Servicios de encriptación y codificación en la nube

Los casos de Google Cloud Platform y Amazon Web Services

Presentación elaborada por Marcos Hidalgo Baños (GPC) y Alejandro Caro Casado (AWS)

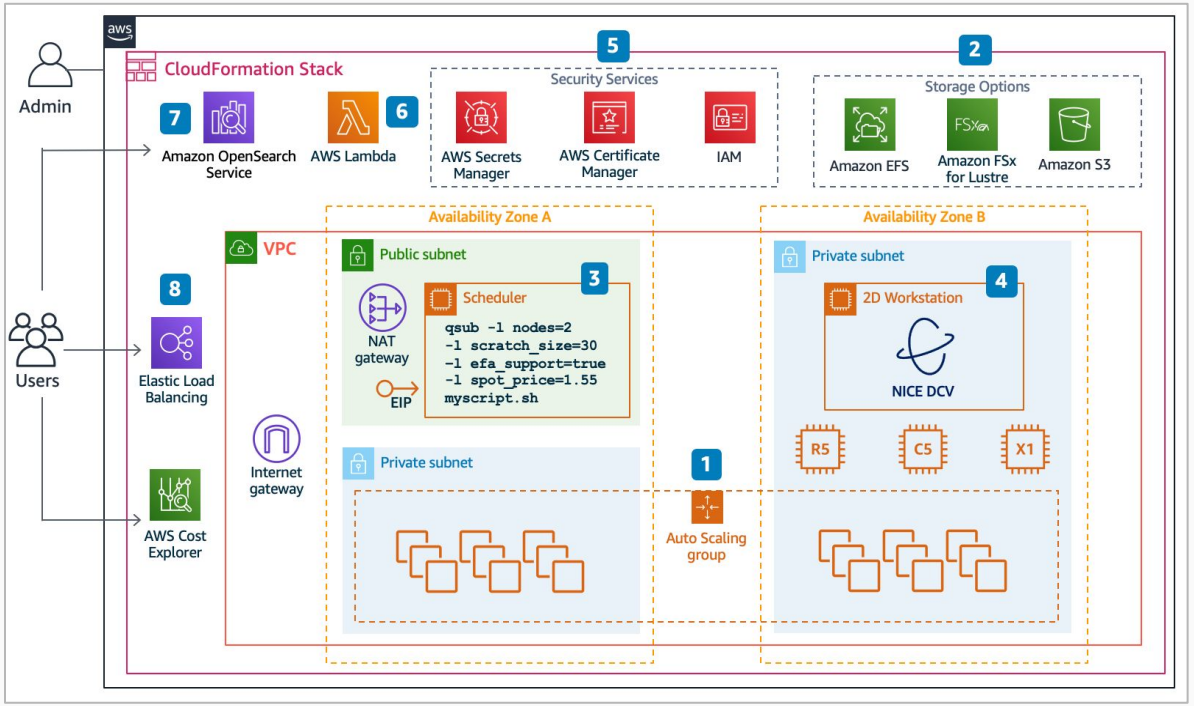
Conceptos de servicio y consola

Todo **proyecto** en la nube está compuesto por un determinado conjunto de **servicios**.

Cada servicio realiza una función concreta dentro del proyecto y deben ser independientes entre sí.

Los servicios son añadidos al proyectos mediante una **consola**, puede ser una interfaz gráfica o interfaz de línea de comandos.

Los dos servicios a presentar son Cloud Key Management Service y Amazon Redshift.



