MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Análisis de brechas de seguridad en el acceso a datos en la nube para soluciones Big Data

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
María Soledad AZÚA CAMPOS

Bajo la dirección de:
Ing. Christian MERCHÁN MILLÁN

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Septiembre del 2018

Análisis de brechas de seguridad en el acceso a datos en la nube para soluciones Big data

Analysis of security gaps in access to data in the cloud for Big Data solutions.

María Soledad AZÚA CAMPOS[1]
Ing. Christian MERCHÁN MILLÁN[2]

Resumen

Los proveedores de almacenamiento de datos en la nube, permiten a sus clientes compartir o guardar cualquier tipo de información, tales como archivos o documentos desde cualquier dispositivo conectado al internet. El usuario busca que estos proveedores logren mantener sus datos seguros y protegidos ante ataques externos, ransomware o cualquier tipo de filtración de datos que vuelvan vulnerable la información almacenada. El presente trabajo investigativo, tiene como finalidad, identificar las brechas de seguridad en el acceso, existentes en dos de los proveedores de servicio de almacenamiento en la nube. Para el presente estudio se tomó como referencia a Amazon y Google Cloud, los mismos que fueron escogidos bajo el análisis de encuestas internacionales y locales (Ecuador); se delimitaron como indicadores el uso de los servicios públicos en la nube como lo indica SADA Systems, destacando a Google Cloud con el 49% como uno de los primeros a nivel internacional. Otro de los indicadores fue por los proveedores de IaaS público, que lidera en la parte de ingresos económicos colocando a Amazon en el puesto número uno, por poseer más del 51,80% de todo el mercado. Para identificar la tendencia en el Ecuador, se encuestaron a once PYMES cuya dedicación es de diferentes índoles y se localizan en puntos geográficos distintos del país. Uno de los principales requerimientos de las PYMES encuestadas para optar por una solución de almacenamiento en la nube es el control de acceso (Autenticación de usuarios y Aplicaciones), identificando que Google Cloud y Amazon son los proveedores de servicio en la nube más requeridos por ellos. Para identificar las brechas de seguridad en el acceso de los dos proveedores seleccionados, se trabajó con el Modelo de Seguridad y Privacidad de la Información (SPI), presentando en su inicio las características de cada uno de los proveedores para el almacenamiento de datos en la nube en lo que respecta al control de acceso. Se realizó la comparación de los dos proveedores en Identificación, Autenticación y Autorización, evaluando las brechas de seguridad existentes entre Amazon y Google Cloud, se identificó que la administración incorrecta y el desconocimiento de los múltiples recursos que los proveedores poseen, generan una puerta de acceso a los ataques y se torna una vulnerabilidad para los involucrados.

Palabras clave: Big Data, almacenamiento en la nube, autenticación, control de acceso, brechas de seguridad.

[1] Estudiante en Facultad de Posgrado, Maestría en Auditoría en Tecnologías de la Información, Universidad de Especialidades Espíritu Santo – Ecuador.

[2] Magíster en Seguridad Informática Aplicada. Director de Trabajo de Titulación de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador.

Abstract

Providers of data storage in the cloud, allow their customers to share or save any type of information, such as files or documents from any device connected to the Internet. The user seeks that these providers manage to keep their data safe and protected from external attacks, ransomware or any type of data leakage that makes the stored information vulnerable. The purpose of this research work is to identify security breaches in access, existing in two of the storage service providers in the cloud. For the present study, Amazon and Google Cloud were taken as references, the same ones that were chosen under the analysis of international and local surveys (Ecuador); The use of public services in the cloud was defined as indicators, as indicated by SADA Systems, highlighting Google Cloud with 49% as one of the first at the international level. Another of the indicators was by the suppliers of public IaaS, which leads in the part of economic income placing Amazon in the number one position, having more than 51.80% of the entire market. To identify the trend in Ecuador, eleven SMEs were surveyed whose dedication is of different types and they are located in different geographical points of the country. One of the main requirements of the SMEs surveyed to opt for a storage solution in the cloud is access control (Authentication of users and applications), identifying that Google Cloud and Amazon are the cloud service providers most required by them. To identify security gaps in the access of the two selected providers, we worked with the Information Security and Privacy Model (SPI), presenting at the beginning the characteristics of each of the providers for the storage of data in the cloud in regards to access control. The comparison of the two providers in Identification, Authentication and Authorization was made, evaluating the existing security gaps between Amazon and Google Cloud, it was identified that the incorrect administration and the ignorance of the multiple resources that the providers possess, generate an access door to attacks and becomes a vulnerability for those involved.

Key words | Big Data, cloud storage, authentication, access control, gaps security.

INTRODUCCIÓN

En la actualidad se genera gran volumen de datos cada día. Aproximadamente se producen 2,5 trillones de bytes de múltiples fuentes. (IBM, 2017) A esto es lo que conocemos como Big data, el gran conjunto de datos, tanto estructurados como no estructurados cuyo volumen, variabilidad y velocidad de crecimiento hace compleja su obtención, almacenamiento y procesamiento de una forma tradicional (Camargo, Camargo, & Joyanes, 2015).

Para la gestión de estos datos masivos se han implementado la utilización de tecnologías de almacenamiento y procesamiento de información más avanzadas para acceder a ellos de una forma rápida y eficaz, así las organizaciones en forma general, pueden realizar la toma decisiones de un entorno real para mejorar las estrategias a utilizar (Murillo & Basanta, 2016).

Según Suárez, Suárez, & Abád (2015) mencionan que en la última década en el Ecuador, las pequeñas y medianas empresas (PYMES), han presentado un crecimiento en todo el territorio, además que las ciudades con la mayor cantidad de PYMES se encuentran en: Guayas 44%, Quito 42%, Cuenca 14%.

Gómez (2017) define a la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizada sobre un sistema o red informática, cuyos efectos puede conllevar daño sobre la información o comprometer su confiabilidad, autenticidad o integridad disminuir el rendimiento de los equipos o bloquear el acceso de usuario autorizado al sistema.

