Preparación de Artículos revista Vínculos: Ciencia, Tecnología y Sociedad

Fecha de envío:

Fecha de recepción:

Fecha de aceptación:

Seguridad en la nube, evolución indispensable en el siglo XXI

Security in the cloud, indispensable evolution in the 21st century

Ximena Galindo Ramírez[1] Miguel Andrés Gómez Duarte[2] Jairo Hernández Gutiérrez[3]

Resumen*:* En el presente documento se lleva a cabo una revisión de la literatura sobre la seguridad en la computación en la nube. La incertidumbre e inquietudes respecto a la seguridad de la información y el derecho a la privacidad de los datos de los usuarios de los sistemas que siguen el modelo de la nube, están constantemente en cuestión. El objetivo de la revisión es identificar la seguridad aplicada a la infraestructura, al software y la plataforma de la computación en la nube, desde la cual se identifiquen los servicios que la componen y sea validada su evolución y su impacto tecnológico. Se hace énfasis en el análisis de seguridad de los modelos IaaS, PaaS y SaaS. A partir de una metodología cualitativa de tipo descriptivo se hizo la consulta de 30 documentos, en su mayoría, de tipo investigativo académico. Las conclusiones de la revisión apuntan a que en la medida que se hacen más externos, los modelos de servicio de computación en la nube son más vulnerables respecto a la seguridad. Frente a esto, se plantean algunas estrategias de seguridad que se han desarrollado con el fin de fortalecer estos modelos, principalmente los SaaS, que se consideran sensibles en el tratamiento de la información.

[1] Tecnóloga en sistematización de datos, Universidad Distrital Francisco José de Caldas, Colombia, Bogotá. Afiliación institucional: 3Y Solutions S.A.S., Colombia. Correo electrónico: ximena.galindo.r@gmail.com, ORCID: https://orcid.org/0000-0003-0617-9403

[2] Tecnólogo en sistematización de datos, Universidad Distrital Francisco José de Caldas, Colombia, Bogotá. Afiliación institucional: MILL, Colombia. Correo electrónico: migmz15@gmail.com, ORCID: https://orcid.org/0000-0003-3676-2915

[3]Magister en Administración de empresas con especialidad en dirección de proyectos, especialista en servicios telemáticos e interconexión de redes, Ingeniero de sistemas, Docente de vinculación especial Universidad Distrital Francisco José de Caldas, Colombia, Bogotá. Correo electrónico: jhernandezg@udistrital.edu.co ORCID: https://orcid.org/0000-0003-3908-2763

Palabras clave: computación en la nube, evolución tecnológica, modelos de servicio IaaS, PaaS, SaaS, seguridad en la nube.

Abstract: In this document is carried out a literature review on cloud computing. The uncertainty and concerns regarding the security of information and the right to privacy of the data of users of systems that follow the model of the cloud, are constantly in question. The aim of the review is to identify the security applied to the infrastructure, software and the cloud computing platform, from which the services that compose it are identified and its evolution and its technological impact are validated. Emphasis is placed on the analysis of the IaaS, PaaS and SaaS models. From a qualitative descriptive methodology, 30 documents were consulted, most of them of academic research type. The findings of the review suggest that as they become more external, cloud computing service models are more vulnerable to security. Faced with this, some security strategies are proposed that have been developed in order to strengthen these models, mainly the SaaS, which are the most vulnerable.

Keywords: Cloud computing, technological evolution, IaaS service models, PaaS, SaaS, cloud security.

1. Introducción

Actualmente, y desde inicios del siglo XXI, la computación en la nube o *Cloud Computing* se ha considerado, junto con el resto de las herramientas de la Internet (*Big Data*, Internet de las cosas), un paradigma de la computación disruptivo [1]. A lo largo de casi dos décadas de desarrollo, la Computación en la Nube ha sido implementada en diferentes sectores: educativo, salud, servicios públicos, turismo;

también en pymes y grandes empresas. Esto se debe a que el entorno *Cloud* o "la nube" como sencillamente se le llama aporta múltiples ventajas debido a su versatilidad, flexibilidad y agilidad de los sistemas informáticos [2]. Entre los múltiples beneficios que se le atribuyen, se encuentra su ubicuidad y conveniencia, el hecho de que se ajuste según demanda, y que solamente necesite de una red de computadores (cuyo tamaño depende de las necesidades y recursos) para generar un espacio para compartir recursos. Además, ese conjunto de recursos puede ser aprovisionados y liberados casi de manera inmediata y sin mayor participación por parte de los proveedores o administradores que administren con ellos [3].

Bajo el concepto de "Todo como un servicio" (EaaS, *Everyting as a Service*), la Computación en la nube ha generado impacto significativo en diversos tipos de servicios ofrecidos, como el modelo cliente-servidor y también en infraestructura computacional, como redes, almacenamiento y procesamiento de información. Los servicios del entorno *Cloud* son, en términos generales, de tres tipos: Software como servicio (SaaS), Plataforma como servicio (PaaS) e Infraestructura como servicio (IaaS). Cada uno de estos entornos ha sido implementado en grandes industrias informáticas y tecnológicas como IBM, Microsoft, Oracle, Hewlett-packard, Cisco, y otras más, han incursionado en la oferta de productos y servicios de los servicios mencionados. Esto ha provocado que las operadoras internacionales de telecomunicaciones busquen asociarse con las grandes empresas del internet y las redes como Google, Yahoo, Facebook o Twitter [4].

Aunque parezca una realidad propia de empresas que manejan grandes masas de información, la computación en la nube es mucho más cercana a la realidad de una sola persona. Desde un dispositivo celular, PC o Tablet, una persona puede enviar correos desde su cuenta de Google o Hotmail, mientras escucha música desde una aplicación como Deezer o Spotify, consultar fotografías en Flickr o Pinterest,

y ubicar un lugar desde Google Maps; este conjunto de actividades que se realizan simultáneamente son propias de la computación en la nube. Para poder acceder a ellas, los usuarios solamente requieren de una cuenta de correo, o pueden acceder desde sus cuentas de Facebook. Cada vez que una persona hace uso de alguno de los servicios de la nube, lo cual es una actividad casi continua, queda registrado en la red de almacenamiento masivo de datos. Frente a esta larga lista de beneficios y posibilidades que se abren para el usuario, también se plantean dudas e incertidumbres respecto a la protección y privacidad de sus datos.

Basta recordar una de las noticias más recientes y polémicas protagonizadas por la compañía Facebook, la cual protagonizó un escándalo por permitir la filtración de datos para usos políticos. Según la investigación realizada y publicada por los diarios *The New York Times* y *The Observer*, los datos personales de 50 millones de usuarios de Facebook fueron filtrados y usados por la firma británica *Cambridge Analytica* para influir en la intención de voto en la campaña política de Donald Trump y en la decisión por el Brexit en Reino Unido. A partir de la recolección de datos sobre los gustos, intereses y búsquedas de los 50 millones de usuarios infiltrados, se filtró la información por medio de una aplicación desarrollada por un académico de la Universidad de Cambridge. El problema legal se encontró en que, de esa cantidad de usuarios, solamente 270.000 habían dado su consentimiento para ceder datos sobre su personalidad para investigaciones académicas. El resto de la información fue obtenida sin consentimiento [5].

De acuerdo con lo dicho, la necesidad de desarrollar, perfeccionar y proponer nuevos sistemas de seguridad de la nube es apremiante. La complejidad de esta tarea se encuentra en que, a la vez que las herramientas de internet se perfeccionan día a día para brindar mayores usos y más sofisticación, los ataques también se modifican y reinventan, motivo por el cual resulta difícil identificarlos. Por este

motivo, la investigación sobre este aspecto debe estar orientada en presentar datos, análisis y propuestas que sean actualizadas continuamente [6]. Es necesario recopilar los aportes existentes y desarrollar nuevas soluciones y alternativas sobre la base de experiencias positivas y las que no, con el fin de fortalecer la seguridad de la comunidad digital. En concreto, se plantea como problemática la necesidad de identificar cuál es el estado de la infraestructura, software y plataforma de servicios de la tecnología en la nube, por lo que también resulta clave rastrear en su evolución cuál ha sido su impacto y el desarrollo que ha tenido.

