas para Amazon S3, AWS IAM y Amazon DynamoDB
- Licencias de Software

Además, AWS Audit Manager soporta controles y frameworks definidos a medida

aws

Mito Nro. 4

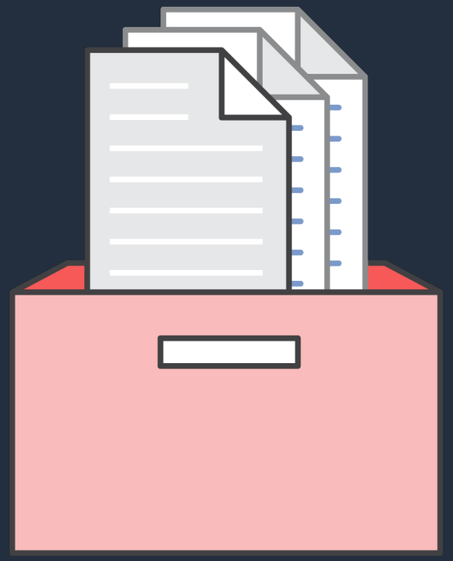
"Cuando ponga mis datos en la nube pierdo propiedad de ellos y podrían moverse a diferentes países"

Demitificado

aws

El Cliente es el dueño del los datos, controla el acceso y ubicación

Propiedad



Acceso

Trazabilidad

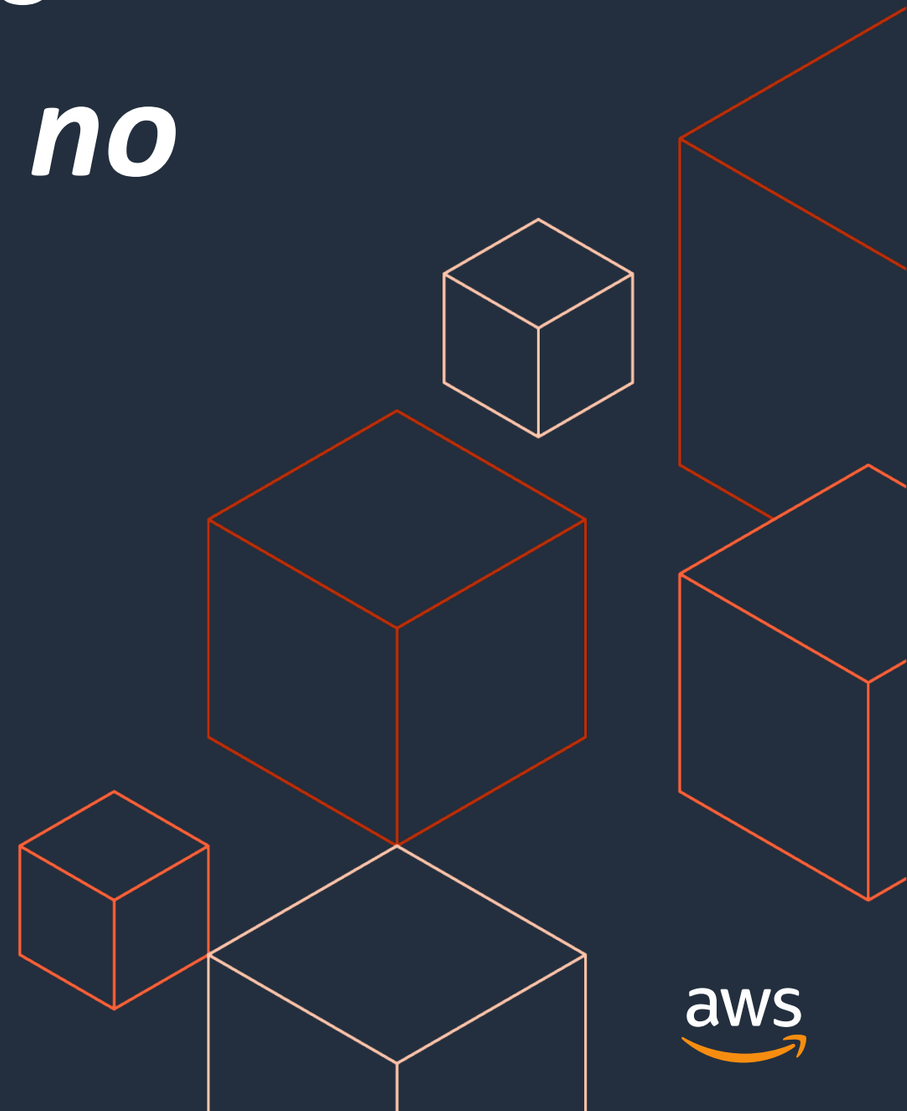
Usted conserva la propiedad y el control de su contenido, y elige en qué **región** reside el contenido.

