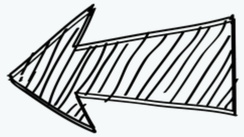
Cloud Computing - AWS

ACADEMIA CONSULTEC

Presentado por **Alejandro Chacón**
www.consultec-ti.com

Agenda

- Intro
- Almacenamiento S3



- Networking
- Cómputo y Almacenamiento
- Integración y Monitoreo
- Bases de Datos
- Seguridad
- Despliegues y Gestión de Infraestructura

ACADEMIA CONSULTEC

AWS Ecosistema

Well Architected y los 6 Pilares

ACADEMIA CONSULTEC

AWS Ecosistema

Infraestructura Global

- AWS Regions
- AWS Zonas de Disponibilidad
- AWS Centro de Datos
- AWS Edge Locations
  - Puntos de Presencia

ACADEMIA CONSULTEC

AWS Ecosistema

Comparativa de servicios en nubes públicas

Service	AWS	Azure	GCP
Compute	Amazon EC2, AWS Lambda, Amazon ECS, AWS Fargate	Azure Virtual Machines, Azure Functions, Azure Kubernetes Service (AKS)	Google Compute Engine, Cloud Functions, Google Kubernetes Engine (GKE)
Storage	Amazon S3, Amazon EBS, Amazon Glacier, Amazon Elastic File System (EFS)	Azure Blob Storage, Azure Files, Azure Disk Storage	Google Cloud Storage, Cloud SQL, Cloud Spanner
Database	Amazon RDS, Amazon DynamoDB, Amazon Redshift, Amazon Neptune	Azure SQL Database, Azure Cosmos DB, Azure Database for PostgreSQL, Azure Database for MySQL	Google Cloud SQL, Cloud Spanner, Cloud Bigtable
Networking	Amazon VPC, Amazon Route 53, Elastic Load Balancing (ELB), AWS Direct Connect	Azure Virtual Network, Azure DNS, Azure Load Balancer, Azure ExpressRoute	Google Virtual Private Cloud (VPC), Cloud DNS, Cloud Load Balancing, Cloud Interconnect
Analytics	Amazon EMR, Amazon Kinesis, Amazon Redshift, AWS Glue	Azure HDInsight, Azure Stream Analytics, Azure Data Factory, Azure Databricks	Google Cloud Dataproc, Cloud Dataflow, BigQuery
Security	AWS Identity and Access Management (IAM), Amazon Inspector, Amazon GuardDuty, AWS WAF	Azure Active Directory (AD), Azure Security Center, Azure Sentinel, Azure Firewall	Google Cloud Identity and Access Management (IAM), Cloud Security Command Center, Cloud Armor

ACADEMIA CONSULTEC

AWS S3

- Intro
- Generalidades
- Seguridad
- Versionado
- Durabilidad y Disponibilidad
- Clases de almacenamiento
- Encriptado

ACADEMIA CONSULTEC

AWS Simple Storage Service
Introduccion

- Es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector. Los clientes de todos los tamaños y sectores pueden utilizar Amazon S3 para almacenar y proteger cualquier cantidad de datos para diversos casos de uso, tales como lagos de datos, sitios web, aplicaciones móviles, copia de seguridad y restauración, archivado, aplicaciones empresariales, dispositivos IoT y análisis de big data. Amazon S3 proporciona funciones de gestión para que pueda optimizar, organizar y configurar el acceso a sus datos para satisfacer sus requisitos empresariales, organizativos y de conformidad específicos.

ACADEMIA CONSULTEC

AWS Simple Storage Service
Casos de Uso

- Respaldos
- Recuperación ante desastres
- Almacenamiento en la nube híbrido
- hosting web / web estaticas
- hosting de contenido digital (media)
- Lagos de Datos (Data Analytics)
- entrega de software y mucho más.

