



Mitos de la seguridad en la nube ¡eliminados!

Dario Goldfarb

Security Architect, Amazon Web Services, LATAM

goldfarb@amazon.com



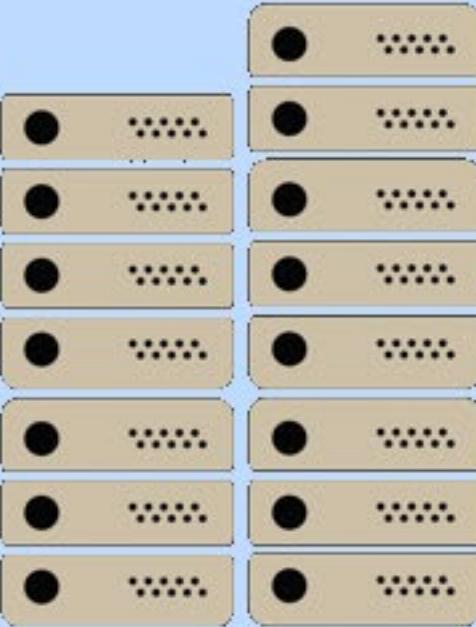
Mito Nro. 1

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

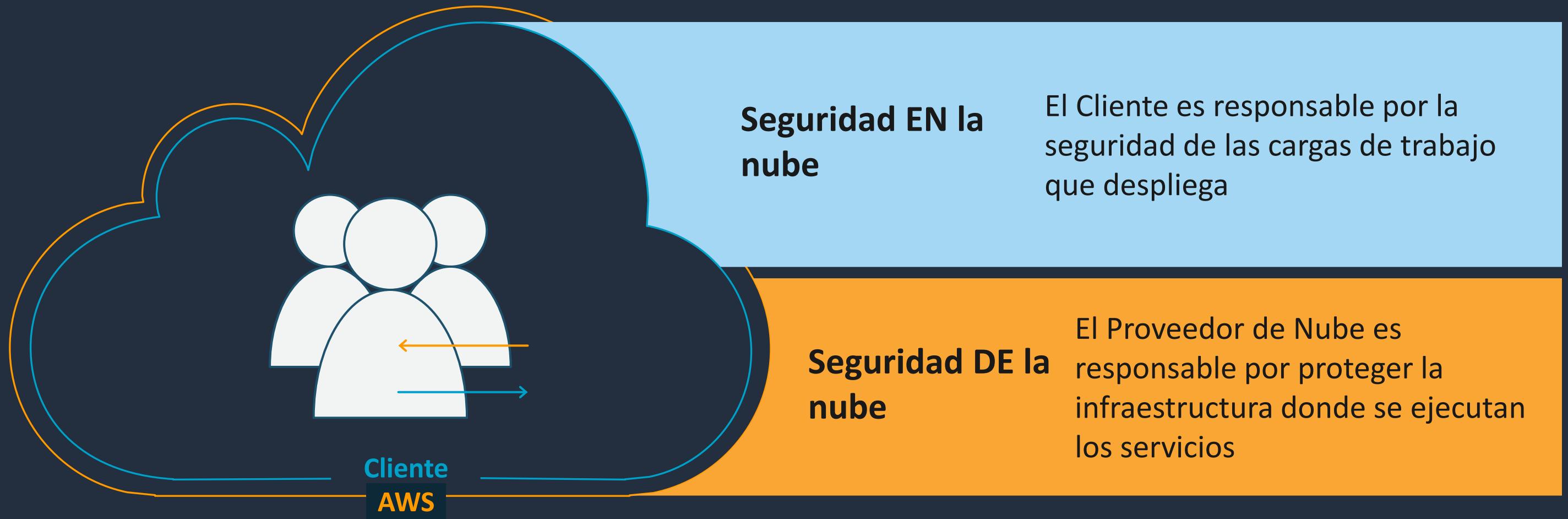
Demitificado



Hay mas transformación al
moverse a la nube que esto ...



Modelo de Responsabilidad Compartida

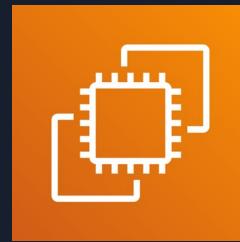


En la nube **no estás solo** defendiendo la seguridad de tus datos y aplicaciones