aws

Mito Nro. 5

"Mi negocio requiere datos personales confidenciales, no puedo usar la nube"

Demitificado

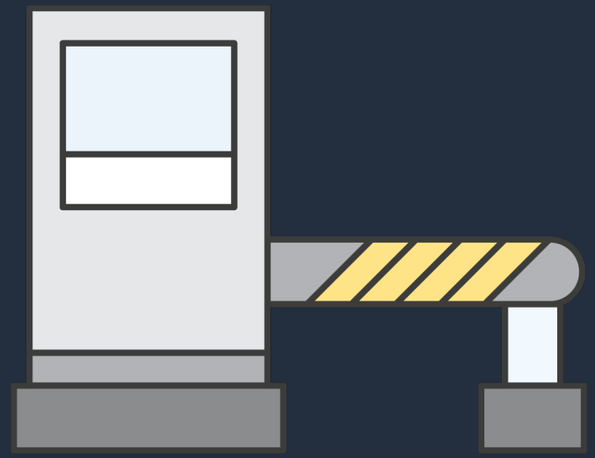


aws

Protección del almacenamiento de objetos (Amazon S3)

S3 privado por defecto

Public Access Block



AWS KMS

Los objetos en S3 son privados por defecto. Se pueden definir políticas centralizadas de bloqueo de acceso publico y el uso de cifrado agrega una nueva capa de control de acceso

aws

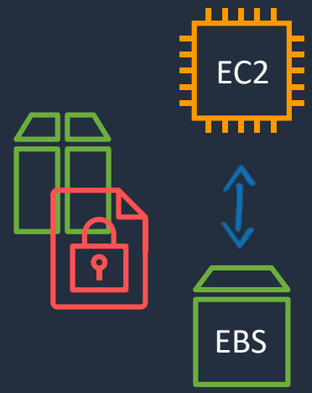
Cifrado de extremo a extremo: En reposo

AWS Key Management Service (KMS) - CloudHSM

AWS KMS

Cifrado de Volumen

- Cifrado de disco (EBS)
- Archivos
- Soluciones de Partner / Marketplace



Cifrado de Objetos

- Cifrado del lado del servidor (SSE-S3)
- S3 SSE con claves administradas por el cliente (KMS)
- Cifrado del lado del cliente

Cifrado de Base de Datos

- MS SQL
- ORACLE
- MYSQL
- PostgreSQL
- Redshift

aws

AWS KMS: Servicio gestionado de gestión de claves

- Usted controla la autenticación y la autorización
- AWS se encarga de la alta disponibilidad, durabilidad y escalabilidad
- Disminuye la latencia hasta sus aplicaciones ya que está en la nube
- **Integración** completa con servicios gestionados en la nube

AWS Key Management Service

aws

AWS KMS: Servicio gestionado de gestión de claves

- Servicio brindado con Hardware appliances que no permiten la extracción de clave a ningún admin de AWS y son a prueba de manipulaciones (tamper proof)
- Permite configurar la rotación anual de llaves.
- El servicio soporta el uso de **AWS CloudHSM** como repositorio para cuando alguna regulación requiera claves almacenadas en HSM dedicados.
- Soporta claves simétricas, asimétricas y firma digital

AWS Key Management Service

aws

Mito Nro. 6

"No puedo usar la nube para almacenar datos confidenciales porque todos podrían accederlos"