Nasdaq

Nasdaq stores 7 years of data into S3 Glacier

Sysco®

Sysco runs analytics on its data and gain business insights

ACADEMIA CONSULTEC

AWS Simple Storage Service
Buckets

- Almacenamiento de Objetos en “Buckets” (Directorios)
- deben tener un único nombre “Global”
- se presenta como un servicio global, pero los buckets están definidos a nivel de regiones (us-east-1)
- convención de nombres:
  - sin mayusculas y underscore
  - 3-63 long de caracteres
  - no puede ser IP
  - Debe comenzar en mayúscula o números.
  - no debe comenzar con el prefijo xn–
  - no debe terminar con el sufijo -s3alias

S3 Bucket

ACADEMIA CONSULTEC

AWS Simple Storage Service
Objectos

- Los objetos son como archivos, tienen una llave para identificarlas.
- una llave (key) es una ruta completa (path):
  - s3://academia-ctec/archivo.txt
  - s3://academia-ctec/carpeta01/carpeta0101/archivo.txt
- Una llave está compuesta de un prefijo + nombre de objeto.
  - s3://academica-ctec/carpeta01/carpeta0101/archivo.txt
- No existen conceptos de directorios dentro de los buckets (Web console te hará pensar lo contrario!)
- son solo llaves con nombres extensos que contienen slashes (“/”)

S3 Bucket
with Objects

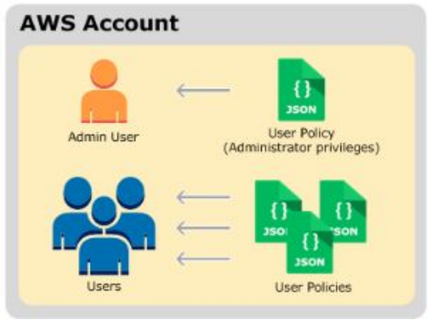
ACADEMIA CONSULTEC

AWS Simple Storage Service
Objectos+

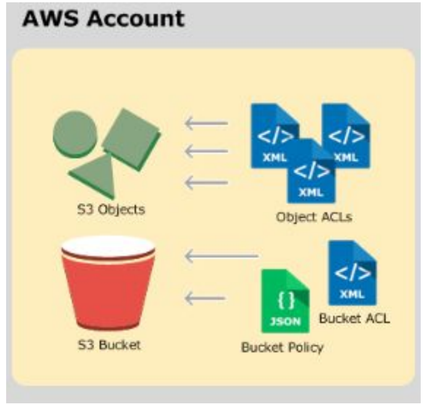
- Contenido del cuerpo del objeto:
  - Max es 5TB (5000GB)
  - si subimos mas de 5GB, debemos usar subida “multi-parte”
- Metadata (lista de pares key/valor)
- tags (unicode key/valor - hasta 10, útiles para seguridad)
- version ID (si activamos el versionado)

S3 Bucket
with Objects

AWS Simple Storage Service
Seguridad



- Basado en el usuario
  - IAM policies - llamados a la API deben ser permitidos para un especifico usuario desde IAM
- Basado en el recurso
  - Bucket Policies - reglas desde la consola S3 - cross account
  - Object ACL - permisos granulares (puede ser deshabilitado)
  - Bucket ACL - menos usado!



Notas: un principal puede acceder a un objeto S3 si:

- si el permiso de usuario IAM lo permite o la política del recurso la permite

Encriptación: es posible usar llaves de encriptación.