Modelo de responsabilidad compartida

Tipos de servicios

Servicios de
infraestructura



Servicios encapsulados
o gestionados

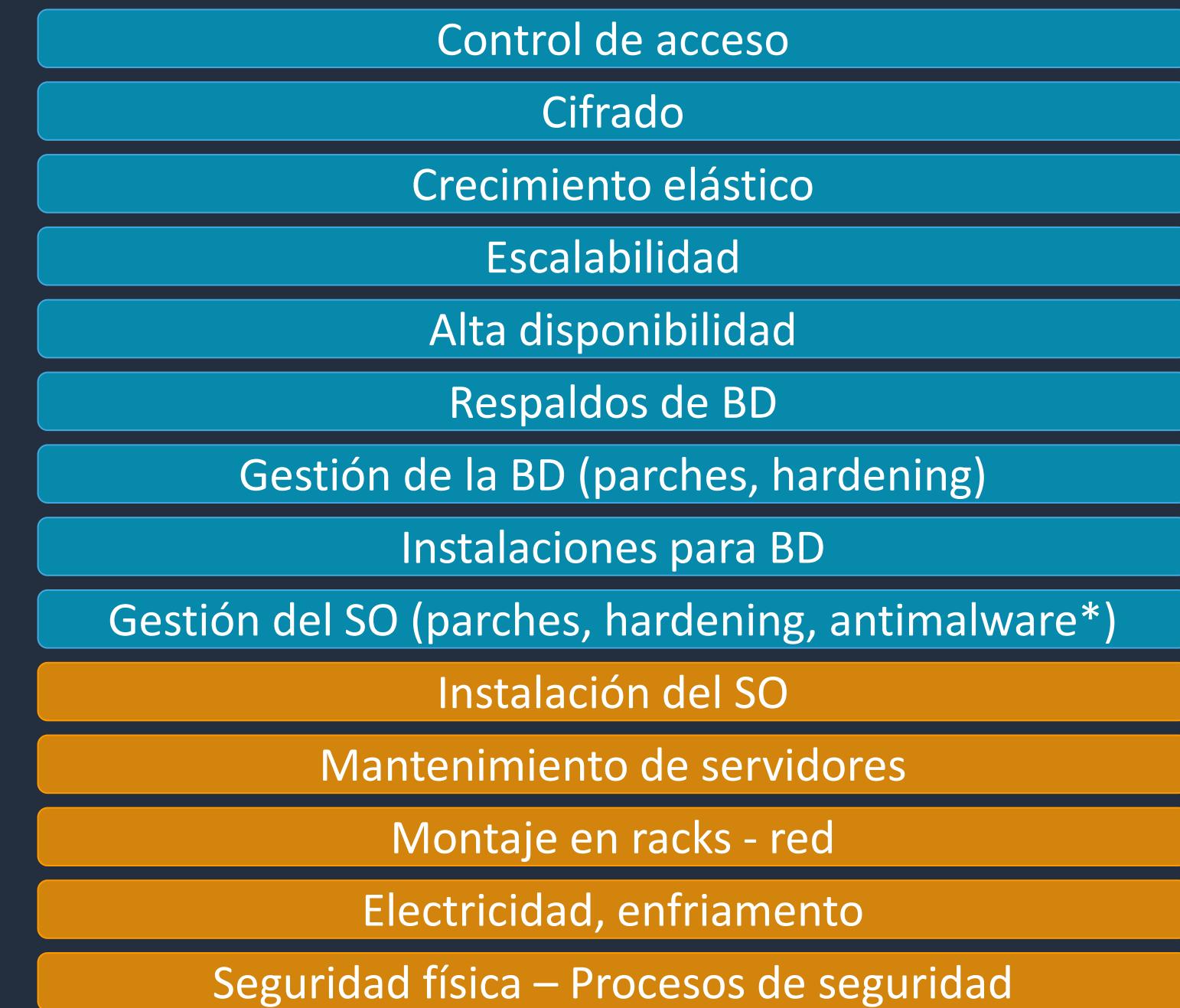


Servicios abstractos



Modelo de responsabilidad compartida

Ejemplo: bases de datos



Modelo de responsabilidad compartida

Ejemplo: bases de datos



Modelo de responsabilidad compartida

Ejemplo: bases de datos



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, enfriamiento
Seguridad física – Procesos de seguridad



Mito Nro. 2

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

Demitificado



Seguridad de la nube

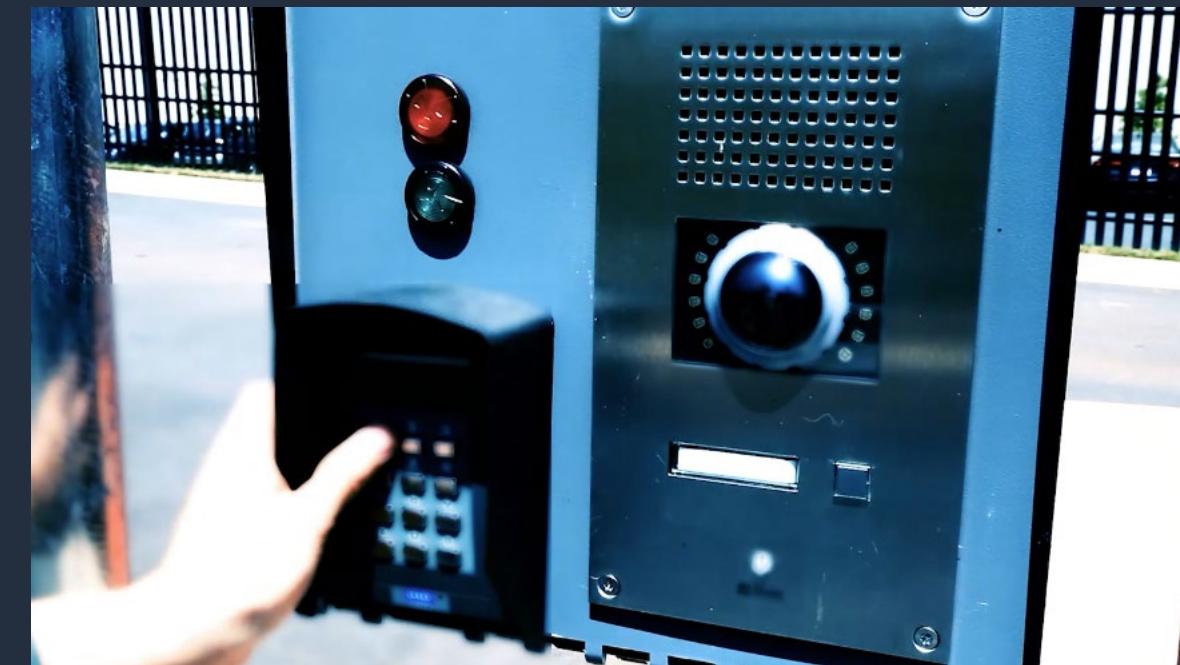
¿Cómo AWS hace su parte?



