



Revista Logos Ciencia & Tecnología

ISSN: 2145-594X

ISSN: 2422-4200

Policía Nacional de Colombia

Cárdenas Sánchez, Brian Camilo; Olarte Rojas, Carlos Arturo
Análisis de seguridad entre microservicios con *Amazon Web Service*
Revista Logos Ciencia & Tecnología, vol. 14, núm. 2, 2022, Mayo-Agosto, pp. 42-52
Policía Nacional de Colombia

DOI: <https://doi.org/10.22335/rlct.v14i2.1546>

Disponible en: <https://www.redalyc.org/articulo.oa?id=517775405004>

- ▶ [Cómo citar el artículo](#)
- ▶ [Número completo](#)
- ▶ [Más información del artículo](#)
- ▶ [Página de la revista en redalyc.org](#)

UNAM redalyc.org

Sistema de Información Científica Redalyc
Red de Revistas Científicas de América Latina y el Caribe, España y Portugal
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso
abierto

Análisis de seguridad entre microservicios con Amazon Web Service

Amazon Web Service Microservice Security Analysis

Análise de segurança de microserviços da Amazon Web Service

Brian Camilo Cárdenas Sánchez^{a*} | Carlos Arturo Olarte Rojas^b

^a <https://orcid.org/0000-0003-2140-6715> Universidad Distrital Francisco José de Caldas, Bogotá D. C., Colombia

^b <https://orcid.org/0000-0002-8374-2821> Universidad Distrital Francisco José de Caldas, Bogotá D. C., Colombia

- Fecha de recepción: 2022-02-04
 - Fecha concepto de evaluación: 2022-05-04
 - Fecha de aprobación: 2022-05-09
- <https://doi.org/10.22335/rlct.v14i2.1546>

Para citar este artículo/To reference this article/Para citar este artigo: Cárdenas-Sánchez, B. C., & Olarte-Rojas, C. A. (2022). Análisis de seguridad entre microservicios con Amazon Web Service. *Revista Logos Ciencia & Tecnología*, 14(2), 42-52. <https://doi.org/10.22335/rlct.v14i2.1546>

RESUMEN

En las últimas décadas, el aumento en el uso de sistemas de información, de las comunicaciones y la posibilidad de compartir datos al instante, a través de Internet, han traído consigo términos como la ciberseguridad, ya que desde los inicios han existido personas inescrupulosas que desean obtener información confidencial; es por ello que cada año se desarrollan nuevos vectores de ataque y con ello nuevos métodos para persuadirlos. Actualmente, existe un auge creciente sobre tecnologías basadas en microservicios y en el *cloud computing*, esto debido a su alta escalabilidad, mantenibilidad y facilidad para crear infraestructuras de forma segura. *Amazon Web Service* (AWS) ofrece diversos servicios que permiten convertir plataformas sencillas en aplicaciones robustas, usando diferentes tecnologías y bases de datos, así como también permite agregar seguridad tanto a las aplicaciones como a los datos que son la fuente principal de todo sistema; por esta razón, se realiza una exploración a la encriptación de bases de datos y documentos, usando servicios de *Amazon Web Service* como *Key Management Service*, *Amazon Relational Database Service* y S3. En conclusión, en caso de que un ataque se materialice, las bases de datos y los archivos encriptados no pueden ser legibles por personas malintencionadas,

Palabras clave: Encriptación, cifrado, cibercrimen, seguridad de datos

ABSTRACT

The increase in the use of information systems, of communications through the Internet in recent decades and the possibility of sharing data instantly have brought with them terms such as cybersecurity, since, from the beginning, there have been unscrupulous people who want to obtain confidential information, that is why new attack vectors are invented every year and with it new methods to persuade them, there is currently a growing boom on technologies based on microservices and cloud computing, this due to its high scalability, maintainability and facility to create infrastructure safely. Amazon web services offers various services that allow you to convert simple platforms into robust applications with different connections, using different technologies and databases, as well as allowing you to add security to both the applications and the data, this last concept is the main source of any system. This is why in this article an exploration of the encryption on databases and documents is made, using AWS services such as Key

management server, Relational database service and S3, at the end it will be found that the encrypted files and databases will not be readable by malicious people, in case an attack materializes.

Keywords: Encryption, cipher, computer crime, data security

RESUMO

Nas últimas décadas, o aumento da utilização de sistemas de informação, comunicações e a possibilidade de partilhar dados instantaneamente através da Internet trouxeram consigo termos como a ciber-segurança, desde o início que existem pessoas sem escrúpulos que querem obter informações confidenciais; é por isso que todos os anos são desenvolvidos novos vectores de ataque e com eles novos métodos para os persuadir. Actualmente, há um boom crescente nas tecnologias baseadas em microserviços e computação em nuvem, devido à sua elevada escalabilidade, capacidade de manutenção e facilidade de criação de infra-estruturas seguras. Amazon Web Service (AWS) oferece vários serviços que permitem converter plataformas simples em aplicações robustas, utilizando diferentes tecnologias e bases de dados, bem como adicionar segurança tanto às aplicações como aos dados que são a principal fonte de qualquer sistema; por esta razão, é realizada uma exploração da encriptação de bases de dados e documentos, utilizando serviços Amazon Web Service, tais como o Serviço de Gestão de Chaves, o Serviço de Bases de Dados Relacionais da Amazon e o S3. Em conclusão, no caso de um ataque se materializar, as bases de dados e ficheiros encriptados não podem ser lidos por pessoas mal intencionadas.