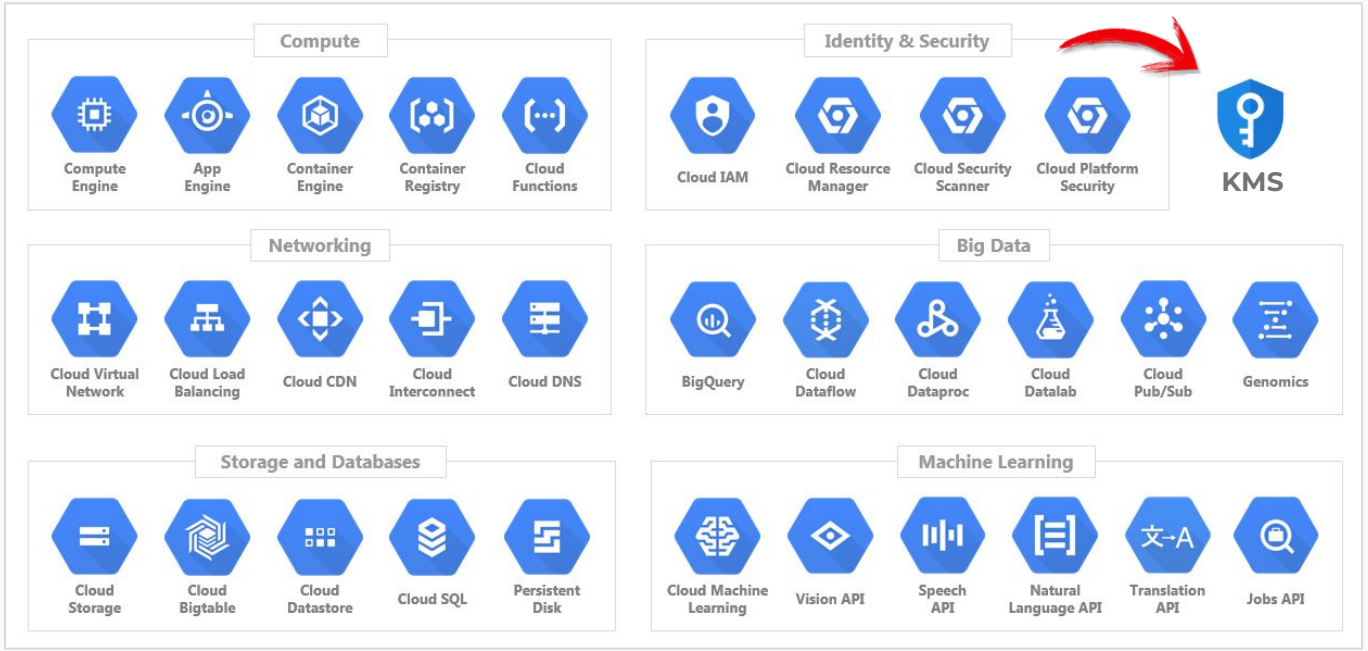
Ejemplo de un proyecto en la nube de AWS