Con el fin de plantear una solución a la problemática enunciada, en el presente documento se realiza una investigación sobre la seguridad aplicada a la infraestructura, al software y la plataforma de la computación en la nube, desde la cual se identifiquen los servicios que la componen y sea validada su evolución y su impacto tecnológico. Para lograr este objetivo, se propone investigar de manera particular cada uno de sus modelos de servicios. En primer lugar, se realizará una evaluación de la seguridad aplicada a los modelos IaaS, PaaS y SaaS. Posteriormente, se analizan las metodologías utilizadas para seguridad en la nube. Con base en la información recolectada es posible integrar los resultados de investigaciones culminadas en el tema de seguridad en la nube para revisar avances, tendencias y retos.

Dentro del alcance de este documento se pretende contribuir con el análisis de las investigaciones publicadas hasta el momento, que resulten más relevantes en relación con el desarrollo de la seguridad en la computación en la nube. Es posible tener una perspectiva amplia del desarrollo que ha tenido esta tecnología, y en qué ámbitos o sectores es en los que se implementa actualmente debido a su demanda, se analiza, uno por uno, los modelos de seguridad IaaS, PaaS y SaaS, orientando sobre el impacto que han tenido e identificando las áreas en las que se pueda mejorar el desempeño. En esta línea, también es

posible identificar cuáles son las proyecciones de la computación en la nube para determinar hacia dónde debe dirigir su mirada la investigación relacionada con la seguridad de esta tecnología.

2. Antecedentes de investigación

Es importante que en el proceso de revisión de literatura se analicen investigaciones similares en las cuales se hayan revisado los mecanismos y principios de seguridad en la nube, con la finalidad de observar los resultados a los que se llegaron. Por ejemplo, en [7], se ha desarrollado una guía con los lineamentos básicos que deben considerar las entidades del Estado para conservar la seguridad en este tipo de ambientes, a partir de estrategias basadas en la prevención y análisis de riesgos. Es clave que las entidades tengan un control de los servidores y la infraestructura a través de la cual se usan los servicios de nube, lo cual genera mayor seguridad sobre la información tratada.

En este sentido, la evaluación se destaca como un componente central de la seguridad en la nube, pues permite conocer cuáles son los activos, recursos e información asociada, así como los responsables de su manejo**.** Se puede decir, por tanto, que de acuerdo con las consideraciones de [7], la seguridad en la nube depende de un control evaluativo de riesgos que permite analizar los controles que se han seleccionado, los aspectos relacionados con el cumplimiento legal y las características asociadas a la información compartida.

Por otro lado, [8] señala que la principal problemática que existe asociada a la seguridad en la nube es que se establece un proceso de materialización de datos a través de contactos, lo cual genera una externalización de la información que limita el control del responsable. Ante esta situación, es clave que las prácticas de negocio en la nube incorporen la seguridad de los datos personales como elemento básico y esencial de la arquitectura. Por otro lado, las medidas de seguridad deben incluir una evaluación integral del ciclo de tratamiento de la información, a través de cada una de las operaciones que se realicen. Se plantea igualmente, la importancia de mantener un enfoque preventivo y de análisis de riesgos, el cual varía de acuerdo con las necesidades y características de cada una de las empresas.

Un antecedente también muy importante es el artículo de [9], en el cual se analizan las respuestas de los niveles de seguridad de la nube cuando se efectúan los siguientes tipos de amenazas:

- Negación de servicios: Que niega el ingreso a la nube por parte de los usuarios autorizados.
- Fuerza bruta: Se busca cuál es la contraseña probando miles de combinaciones.
- Dominio fantasma: Evita que se acabe el tiempo de vida de un subdominio falso en el caché de servidores DNS.
- Llamada telefónica: Ingeniería social para extraer contraseñas.
- Robo de contraseña: Se aprovechan los malos hábitos de cuidado y seguridad de los usuarios para extraer las contraseñas.

Al aplicar estos ataques en una infraestructura generado por medio de la tecnología *cloud computing*, se concluye que:

La vulnerabilidad general de la infraestructura, destacando que el ataque más efectivo de los testeados para vulnerar este tipo de tecnología es el de robo de contraseña., por el contrario, y en positivo, el nivel de seguridad que muestra más robustez tras recibir los cinco ataques diseñados, es el de negación de servicios [9].

De esta manera, se puede observar que la infraestructura *cloud computing* es bastante permeable a los ataques, razón por la cual se recomienda definir con claridad las normas y políticas de uso, realizando además auditorías informáticas que permitan medir la calidad de los activos y de los protocolos de seguridad.

Finalmente, también se resalta el estudio desarrollado por [10], quienes reconocen que el uso de la nube ha generado enormes retos en el mundo organizacional para mantener la privacidad y seguridad de la información, debido al alto nivel de interconexión y conectividad. Son graves los perjuicios que se generan a partir de este conjunto de amenazas a la seguridad, dentro de los que se resalta la suplantación, manipulación de la información, divulgación, cambios en las funciones y alteración.

Por tanto, proponen los autores anterior mente mencionados, mejorar los esquemas y medidas de seguridad en la nube, es preciso considerar que los datos se convierten en información cuando pasan de ser un conjunto abstracto de elementos que dan cuenta de una situación, a representar una solución concreta que ayuda a responder a las necesidades particulares del usuario. Por lo tanto, los datos que son manipulados, transformados y compartidos en la nube deben poseer una alta calidad informática, la cual debe ser protegida mediante sistemas de seguridad que a su vez estén regulados decretos y normas que garanticen su uso y su implementación adecuada.

En síntesis, de acuerdo con los antecedentes que han sido analizados, se puede decir que, sin unas buenas medidas de seguridad, y sin la aplicación de un conjunto de normas y decretos que garanticen la protección de los datos compartidos en la nube, se pueden convertir en sistemas de información vulnerables, por lo cual los datos que contienen pueden ser manipulados por usuarios no autorizados con fines distintos a los cuales fueron en un principio desarrollados.

3. Metodología

La metodología a aplicar para cumplir con estos objetivos es de enfoque cualitativo de tipo descriptivo. Esto quiere decir que se concibe la temática trabajada, la seguridad en la computación en la nube, como un elemento complejo compuesto por múltiples relaciones que impiden tener una sola versión o perspectiva sobre ella. En tanto que se pretende hacer un análisis de cada uno de los elementos que conforman la tecnología en la nube, se reconoce que el diseño, uso y desempeño de estos dependen del modo como las personas, a lo largo de su existencia, la han implementado. Además, lo que se busca es la multiplicidad y diversidad de datos que permitan tener una visión mucho más amplia y, a la vez, profunda del mundo de la tecnología de la nube y su desarrollo en relación con la seguridad.

Se aplica como técnica la revisión de literatura, desde la cual se pretende obtener los datos suficientes para cumplir con los objetivos propuestos. Esta revisión se ha ejecutado a través de la aplicación de una matriz de recolección de información. Las principales fuentes de recolección de información fueron

libros y revistas de tipo investigativo en el cual se realizó un desarrollo teórico y práctico a la computación en la nube. También se han rastreado artículos que comparten las inquietudes planteadas en esta investigación, y plantean antecedentes y aportes significativos con el ánimo de que el documento a presentar sea lo más actualizado posible. Informes emitidos por organizaciones oficiales o no, así como normatividad y documentos guía también son recursos que complementan la información.