Esta son algunas de las dificultades que pasan las pequeñas y medianas empresas tanto en el Ecuador como en el mundo. Por las encuestas analizadas en el apartado anterior, múltiples son las organizaciones que almacenan sus datos en la nube (Cloud storage).

El objetivo del presente trabajo es analizar las brechas de seguridad para el acceso a datos en la nube para soluciones Big data de los proveedores Amazon y Google Cloud, la que se realizó a través del Modelo de seguridad de la Información: Infraestructura como un servicio, Plataforma como un servicio y Software como un servicio (IaaS, PaaS y SaaS sus siglas en inglés) (Kepes, Ben, 2011). Se analizaron las encuestas realizadas por SADA Systems y Gartner las mismas que corresponden al nivel internacional, la autora de esta investigación realizó encuestas a once PYMES del Ecuador, con el fin de establecer entre todos los datos existentes, cuáles son las tendencias a escoger de los proveedores de almacenamiento en la nube y qué beneficios se esperan obtener de ellos, para este caso se obtuvieron dos de las múltiples existentes en el mundo, Amazon y Google Cloud.

La importancia de este trabajo radica en la presentación a las empresas y usuarios de las características de cada uno de los proveedores para el almacenamiento de datos en la nube en lo que respecta al control de acceso. Se comparó los dos proveedores, respaldados en la comparativa de gestión de identidad y acceso (Tabla.2), en el aspecto de comunicación (conexión, registro y login) evaluando las brechas de seguridad existentes entre Amazon y Google Cloud.

MARCO TEÓRICO

Big Data

Según indica Sevillano (2013) Big Data es una tecnología para transformar la analítica de grandes volúmenes de datos, pero es también una tecnología disruptiva. Por su parte Serrat (2013) define a Big Data como el sector de las tecnologías de la información y la comunicación (TIC) que se preocupa de cómo almacenar y tratar grandes cantidades de información o conjuntos de datos.

Una de las aproximaciones más completas es la que realiza, Puyol (2014) quien define Big Data como una nueva generación de tecnologías y arquitecturas diseñadas para extraer valor económico de grandes volúmenes

de una amplia variedad de datos, mediante la capacidad de captura, descubrimiento y/o análisis a gran velocidad. Esta definición abarca hardware, software y servicios de integración, organización, gestión, análisis y presentación de datos que se caracteriza con las cuatro Vs: Volumen, Variedad, Velocidad y Valor. Existe una V adicional como característica fundamental de Big Data determinada por el autor como *Veracidad* siendo la relación que hay entre Señal (data con valor) frente a Ruido (data sin valor) (Sunqu, 2016).

Existe una gran variedad de definiciones de Big Data, cada una de ellas con cierto parecido, sin embargo, en conjunto puede producir cierta confusión sobre el término, por tal razón desde el análisis de varios autores, se puede inferir, que Big Data se aplica para el tratamiento de la aquella información que es imposible ser analizada o procesada mediante tecnologías o herramientas tradicionales (Pérez M. , 2015).

Uno de los desafíos más grandes de las organizaciones en la actualidad es el tratamiento de Big Data, por lo general ellas generan o tienen acceso a infinidad de información, pero no logran obtener un procesamiento que les permita dar valor añadido a la misma (Pérez M. , 2015).

Big Data en las organizaciones

Joyanes (2016) establece que la adopción de Big Data en organizaciones y empresas implica más que la instalación y puesta en marcha del software adecuado, es necesario un cambio organizacional en las empresas y en su personal, por ello es imprescindible una formación especializada al personal en la utilización de las herramientas de Big Data con el objeto principal de capturar, almacenar y manipular los grandes volúmenes de datos en beneficio de la productividad de la empresa.

A su vez, López (2012) determina que la gran cantidad de aplicaciones de Big Data, según International Business Machines IBM, muestra las cinco orientaciones preferentes a la hora de aplicar Big Data en organizaciones, en la que el 49% de las organizaciones prefieren aplicar Big Data para centrarse en el cliente, el 18% en optimización operativa, el 15% en gestión financiera y de riesgo, el 14% en el nuevo modelo empresarial y un 4% en colaboración empresarial.

Hierro (2016) manifiesta que cualquier organización tiene que tener claro de dónde vienen los datos y las fuentes de información, para poder analizar qué es lo importante y qué objetivos se pueden desarrollar en una estrategia de implantación de un sistema de Big Data. El servicio que está revolucionando a las organizaciones en su infraestructura de tecnología de la información es el servicio en la nube. La característica principal de esta revolución radica en el cambio de la inversión de esfuerzo en término de diseño, construcción, implantación y mantenimiento de toda la infraestructura del sistema y de los servicios que se encuentran apoyados en el provedor de servicios en la nube (Management Solution, 2012).

Almacenamiento en la nube

El nuevo paradigma para las empresas es la Computación en la nube, la cual representa una manera distinta de hacer las cosas, porque brinda servicios informáticos en la red de forma rápida y flexible; incluye basta cantidades de informacion, la misma que se obtiene mediante dispositivos conectados a la Web, la nube brinda servicios de hardware, sistemas, software o almacenamiento por parte de provedores (Galmes, 2016).

Arquitectura en la Nube

Según Areitio (2010) las arquitecturas de servicios en la nube estan dados por; Nube Software as a Service (Saas), el mismo que utiliza las aplicaciones del proveedor sobre una red; Platform as a Service (Paas), esta despliega aplicaciones creadas por el cliente a una nube, Infraestructure as a service (Iaas) esta arrienda procesamiento, almacenamiento,

capacidad de red y otros recursos de computación fundamentales.

Tipos de nube computacionales

Existen tres tipos de nubes: a) Las públicas, son administradas externamente por terceros, la ubicación de la informacion de los diferentes clientes pueden almacenarse en el mismo servidor, sus usuarios emplean todas las capas de la infraestructura de la nube; b) las privadas, el provedor es dueño del servidor, red y disco, él decide qué usuarios están autorizados para emplear esta infraestructura, este tipo de almacenamiento es manejado por un administrador quien controla las aplicaciones; c) las nubes híbridas, que son una combinación entre la nube pública y la privada, permite compartir datos y aplicaciones entre ellas (Ávila, 2011).