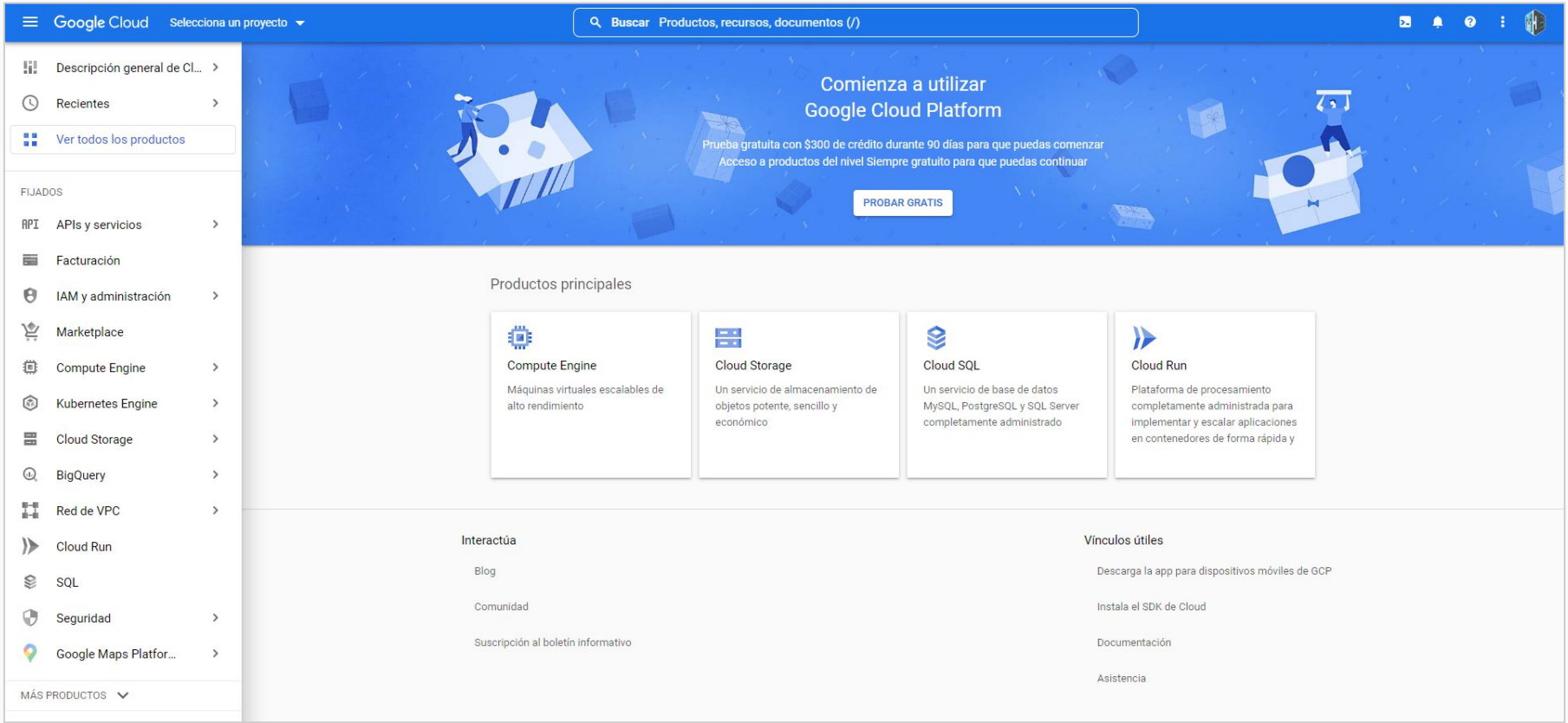
Google Cloud Platform - GCP

Cuadro resumen de las principales secciones de servicios por ámbito.

Notar que se muestran las más **representativas**, no siendo por lo tanto un listado exhaustivo.

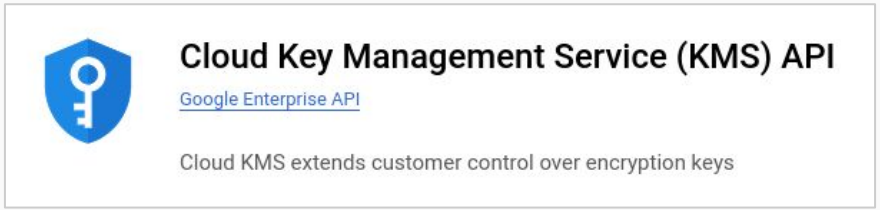
Centraremos nuestro estudio en KMS, el cual es uno de los principales servicios de Seguridad.





Enlace a la página que se muestra → console.cloud.google.com/getting-started

Servicios de encriptación de claves en la nube



"Google Cloud KMS permite a los clientes administrar claves de encriptación y realizar operaciones criptográficas con esas claves"

¿Qué tipos de claves existen en KMS?

RSA 2048	AES256
RSA 3072	EC P256
RSA 4096	EC P384

Simétricas y Asimétricas

¿Para qué se pueden usar las claves en KMS?