Palavras-chave: Criptografia, encriptação, cibercrime, segurança de dados.

Introducción

Cada día son más los esfuerzos enfocados en incrementar la seguridad de los sistemas de información y ninguna entidad o empresa está exenta de pasar por una fuga de datos; por esta razón, cada año se invierte más en seguridad informática y en sus diferentes frentes como infraestructura, red e información. Según Digital Information World (2021) en su reporte anual de enero del 2021, en el 2020 se incrementó la inversión en ciberseguridad en un 10% respecto al año anterior, para el 2021 se tuvo un incremento del 56 % y se espera que para el siguiente reporte de 2022 se supere el 69 %. De igual forma, los servicios en la nube tuvieron un crecimiento del 33 %, esto debido a la pandemia que generó el COVID-19 donde la cibercriminalidad aumentó y con ella los diferentes tipos de delitos informáticos que no tienen fronteras, los cuales causaron daños, robos de información de usuarios particulares, organizaciones con y sin ánimo de lucro (nacionales e internacionales), entidades públicas y hasta hospitales.

En los sitios web y mapas interactivos sobre ciberseguridad se han encontrado integrados *malware*, *spyware* y troyanos, que pueden penetrar en los sistemas por medio de correos electrónicos con

enlaces o archivos adjuntos infectados, y es así como piratean los datos de acceso de los empleados o aprovechan la vulnerabilidad de los sistemas (Interpol, 2020).

La pandemia del coronavirus azotó no solo a los seres humanos sino a distintos negocios y los obligó a tomar decisiones para proteger y salvaguardar de manera más eficiente y económica su información. La implementación de arquitecturas informáticas en la nube permite reinventar estrategias comerciales y de servicios, no solo en el uso de equipos informáticos, sino también porque la nube ofrece ambientes de desarrollo, pruebas, datos asequibles y altos niveles de seguridad, integridad, disponibilidad y confidencialidad.

Por lo anterior, *Amazon Web Service* (AWS) es una de las plataformas en la nube más usadas en la actualidad y según el reporte de Stackoverflow (2021) AWS tiene una gran cantidad de servicios que pueden ser usados en diferentes niveles de seguridad; por esta razón, en este artículo se habla principalmente de aquellos que sean aplicables a microservicios para incrementar la seguridad, con un enfoque en el cifrado y protección de datos, archivos y bases de datos.

■ Metodología

La presente investigación se hace bajo una metodología cualitativa y tiene como propósito comprender la forma en la que se pueden encriptar y salvaguardar la información de las bases de datos de quienes estén interesados en la protección de estos, teniendo en cuenta que esto se realiza en un entorno orientado a microservicios en *Amazon Web Service*; del mismo modo, el alcance de esta investigación es exploratoria, puesto que se basa en información de páginas oficiales (*Amazon Web Services*) y se busca la mejor vía para resguardar la información de manera eficiente, mantenible y escalable, esto con el fin de dar a conocer algunos de los servicios más comunes en el uso de microservicios y encriptación de datos. El análisis que se lleva a cabo para este caso de estudio consiste en comparar cómo se visualiza una cierta información que está cifrada y encriptada ante un intento de robo de datos con la ayuda de los servicios de *Amazon Web Service* y así concluir sobre sus ventajas y desventajas.

Amenazas cibernéticas

Por muchos años la ciberdelincuencia ha sido un problema y por eso ha nacido la necesidad de proteger los datos de los clientes y de la compañía; sin embargo, en algunos casos las barreras de seguridad son burladas. A modo de ejemplo, Pagnnota (2016) presenta algunos casos de robos de datos a grandes y medianas compañías: Yahoo (2013) fue víctima de un ataque donde tuvo una fuga de alrededor de 500 millones de cuentas, entre los datos robados se encuentran contraseñas y correos; MySpace (2013) fue víctima de una fuga de información de 427 millones de cuentas, al igual que Yahoo los datos vulnerados fueron correos y contraseñas (The Hacker News, 2016); Adult Friend-Finder (2016) presentó un robo de 400 millones de registros donde se expusieron datos como correos, contraseñas, Ips de ubicación, entre otros; Fling.com (2016) tuvo un robo de 40 millones de datos como correos y preferencias sexuales de sus clientes; 17 Media (2016) fue víctima de un ataque donde 30 millones de registros fueron expuestos con números de teléfonos y direcciones IP; Ebay, 145 millones de datos; LinkedIn, 117 millones de cuentas; VK, 100 millones de clientes afectados; Amadeus (2019), datos de los vuelos de los pasa-

jeros; Fornite (2019), datos personales y de tarjetas de crédito, según Lyons; Prestige software (2020) expuso datos personales de preferencia hotelera de sus clientes; Vueling (2020) sufrió una inyección SQL que dejó al descubierto miles de datos de sus clientes; en Twitter (2020) bloquearon cuentas de usuarios en la llamada “estafa del bitcoin”; entre muchas otras empresas que han sido vulneradas por estos ataques.