Ventajas y desventajas del Almacenamiento en la nube

Dean & Saleh (2010) manifiestan que existen algunas ventajas y desventajas concernientes al almacenamiento en la nube, entre sus principales ventajas destacan costo, competitividad, disponibilidad, abstracción de la parte técnica, acceso desde cualquier punto geográfico, escalabilidad y concentración de esfuerzo en los procesos de negocio; a su vez las desventajas mostradas en el almacenamiento en la nube son: privacidad, disponibilidad, falta de control sobre recursos y dependencia.

Entre las principales ventajas que brinda la computación en la nube está el minimizar el gasto de capital a través de la reducción de infraestructuras tales como hardware y software así como de mantenimiento; se crea independencia de localización y dispositivo. Además se mejora el uso y la eficiencia, aumento de la escalabilidad y elasticidad, se crean nuevas forma de colaboración de grupo unido a ello no requiere de espacio físico para almacenar servidores y bases de datos porque estos se encuentran, brindando de esta manera independencia de sistemas operativos y capacidad de almacenamiento virtual ilimitada, también existen desventajas en el almacenamiento en la nube, siendo la más relevante la privacidad y protección de programas y datos, existiendo en algunos casos carencia de control así como de fiabilidad, otro de los inconvenientes es la no portabilidad de una aplicación construida para un servido de nube a otro proveedor de servicios de cloud computing (Areitio, 2010).

Normas de seguridad para almacenamiento en la nube

ISO (2018) fue publicada en julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en la nube. La norma se complementa con la norma ISO 27001 e ISO 27002 en el ámbito de gestión de la seguridad de la información y que se dirige de forma específica a los proveedores de servicios de nube.

Fernández & Recio (2018) manifiestan que la ISO/IEC 27018 permite aclarar y reforzar las obligaciones exigibles al cliente de servicios, al responsable del tratamiento y al proveedor de servicios. Así mismo, el Esquema Nacional de Seguridad puede beneficiarse tanto de la ISO/IEC 27018 y la futura ISO/IEC 27017, también permitirán supervisar el cumplimiento del proveedor de servicios basándose en las auditorías que terceros hagan sobre el mismo.

Principales proveedores de almacenamiento en la nube

Entre los principales proveedores de almacenamiento en la nube destacan los siguientes: Amazon , IBM, Google y Windows.

Amazon S3

AWS (2018) manifiesta ser una plataforma de servicios de nube, además ofrece potencia de cómputo, almacenamiento de bases de datos, entrega de contenido y otra funcionalidad para

ayudar a las empresas a escalar y crecer. Así mismo posee el servicio de Amazon Simple Storage Service (Amazon S3) que brinda el servicio de almacenamiento de objetos creado, para almacenar y recuperar volumen de datos desde cualquier ubicación: sitios web y aplicaciones móviles, aplicaciones corporativas y datos de sensores o dispositivos IoT.

AWS (2018) señala que Amazon S3 está diseñado para ofrecer una durabilidad del 99,9% y almacena datos para millones de aplicaciones utilizadas por líderes de mercados de todas las industrias, S3 ofrece la funcionalidad de consulta en el lugar, lo que le permite ejecutar análisis eficientes directamente en los datos en reposo, además es el servicio de almacenamiento en la nube con mayor nivel de compatibilidad disponible, ya que se integra con la mayoría de las soluciones de terceros, socios integradores de sistemas y otros servicios de AWS.

International Business Machines IBM

Vázquez (2015) manifiesta que los servicios de cloud computing de IBM incluyen también el almacenamiento con IBM Smart Business Storage Cloud, el cual surgió por el crecimiento en los volúmenes de datos y la diversidad de formatos de archivo, así esta solución permite que los usuarios tengan un acceso eficiente, rentable y experimenten una disminución del rendimiento e interrupciones.

Google Cloud

Google Cloud (2018) combina un modelo de seguridad, infraestructura a escala mundial y capacidad única para innovar, que mantiene a la empresa protegida y al día en el cumplimiento de las normativas pertinentes.

La seguridad con la que cuenta Google Cloud, en su infraestructura está diseñada en capas progresivas, desde la seguridad física de los centros de datos, pasando por la seguridad del hardware y el software subyacentes, hasta los procesos y las restricciones técnicas que aumentan la seguridad operativa (Google Cloud, 2017).

Seguridad en el almacenamiento en la nube

Fernandez (2012) la seguridad es una de las herramientas o instrumentos de que disponemos para asegurar el respeto a la protección de datos, la seguridad abarca varios ámbitos –disponibilidad, autenticación, integridad y confidencialidad– siendo el último de ellos el más relacionado con la libertad informática.

Figura 1. Seguridad en la nube

Fuente**:** AWS (2018)

Así como la seguridad de la tecnología de la información tradicional, la seguridad en la nube tiene algunas funciones similares entre ellas la protección de los datos contra eliminación, robo o filtración. Los servicios de almacenamiento en la nube permiten trabajar a escala y proteger la información de una forma ágil y sencilla. A su vez cierta información que se almacena en la nube puede demandar más requisitos tal es el caso de información de tarjetas de crédito o información sanitaria. Existen empresas que tienen agentes externos que rigen o auditan su capacidad de resguardo y seguridad de la información para el beneficio de los clientes (AWS, 2018).

Es necesario entender que la responsabilidad de la seguridad del almacenamiento en la nube está a cargo de los actores que intervienen. Por un lado el proveedor de la infraestructura informática donde se hospeda los programas siguiendo el modelo de Cloud Computing. El cliente el cual contrata el servicio en la nube y el usuario final que utiliza el programa o a la

información de acuerdo a los requerimientos y autorizaciones requeridas por el cliente (Programación Integral, 2018)

Así como lo define Pérez et al (2011) una empresa o entidad utiliza las capacidades de la computación en la nube, necesita que el administrador del sistema establezca un correcto control de acceso para garantizar que los usuarios solo utilizan los datos o procesos para los que han sido autorizados.