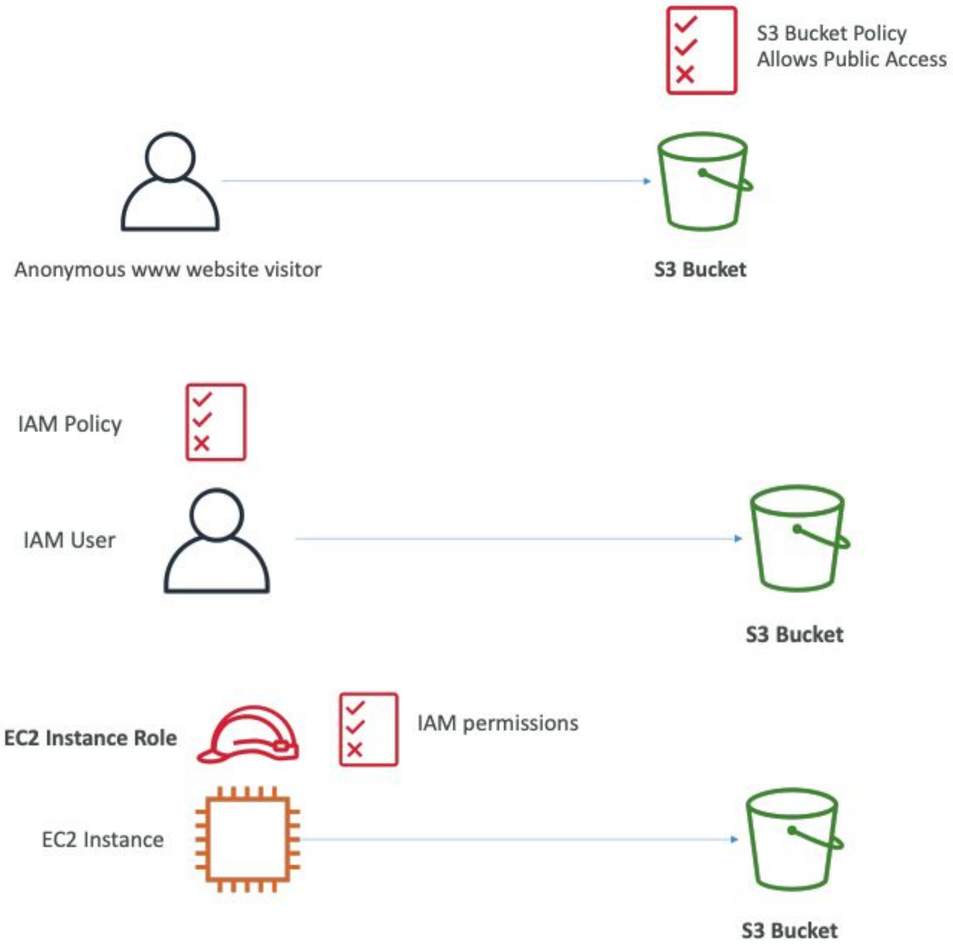
ACADEMIA CONSULTEC

AWS Simple Storage Service
Politicas en Buckets

- Políticas basadas en JSON:
  - recursos: buckets/objetos
  - efecto: Allow/Deny
  - Acciones: conjunto de API para permitir o denegar
  - Principal: la cuenta o usuario en aplicar la política.
- Politicas para S3:
  - ofrece acceso público al bucket
  - forza objetos a ser encriptados al subirlos
  - permite acceso hacia otras cuentas (CrossAccount)

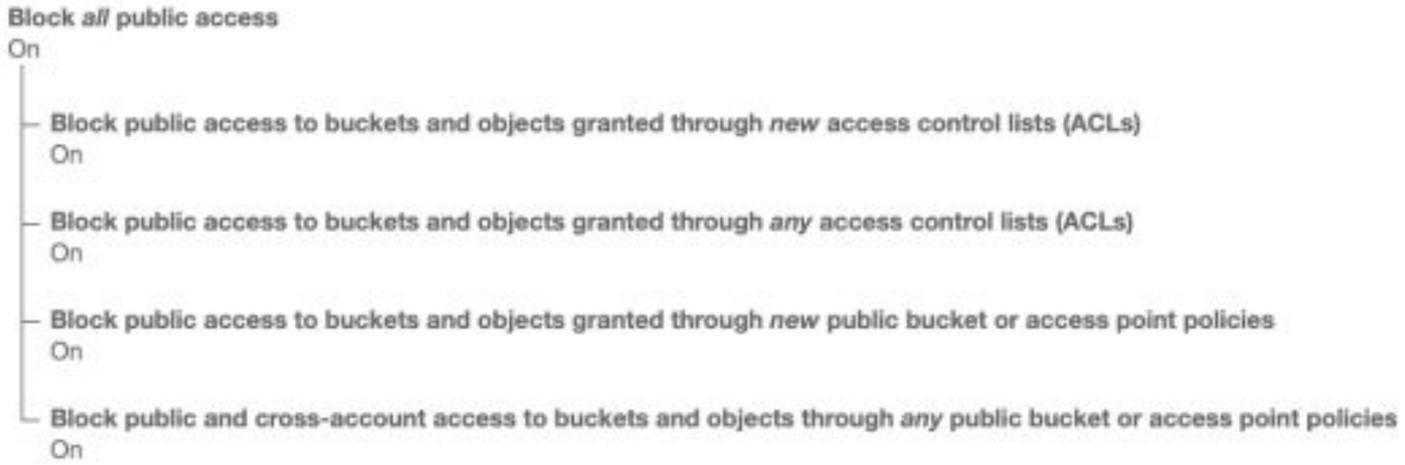
Ejemplos:

- politicas del bucket - public
- permisos desde IAM
- Roles IAM



ACADEMIA CONSULTEC

AWS Simple Storage Service
Politicas en Buckets - Block Public Access

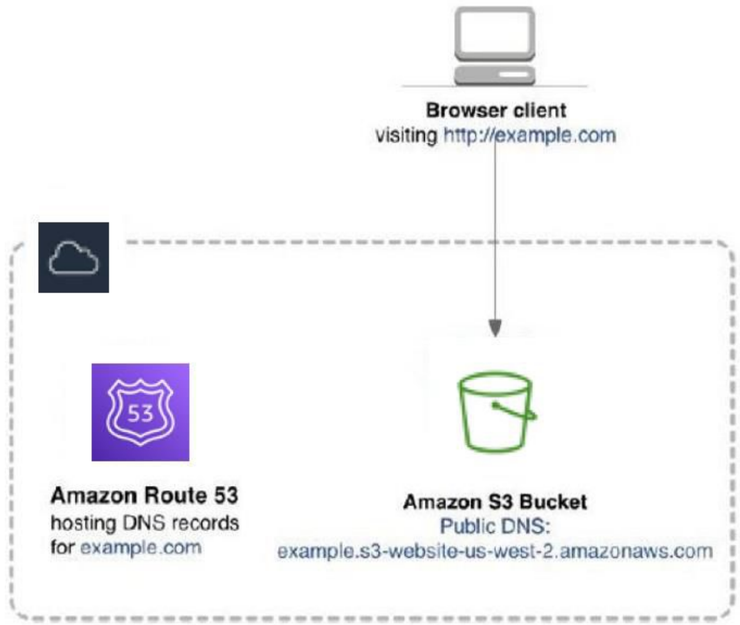


- Estas configuraciones fueron creadas para prevenir pérdida de datos en las compañías.
- esto puede ser configurado a nivel de cuentas AWS

ACADEMIA CONSULTEC

AWS Simple Storage Service
Static Web Hosting

- en S3 podemos alojar websites accesibles desde internet.
- La URL de la web dependerá de la región.
- Si obtenemos un error 403 (Forbidden), debemos asegurarnos de tener habilitado la lectura pública.



- **s3-website guion (-) región** - `http://bucket-name.s3-website-Region.amazonaws.com`
- **s3-web punto (.) Región** - `http://bucket-name.s3-website.Region.amazonaws.com`

ACADEMIA CONSULTEC

AWS Simple Storage Service
Versionado

- Podemos versionar archivos en S3
- Se habilitan a nivel de buckets
- es una buena práctica versionar los buckets
  - protege contra borrados sin intención, habilidad para hacer restore a una versión.
  - facil rollback a una version previa.

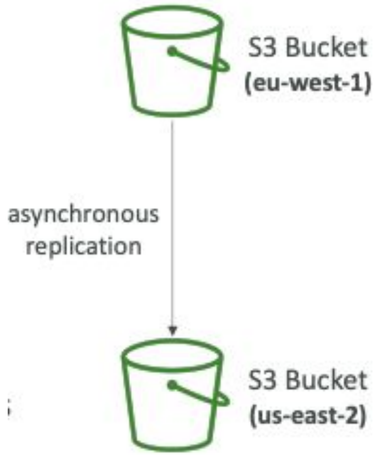
Notas:

- Suspender el versionado no borra las versiones previas
- cualquier archivo que no fue versionado antes de habilitar el versionado, se les asignará la versión: null.