No obstante, el objetivo de los atacantes no siempre es robar información para venderla en el mercado negro, sino que muchas veces la meta es secuestrar la información, por medio de un *ransomware*, y posteriormente pedir una suma de dinero por el rescate. Un ejemplo de una compañía afectada es CNA Financiamiento, donde en marzo de 2021 fue vulnerada, logrando que esta pagara 40 millones de dólares para recuperar todos los datos involucrados. Específicamente en Colombia, según publicaciones de CaiVirtual, durante el 2019 hubo un incremento del 54 % de cibercriminales de diferentes tipos y el balance de 2020 indica que hubo un incremento del 82 % respecto al año anterior, es decir, se habla de un incremento de más del 100 % respecto al 2018 (Pagnnota, 2016; The Hacker News, 2016; DataBreach.net, 2019; Computing, 2020; ARN, s.f.; Lyons, 2021; Waldman, 2021; Mehrotra y Turton, 2021; Ceballos et al., 2019; Centro Cibernético Policial, 2020; Naren et al., 2014).

Las amenazas cibernéticas son reales y año tras año se actualizan para lograr mejores vectores de ataque, por lo tanto, es importante atacar el problema de raíz con tecnologías actuales que garanticen tapar las brechas de seguridad que se han dado debido a la coyuntura digital.

Cloud Computing Service

El cloud computing service es un conjunto de servicios que están albergados en una nube pública y que pueden ser usados desde diferentes frentes de infraestructura (Mesa Sectorial Cloud Computing, 2010), donde nacen otros términos como *Infraestructure as a Service* (IaaS), *Platform as a Service* (PaaS) y *Software as a Service* (SaaS) (Abdullah, 2017). Dichos términos se especifican de la siguiente manera:

- *IaaS (Infrastructure as a Service)*: abarca todos los elementos que se pueden usar para implementación de una red, centro de cómputo, servidor o de cualquier otra infraestructura que podamos imaginar, por ejemplo, se pueden contratar servidores, máquinas virtuales, *firewall*, *Demilitarized Zone (DMZ)*, *Virtual Private Cloud (VPC)*, canales dedicados, similar routers, data centers, bases de datos, entre otros. La principal característica de trabajar con elementos en la nube es que su escalabilidad es horizontal y su costo de implementación es bajo y fácil debido a que puede ser adquirido, primero, con un bajo procesamiento (lo que implica menos costos) y posteriormente puede incrementar las capacidades de los servidores (data center, base de datos o cualquier otro elemento que lo requiera), es decir, la infraestructura en la nube crece de manera flexible con base en el crecimiento del negocio. Esto se conoce como escalabilidad horizontal.
- *PaaS (Platform as a service)*: se encarga de la administración y creación de los servicios, sin embargo, estos servicios son muy genéricos, es decir, pueden ser usados por cualquier negocio. Por ejemplo, un servicio de biometría puede ser usado por cualquier empresa, sin embargo, debe ser configurado a las diferentes reglas que maneja cada core.
- *SaaS (Software as a service)*: es un modelo de distribución de software que permite a los usuarios conectarse a aplicaciones basadas en la nube, a través de Internet, y usarlas. Además, existe una gran ventaja, ya que permite incrementar el conjunto de servicios contratados con base en el crecimiento del negocio, es decir un escalamiento horizontal.

Algoritmos de Encriptación

AES (Advanced Encryption Standard): es un algoritmo de encriptación simétrico que usa la misma llave para encriptar y desencriptar, es decir, utiliza un algoritmo matemático llamado SPN (*Substitution Permutation Network*), el cual consiste en aplicar múltiples rondas de forma alterna, lo que permite que la información vaya perdiendo su sentido semántico y finalmente sea ilegible, esta misma técnica de permutación por rondas es lo que hace

que AES sea tan seguro, ya que para una llave de 256 bits pueden existir 1.1×10^{77} combinaciones posibles, por lo tanto el costo de encontrar la clave por fuerza bruta es muy elevado, incluso los computadores más potentes de la época se demoran años en encontrar la clave (Abdullah, 2017).

GCM (Galois/Counter Mode): es un algoritmo que busca incrementar la velocidad de cifrado de los algoritmos simétricos, este también funciona con iteraciones y rondas. Su eficiencia se da en el uso de vectores de inicialización (*IV Initialization Vector*) en los bloques de bits, de esta manera realiza operaciones sencillas como un XOR bit a bit o bitwise XOR, así como también aplica algoritmos matemáticos, esto hace que la eficiencia del algoritmo sea mayor y por ende su costo se da en un tiempo menor (McGrew y Viega, 2004).