Control de acceso

Gemalto (2018) manifiesta que cuando los datos y las aplicaciones se trasladan a la nube, el acceso de los usuarios se efectúa por defecto de forma remota. Por lo tanto, las organizaciones deben aplicar controles de acceso para los recursos empresariales que residen tanto en la nube como dentro de los límites del centro de datos. Con los perímetros de seguridad empresarial cada vez más borrosos, las organizaciones tienen dificultades para costear, implementar y gestionar políticas de acceso unificadas y coherentes para los recursos de TI distribuidos.

METODOLOGÍA.

La metodología empleada en el trabajo de investigación es de tipo cuantitativo, porque requirió de datos estadísticos en la bibliografía existente, así como de encuestas realizadas por la autora, la misma que fue aplicada a nivel del Ecuador en las Pequeñas y Medianas Empresas (PYMES), determinando los requerimientos destacados en seguridad para el almacenamiento en la nube de ellas y las tendencias de proveedores a nivel mundial y local. Así mismo

Para alcanzar el objetivo se propusieron varias tareas que se detallan a continuación: se identificó la información actualizada sobre Big data y lo relacionado a las organizaciones, se revisó la bibliografía relacionada al almacenamiento en la nube y los diferentes modelos como son, nube pública, privada e hibrida, y los servicio tales como Iaas, PaaS y SaaS, así como las normas de seguridad para almacenamiento en la nube entre ellas la ISO 27018, ISO 27001 e ISO27002 que regulan el ámbito de gestión de la seguridad de la Información.

Se tomaron como referencia las encuestas realizadas por SADA Systems, que marca la tendencia de las soluciones en la nube de impacto mundial, así como lo expresa Seybert & Petronela (2014), además se realizaron encuestas a once PYMES a nivel del Ecuador de diferentes razones sociales que dieron la facilidad de realizar la respectiva encuesta en su institución. Con esta información se realizó el análisis de las tendencias de almacenamiento en la nube a nivel del mundo y en el Ecuador; posteriormente se estableció la comparación entre ambos análisis para definir los dos proveedores de mayor acogida para el almacenamiento de datos.

Finalmente en base al requerimiento más destacado por las empresas encuestadas sobre la seguridad en el almacenamiento en la nube, se realizó el análisis del acceso a la información a través de comparación entre los dos proveedores de almacenamiento con mayor tendencia de uso y así ese estableció las brechas existentes entre ellos. El alcance de esta investigación es el beneficio que obtienen las empresas y los usuarios sobre las tendencias, características y brechas de seguridad encontradas de los proveedores de almacenamiento en la nube descritos en este trabajo.

ANÁLISIS DE RESULTADOS

En el siguiente apartado se realizó el estudio las encuestas obtenidas a nivel mundial y las realizadas en el Ecuador y fijar los dos proveedores de almacenamiento en la nube con mayor aceptación, a estos dos proveedores se les realizó el análisis comparativo de acceso a la información y se estableció las brechas existentes.

SADA Systems (2016) realizó encuesta a más de gerentes de TI sobre el uso de los servicios

públicos en la nube, y encontró que el 84% de los gerentes de TI encuestados están utilizando la infraestructura de nube pública hoy día, en lugar de los centros de datos corporativos, de esta encuestas se obtuvieron los siguientes resultados: Google Cloud Platform 49%, Microsoft Azure 48%, Amazon Web Services 42 %. Mostrando la tendencia de aceptación de Google Cloud para el 2017.

Según Data Center Market (2018), el ranking de proveedores de IaaS público lo lidera con claridad Amazon Web Services, que el pasado año ingresó por este concepto 12,221 millones de dólares y se llevó algo más de un 51,80% de todo el mercado, a mucha distancia se colocó Microsoft con Azure, seguido de la compañía de Windows que facturó 3,130 millones de dólares, un 13,% del total, el e-commerce chino Alibaba fue el tercer proveedor de la lista, con un 4,6% de cuota, mientas que Google quedó en cuarta posición, con 780 millones y un 3,3% de share.

Tabla 1. Valores del servicio en la nube pública de IaaS en el mundo

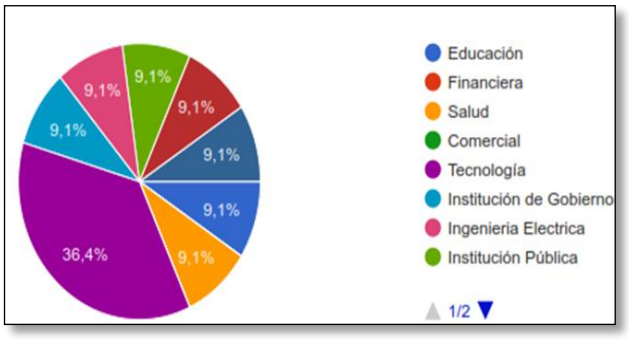
Compañía	Ingresos 2017	2017 Cuota de mercado (%)	Ingresos 2016	2016 Cuota de mercado (%)	Evolución %
Amazon	12.221	51.80	9.775	53.7	25.0
Microsoft	3.130	13.3	1.579	8.7	98.20
Alibaba	1091	4.6	670	3.7	62.70
Google	780	3.3	500	2.7	56.0
Rackspace	457	1.9	297	1.6	53.90
Otro	5.902	25	5.392	29.6	9.50
Total	23.580	100.0	18.213	100.0	29.50

Fuente: Gartner (Agosto 2018)

Con los datos obtenidos, se puede destacar que el posicionamiento en el mercado desde dos puntos diferentes, muestran que, Google Cloud está en el puesto uno, con el 49% de aceptación en el uso la infraestructura de nube pública (Systems, 2016).
Por otro lado, realizando el análisis de mayor rentabilidad económica (Data Center Market, 2018), ubica a Amazon en el puesto uno, con el 51,80% de ingresos con relación a los otros proveedores de servicio en la nube.
Por los datos internacionales analizados se escogieron los proveedores de servicio en la nube a Google Cloud y Amazon.

En el Ecuador se realizaron encuestas online a once PYMES (Anexo 1), de diferente razón social.