Los recursos para acceder a las fuentes son, fundamentalmente, las bases de datos abiertas a las que se accede por internet. Los criterios de búsqueda se establecieron de acuerdo con las categorías de investigación: computación en la nube o *cloud computing*, seguridad o *security cloud computing*, IaaS, PaaS, SaaS. Se dio prioridad a las investigaciones desarrolladas durante los últimos cinco años (se tuvieron en cuenta algunas desarrolladas en años anteriores, sin embargo, que no fueran anteriores a 2010). En total, se realizó la revisión de treinta documentos que, en su mayoría, son artículos investigativos publicados en revistas académicas. Debido al alcance, se seleccionaron documentos escritos en inglés y en español a los que fuera posible acceder sin entrar con suscripciones pagas o con acceso especial. Por lo tanto, toda la información que hace parte del cuerpo de este documento está disponible para su consulta, sin ningún tipo de restricción.

4. Marco Teórico

Las características básicas de la computación en la nube, son recogidas en la definición planteada por el Instituto Nacional de Estándares de Tecnología de los Estados Unidos, [11]:

> La Computación en la nube es un modelo para habilitar el acceso a un conjunto de recursos computacionales (redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo administrativo o interacción del proveedor de servicios. [11].

Por lo tanto, se trata de una herramienta que es proveniente de un lugar indeterminado que solo conoce el proveedor, quien desarrolla el aplicativo para que la herramienta pueda ser utilizada como un servicio en internet. En este sentido, para el usuario es irrelevante conocer el lugar donde encuentra el servidor, sino poder hacer uso de la información y las herramientas que este ofrece cuando lo necesite. La Figura 1 presenta una comparación entre el esquema de funcionamiento de administración y acceso a la información local, que tuvo desarrollo previamente a la computación en la nube, y cómo cambia este esquema con esta nueva herramienta.

Figura 1. Comparación entre el modelo de cómputo local y el modelo de computación en la nube.
Fuente: elaboración propia.

En la primera columna se puede ver un sistema de acceso a información a partir de una red de computadores que se conectaban por un servidor a un proveedor central. Para poder acceder a los datos contenidos por el proveedor había que estar de algún modo físico conectado al servidor, lo que implicaba costos operacionales en la actualización de la tecnología (hardware) y del software, así como el periódico mantenimiento preventivo y correctivo [12]. Por otro lado, “la nube es un sistema computacional paralelo y distribuido que consiste en la interacción y virtualización de recursos que son presentados como uno solo” [12].

Existen cuatro grupos que conforman el conjunto de recursos de este sistema. Se encuentra el hardware (compuesto por un hardware de virtualización y chips de multiprocesador "multi-core"); las tecnologías de internet, conformadas por la web 2.0, los servicios web, la mezcla de múltiples herramientas y el SOA (*Service-Oriented Architecture*); los sistemas de administración, donde se encuentran la computación autónoma y la automatización de la base de datos; y se encuentra la computación distribuida, la cual contiene la computación de utilidad y redes [12].

Los orígenes de este modelo se encuentran, según el relato de [13] en el punto de partida del *Utility Computing*, un concepto desarrollado por John McCarty en 1961 [14], quien propuso que la computación sería la herramienta de trabajo principal del futuro, entonces esta debía estar organizada como un bien de utilidad pública, de manera que se convirtiera en la base de una nueva industria. Posteriormente, en 1969, Leonard Kleinrock [15] pronosticaba que las redes de computación serían más sofisticadas y se expandirían las utilidades de la computación.

Es hasta la mitad de los años 90 que las utilidades de la computación, basadas en el internet, empiezan a presentar un desarrollo de carácter masivo con los sistemas de búsqueda como Google y Yahoo, el surgimiento de las páginas administradoras de correo electrónico, y las plataformas públicas como MySpace, Facebook y Youtube. La pionera en la oferta de servicios aprovisionados remotamente fue Salesforce.com, quien aplicó el concepto dentro de empresas en los años 90. Con el inicio del siglo XXI, Amazon.com lanzó la plataforma *Amazon Web Services* (AWS), un catálogo de servicios dirigidos a empresas que proveía, de manera remota, almacenamiento, recursos computacionales y funcionalidades para negocios.

Ahora bien, el término "*Network Cloud*", "*Cloud*" o "Nube" fue utilizado por primera vez en los inicios de la década de los 90 dentro de la industria de las redes, se trata de una abstracción (aunque más bien parece una alegoría) de los métodos de entrega de datos a través de redes heterogéneas, tanto públicas como privadas, que son presentadas como un paquete de redes. El uso del término *Cloud computing* fue utilizado en el área comercial desde 2006, a partir del lanzamiento de los servicios denominados *Elastic Compute Cloud* (EC2) de Amazon. Se trató de servicios que permitían a las organizaciones alquilar su capacidad de almacenamiento y procesamiento para iniciar emprendimientos relacionados con el desarrollo de aplicaciones. En esta misma fecha, Google Apps inició un proceso similar que, tres años

después, se convirtió en el *Google App Engine*, una de las industrias más poderosas en el desarrollo de tecnologías de la nube [13].

Existen diferentes tipos de nubes, de acuerdo con el servicio que brindan. Las públicas, las cuales están basadas en redes globales de centros de datos cuyos servicios se ofrecen por pago o libremente. Las privadas, que se desarrollan específicamente de acuerdo con el tipo de hardware que dispone la organización que la solicita. Nubes híbridas, en tanto que integran funciones de las nubes públicas y privadas. Y las comunitarias, que se enfocan en la posibilidad de compartir seguridad, privacidad y requisitos para gestionar conjuntamente por varias organizaciones o personas [16].

4.1. Características principales del Cloud Computing

Es posible realizar una síntesis de las características principales del *Cloud Computing*, siguiendo a Kezherashvili. [17]

a. Autoservicio bajo demanda: El usuario es el que determina cuáles de los recursos computacionales ofrecidos quiere aprovisionar, para lo cual solo requiere de un dispositivo de ingreso. No hay necesidad de interacción humana para este proceso.
b. Permite el acceso a la red, bien sea de manera pública o privada: Para esto, el usuario solamente necesita tener acceso a internet, un dispositivo desde el cual acceder a la red. En caso de tratarse de una nube privada, requiere de autorización previa o de una contraseña, la cual es suministrada por el proveedor o el administrador de la red.
c. Asignación de recursos en modo multiusuario: “En el *cloud computing* el proveedor tiene una única aplicación que abre a todos los usuarios que desean utilizarla, estableciendo unos recursos de acceso y prestaciones distintos para cada usuario” [17]. Esto quiere decir que puede existir un número ilimitado de internautas haciendo uso de la misma herramienta, según el tipo de acceso que tenga.
d. Rápido crecimiento: Los proveedores invierten para ofrecer a los usuarios grandes cantidades de almacenamiento que pueden ser ofrecidas de manera ilimitada o limitada gratuitamente. En caso de que la capacidad de almacenamiento sea limitada, el proveedor generalmente ofrece a los usuarios un paquete de capacidad más alto por un costo específico.

e. Servicio medido: La nube integra programas de control automático y optimizado de utilización de dato, los cuales pueden llegar a ser monitoreados y controlados tanto por el proveedor como por el usuario.
f. Elasticidad y escalabilidad: Las aplicaciones de la nube son elásticas en tanto que ofrecen velocidad, son fáciles de utilizar y se adaptan de acuerdo con las necesidades de los usuarios. Son escalables en la medida que se puede hacer un uso de ellas sin importar el cambio en la intensidad de dicho uso, todo depende de la gratuidad del servicio.
g. Seguridad: En principio, los datos suministrados por el usuario para poder hacer uso de las tecnologías de la nube, se encuentran protegidos en *Data Centers*, las cuales son organizaciones que se encargan específicamente de la protección y cuidado de estos datos. Estas empresas se encargan de desarrollar sistemas y programas de seguridad (hardware y software) para cuidar de la integridad de los datos de los usuarios.

4.2. Beneficios y desventajas

Con base en las características enunciadas del *Cloud Computing* es posible identificar tanto los beneficios como las desventajas de este modelo. Entre las ventajas que enuncian los autores consultados que se detienen en desarrollar este aspecto ([12-13],[18]) es posible concretar las siguientes:

En primer lugar, la computación en la nube significa reducción de costos operativos y reducción o eliminación de inversión en esta materia. Tal como se dijo anteriormente, mantener un sistema de redes local implicaba múltiples gastos, los cuales quedan reducidos con las tecnologías de la nube porque los usuarios (empresas o usuarios independientes, e incluso desarrolladores de aplicaciones) ya no se hacen cargo de ellos, sino las grandes empresas proveedoras [18].