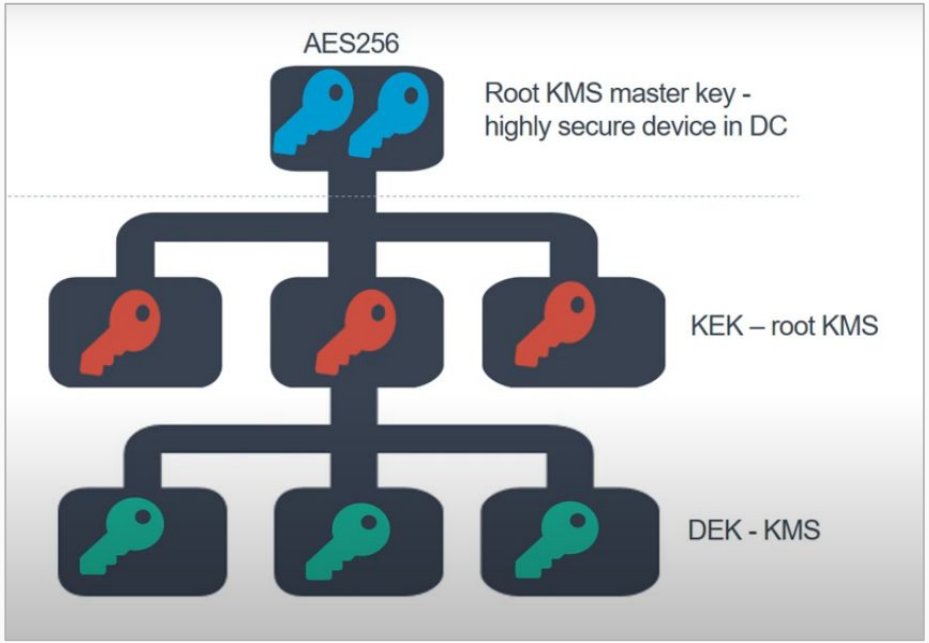
Se puede generar, usar, rotar y destruir toda clave que pertenezca a un **Keyring** (llavero), siendo agrupados según su región geográfica.

¿Hay otros servicios que extiendan a KMS?

Servicios como **EKM** (External Key Management) permiten que las claves se guarden en infraestructuras de terceros y no en los servidores de Google.

Servicios de encriptación de claves en la nube

Jerarquía de claves de encriptación por defecto en KMS.



Root KMS Master Key
Custodiadas de manera física en los centros seguros de Google, permiten desencriptar y utilizar las KEK. Extremadamente robustas y de acceso restringido.

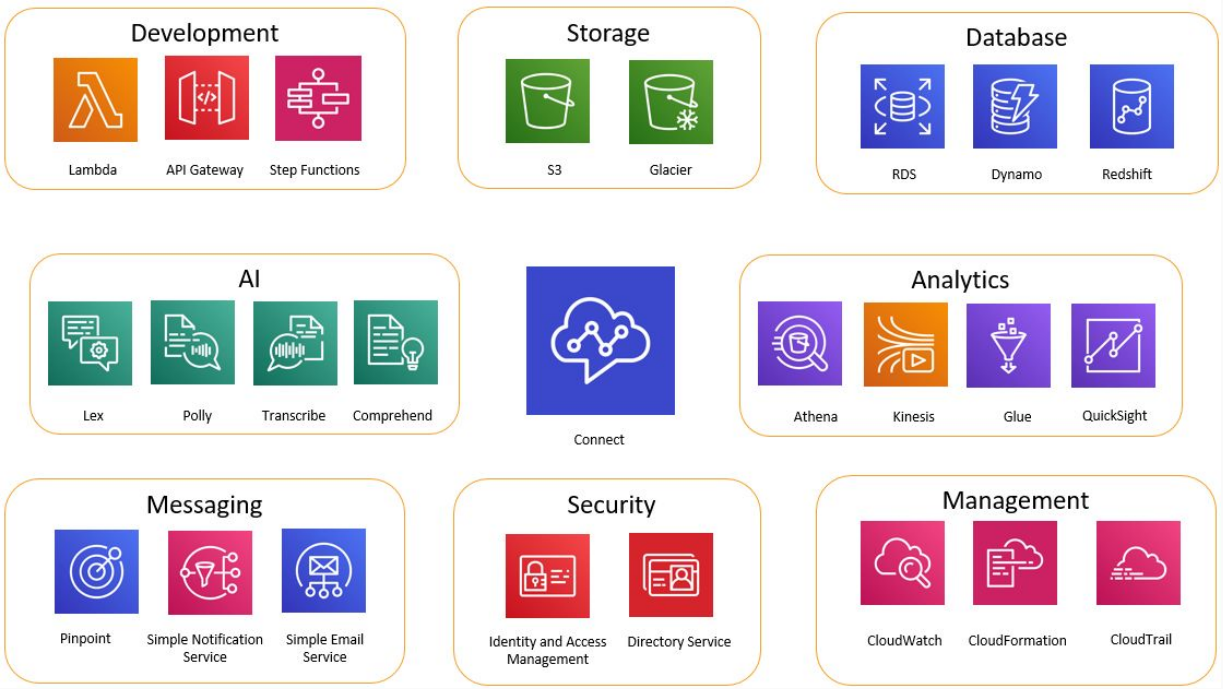
KEK - Key Encryption Key
Cada vez que el usuario quiere desencriptar una DEX para utilizarla, debe llamar al servicio KMS para que su KEK correspondiente la desenvuelva. También están controladas por el propio sistema de Google.