Demitificado

aws

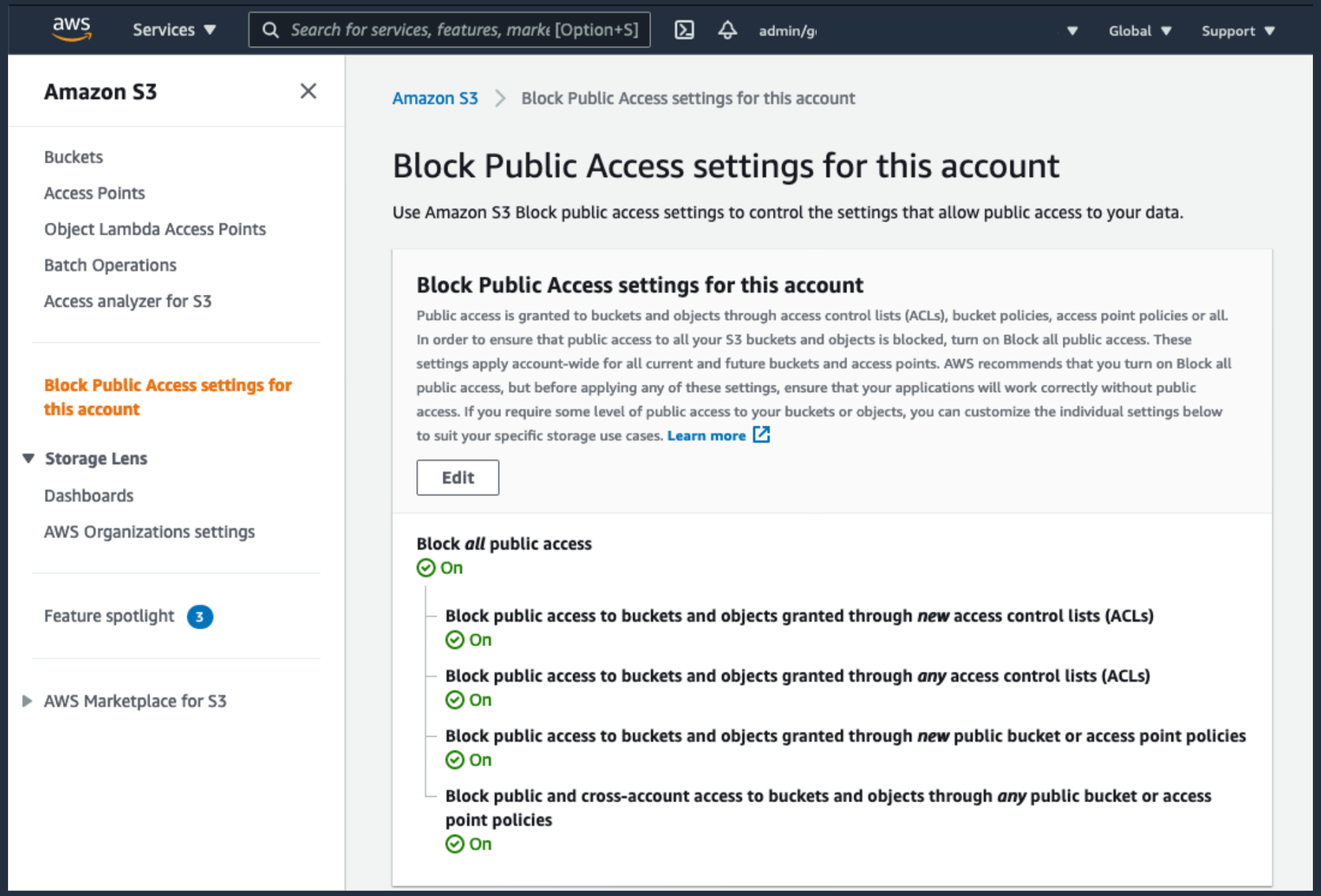
Los servicios vienen preconfigurados de modo seguro