Protección del perímetro



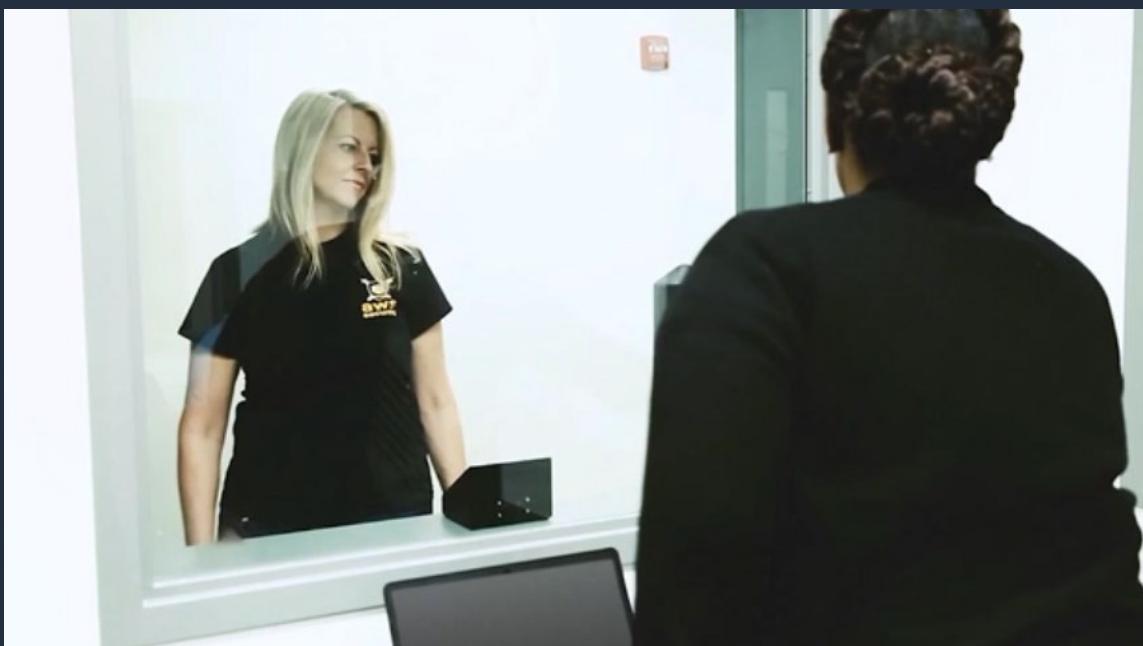
Protección del perímetro



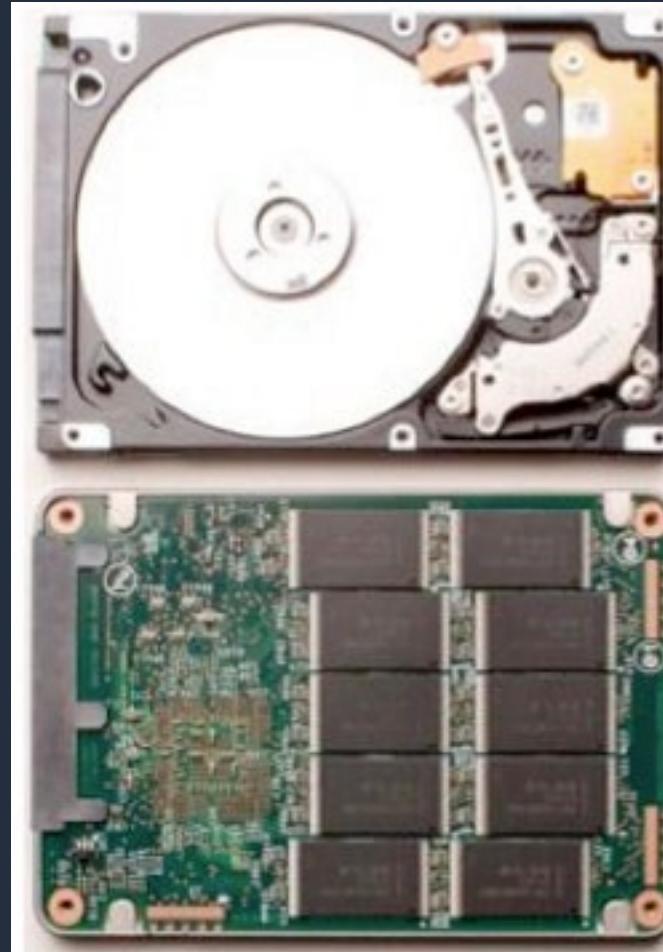
Protección del acceso a las salas del datacenter



Protección del acceso a las salas del datacenter



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

Mito Nro. 3

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

Demitificado



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



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

+143

certificaciones y
acreditaciones
de seguridad
y conformidad

+2600

controles de
seguridad
auditados
anualmente

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

© 2021, Amazon Web Services, Inc. or its Affiliates.

