SEGURIDAD EN SOFTWARE E INFRAESTRUCTURA COMO SERVICIO DE LA COMPUTACIÓN EN LA NUBE.

HECTOR ISAAC HERNANDEZ VERGARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA

ESCUELA DE CIENCIAS BÁSICAS, TEGNOLOGÍA E INGENIERÍA

ECBTI

CEAD MEDELLÍN

MEDELLÍN

2019

SEGURIDAD EN SOFTWARE E INFRAESTRUCTURA COMO SERVICIO EN LA COMPUTACIÓN EN LA NUBE.

HECTOR ISAAC HERNANDEZ VERGARA

MONOGRAFÍA PARA OPTAR POR EL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA

YOLIMA MERCADO

DIRECTORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TEGNOLOGÍA E INGENIERÍA

ECBTI

CEAD MEDELLÍN

MEDELLÍN

2019

CONTENIDO

pág

LISTA DE FIGURAS.

TITULO

SEGURIDAD EN SOFTWARE E INFRAESTRUCTURA COMO SERVICIO DE LA COMPUTACIÓN EN LA NUBE.

INTRODUCCIÓN

En los últimos años la computación en la nube se ha vuelto un modelo novedoso y llamativo para las organizaciones, ya que aparte de apalancar los procesos internos, también tiene un fuerte impacto de manera positiva en el ahorro de los recursos económicos, relacionados con los sistemas de información dentro de las compañías. Este modelo permite y brinda a estas compañías a tener mucho más centralizados sus diferentes servicios tecnológicos otorgando toda la responsabilidad al proveedor de dicho servicio, como la integridad, confidencialidad, disponibilidad y privacidad de la información.

Con el desarrollo de este trabajo se busca identificar de qué forma y por medio de cuales mecanismos o herramientas, los proveedores de servicios de computación en la nube garantizan la seguridad de la información de los diferentes clientes de modo que al momento de llegar a ofrecer uno de estos tipos de servicios, se pueda dar a conocer a los clientes que la seguridad es una de las prioridades de estos proveedores y que identifiquen las ventajas y beneficios que trae migrar sus servicios y procesos internos a un modelo Cloud. Además se busca que las organizaciones que desconfían de la seguridad que ofrece dicho modelo, identifiquen que este sí es un modelo seguro que ofrece la mejor tecnología para protección de los activos de sus clientes y que en ocasiones dicha seguridad es mucho más alta que la que se puede tener en un Datacenter local, por esto es importante conocer las bases y fundamentos de seguridad de esta tecnología para así comprender este modelo como una herramienta para el progreso de las organizaciones.

Cabe resaltar que un modelo basado en cloud computing, genera un sin número de beneficios para las organizaciones y el desarrollo de las actividades de sus empleados, teniendo una disponibilidad de servicios de 24/7, 365 días al año, donde se garanticen las conexiones seguras sin importar ubicación y hora en la que se desee acceder a la información.

1. FORMULACIÓN DEL PROBLEMA

Actualmente existen organizaciones que siguen desconfiando de la seguridad ofrecida por los servicios de la computación en la nube, en la capacidad de proteger la integridad, confidencialidad y disponibilidad de sus servicios, no obstante se logra identificar un problema de confianza, razón por la cual estas organizaciones siguen trabajando de manera tradicional sin saber aún los grandes beneficios y ventajas que trae la computación en la nube.

Este problema surge cuando las organizaciones no están completamente documentadas sobre el tema, cuando no tienen las bases necesarias para tomar una decisión con respecto a una posible migración a la nube, siempre pensando que si la información no se tiene resguardada localmente, esta se encuentra totalmente insegura y se pierde el control sobre la misma, esto sucede en mucha ocasiones cuando se llega a estas compañías a ofrecer mejorar sus plataformas tecnológicas ofreciendo servicios de computación en la nube, y la primer barrera que se encuentra es la desinformación frente a este tema y el temor a las nuevas soluciones, ignorando por completo la cantidad de beneficio que pueden llegar a tener. Es importante que se entienda y reconozca que actualmente el riesgo siempre va a existir independientemente del medio utilizado, pero se busca que se confíe en la computación en la nube y los servicios que ofrece para el crecimiento de las compañías teniendo en cuenta que los beneficios son bastante tangibles en aspectos económicos con relación a espacios físicos, infraestructura y recursos necesarios.

Las empresas actualmente tienen que invertir grandes cantidades de dinero en compra de servidores, equipos de infraestructura de telecomunicaciones, equipos de infraestructura de respaldo eléctrico, personal que esté a cargo del funcionamiento de todo lo anterior (seguridad, mantenimiento, etc), con lo cual tener un centro local de información es muy costoso.

Con la realización de este análisis y estudio se deben buscar respuestas muy concisas y efectivas de cómo tiene la computación en la nube cubiertas todas la dudas que genera respecto a su seguridad, ya que son estas las que hacen que las empresas no se inclinen aún por hacer parte de esta forma de trabajo y constantemente está latente la siguiente incógnita:

¿Por qué en la actualidad se sigue desconfiando de la seguridad que ofrece la computación en la nube para el software y la infraestructura cómo servicio?

2. JUSTIFICACIÓN

Por medio de este análisis, se dará a conocer a las organizaciones las ventajas de adoptar el modelo de la computación en la nube, sus características, atributos y mejoras que pueden aportar para los negocios, donde siempre prevalece el tema de la seguridad para los activos de información de las compañías, analizando cada uno de los autores, sus métodos y mecanismos que ponen a disposición de cada uno de los proveedores de servicios cloud, se busca aclarar cada una de las dudas que se generan con respecto a la seguridad de dicho modelo y el control que ellos mismos (clientes) pueden tener sobre sus datos.

Es muy importante conocer todas las ventajas en el ahorro, tanto de recursos físicos como económicos, ya que estos son una pieza fundamental para toda organización, además, no se puede olvidar que la computación en la nube ofrece una disponibilidad de 7/24, 365 días al año permitiendo el acceso a la información sin importar el lugar o la hora pero lo más importante sin lugar a duda es el dinero que se pueden ahorrar al adoptar este modelo que es realmente significativo.

La revista Dinero " el 62% de las compañías más grandes en Colombia ya usan computación en la nube, principalmente soluciones de mensajería y colaboración, CRM, gestión del talento humano e infraestructura, lo que demuestra una gran penetración del mercado colombiano"[1], esto permitiendo optimizar sus recursos propios, los cuales evidentemente al ser utilizados incrementan los costos de manera significativa, no sólo por el hecho de tener que adecuar plataformas en infraestructura que soporten dichos procesos sino también los costos que genera el mantenimiento y la mano de obra necesaria ante cualquier actualización, falla o ajuste.

Con el desarrollo de este análisis es factible el apoyo a las organizaciones a tener mayor claridad respecto a la seguridad ofrecida para el software y la infraestructura como servicio cloud y logren adoptar este modelo para la mejora del negocio.

---

[1] Dinero. El 62% de las compañías más grandes ya usan cloud computing. [Online]. Bogotá: Empresa. 2012., 1 p. Disponible en internet: <http://www.dinero.com/negocios/tecnologia/articulo/el-62-companias-mas-grandes-usan-cloud-computing/141978>

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Analizar cómo la seguridad ofrecida hoy día por la computación en la nube en los servicios SaaS e IaaS, garantizan la confiabilidad, integridad, y disponibilidad de los datos.

3.2. OBJETIVOS ESPECIFICOS

1. Recopilar información de la situación actual de seguridad sobre los servicios SaaS e IaaS ofrecido por la computación en la nube.

2. Establecer las ventajas y beneficios que ofrece la computación en la nube y de qué forma se pueden ver reflejados en la economía de las empresas.

3. Conocer los métodos y prácticas que ofrece la computación en la nube que garantizan la disponibilidad, confidencialidad y la integridad de la información en los servicios SaaS e IaaS.

4. Analizar el grado de seguridad que ofrecen actualmente los proveedores servicios SaaS e IaaS en la computación en la nube y los diferentes controles para la protección de la información de sus clientes.

4. MARCO DE REFERENCIA

4.1. MARCO TEÓRICO

Todos los modelos de servicio que ofrece la computación en la nube, son bastante llamativos para muchas organizaciones hoy por hoy, pero como todo, existen algunas que no confían y el solo hecho de pensar en no saber el lugar exacto de la ubicación de sus datos, los hace dudar de la seguridad que está tecnología ofrece sobretodo que en la mayoría de las veces el almacenamiento de los datos no es en el mismo país y las leyes para la protección de los datos siempre es diferente, es por eso que Microsoft le da mucha importancia a este tema y lo considera una posible vulnerabilidad a la seguridad de estos servicios. “Esto se vuelve aún más importante cuando se considera el tema del almacenamiento de datos en jurisdicciones donde las leyes de privacidad de datos difieren de las del país anfitrión de la empresa.” [2]

> Actualmente, organismos internacionales líderes en la seguridad informática y gobierno de TI, han adaptado prácticas y técnicas globalmente conocidas a los servicios de la nube. Por ejemplo, ISACA ha publicado diferentes guías basadas en el marco Cobit 5 para la implementación de controles y aseguramiento de la nube. Asimismo, ISO 27001 actualmente cuenta con la versión borrador (ISO/IEC 27017) que sirve de orientación sobre los elementos de seguridad de la información para la computación en nube, incluyendo recomendaciones para la aplicación de los controles de seguridad Específicos[3]

Realizado un estudio solo para países europeos, se identificó que el 6 por ciento de las compañías piensan que la computación en la nube no es más que un tema de una moda que pronto acabará y un 9 por ciento de estas creen que este nuevo modelo, con su evolución dará mucho de qué hablar. Por otra parte el 85 por ciento restantes, son compañías que aún no tiene clara su posición frente a este

[2] SHINDER, Thomas W. Microsoft Reference Architecture for Private Cloud: Cloud Security Introduction. [Online]. Microsoft 2011.,1 p. Disponible en internet: <https://social.technet.microsoft.com/wiki/contents/articles/3801.cloud-security-introduction.aspx>

[3] TÜCKLER, Hjalmar. Evolución de la computación en la nube en AL. [Online]. La prensa 2014.,2 p. Disponible en internet: <https://www.laprensa.com.ni/2014/10/25/economia/215932-evolucion-de-la-computacion-en-la-nube-en-al-telecomunicaciones >

modelo. “El principal motivo esgrimido para esta indecisión está en que no ven claras las ventajas técnicas o el ahorro de costes que se puede conseguir con este tipo de tecnología.”[4]

Por otra parte, en América Latina la computación en la nube está llevando su proceso de adaptación un poco más lento, pero existen algunos países como Brasil, Argentina y algo de Colombia, que han logrado identificar los beneficios y ventajas que trae este modelo para las organizaciones en pro del mejoramiento de sus servicios y por ende la parte económica de sus respectivos negocios.

La mayoría de las preocupaciones empresariales en la implementación de servicios cloud, radica en el sacrificio de sus niveles de seguridad, pero esto se debe normalmente al desconocimiento y la falta de información sobre este nuevo modelo y sus tecnologías. Adoptar este nuevo modelo implica tener un buen asesoramiento y sobretodo tener muy claro qué tipo de proceso se desea llevar a la nube, para así poder seleccionar el servicio adecuado pero sobretodo el proveedor más conveniente, los autores Sumner Blount y Rob Zanella nos mencionan en su obra Cloud Security and Governance: Who's on Your Cloud?, una serie de certificaciones que tienen la gran mayoría de las empresas que prestan este tipo de servicios cloud,

> Al evaluar la infraestructura de seguridad de un proveedor de la nube, analice su conformidad con los marcos, como COSO, CobiT, ISO27001, SAS 70, o cualquier otro marco que pueda ser adecuado para sus necesidades. Si tiene, por ejemplo, un Certificación SAS 70, esto demostrará que ha establecido una infraestructura de seguridad integral y efectiva, que debería proporcionarle con cierta comodidad en cuanto a su capacidad para cumplir con sus requisitos de seguridad.[5]

Esto con el fin de brindar a los clientes un nivel de confianza mucho mayor, para que estos sientan la tranquilidad necesaria al momento de adquirir uno de estos productos y saber que el proveedor seleccionado, cumple con altos estándares de

[4] ROBERTO, Carlos. La desconfianza hacia la nube en las empresas. [Online]. TicPymes. 2011., 1 p. Disponible en internet: <https://www.pymesyautonomos.com/tecnologia/la-desconfianza-hacia-la-nube-en-las-empresas>

[5] BLOUNT, Sumner; ZANELLA, Rob. Cloud Security and Governance: Who's on Your Cloud?. [Online]. IT Governance Publishing. 2010. Base de datos: eBook Collection. Disponible en internet: <http://eds.a.ebscohost.com.consultaremota.upb.edu.co/eds/ebookviewer/ebook/bmxlYmtfXzM5MTEyMF9fQU41?sid=2b007c10-744b-41ed-bb89-b4d54f0918fa@sessionmgr4006&vid=3&format=EB>

calidad con respeto a la seguridad y la protección de la información de cada uno de los diferentes clientes
Por otra parte es importante recalcar que la seguridad que brinda los proveedores de servicios, no se basan en el funcionamiento de diferentes elementos o herramientas tecnológicas, sino en el trabajo conjunto de herramientas tecnológicas, procesos, proveedores y clientes que juntos llevan a cumplir con el porcentaje de seguridad requerido para dichos servicios.

Dentro de los pilares fundamentales para la seguridad y protección de la información se tiene:

Protección de datos y privacidad.
Ésta a su vez está conformada por diferentes elementos de vital importancia para el correcto manejo de esta característica.

- Segregación de los datos: La idea de esta característica es almacenar la información separada de forma segura, es decir, la información se divide y es almacenada en diferentes servidores sean virtuales o no.

- Ubicación de los datos: Esta es una de las grandes características que posee el modelo cloud, ya que con esta garantizan la disponibilidad de los recursos así como también planes de emergencia y de continuidad de negocio ante una posible eventualidad en uno de sus servidores.

- Protección de datos almacenados: Para este tema, se cuenta con diferentes mecanismo de protección, entre ellos uno vital que es la encriptación de información en las bases de datos, pero también existen los controles de acceso, el perfilamiento de usuarios, los logs de auditoria y trazabilidad de cada una de las interacciones con los datos.

- Copia de seguridad: Todos los proveedores de servicios garantizan copias de seguridad periódicas para sus clientes, igualmente, estas siempre son almacenas en diferentes servidores como planes de contingencia para la continuidad de los negocios.

Así mismo se está pasando a transformar el miedo y la desconfianza de las compañías con respecto a este modelo, a una verdadera confianza mediante un hecho de mentalidad por información verídica por parte de otras organizaciones que pasaron por el proceso de migración, donde se debe llevar a los clientes a

entender que disponer del 100 por ciento de los recursos informáticos organizacionales en las propias oficinas o instalaciones, hoy en día es poco rentable, inflexible, aumenta el costos de mantenimiento, es más inseguro y se corre mayor riesgo que si se tienen a nivel cloud.

Más allá de la tecnología que se desee utilizar o del proveedor de servicios, cualquier empresa que esté pensando en la migración de sus procesos de IT al modelo de la computación en la nube, debería analizar una serie de interrogantes, además es fundamental que las empresas definan al detalle una estrategia de transición y conocimiento para luego elaborar un plan de negocio e implantación factible y viable antes de llevar a cabo la transición.

La primera y fundamental es no decir que si subirse o no a este modelo, sino más bien la decisión debería estar entre que subir a la nube. Es así como se deberían identificar todas aquellas actividades críticas pero de mucho valor para la organización identificando la importancia de las tecnologías en estas actividades, así entonces una transición a la nube necesitará de un análisis muy detallado que permita justificar el porqué del cambio de modelo.

Otra pregunta importante que se debe hacer el negocio es, definir que si lo decidido a subir a la nube, que valor ofrece para la compañía y si de verdad fortalecerá algún proceso complejo para la misma.

Un buen plan de transición así la computación en la nube debería tener algunos de los siguientes elementos.

Descubrimiento.

Dentro del descubrimiento es importante tener en cuenta aspectos fundamentales como la identificación de objetivos del negocio y del área de TI frente a los desafíos de hacer una transición a este nuevo modelo, es decir, se deben identificar todas las aplicaciones que son potencialmente factibles a ser trasladadas, analizar las ventaja y desventajas que traen consigo mismo este tipo de procesos y por último se debe determinar e identificar cuáles son las características de las aplicaciones de alto nivel, complejidad para así tener una visión mucho más clara y completa de los procesos en las aplicaciones.

Evaluación.

Dentro del proceso de evaluación ya se comienza con un análisis más a detalle de cada una de las aplicaciones o procesos que se definieron a ser implementados en la nube, se determinan las características de cada una de ellas de manera muy detallada para posteriormente definir un proceso o estrategia para realizar la implantación.

Puesta en Marcha.

Una vez se tiene una versión inicial, se debe realizar una prueba piloto con una muestra de usuarios considerable, la cual abarque cada una de las funcionalidades migradas a la nube. Posteriormente al piloto se deben recopilar las evidencias y hallazgos que arrojó dicho plan para así definir el argumento del negocio para el éxito de la migración. Una vez analizados los posibles puntos a mejorar se puede entonces realizar un piloto completo de las funcionalidades en cada aplicación y así obtener un proceso completo en la nube.

Formación.

Este es uno de los puntos más importantes en la adaptación de cualquier nueva tecnología, más allá de las metodologías o la infraestructura a utilizar, lo primordial siempre van a ser las personas que van a interactuar con dicha tecnología. Es vital para todo negocio que las personas pongan su compromiso, motivación y conocimiento para el éxito de un proceso tan delicado como es un cambio de concepto tecnológico. Es esencial contar con un plan de formación que prepare a los usuarios para el cambio en la tecnología. Para lograr los resultados esperados es fundamental realizar una formación inicial con un equipo de trabajo el cual debe estar aislado y enfocado solo en este nuevo proyecto de transición para así lograr la concentración únicamente el proyecto.