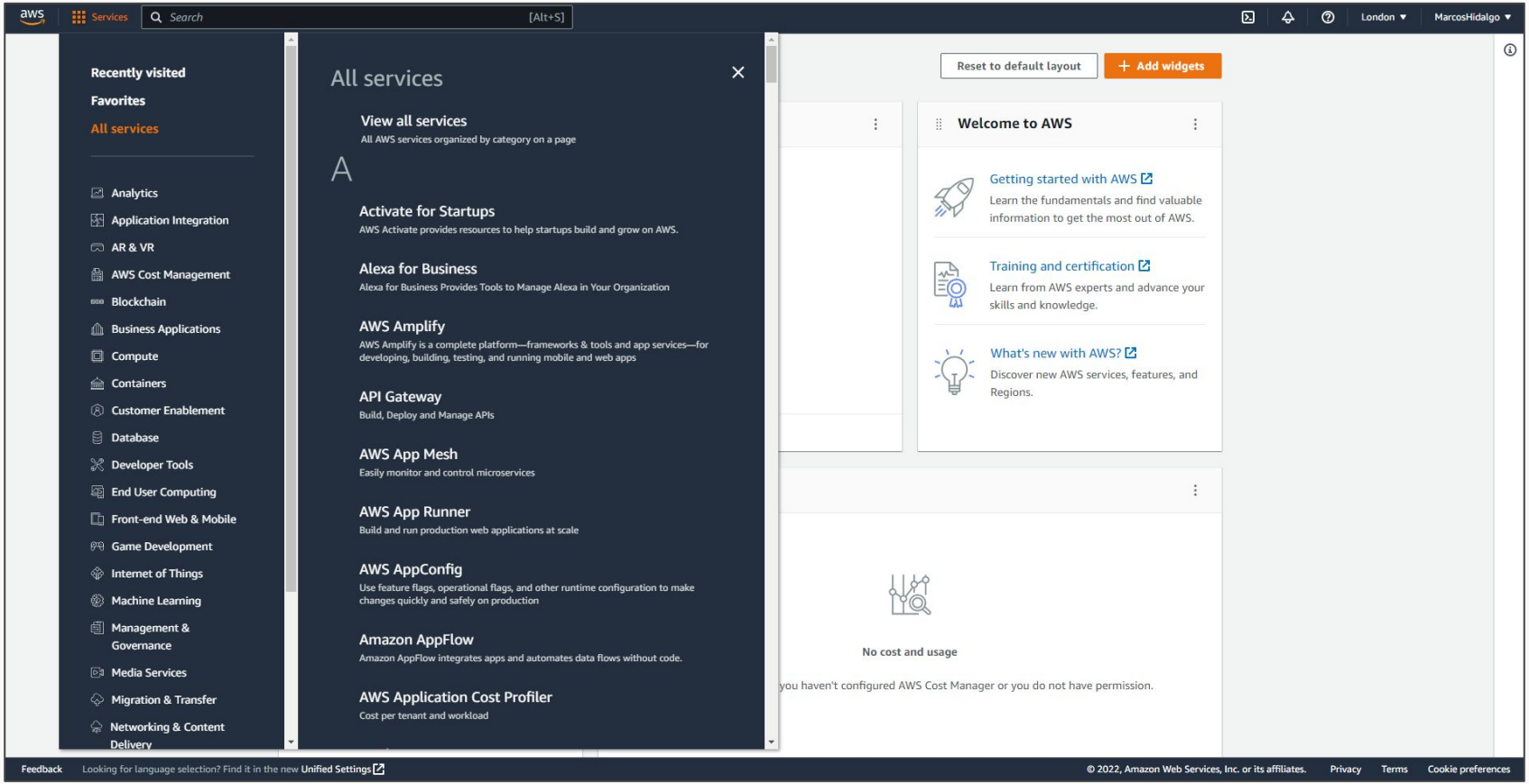
DEK - Data Encryption Key
Son las claves que el usuario usa en sus proyectos para encriptar los datos sensibles de su aplicación.