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



Informes de cumplimiento regulatorio: AWS Artifact



AWS Services ▾ Search for services, features, marketplace products, and docs [Option+S] Admin/goldfarb-lsengard @ securitypoc ▾ Global ▾ Support ▾

Reports (72) Search reports

Title Reporting period Category Description

Service Organization Controls (SOC) 2 Report - Current	April 1, 2020 to September 30, 2020	Certifications and Attestations	The AWS SOC 2 Type 2 report evaluates the AWS controls that meet the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants (AICPA) TSP section 100, Trust Services Principles and Criteria. This is our most recent SOC 2 report. SOC reports are audits performed over a period of time and do not expire. Our auditors perform our SOC audits twice a year over a period of 6 months – Oct 1-Mar 31 and Apr 1-Sept 30. Once the audit period is over, our auditors prepare their audit report which is then released in May and November, respectively. Should you seek assurance that we have maintained the control environment described in this most recent SOC report, we make a SOC Continued Operations Letter available to you in Artifact. Scroll down to the bottom of the page to download it.
PCI DSS Attestation of Compliance (AOC) and Responsibility Summary-Previous	June 22, 2020 to June 21, 2021	Certifications and Attestations	This is the previous AWS PCI assessment package dated December 13, 2019. It is available for AWS customers with a card data environment (CDE) that stores, transmits, or processes cardholder data in the AWS Cloud. An external Qualified Security Assessor Company (QSAC), Coalfire Systems Inc. has validated that AWS has successfully completed PCI Data Security Standards 3.2.1 Level 1 Service Provider assessment and were found to be compliant.
PCI 3DS Attestation of Compliance (AOC) and Responsibility Summary – Previous	June 8, 2020 to June 7, 2021	Certifications and Attestations	This is the previous AWS PCI 3DS assessment package dated June 8, 2020. An external Qualified Security Assessor Company (QSAC), Coalfire Systems Inc. has validated that AWS has successfully completed PCI 3DS Core Security Standard v1.0 assessment and were found to be compliant.
FedRAMP Customer Package	September 14, 2020 to current	Certifications and Attestations	The AWS FedRAMP Customer Package is intended for use by customers when building applications and solutions on AWS that need to pursue a FedRAMP assessment and accreditation. It is also useful for customers assessing AWS against the NIST 800-53, FedRAMP, or DoD SRG requirements. The documents available in this package include: AWS East/West and GovCloud Executive Briefing, Control Implementation Summary (CIS), Customer Responsibility Matrix (CRM), E-Authentication, FIPS-199 Categorization, Privacy

Copy link Download report

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72

Report navigation icons: back, forward, search, refresh, settings, help.

AWS Compliance Center

AWS Compliance Center Overview

Search Country / Region

Filter by

Clear all filters

Location

Asia Pacific

Europe, Middle East, & Africa

Latin America

North America

1-6 (6)

Sort by:

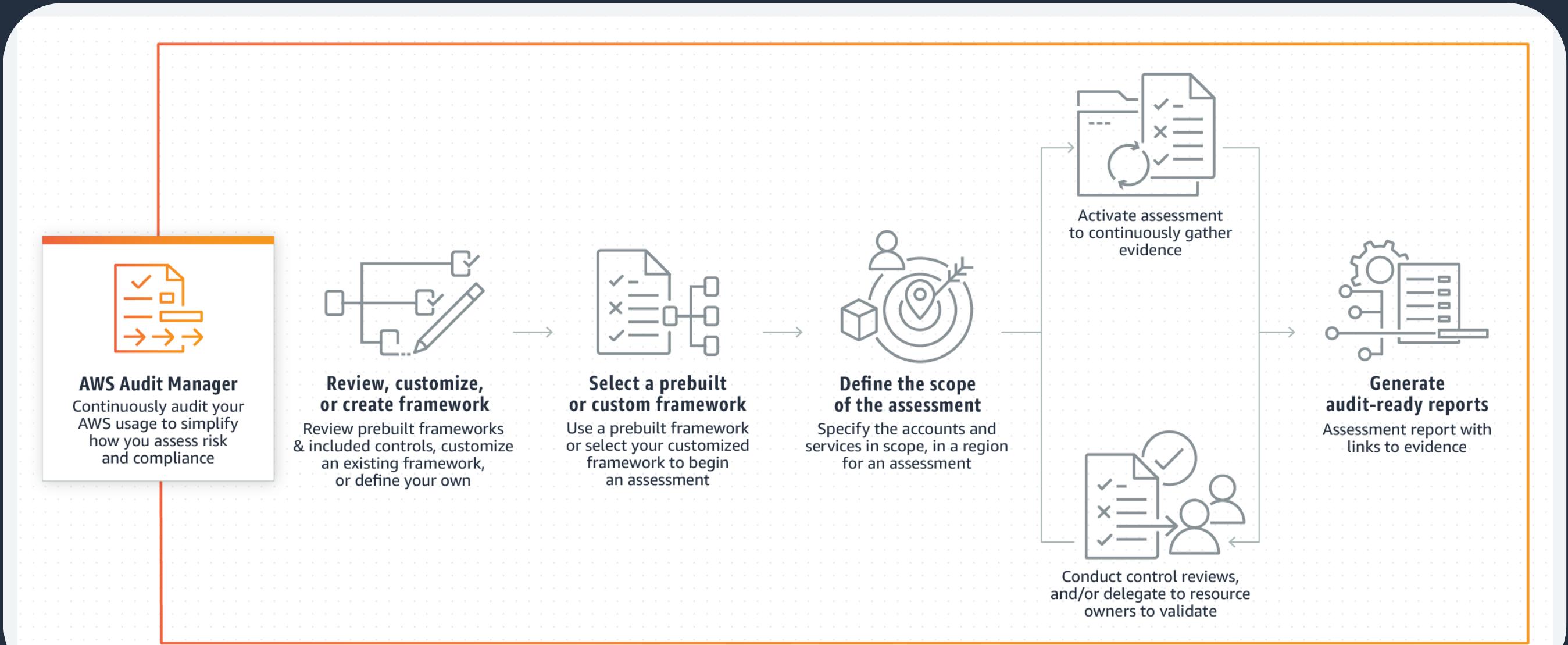
Name ▾

CLOUD USE PERMITTED	CLOUD USE PERMITTED	CLOUD USE PERMITTED
 Argentina <p>The Banco Central de la República Argentina, or "BCRA" (Central Bank of Argentina), is the primary financial supervisory authority in Argentina responsible for the regulation, inspection and supervision of financial institutions, including banking and credit institutions and payments processors.</p> <p>The Comisión Nacional de Valores, or "CNV" (National Securities Exchange Commission), regulates the Argentinean capital markets, including</p> <p>Last updated July 2020</p>	 Brazil <p>The Banco Central do Brasil or "BCB" (Brazil Central Bank) is the principal monetary authority and banking industry regulator.</p> <p>The Comissão de Valores Mobiliários or "CVM" (Securities and Exchange Commission of Brazil) is the securities market authority and regulates the capital markets and its participants.</p> <p>The Superintendência de Seguros Privados or "SUSEP" (Superintendent of Private Insurance) is the regulator for</p> <p>Last updated July 2020</p>	 Chile <p>The Superintendencia de Bancos e Instituciones Financieras or "SBIF" (Superintendence of Banks and Financial Institutions of Chile) and Banco Central de Chile (Central Bank of Chile) are the primary financial supervisory authority for banks, credit institutions, debit and credit card issuers, and payment processors.</p> <p>The Comisión para el Mercado Financiero or "CMF" (Financial Markets Commission) supervises stocks, brokers, listed corporations, and investment</p> <p>Last updated April 2019</p>
CLOUD USE PERMITTED	CLOUD USE PERMITTED	CLOUD USE PERMITTED
 Colombia	 Mexico	 Panama

Información específica 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

Mito Nro. 4

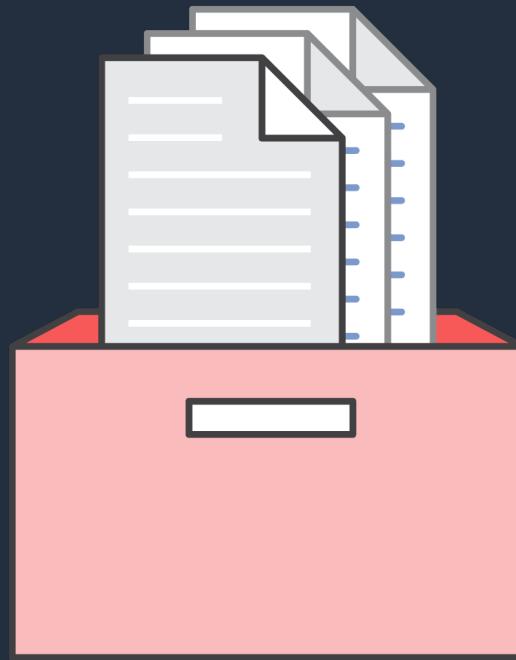
"Cuando ponga mis datos en la nube pierdo propiedad de ellos y podrían moverse a diferentes países"