En resumen y como lo mencionan los autores Sumner Blount y Rob Zanella, para la protección y privacidad de la información confidencial, los proveedores de servicios cloud, están enfocando sus esfuerzos en determinar y ofrecer los modelos correctos a cada cliente, “los tipos y la fuerza de sus controles de seguridad. Sus requisitos y procedimientos establecidos para la clasificación,

manejo y retención de los datos guiarán su estrategia completa en torno a estos controles de seguridad clave."[6]

4.3. MARCO CONCEPTUAL

ACTIVOS DE INFORMACIÓN: Estos son todos los elementos que conforman un sistema de información, desde los recursos físicos, como equipo, servidores, datos, y así también los mismos usuarios son catalogados como activos.

AMENAZAS: El término amenaza es una palabra que se utiliza para hacer referencia al riesgo o posible peligro que una situación, un objeto o una circunstancia específica puede conllevar a uno mismo o a terceros.

ATACANTE: Persona u organizaciones que lleva a cabo los diferentes ataques a las organizaciones, buscando sacar provecho de dicha situación, sea por temas económicos, vengativos o simple diversión.

ATAQUES: Un ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.

AUDITORIAS: Las autorías son un mecanismo de control, que buscan por medio de verificaciones analizar el comportamiento de una política establecida y evaluar si estas si están siendo aplicadas y cumplidas por parte de los proveedores.

COMPUTACIÓN EN LA NUBE: Nuevo modelo informático por medio del cual, las organizaciones y personas hacen uso de diferentes recursos sin necesidad de tenerlos ubicados en sus instalaciones, por ejemplo, aplicaciones web, bases de datos, infraestructura lógica e infraestructura física.

CONFIDENCIALIDAD: Característica que busca proteger la información para que no sea interceptada por las personas inadecuadas.

[6] BLOUNT, Sumner; ZANELLA, Rob. Cloud Security and Governance: Who's on Your Cloud?. [Online]. IT Governance Publishing. 2010. Base de datos: eBook Collection. Disponible en internet: <http://eds.a.ebscohost.com.consultaremota.upb.edu.co/eds/ebookviewer/ebook/bmxlYmtfXzM5MTEyMF9fQU41?sid=2b007c10-744b-41ed-bb89-b4d54f0918fa@sessionmgr4006&vid=3&format=EB>

CONTROLES DE SEGURIDAD: Son aquellos mecanismos utilizados por una organización que se encargan de ejecutar las tareas que pretenden proteger los activos de información.

DISPONIBILIDAD: Característica dentro de las tecnologías de la información que busca que un recurso siempre se encuentre disponible para el uso de los usuarios de un sistema.

ELASTICIDAD: Es una característica que permite a los usuarios dependiendo del servicio adquirido aumentar o disminuir los recursos informáticos con los que cuentan según sus necesidades, de la misma forma es posible liberar recursos para que sean utilizados en otros procesos cuando ya no sean necesarios.

ESCALABILIDAD: Es una característica que permite a los usuarios hacer uso de lo estrictamente necesario dentro de una organización a nivel de recursos tecnológicos, es decir, de estar utilizando un porcentaje menor del total de una aplicación se puede pasar a utilizar un cien por ciento con total normalidad, rapidez, y transparencia para usuarios finales.

IAAS: Modelo de servicio ofrecido por la computación en la nube, el cual se refiere a Infraestructura como servicio, el objetivo de este tipo de servicio es proveer a sus clientes un modelo de infraestructura tecnológica en la nube, es decir, le permite a sus clientes la utilización de sus recursos físicos como redes de datos, servidores bases de datos, firewall, entre muchos más.

INTEGRIDAD: Esta es la característica que busca que la información dentro de un sistema de información mantenga siempre su originalidad para garantizar a los usuarios que hagan uso de ella de la veracidad de la misma.

PAAS: Modelo de servicio ofrecido por la computación en la nube, que permite a los usuarios desplegar en la infraestructura adquirida aplicaciones creadas por ellos mismos, permite la utilización de frameworks, kits de herramientas, lenguajes de programación y todas las herramientas que el proveedor pone a su disposición para la construcción de nuevas aplicaciones.

PRIVACIDAD: Los proveedores tienen como obligación, asegurar la información de todos sus clientes, siendo muchos de estos datos críticos como por ejemplo números de tarjetas de crédito, saldos bancarios, extractos, entre muchos más,

toda esta información es enmascarados o encriptados y además, solo los usuarios autorizados son quienes tienen el acceso a los datos en su totalidad.

SAAS: Modelo de servicio ofrecido por la computación en la nube, donde los usuarios pagan para utilizar ciertas aplicaciones sin tener la necesidad de que estas se encuentren instaladas en los servidores de las compañías, sino por el contrario en los servidores del proveedor.

TRANSACCIONES: Acciones que son realizadas dentro de un sistema de información, como por ejemplo consultas, actualizaciones de datos, eliminaciones y cualquier tipo de actividad que genere alteración a la información.

TRAZABILIDAD: Es una característica que se usa para saber los eventos y acciones ocurridas durante un periodo de tiempo, por medio de este elemento es posible la realización de auditorías y controles de seguridad.

VIRTUALIZACIÓN: Mecanismo que permiten la generación de una sola instancia de trabajo o una combinación de muchas, con diferentes sistemas operativos, servidores de red, aplicaciones, entornos informáticos, dispositivos de almacenamiento y otros recursos necesarios.

VULNERABILIDADES: Son todas aquellas debilidades que presentan los activos de información dentro de una organización y las cuales si no son tratadas de forma adecuada pueden llegar a ser contraproducentes para el funcionamiento de los activos.

RSA: Algoritmo que se encarga de cifrar la información de forma asimétrica, el cual provee un servicio de autenticidad e integración de los datos, trabajando con la infraestructura llamada clave pública, que consta de dos clave para verificación de autenticidad con una clave pública y otra privada.

4.3. MARCO LEGAL

Se debe remarcar que para Colombia existen unas series de leyes y normas implementadas que se encargan de juzgar y judicializar a todo aquel individuo que incurra o altera la protección de una u otra forma los sistemas de información tanto privados como públicos, dos de ellas están directamente relacionadas con la seguridad de los servicios ofrecidos por la computación en la nube, y por eso se mencionarán algunas características de ellas:

Ley 1273 de 2009 Nivel Nacional.

La Ley 1273 Del 5 De Enero De 2009 "De La Protección De La Información Y De Los Datos"[7]

Más allá de que la computación en la nube en la gran mayoría de las ocasiones maneja Datacenters fuera del país de consumo, para los consumidores colombianos es de suma importancia, tener una ley o normativa que proteja sus recursos informáticos, en este caso los datos, los cuales son el insumo más importante dentro de las organizaciones, por eso es que claramente este modelo de servicios ante una falta o falla que vaya en contra de la ley definida en territorio colombiano, deberá ser juzgado y evaluado por medio de la misma, asumiendo total responsabilidad ante posibles vulnerabilidades.

Esta ley está divida en dos capítulos pero el capítulo número uno está relacionado directamente con los posibles eventos que podrían suceder con los proveedores de servicios de la computación en la nube.

CAPITULO. I

"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos."

Este capítulo es tal vez el que está más relacionado con los servicios y las normas que deberán cumplir y garantizar los proveedores de servicios cloud. Para estos proveedores es de suma importancia garantizar a sus clientes que para la información que resguardan cumplen con la confidencialidad, la integridad y la disponibilidad que amerita, para que estos sean servicios seguros para los clientes. Permitir accesos no deseados o abusivos, obstaculizar el acceso,

[7] COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1273 (5, enero, 2009). De La Protección De La Información Y De Los Datos. Ministerio TIC. Bogota D.C., 2009. 4 p.

interceptar la información ajena de sus clientes, realizar daños a la data o infraestructura digital, entre otros eventos más deben ser juzgados mediante los siguientes artículos de dicha ley:

Artículo 269A: Acceso abusivo a un sistema informático.

En el mundo de las tecnologías de la información, es muy común oír que se presenta ataques e ingresos a sistemas no autorizados, este es uno de los más comunes y la computación en la nube debe garantizar que este riesgo sea mitigado para garantizar la seguridad de la información.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Este delito es frecuente en la actualidad, donde delincuentes informáticos buscan detener la presentación de un servicio informático y para restablecerlo muchas veces piden sobornos o pagos de dineros muy elevados.

Artículo 269C: Interceptación de datos informáticos.

Esta acción busca poder obtener la información de los usuarios de una red de datos, para sí luego utilizarlos y sacar provecho de esto, es muy común la interceptación de credenciales de redes sociales y de datos bancarios.

Artículo 269D: Daño Informático.

Este se presenta poca veces, pero es latente el mundo informático, acá el delincuente lo que busca es destruir los recursos informáticos de una persona u organización. En ocasiones antes de realizar dichos daños solicita le sea pagado dinero para no realizar los daños.

Artículo 269E: Uso de software malicioso.

Este delito es quizás el más frecuente hoy en día, el delincuente busca por medio de una descarga, un correo electrónico con un adjunto o un ejecutable, instalar en los equipos un virus que le permita realizar diferentes acciones, desde la

manipulación del equipo hasta la captura de toda la información que allí se encuentre.

Artículo 269G: Suplantación de sitios web para capturar datos personales.

Para este los delincuentes buscan engañar a sus víctimas suplantando sitios como bancos, comercio electrónico, correos, entre otros, con esta modalidad logran capturar información valiosa de los usuarios y poder realizar fraudes y robos.

CAPITULO. II

De los atentados informáticos y otras infracciones

Para este capítulo, los proveedores de servicios en computación en la nube deberán hacerse responsables de los hurtos magnéticos que pueden llegar a tener en su infraestructura, además de controlar la transferencia de información de una manera controlada y registrada en logs de auditoria. De infringir en estos dos puntos, ésta ley colombiana por medio de los siguientes artículos juzgará y hará responsables a dichos proveedores por estos fallos.

Artículo 269I: Hurto por medios informáticos y semejantes.

Por el boom que se vive hoy en día con la tecnología, este delito es probablemente el que más llama la atención para los delincuentes ya que los usuarios no toman las medidas de seguridad para realizar transacciones desde sus dispositivos, es allí donde los delincuentes aprovechan para realizar sus fraudes.

Ley 1581 de 2012 Nivel Nacional.

"Por la cual se dictan disposiciones generales para la protección de datos personales"[8]

[8] EL CONGRESO DE COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C., 2012. 10 p.

Esta ley Colombiana hace énfasis al buen uso que se le debe de dar a los datos recolectados por parte de los clientes y almacenados en bases de datos, archivos o ficheros. Para los servicios de la computación en la nube aplican claramente ya que este modelo de servicio aloja gran información de los diferentes clientes y debe velar por la seguridad y la protección de los datos. Sabiendo que la ley es colombiana, dependiendo del tipo de servicio, es decir, si el cliente es de esta nacionalidad y el proveedor de dichos servicios realiza sus operaciones fuera de dicho territorio, también deberá regirse por esta normativa y cumplirla a cabalidad. Artículo relacionado con dicho procedimiento: *"Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*[9]

El proveedor de servicios cloud es consiente que sus clientes son los propietarios de la información y por ende cualquier operación que estos deseen realizar con dicha data, las acciones realizadas con dicha información, debe ser comunicada con los propietarios de esta, de lo contrario se estaría violando el siguiente artículo de esta ley: "Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada."[10]

Envío de información por fuera de las diferentes plataformas del modelo adoptado, es comunicado con los propietarios de dicha información, donde se les informa de que esta data va a ser utilizada por otros sistemas y que se requiere de autorización, incumpliendo esta norma se estaría violando el siguiente artículo de dicha ley: "Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización."[11]

La información y data que manejan estas bases de datos, siempre están a disposición de los usuarios propietarios o a quienes tengan acceso a la misma. Es de total responsabilidad que dicha información esté disponible cuando los usuarios la requieran, este punto lo rige la ley con el siguiente artículo: "Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data"[12]

[9] EL CONGRESO DE COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C., 2012. 10 p.
[10] Ibid., p. 10
[11] Ibid., p. 10
[12] Ibid., p. 10

5. METODOLOGÍA

El desarrollo de esta monografía investigativa, se basa en la recopilación de información de diferentes autores acerca de la seguridad de la computación en la nube, métodos, mecanismo y herramientas que ofrecen los proveedores de dichos servicios para garantizar la seguridad de los activos de sus clientes. Por medio de la lectura, la investigación y de la información, se realiza un profundo análisis de cada uno de los diferentes elementos que fortalecen la seguridad, para identificar de qué forma se da la protección a la confidencialidad, disponibilidad e integridad de la información.

El análisis parte de la identificación del problema de desconfianza que aún genera la computación en la nube para algunas organizaciones, para lograr el contexto general, lo primero que se debe aclarar es el funcionamiento de la computación en la nube, sus modelos de servicio, modelos de implementación, ventajas, desventajas para sí lograr llegar al objetivo de identificar de qué forma se protege la información en un entorno Cloud.

Luego de tener un contexto general de la computación en la nube, se analizan cada uno de los mecanismos que ofrece la computación en la nube para el aseguramiento de la integridad de la información, mecanismos, herramientas, procesos entre otros elementos que fortalecen esta característica y así poder confirmar que la computación en la nube garantiza la integridad de la información en el software e infraestructura como servicios.

De la misma manera se realiza el análisis a la información recopilada para garantizar la confidencialidad de la información en los servicios software e infraestructura como servicios, mecanismos, herramientas, proceso que ayudan a garantizar esta característica

Continuando con el análisis, se identifican los mecanismos, herramientas y procesos que utiliza la computación en la nube para garantizar una alta disponibilidad en sus servicios, como el software y la infraestructura como servicio, todas las ventajas que este modelo presenta para que los clientes tengan 7*24 365 días al año su información a la mano sin importar el tipo de conexión o ubicación, pero donde siempre prevalece la seguridad para este tipo de activo.

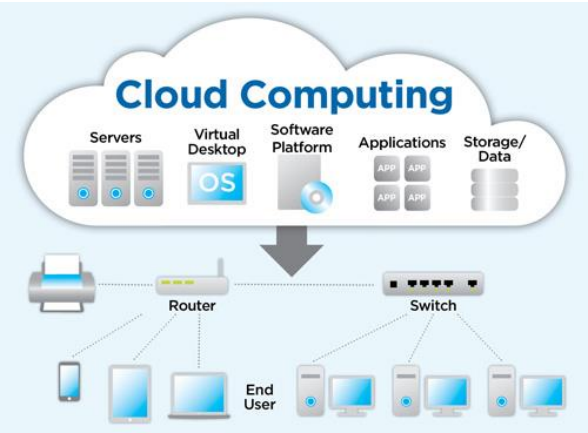
Por último y con la identificación de cada uno de los mecanismos, se puede entonces realizar un nuevo análisis para dar respuesta al interrogante que se genera sobre la seguridad de la computación en la nube, específicamente en software e infraestructura como servicios para lograr concluir los niveles de seguridad que se manejan por parte de los proveedores de este tipo de servicio donde estos garantizan por medio de dichos mecanismos, una alta integridad, confidencialidad y disponibilidad de la información de sus clientes.

6. SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA COMPUTACIÓN EN LA NUBE PARA SAAS E IAAS.

6.1. COMPUTACIÓN EN LA NUBE

Hoy en día hablar de computación en la nube para muchos sigue siendo sinónimo de inseguridad y preocupación con la integridad de la información, pero curiosamente hoy en día la gran mayoría de los dispositivos y aplicaciones que usan las personas, tiene involucrado la tecnología de la computación en la nube, tan sencillo que imágenes, videos y música se almacena en la nube y no necesariamente en los dispositivos, es así que podemos acceder a toda esta información solo con tener una conexión a internet y las credenciales necesarias para acceder a ella. “Entre 2008 y 2009, surgió el nuevo paradigma tecnológico de la Nube, con todas sus tecnologías asociadas que, al poco tiempo, despegó con su llegada al gran público. Dos grandes cabeceras económicas mundiales, Business Week y The Economist, ya preveían en 2008 el advenimiento de esta arquitectura, y analizaron con detalle la computación en nube y su impacto en las corporaciones”.[13] En la figura 1 se observa que los servicios SaaS, IaaS, virtualización y almacenamiento no hacen parte de la red interna de una organización, sino que por el contrario se encuentran alojados en la nube y por medio de una conexión a internet se tiene acceso a todos estos.

Figura 1. Modelo Cloud Computing



Fuente: http://bambinoides.com/it/cloud-computing/

[13] JOYANES AGUILAR, Luis. COMPUTACIÓN EN LA NUBE: Notas para una estrategia española en cloud computing. S.A 2012. 24

Por otra parte Luis Joyanes Aguilar, define en su obra Computación en la nube: estrategias de cloud computing en las empresas, que la computación en la nube es:

> La nube es la plataforma tecnológica por excelencia de la década actual y, posiblemente, del futuro de la computación y se ha convertido en el término de moda de todos los medios de comunicación a nivel mundial. Con la computación en nube todo lo que hace en su computadora ahora estará en la Web y podrá acceder a sus programas y documentos desde cualquier lugar en cualquier PC conectada a Internet[14].