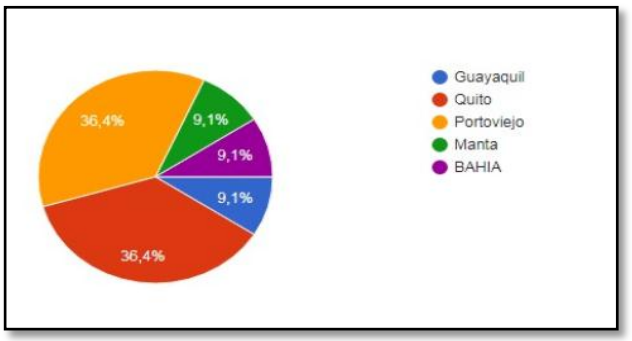
Gráfico1. Dedicación de las PYMES de Ecuador



Fuente: La autora (2018)

El sector dedicado a Tecnología alcanzó el mayor porcentaje de los encuestados el 36.4% significando cuatro de las once empresas en total. El sector de Educación, Financiera, Salud, Comercial, Institución de Gobierno, Ingeniería Eléctrica e Instituciones Públicas en general lograron un porcentaje similar con un 9,1% cada una.
Con los datos estadísticos se demuestra que las PYMES encuestadas están localizadas en diferentes ciudades del Ecuador

Gráfico 2. Dedicación de las PYMES de Ecuador

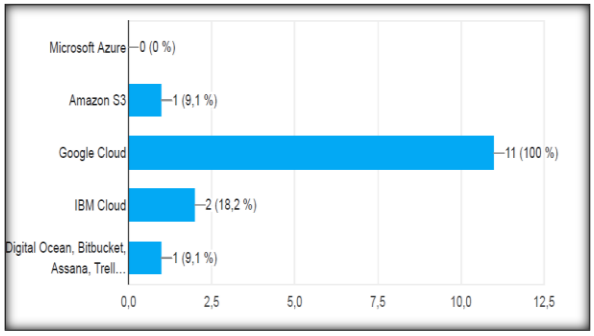


Fuente: La autora (2018)

Las ciudades donde se donde hubo mayor apertura por parte de las empresas para la encuesta realizada fue Quito y Portoviejo con un 36,4% seguido del resto de ciudades Guayaquil, Manta y Bahía con un 9,10% cada una.

Otro de las interrogantes planteada fue concerniente al proveedor de preferencia para el almacenamiento en la nube, obteniendo los resultados que se muestran a continuación:

Gráfico 3. Proveedor de preferencia en las PYMES

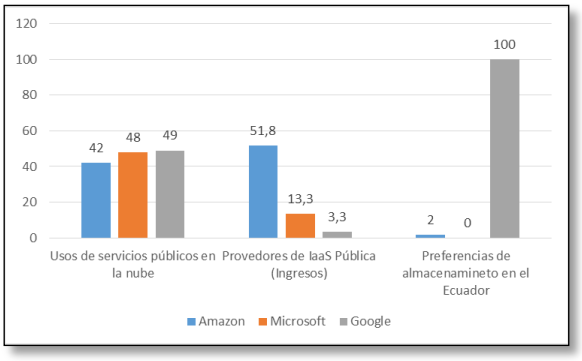


Fuente La autora (2018)

Se destaca que las preferencias al momento de almacenar información en la nube, están entre Google Cloud, IBM y Amazon.

Con los valores analizados en el estudio a nivel mundial y las encuestas planteadas a nivel local (Ecuador), se estable el gráfico estadístico **4** en el cual se compara los diferentes criterios en cuanto a los proveedores de almacenamiento en la nube en los aspectos de uso de servicios públicos en la nube, el análisis de mayor rentabilidad económica y las preferencias de almacenamiento en el Ecuador. Siendo predominantes Amazon y Google Cloud en dos de los tres aspectos analizados.

Gráfico 4. Resultados de encuestas de los aspectos analizados



Fuente La autora (2018)

Con base en el gráfico anterior se puede observar que Google es el de mayor uso dentro de los servicios públicos en la nube a nivel internacional y con mayor preferencia a nivel de las PYMES en el Ecuador, a su vez Amazon es destacado por su uso a nivel internacional y la empresa con mayor rentabilidad en los últimos años (Data Center Market, 2018).
Por tanto, Google Cloud y Amazon, servirán como punto de referencia para el análisis del acceso a la información en la nube y establecer las brechas existentes entre ellas.

Herrera (2011) indica que la protección de la privacidad en la nube es similar a la protección de la privacidad de datos en general. También está involucrada en cada etapa del ciclo de vida de los datos. Pero a causa de la apertura y los "multi-usuarios" característico de cloud computing, el contenido de la protección de la privacidad en la nube tiene sus particularidades, por lo que define el Modelo de seguridad SPI en el cual detalla cuatro aspectos generales de la arquitectura: Software de Seguridad, Plataforma de Seguridad, Infraestructura de Seguridad, Auditoría y Cumplimiento.

Tomando como referencia lo antes indicado y luego de la elección de las dos soluciones de almacenamiento en la nube Google Cloud y Amazon, se realizó la revisión comparativa entre estos dos proveedores en la identidad y acceso.

Análisis comparativo entre Google Cloud Platform (GCP) y Amazon (AWS)

AMAZON (AWS)

El proveedor configura múltiples cuentas para cada equipo, a los mismos que asigna permisos y políticas en cada cuenta. Reduce la complejidad de administrar múltiples cuentas, configurando la facturación consolidada e implementando las organizaciones de AWS.

Identidades

Cuenta de Usuario o Identidades de usuarios finales

AWS divide en dos grupos las identidades para acceder a los recursos ingresados en la nube.

El primero es la identidad del usuario final, constituida por su inicio de sesión corporativo habitual. Estos usuarios finales también pueden representarse mediante el uso de cuentas de IAM (Identity and Access Management). AWS administra la cuenta raíz que es una obligación para cada cuenta creada. Además, brinda una lista de mejores prácticas para ayudar a proteger las claves de acceso raíz de su cuenta. Entre las mejores prácticas para proteger la clave de acceso a la cuenta de AWS están:

- Crear una cuenta de usuario en AWS cuando sea absolutamente necesario. En caso de hacerlo, crear un usuario en IAM que tenga privilegios administrativos.
- El usuario debe eliminar su clave de usuario si no la requiere, en caso de conservarla debe cambiar la clave de acceso regularmente.
- No comparta su contraseña de cuenta de AWS ni las claves de acceso con nadie.
- Use una contraseña segura para ayudar a proteger el acceso a la cuenta de AWS.
- Habilite la autenticación de múltiples factores de AWS, Autenticación multifactor (MFA) en su cuenta de AWS. Para obtener más información.
- Para permitir el acceso a sus recursos de nube de AWS, puede configurar usuarios de IAM, que son identidades creadas dentro de AWS, o puede configurar la federación desde su directorio corporativo (AWS, 2018).