Los usuarios tienen acceso a grandes cantidades de capacidad de almacenamiento, así como de aumentar o disminuir el consumo de los recursos (software o hardware) de acuerdo con sus necesidades [19]. También se optimizan recursos informáticos y de energía, pues las plataformas de servicio son tan amplias para recibir a múltiples y, en ocasiones, ilimitados usuarios, a los cuales se garantiza la seguridad, actualización y control constante de las herramientas ofrecidas. En este sentido, como afirman [20], los usuarios pueden invertir su tiempo y recursos “en el traslado de gastos de inversión (CAPEX) a gastos

de operación (OPEX)" [20]. en otras actividades agilizadas por las herramientas que encuentran en la nube. De hecho, con relación al uso de energía, los beneficios son de carácter global en la medida que el *cloud computing* es amigable con el medio ambiente porque las máquinas utilizan menos vatios (de 30 a 2) para hacer uso de las herramientas [21].

En el aspecto económico, por otro tanto, el Informe del Centro para la investigación en economía y negocios dirigido al Parlamento Europeo [22], indica que esta tecnología significa una revolución en relación con el aumento de la productividad que puede tener efectos en la generación de empleo, el desarrollo empresarial y su ventaja competitiva; en este sentido, el *cloud computing* viene a ser una de las herramientas fundamentales para enfrentar la crisis económica causada por la incertidumbre.

Orientado hacia las empresas [20] consideran que otras ventajas tienen que ver con la posibilidad de vincularse con facilidad a los procesos propios de la globalización, debido al acceso fácil y remoto. También se encuentra beneficiada la gestión de personal IT, porque es posible tercerizar el servicio para los usuarios finales. Se reduce la exposición al riesgo de ataques cibernéticos, y la implementación de normas y reglamentaciones de seguridad.

Por otro lado, las desventajas de la computación en la nube se encuentran en aspectos que pueden ser manejables, como la pérdida de control de los sistemas de cómputo, lo que les quita cierta autonomía o independencia a los usuarios; se encuentra la dependencia tanto al acceso a internet como a los proveedores, los cuales, cuando experimentan fallos, pueden afectar la productividad, disponibilidad a las herramientas y la seguridad de los usuarios [19]. En la misma línea, el desarrollo y avance de estas tecnologías dependen del proveedor, por lo que pueden no llegar a responder a las necesidades de los usuarios [18]. También puede verse afectada la productividad del usuario cuando exista dificultades para integrar la tecnología de la nube con los sistemas propios, sobre todo si estos son muy sofisticados o especializados [20].

Finalmente, se hace hincapié en el problema de la seguridad en la administración, protección, control y salvaguardia de los datos personales de los usuarios. Es importante recordar que, para hacer uso de los beneficios de las tecnologías en la nube, los usuarios requieren solamente de una cuenta de correo electrónico, el registro en una red social como Facebook o ingresar su número telefónico. Sin embargo,

tanto la información que puede estar asociada a una cuenta privada a una red social, o los datos de los que se puede disponer con un número telefónico, ya son elementos suficientes para que los criminales cibernéticos busquen robar o vulnerar a los usuarios. De hecho, es necesario resaltar que, ya para el uso de servicios pagos o la realización de transacciones en línea (como pago de facturas, suscripciones o compras por internet), el usuario se arriesga a que sus datos sean interceptados y utilizados de manera ilegal. Por este motivo, de todas las desventajas enunciadas, la relacionada con la seguridad es a la que mayor atención se le ha prestado.

4.3. Modelos de servicio de Cloud Computing: IaaS, PaaS y SaaS

Con el fin de rastrear cómo se gestiona la seguridad dentro de la nube, se realizará una presentación de cada uno de los tres modelos de servicios que se han desarrollado en esta. Se trata de los tres niveles de función de los servicios a los que se puede acceder, los cuales se diferencian por su lógica, que va de la más interna a la más externa: Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS), y Software como servicio (SaaS), tal como se evidencia en la Figura 2.

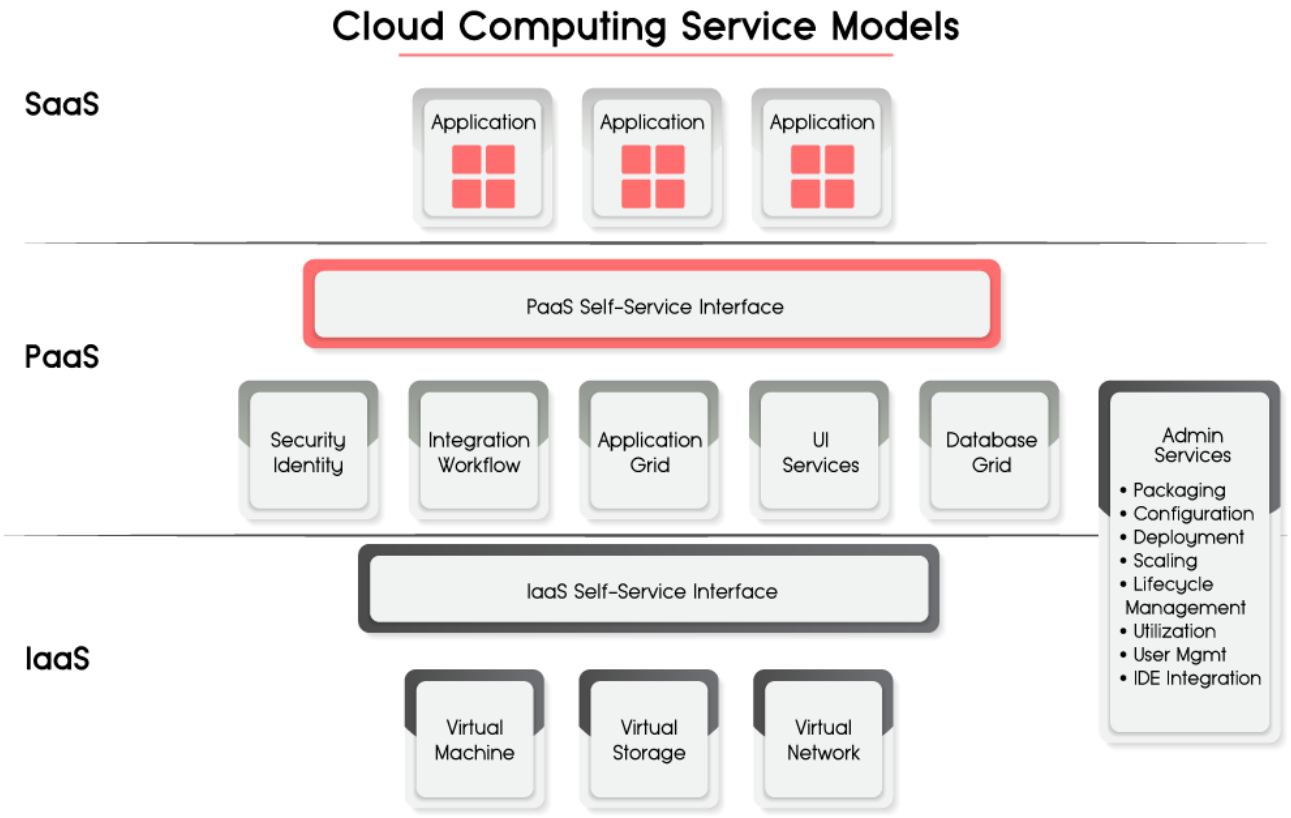

Figura 2. Modelos de servicio de Cloud Computing [23].

A continuación, se presenta cada modelo enfocándose en la seguridad que se presenta para cada uno de ellos. Adicionalmente se mencionarán aspectos como los impactos que ha generado cada uno de ellos, sus costos de implementación, los logros que se han obtenido, sus principales aportes, las metodologías que se han desarrollado para su uso y los ámbitos de funcionamiento.