Es decir que los usuario finales y no finales como administradores del sistema y áreas de las tecnologías de la información ya no deberá preocuparse por la inversión en equipos de cómputo y servidores para soportar los servicios de la compañía, mucho menos en licencias de software, en actualizaciones, en mantenimiento, "en renovación o en gestión de recursos, sino al contrario que ese tipo de responsabilidades son única y exclusivamente del proveedor de servicio seleccionado responsable de dichas variables".[15]

Si se analiza una definición dada por Peter Mell (NIST), Tim Grance (NIST), estos dicen que:

> La computación en la nube es un modelo que permite acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y lanzarse rápidamente con un mínimo esfuerzo administrativo o la interacción del proveedor de servicios. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación.[16]

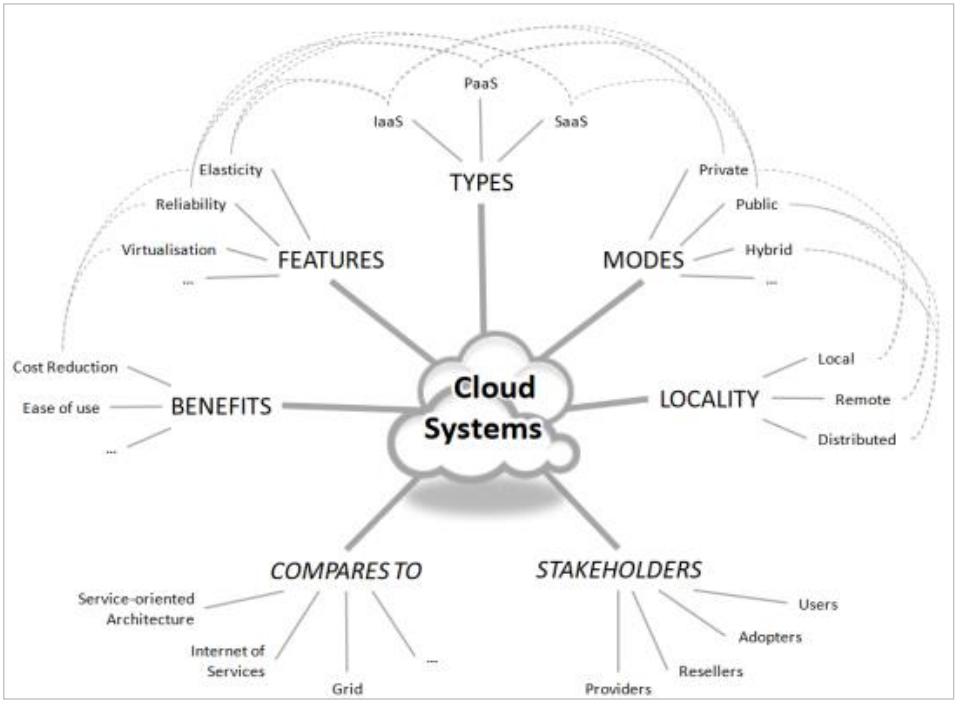
[14] JOYANES AGUILAR, Luis. Computación en la nube: estrategias de cloud computing en las empresas. Mexico. Alfaomega, S.A., 2012. p, 35p

[15] MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [Online]. Gaithersburg. NITS. 2011., 1 p. Disponible en internet: <https://csrc.nist.gov/publications/detail/sp/800-145/final>

[16] Ibid., p. 10

En la figura 2, se puede observar que no son solo modelos y tipos los que componen la computación en la nube sino también características, beneficios, ubicación, usuarios involucrados y comparación frente a otras tecnologías que lo definen como un modelo estable.

Figura 2. Características Cloud Computing.



Fuente: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

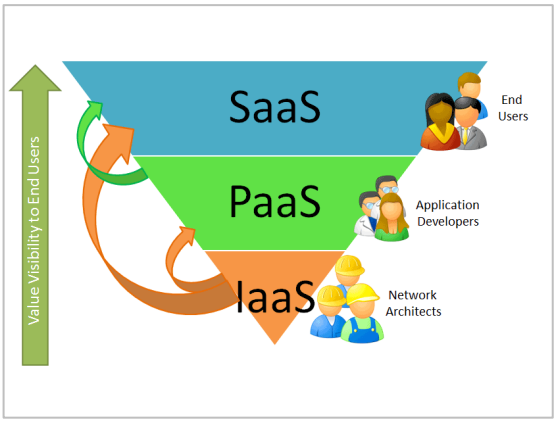
6.2. MODELOS DE SERVICIO

La computación en la nube, desde hace varios años define los conceptos que pueden ser fundamentales para este novedoso modelo, que se han ido transformando para las empresas tradicionales en una solución que apalanca el desarrollo de las tecnología tales como SaaS, IaaS y PaaS. “Estos tres conceptos tienen que estar en el radar de cualquier gerente –sea de una empresa de tecnología o no porque pueden ser las herramientas claves para generar valor y convertirse en líder de su mercado.”[17]

[17] SANTOS, Mateo. SaaS, IaaS y PaaS: ¿qué son, cómo usarlos y para qué?. [Online]. Bogotá. Enter.com. 2015. Disponible en internet: : <http://www.enter.co/guias/tecnoguias-para-empresas/saas-iaas-y-paas-que-son-como-usarlos-y-para-que/>

En la figura 3 se puede evidenciar que para cada servicio cloud, exciten unos actores involucrados, los usuarios finales interactúan con los servicios SaaS, desarrolladores con PaaS y arquitectos de soluciones con IaaS.

Figura 3. Modelos de servicio.



Fuente: https://wintubuntu.wordpress.com/2014/03/31/capas-del-cloud-computing/

- SaaS – Software as a Service

Software as a Service presta la facilidad de utilizar ciertas aplicaciones sin tener la necesidad de que estas se encuentren instaladas en los servidores de las compañías, sino por el contrarios en los servidores del proveedor y sean estos quienes se deben encargar de la disponibilidad, integridad y seguridad de la información.

> Peter Mell y Tim Grance del National Institute of Standards and Technology (NIST), definen SaaS como "la capacidad provista al consumidor es usar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Se puede acceder a las aplicaciones desde varios dispositivos cliente a través de una interfaz de cliente ligero, como un navegador web (por ejemplo, correo electrónico basado en web). El consumidor no administra ni controla la infraestructura subyacente de la nube, incluida la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de aplicaciones individuales, con la posible excepción de usuarios limitados.[18]

Markos Goikolea dice que "Un sistema SaaS o Software as a Service, es un modelo de distribución de software en el que tanto el software como los datos

[18] MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [Online]. Gaithersburg. NITS. 2010. Disponible en internet: <https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf>

manejados son centralizados y alojados en un único servidor externo a la empresa. Esto implica que el software utilizado por la empresa no se encuentra en la misma, sino que un proveedor se ocupa del hosting de dicho software en la nube, así como del mantenimiento y el soporte".[19]

El componente SaaS es entonces el modelo de software como servicios, es decir, las empresas no desarrollan o implementan las aplicaciones, estas solo se encargan de contratar el servicio y bajo una conexión a internet realizan la utilización de las aplicaciones, esto viene acompañado de soporte técnico y acompañamiento remoto en casi todos los escenarios. Una de las ventajas más importantes de este modelo de servicio, es que las empresas se "Desentienden" de cosas como las actualizaciones, mantenimiento, alojamiento entre otros factores, esta ventaja se ve reflejada claramente en la parte económica de las organizaciones.

Para el gigante tecnológico Microsoft SaaS es:

> La capacidad provista al consumidor es usar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. El consumidor no administra ni controla la infraestructura subyacente de la nube, incluidos la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de aplicaciones individuales, con la posible excepción de la configuración de la aplicación específica del usuario definida por el proveedor.[20]

- IaaS – Infrastructure as a Service

Por otro lado y no menos importante está el servicio de infraestructura como servicios IaaS, el cual se refiere a Infraestructura como servicio, el objetivo de este tipo de servicio es proveer a sus clientes un modelo de infraestructura tecnológica en la nube, es decir, un proveedor de servicios localmente posee servidores los cuales pone a disposición de sus cliente para que estos hagan uso de ellos de la manera en que lo desee, esto trayendo ventajas y beneficios importante sobre todo en el tema económico que genera tener esta infraestructura física y local dentro de las instalaciones propias, así entonces este servicio ofrece la implementación de toda una infraestructura de red para las organizaciones el cual puede incluir desde la aplicación más básica hasta, sistemas operativos y

[19] GOIKOLEA, Markos. ¿Qué es un sistema SaaS? Definición y ventajas. [Online]. Digital Business. 2014. Disponible en internet: <http://www.iebschool.com/blog/que-es-saas-definicion-ventajas-digital-business/>

[20] LOEFFLER, Bill. Cloud Computing: What is Infrastructure as a Service. [Online]. Microsoft.2011. Disponible en internet: <https://technet.microsoft.com/en-us/library/hh509051.aspx>

elementos de configuración y seguridad dentro de una red privada. La NIST define IaaS como:

> La capacidad provista al consumidor es proporcionar procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura subyacente de la nube, pero tiene control sobre los sistemas operativos, el almacenamiento, las aplicaciones desplegadas y posiblemente el control limitado de los componentes de red seleccionados.[21]

Margaret Rouse hace una definición muy concreta y entendible de lo que para ella es IaaS, definiendo ese modelo de servicio como "una forma de computación en la nube que proporciona recursos informáticos virtualizados a través de Internet. IaaS es una de las tres categorías principales de servicios de computación en la nube, junto con el software como servicio (SaaS) y la plataforma como servicio".[22]

Dentro de los modelos de servicio ofrecidos por la computación en la nube existe un último llamada plataforma como servicio PaaS, en el cual se busca proveer al usuario final una infraestructura capaz de soportar nuevas aplicaciones creadas por ellos mismos utilizando diferentes métodos y lenguajes de programación y herramientas que se pueden acoplar a las tecnologías utilizadas por el proveedor de servicios. En este tipo de servicio el usuario final no se encarga de administrar ni controlar todo lo relacionado con la infraestructura de desarrollo sino que su responsabilidad está en el control de las aplicaciones implementadas y de todas las configuraciones necesarias que se requieren para el alojamiento de la aplicación.

- PaaS - Platform as a Service

Por último se tiene plataforma como servicio, este les permite a los usuarios finales de desplegar en la infraestructura adquirida al proveedor de servicios aplicaciones creadas por el cliente, incluso hasta el punto de llegar adquiridas, además este tipo de servicio permite la utilización de frameworks, kits de herramientas, lenguajes de programación y todas las herramientas que el proveedor pone a su disposición para la construcción de nuevas aplicaciones. Así entonces El proveedor recibe un pago por brindar la plataforma y los servicios de ventas y distribución, permitiendo la distribución de aplicaciones de software

[21] MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [Online]. Gaithersburg. NITS. 2010. Disponible en internet: <https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf>

[22] ROUSE, Margaret. Infrastructure as a Service (IaaS). [Online]. TechTarget. 2014. Disponible en internet: <http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS>

creadas por el cliente. En este caso entonces el cliente no controla la infraestructura que soporta estos servicios, pero si logra controlar las aplicaciones y servicios desplegados además de algunas variables de ambiente.

Según Tim Mather, PaaS "los desarrolladores usan los bloques de construcción del entorno de desarrollo del proveedor para crear sus propias aplicaciones". [23] Estas herramientas son plataformas alojadas en la nube para las cuales lo único que se necesita para acceder es una buena conexión a internet. Una de las ventajas de contar con este servicio, es que los desarrolladores no se ven en la necesidad de instalar ningún tipo de herramienta en sus equipos de trabajo para luego realizar las implementaciones de sus desarrollos sin ninguna habilidad específica.

Los servicios PaaS tienen algunas características que lo hacen mucho más funcional, como por ejemplo:

Herramientas de desarrollo multiusuario, estas permiten múltiples usuarios, cada uno con diferentes proyectos activos al tiempo.

Arquitectura de despliegue de multiusuario. En PaaS, la escalabilidad de la aplicación y los niveles de datos debe estar incorporada.
Administración integrada. Las soluciones de desarrollo tradicionales no están asociadas con el monitoreo en el tiempo de ejecución, PaaS tiene la capacidad de monitoreo e integrarse en la plataforma de desarrollo.

6.3. MODELOS DE IMPLEMENTACIÓN

Por último se tienen los modelos de implementación que posee la computación en la nube, estos modelos son los diferentes tipos de soluciones que ofrece la computación en la nube para los usuarios, estas permiten que cada una de ellas ofrezca diferentes alternativas, ventajas y que se ajusten a las necesidades de los usuarios.

- Nube privada: "La infraestructura en nube está preparada para el uso exclusivo de una única organización que comprende varios consumidores

[23] MATHER, Tim. KUMARASWANY Subra. LATID Shahed. Cloud Security, an Enterprice Perpective on Risk Compliance. O'REILLY Media, Inc. 2009. 338p

(por ejemplo, unidades de negocio). Puede ser de propiedad, administrada y operada por la organización, un tercero o una combinación de ellos y puede existir dentro o fuera de las instalaciones."[24]

- Nube para una comunidad: "La infraestructura en la nube es compartida por varias organizaciones y es compatible con una comunidad específica que ha compartido inquietudes (por ejemplo, misión, requisitos de seguridad, política y consideraciones de cumplimiento). Puede ser administrado por las organizaciones o un tercero y puede existir dentro o fuera de los locales". [25]

- Nube Pública: La infraestructura en la nube ofrece un servicio público para gran parte de la comunidad tecnológica y esta nube siempre es propiedad del proveedor de servicios que ofrece este tipo de nube.

> Las empresas pueden usar la funcionalidad en la nube de otros, respectivamente, ofrecer sus propios servicios a usuarios fuera de la empresa. Proporcionar al usuario la capacidad real de explotar las características de la nube para sus propios fines también permite a otras empresas externalizar sus servicios a dichos proveedores de la nube, reduciendo así los costos y el esfuerzo para construir su propia infraestructura. Como se observa en el contexto de los tipos de nubes, el alcance de las funcionalidades puede ser diferente.[26]

- Nube Hibrida: "La infraestructura de la nube es una composición de dos o más nubes (privada, comunidad o público) que siguen siendo entidades únicas pero están unidas por tecnología estandarizada o patentada que permite datos y aplicaciones portabilidad (por ejemplo, explosión de nubes para equilibrar la carga entre nubes)".[27]

---

[24] Primorac, Carlos R. Computación en la nube. Trabajo de grado en Licenciatura en Sistemas de Información Comunicaciones de Datos. Universidad Nacional del Nordeste. Facultad de Ciencias Exactas y Naturales y Agrimensura. 2014. 13 p.

[25] LOL, Cloud. Modelos de Implementación. [Online]. Lol Cloud. 2017. Disponible en internet: <https://www.licenciasonline.com/bo/es/cloud/modelos-de-implementacion>

[26] European Commission, Information Society and Media, "The Future of Cloud Computing. Opportunities for European Cloud Computing beyond 2010". [Online]. CORDIS. 2010, Disponible en internet: : <http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf>

[27] MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [Online]. Gaithersburg. NITS. 2010. Disponible en internet: <https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf>

6.4. CARACTERÍSTICAS

- Elasticidad: Esta característica permite a los usuarios dependiendo del servicio adquirido aumentar o disminuir los recursos informáticos con los que cuentan según sus necesidades, de la misma forma es posible liberar recursos para que sean utilizados en otros procesos cuando ya no sean necesarios. Es decir, se tiene la capacidad de reutilizar los recursos contratados donde más se requiera, en algunos de estos casos, esta actividad puede ser de forma automática, Algunas de estos servicios prestan esta útil funcionalidad para optimizar el consumo de estos recursos y enfocarse en los que si de alguno u otra forma requieren más ayuda.

- Escalabilidad: La escalabilidad permite a los usuarios hacer uso de lo estrictamente necesario dentro de una organización a nivel de recursos tecnológicos, es decir, de estar utilizando un porcentaje menor de una aplicación se puede pasar a utilizar un cien por ciento con total normalidad, rapidez, y transparencia para usuarios finales, además esta característica permite la integración de muchísimos otros sistemas con los servicios de la computación en la nube y así como la capacidad de escalar de forma masiva el ancho de banda y el espacio de almacenamiento.

- Multi-uso: Esta característica es quizás una de las más llamativas cuando de computación en la nube se trata, este modelo permite a los usuarios a compartir diferentes recursos, es decir, múltiples usuarios usando los mismos recursos en el nivel de red, nivel de host y nivel de aplicación. Esto a comparación del servicio tradicional uno a uno, tiene la ventaja de permitir que en una única aplicación esté disponible para muchos usuarios, estableciendo unos recursos de acceso y prestaciones distintos para cada usuario.

- Pago por uso: Esta característica es muy importante para los usuarios, ya que estos solo pagan por los recursos que realmente están usando y por el tiempo que los requieren, así entonces al final los cliente no pagaran un monto fijo cada vez sino que este será variable dependiendo de la utilización de los recursos tecnológicos.

- Auto-Aprovisionamiento: Esta característica permite a los usuarios aprovisionar los recursos computacionales según las necesidades de la organización, según sus alcances, es decir, los usuarios están en la potestad de activar o inactivar recursos adicionales como por ejemplo capacidad de procesamiento, software, almacenamiento y recursos de red.

7. BENEFICIOS, VENTAJAS Y DESVENTAJAS DE LA COMPUTACIÓN EN LA NUBE Y SUS SERVICIOS SAAS E IAAS.

7.1. VENTAJAS Y BENEFICIOS DE LA COMPUTACIÓN EN LA NUBE

Toda nueva tecnología debe traer consigo misma mejoras y ventajas que ayuden no solo a las organizaciones sino también a las personas con sus procesos el manejo de su información y por supuesto la seguridad de sus activos de información.

- Reducción de costos: La reducción de costos es quizás la ventaja más atractiva cuando de computación en la nuble se trata, de no serlo, es una de las más evidente de todas las que ofrece esta tecnología. Cuando se deja toda la responsabilidad de la implementación de la infraestructura y software al proveedor de servicios, el cliente no debe preocuparse por adquirir y configurar todos los equipos de cómputo necesarios para la implementación de una solución, además de capacitar a todos los usuarios para la configuración y mantenimiento de los equipos. Por otro lado los clientes que adquieren cualquier tipo de servicio ofrecido en la nube, únicamente deben pagar por los recursos que utilizan, y no como en otros servicios que cobran cargos únicos, esto les permite que los costos sean los correctos y así es posible diseñar planes de pago a partir del tiempo en que éste se utiliza la memoria, el procesamiento y el almacenamiento.