Cuentas de servicio o identidades programáticas

En segundo lugar, las identidades programáticas, permiten que el código de la aplicación acceda a los recursos de la nube, en AWS, si se llaman a las API desde un recurso informático que no pertenece a AWS, se deben crear un usuario IAM.

Cuando se crea un perfil de instancia que esté adjuntado a la instancia, se debe emplear la identidad programática en una instancia de nube programática elástica (EC2), teniendo que estar el perfil en una función IAM y puede proporcionar las credenciales de la función a una aplicación que se ejecuta en la instancia. Un rol de IAM en AWS, permite que un usuario, un grupo o una aplicación ejecutada en EC2 o en un dispositivo móvil asuma los permisos definidos por el rol, es decir que las credenciales transitorias se crean y se aplican a la entidad que asume el rol (AW, 2018).

Autorización o Atribución de permisos políticas de Amazon Web Services

Se debe tener en cuenta que una colección de permisos para Google Cloud Platform (GCP) se llama rol, mientras que para AWS se llama política. Las políticas administrativas de AWS, son aquellas políticas autónomas de AWS IAM, que se unen a varios grupos o usuarios. Las políticas administrativas pueden ser administradas por AWS o creada y administrada desde la cuenta del usuario desde AWS. Además de adjuntar la política a una identidad, lo puede hacer también a un recurso. AWS está constituido por una serie de recursos, es decir, un usuario de IAM es un recurso. Cuando utiliza AWS API, AWS CLI o AWS Management Console para realizar una acción tal como la creación de usuario, este envía una solicitud para esa acción, luego verifica que el principal esté autenticado y autorizado para realizar la acción especificada en el recurso. Durante la autorización, AWS evalúa las políticas que se aplican a su contexto de solicitud en función del tipo y categoría de política, AWS admite

políticas basadas en identidad, políticas basadas en recursos (AWS, 2018).

Google Cloud

Google Cloud Platform otorga permisos a usuarios, grupos y aplicaciones. Estos logran que la entidad autorizada tenga un acceso claramente definido a sus recursos en la nube, no confundir con los permisos que les da a sus clientes para acceder a sus aplicaciones. Brinda recursos de que permiten agrupar y organizar de una forma aquellos insumos encapsulados como Google Cloud Pub / Sub topics, máquinas virtuales (VM) de Google Compute Engine para así administrar la configuración, el control y el acceso. Los recursos de Cloud Platform forman parte del proyecto. Una cuenta individual puede administrar varios proyectos, los proyectos pueden ser administrados por separado o en un recurso de la organización (Google Cloud, 2018) .

Identidades

Cuenta de Usuario o Identidades del usuario final es aquella que se representan por los inicios de sesiones corporativas usuales.

Acceso de usuario final en Cloud Platform

Cloud Platform, tiene dos opciones principales para asignar la propiedad del proyecto: Creando un proyecto que tenga uno o varios propietarios con acceso completo a recursos del mismo y la segunda, teniendo proyectos que no posean propietario específico. Cloud IAM no permite administrar identidades de usuario final en Google Cloud sin embargo permite establecer acceso a los usuarios que crea y los administra por otros medios. Google Cloud IAM, concede permiso para el acceso a los miembros de; Cuenta Google, Cuenta de servicio, Grupo de Google, Dominio de G Suite y Dominio de Identidades de nube. El usuario de GCP que no emplea el dominio de G Suite para administrar a sus usuarios, puede federar su subconjunto existente de usuarios operacionales de muchos directorios de usuarios populares como Active Directory. Ayudando esta orientación el uso de identidades corporativas existentes (Google Cloud, 2017).

Identidades programáticas en Cloud Platform

La cuenta de servicios en Cloud Platform son cuentas especiales que las aplicaciones pueden emplear a través de programación a los servicios de Google, estas cuentas pertenecen a la aplicación de Compute Engine, en lugar del usuario final, esta cuenta de servicio puede contener hasta dos claves de cuenta de servicio, las mismas que son usadas para su autenticación en Google, conservando el usuario recibe la clave privada y Google conserva la clave pública, se pueden crear cuentas de servicios personalizadas en proyectos de GCP, empleando GCP Console, Cloud IAM, Apl o gcloud. Una de las ventajas de las cuentas de servicio de Cloud IAM es de tratar como recurso a una identidad, esta cuenta de servicio tiene una identidad y el usuario le da los permisos al otorgarle un rol para acceder al recurso tal es el caso de un proyecto (Google Cloud, 2017).

Autorización o Atribución de permisos políticas de Google Cloud Platform

Cloud Platform usa los términos rol y política, una colección de permisos en Cloud Platform se llama rol, GCP facilita una descripción general de la Administración de identidades y accesos (IAM) y su uso para controlar el acceso a depósitos y objetos en Cloud Storage (Google Cloud, 2018)

Cloud Storage, muestra las opciones de control de acceso, las mismas que se detallan: Permisos de Identity and Access Management (IAM) : Otorgue acceso a los depósitos y acceso masivo a los objetos de un contenedor, los permisos de IAM le brindan un amplio control sobre sus proyectos, pero no un control preciso sobre los objetos individuales, Listas de control de acceso (ACL) otorgar acceso de lectura o escritura a usuarios para objetos individuales, en la mayoría de los casos, debe usar permisos

IAM en lugar de ACL. URLs firmadas (autenticación de cadena de consulta), permite acceso de lectura o escritura de tiempo limitado a un objeto a través de una URL (Google Cloud, 2017).