- **Infraestructura como servicio (IaaS)**

La definición propuesta por el Ministerio de Tecnología de la Información y la Comunicación de Colombia, [24], para este modelo de servicio indica que:

Este modelo de servicio proporciona al consumidor de nube, capacidades de procesamiento, almacenamiento, redes y otros recursos de computación fundamentales donde el consumidor es capaz de desplegar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones [24].

En este caso, el poder del usuario se encuentra en el modo como gestiona los sistemas operativos que hay en la nube y administra el almacenamiento, las aplicaciones y los componentes de red (esto en un nivel limitado y controlado por el proveedor). Entre los servicios de tipo IaaS se encuentran: Copia de seguridad y recuperación, cómputo, redes de distribución de contenido (CDN), gestión de servicios, almacenamiento, computación por lotes, y servicios tecnológicos de Internet de las Cosas (IoT, por sus siglas en inglés).

Los beneficios de IaaS son los siguientes:

En primer lugar, la productividad debido a una transición rápida a la nube, dado que estos sistemas permiten que las empresas de emprendimiento y en fase de crecimiento puedan ofrecer servicios en la nube para sus clientes con muy poca inversión. En segundo lugar, todas las características y los componentes de las aplicaciones o de sus permisos son compatibles con las IaaS. En tercer lugar, las aplicaciones que tienen un gran nivel de control pueden ser construidas en IaaS: "Los desarrolladores y los profesionales de TI tienen acceso a la base de las aplicaciones, a los subsistemas de modo de usuario y al sistema operativo kernel para que la VM se pueda personalizar según las necesidades de los dominios empresariales que atienden" [24]. Finalmente, IaaS ofrece soluciones de portabilidad de los bienes de la aplicación, como la fragmentación del desarrollo en un disco virtual que contiene tanto los sistemas operativos como las aplicaciones desplegadas [25].

- **Plataforma como servicio (PaaS)**

PaaS es un nivel intermedio entre la gestión interna y externa de la computación en la nube. En específico, este modelo toma infraestructura de aplicaciones, sistemas operativos, middleware y detalles de la configuración para que los desarrolladores puedan aprovisionar, desarrollar, crear, probar e implementar aplicaciones sin la necesidad de asistencia de TI. Las herramientas de PaaS son proveídas mediante un sistema de "autoservicio por demanda, recursos, automatización y un contenedor de tiempo de ejecución de plataforma alojada" (p.5). Esto quiere decir que por medio de este modelo no es necesario contar con algún tipo de recurso físico ni copiar archivos de un ambiente a otro para desarrollar la aplicación en tanto que dichos recursos ya se encuentran automatizados [26].

Entre los ejemplos de servicio PaaS se encuentran la inteligencia de negocios, las bases de datos, desarrollos de pruebas a través de plataformas, plataformas para uso de aplicaciones de integración, e implementación de aplicaciones de uso general [24].

Los beneficios que aporta PaaS son, entre otros, las capacidades de escalamiento, que hacen posible que la aplicación acceda directamente a un ambiente IDE por medio de un plug-in y que quede alojada en el contenedor que contiene los recursos, hasta el momento que los requiere. También este modelo ofrece "alta disponibilidad, configuración automática, balanceo de carga y herramientas de administración" [24], Entre sus funciones se encuentra la posibilidad de generar varias copias en la misma nube, sobre todo para aplicaciones que requieran estar aisladas y tener un acceso restringido, finalmente, PaaS permite que las compañías combinen recursos y datos locales personalizados de diferentes servicios Web [27].

La seguridad, en el caso de PaaS, depende de la elección que se haga en orden con los objetivos de la implementación de la organización que la adopta. Por esto, si el objetivo principal es la seguridad de los datos, es necesario tener en cuenta el entorno regulador en el que la aplicación opera o el lugar en donde se encuentran los datos, así como tomar decisiones sobre si los clientes o usuarios están o no autorizados para enviar datos a una aplicación cuando esta no hace parte de su centro de datos [26].

- **Software como servicio (SaaS)**

Se trata de software que se caracteriza por poseer, entregar y administrar a uno o más proveedores de manera remota. Es la versión más externa de la computación en la nube en la medida que el proveedor proporciona el software de acuerdo con unas definiciones de códigos y datos comunes preestablecidos, a los cuales acceden los clientes, en cualquier momento y lugar, con base en el tipo de contrato o suscripción realizada. Por este motivo es que este modelo también recibe el nombre de "*On demand*". Este modelo libera a las empresas usuarias de la carga de tener algún tipo de infraestructura para que sus clientes accedan a sus servicios; las aplicaciones necesarias se encuentran hospedadas en un ISV (Independent Software Vendor), a las cuales el cliente tiene acceso directo, por medio de internet y un dispositivo para usarlas [28].

Se incluyen como soluciones SaaS, las CRM, ERP, cobros y facturación, manejo de información en la web y *e-commerce* [29]. Entre los beneficios de SaaS es posible mencionar que los usuarios no se encargan del mantenimiento, actualización o supervisión de la aplicación. Igualmente, es el proveedor quien debe encargarse de la seguridad y de las copias de seguridad de los datos, esto depende del tipo de contrato establecido por la empresa que lo adquiere. En tanto que es el servicio más externo y expandido, los usuarios registrados pueden acceder a él en cualquier momento y lugar. Estos servicios no requieren instalación ni revisiones iniciales.

Tal como se puede ver, la seguridad en los modelos de servicio *Cloud Computing* varía de acuerdo con el nivel de acceso y despliegue de las mismas. En este sentido, la IaaS son las más seguras en la medida que ofrecen mayor control en la administración de los datos y los componentes de las aplicaciones, mientras que las SaaS son las más propensas a ser vulnerables. Hay que tener en cuenta que las SaaS corresponden al modelo de servicio más difundido y masivo, de allí que se relacionen en mayor medida las ventajas y desventajas enumeradas en el desarrollo del marco teórico de investigación, con estas herramientas. Las PaaS se encuentran en un nivel intermedio, en la medida que se hacen de más fácil acceso, se hacen más vulnerables.

En relación con la implementación, alcances, logros y ámbitos de funcionamiento de los modelos de servicio, es posible enumerar investigaciones que se enfocan en el desarrollo de metodologías y estrategias para contribuir en la gestión de pequeñas y medianas empresas ([10]; [29]; [30]). En el ámbito educativo, se proponen grupos de investigación relacionadas con la infraestructura *Cloud Computing* con el fin de contribuir en el desarrollo de los modelos e implementarlos en diferentes áreas ([3]; [31]), o implementación para fortalecer los procesos educativos de la educación media y superior [32].

Finalmente, los desarrollos específicos sobre seguridad en la computación en la nube tienen los siguientes puntos de enfoque: Por un lado, hay investigaciones que buscan determinar qué tan conscientes son los usuarios de los procesos de sincronización de datos y otros procesos que tienen que ver con sus datos o la información que administran en la nube, los resultados de dichas investigaciones establecen que el 87% de la muestra (250 alumnos) que utiliza la nube siente un nivel de seguridad bueno, el 30% de la muestra no utiliza la nube como respaldo de datos, el 50% de la muestra no se da cuenta de la sincronización de datos que realizan sus dispositivos. Un factor que se denoto fue que el 87% de la

población utiliza claves seguras (contiene letras números y símbolos) de acceso para resguardar sus datos y evitar intromisiones en sus cuentas ya que al no tener bien seguro sus accesos corren el riesgo de que hackeen sus cuentas. [33].

5. Resultados obtenidos

En esta sección se analizó específicamente el tema de seguridad en la nube, de acuerdo con el planteamiento que se ha desarrollado en el marco teórico y el proceso de revisión de literatura.

De acuerdo con [34], en la sociedad de la información la calidad de gestión de los datos compartidos y manipulados a través de herramientas electrónicas y digitales reflejan la gestión administrativa de las entidades e instituciones.