- Accesibilidad: Las aplicaciones ofrecidas por la computación en la nube ofrecen una gran ventaja cuando de accesibilidad se trata, es decir, se le permite a los usuarios hacer uso de ellas desde cualquier dispositivo físico siempre y cuando este esté conectado a Internet. Lo más común es acceder a ellas (aplicaciones) desde un navegador web, pero con este nuevo modelo es posible utilizar las aplicaciones no únicamente desde un equipo de cómputo, sino que también permitiendo a los usuarios hacer uso desde dispositivos móviles como smartphones y en ocasiones permitiendo hacer operaciones sin internet, esto último utilizando la memoria cache de los dispositivos.

- Disponibilidad: Esta característica hace también muy atractivo y llamativo el modelo de la computación en la nube, ya que el cliente no debe preocuparse por estar verificando si los aplicativos o la infraestructura se están ejecutando, el proveedor de servicios es quien debe garantizar que

los servicios ofrecidos siempre estén disponible para el uso de sus clientes. Así entonces el proveedor debe asegurar que su infraestructura cuenta con los recursos necesarios y la tecnología de punta para esta actividad ya que de no garantizar la disponibilidad estaría incumpliendo uno de los hitos más importantes de este modelo. Algunos proveedores hacen uso de la virtualización para diseñar infraestructuras redundantes y así ofrecer servicios constantes de acuerdo a las necesidades de los clientes.

- Seguridad: Dentro de las ventajas no se puede olvidar el tema de seguridad, cada vez se trabaja más en este tema ya que este sin duda alguna es el pilar fundamental para que este tipo de tecnología funcione de la manera que todos los clientes esperan, es decir, Los proveedores de computación en la nube deben garantizar que la seguridad de sus servicios tengan la más alta calidad en términos de seguridad y se utilicen las metodologías y estándares más completos para hacer de estos modelos seguros.

7.2. DESVENTAJAS.

No todo es perfecto en el mundo de la tecnología y la computación en la nube no es la excepción, este modelo también tiene ciertas desventajas que en muchas oportunidades hace que los usuarios desconfíen del modelo, pero que realmente no influyen en su capacidad de trabajo, algunas de ellas son:

- Relación con proveedor de servicios: Tener la información centralizada en servidores externos, es decir, por fuera de la red empresarial implica tener una interdependencia con los proveedores de servicios para cualquier tipo de solicitud sea en términos de mejora, actualización o manipulación en los servicios.

- Privacidad: Es normal que cuando se hable de computación en la nube, se relacione con inseguridad en la información ya que se está dejando como responsable de la seguridad de los datos al proveedor de servicio. Entonces al tener la información del lado del proveedor se vuelve difícil confiar que se va a tener privacidad sobre la información sensible que manejan los negocios, y que este puede estar a disposición de terceros.

- Control de recursos: Cuando todos los recursos de información se tienen en una infraestructura e incluso las aplicaciones ejecutándose sobre servidores

que se encuentran en la nube, el cliente pierde total control sobre todos los recursos e incluso y muy importante sobre toda la información de su negocio, una vez que ésta información es subida a la nube el control pasa a ser del proveedor de servicios.

7.3. AMENAZAS

Aunque la seguridad en la nube sigue fortaleciendo cada vez más su seguridad, para nadie es un misterio que siguen existiendo riesgos y amenazas en las cuales los proveedores de servicios deben poner total atención para poder garantizar la integridad y la confidencialidad de la información que manejan. Dentro de las amenazas podemos encontrar:

- Amenazas técnicas: Estas amenazas son de carácter tecnológico, es decir, una mala configuración en la tecnología da pie a que se abran las vulnerabilidades y por ende las amenazas. Estas son las culpables de los ciberataques en las redes de datos, afectando tanto software como hardware, como lo son los ataques DoS, ping de la muerte, TCP Session Hijacking, Inyección SQL, Cross-Site Request, virus, malware, entre muchos más. Este listado de posibles ataques cada vez se fortalece más y debe ser considerado y trabaja para mitigar sus riesgos.

- Amenazas contractuales: Este tipo de amenazas en su mayoría son causadas por malas definiciones, ambigüedades en los términos de los contratos, sobrecosto en los servicios, facturación engañosa, todas estas y muchas más generan vulnerabilidades que representan de alguna forma amenazas latentes ya que posiblemente fue una implementación equivoca, la cual permitirá ciertos ataques.

- Amenazas Jurisdiccionales: Esta amenaza hace referencia al manejo de la información fuera de un área limítrofe según el país donde se está ubicado, es decir, dependiendo del tipo de información esta puede o no estar en la nube, en ocasiones no se tienen en cuenta estas regulaciones y toda la información se envía a la nube.

- Amenazas organizacionales: Este tipo de amenazas es quizás uno de los difíciles de controlar, es decir, las personas que desempeñan sus labores por medio de los diferentes sistemas de información, suelen ser quien más

puertas abiertas dejan para que se produzcan los posibles ataques, sesiones abiertas, trabajo remoto, conexiones no seguras, todo estos incumplimientos a las políticas de seguridad traen consigo mismo un sinfín de vulnerabilidades que pueden ser aprovechadas por la criminalidad. Por esta razón si los empleados no se encuentran bien formados y capacitados en el compromiso que se tiene con la seguridad, estos pasan a ser el eslabón que puede quebrar la cadena de la seguridad en las organizaciones.

7.4. VULNERABILIDADES Y/O INCIDENTES

Más allá de que es un modelo bastante seguro y que cuenta con los más altos estándares de seguridad, la computación en la nube no deja de tener algunas vulnerabilidades o incidentes si no se toman las precauciones adecuadas en el tiempo correcto. "Los malos actores pueden aprovechar los recursos de computación en la nube para dirigirse a usuarios, organizaciones u otros proveedores de la nube. Los ejemplos de uso indebido de recursos basados en la nube incluyen el lanzamiento de ataques distribuidos de denegación de servicio, correo no deseado y campañas de Phishing"[28]. Algunas de estas vulnerabilidades se mencionan a continuación:

- DDoS: Desde los inicios de la computación en la nube hasta la actualidad los ataques de denegación de servicios se han hecho cada vez más populares, estos siempre fueron ataques impensados, pero a medida que se fortalecía este modelo, este tipo de ataques también en contra de las plataformas en la nube. Hoy en día con la gran cantidad de recursos que posee la computación en la nube han hecho que los ataques DDoS sean cada vez más difíciles de iniciar pero sin decir que están cien por ciento controlados, aunque sí mucho más que en años anteriores. La computación en la nube ofrece un servicio de multiplataforma (equipo portátiles, teléfonos inteligentes, tabletas) los ataques DDoS han aumentado considerablemente en cuanto a la viabilidad. Si se experimenta un tráfico de datos lo suficientemente alto en un sistema no

[28] VIOLINO, Bob. The dirty dozen: 12 top cloud security threats for 2018. [Online]. CSO Online. 2018. Disponible en internet: <https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html>

solo en la computación en la nube sino también en local, puede reducirse por completo o experimentar dificultades del consumo de los servicios.

- Servicios compartidos: La computación en la nube ofrece diferentes tipos de modelos de implementación, varias de estas soluciones en la nube no brindan la seguridad requerida para los diferentes clientes, lo cual los lleva tener que compartir diferentes tipos de recursos, aplicaciones y sistemas. Esta situación, da pie para que puedan generarse nuevas amenazas por parte de otros clientes y por ser un servicio de computación en la nube compartido, todas las amenazas dirigidas a un cliente también podrían afectar a otros clientes.

- Negligencia de los empleados: La importancia del manejo de los empleados dentro de un esquema de seguridad para los activos de información es vital, lastimosamente estos siguen y seguirán siendo una de las principales vulnerabilidades de seguridad para los sistemas de información ya que no le dan la importancia requerida. Los empleados en la actualidad pueden iniciar sesión en diferentes soluciones en la nube desde sus teléfonos inteligentes, tabletas y PC de escritorio domésticas, lo cual con un mal manejo puede dejar al sistema vulnerable a muchas más amenazas externas.

- Pérdida de datos y copias de seguridad de datos inadecuadas: Las copias de seguridad o backups son fundamentales en la seguridad de los datos en la computación en la nube, pero las configuraciones inadecuadas y la sincronización incorrecta de datos han abierto la puerta para que las empresas sean vulnerables al ransomware. Este tipo de ataques van dirigidos a capturar, bloquear y retener la información de las empresas hasta que se pague un rescate y pero aún no se sabe si el regreso de la información es completa. Con las implementaciones de respaldo de información apropiadas, las empresas ya no deberán preocuparse por este tipo de ataques. Ahora no da perdida de información únicamente por ataques dirigidos, “Una eliminación accidental por el proveedor de servicios en la nube o una catástrofe física como un incendio o terremoto puede ocasionar la pérdida permanente”[29], con las medidas necesarias y

[29] VIOLINO, Bob. The dirty dozen: 12 top cloud security threats for 2018. [Online]. CSO Online. 2018. Disponible en internet: <https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html>

los respaldos bien ejecutados es posible mitigar estas pérdidas de información.

- Phishing e ingeniería social: Aunque es muy común en otros modelos de implementación, la computación en la nube también se ve afectada por este tipo de incidentes. Estos van de la mano con la negligencia de los empleados, ya que es cada vez más común ver usuarios entrar a links de baja confianza o ingresando a sitios no seguros evadiendo las políticas de seguridad. El Phishing y la ingeniería social buscan aprovecharse de las vulnerabilidades humanas para acceder a la información confidencial de los usuarios así entonces un usuario malintencionado puede entrar en un sistema con facilidad sin importar su ubicación ya que la computación en la nube se lo permite. "Con las credenciales robadas, los atacantes a menudo pueden acceder a las áreas críticas de los servicios de computación en la nube, lo que les permite poner en peligro la confidencialidad, la integridad y la disponibilidad de esos servicios."[30] Para controlar este tipo de incidentes, a los empleados se les debe capacitar y orientar sobre phishing e ingeniería social para evitar este tipo de ataques.

Más allá de que se identifican una seria de amenazas e incidentes, la computación en la nube, trabaja cada vez para que cada una de estas brechas a la seguridad sean mitigadas para garantizar un alto nivel de seguridad, es importante recordar que todas estas amenazas no son solo responsabilidad de los proveedores de servicios, sino también de los clientes y sus empleados.

[30] VIOLINO, Bob. The dirty dozen: 12 top cloud security threats for 2018. [Online]. CSO Online. 2018. Disponible en internet: <https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html>

8. DISPONIBILIDAD, CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN EN SERVICIOS SAAS E IAAS.

Para toda organización es de suma importancia la protección y la seguridad de sus activos de información, por esto se debe proteger la infraestructura física, es decir, el hardware de TI (servidores, enrutadores, cables, etc.) ante posibles accesos no autorizados, interferencias de datos, robos y fugas de información, desastres naturales como incendios, inundaciones, entre otros. “Esto normalmente se logra al servir a las aplicaciones en la nube de centros de datos de 'clase mundial' (es decir, profesionalmente diseñados, diseñados, construidos, administrados, monitoreados y mantenidos).”[31]

Los proveedores tienen como obligación, asegurar la información de todos sus clientes, siendo muchos de estos datos críticos como por ejemplo números de tarjetas de crédito, saldos bancarios, extractos, entre muchos más, toda esta información es enmascarados o encriptados y además, solo los usuarios autorizados son quienes tienen el acceso a los datos en su totalidad. Además, las identidades y credenciales de acceso a los diferentes sistemas, son protegidas, al igual que toda la información recopila por el proveedor está bajo su responsabilidad ante cualquier alteración no deseada. Más adelante en este documento se profundizará mucho más sobre el tema de privacidad en la computación en la nube.

A continuación se explica cuáles son los mecanismos que ofrece la computación en la nube para conservar y velar porque se cumpla la seguridad en la información.

8.1. CONTROLES DE SEGURIDAD PARA LOS SERVICIOS SAAS E IAAS

Un modelo de seguridad en la nube computación en la nube, es eficiente si identifica los posibles problemas a los que se está expuesto y la a administración y gestión que se debe realizar para controlar dichas amenazas. Cada proveedor de servicios en computación en la nube, tiene que saber, identificar y clasificar sus vulnerabilidades para trabajar en ellas y definir un conjunto de controles que

[31] Cloud computing security. From Wikipedia, the free enciclopedia. [Online]. 2018. Disponible en internet: <https://en.wikipedia.org/wiki/Cloud_computing_security#Security_and_privacy>

ayuden a defenderse y proteger sus servicios ofrecidos. La idea de cada control es salvaguardar cualquier debilidad en el sistema para así mínimizar el impacto ante un posible ataque.

Un proveedor de estos servicios deberá contar mínimo con uno de los siguientes controles para asegurar la protección a su servicio.

Controles de disuasión.

Los controles de disuasión, se encargan de minimizar los ataques a un sistema sobre el modelo de la computación en la nube, estos controles deben reducir el nivel de las amenaza al informar a los posibles atacantes que habrá consecuencias adversas para ellos si proceden.

Controles preventivos.

Como su nombre lo indica, estos controles se encargan de prevenir ataques y fortalecer los sistemas contra incidentes, pero su principal objetivo es reducirlos, y no eliminando las vulnerabilidades. Estos controles aportan a la seguridad de la computación en la nube, para que sus servicios puedan evitar de manera temprana y oportuna, posibles alteraciones o accesos no deseados dentro de su modelo. Dentro de estos podemos encontrar Firewall o IPS, los cuales en ocasiones realizan tareas similares.

A continuación se explica el funcionamiento de cada uno de estos mecanismos de seguridad.

- Firewall cloud.

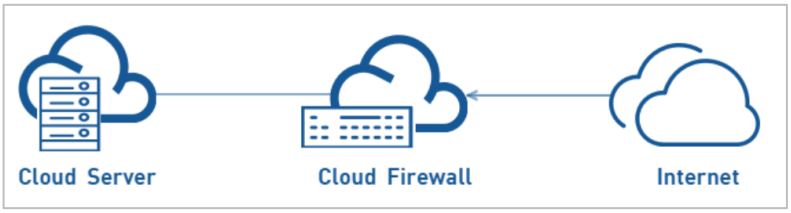
  Los proveedores de computación en la nube, también deben garantizar y controlar quienes, qué y cuándo ingresa a sus centros de datos, por medio de Firewall basados en lograr identificar y verificar los paquetes entrantes y salientes por medio de las políticas de acceso previamente definidas para así lograr bloquear el tráfico malicioso con el fin de proteger la red, la información y activos reales y virtuales.

Este tipo de firewall, son servicios basados en la nube y diseñados para ejecutarse dentro del centro de datos virtual del proveedor de servicios, donde este mecanismo se ejecuta en los servidores virtuales para proteger el tráfico que va hacia, desde y entre aplicaciones en la nube.

Sabiendo y teniendo claro el concepto de computación en la nube, todos los usuarios autorizados pueden acceder a la información sin importar lugar, la hora, tipo de dispositivo o conexión, allí es donde entra la magia de firewall para identificarlo y permitirle el ingreso o no de sus requerimientos hacia el centro de datos cloud.

El funcionamiento de este dispositivo se puede ver gráficamente en la figura 4, donde toda solicitud enviada a los servidores cloud deben pasar por un firewall que realiza con controles respectivos de seguridad.

Figura 4. Cloud Firewall



Tomada de: http://www.adaptixnetworks.com/cloud/cloud-server/

- IPS: Son mecanismos para ejercer control dentro de una red informática y así poder ejercer control en los diferentes sistemas y poder evitar diferentes ataques. Este a diferencia del IDS, logra identificar el posible ataque pero también intenta detenerlo o evitar que sea exitoso, es decir, el IPS por medio de políticas de seguridad puede proteger de un hipotético ataque. Así mismo estos se clasifican en 4: Basados en red lan, basados en red wireless, análisis de comportamiento de red y basados en host.

  Características IPS.

  - ✓ Monitoreo de operación y soporte del dispositivo 5x8 o 7x24 según las necesidades del cliente. Adición, eliminación y ajuste de firmas 5x8 o 7x24 según las necesidades del cliente.

- ✓ Actualización automática con verificación manual de las bases de firmas de las funcionalidades de IPS. Actualizaciones de software (firmware) de los dispositivos según los liberen los fabricantes y sean homologados por nuestra área de servicios. Análisis para la definición del grupo inicial de firmas de IPS.
- ✓ El dispositivo para la prestación del servicio se incluye dentro de la tarifa mensual por el servicio. Los dispositivos administrados pueden estar ubicados en diferentes ubicaciones físicas y tipológicas. Comunicación segura desde y hacia el SOC (Security Operations Center) de 360 Security Group.

- ✓ Soporte en sitio ante la imposibilidad del SOC para acceder remotamente al dispositivo. Plataforma de servicios unificada y especializada para la prestación de servicios administrados de seguridad. Diversas formas de comunicación con nuestro SOC: Portal Seguro de Servicio, PBX y Líneas Celulares de Servicio.
- ✓ Análisis de logs del dispositivo y correlación con logs de otros dispositivos administrados que tenga contratados el cliente. Reportes de servicio con frecuencia mensual y ante la ocurrencia de incidentes y eventos especiales.

Controles detectores.

Estos controles, son los encargados de detectar y reaccionar de manera adecuada y oportuna frente a cualquier incidente o ataque que se esté llevando acabo, es decir, estos deberán indicar que es lo que está ocurriendo y cuál es la mejor forma para contrarrestar la situación para evitar daños mucho mayores dentro de la infraestructura. Así entonces, estos controles son de gran importancia ante un posible ataque, ya que estos controles son los que ayudarán a la solución del problema.

Dentro de los controles detectores se puede evidenciar un mecanismo llamada IDS.

- El IDS (Sistema de Detección de Intrusos), permite dar a una red una seguridad preventiva ante actividades sospechosas que pueden generar ataques o intrusos en un sistema, el principal objetivo de este mecanismo es

estar informando a los administradores de posibles actividades anormales realizando un seguimiento al tráfico en la red. Los IDS se clasifican en dos:

N-IDS, garantiza la seguridad en la red.
H-IDS, garantiza la seguridad en el host.