Amazon Web Services - AWS

Una pequeña imagen de los principales servicios que nos puede llegar a ofrecer AWS.

Nos centraremos en los servicios de Base de Datos, de donde destacaremos Redshift puesto que utiliza codificación para realizar sus operaciones.





Enlace a la página que se muestra → eu-west-2.console.aws.amazon.com/console

Servicios de codificación en bases de datos

"Amazon Redshift es un servicio de almacenamiento y análisis de datos que proporciona una base de datos altamente escalable que se utiliza para análisis de datos a gran escala. "

¿Qué tipos de codificación utiliza?

RAW	Diccionario de bytes	
AZ64	Delta	LZO
Mostly	Text255	Text32k
ZSTD	Run length	

¿Por qué codificamos los datos?

Redshift codifica las columnas para poder reducir el tamaño de los datos cuando se almacenen, aunque no todos los tipos de datos pueden ser codificados.

Servicios de codificación en bases de datos

Tipo de codificación	Tipos de datos
Raw (sin comprimir)	Todos
AZ64	SMALLINT, INTEGER, BIGINT, DECIMAL, DATE, TIMESTAMP, TIMESTAMPTZ
Diccionario de bytes	SMALLINT, INTEGER, BIGINT, DECIMAL, REAL, DOUBLE PRECISION, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ
Delta	SMALLINT, INT, BIGINT, DATE, TIMESTAMP, DECIMAL INT, BIGINT, DATE, TIMESTAMP, DECIMAL
LZO	SMALLINT, INTEGER, BIGINT, DECIMAL, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ, SUPER
Mostly*n*	SMALLINT, INT, BIGINT, DECIMAL INT, BIGINT, DECIMAL
Run-length	SMALLINT, INTEGER, BIGINT, DECIMAL, REAL, DOUBLE PRECISION, BOOLEAN, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ
Texto	Solo VARCHAR Solo VARCHAR
Zstandard	SMALLINT, INTEGER, BIGINT, DECIMAL, REAL, DOUBLE PRECISION, BOOLEAN, CHAR, VARCHAR, DATE, TIMESTAMP, TIMESTAMPTZ, SUPER

Codificación AZ64
Es un algoritmo codificado de compresión que se ha diseñado para lograr una alta relación de compresión y un procesamiento mejorado de las consultas. El algoritmo comprime grupos de valores de datos más pequeños.

Codificación por Texto
Son útiles para comprimir columnas VARCHAR en las que se repiten con frecuencia las mismas palabras. Se crea un diccionario independiente de palabras únicas para cada bloque de los valores de columna del disco

Codificación Delta
La codificación Delta comprime los datos al registrar la diferencia entre los valores que se suceden en la columna. Esta diferencia se registra en un diccionario independiente para cada bloque de valores de columnas del disco.

Conclusiones de la investigación

GENERALES.

La nube puede emplearse como herramienta en contextos muy diferentes.

Los servicios en la nube son similares independientemente del proveedor.

CONCRETAS.

La administración de datos sensibles en la nube es un asunto de seguridad que no tiene una solución general para todos los casos.

- KMS establece una jerarquía centralizada, pero habilita alternativas.
- Redshift nos ofrece tipos de codificación según el tipo de datos.

Referencias bibliográficas

- cloud.google.com/security-key-management
  cloud.google.com/docs/security/key-management-deep-dive
  Documentación oficial y raíz de otros artículos.
- youtube.com/watch?v=GDECKM9iW0w
  Vídeo sobre la arquitectura de KMS.
- docs.aws.amazon.com
  aws.amazon.com/es/what-is-aws
  docs.aws.amazon.com/es_es/redshift/latest/dg/welcome.html
  Documentación oficial de AWS y Redshift.