A pesar de ello, de acuerdo con las apreciaciones de [35], a la seguridad que debe tener la información digital muchas veces no se le da la importancia necesaria, pues no se incluye en la estructura orgánica de las entidades, lo que implica que no se inviertan los recursos económicos necesarios para garantizar la protección de los datos, y no se provea un personal capacitado para su óptimo manejo y administración.

A ello se le suma el hecho de que en muchos países no se cuenta a nivel jurídico con una normatividad estricta para proteger la información y los contenidos que se generan y comparten a través de la nube [36]. Otra de las problemáticas que afrontan las personas e instituciones en torno a este tema, explican [34], está directamente asociada a la carencia de un proceso de valoración de la información que cumpla con las necesidades planteadas desde el marco normativo, funcional y estructural de las entidades, generando altos niveles de ineficiencia administrativa, ante la incapacidad de proteger y preservar los intereses de los usuarios.

En este sentido, siguiendo la argumentación planteada por [8], una normatividad eficiente para proteger a este tipo de dispositivos digitales se constituye en la base para formular y reformular procesos, políticas y actividades asociadas a la gestión de la información a nivel social y empresarial.

Ante esta situación, es importante considerar que existen una serie de componentes *Cloud* desde la perspectiva de la seguridad, que permitan mejorar la gestión eficiente de los datos y la información, sin

comprometer la confidencialidad de los usuarios. Dentro de dichos componentes se destacan los siguientes, de acuerdo con el análisis que realizan autores como [37]; y [9]:

- Servicios de aprovisionamiento *cloud*: Este tipo de servicios ayudan a mejorar las capacidades del sistema para reconstituir los servicios y mejorar la provisión en múltiples centros de datos.

- Servicios de almacenamiento de datos *cloud*: Ayudan a generar procesos de replicación automática, a partir de la dispersión de los datos por zonas, estableciendo de esta manera servicios de seguridad y confidencialidad asociados a las necesidades particulares.

- Infraestructura de procesamiento *cloud:* Esta infraestructura ayuda a proteger masters (maquetas para la construcción de los procesadores) y sacar imágenes seguras. De esta manera, se favorece el aislamiento de procesos y multi-arrendamiento de aplicaciones.

- Servicios de soporte *cloud*: Se establecen mecanismos para controlar la seguridad bajo demanda, a través del establecimiento de procesos como el *log in* (controla el acceso individual utilizando credenciales provistas por el usuario) y la utilización de herramientas de firewall.

- Seguridad perimétrica y de red *cloud:* Se desarrollan mecanismos de seguridad contra la denegación de servicios distribuida o DDoS, las capacidades VLAN, la seguridad perimétrica como IAM/IDS/ IPS, firewall y autenticación.

Además de estas componentes, con el fin de mejorar los esquemas y medidas de seguridad en la nube, [8] explica es preciso considerar que los datos se convierten en información cuando pasan de ser un conjunto abstracto de elementos que dan cuenta de una situación, a representar una solución concreta que ayuda a responder a las necesidades particulares del usuario. Por lo tanto, los datos que son manipulados, transformados y compartidos en la nube deben poseer una alta calidad informática, la cual debe ser protegida mediante sistemas de seguridad que a su vez deben ser regulados por decretos y normas que garanticen su uso y su implementación adecuada.

Finalmente, otro factor sumamente relevante para mejorar los procesos de seguridad en la nube, consiste en conocer el ciclo de vida de los datos, lo cual es necesario gestionar la información de manera adecuada, a través de principios que permitan mejorar el uso eficiente. En particular, siguiendo las apreciaciones de [7], se propone el siguiente ciclo de vida de los datos (Figura 3):

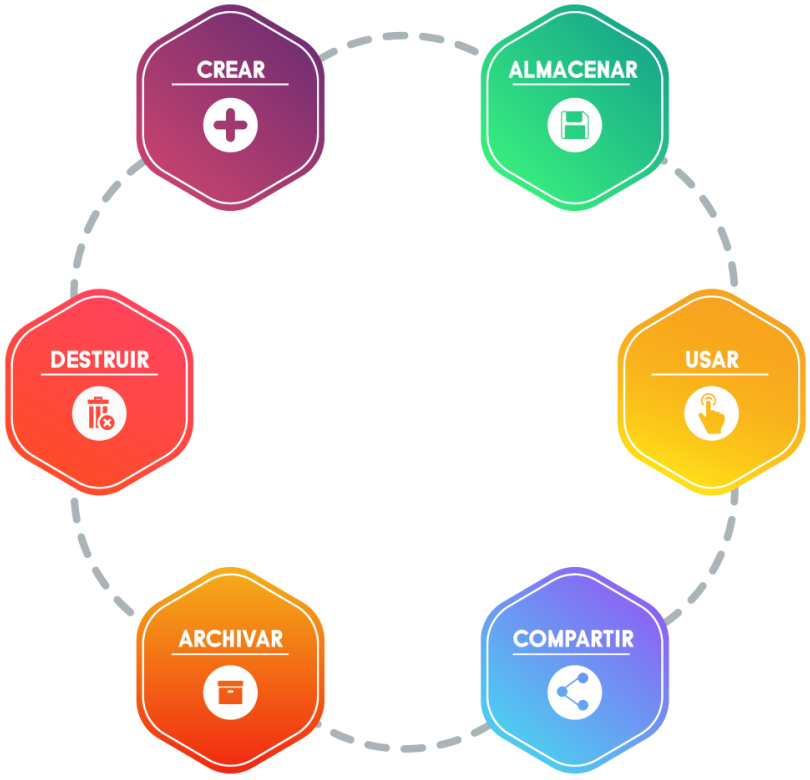

Figura 3. Ciclo de vida de los datos [7].

En una primera instancia los datos se crean esto puede considerarse como un nuevo contenido; el almacenamiento se da cuando se ubican los datos en algún repositorio; el tercer ítem que se refiere a usar los datos va desde la consulta hasta el procesamiento de los mismos; compartir se evidencia cuando la información se transfiere entre personas, entidades o colaboradores; los datos se archivan cuando no se requiere un uso constante de ellos; y finalmente se pasan a destruir cuando ya la información que contienen no se desea volver a usar. El ciclo descrito permite evidenciar que el tratamiento de datos, o en su mayor conjunto, de información, tiene fases que requieren seguridad en sus distintos niveles, hacer

un seguimiento al ciclo de vida se hace relevante en el proceso de la identificación de riesgos de seguridad y con ello la valoración e identificación de controles, cuando para su proceso se consideran servicios en la nube se deben aplicar las consideraciones pertinentes para la protección de datos esto se puede con la inclusión de una arquitectura de almacenamiento *cloud*, del uso de tecnologías apropiadas que soporten mecanismos de cifrado, de autenticación y monitoreo constante.