Características de IDS

- ✓ Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado. Sin embargo, no debe ser una "caja negra" (debe ser examinable desde el exterior).
- ✓ Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.
- ✓ En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
- ✓ Debe imponer mínima sobrecarga sobre el sistema. Un sistema que relentiza la máquina, simplemente no será utilizado.
- ✓ Debe observar desviaciones sobre el comportamiento estándar.
- ✓ Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
- ✓ Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo.
- ✓ Debe ser difícil de "engañar".

Controles correctivos.

Como su nombre lo indica, los controles correctivos son aquellos que una vez se materializó un ataque a nuestro sistema de información, estos reducen las consecuencias de un incidente, para lograr minimizar el daño. Normalmente estos controles realizan su trabajo en ocasiones durante o después de un incidente.

Así entonces, cada proveedor antes de ofrecer servicios de computación en la nube, está en la obligación de realizar un estudio y un análisis de riesgos a sus sistemas, para identificar a que posibles amenazas está exponiendo sus servicios para identificar la probabilidad de ocurrencia, para así definir y realizar un

planteamiento e implementación de controles, que garantizan la mitigación en la reducción de ataques o incidentes, que afectan la seguridad en sus servicios.

8.2. MECANISMOS PARA LA PROTECCIÓN DE LA INTEGRIDAD

A continuación se enumeran algunas de las herramientas que utiliza la computación en la nube para garantizar los movimientos realizados en sus sistemas de información son:

- Log de transacciones.

  La computación en la nube, también cuenta con una herramienta la cual permite saber en tiempo real que es lo que se va realizando a cada uno de los datos en la base de datos. Este mecanismo es conocido como Logs de transacciones. Esta herramienta se define como una tabla más dentro de la base de datos donde todos los cambios realizados a los datos son registrados, es decir todas las operaciones que un usuario realice sobre los registros almacenados (insert-update-delete) generan un nuevo registro por cada transacción realizada generando una bitácora de cuando inició, que se hizo dentro de ella y si se completó exitosamente.
  Así entonces los logs de transacciones permiten a los clientes de la computación en la nube, saber exactamente que está ocurriendo con sus datos, que usuarios intervienen en ellos y de que forman lo hacen y así poder garantizar la integridad de los mismos.

- Auditorias.

  Las auditorias dentro de servicios de la computación en la nube, son otro de los mecanismos que este nuevo modelo ofrece a sus clientes para que estos estén al tanto del correcto funcionamiento de cada una de las operaciones ofrecidas todo esto en pro de la seguridad de la información de cada uno de los clientes. “Los clientes necesitan definir el alcance del RTA. Por ejemplo, los clientes deben validar las prestaciones del nivel de servicio, la seguridad de los

datos en reposo y la seguridad física del centro de datos."32, es decir, el cliente siempre va querer saber si se están cumpliendo las normas, controles y parámetros establecidos para controlar la seguridad en los datos, en los controles de acceso, dispositivos físicos, redes de comunicaciones, aplicaciones, entre muchos más elementos.
Es así como los proveedores de dicho servicios, deben estar en la capacidad de realizar sus propias auditorías internas pero a su vez están en la capacidad de permitir la realización de auditorías externas cuando el cliente lo desee.

Auditorías internas: Con este tipo de auditoria, los proveedores de servicios de computación en la nube, ofrecen a sus clientes velar por el cumplimiento de cada uno de sus propios controles de seguridad establecidos y definidos con sus clientes, es decir, buscan por medio de este mecanismo determinar si los controles han operado efectivamente, esto ayudando a detectar posibles fallas en la seguridad o problemas potenciales que puedan investigados y tratados de manera oportuna y efectiva.

Los controles que diseñan dichos proveedores, son diseñados para prevenir la ocurrencia de grandes problemas, la detección temprana de estos y la corrección rápida y efectiva y así lograr contribuirá en la mejora continua de la seguridad de la información.

Auditoria externa: Los proveedores de la computación en la nube, permiten que se les realice procesos de auditoría externa, para así verificar el correcto funcionamiento de los controles de seguridad implementados dentro de sus plataformas, es decir, terceros son contratados para verificar si se están cumpliendo y de qué forma los controles definidos, esto con el fin de que los clientes se sientan cómodos con la efectividad de cada uno de los métodos de seguridad definidos. A continuación algunos de los procesos de auditorías externas empleados por los proveedores de computación en la nube.

[32] MATHER, Tim. KUMARASWANY Subra. LATID Shahed. Cloud Security, an Enterprice Perpective on Risk Compliance. O'REILLY Media, Inc. 2009. 338p

- Servicios externos de controles.

  SAS 70: Es un estándar en procesos de auditoría la cual es reconocida internacionalmente la cual se enfocado en los controles internos y externos que posee una empresa que ofrece servicios. Este tipo de auditoria busca verificar los siguientes escenarios:

  - ✓ Tener procesos de nómina perfectos.
  - ✓ Garantizar la operación sobre casi cualquier condición de contingencia.
  - ✓ Garantizar la integridad de la información del cliente.
  - ✓ Garantizar la confidencialidad de la información del cliente.
  - ✓ Tener evidencias de todo lo ejecutado en la nómina, con nombre, hora, responsable, etc.
  - ✓ Evitar al cliente contingencias fiscales y con el IMSS.

  SysTrust: "Auditoría de controles basada en principios y criterios definidos de seguridad, disponibilidad, confidencialidad e integridad del procesamiento. Destinado a aplicar a la confiabilidad de cualquier sistema."[33]

  WebTrust: "Se basa en una serie de principios y criterios diseñados para promover la confianza entre los consumidores y las empresas que realizan negocios en Internet."[34], es decir, por medio de servicios de aseguramiento evalúa si un sitio web cumple o no con alguno de los principios y criterios de los servicios de confianza.

  ISO 27001: Auditoría del Sistema de gestión de la seguridad de la información dentro de una organización, donde se busca proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Todo esto con base en una identificación evaluación de riesgos para luego definir e implementar las acciones necesarias para evitar que estos riesgos se materialicen y ponga en duda los controles de seguridad de los proveedores de servicios de computación en la nube.

[33] MATHER, Tim. KUMARASWANY Subra. LATID Shahed. Cloud Security, an Enterprice Perpective on Risk Compliance. O'REILLY Media, Inc. 2009. 338p

[34] SAS 70. [Online]. American Institute of Certified Public Accountants (AICPA). 2018 Disponible en internet: <http://sas70.com/FAQRetrieve.aspx?ID=33288>

8.3. MECANISMOS PARA LA PROTECCIÓN DE LA CONFIDENCIALIDAD

La computación en la nube debe de hacer uso de las últimas y más avanzadas tecnologías para que prevalezca la confidencialidad de la información, ya que esta es uno de los pilares fundamentales que hacen de este modelo uno de los más seguros, a continuación algunos de estos mecanismos:

- Encriptación simple: Este es uno de los mecanismos más utilizados para proteger y salvaguardar los datos que los usuarios usarán o almacenarán en la nube. Este mecanismo le permite cómodamente y con seguridad a los servicios de la nube, debido a que toda la información allí almacenada por los proveedores de la nube se encuentran protegidos con diferentes métodos de encriptación.

  Así entonces este mecanismo lo podemos definir como: "Corresponde a una tecnología que permite la transmisión segura de información, al codificar los datos transmitidos usando una fórmula matemática que "desmenuza" los datos. Asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos."[35]

  Este mecanismo permite proteger datos críticos de los clientes, sin importar el entorno donde se encuentren, ya que los datos ya no están bajo control de los clientes. "En la nube, no podemos darnos el lujo de tener un control físico real sobre el almacenamiento de la información, por lo que la única manera de garantizar que la información esté protegida es almacenarla criptográficamente, con nosotros manteniendo el control de la información criptográfica llave."[36]

  Algunos proveedores de servicios en la nube, ofrecen cifrar los datos una vez recibidos, esto para garantizar que toda la información recibida que se está almacenando o transmitiendo esté protegida por el cifrado de forma predeterminada.

- Encriptación Homomórfica: Estas permiten que las operaciones matemáticas complejas se realicen en datos encriptados sin comprometer el cifrado. Debido

[35] ANCELIT, ANALIDA Y SHARITO. Encriptacion de datos. [Online]. Blogger.com. 2007. Disponible en internet: <http://encriptaciondedatos.blogspot.com.co/2007/09/encriptacion-de-datos.html>

[36] NATE Lord. Cryptography in the Cloud: Securing Cloud Data with Encryption. [Online]. digitalguardian.com 2017.Disponible en internet: <https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption>

a que los datos en un esquema de cifrado homomórfico conservan la misma estructura, las operaciones matemáticas idénticas, ya sea que se realicen en datos cifrados o descifrados, arrojarán resultados equivalentes. El cifrado homomórfico desempeña un papel importante en la computación en la nube, permitiendo a las empresas almacenar datos encriptados en una nube pública y aprovechar los servicios analíticos del proveedor de la nube.

- Algoritmos de encriptación

  La encriptación de datos a su vez utiliza otros componentes (algoritmos de cifrado) para que este mecanismo logre ser seguro y confiable, a continuación algunos de ellos:

  Algoritmo RSA: Rivest–Shamir–Adleman, "RSA es básicamente un algoritmo de cifrado / descifrado asimétrico. Es asimétrico en el sentido de que aquí la clave pública distribuida a todos a través de la cual se puede encriptar el mensaje y la clave privada que se usa para el descifrado se mantiene en secreto y no se comparte con todos."37 Es decir, este mecanismo genera un bloque de cifrado en el que cada mensaje se le asigna a un número entero, generando dos tipos de claves privada y pública, donde la clave pública debe ser conocida por todos los usuarios, mientras que la clave privada es conocida únicamente por el usuario que originalmente posee los datos.

  Algoritmo AES: Advanced Encryption Standard (AES), es un cifrado de bloque simétrico que utiliza con una longitud de caracteres para la clave de 128 bits. Este mecanismo es uno de los más utilizados hoy por hoy para el cifrado de información por los proveedores de servicios de computación en la nube. Cualquier solicitud para acceder a la información debe suceder luego de que se descifre en el extremo del usuario y el usuario pueda leer los datos de texto sin formato.

[37] RACHNA, Arora; ANSHU, Parashar. Secure User Data in Cloud Computing Using Encryption Algorithms. [Online]. International Journal of Engineering Research and Applications (IJERA) 2013. ISSN: 2248-9622. Disponible en internet: <https://pdfs.semanticscholar.org/9799/a9f9bec6cf85715ca236035b5d89204b326a.pdf>

Algoritmo DES: El Estándar de encriptación de datos (DES), es un algoritmo de clave simétrica, que se encarga de realizar un cifrado de bloques que también se encarga de generar en bloques de tamaño de 64 bits cada uno de los datos enviados por el cliente. Este mecanismo utiliza el mismo algoritmo para el cifrado y descifrado, con pequeñas diferencias. La longitud de clave de este algoritmo es de 56 bits; sin embargo, una clave de 64 bits es una entrada valida.

Algoritmo Blowfish: Este es un algoritmo criptográfico de clave simétrica, el cual se encarga de cifrar la información en bloques de 64 bits con una clave de longitud variable de 128-448 bits, además cuenta con las siguientes características.

- ✓ Velocidad de cifrado de Blowfish rápida en 32 bits microprocesadores es de 26 ciclos de reloj por byte.
- ✓ Compact- Blowfish puede ejecutarse en menos de 5 kb de memoria.
- ✓ Simple-Blowfish usa solo operación primitiva, como la adición, XOR y la tabla de búsqueda, por lo que su diseño e implementación son simples.
- ✓ Seguro: Blowfish tiene una longitud de clave variable de hasta 448 bits de longitud, por lo que es seguro y flexible.Blowfish se adapta a las aplicaciones donde la clave permanece constante durante un tiempo prolongado (por ejemplo, el cifrado del enlace de comunicaciones), pero no donde la clave cambia con frecuencia (por ejemplo, conmutación de paquetes).

8.4. MECANISMOS PARA LA PROTECCIÓN DE LA DISPONIBILIDAD

La disponibilidad es una de las grandes características y ventajas que tiene el modelo de computación en la nube, este permite tener servicios activos y funcionando los 365 días del año las 24 horas, esta disponibilidad es posible cumplirla con la implementación de algunos de los siguientes mecanismos:

- Balanceo de carga:

"El equilibrio de carga en la nube es el proceso de distribución de cargas de trabajo a través de múltiples recursos informáticos."[38], es decir, este mecanismo

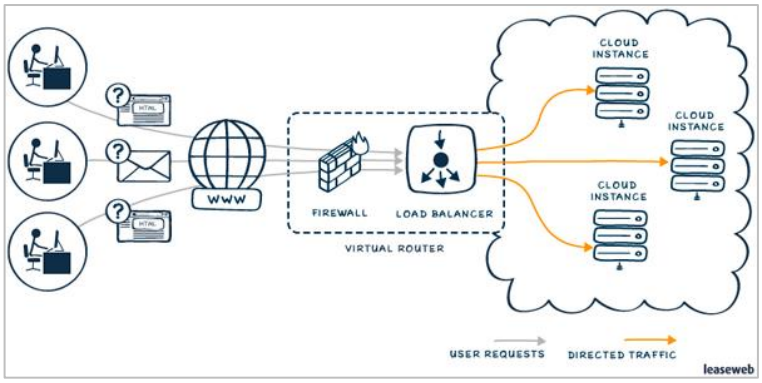
[38] Wikipedia. Cloud load balancing. [Online]. From Wikipedia, the free enciclopedia. 2018. Disponible en internet: <https://en.wikipedia.org/wiki/Cloud_load_balancing>

permite mejorar la disponibilidad de todos los recursos informáticos ya que proporciona un rendimiento mucho mas alto en un tiempo de respuesta menor, además este de reducir las fallas que pueden afectar los sistema de la nube. Cuando uno de los elementos que compone la infraestructura cloud falla, el equilibrador de carga realiza el cambio a los otros recursos disponibles en tiempo real y de manera automática mejorando la disponibilidad y el rendimiento de cada uno de los servidores.

Utilizando una configuración simple, el equilibrador de carga reenviará las conexiones por turnos, yendo a través de cada instancia asignada sucesivamente.

El balanceo de carga en la nube ofrece tener escalabilidad y la agilidad para cumplir con las demandas y las carga de trabajo reubicada y para mejorar la disponibilidad general, como se evidencia en la Figura 5 se puede visualizar que las peticiones pueden ser repartidas a diversos servidores, sin dejar de mencionar que optimiza la distribución del tráfico para que haya una mejor respuesta de los servidores a cada petición realizada por los usuarios.

Figura 5. Arquitectura balanceo de carga



Recuperado de: http://blog.leaseweb.com/2013/08/09/controlling-traffic-in-your-cloud/

El balanceo de carga cloud ofrece algunos mecanismos:

Algoritmos de programación: “Es el algoritmo que asigna cargas de trabajo a nodos en orden libre. Es simple, pero no tiene en cuenta el tiempo de ejecución esperado de cada nodo.”[39]

[39] WANG, S. C.; Yan, K. Q.; Liao, W. P.; Wang, S. S. (2010), "Towards a load balancing in a three-level cloud computing network", Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT), IEEE: 108–113, ISBN 978-1-4244-5537-9

Políticas de balanceo de carga: Dependiendo de la información o requerimiento solicitado, se define una serie de políticas que de manera automática deciden cual nodo es el más adecuado para completar una solicitud y dar una respuesta inmediata al cliente.

Un estudio comparativo de algoritmos: "El muestreo aleatorio sesgado basa su asignación de trabajo en la red representada por un gráfico dirigido. Para cada nodo de ejecución en este gráfico, en grado significa recursos disponibles y fuera de grado significa trabajos asignados."[40]

- Almacenamiento distributivo (Redundancia)

El almacenamiento en la nube está compuesto por diversos recursos y mecanismos distribuidos, pero siendo para los usuarios un único sistema, a menudo denominado redundancia o almacenamiento distribuido. Este tipo de esquemas, permite a los proveedores de servicios de computación en la nube, tener un alto nivel de control respecto a las fallas mediante redundancia y distribución de datos que allí se almacenan, además, también controla la creación de copias y al versionamiento con respecto a las réplicas de datos

Una arquitectura de red representativa para el almacenamiento de datos en la nube se compone de tres entidades, identificadas como:

- ✓ Usuarios: quienes tienen los datos para ser almacenados en la nube y dependen de la nube para el cálculo de datos
- ✓ Cloud Service Provider (CSP): que cuenta con recursos y experiencia significativos en la creación y administración de servidores en la nube distribuidos, posee y opera el sistema de computación en la nube
- ✓ Auditor de terceros (TPA): que tiene experiencia y capacidades que los usuarios pueden no tener

Este mecanismo es una técnica implementada que puede lograr una alta seguridad al dividir los datos del usuario en diferentes fragmentos. Estos fragmentos de información son cifrados y almacenan en bases de datos separadas (en ocasiones separadas geográficamente) que siguen el concepto de distribución de datos a través de la nube. Debido a que cada segmento de datos

[40] Wikipedia. Cloud load balancing. [Online]. From Wikipedia, the free enciclopedia. 2017. Disponible en internet: <https://en.wikipedia.org/wiki/Cloud_load_balancing>

está encriptado y distribuido por separado en bases de datos a través de la nube, esto proporciona seguridad mejorada contra diferentes tipos de ataques.

Es así como esta técnica ayuda al fortalecimiento de la disponibilidad en un entorno Cloud dinámico para sus clientes, sin que estos tengan ningún tipo de inconveniente al momento de requerir sus datos. La redundancia o replicación de información entonces, aumentará la elasticidad del sistema de la nube además de la seguridad de los datos.

8.5. VIRTUALIZACIÓN

"La virtualización es el proceso de crear un entorno virtual en un servidor existente para ejecutar el programa deseado, sin interferir con otros servicios proporcionados por el servidor o la plataforma de host a otros usuarios"[41]. Es decir, las virtualizaciones permiten la generación de una sola instancia de trabajo o una combinación de muchas, con diferentes sistemas operativos, servidores de red, aplicaciones, entornos informáticos, dispositivos de almacenamiento y otros recursos necesarios.