Servicios de Amazon Web Service

Amazon Web Service es una plataforma que ofrece una amplia colección de servicios que se pueden usar en diferentes niveles de infraestructura, donde se pueden encontrar los servicios de seguridad necesarios para frenar distintos vectores de ataque. Los servicios más comunes para construir microservicios, proteger datos, cifrados..., son:

- *Amazon ECS (Elastic Container Service)*: estos contenedores están dispuestos en una red que puede ser privada o pública, es decir, puede existir una red donde solo se reconozcan las APIs de cierto sistema y otra red donde esté la salida, es decir, la cara del sistema y la salida al internet, en otras palabras, por donde se conecta el cliente. Concretamente, Amazon ECS permite tener un panel de administración para la orquestación de los servicios y, a nivel de seguridad, permite usar la VPC (*Virtual Private Cloud*) con los grupos de seguridad y la red ACLs para ofrecer control total de lo que entra y sale de la red. Además, se puede administrar el permiso de acceso para los demás contenedores con el uso de IAM (*Identity and Access Management*), de modo tal que restringe o habilita el acceso de cada usuario.
- *Amazon EKS (Elastic Kubernetes Service)*: los kubernetes son la orquestación de los diferen-

tes contenedores, es decir, estos son los que orquestan las aplicaciones internas, y así se puede definir el tipo de red y dónde se va a conectar dentro del contenedor; además, los kubernetes, como la orquestación de los contenedores, permite la administración centralizada de los mismos y esto es muy útil cuando la cantidad de contenedores de una empresa crece mucho, ya que permite definir accesos entre los diferentes contenedores y las Api del sistema. Concretamente, Amazon EKS permite usar aplicaciones certificadas por un ambiente de kubernetes en AWS, lo que agrega seguridad a los *clusters* y automatiza tareas como actualización de los últimos parches (previamente validados), todo esto mientras se administra de forma centralizada los ECS (página oficial de Amazon).

- Amazon EBS (*Elastic Block Store*): es un servicio para almacenamiento de datos en bloque de alto rendimiento. El término de almacenamiento de datos por bloque es el almacenamiento de datos como si se tratase de una curato documental, los archivos están divididos en secciones, donde se encuentran carpetas y dentro de ellas documentos y hojas, algo similar es este tipo de almacenamiento; sin embargo, *Amazon Web Service* mezcla este tipo de almacenamiento con motores de bases de datos relacionales y no relacionales, con lo que este servicio es muy flexible para negocios que deseen guardar datos en forma de archivo o simplemente deseen guardar información de sus clientes en motores relacionales o no relacionales; además, permite una administración centralizada donde se pueden crecer horizontalmente con base en las necesidades del negocio, lo que permite realizar análisis de datos (*big data*) en cualquier momento del crecimiento del negocio o en una fecha particular (página oficial de Amazon).
- Amazon Macie: es un servicio de seguridad y privacidad de datos de información completamente administrado que utiliza inteligencia artificial para proteger grandes cantidades de datos confidenciales y entre sus beneficios están una evaluación de privacidad y seguridad de datos programados, por lo que continuamente arroja alertas y recomendaciones para mejorar dichas características. Además, Identifica los datos confidenciales en las mi-

graciones de datos, sean masivas o no. Esto puede ocurrir cuando se quiere pasar a RDS, Amazon Aurora, Amazon S3, EBS o cualquier otro servicio para almacenar información, y así permite disminuir vectores de ataque cuando se realizan migraciones de datos (página oficial de Amazon).

- Amazon KMS (*Key Management Service*): permite la creación de llaves de diferentes tipos (común, pública o privada), la centralización del almacenado de estas llaves y a su vez la administración centralizada de las mismas, con el propósito de definir accesos y ocultar su contenido, de este modo nadie puede saber el contenido de la llave a excepción de los servicios que tengan el acceso a ella. Este control, aunque simple, le otorga a los servicios un gran nivel de seguridad, ya sea para encriptar, desencriptar, cifrar o descifrar datos, incluso se puede usar para la creación de llaves que permitan determinar los token de acceso a la aplicación. Tiene una gran variedad de aplicaciones y todas enfocadas a proteger los datos por medio de la administración de llaves. Debido a la centralización del almacenamiento de claves, estas pueden configurarse para ser usadas exclusivamente en ciertas aplicaciones o servicios, de modo tal que solo se puede acceder a ella usando servicios específicos, por lo tanto, las claves son completamente restringidas para otros servicios que intenten usarlas (página oficial de Amazon).
- Las llaves de KMS constan de un conjunto de almacenado de claves, estas son de 256 *bits* y usan un estándar de encriptación AES (*Advanced Encryption Standard*), lo hace en conjunto con GCM (Galois/Counter Mode), el cual es un algoritmo usado en claves asimétricas para aumentar su velocidad de encriptado, por lo tanto, el impacto en la lectura de datos es mínimo (página oficial de Amazon). KMS a su vez realiza backups automáticamente de la base de datos RDS, los cuales se pueden programar.
- Amazon RDS (*Relational Database Service*): es un servicio que permite crear bases de datos. Esta herramienta, a diferencia de otras tiene una ventaja, pues encripta los datos de forma

predeterminada, ya sea con una llave generada automáticamente o una llave generada por KMS (página oficial de Amazon), esto con el objetivo de que los datos sean ilegibles, lo cual garantiza que la información no va a poder ser leída en caso de fuga de datos (página oficial de Amazon).

- *Amazon Secrets Manager*: es muy útil para ocultar información confidencial dentro de las aplicaciones, tales como cadenas de conexiones, claves, llaves, subscriptions keys, scope y cualquier otro dato que se pueda considerar como confidencial o secreto. También, posee un panel de administrador que permite especificar los servicios que usarán los secretos a nivel de la aplicación, así como recuperar datos de los diferentes servicios que adquieren los datos como Api, RDS, RedShift, etc. Este servicio es muy útil, principalmente, para ocultar los datos de los ambientes de producción de los participantes en la construcción de software (página oficial de Amazon).