Los servicios de la nube no existirían si no hubiera información que requiere ser almacenada y de alguna manera procesada y/o transmitida, la investigación realizada permite obtener el amplio panorama que se ha constituido en la sociedad del conocimiento con el tratamiento de la tecnología, es evidente la necesidad que se requiere para asegurar la información desde su forma más simple que se puede denominar como dato, tal como se mencionó previamente es importante conocer el funcionamiento desde el nivel más básico hasta el que pueda considerarse el más complejo para otorgar seguridad. Con el fin de incrementar las capacidades de seguridad en los servicios de la nube, se considera un conjunto que acoge la seguridad de la información con sus pilares, integridad, confidencialidad y disponibilidad, con una arquitectura física que se dote de buenas cualidades tanto en software como hardware, además de estar monitoreando constantemente las posibles vulnerabilidades que pueden afectar a cada servicio o sistema. Actualmente se dispone de métodos, herramientas y dispositivos para dar correspondencia a la seguridad, estos deben ser seleccionados acorde a la necesidad que se presente en cada organización y las implicaciones legales a las que se pueda someter si incurre en fallos de seguridad. Se propone el siguiente esquema para la seguridad de los servicios en la nube (Figura 4):

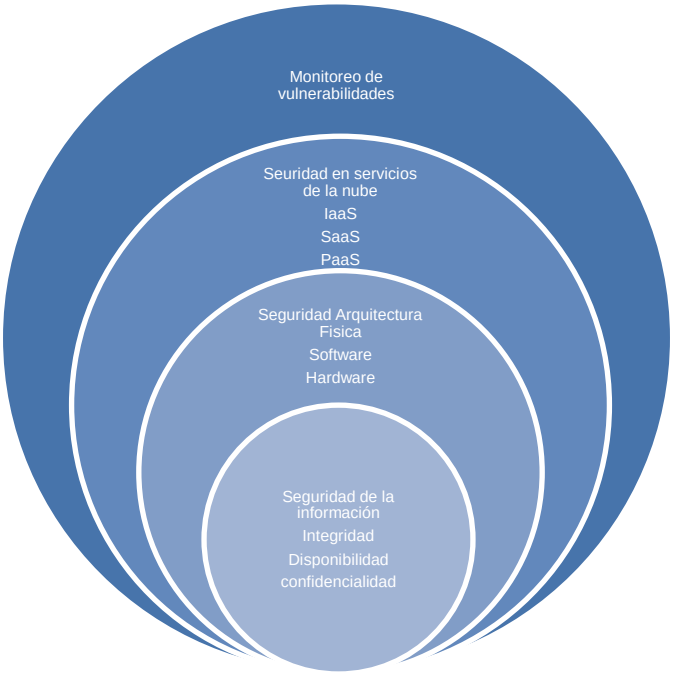

Figura 4. Esquema para la seguridad de los servicios en la nube.
Fuente: elaboración propia.

6. Conclusiones

El *Cloud Computing* (CC) o computación en la nube es una de las más recientes y actualizadas tecnologías de la información y la comunicación que tiene como principal característica el que no es necesario acceder a esta desde un equipo específico. Esto abre las puertas a nuevas posibilidades de desarrollo, productividad y conocimiento, pero también, presenta retos y desafíos en relación con el uso y gestión de datos de los clientes o usuarios que cotidianamente acceden a modelos de servicio, sobre todo los SaaS.

En relación con la problemática sobre la seguridad de estos modelos de servicio, se sigue a [38], quienes consideran que algunos de los problemas de seguridad que enfrenta este sistema son resultado del uso de tecnologías como la virtualización y las aplicaciones. La multi-tenencia y el aislamiento es el principal problema de seguridad en este caso, la cual requiere una solución de orden vertical desde las SaaS hacia

la infraestructura física. El papel de la gestión de seguridad es fundamental para administrar y controlar todos los procesos de seguridad. Finalmente señalan que los modelos de servicio de nube deben tener un sistema de seguridad holístico y envolvente que haga que cada objeto que sea ingresado a la plataforma de nube deba pasar primero por los componentes de seguridad.

Existen diferentes investigaciones que, partiendo de las circunstancias de seguridad que enfrenta cada modelo de servicio, plantean un marco de referencia o algunas estrategias que permitan enfrentar la vulnerabilidad a la que están expuestos los datos de los usuarios de la computación en la nube. [39] proponen un marco de adopción de Cloud Computing para nubes de negocio. Para ello se integran las tres principales tecnologías de seguridad, firewall, administración de identidades y encriptación basada en el desarrollo de tecnologías para sincronizar y compartir archivos. Todo esto en línea con la normatividad y reglamentación existente en relación con la protección de datos. Un marco de seguridad (CCAF, por sus siglas en inglés) multi-legalizado puede ofrecer valor agregado, velocidad y veracidad para los servicios de Big Data operados en la nube. En esta misma línea se orienta la investigación de [40].

Por su parte, [41], consideran que, para garantizar la seguridad del *Cloud Computing*, en cualquiera de sus modelos de servicios, es necesario profundizar en el análisis de los protocolos de acceso y uso de estos para estandarizarlos. De esta investigación es importante resaltar las cuestiones legales y cuasi-legales desarrolladas por McDonald sobre los contratos entre los proveedores y los clientes o usuarios de los servicios de la nube, dado que en ellos se contemplan aspectos como la confidencialidad, la ubicación, la propiedad de los datos, el uso no autorizado de estos y los acuerdos sobre el servicio.

7. Discusión

El análisis que se ha planteado en torno a la seguridad en la nube permite comprender la importancia de establecer mecanismos efectivos que garanticen la privacidad y confidencialidad de los datos y de la información que es adquirida, manipulada y registrada a través de diferentes procesos organizacionales como aquellos referidos al inventario, la logística, el conocimiento del entorno y el relacionamiento con los clientes, y que son administrados a través de entornos digitales y virtuales.

Ante los problemas de seguridad en la nube existen dos factores claves que se deben considerar para mantener y garantizar la confidencialidad y uso adecuado de los datos. En primer lugar, es fundamental que en el diseño de la arquitectura de la nube se reconozca la necesidad de confidencialidad de los usuarios, con el fin de mejorar las cualidades del software y del hardware, limitando de esta manera las posibilidades de filtrar los datos y de acceder a los sistemas operativos que se encuentran interconectados en la red.

En segunda instancia, es preciso fortalecer el marco legal en los países para establecer principios y normas claras de uso de la nube, señalando las penas y sanciones que tendrían que cumplir las personas o atacantes que ingresen de manera no autorizada a los datos. Robustecer el marco legal implica desarrollo estudios que permitan reconocer y entender las funciones que tiene la nube, la manera en que conectan los datos, y las vulnerabilidades a las cuales pueden estar sometidos en medio de los procesos de intercambio de información.

Se pueden reconocer cinco elementos centrales que orientan los procesos y mecanismos y seguridad en la nube:

- Incluir un pensamiento estratégico orientado a la seguridad desde la fase de diseño de la nube.

- Generar un software de actualización continua de los mecanismos de seguridad, teniendo en cuenta que los atacantes desarrollan nuevas formas de atacar y hacer vulnerables los sistemas.

- Desarrollar actualizaciones de información en cuanto a la gestión de vulnerabilidad, además publicar de manera constante resultados en torno a los tipos de ataques que existen.

- Priorizar las medidas de seguridad de acuerdo con los tipos de ataques, y con las principales vulnerabilidades que están encontrando los atacantes en los sistemas.

- Capacitar a todos los fabricantes, distribuidores y desarrolladores en temas asociados a la seguridad, con el fin de generar criterios conjuntos y sólidos de prevención.

En conjunto, siguiendo estos principios es posible avanzar en el desarrollo de esquemas de seguridad más eficientes en el manejo de la nube, lo cual es clave considerando las dinámicas actuales de las organizaciones, el impacto tecnológico y las trasformaciones que se han suscitado en el mundo de acuerdo con el desarrollo de elementos como la interactividad digital, la interconexión y la difusión de información en la red.

Referencias

[1] D. Marinescu, "Cloud Computing". 2nd Edition. City: Morgan Kaufmann, 2017

[2] Deloitte. (s.f.). "El futuro de los servicios Cloud Software como servicio. Resultado encuesta a expertos". [En línea]. Disponible en: https://www2.deloitte.com/es/es/pages/technology/solutions/Servicios%20Cloud.html

[3] M. Murazzo, F. Tinetti, N. Rodríguez y M. Guevara, "Infraestructura de Cloud Computing". 2015 [En línea]. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/46197/Documento_completo.pdf?sequence=1

[4] I. Orozco y O. Jacobs, O. "La nueva era de los negocios: computación en la nube". *Télématique*, vol. 15, no. 2, 2016, pp. 172-191.

[5] R. Ríos, "El escándalo de Facebook y Cambridge Analytica". [En línea] Disponible en: https://www.amic.media/media/files/file_352_1532.pdf

[6] G. Cuzme, "El internet de las cosas y las consideraciones de seguridad", Trabajo de maestría, Quito: Pontifica Universidad Católica del Ecuador, 2015.