Demitificado



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

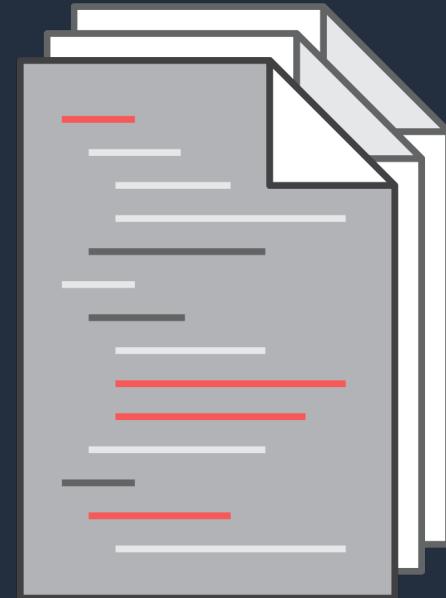
Propiedad



Acceso



Trazabilidad

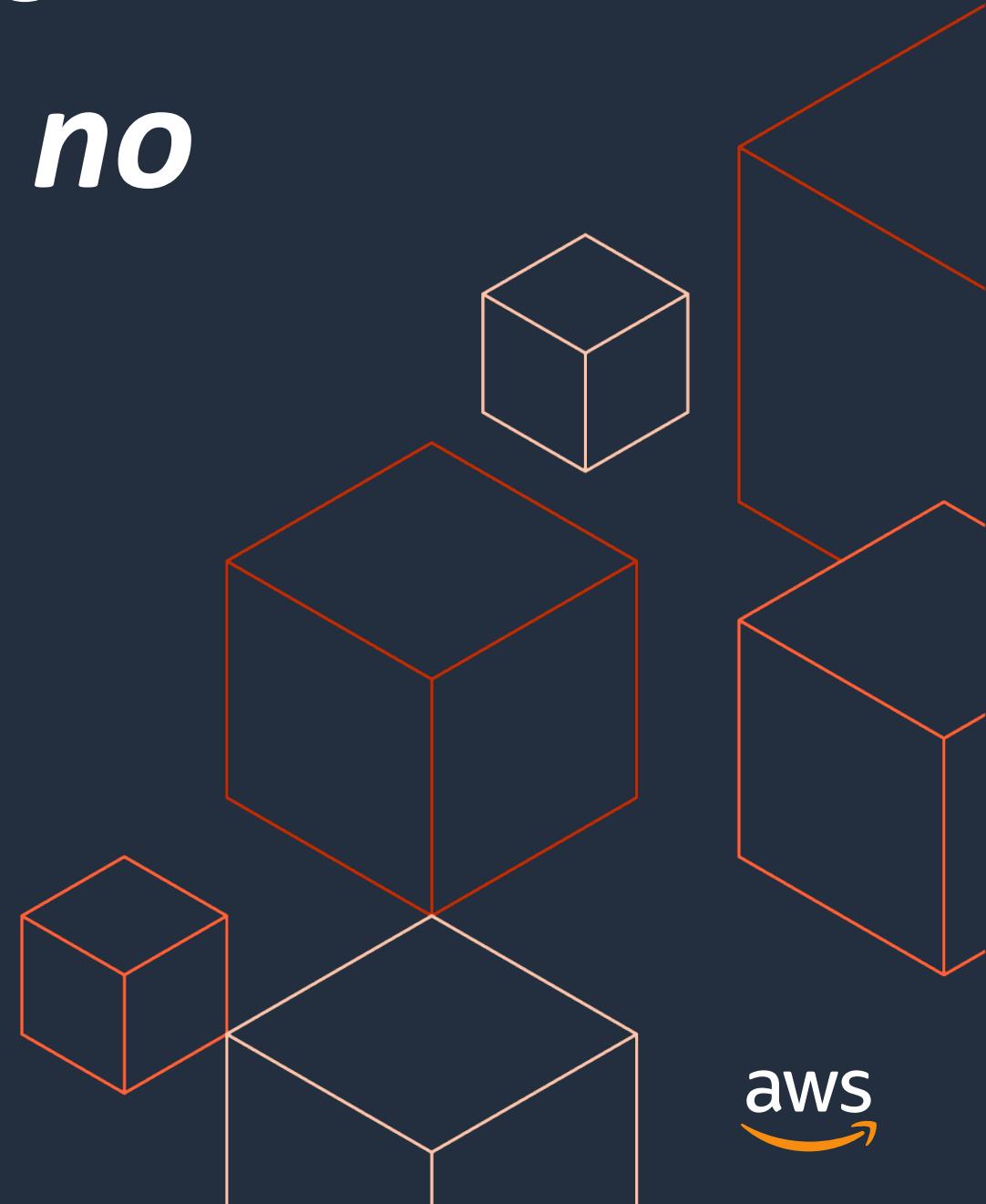


Usted conserva la propiedad y el control de su contenido, y elige en qué **región** reside el contenido.

Mito Nro. 5

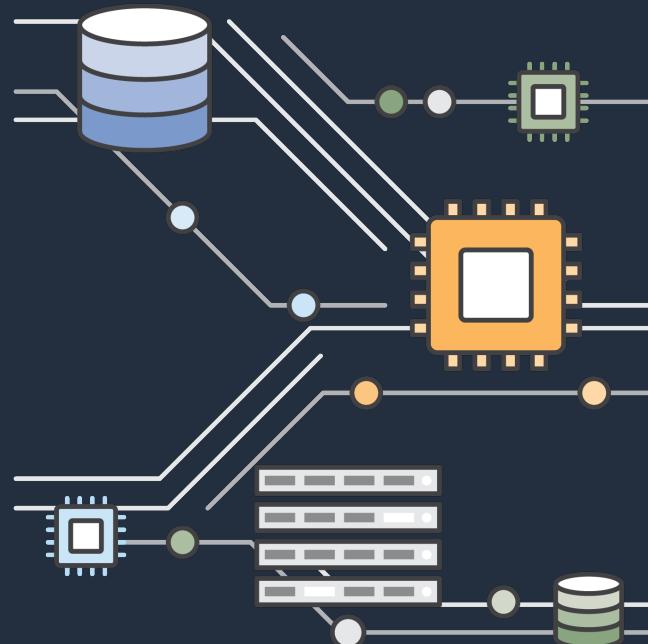
"Mi negocio requiere datos personales confidenciales, no puedo usar la nube"

Demitificado

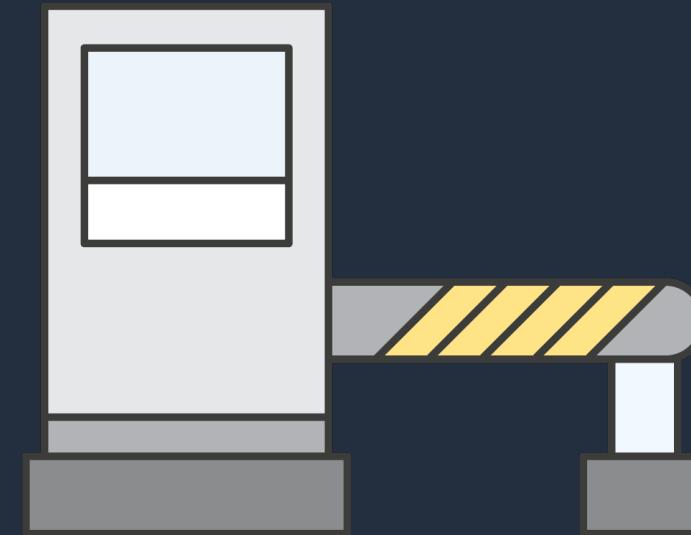


Protección del almacenamiento de objetos (Amazon S3)