Protección y cifrado de datos

Una vez identificados los servicios que se pueden usar a través de AWS es necesario detectar la fuente principal, los datos, ya que por su gran valor corporativo es indispensable protegerlos, por este motivo se deben planear y ejecutar estrategias que garanticen que no van a caer en manos equivocadas, y si esto llegase a ocurrir, que no logren ser leídos. En este punto es importante resaltar las tres características principales de la información: la integridad, la disponibilidad y la confidencialidad. La disponibilidad de los datos es proporcionada por las Api que están alojadas en el ECS, las Api se encargan de actuar como interfaz para proveer los datos a quienes tengan accesos a ellos, así como también permite la integridad de los mismos, ya que, al estar dentro de un EKS las Api no pueden ser alteradas con el fin de modificar la información; por último, la confidencialidad de los datos, se trata por medio de los servicios de encriptación de datos usando las llaves que provee KMS (página oficial de Amazon).

La RDS permite realizar bases de datos cifradas con el propósito de no acceder a la información de forma sencilla, por eso, es necesario tener la llave aportada por KMS y después asociarla a la RDS. Estos dos servicios permiten tener bases de datos seguras que garantizan que la información sea ilegible, en caso de la irrupción de un intruso, debido al alto nivel de encriptación que ya se ha mencionado.

Por otro lado, S3 permite guardar documentos y archivos, aunque predeterminadamente no son encriptados, esta característica se puede configurar para que lo haga por medio de las llaves de KMS; es decir, se puede tener una llave para RDS y otra para S3 o bien una misma para ambas, aunque se aconseja el manejo de llaves de manera individual.

Caso de estudio

Este caso de estudio da cuenta de la encriptación de datos donde se usan las llaves de KMS para encriptar un documento en S3 y después encriptar una base de datos en RDS. Para la encriptación de los datos se genera una llave simétrica, la cual es aplicada a los datos que se quieren proteger, esto da como resultado el archivo ya protegido el cual es guardado en el storage; sin embargo, la parte más importante se da en la manera como se guarda o protege la llave que permite desencriptar los datos; para esto se requiere una llave maestra, la cual permite encriptar la llave que se usó para encriptar los datos y esta llave es guardada en el mismo storage en el que se encuentra el archivo. Ahora bien, es menester tener presente que sin la llave maestra no es posible acceder a los datos. Así mismo, no debe haber preocupación porque la llave maestra es almacenada en otros servicios especializados para llaves maestras, los cuales pueden ser AWS CloudHSM o AWS KMS entre otras que ofrece Amazon Web Service.

Prueba de funcionamiento de KMS:

Al no ser posible acceder a los archivos encriptados directamente en los servicios de Amazon Web Services, a continuación se observa una simulación del funcionamiento en un archivo plano que simula ser una Base de datos RDS (Figura 1):

Creación de un usuario para la simulación

Se realiza la creación de un usuario “Simulator-kms”, el cual se le conceden los privilegios de acceso y manejo de la KMS.

Creación de privilegios

Para conceder parte de los privilegios del usuario se debe crear un grupo “Simulator-kms-group” en el cual se especifica solamente permisos de KMS al usuario creado.

Descargar claves

Con la creación del usuario y asignación de privilegios se generan unas credenciales con las cuales se pueden

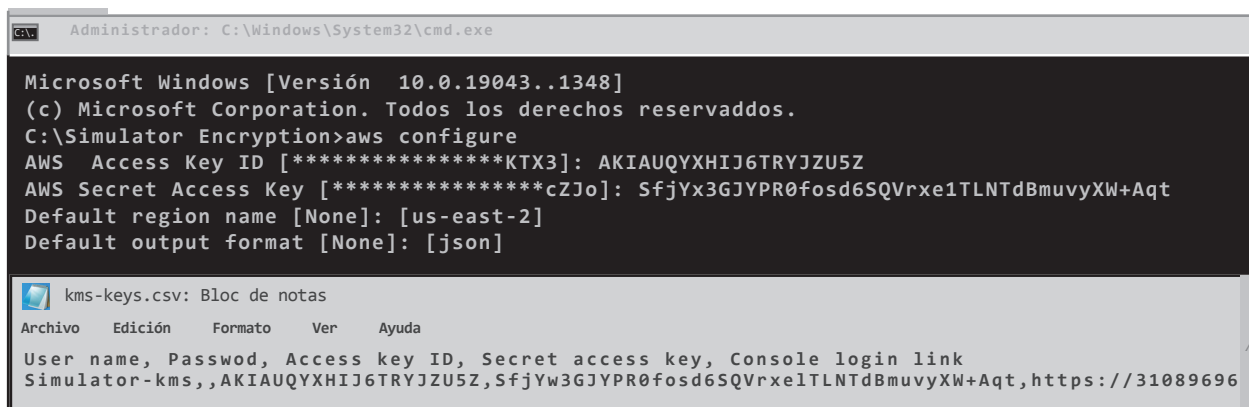
acceder a la KMS. Por lo tanto, para la simulación es necesario descargarlas localmente.