[7] MinTIC. "Seguridad y privacidad de la información". [En línea]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

[8] R. Herrera, "Cloud computing y seguridad: despejando nubes para proteger los datos personales". *Revista de Derecho y Ciencias Penales,* vol. 17, no. 4, 2011, 43-58.

[9] J. Heredia, J. Coronel y A. Cortés. "Confiar en una nube: Estudio de Seguridad en Tecnología Cloud Computing utilizando Backtrack 5 y Medusa". *Revista EPN*, vol. *34,* no. 2, 2014, 12-24.

[10] J. Del Vecchio, F. Paternina y C. Henríquez, "La computación en la nube: un modelo para el desarrollo de las empresas". *Prospectiva*, vol. 13, no. 2, 2015, pp. 81-87. [En línea]. Disponible en: https://doi.org/10.15665/rp.v13i2.490

[11] National Institute of Satandars and Technology, NIST. (septiembre de 2011). The NIST definition of Cloud Computing. US Department of Commerce. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[12] Network Startup Resource Center, NSRC. "Diseño de Redes Universitarias, de Educación e Investigación. Computación en la nube" [En línea]. Disponible en: https://nsrc.org/.../WALC2013%20-%20Cloud%20Computing%20-%20Final.pdf

[13] T. Erl, M. Zaigham y R. Puttini, "Cloud Computing". Concepts, Technology & Architecture. Massachusetts: Prentice Hall, 2013.

[14] Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G., & Vakali, A. (2009). Cloud computing: Distributed internet computing for IT and scientific research. IEEE Internet computing, 13(5), 10-13.

[15] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. ACM SIGCOMM Computer Communication Review, 39(5), 22-31.

[16] E. García, "Computo en las nubes, características y beneficios". Cuba y la nube. 6, Especial UNICA, 2017, pp. 15-30.

[17] Gerla, M., & Kleinrock, L. (2011). Vehicular networks and the future of the mobile internet. Computer Networks, 55(2), 457-469.

[18] W. Diaz, "Computación en la nube y su seguridad". Universidad Piloto de Colombia. [En línea]. Disponible en: http://polux.unipiloto.edu.co:8080/00002645.pdf

[19] Autoridad Nacional para la Innovación Gubernamental. "Cloud Computing". [En línea]. Disponible en: http://www.innovacion.gob.pa/descargas/FAQ_CloudComputing.pdf

[20] C. Varela, J. Portella y L. Pallares, "Computación en la nube: un nuevo paradigma en las tecnologías de la información y la comunicación". *Redes de ingeniería*, volumen especial, pp. 138-146. [en línea]. Disponible en: http://revistas.udistrital.edu.co/ojs/index.php/REDES/index

[21] H. Barrios, C. Lucero y A. Veras. "Computación en la nube". Chile, Universidad Técnica Federico Santa María, 2009 [En línea]. Disponible en: http://profesores.elo.utfsm.cl/~agv/elo322/1s09/project/reports/ComputacionEnLaNube.pdf

[22] Centre for economics and burisness research. "The cloud dividend: Part one. The economic benefits of cloud computing to business and the wider EMEA economy France, Germany, Italy, Spain and the UK" [En línea]. Disponible en: https://uk.emc.com/collateral/microsites/2010/cloud-dividend/cloud-dividend-report.pdf

[23] Oracle. "Infraestructure as a Service (IaaS). Cloud Computing for Enterprises. Oracle Corporation". 2010 [En línea]. Disponible en: https://www.oracle.com/technetwork/topics/cloud/whatsnew/iaas-systems-300325.pdf

[24] MinTICic. "G.ST.02 Guía de Computación en la nube. Arquitectura TI Colombia". Marco de Referencia, versión 1, pp. 1-44, 2017. [En línea]. Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html

[25] Craun, B. (noviembre de 2016). Cloud computing, IaaS and PaaS. *The RND Group, Inc.* [En línea]. Disponible en: http://www.rndgroup.com/content/publications/cloud-computing-iaas-and-paas/index.html

[26] Redhat. (2016). "Plataforma como servicio o PaaS, devops e integración de aplicaciones". Red Hat Enterprise Linux. [En línea]. Disponible en: https://www.redhat.com/cms/managed-files/so-paas-devops-application-integration-ebook-inc0280109-150dpi-es.pdf

[27] Intel. "¿Qué es PaaS?" Documento Técnico. Intel IT Center, 2014 [En línea]. Disponible en: https://www.intel.la/content/www/xl/es/cloud-computing/cloud-computing-what-is-paas-cloud-demand-paper.html

[28] M. Moreno, "Computación en la Nube". Serie Documentos de Trabajo, 2015, pp. 1-18.

[29] Plazas, M. y Romero, F. (2016). Implementación de SaaS por parte de las MiPymes en Colombia: caso aplicado en el sector de sistemas hidráulicos y equipos de bombeo. [Trabajo de grado]. Bogotá: Universidad Católica de Colombia. [En línea]. Disponible en: https://doi.org/10.17533/udea.rfnsp.v34n2a09

[30] Wilches, J. Moreno, F y Gonzalez, A. "Desarrollo de una metodología que ayude a las empresas pequeñas en colombia en la toma de decisiones para la tercerización de software como servicio (saas) e infraestructura como servicio (iaas)." (2017). [Especialización en gerencia de tecnología]. Bogotá: Universidad EAN. [En línea]. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/9047/MorenoFernando2017.pdf?sequence=1

[31] M. Murazzo y N. Rodríguez, "Evaluación del Impacto de Migración al Cloud". (2016) . Departamento e Instituto de Informática – UNSJ – Facultad de Ciencias Exactas, Físicas y Naturales. Complejo Universitario Islas Malvinas.

[32] S. Torres, "Educación en la nube. Un nuevo reto para los docentes de Educación Media Superior. Revista Iberoamericana para la Investigación y el Desarrollo Educativo", 2007, pp. 1-17. [En línea]. Disponible en: https://doi.org/10.23913/ride.v7i13.246

[33] C. Ortega, J. Ortega, J. Becerra y H. Quintanilla, "Caracterización de la sensación de seguridad de los datos al utilizar sincronización en la nube". Pistas Educativas, 2015, pp. 62-75.

[34] C. Karlof y D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures". *Ad hoc networks, 1*, 2003, pp. 293-315. [En línea]. Disponible en: https://doi.org/10.1016/s1570-8705(03)00008-8

[35] R. Weber, "Internet of things – Governance quo vadis? *Computer law & security review*, vol. *29*, no. 4, 2013, 341- 3. [En línea]. Disponible en: https://doi.org/10.1016/j.clsr.2013.05.010

[36] M. Al-Ameen y J. Liu, "Security and privacy issues in wireless sensor networks for healthcare applications". *Journal of medical systems,* vol. *36*, no. 1, 2012, 93-101. [En línea]. Disponible en: https://doi.org/10.1007/s10916-010-9449-4

[37] A. Areitio, "Protección del Cloud Computing en seguridad y privacidad". *REE,* vol. *2*, no. 4, 2010, 72-89.

[38] M. Morsy, J. Grundy y I. Muller, "An Analysis of the Cloud Computing Security" Problem. Conference: Asia Pacific Cloud Workshop, Australia, 2010.

[39] V. Chang, Y. Kuo y M. Ramachandran, "Cloud Computing Adoption Framework – a security framework for business clouds". Future Gneration Computer System, 57, 2016, pp. 24-41. [En línea]. Disponible en: https://doi.org/10.1016/j.future.2015.09.031

[40] J. González, D. Piccirillli y M. Pollo-Cattaneo, "Modelo de análisis relativo a la protección de datos personales para proyectos de cómputo en la nube. XVIII Workshop de Investigadores en Ciencias de la Computación". [En línea]. Disponible en: http://sedici.unlp.edu.ar/handle/10915/53258

[41] J. Padilla y J. Pinzón, "Estándares para Cloud Computing: estado del arte y análisis de protocolos para varias nubes". *Puente*, vol. 9, no. 2, 2015, pp.33-40.