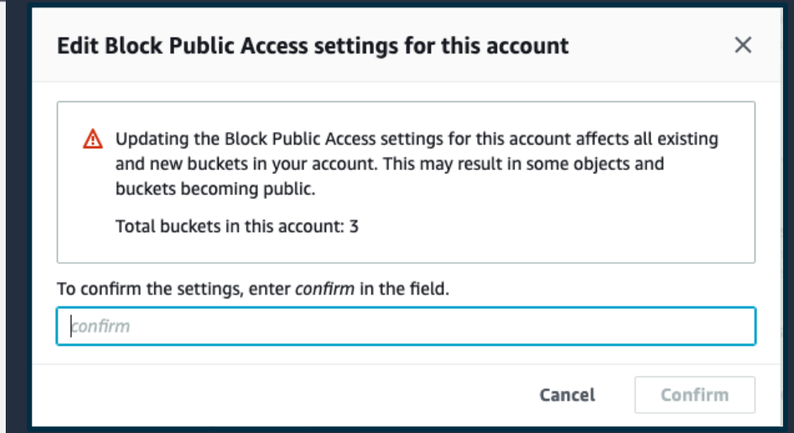
- Nuevos usuarios no tienen ningún permiso asignado
- Nuevos Buckets no permiten ningún permiso asignado
  (almacenamiento de objetos)
- Bloqueo de acceso público
  (Block Public Access)
  - Nuevas Cuentas → Bloqueo a nivel Cuenta
  - Nuevos Buckets → Bloqueo a nivel Bucket

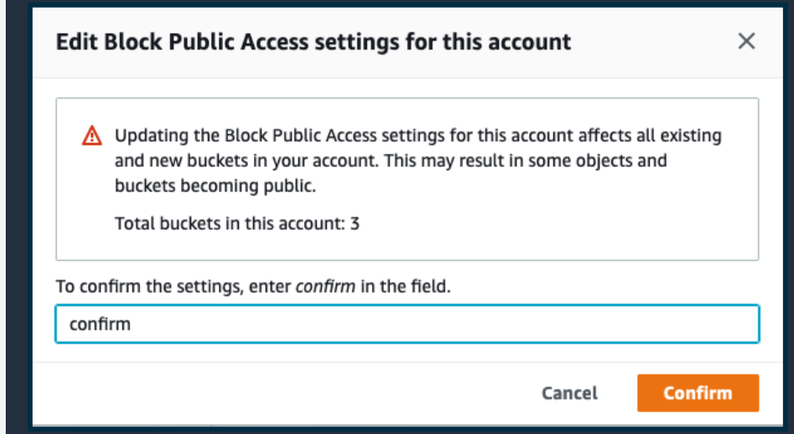
Los clientes cuentan con la flexibilidad de definir quien puede acceder a sus datos, AWS ofrece multiples herramientas para entender como están configurados los permisos

aws

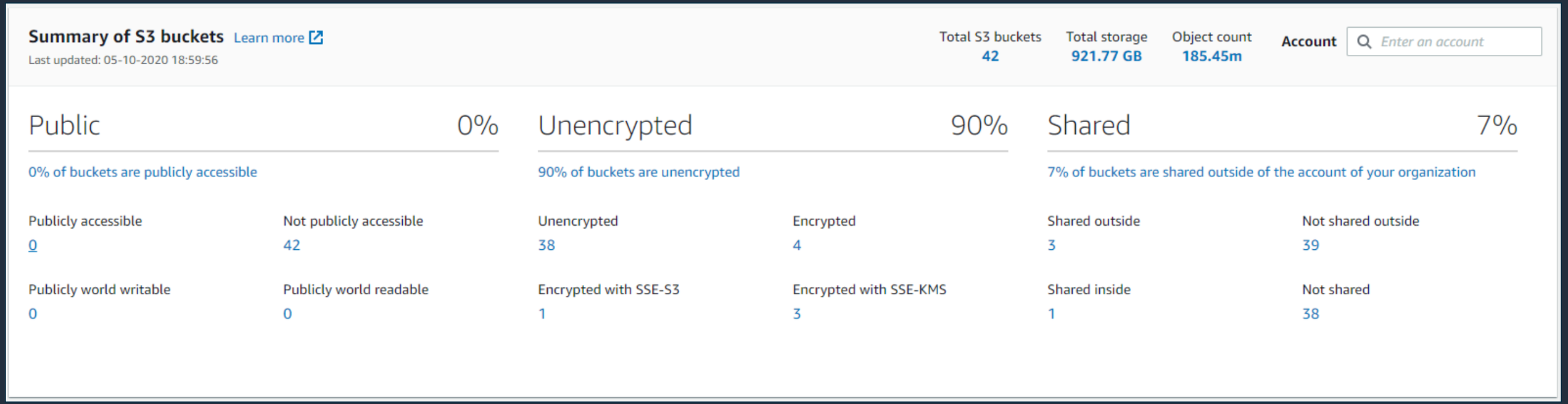
Block Public Access – Activado por defecto







Amazon Macie: Visibilidad – Inventario de S3 Buckets



- ¿Que porcentaje de mis Buckets están públicos ?
- ¿Que porcentaje de mis datos están cifrados ?
- ¿Cuantos usando mis claves en KMS?
- ¿Cuantos Buckets están siendo usados por cuentas fuera de mi organización?