S3 privado por defecto



Public Access Block



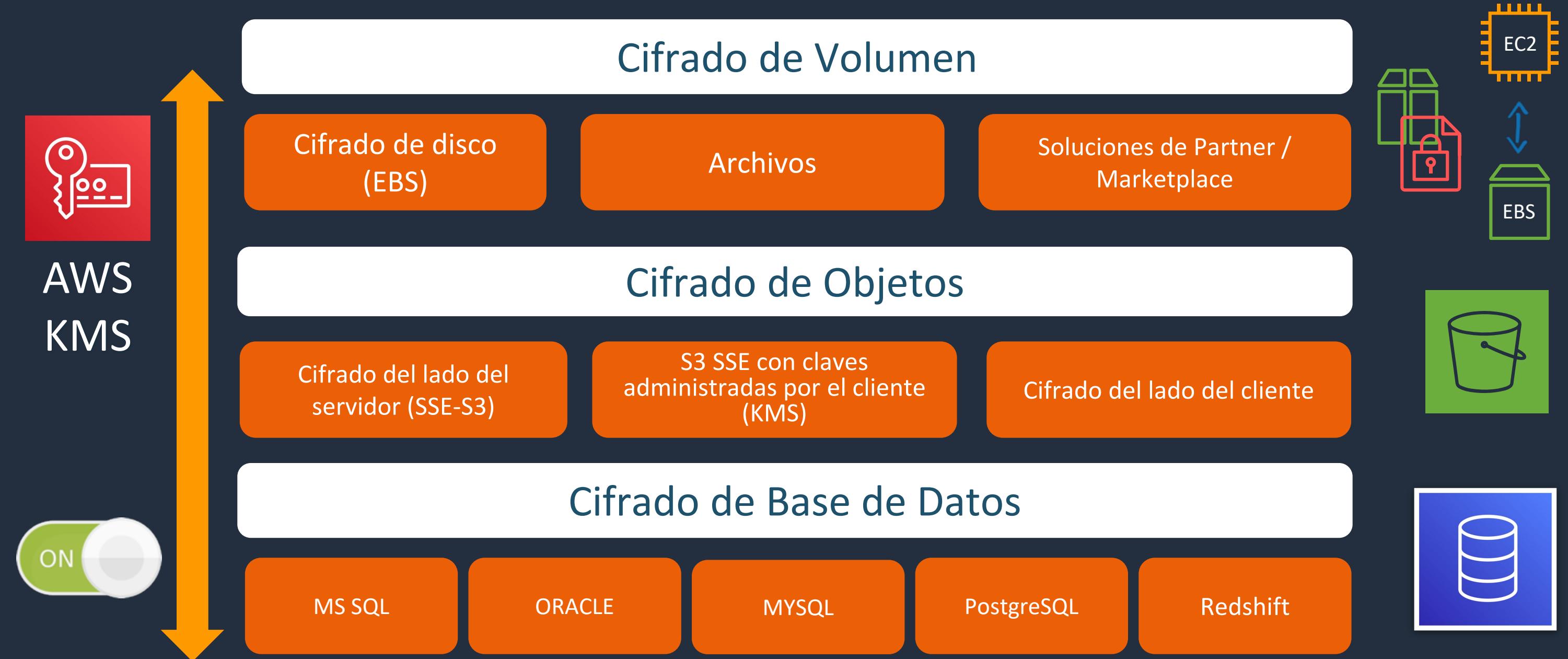
AWS KMS



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

Cifrado de extremo a extremo: En reposo

AWS Key Management Service (KMS) - CloudHSM



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 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



Mito Nro. 6

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

Demitificado



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

Block Public Access – Activado por defecto

The screenshot shows the AWS S3 console with the 'Block Public Access settings for this account' page open. The left sidebar includes links for Buckets, Access Points, Object Lambda Access Points, Batch Operations, Access analyzer for S3, and 'Block Public Access settings for this account' (which is highlighted in orange). The main content area displays the 'Block Public Access settings for this account' section, which contains a warning about updating settings affecting all buckets, a note about total buckets (3), and a 'confirm' input field. Two identical confirmation dialogs are shown on the right, one above the other, both prompting for confirmation with the word 'confirm' entered in the field.

AWS Services ▾ Search for services, features, markets [Option+S] admin/g Global Support

Amazon S3 X

Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3

Block Public Access settings for this account

Amazon S3 > Block Public Access settings for this account

Block Public Access settings for this account

Use Amazon S3 Block public access settings to control the settings that allow public access to your data.