En otras palabras, la virtualización es una de las principales formas para ahorrar recursos económicos dentro de las compañías, por ende se ve una reducción significativa en la adquisición de equipos (hardware) y a su vez un ahorro de energía, esto sin contar con el tiempo y los recursos necesarios para una eventual mantenimiento de instancias. Así entonces, la virtualización permite que se comparta una única instancia física de un recurso o sistema con múltiples clientes y organizaciones.

"La virtualización en la computación en la nube le permite ejecutar múltiples aplicaciones y sistemas operativos en el mismo servidor, lo que permite una utilización eficiente de los recursos y reduce los costos."[42] La virtualización es sumamente importante en el modelo de la computación en la nube, ya que la idea es no tener un único servidor por cliente sino por el contrario en un único servidor

[41] The Different Types of Virtualization in Cloud Computing – Explained. [Online]. Redswitches.com. 2017. Disponible en internet: <https://redswitches.com/blog/different-types-virtualization-cloud-computing-explained/>

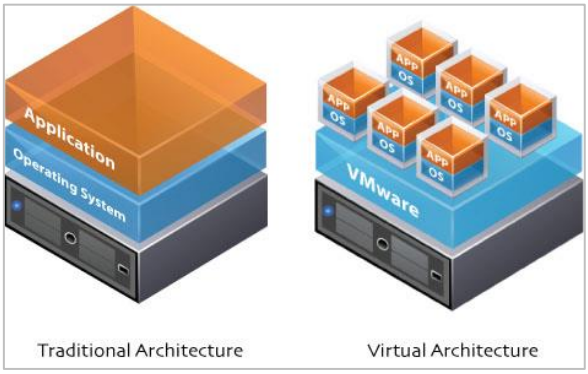
[42] The Different Types of Virtualization in Cloud Computing – Explained. [Online]. Redswitches.com. 2017. Disponible en internet: <https://redswitches.com/blog/different-types-virtualization-cloud-computing-explained/>

virtualizar diferentes entornos de trabajo para diferentes organizaciones, es decir, los clientes comparten los datos presentes que almacenan en la nube, pero realmente por medio de la virtualización los usuarios comparten una o varias Infraestructura.

Uno de los principales objetivos de la virtualización es el de proporcionar a las aplicaciones versiones estándar para todos los usuarios que hacen uso de ella, por ejemplo si es necesaria una actualización a una corrección de un incidente, los proveedores no deben realizar está a cada uno de los servicios de los clientes sino únicamente a los servidores donde almacenan o está configurada la virtualización.

En la Figura 5, se puede ver un ejemplo de arquitectura tradicional vs una virtualizada, donde se evidencia como la virtualización cloud, genera varios nodos (Servidores) que permiten una alta disponibilidad.

Figura 6. Arquitectura virtualización.



Fuente: https://redswitches.com/blog/different-types-virtualization-cloud-computing-explained/

La virtualización ofrece varios tipos de servicios a virtualizar, a continuación analizaremos cada uno de ellos.

Virtualización de Hardware.

Este tipo de virtualización se basa en el concepto simular un hardware o un servidor físico el cual puede estar compuesto de múltiples segmentos o servidores de hardware más pequeños, esto entonces reúne varios servidores físicos en un único servidor virtual que se ejecuta en un solo servidor físico primario. Cada uno de los demás servidores pequeños pueden contener una máquina virtual, pero

todo el clúster de servidores se trata como un único dispositivo por cualquier proceso que solicite el hardware.

- Virtualización de Software.

> "La virtualización de software implica la creación de una operación de múltiples entornos virtuales en la máquina host. Crea un sistema informático completo con hardware que permite ejecutar el sistema operativo invitado. Por ejemplo, le permite ejecutar el sistema operativo Android en una máquina host de forma nativa utilizando un sistema operativo Microsoft Windows, utilizando el mismo hardware que la máquina host."[43]

- Virtualización de almacenamiento.

La virtualización de almacenamiento se da por un conjunto de servidores que son administrados por un único sistema de almacenamiento virtual, es decir, los servidores saben no deben saber dónde están ubicados los datos, y en "su lugar funcionan más como abejas obreras en una colmena"[44]. Esta virtualización permite hacer el seguimiento del almacenamiento desde múltiples plataformas para administrar y utilizarla como un único repositorio el software de virtualización. Esto permite tener más ventajas a la hora del almacenamiento en en los dispositivos dirigidos a esta actividad con diferentes capacidades y velocidades, menos tiempo de no productividad, balanceo de cargas de trabajo y una mejor optimización del rendimiento de todos los recursos del sistema.

- Virtualización de Network.

Este tipo de virtualización permite ejecutar múltiples redes virtuales que tienen un control y un plano de datos separados. Esta permite la administración y monitoreo de una red como una única entidad administrativa desde una única consola de administración. La virtualización de red también puede traer consigo

[43] The Different Types of Virtualization in Cloud Computing – Explained. [Online]. Redswitches.com. 2017. Disponible en internet: <https://redswitches.com/blog/different-types-virtualization-cloud-computing-explained/>

[44] NAMRATA, Bisht. Virtualization In Cloud Computing and Types. [Online]. Advant Navis Business Park Graphic Era University (GEU) Dehradun. 2018. Disponible en internet: <https://www.geeksforgeeks.org/virtualization-cloud-computing-types/>

misma la virtualización del almacenamiento, la cual implica administrar todo el almacenamiento en un único servidor.

La virtualización tiene como objetivo optimizar el funcionamiento de la red de los volúmenes de transferencia de datos, flexibilidad, escalabilidad, confiabilidad y seguridad. “Automatiza muchas tareas administrativas de red, que en realidad disfrazan la verdadera complejidad de una red. Todos los servidores y servicios de red se consideran un conjunto de recursos, que se pueden usar sin tener en cuenta los componentes físicos”[45].

[45] TECHOPEDIA. Network Virtualization. [Online]. techopedia.com. 2018. Disponible en internet: <https://www.techopedia.com/definition/655/network-virtualization>

9. ANALISIS DEL GRADO DE SEGURIDAD EN SERVICIOS SAAS E IAAS EN LA COMPUTACIÓN EN LA NUBE.

Realizado el análisis de cada uno de los textos de los diferentes autores se logró identificar los mecanismos, herramientas, soluciones y procesos que los proveedores de servicios de computación en la nube utilizan, para mejorar sus esquemas de seguridad respecto a dichos servicios y poder brindar a sus clientes plataformas mucho más seguras y protegidas para el beneficio general.

Lo primero que se debe mencionar es que los proveedores de este modelo, cuentan con una infraestructura de red bastante protegida para así lograr asegurar los servicios que ofrecen. Para esto realizan una protección a sus dispositivos físicos (servidores, enrutadores, cables, etc.) ante posibles accesos no autorizados, interferencias de datos, robos y fugas de información, desastres naturales como incendios, inundaciones, entre otros.

Los servicios que ofrece la computación en la nube utilizan los más altos estándares de seguridad y metodologías reconocidas, además, cuentan con medidas de seguridad lo suficientemente fiables y es bastante complejo que alguien logre vulnerar estas medidas para acceder a la información o datos.

Todos los servicios de la nube además, cuentan con backups o copias de seguridad programadas para que se ejecuten automáticamente. Esto le da un poco más de tranquilidad a los usuarios ya que no debe preocuparse por una pérdida de sus datos y archivos, y en un caso hipotético donde esto suceda, las copias de seguridad entrarían a cumplir con su objetivo. Una de las ventajas de estos tipos de backups, es que al ser automáticos aumentan el tiempo de productividad, disminuye esfuerzos y además no consumes recursos propios de tus dispositivos

Este tipo de proveedores tiene internamente un diseño e implementación de controles, tanto disuasivos, preventivos, como correctivos, además estos garantizan para la protección de la red con la utilización de mecanismos como los Firewall cloud, sistema de prevención de intrusos IPS y Sistema de Detección de Intrusos IDS, todos estos para garantizar la seguridad de la red de sus instalaciones y sobretodo servidores donde corren los procesos que ofrecen.

Los proveedores de servicios de computación en la nube, cuentan con sistemas antivirus de última tecnología y con bases de datos actualizadas para lograr

proteger la información de sus clientes ante cualquier malware. En otras palabras, la información sensibles de las organizaciones, estarán mucho más seguras de virus informáticos o perdidas en la nube que en el disco duro de un equipo de la empresa, además, ofrecen centros de cómputo con lo más alto en tecnología para asegurar sus servicios, donde se debe centralizar en la protección de estas instalaciones y su correcto manejo, para esto también debe saber, de qué forma son protegidos.

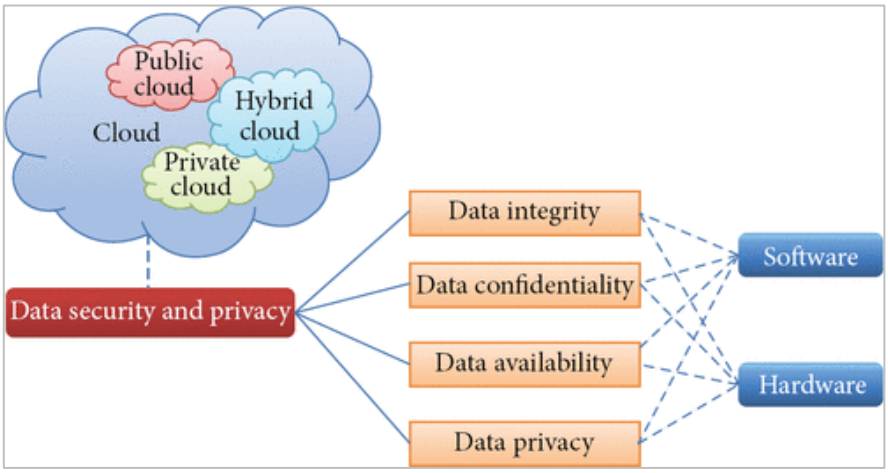
Por otra parte, para software y la infraestructura como servicio, estos garantizan la integridad, confidencialidad y disponibilidad en la información, por medio de una serie de mecanismos, herramientas y procesos para la satisfacción de sus clientes.

- Seguridad de los datos.

La seguridad de los datos y la protección de la privacidad, como se mencionó anteriormente son los dos factores principales de las preocupaciones de los usuarios sobre la tecnología de la nube, esta es quizás la inquietud que más se hacen los usuarios que piensan en servicios o infraestructura en la nube, “¿Y mis datos si están lo suficientemente protegidos”, “¿qué metadatos tiene el proveedor sobre sus datos, cómo está asegurado y qué acceso tiene usted, el cliente, a esos metadatos?” ya que desconocen de qué forma este nuevo modelo se encarga de proteger de manera segura el activo más valioso para sus clientes.

En la figura 7 se puede apoyar el análisis realizado donde se logran identificar cuáles son las características que conforman la seguridad de los datos, dentro de un modelo de computación en la nube, subrayando que la confidencialidad, integridad, disponibilidad y privacidad son pilares fundamentales para la seguridad de la computación en la nube.

Figura 7. Organization of data security and privacy in cloud computing.



Tomada de: http://journals.sagepub.com/doi/full/10.1155/2014/190903

La seguridad de los datos dentro de un modelo de computación en la nube, se basa en los siguientes cuatro elementos:

- Integridad de la información
- Confidencialidad de la información.
- Disponibilidad de la información
- Privacidad de la información.

Cada uno de los elementos anteriores, limitan y minimizan posibles afectaciones de los datos en un sistema de información bajo el modelo de la computación en la nube, a continuación se explicará cada uno de ellos.

9.1. INTEGRIDAD DE LA INFORMACIÓN

Este elemento, es quizás el más críticos en cualquier sistema de información, por tanto la computación en la nube ofrece por medio de sistemas independiente de base de datos, es decir, la integridad se mantiene por medio de las restricciones y transacciones dentro de la base de datos, las cuales terminan siendo controladas por un sistema de administración de bases de datos. Las transacciones deben seguir las propiedades ACID (atomicidad, consistencia, aislamiento y durabilidad) para garantizar la integridad de los datos.

También, la computación en la nube, ofrece un control de acceso a los datos, por medio del cual garantiza qué nivel de acceso tiene cada uno de los usuarios dentro del sistema autenticado, para así lograr proteger los activos de información dentro de la base de datos.

Dentro de la computación en la nube, la integridad de los datos controla que los usuarios no autorizados no se les permitan realizar ningún tipo de alteración a la información. “La integridad de los datos es la base para proporcionar servicios de computación en la nube como SaaS, PaaS e IaaS.”[46]

La computación en la nube evita los accesos no autorizados, de esta forma brinda a las organizaciones una mayor confianza en la integridad de los datos. Además, por medio de mecanismos de monitoreo, brinda una mayor visibilidad controlar e identificar quién, cuándo o qué, trató o está tratando de alterar la información de un sistema, claramente una violación a la integridad. Es por esto que los proveedores de computación en nube siempre garantizan la integridad y precisión de los datos y en caso de ser burlada, tiene como informar e indicar con detalles que fue lo que ocurrió.

Tanto SaaS con IaaS deben velar por la integridad de la información, para esto la computación en la nube apalanca estos servicios en los mecanismo y herramientas analizados, como los log de transacciones, los cuales se definen como un registro dentro de la base de datos donde todos los cambios realizados a los datos son registrados, es decir todas las operaciones que un usuario realice sobre los registros almacenados (insert-update-delete) generan un nuevo registro

[46] YUNCHUAN Sun, JUNSHENG Zhang, YONGPING Xiong, GUANGYU Zhu. Data Security and Privacy in Cloud Computing. [Online]. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks. 2014. 4 p. Disponible en internet: <http://journals.sagepub.com/doi/full/10.1155/2014/190903>

por cada transacción realizada generando una bitácora de cuando inició, que se hizo dentro de ella y si se completó exitosamente.

Además para estos dos servicios, se demuestra el desarrollo de procesos de autorías para que los clientes estén al tanto del correcto funcionamiento de cada una de las operaciones y servicios ofrecidos, todo esto en pro de la seguridad de la información de cada uno de los clientes, con esto se le garantiza al cliente que se está haciendo un control detallado al cumplimiento de las normas, controles y parámetros establecidos para controlar la seguridad en los datos, en los controles de acceso, dispositivos físicos, redes de comunicaciones, aplicaciones, entre muchos más elementos.

También es importante remarcar que la mayoría de empresas que ofrecen servicios de computación en la nube, se les realizan periódicamente auditorías externas y los resultados son dados a conocer a todos sus clientes para tranquildad de ellos, además de contar con certificaciones ISO 27000.

Como en muchas de las tecnologías existen diferentes métodos de autenticación, pero la gran mayoría trata de volver estos métodos un poco más seguros por medio de técnicas encriptación.

Para las autenticaciones se busca entonces evitar el ingreso y uso no contemplado a los recursos de una red o sistema. La criptografía busca proveer la seguridad de las redes informáticas tanto públicas como privadas, y así proteger la confidencialidad de la información transmitida la integridad y la disponibilidad de la misma.

La computación en la nube también hace uso de las técnicas de encriptación para proteger sus servicios de accesos no autorizados o intentos de vulnerar las conexiones pero ve que estos métodos o técnicas deben ser mejorados y optimizados para seguir garantizando una alta calidad en términos de seguridad.

Microsoft recalca la importancia de las autenticaciones y accesos a los servicios de la computación en la nube donde estos “presentan nuevos desafíos en autenticación y autorización, ya que las organizaciones deben ser capaces de identificar a los usuarios con confianza sin generar gastos indirectos excesivos relacionados con el aprovisionamiento de cuentas”. [47]

[47] HINDER, Thomas W. Microsoft Reference Architecture for Private Cloud: Cloud Security Introduction. [Online]. Microsoft 2011.,1 p. Disponible en internet: <https://social.technet.microsoft.com/wiki/contents/articles/3801.cloud-security-introduction.aspx>

9.2. CONFIDENCIALIDAD DE LA INFORMACIÓN

Dentro de este modelo, los proveedores de dichos servicios buscan siempre mantener la confidencialidad de la información por medio de un conjunto de reglas que delimita el acceso a la información; la integridad es la forma de garantizar de que la información es veraz, mientras que la disponibilidad es quien garantiza que siempre se tiene acceso a la información.

Por otra parte, también se busca que estos servicios sean lo suficientemente confiables, porque lo que hace es albergar información muy importante para la empresa, la cual tiene un valor incalculable, esta debe permanecer intacta para poder cumplir a cabalidad la tarea encomendada; si no es así, esto podría generar graves problemas para la empresa los cuales podrían traducirse en pérdida de dinero; por todo lo anterior, se han generado políticas de seguridad en donde se crean cláusulas que se deben cumplir para evitar que la información deje de ser confiable, porque si esto sucede ya no va a servir de mucho. Para culminar con una explicación exacta de este concepto podemos decir que la confidencialidad está completamente ligada a que a la información sólo pueda tener acceso personal con permisos expresos para tal fin, el resto de las personas no pueden acceder a ella.

La computación en la nube se apalanca de varios procesos para garantizar la confidencialidad de la información que protegen. Dentro de las principales técnicas esta la más importante que es el cifrado de datos, esta se realiza por medio de Los algoritmos de criptografía son los más eficientes herramienta para garantizar la seguridad del almacenamiento de datos en el nube. De hecho, hay muchas encriptaciones algoritmos que pueden encriptar los datos y convertir en un formato incomprensible, para asegurar su confidencialidad.

Para asegurar la confidencialidad de la información tanto el servicio de SaaS como de IaaS, los proveedores de estos servicios utilizan herramientas y mecanismos de encriptación que permiten que la información tenga un grado de seguridad con respecto a la movilidad de esta y ante una mínima posibilidad de ser interceptada. Este modelo se apalanca para la encriptación de la información de forma simple u homomórfica, por medio de la utilización de diferentes tipos de algoritmos de encriptación como RSA, AES, DES, Blowfish, que garantiza a sus cliente que la

información al momento de viajar y ser almacenada en sus bases de datos, no se está haciendo de manera plana y que su contenido está siendo protegido.