Mito Nro. 7

"En la nube no puedo controlar la eliminación de mis datos y no puedo verificar que se hayan eliminado"

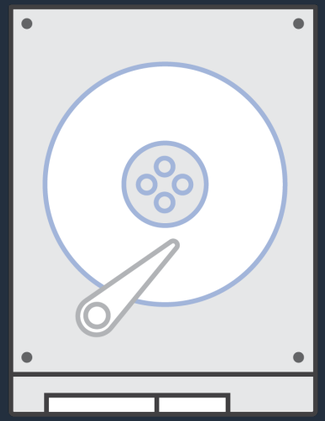
Demitificado

aws

¿Cómo AWS maneja la eliminación segura de datos?

EliminaciónLógica

EliminaciónFísica



Proceso Auditado

- Cuando eliminas tus datos AWS realiza múltiples pasos para la eliminación segura (wipe) antes de otorgar el medio de almacenamiento para otro uso
- Al llegar al fin de su vida útil se ocupa de la destrucción segura del medio.
- Este proceso es validado por auditores independientes de terceros.

aws

Servicios de seguridad gestionados

Identidades y Accesos

- AWS Identity & Access Management (IAM) — Free
- AWS Organizations — Free
- AWS Control Tower — Free
- AWS Cognito — Free Tier
- AWS Directory Service — Free Trial
- AWS IAM Identity Center — Free
- AWS Secrets Manager — Free Trial
- IAM Access Analyzer — Free

Controles de Detección

- AWS CloudTrail — Free Tier
- AWS Security Hub — Free Trial
- AWS Config
- Amazon CloudWatch — Free Tier
- Amazon GuardDuty — Free Trial
- VPC Flow Logs
- Traffic Mirroring
- Trusted Advisor — Free

Seguridad en Infraestructura

- AWS Systems Manager — Free
- AWS Shield — Free Tier (standard)
- AWS WAF
- AWS Firewall Manager
- AWS Network Firewall
- Amazon Inspector — Free Trial
- Amazon Virtual Private Cloud (VPC)
- EC2 Image Builder — Free

Protección de Datos

- AWS Key Management Service (KMS) — Free Tier
- AWS CloudHSM
- AWS Certificate Manager — Free Tier
- Amazon Macie — Free Tier, Free Trial
- Server-Side Encryption — Free
- S3 Block Public Access — Free

Respuesta ante Incidentes

- AWS Config Rules
- AWS Lambda — Free Tier
- Amazon Detective — Free Trial
- AWS Step Functions — Free Tier
- AWS CloudEndure DR
- AWS Backup
- AWS SSM Automations

Compliance

- AWS Artifact — Free
- AWS Audit Manager — Free Trial

https://aws.amazon.com/es/products/security/

Más de 1400 Soluciones e imágenes de seguridad en el AWS Marketplace, Pay as you go o BYOL.

En la nube podemos alcanzar mejores niveles de seguridad, con menor costo operativo

200+ certificaciones de cumplimiento regulatorio y acreditaciones
- Simplificación de auditorías (GAP)
- Auditoría unificada – Servicios integrados

Infraestructura construida para satisfacer los requerimientos de seguridad más altos, como organizaciones militares y bancos

- Potentes servicios de seguridad y características de seguridad nativas a bajo costo o gratuitos
- Marketplace con soluciones

- Modelo de responsabilidad compartida
- Servicios gestionados
- Equipos de seguridad 24/7

Reducción de los caminos de ataque y mejor contención

aws

¡ Gracias !

¿ Preguntas ?

Dario Goldfarb

goldfarb@amazon.com

https://www.linkedin.com/in/dariolucas/

@dario_goldfarb