ACADEMIA CONSULTEC

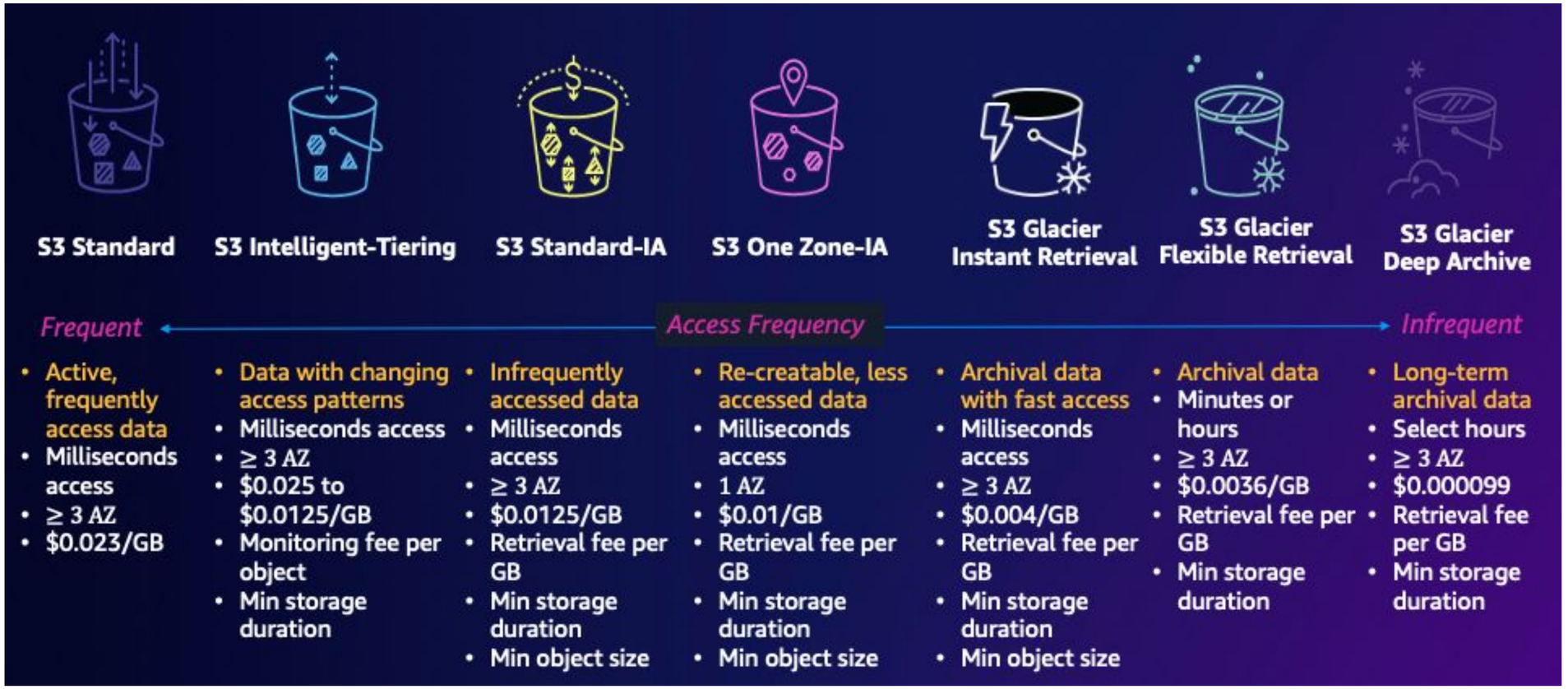
AWS Simple Storage Service
Replicaciones (CRR & SRR)

- Se debe habilitar el versionado en el bucket fuente y destino.
- Replicaciones:
  - Cross-Region (CRR)
  - Same-Region (SRR)
- los buckets pueden estar en diferentes cuentas AWS
- el copiado es asíncrono
- debemos tener los permisos S3 apropiados configurados.
- Casos de Uso:
  - CRR - compliance, baja latencia, replicación entre cuentas.
  - SRR - logs agregados, replicación en vivo entre cuentas productivas y de pruebas.



ACADEMIA CONSULTEC

AWS Simple Storage Service
Clases de Almacenamiento



- Amazon S3 Glacier Deep Archive
- Amazon S3 Intelligent Tiering

ACADEMIA CONSULTEC

AWS Simple Storage Service
Durabilidad y Disponibilidad

- Durability
  - Alta durabilidad (Once 9's) de objetos a través de múltiples AZ.
  - Si almacenas 10 millones de objetos en S3, podrías incurrir en la pérdida de un objeto una vez cada 10000 años.
  - Lo mismo aplica para todos las clases de almacenamiento.
- Availability
  - Se mide qué tan fácilmente el servicio se encuentra disponible.
  - varía dependiente de la clase de almacenamiento
  - Ejemplo: S3 Standard tiene 99.99% de disponibilidad