Block Public Access settings for this account

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for all current and future buckets and access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

On

- Block public access to buckets and objects granted through **new** access control lists (ACLs)
On
- Block public access to buckets and objects granted through **any** access control lists (ACLs)
On
- Block public access to buckets and objects granted through **new** public bucket or access point policies
On
- Block public and cross-account access to buckets and objects through **any** public bucket or access point policies
On

Edit Block Public Access settings for this account

Updating the Block Public Access settings for this account affects all existing and new buckets in your account. This may result in some objects and buckets becoming public.
Total buckets in this account: 3

To confirm the settings, enter *confirm* in the field.

confirm

Cancel **Confirm**

Edit Block Public Access settings for this account

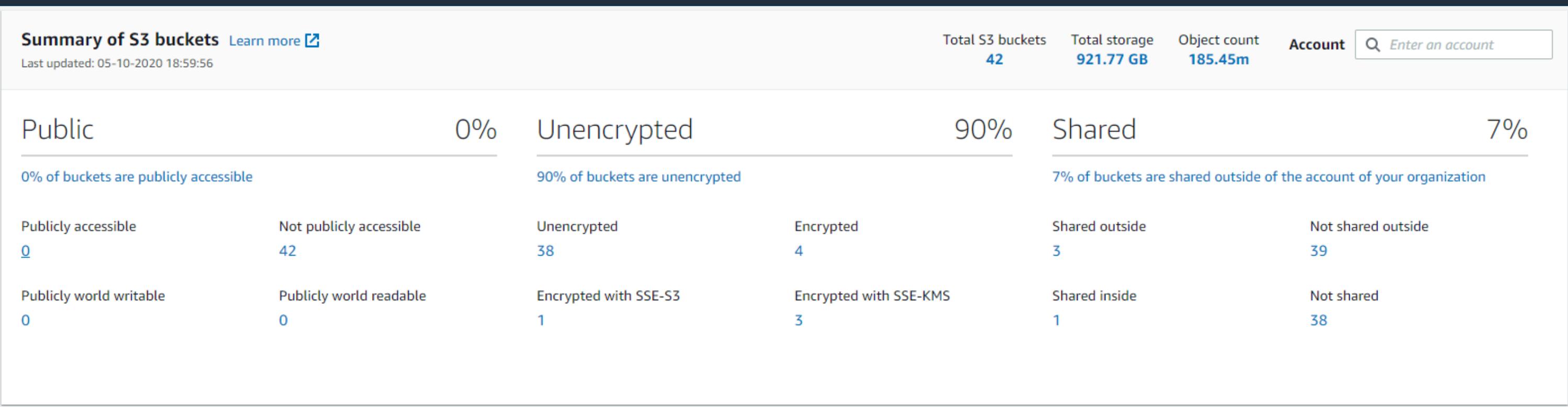
Updating the Block Public Access settings for this account affects all existing and new buckets in your account. This may result in some objects and buckets becoming public.
Total buckets in this account: 3

To confirm the settings, enter *confirm* in the field.

confirm

Cancel **Confirm**

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

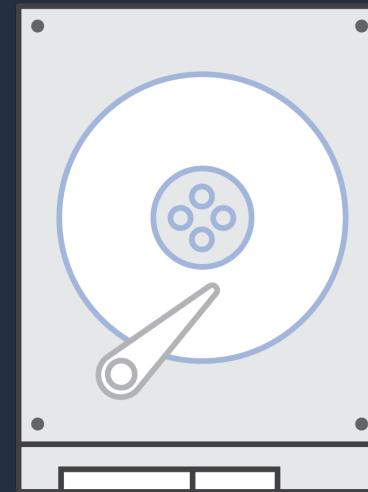


¿Cómo AWS maneja la eliminación segura de datos?

Eliminación Lógica



Eliminación Física

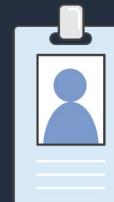


Proceso Auditado



- 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.

Servicios de seguridad gestionados

				
Identidades y Accesos	Controles de Detección	Seguridad en Infraestructura	Protección de Datos	Respuesta ante Incidentes
AWS Identity & Access Management (IAM) <small>Free</small>	AWS CloudTrail <small>Free Tier</small>	AWS Systems Manager <small>Free</small>	AWS Key Management Service (KMS) <small>Free Tier</small>	AWS Config Rules
AWS Organizations <small>Free</small>	AWS Security Hub <small>Free Trial</small>	AWS Shield <small>Free Tier (standard)</small>	AWS CloudHSM	AWS Lambda <small>Free Tier</small>
AWS Control Tower <small>Free</small>	AWS Config	AWS WAF	AWS Certificate Manager <small>Free Tier</small>	Amazon Detective <small>Free Trial</small>
AWS Cognito <small>Free Tier</small>	Amazon CloudWatch <small>Free Tier</small>	AWS Firewall Manager	Amazon Macie <small>Free Tier Free Trial</small>	AWS Step Functions <small>Free Tier</small>
AWS Directory Service <small>Free Trial</small>	Amazon GuardDuty <small>Free Trial</small>	AWS Network Firewall	Server-Side Encryption <small>Free</small>	AWS CloudEndure DR
AWS IAM Identity Center <small>Free</small>	VPC Flow Logs	Amazon Inspector <small>Free Trial</small>	S3 Block Public Access <small>Free</small>	AWS Backup
AWS Secrets Manager <small>Free Trial</small>	Traffic Mirroring	Amazon Virtual Private Cloud (VPC)		AWS SSM Automations
IAM Access Analyzer <small>Free</small>	Trusted Advisor <small>Free</small>	EC2 Image Builder <small>Free</small>	AWS Artifact <small>Free</small>	AWS Audit Manager <small>Free Trial</small>

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

© 2021, Amazon Web Services, Inc. or its Affiliates.

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





¡ Gracias !

¿ Preguntas ?

Dario Goldfarb

goldfarb@amazon.com

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

@dario_goldfarb