Al usar permisos IAM proporciona control de acceso de nivel empresarial en toda Google Cloud Platform y permite permisos otorgados a recursos principales, como proyectos, para ser heredado por recursos secundarios, como cubos y objetos (Google Cloud, 2018).

Gestión de identidad y acceso			
Idetificación y Autenticación	Cuenta de Usuario o Identidades de usuarios finales	Amazon	Administrado en IAM. AWS administra la cuenta de raíz, obligación para cada cuenta creada Identidad federada al sistema de gestión de identidad externa
		Google Cloud	Administrado fuera del servicio Cloud IAM.Cloud IAM concede permiso para los miembros. Identidad federada al sistema de gestión de identidad externa
	Cuentas de servicio o identidades programáticas	Amazon	Rol de IAM y perfil de instancia. EL código de aplicación accede a los recursos de la nube. Las credenciales transistorias se crean en la entidad que asume el rol. AWS autenticación multifactor, es para cuenta con privilegio incluye opciones para autenticadores basado en hardware
		Google Cloud	Cuenta de Servicio Cloud IAM. La cuenta de servicio posee hasta dos claves de cuenta se servicio. Trata como recurso a una identidad.
Autorización	Autorización o Atribución de permisos	Amazon	Políticas Políticas Administradas, Evalúa las políticas que se aplica. Admite política basada en identidad
		Google Cloud	Roles Roles Predefinidos. Facilita la descripción de la Administración de identidades y acceso
	Políticas	Amazon	Documento que enumera explicitamente los permisos Política Adjunta un usuario o grupo de IAM o recurso
		Google Cloud	Lista de enlaces. Un enlace vincula una lista de miembros a un rol. Política adjunta al recurso

Tabla 2. Comparativa de gestión de identidad y acceso.

Fuente: La autora

Análisis de la tabla 2. Comparativa de gestión de identidad y acceso

1. El Primer análisis de la tabla antes expuesta determina que ambos proveedores aportan soluciones para los distintos tipos de necesidad que tengamos con lo que respecta en identidad y acceso.

2. Con respecto a la identidad de usuarios ambos proveedores presentan fortalezas, como es el administrado IAM, pero que a su vez se torna en una brecha de seguridad si no se posee el conocimiento para administrarla. Amazon por su parte permite la administración de usuarios en IAM, como permite administrar la cuenta raíz debe manejarse buenas prácticas para así evitar el acceso a la cuenta AWS. Entorno a Google los usuarios finales son administrados fuera del servicio Cloud IAM por lo que la robustez de las cuentas de usuarios finales sino es bien administrada por la entidad podrían permitir dejar una brecha de seguridad.

3. Google Cloud y Amazon cuentan un beneficio que añade seguridad extra al proceso de autenticación, eso es denominado autenticación Multifactor, pese a ello debe ser configurado por la entidad o administrador y en el caso de Amazon es para cuentas con privilegios, no todas. Así como en el anterior apartado el desconocimiento de la administración de esta gran solución para el almacenamiento en la nube puede privar de reforzamiento de seguridades a las empresas.

CONCLUSIONES

De los resultados estadísticos obtenidos por empresas internacionales y a las PYMES de Ecuador se estableció que las preferencias en proveedores de almacenamiento en la nube, se encuentra entre Google Cloud y Amazon.

Los proveedores de soluciones en la nube para Big Data, Amazon y Google Cloud están posicionados en el mercado nacional e internacional por ofertar, múltiples soluciones a los requerimientos del cliente, entre ellas robustez en la autenticación y administración de permisos.

En seguridad de almacenamiento de datos existen elementos comunes que todas las organizaciones deben tener en cuenta a la hora de aplicar sus medidas: las personas, los procesos y la tecnología. Google Cloud y Amazon demuestran en sus criterios de Autenticación y Autorización o Permisos, ser

dos grandes compañías de almacenamiento en la nube (Tabla 2). El análisis comparativo demuestra que una de las brechas de seguridad que puede existir en el almacenamiento en la nube con los proveedores mencionados es el desconocimiento de la administración y de los múltiples recursos que estos poseen, que serían una puerta de acceso a los ataques y en parte ser una vulnerabilidad para el proveedor y la empresa.

El presente estudio tuvo algunos limitantes, entre ellos el contacto con las PYMES que fueron encuestadas, por encontrarse en diferentes lugares del país, se decidió realizar las encuestas de forma electrónica, a su vez pese a que existen análisis comparativos realizados de los proveedores de almacenamiento en la nube es escaza la bibliografía que detalle la identidad y acceso en los proveedores seleccionados.

En el estudio de las encuestas aplicadas a las PYMES del Ecuador, podría sugerirse como una investigación futura el profundizar el análisis de brechas de seguridad en el acceso para almacenamiento en la nube focalizándolo hacia el cumplimiento de alguna norma que respalda estas seguridades.

Referencia Bibliográfica

Amazon Web Services. (2018). Recuperado el 28 de 08 de 2018

Areitio, J. (2010). Protección del Cloud Computing en. *REE* , 42-48.

Ávila, O. (2011). Coputación en la Nube. *Contactos 80*, 45-52.

AWS. (2018). *Amazon S3*. Recuperado el 28 de agosto de 2018, de Almacenamiento de objetos creado para almacenar y recuperar cualquier volumen de datos desde cualquier ubucación: https://aws.amazon.com/es/s3/

AWS. (2018). *AWS.* Recuperado el 30 de agosto de 2018, de AWS Identity and Access Management: https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/iam-ug.pdf#reference_policies_examples_ec2_instances-subnet

AWS. (2018). *Bloquee sus claves de acceso de usuario root de la cuenta de AWS*. Recuperado el 28 de Agosto de 2018, de https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials

AWS. (2018). *Control de acceso mediante políticas*. Recuperado el 25 de agosto de 2018, de https://docs.aws.amazon.com/IAM/latest/UserGuide/access_controlling.html#TypesPermissions

AWS. (2018). *The Beginner´s Guide to Cloud Security*. Recuperado el 28 de agosto de 2018, de

https://aws.amazon.com/es/security/introduction-to-cloud-security/

Camargo, J., Camargo, J., & Joyanes, L. (2015). Conociendo Big Data. *Facultad de Ingeniería (Fac.Ing.)*, 63-77.