La encriptación entonces no solo se encarga de proteger los accesos y las conexiones sino también de ocultar la información que es visible al "ojo" humano para protegerla de accesos no autorizado, interceptaciones, edición y manipulación.

9.3. DISPONIBILIDAD DE LA INFORMACIÓN

La disponibilidad es el grado o la medida en que los datos almacenados por el proveedor de servicios cloud, son fácilmente utilizados sin importar la ubicación, horario o dispositivo, es decir, una buena disponibilidad de información, se basa en que el cliente siempre cuente con sus datos 7/24 los 365 días del años.

"La alta disponibilidad es, en última instancia, el santo grial de la nube. Incorpora la idea de acceso en cualquier lugar y en cualquier momento a servicios, herramientas y datos, y es el habilitador de visiones de un futuro con empresas sin oficinas físicas o de empresas globales con sistemas de TI completamente integrados y unificados"[48]

Este elemento es también uno de los grandes desafíos de la computación en la nube, la buena noticia es que cada vez se ofrecen nuevos y mejorados mecanismos que se ofrecen los proveedores de la computación en la nube a sus clientes, para que estos siempre puedan contar con la información en el momento que sea necesario. Como cualquier sistema de información es normal que en algún momento se presente algún tipo de falla o avería que afecte la disponibilidad, es por esto que este nuevo modelo adopta algún mecanismo que logran mantener grandes volúmenes de datos durante largos períodos a disposición de sus clientes.

Es de suma importancia la disponibilidad de los servicios para los clientes de dicho modelo, por esto la computación en la nube, apalanca y fortalece este servicio por medio de mecanismos que garanticen una alta disponibilidad de sus servicios, haciendo uso de herramientas como el balance de carga y el almacenamiento

[48] RODRIGUES, Thoran. What high availability for cloud services means in the real world. [Online]. The Enterprise Cloud. 2011. Disponible en internet: <https://www.techrepublic.com/blog/the-enterprise-cloud/what-high-availability-for-cloud-services-means-in-the-real-world/>

distribuido. Con estas dos herramientas, lo que buscan los proveedores de dicho servicio, es optimizar el funcionamiento de sus dispositivos para que estos operen de una forma adecuada y así logren responder cada vez que les sea necesitado por tarde cliente. Principalmente el balanceo de carga lo que le permitirá al proveedor es la utilización segmentada de los servicio y distribuir de manera equitativa la demanda de los clientes para así no saturar una sola maquina sino que por el contrario al mismo tiempo varias máquinas trabajen en conjunto y el regimiento sea mucho mejor.

El tema del almacenamiento es uno de los más importantes pilares de la computación en la nube, este es un punto que quizás interesa más a los clientes ya que es allí, al conocer el funcionamiento donde se deciden a adaptarse al nuevo modelo. Es por esto que los proveedores de estos servicios diseñan diferentes estrategias y proceso para mitigar y disminuir los riesgos y uno de ellos es el almacenamiento distributivo, es decir, la información de un cliente no se encuentra almacenada en un único servidor sino que por el contrario esta es replicada en diferentes dispositivos que a su vez están ubicados geográficamente en diferentes lugares, esto para garantizar que si por alguna falla de carácter natural (Terremotos, incendio, inundaciones, tormentas, entre otras), un servidor diferente pueda iniciar su respaldo y la transición de uno a otro sea totalmente transparente para el cliente y que el servicio siempre esté disponible para ser usado.

9.4. PRIVACIDAD DE LA INFORMACIÓN

Uno de los principales pilares que debe garantizar la computación en la nube, la privacidad de la información, cuando hablamos de este término, podemos entender de primer momento que se hace referencia al ocultamiento algún tipo de datos frente a entes externos, en realidad esto va mucho más allá, es decir, la privacidad que deben ofrecer los proveedores de la computación en la nube, se basa en la recopilación, el uso, la divulgación, el almacenamiento y la alteración a datos confidenciales, por ende la privacidad se debe velar a las organizaciones en el manejo transparente de los datos y las buenas prácticas de la organización en torno al manejo información personal.

“El correcto establecimiento de políticas de privacidad de la información en este tipo de servicios (sea SaaS, PaaS, IaaS) evita que datos como: nombre, tarjeta de crédito, registros biométricos, etc., puedan ser usados para distinguir o

rastrear la identidad de un individuo; y éstos se utilicen para cometer fraudes, robos de identidad, envío de correo no deseado, entre otros."[49]

Los proveedores de servicios deben garantizar que cumplen con políticas de seguridad que garantices la seguridad de la información que albergan y que a su vez mantenga la privacidad de la misma, pero acá lo importante es que los clientes conozcan estas políticas y sepan de qué forma su proveedor, cumple con las reglas mínimas para velar por la privacidad de la información de sus procesos.

A continuación algunos puntos fundamentales utilizados para mantener la privacidad en la información confidencial:

- Dar a conocer a los usuarios toda la información relacionada con las prácticas y procedimientos de seguridad que se incluyen en los Niveles de Servicio.
- Dar a conocer a sus clientes, donde se encuentra almacenada su información, en términos de la localización geográfica.

- Aplicar y demostrar de qué forma los requisitos de acceso a la información impuestas por los usuarios están siendo implementados.

- Para la información almacenada, creada, generada, alterada o eliminada, en cualquier otra forma asociada con la propiedad intelectual del usuario, no podrá reclamarse como de propiedad del proveedor.

- Debe estar muy claro el alcance de la política de privacidad de la compañía con respecto a qué puede y no hacer el proveedor con la información del usuario.

- Implementar mecanismos de auditorías o log de eventos donde se evidencia cada acceso o alteración a la información.

- Demostrar que se tiene implementados mecanismos de cifrado de información robusto para el de almacenamiento de la información, para evitar una fácil visualización de ellos cuando estos sean reciclados.

[49] GARCÍA VIZCAÍNO, Julio; CRUZ VALENCIA, Galvy. Privacidad de la Información en la Nube. [Online]. México. 2018. Disponible en internet: <https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube>

- Destruir toda la información, cuando el usuario lo requiera, en todas las localizaciones físicas y lógicas demostrando los resultados de dicha actividad.

Así como los proveedores de servicios de computación en la nube son en gran parte los responsables de la privacidad de la información, los usuarios también debe cumplir con algunas acciones que apoyen y fortalezcan los procesos del proveedor, a continuación alguna de estas acciones:

- Identifica las leyes y directivas del país donde la información se ubica físicamente.

- Definir y analizar, cuales son los usuarios que deben tener acceso a la información, y que acciones pueden realizar sobre ella.

- Tener una segmentación o clasificación de la información para identificar el grado de importancia de la misma. Revelar información cuando sea requerida por una autoridad legal.

- Comprender los procesos de retiro de almacenamiento por del proveedor.

- Desarrollar planes de retención y destrucción de la información.

Es así entonces que a la inquietud de ¿por qué en la actualidad se sigue desconfiando de la seguridad que ofrece la computación en la nube para el software y la infraestructura cómo servicio? Personalmente diría que se debe a la falta de información clara y concisa acerca de la seguridad de la computación en la nube, ya que es uno de los modelos más seguros de la actualidad con respecto a la seguridad de la información, por encima de grandes datacenters de enormes organizaciones.

"Los datos procesados o almacenados fuera de los límites físicos de una organización, su firewall y otros controles de seguridad conllevan un nivel de riesgo inherente." [50]

[50] WAYNE Jansen; GRANCE Timothy. Guidelines on Security and Privacy in Public Cloud Computing. [Online]. NIST US Departament or Commerce. 2011. Disponible en internet: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>

CONCLUSIONES

Se recopiló y analizó la información necesaria acerca de la situación actual de la computación en la nube, sus modelos de servicios, modelos de implementación y sus principales características en los servicios SaaS e IaaS.

Se identificaron todas las ventajas y beneficios que ofrece la computación en la nube entre ellas la reducción de costos ya que esta es quizás la ventaja más atractiva, de no serlo, es una de las más evidente de todas las que ofrece esta tecnología, además otra de las principales ventajas es la disponibilidad y accesibilidad que estos servicios, ya que ofrecen un alto porcentaje de prestación de sus servicios sin fallas de interrupción.

Como todo modelo o servicio que se presta, se identificaron algunas desventajas, las cuales no hacen que estos servicios dejen de ser atractivos para los clientes, una de ella son las amenazas organizacionales, estás apuntan a algunos descuidos, como puertas abiertas que se produzcan posibles ataques, sesiones abiertas, trabajo remoto, conexiones no seguras, todo estos incumplimientos a las políticas de seguridad traen consigo mismo un sinfín de vulnerabilidades que pueden ser aprovechadas por la criminalidad

Se evidenció como para los proveedores de servicios SaaS e IaaS, implementan diferentes controles para la seguridad en generar de su infraestructura tecnológica como los son controles de disuasión, los cuales ayudan con la disminución de posibles ataques, también y no menos importante están los controles preventivos, estos son de mucha ayuda en estos modelos ya que están trabajando constantemente para la prevención de ataques y fortalecer los sistema contra incidentes, pero su principal objetivo es reducirlos. En los tipos de controles se identificaron mecanismos como firewall cloud e IPS (Sistema de prevención de intrusos).

De igual forma se identificó que la computación en la nube apalanca sus procesos de seguridad en mecanismos de detección temprana de incidentes, como los IDS (Sistema de Detección de Intrusos), con este puede detectar y reaccionar de manera adecuada y oportuna frente a cualquier incidente o ataque que se esté llevando acabo. Todo esto en caso de una eventual afectación.

Se identificó que por medio de los logs de transacciones, la computación en la nube garantiza la integridad de la información y de todo lo que vaya sucediendo con sus servicios o sistemas, vaya quedando grabado en sus bases de datos, es

decir, permiten a los clientes de la computación en la nube, saber exactamente que está ocurriendo con sus datos, que usuarios intervienen en ellos y de que forman lo hacen y así poder garantizar la integridad de los mismos.

Como cualquier sistema de información, los servicios SaaS e IaaS ofrecidos por la computación en la nube, son periódicamente auditados, tanto internamente como por personal externo experto en la seguridad de dichos servicios, esto para garantizar a los clientes que los proveedores cumplen con las medidas y normativas definidas para la seguridad de la información.

La utilización de los diferentes métodos de encriptación de la información, evidenció que estos son mecanismos muy utilizados y de alto nivel de confidencialidad para el manejo de la información de los clientes dentro de los servicios cloud, los cuales garantizan a los clientes que su información está siendo codificada no solo cuando ésta está en tránsito por la red sino también que es encriptadas al momento de ser almacena, esto con la última tecnología a nivel de algoritmos de encriptación a nivel mundial como RSA, DES, AES.

La disponibilidad es uno de los pilares de los servicios cloud, esto debido al método de distribución de carga y almacenamiento distribuido. Así como también lo es la ubicación de datacenter en diferentes zonas geográficas, se identificó que eso asegura una alta disponibilidad de los servicios, ya que la información siempre está replicada en otro servidor y al momento en que uno deja de funcionar, inmediatamente alguno de los demás comienza a operar, siendo esto totalmente transparente para los usuarios.

RECOMENDACIONES

La computación en la nube puede generar dudas con respecto a la seguridad, pero la utilización de los servicios ofrecidos como el SaaS e IaaS brindan mecanismos de última tecnología que permiten despejar todo es tipo de dudas y aclarar y poner en evidencia el alto nivel de seguridad que promete.

Es importante reconocer que uno de los pilares de la seguridad de la información es el más preciado para la computación en la nube, la confidencialidad no es uno de los puntos frágiles de este modelo, por el contrario es una de las fortalezas que ofrece a los clientes para asegurar y no tener duda del alto grado de resguardo de la información

Tener a todo tiempo disponible los recursos es otra de las características que ofrece la computación en la nube, con la computación en la nube, poder acceder en cualquier momento a la información se vuelve un plus para este modelo sin importar el dispositivo, por esta razón es totalmente recomendable la implementación de dicho modelo para tener la estabilidad y disponibilidad que requieren hoy en día las organizaciones

Integridad ofrecida por el modelo cloud, ayudará a las organizaciones a tener claro que es lo que va pasando con la información y modelo, permitirá tener claridad por medio de auditorías y log que ayudarán a tener un panorama claro de que forma se está interactuando con los datos.

La responsabilidad sobre el manejo de la seguridad cloud no es únicamente del proveedor, se debe tener en cuenta que internamente deben existir procesos de protección de la información empresarial para los usuarios, que permitan brindar y dar a conocer las políticas de seguridad de información internas y que están sean evaluadas y auditadas periódicamente.

Los proveedores de servicios cloud demuestran de una forma verídica los diferentes controles y métodos que utilizan para proteger la integridad, confidencialidad y disponibilidad de la información en sus servicios y así a los clientes se les puede demostrar que es un servicio en el cual se puede confiar para la implementación de sus procesos organizacionales.

Los proveedores de estos servicios, siempre demuestran sus planes de acción frente a posibles fallas de seguridad y comprueben el grado real de probabilidad

de que sus servicios dejen de funcionar, esto es importante para tener claro el panorama ante una posible eventualidad de qué forma se proceden.

La computación en la nube ofrece y garantiza un servicio de backup periódico, que ayudan a asegurar que los datos sean almacenados en sitios diferentes en función de una correcta disponibilidad tanto de información como de servicios, esto le permitirá a los clientes a siempre poder tener disponible la información sin importar el contexto.

Los proveedores de servicios IaaS e Iaas cuentan con certificación en norma ISO 27001 y 27002, ISO 31000 los cuales garanticen métodos efectivos para la seguridad de la información.

Tener en cuenta que ante una posible violación de las leyes colombianas frente a la seguridad de los datos y la información, los proveedores de servicios cloud puedan ser sometidos y juzgados por medio de esta ante una posible vulneración de la misma.

BIBLIOGRAFÍA

ANCELIT, ANALIDA Y SHARITO. Encriptacion de datos. [En línea]. Blogger.com. 2007. Disponible en: http://encriptaciondedatos.blogspot.com.co/2007/09/encriptacion-de-datos.html

BLOUNT, Sumner; ZANELLA, Rob. Cloud Security and Governance: Who's on Your Cloud?. [En línea]. IT Governance Publishing. 2010. Base de datos: eBook Collection. Disponible en http://eds.a.ebscohost.com.consultaremota.upb.edu.co/eds/ebookviewer/ebook/bmxlYmtfXzM5MTEyMF9fQU41?sid=2b007c10-744b-41ed-bb89-b4d54f0918fa@sessionmgr4006&vid=3&format=EB

Cloud computing security. From Wikipedia, the free enciclopedia. [En línea]. 2018. Disponible en https://en.wikipedia.org/wiki/Cloud_computing_security#Security_and_privacy

COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1273 (5, enero, 2009). De La Protección De La Información Y De Los Datos. Ministerio TIC. Bogota D.C., 2009.

Dinero. El 62% de las compañías más grandes ya usan cloud computing. [En línea]. Bogotá: Dinero. 2012.,1 p. Disponible en http://www.dinero.com/negocios/tecnologia/articulo/el-62-companias-mas-grandes-usan-cloud-computing/141978

EL CONGRESO DE COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C., 2012.

European Commission, Information Society and Media, “The Future of Cloud Computing. Opportunities for European Cloud Computing beyond 2010”. [En línea]. CORDIS. 2010, disponible en: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

GARCÍA VIZCAÍNO, Julio; CRUZ VALENCIA, Galvy. Privacidad de la Información en la Nube. [En línea]. México. 2018. Disponible en https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

GOIKOLEA, Markos. ¿Qué es un sistema SaaS? Definición y ventajas. [En línea]. Digital Business. 2014. Disponible en http://www.iebschool.com/blog/que-es-saas-definicion-ventajas-digital-business/
JOYANES AGUILAR, Luis. COMPUTACIÓN EN LA NUBE: Notas para una estrategia española en cloud computing. S.A 2012.

LOEFFLER, Bill. Cloud Computing: What is Infrastructure as a Service. [En línea]. Microsoft.2011. Disponible en https://technet.microsoft.com/en-us/library/hh509051.aspx

LOL, Cloud. Modelos de Implementación. [En línea]. Lol Cloud. 2017. Disponible en https://www.licenciasonline.com/bo/es/cloud/modelos-de-implementacion

MATHER, Tim. KUMARASWANY Subra. LATID Shahed. Cloud Security, an Enterprice Perpective on Risk Compliance. O'REILLY Media, Inc. 2009.

MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [En línea]. Gaithersburg. NITS. 2011., 1 p. Disponible en https://csrc.nist.gov/publications/detail/sp/800-145/final

MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [En línea]. Gaithersburg. NITS. 2010. Disponible en https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf

NAMRATA, Bisht. Virtualization In Cloud Computing and Types. [En línea]. Advant Navis Business Park Graphic Era University (GEU) Dehradun. 2018. Disponible en https://www.geeksforgeeks.org/virtualization-cloud-computing-types/

NATE Lord. Cryptography in the Cloud: Securing Cloud Data with Encryption. [En línea]. digitalguardian.com 2017.Disponible en: https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption

Primorac, Carlos R. Computación en la nube. Trabajo de grado en Licenciatura en Sistemas de Información Comunicaciones de Datos. Universidad Nacional del Nordeste. Facultad de Ciencias Exactas y Naturales y Agrimensura. 2014.