Configuración de las llaves

Con el archivo que se genera se debe realizar la configuración del ambiente a trabajar, para esto se usa el comando “aws configure” en el cual se debe ingresar el *access key* y *secret key* generados anteriormente, adicionalmente la región y tipo de formato de salida que se quiere manejar.

Figura 1

Configuración de credenciales y llaves para pruebas locales



```
Administrador: C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19043.1348]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Simulator Encryption>aws configure
AWS Access Key ID [*****KTX3]: AKIAUQYXHJ6TRYJZU5Z
AWS Secret Access Key [*****cZJo]: SfjYx3GJYPR0fosd6SQVrxe1TLNTdBmuvyXW+Aqt
Default region name [None]: [us-east-2]
Default output format [None]: [json]

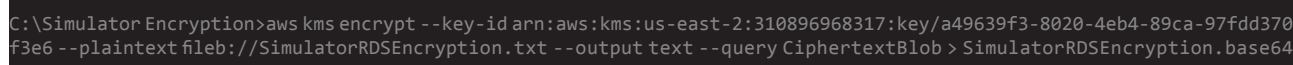
kms-keys.csv: Bloc de notas
Archivo Edición Formato Ver Ayuda
User name, Passwod, Access key ID, Secret access key, Console login link
Simulator-kms,,AKIAUQYXHJ6TRYJZU5Z,SfjYw3GJYPR0fosd6SQVrxe1TLNTdBmuvyXW+Aqt,https://31089696
```

Archivo prueba

El archivo prueba que va a simular un RDS de AWS para encriptar con KMS es un archivo de texto en el cual se tiene el mensaje “¡¡This is DataBase in AWS!!” el cual simula la información dentro de un RDS.

Figura 2

Comando de encriptación y cifrado del archivo de prueba



```
C:\Simulator Encryption>aws kms encrypt --key-id arn:aws:kms:us-east-2:310896968317:key/a49639f3-8020-4eb4-89ca-97fdd370f3e6 --plaintext fileb://SimulatorRDEncryption.txt --output text --query CiphertextBlob > SimulatorRDEncryption.base64
```

Encriptar

Para proceder con la encriptación del archivo se realiza el siguiente comando, donde “SimulatorRDEncryption.txt” es el archivo inicial y “SimulatorRDEncryption.Base64” es el archivo resultante.

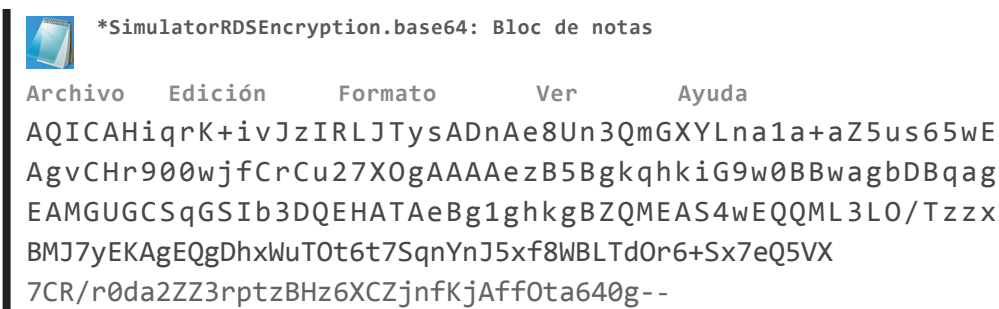
Archivo cifrado y codificado

Luego de la ejecución del código, el archivo resultante se ve de la siguiente manera, donde ha

sido encriptado y cifrado en base 64 para mayor seguridad, este sería el proceso que realiza los servicios de AWS junto a KMS. En caso de que se pueda visualizar, se observa en la figura 3.

Figura 3

Visualización de archivo encriptado y cifrado luego de correr el comando



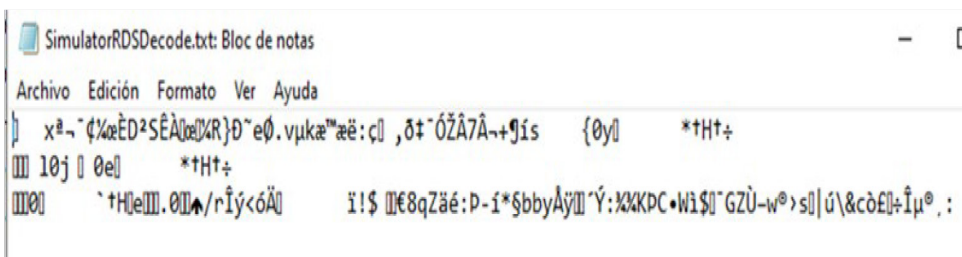
Intento de robo de información

En el caso hipotético que se logre filtrar la información y los ciberdelincuentes intenten decodificarla para conocer la información real que se tiene en la

base de datos RDS, que es la que se está simulando, el archivo se ve como se muestra en la Figura 4. Esto sucede porque no se tiene la llave maestra para descryptar y solo se intenta decodificar la información, por lo tanto no es legible.

Figura 4

Visualización de un archivo cuando se intenta decodificar sin la llave de cifrado



Descryptar el Archivo

Para descryptar el archivo se corre el comando que a continuación se presenta (Figura 5) donde “SimulatorRDSDecode.txt” es el archivo que se intenta decodificar y “SimulatorRDSDecrypt.base64” es el archivo resultante. En el archivo que se obtiene, como se ve en la Figura 6, la información sigue sin ser legible, ya que aún está codificado en base 64.