Data Center Market. (22 de agosto de 2018). El mercado mundial de servicios de nube pública IaaS creció casi un 30% en 2017.

Dean, D., & Saleh, T. (2010). Captar el verdadero valor del 'cloud computing'. *Harvard deusto business review*, 35-46.

Fernandez, C. (2012). Algunos retos de la protección de datos en la sociedad del conocimiento, especial detenimiento en la computación en la nube(Cloud Computing). *Revista de derecho UNEC*, 125-145.

Fernández, C., & Recio, M. (2018). *Privacidad Elevada a la nube.* Recuperado el 2018 de julio de 15, de https://portal.aenormas.aenor.com/revista/pdf/nov15/20nov15.pdf

Galmes, A. (enero de 2016). *openacces.* Recuperado el 18 de agosto de 2018, de Sobre la Seguridad de almacenamiento en la Nube: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/45887/1/Agalmesh_TFM_0116.pdf

Gemalto. (2018). *Seguridad de SaaS:control de acceso a la nube* . Recuperado el 26 de agosto de 2018, de https://safenet.gemalto.es/cloud-data-security/saas-security-cloud-access-control/

Gómez, Á. (2017). *Enciclopedia de la Sefuridad informática 2da edición.* España: RA-MA,S.A.

Google Cloud. (enero de 2017). *Google Cloud.* Recuperado el 30 de agosto de 2018, de Google Infrastructure Security Design Overview: https://cloud.google.com/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf?hl=es

Google Cloud. (06 de noviembre de 2017). *Google Cloud*. Recuperado el 24 de julio de 2018, de Productos de Seguridad: 24https://cloud.google.com/iam/docs/overview

Google Cloud. (2017). *La seguridad nuestra prioridad*. Recuperado el 30 de agosto de 2018, de Un nuevo referentee en materia de seguridad y privacidad: https://www.google.com/intl/es/cloud/security/

Google Cloud. (nayo de 2018). *Google Cloud*. Recuperado el 25 de junio de 2018, de Condianza y Seguridad : https://cloud.google.com/security/?hl=es

Google Cloud. (2018). *Google Cloud*. Recuperado el 30 de marzo de 2018, de Opciones de control de Acceso: https://cloud.google.com/storage/docs/access-control/

Google Cloud. (2018). *Resumen para directores de informáticca* . Recuperado el 30 de agosto de 2018, de https://cloud.google.com/security/security-design/?hl=es

Herrera, R. (2011). CLOUD COMPUTING T SEGURIDAD: DESPEJNDO NUBES PARA PROTEGER LOS DATOS PERSONALES. *Revista de Derecho y Cencias Penales*, 43-58.

Hierro, J. (30 de agosto de 2016). *IEBS.* Recuperado el 20 de Abril de 2018, de Uso y empleo del Big Data en las empresas: https://www.iebschool.com/blog/big-data-en-las-empresas-big-data/

IBM. (2017). *IBM*. Recuperado el 18 de febrero de 2018, de What is Big Data Analytics?.: https://www.ibm.com/analytics/hadoop/big-data-analytics

ISO. (2018). *Online Browsing Platform*. Recuperado el 20 de marzo de 2018, de https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en

Joyanes, L. (2016). *Big Data Análisis de Grandes volúmenes de datos en Organizaciones.* México: Alfaomega Grupo Editor S.A.

Kepes, Ben. (2011). *Diversity Limited.* Recuperado el 8 de agosto de 2018, de http://www.diversity.net.nz/wp-content/uploads/2011/03/Understanding-the-Cloud-Computing-Stack.pdf

López, D. (2012). Análisis de las posibilidades de uso de Big Data en las Organizaciones. Cantabria, España.

Management Solution. (2012). *Management Solution.* Recuperado el 06 de julio de 2018, de La nube: oportunidades y retos para los integrantes de la cadena de valor: https://www.managementsolutions.com/sites/default/files/publicaciones/esp/La-nube.pdf

Murillo, M., & Basanta, P. (marzo de 2016). Sistema big data para el análisis de rutas de taxis en NYC. Madrid, España.

Pérez, M. (2015). *BIG DATA Técnicas, Herramientas y aplicaciones.* México: Alfaomega Grupo Editor S.A.

Pérez, P., Gutierrez, C., Eduardo, Á., De la Fuente, S., & García, L. (2011). *Guía para empresas: seguridad y privacidad del cloud computing.* Recuperado el 30 de agosto de 2018, de https://www.leonoticias.com/adjuntos/fichero_63594_20111026.pdf

Programación Integral. (2018). *Programación Integral.* Recuperado el 30 de agosto de 2018, de Seguridad y Privaccidad de Cloud Computing : https://www.programacionintegral.es/actualidad/nos-interesa/item/737-seguridad-y-privacidad-del-cloud-computing#cararct

Puyol, J. (2014). Una aproximacion a Big Data . *Revista de Derecho UNED*, 471-505.

Serrat, R. (noviembre de 2013). BIG DATA-ANÁLISIS DE HERRAMIETAS Y SOLUCIONES. Barcelona, España.

Sevillano. (2013). BIG DATA. *Revista economía Industrial*, 71-86.

Seybert, H., & Petronela, R. (2014). Half of Europeans used the internet on the go and a fifth saved files on internet storage space in 2014. *eurostat*, 1-9.

Suárez, A., Suárez, P., & Abád, C. (2015). Aplicabilidad de las tecnologías de la información de Computación en la Nube en PYMES Ecuatorianas. *Revista Tecnológica ESPOL-RTE*, 361-377.

Sunqu. (2016). *CONCEPTOS Y ECOSISTEMAS BIG DATA.* España: Ticxar.

Systems, S. (2016). *Public Cloud More Secure.* Recuperado el 08 de 09 de 2018, de https://sadasystems.com/2016-public-cloud-survey-infographic.pdf

Vázquez, S. (2015). Tecnologías de almacenamiento de información en el ambiente digital. *e-Ciencias de la Información*, 1-18.