RACHNA, Arora; ANSHU, Parashar. Secure User Data in Cloud Computing Using Encryption Algorithms. [En línea]. International Journal of Engineering Research and Applications (IJERA) 2013. ISSN: 2248-9622. Disponible en: https://pdfs.semanticscholar.org/9799/a9f9bec6cf85715ca236035b5d89204b326a.pdf

ROBERTO, Carlos. La desconfianza hacia la nube en las empresas. [En línea]. TicPymes. 2011.,2 p. Disponible en https://www.pymesyautonomos.com/tecnologia/la-desconfianza-hacia-la-nube-en-las-empresas

RODRIGUES, Thoran. What high availability for cloud services means in the real world. [En línea]. The Enterprise Cloud. 2011. Disponible en https://www.techrepublic.com/blog/the-enterprise-cloud/what-high-availability-for-cloud-services-means-in-the-real-world/

ROUSE, Margaret. Infrastructure as a Service (IaaS). [En línea]. TechTarget. 2014. Disponible en http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

SANTOS, Mateo. SaaS, IaaS y PaaS: ¿qué son, cómo usarlos y para qué?. [En línea]. Bogotá. Enter.com. 2015. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/saas-iaas-y-paas-que-son-como-usarlos-y-para-que/

SAS 70. [En línea]. American Institute of Certified Public Accountants (AICPA). 2018 Disponible en http://sas70.com/FAQRetrieve.aspx?ID=33288

SHINDER, Thomas W. Microsoft Reference Architecture for Private Cloud: Cloud Security Introduction. [En línea]. Microsoft. 2011.,1 p. Disponible en https://social.technet.microsoft.com/wiki/contents/articles/3801.cloud-security-introduction.aspx

TECHOPEDIA. Network Virtualization. [En línea]. techopedia.com. 2018. Disponible en https://www.techopedia.com/definition/655/network-virtualization

The Different Types of Virtualization in Cloud Computing – Explained. [En línea]. Redswitches.com. 2017. Disponible en https://redswitches.com/blog/different-types-virtualization-cloud-computing-explained/

TÜCKLER, Hjalmar. Evolución de la computación en la nube en AL. [En línea]. La prensa. 2014.,2 p. Disponible en https://www.laprensa.com.ni/2014/10/25/economia/215932-evolucion-de-la-computacion-en-la-nube-en-al-telecomunicaciones

VIOLINO, Bob. The dirty dozen: 12 top cloud security threats for 2018. [En línea]. CSO Online. 2018. Disponible en

https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

WANG, S. C.; Yan, K. Q.; Liao, W. P.; Wang, S. S. (2010), "Towards a load balancing in a three-level cloud computing network", Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT), IEEE: 108–113, ISBN 978-1-4244-5537-9

WAYNE Jansen; GRANCE Timothy. Guidelines on Security and Privacy in Public Cloud Computing. [En línea]. NIST US Departament or Commerce. 2011. Disponible en: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Wikipedia. Cloud load balancing. [En línea]. From Wikipedia, the free enciclopedia. 2018. Disponible en https://en.wikipedia.org/wiki/Cloud_load_balancing

YUNCHUAN Sun, JUNSHENG Zhang, YONGPING Xiong, GUANGYU Zhu. Data Security and Privacy in Cloud Computing. [En línea]. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks. 2014. Disponible en http://journals.sagepub.com/doi/full/10.1155/2014/190903

Anexo ( ) RESUMEN ANALÍTICO DE EDUCACIÓN - RAE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FECHA			Diciembre de 2019				
TITULO			SEGURIDAD EN SOFTWARE E INFRAESTRUCTURA COMO SERVICIO DE LA COMPUTACIÓN EN LA NUBE.				
AUTOR			Héctor Isaac Hernández Vergara				
DIRECTOR (ES)/ ASESOR(ES)			YOLIMA MERCADO				
Año			2019				
DESCRIPCIÓN			Por medio de este documento se dan a conocer los propósitos de la investigación, el problema a resolver, la metodología, las conclusiones y las recomendaciones luego del análisis realizado.				
PAGINAS	9	**TABLAS**	1	**FIGURAS**	1	**ANEXOS**	1

CONTENIDO

PALABRAS CLAVES

Computación en la nube, Nube, Software como servicio, Plataformas como servicio, Infraestructura como servicio, paradigma de computación, vitalización, virtualización, modelos de despliegue, modelos de servicio, Infraestructura.

FORMULACIÓN DEL PROBLEMA

Actualmente existen organizaciones que siguen desconfiando de la seguridad ofrecida por los servicios de la computación en la nube, en la capacidad de proteger la integridad, confidencialidad y disponibilidad de sus servicios, no obstante se logra identificar un problema de confianza, razón por la cual estas organizaciones siguen trabajando de manera tradicional sin saber aún los grandes beneficios y ventajas que trae la computación en la nube.

Este problema surge cuando las organizaciones no están completamente documentadas sobre el tema, cuando no tienen las bases necesarias para tomar una decisión con respecto a una posible migración a la nube, siempre pensando que si la información no se tiene resguardada localmente, esta se encuentra totalmente insegura y se pierde el control sobre la misma, esto sucede en mucha ocasiones cuando se llega a estas compañías a ofrecer mejorar sus plataformas tecnológicas ofreciendo servicios de computación en la nube, y la primer barrera que se encuentra es la desinformación frente a este tema y el temor a las nuevas soluciones, ignorando por completo la cantidad de beneficio que pueden llegar a tener. Es importante que se entienda y reconozca que actualmente el riesgo siempre va a existir independientemente del medio utilizado, pero se busca que se confíe en la computación en la nube y los servicios que ofrece para el crecimiento de las compañías teniendo en cuenta que los beneficios son bastante tangibles en aspectos económicos con relación a espacios físicos, infraestructura y recursos necesarios.

Las empresas actualmente tienen que invertir grandes cantidades de dinero en compra de servidores, equipos de infraestructura de telecomunicaciones, equipos de infraestructura de respaldo eléctrico, personal que esté a cargo del funcionamiento de todo lo anterior (seguridad,

mantenimiento, etc), con lo cual tener un centro local de información es muy costoso.

CONTENIDO

Por medio de este análisis, se dará a conocer a las organizaciones las ventajas de adoptar el modelo de la computación en la nube, sus características, atributos y mejoras que pueden aportar para los negocios, donde siempre prevalece el tema de la seguridad para los activos de información de las compañías, analizando cada uno de los autores, sus métodos y mecanismos que ponen a disposición de cada uno de los proveedores de servicios cloud, se busca aclarar cada una de las dudas que se generan con respecto a la seguridad de dicho modelo y el control que ellos mismos (clientes) pueden tener sobre sus datos, además, Con el desarrollo de este análisis es factible el apoyo a las organizaciones a tener mayor claridad respecto a la seguridad ofrecida para el software y la infraestructura como servicio cloud y logren adoptar este modelo para la mejora del negocio.

OBJETIVOS

OBJETIVO GENERAL

Analizar cómo la seguridad ofrecida hoy día por la computación en la nube en los servicios SaaS e IaaS, garantizan la confiabilidad, integridad, y disponibilidad de los datos.

OBJETIVOS ESPECIFICOS

- Recopilar información de la situación actual de seguridad sobre los servicios SaaS e IaaS ofrecido por la computación en la nube.
- Establecer las ventajas y beneficios que ofrece la computación en la nube y de qué forma se pueden ver reflejados en la economía de las empresas.
- Conocer los métodos y prácticas que ofrece la computación en la nube que garantizan la disponibilidad, confidencialidad y la integridad de la información en los servicios SaaS e IaaS.
- Analizar el grado de seguridad que ofrecen actualmente los proveedores servicios SaaS e IaaS en la computación en la nube y los diferentes controles para la protección de la información de sus clientes.

METODOLOGIA DE INVESTIGACION

El desarrollo de esta monografía investigativa, se basa en la recopilación de información de diferentes autores acerca de la seguridad de la computación en la nube, métodos, mecanismo y herramientas que ofrecen los proveedores de dichos servicios para garantizar la seguridad de los activos de sus clientes. Por medio de la lectura, la investigación y de la información, se realiza un profundo análisis de cada uno de los diferentes elementos que fortalecen la seguridad, para identificar de qué forma se da la protección a la confidencialidad, disponibilidad e integridad de la información.

El análisis parte de la identificación del problema de desconfianza que aún genera la computación en la nube para algunas organizaciones, para lograr el contexto general, lo primero que se debe aclarar es el funcionamiento de la computación en la nube, sus modelos de servicio, modelos de implementación, ventajas, desventajas para sí lograr llegar al objetivo de identificar de qué forma se protege la información en un entorno Cloud.

Por último y con la identificación de cada uno de los mecanismos, se puede entonces realizar un nuevo análisis para dar respuesta al interrogante que se genera sobre la seguridad de la computación en la nube, específicamente en software e infraestructura como servicios para lograr

concluir los niveles de seguridad que se manejan por parte de los proveedores de este tipo de servicio donde estos garantizan por medio de dichos mecanismos, una alta integridad, confidencialidad y disponibilidad de la información de sus clientes.

CONCLUSIONES

La computación en la nube es una opción bastante buena actualmente para que las empresas optimicen Se recopiló y analizó la información necesaria acerca de la situación actual de la computación en la nube, sus modelos de servicios, modelos de implementación y sus principales características en los servicios SaaS e IaaS.

Se identificaron todas las ventajas y beneficios que ofrece la computación en la nube entre ellas la reducción de costos ya que esta es quizás la ventaja más atractiva, de no serlo, es una de las más evidente de todas las que ofrece esta tecnología, además otra de las principales ventajas es la disponibilidad y accesibilidad que estos servicios, ya que ofrecen un alto porcentaje de prestación de sus servicios sin fallas de interrupción.

Como todo modelo o servicio que se presta, se identificaron algunas desventajas, las cuales no hacen que estos servicios dejen de ser atractivos para los clientes, una de ella son las amenazas organizacionales, estás apuntan a algunos descuidos, como puertas abiertas que se produzcan posibles ataques, sesiones abiertas, trabajo remoto, conexiones no seguras, todo estos incumplimientos a las políticas de seguridad traen consigo mismo un sinfín de vulnerabilidades que pueden ser aprovechadas por la criminalidad

RECOMENDACIONES

La computación en la nube puede generar dudas con respecto a la seguridad, pero la utilización de los servicios ofrecidos como el SaaS e IaaS brindan mecanismos de última tecnología que permiten despejar todo es tipo de dudas y aclarar y poner en evidencia el alto nivel de seguridad que promete.

Es importante reconocer que uno de los pilares de la seguridad de la información es el más preciado para la computación en la nube, la confidencialidad no es uno de los puntos frágiles de este modelo, por el contrario es una de las fortalezas que ofrece a los clientes para asegurar y no tener duda del alto grado de resguardo de la información

Tener a todo tiempo disponible los recursos es otra de las características que ofrece la computación en la nube, con la computación en la nube, poder acceder en cualquier momento a la información se vuelve un plus para este modelo sin importar el dispositivo, por esta razón es totalmente recomendable la implementación de dicho modelo para tener la estabilidad y disponibilidad que requieren hoy en día las organizaciones

Integridad ofrecida por el modelo cloud, ayudará a las organizaciones a tener claro que es lo que va pasando con la información y modelo, permitirá tener claridad por medio de auditorías y log que ayudarán a tener un panorama claro de qué forma se está interactuando con los datos.

La responsabilidad sobre el manejo de la seguridad cloud no es únicamente del proveedor, se debe tener en cuenta que internamente deben existir procesos de protección de la información empresarial para los usuarios, que permitan brindar y dar a conocer las políticas de seguridad de información internas y que están sean evaluadas y auditadas periódicamente.

FUENTES BIBLIOGRAFICAS

ANCELIT, ANALIDA Y SHARITO. Encriptacion de datos. [En línea]. Blogger.com. 2007. Disponible en: http://encriptaciondedatos.blogspot.com.co/2007/09/encriptacion-de-datos.html

BLOUNT, Sumner; ZANELLA, Rob. Cloud Security and Governance: Who's on Your Cloud?. [En línea]. IT Governance Publishing. 2010. Base de datos: eBook Collection. Disponible en http://eds.a.ebscohost.com.consultaremota.upb.edu.co/eds/ebookviewer/ebook/bmxlYmtfXzM5MTEyMF9fQU41?sid=2b007c10-744b-41ed-bb89-b4d54f0918fa@sessionmgr4006&vid=3&format=EB

Cloud computing security. From Wikipedia, the free enciclopedia. [En línea]. 2018. Disponible en https://en.wikipedia.org/wiki/Cloud_computing_security#Security_and_privacy
COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1273 (5, enero, 2009). De La Protección De La Información Y De Los Datos. Ministerio TIC. Bogota D.C., 2009.

Dinero. El 62% de las compañías más grandes ya usan cloud computing. [En línea]. Bogotá: Dinero. 2012.,1 p. Disponible en http://www.dinero.com/negocios/tecnologia/articulo/el-62-companias-mas-grandes-usan-cloud-computing/141978

EL CONGRESO DE COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPUBLICA. Decreto 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá D.C., 2012.

European Commission, Information Society and Media, “The Future of Cloud Computing. Opportunities for European Cloud Computing beyond 2010”. [En línea]. CORDIS. 2010, disponible en: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf
GARCÍA VIZCAÍNO, Julio; CRUZ VALENCIA, Galvy. Privacidad de la Información en la Nube. [En línea]. México. 2018. Disponible en https://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

GOIKOLEA, Markos. ¿Qué es un sistema SaaS? Definición y ventajas. [En línea]. Digital Business. 2014. Disponible en
http://www.iebschool.com/blog/que-es-saas-definicion-ventajas-digital-business/

JOYANES AGUILAR, Luis. COMPUTACIÓN EN LA NUBE: Notas para una estrategia española en cloud computing. S.A 2012.

LOEFFLER, Bill. Cloud Computing: What is Infrastructure as a Service. [En línea]. Microsoft.2011. Disponible en https://technet.microsoft.com/en-us/library/hh509051.aspx

LOL, Cloud. Modelos de Implementación. [En línea]. Lol Cloud. 2017. Disponible en https://www.licenciasonline.com/bo/es/cloud/modelos-de-implementacion

MATHER, Tim. KUMARASWANY Subra. LATID Shahed. Cloud Security, an Enterprice Perpective on Risk Compliance. O’REILLY Media, Inc. 2009.

MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [En línea]. Gaithersburg. NITS. 2011., 1 p. Disponible en https://csrc.nist.gov/publications/detail/sp/800-145/final

MELL, Peter. GRANCE, Tim. The NIST Definition of Cloud Computing. [En línea]. Gaithersburg. NITS. 2010. Disponible en https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf

NAMRATA, Bisht. Virtualization In Cloud Computing and Types. [En línea]. Advant Navis Business Park Graphic Era University (GEU) Dehradun. 2018. Disponible en https://www.geeksforgeeks.org/virtualization-cloud-computing-types/

NATE Lord. Cryptography in the Cloud: Securing Cloud Data with Encryption. [En línea]. digitalguardian.com 2017.Disponible en: https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption

Primorac, Carlos R. Computación en la nube. Trabajo de grado en Licenciatura en Sistemas de Información Comunicaciones de Datos. Universidad Nacional del Nordeste. Facultad de Ciencias Exactas y Naturales y Agrimensura. 2014.

RACHNA, Arora; ANSHU, Parashar. Secure User Data in Cloud Computing Using Encryption Algorithms. [En línea]. International Journal of Engineering Research and Applications (IJERA) 2013. ISSN: 2248-9622. Disponible en: https://pdfs.semanticscholar.org/9799/a9f9bec6cf85715ca236035b5d89204b326a.pdf

ROBERTO, Carlos. La desconfianza hacia la nube en las empresas. [En línea]. TicPymes. 2011.,2 p. Disponible en https://www.pymesyautonomos.com/tecnologia/la-desconfianza-hacia-la-nube-en-las-empresas

RODRIGUES, Thoran. What high availability for cloud services means in the real world. [En línea]. The Enterprise Cloud. 2011. Disponible en https://www.techrepublic.com/blog/the-enterprise-cloud/what-high-availability-for-cloud-services-means-in-the-real-world/

ROUSE, Margaret. Infrastructure as a Service (IaaS). [En línea]. TechTarget. 2014. Disponible en http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

SANTOS, Mateo. SaaS, IaaS y PaaS: ¿qué son, cómo usarlos y para qué?. [En línea]. Bogotá. Enter.com. 2015. Disponible en: http://www.enter.co/guias/tecnoguias-para-empresas/saas-iaas-y-paas-que-son-como-usarlos-y-para-que/

SAS 70. [En línea]. American Institute of Certified Public Accountants (AICPA). 2018 Disponible en http://sas70.com/FAQRetrieve.aspx?ID=33288

SHINDER, Thomas W. Microsoft Reference Architecture for Private Cloud: Cloud Security Introduction. [En línea]. Microsoft. 2011.,1 p. Disponible en https://social.technet.microsoft.com/wiki/contents/articles/3801.cloud-security-introduction.aspx

TECHOPEDIA. Network Virtualization. [En línea]. techopedia.com. 2018. Disponible en https://www.techopedia.com/definition/655/network-virtualization

The Different Types of Virtualization in Cloud Computing – Explained. [En línea]. Redswitches.com. 2017. Disponible en https://redswitches.com/blog/different-types-virtualization-cloud-computing-explained/

TÜCKLER, Hjalmar. Evolución de la computación en la nube en AL. [En línea]. La prensa. 2014.,2 p. Disponible en https://www.laprensa.com.ni/2014/10/25/economia/215932-evolucion-de-la-computacion-en-la-nube-en-al-telecomunicaciones

VIOLINO, Bob. The dirty dozen: 12 top cloud security threats for 2018. [En línea]. CSO Online. 2018. Disponible en https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

WANG, S. C.; Yan, K. Q.; Liao, W. P.; Wang, S. S. (2010), "Towards a load balancing in a three-level cloud computing network", Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT), IEEE: 108–113, ISBN 978-1-4244-5537-9

WAYNE Jansen; GRANCE Timothy. Guidelines on Security and Privacy in Public Cloud Computing. [En línea]. NIST US Departament or Commerce. 2011. Disponible en: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Wikipedia. Cloud load balancing. [En línea]. From Wikipedia, the free enciclopedia. 2018. Disponible en https://en.wikipedia.org/wiki/Cloud_load_balancing

YUNCHUAN Sun, JUNSHENG Zhang, YONGPING Xiong, GUANGYU Zhu. Data Security and Privacy in Cloud Computing. [En línea]. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks. 2014. Disponible en http://journals.sagepub.com/doi/full/10.1155/2014/190903