Figura 5

Comando para descryptar el archivo encriptado

```
C:\Simulator Encryption>aws kms decrypt -- ciphertext-blob fileb://SimulatorRDSDecode.txt --output text --query Plaintext > SimulatorRDSDecrypt.base64
```

Figura 6

Visualización de archivo descifrado y no decodificado



Decodificación del archivo

Se corre el comando que se ve en la figura 7 para decodificarlo, donde "SimulatorRDSDecrypt.base64" es el archivo anteriormente decodificado

Figura 7

Decodificación de archivo descifrado

```
C:\Simulator Encryption>certutil -decode SimulatorRDSDecrypt.base64 SimulatorRDSDecrypt.txt
```

Con esto se puede observar que aunque se desee acceder a la información de una forma ilegal o no permitida, mientras no se tengan las llaves con las que fueron codificadas, no es posible acceder a la información.

Creación de llaves KMS

Para la creación de llaves KMS basta con buscar el servicio "Key Management Service (KMS)" y seleccionar la opción de "Crear llave", luego seleccionar el tipo de llave simétrica. Para seleccionar los usuarios que pueden administrar la llave y la definición de los usos de la misma, se listan los usuarios creados y con esto se tiene la llave KMS creada.

Habilitar KMS en RDS AWS

Al momento de crear una base de datos en Amazon Web Services con el servicio de RDS, se encuentra un apartado llamado Encriptación, en el cual se puede habilitar el uso de AWS KMS para encriptar la base de datos creada. Basta con habilitarlo y automáticamente trae las llaves creadas en KMS.

Habilitación de KMS en S3 Amazon Web Services

Al momento de crear el servicio de S3 en el apartado de encriptación se debe habilitar la opción de KMS; luego, se habilita las opciones de tipo de llave que se desea usar, entre ellas AWS KMS en las cuales se listan las KMS creadas con anterioridad. Por último, se debe seleccionar el que se desea usar para el servicio y así continuar con los pasos de creación de servicio S3.

Validación de KMS en Servicios AWS

Para validar KMS en los servicios de AWS, como por ejemplo un servicio de S3 que cuenta con

y "SimulatorRDSDecrypt.txt" el archivo resultante descriptado, para finalizar se obtiene la información que se encriptó y cifró por medio de KMS.

encriptación KMS, en las opciones de "Server-side encryption settings", se puede observar que la encriptación se encuentra habilitada y el servicio usado es AWS Key Management Service o KMS.

Conclusión

Dentro de los hallazgos encontrados se observa que el Amazon Web Services tiene un nivel de seguridad lo suficientemente alto para poderlo denominar impenetrable, esto cumple con los estándares de seguridad esperados para el caso de estudio propuesto donde se esperaba no poder tener acceso a la información guardada bajo el nivel de seguridad suministrado por Key Management Service de Amazon Web Service, y así proteger el mayor activo, los datos, para la mayoría de las compañías; también se pudo demostrar que en el caso hipotético de robo de datos, tal cual como se observó en el caso de estudio "Intento de robo de información" en la Figura 4, esta información es ilegible, gracias a los métodos que se usan con KMS de cifrado y encriptado, además de la forma de guardar y proteger las llaves maestras que permiten encriptar y desencriptar las otras llaves que a su vez encriptan y desencriptan la información, por lo tanto, no es posible acceder a ellas ni a los datos guardados, siendo así una de las formas más seguras para mantener la información a salvo de personas inescrupulosas.

Para finalizar, se encontró que el RDS no es legible incluso dentro de la plataforma de AWS; de tal forma que los empleados internos de una organización no pueden acceder a la información, este sería un caso de seguridad preventiva interna para así evitar ataques desde adentro. Aunque los documentos en S3 con los permisos adecuados puedan ser legibles desde la plataforma, para llegar a acceder a estos

se requiere la llave de KMS relacionada; de esta forma, los archivos también cumplen con la regla de seguridad interna y externa. Asimismo, como se mencionó a lo largo del documento, KMS usa estándares de encriptación AES junto con GCM, lo cual se pudo corroborar al momento de desencriptar la información, ya que es necesario un paso adicional de decodificación, así como también se evidenció que la longitud de los documentos, una vez encriptada la información, es diferente; por lo tanto, se puede demostrar que existe un proceso basado en rondas, tal cual lo hace AES.

Si bien KMS es un excelente servicio para encriptar datos, se podría explorar otros usos dentro del campo de la encriptación de estos, por ejemplo, en la transmisión de datos punto a punto, así como también el costo en tiempos de ejecución al encriptar y desencriptar información en bases de datos altamente demandadas por otros servicios. En suma, este artículo abre la puerta a nuevas investigaciones y casos de estudio en el marco de *cloud computing* y la necesidad de reforzar los sistemas de seguridad en el mismo.

Para esta investigación se tiene como limitante el acceso directo a la información de las bases de datos, al almacenamiento de archivos en los servicios S3 y demás servicios de Amazon Web Service para realizar directamente las pruebas, ya que, justamente, es el nivel de seguridad que brinda los servicios cifrados con AWS KMS.