ACADEMIA CONSULTEC

AWS Simple Storage Service
Clases de Almacenamiento - Comparación

	Standard	Intelligent-Tiering	Standard-IA	One Zone-IA	Glacier Instant Retrieval	Glacier Flexible Retrieval	Glacier Deep Archive
Durability	99.999999999% == (11 9's)						
Availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.9%	99.9%
Availability Zones	>= 3	>= 3	>= 3	1	>= 3	>= 3	>= 3
Min. Storage Duration Charge	None	None	30 Days	30 Days	90 Days	90 Days	180 Days
Min. Billable Object Size	None	None	128 KB	128 KB	128 KB	40 KB	40 KB
Retrieval Fee	None	None	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved

ACADEMIA CONSULTEC

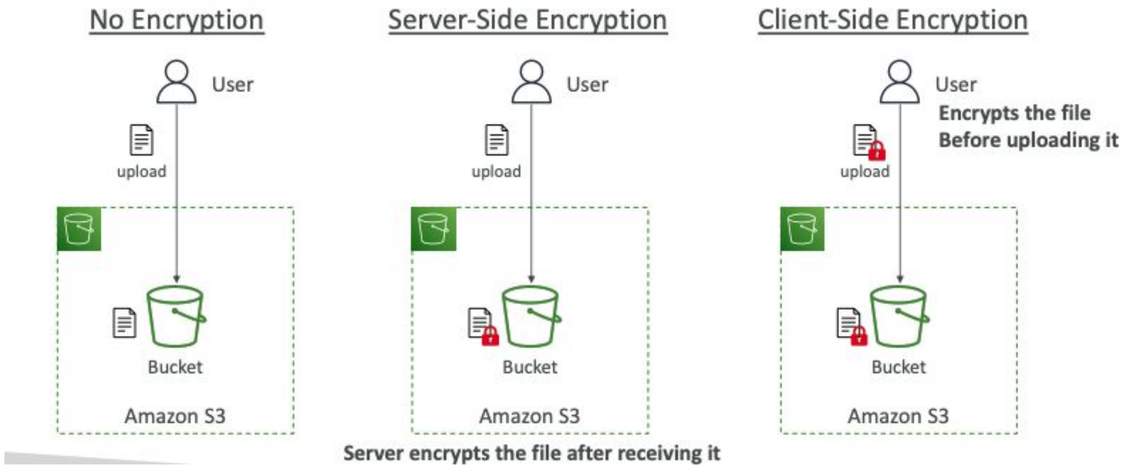
AWS Simple Storage Service
Clases de Almacenamiento - Costos

	Standard	Intelligent-Tiering	Standard-IA	One Zone-IA	Glacier Instant Retrieval	Glacier Flexible Retrieval	Glacier Deep Archive
Storage Cost (per GB per month)	$0.023	$0.0025 - $0.023	%0.0125	$0.01	$0.004	$0.0036	$0.00099
Retrieval Cost (per 1000 request)	**GET:** $0.0004 **POST:** $0.005	**GET:** $0.0004 **POST:** $0.005	**GET:** $0.001 **POST:** $0.01	**GET:** $0.001 **POST:** $0.01	**GET:** $0.01 **POST:** $0.02	**GET:** $0.0004 **POST:** $0.03 **Expedited:** $10 **Standard:** $0.05 **Bulk:** free	**GET:** $0.0004 **POST:** $0.05 **Standard:** $0.10 **Bulk:** $0.025
Retrieval Time	Instantaneous					**Expedited** (1 – 5 mins) **Standard** (3 – 5 hours) Bulk (5 – 12 hours)	**Standard** (12 hours) **Bulk** (48 hours)
Monitoring Cost (pet 1000 objects)		$0.0025					

ACADEMIA CONSULTEC

AWS Simple Storage Service
Encriptado

- Modelo de Responsabilidad Compartida
  - Versionamento S3
  - Politicas del Bucket
  - Configuración de Replicación
  - Logs y monitoreo
  - Clases de almacenamiento S3
  - Encriptación de datos “at rest” y en tránsito
- AWS nos provee:
  - Infraestructura (Seguridad Global)
  - Análisis de vulnerabilidades
  - Validaciones de complimientos de normas.



Ya Volvemos

Un pequeño descanso

Cloud Computing - AWS

ACADEMIA CONSULTEC

Contacto

achacon@consultec-ti.com

info@consultec-ti.com

@consulteclatam

@consultec-ti

consultec-ti.com

Gracias

¡Nos vemos pronto!