■ Conflicto de intereses

Es necesario informar por escrito que no se tiene la existencia de alguna relación entre los autores del artículo y la compañía dueña de los servicios Amazon Web Services tratados en el artículo, la cual pudiera derivar algún posible conflicto de intereses

■ Referencias

- Abdullah, A. M. (2017). Advanced Encryption Standard (AES) algorithm to Encrypt and Decrypt Data. *Cryptography and Network Security*, 16: 1-12. <https://onx.la/acff6>
- Amazon Web Services. (2020). *Guía para desarrolladores: AWS Key Management Service*. [https://docs.](https://docs.aws.amazon.com/es_es/kms/latest/developerguide/kms-dg.pdf#overview)

[aws.amazon.com/es_es/kms/latest/developerguide/kms-dg.pdf#overview](https://docs.aws.amazon.com/es_es/kms/latest/developerguide/kms-dg.pdf#overview)

- Amazon Web Services. (s.f.). *Amazon Elastic Block Store (EBS) Almacenamiento en bloque de alto rendimiento y con facilidad de uso a cualquier escala*. <https://aws.amazon.com/es/ebs/>
- Amazon Web Services. (s.f.). *Amazon Elastic Container Service (Amazon ECS), Ejecutar contenedores de alta seguridad, fiables y escalables*. <https://aws.amazon.com/es/ecs/>
- Amazon Web Services. (s.f.). *AWS cryptographic services and tools guide: Cryptographic algorithms*. <https://docs.aws.amazon.com/crypto/latest/userguide/crypto-ug.pdf#concepts-algorithms>
- Amazon Web Services. (s.f.). *AWS Secrets Manager, Alterne, administre y recupere fácilmente credenciales de bases de datos, claves API y otros datos confidenciales durante todo su ciclo de vida*. <https://aws.amazon.com/es/secrets-manager/>
- ARN. (s.f.). *Top 10 most notorious cyber attacks in history*. <https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/>
- Ceballos, A., Bautista, F., Mesa, L., Argáez, C., Durán, A., Miranda, F., Acevedo, R., Prada, W., Ruiz, J., & Santos, H. (2019). *Tendencias Cibercrimen Colombia 2019-2020*. TicTac. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf
- Centro Cibernético Policial. (2020). *Balance Cibercrimen*. https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf
- Mesa Sectorial Cloud Computing. (2010). *Cloud Computing, una perspectiva para Colombia*. http://www.interactic.com.co/dmdocuments/clud_computing.pdf
- Computing. (2020). *Los 10 ciberataques más grandes de la década*. <https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html>
- Data Breach. (2019). *Amadeus Traveler Data Exposed in a Thwarted Data Leak*. <https://www.databreaches.net/amadeus-traveler-data-exposed-in-a-thwarted-data-leak/>
- Digital Information World. (2021). *Canalys Report Predicts That Cybersecurity Will Demonstrate an Estimated 10 percent Growth*. <https://www.digitalinformationworld.com/2021/01/canalys-report-predicts-that.html>

- Encrypting Amazon RDS resources - Amazon Relational Database Service. <https://aws.amazon.com/es/rds/>
- Interpol. (s.f). *Ciberamenazas relacionadas con la COVID-19*. <https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19>
- Lyons, J. (28 de diciembre de 2021). Worst Cyberattacks of 2021 (So Far). *Sdxcentral*. <https://www.sdxcentral.com/articles/news/worst-cyberattacks-of-2021-so-far/2021/>
- McGrew, D., y Viega, J. (2004). The Security and Performance of the Galois/Counter Mode (GCM) of Operation. En A. Canteaut, y K. Viswanathan (Eds.), *Progress in Cryptology - INDOCRYPT 2004. Lecture Notes in Computer Science*, (pp. 343-355). Heidelberg. https://doi.org/10.1007/978-3-540-30556-9_27
- Mehrotra, K., & Turton, W. (21 de mayo de 2021). CNA Financial Paid \$40 Million in Ransom After March Cyberattack. *Insurance Journal*. <https://www.insurancejournal.com/news/national/2021/05/21/615373.htm>
- Naren, J., Sowmya, S., & Deepika, P. (2014). Layers of Cloud – IaaS, PaaS and SaaS: A Survey. *International Journal of Computer Science and Information Technology*, 5(3): 4477-4480. https://www.researchgate.net/publication/264458816_Layers_of_Cloud_-_IaaS_PaaS_and_SaaS_A_Survey
- Pagnotta, S. (29 de diciembre de 2016). Los 10 incidentes de seguridad más grandes de 2016. *Welivesecurity*. <https://www.welivesecurity.com/la-es/2016/12/29/incidentes-de-seguridad-mas-grandes/>
- Stack Overflow. (2021). *Developer Survey 2021*. <https://insights.stackoverflow.com/survey/2021#overview>
- The Hacker News. (2016). *427 Million Myspace Passwords leaked in major Security Breach*. <https://thehackernews.com/2016/06/myspace-passwords-leaked.html>
- Waldman, A. (5 de junio de 2021) 10 of the biggest cyber attacks of 2020. *TechTarget*. <https://www.techtarget.com/searchsecurity/news/252494362/10-of-the-biggest-cyber-attacks>