ANÁLISIS DE LOS COMPONENTES DE SEGURIDAD INFORMÁTICA EN LA IMPLEMENTACIÓN DE CLOUD COMPUTING EN PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS

ADRIANA MARCELA TORRES GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, DC
2020

ANÁLISIS DE LOS COMPONENTES DE SEGURIDAD INFORMÁTICA EN LA IMPLEMENTACIÓN DE CLOUD COMPUTING EN PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS

ADRIANA MARCELA TORRES GONZÁLEZ

Monografía presentada para optar por el título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
ESP. EDGAR ROBERTO DULCE VILLARREAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, DC
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, abril de 2020

DEDICATORIA

Este proyecto va dedicado a mi familia, especialmente a mi madre, por su infinito apoyo en cada una de mis metas.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Cloud Computing representa una nueva manera de disponibilizar los recursos informáticos para que una empresa lleve a cabo sus actividades económicas, mediante el uso de infraestructura tecnológica virtualizada, almacenada en un servidor de algún proveedor de Cloud Computing o CSP. Sin embargo, para muchos, este modelo puede resultar riesgoso, ya sea por desconocimiento técnico del funcionamiento de Cloud Computing, o porque los datos almacenados que forman parte del diario vivir de la organización son en extremo delicados.

La seguridad informática para las empresas es un aspecto vital, ya que puede comprometer directamente datos delicados, tanto de la organización como de los clientes. Por este motivo la infraestructura tecnológica usada para almacenar e intercambiar información, debe estar diseñada y enfocada para evitar incidentes tales como la interceptación y/o alteración de datos, la suplantación de identidad o la denegación del servicio.

La presente monografía, mediante la revisión de distintas fuentes documentales, busca ser un referente que permita analizar los aspectos de seguridad en la implementación de servicios de Cloud Computing en pequeñas y medianas empresas colombianas, como estrategia para determinar si es conveniente o no el uso de este tipo de infraestructura en el manejo de información delicada.

Palabras clave: Cloud Computing, IaaS, SaaS, PaaS, Seguridad Informática

ABSTRACT

Cloud Computing represents a new way of having the computer resources for a company to carry out its economic activities, through the use of virtualized technological infrastructure, stored on a server of a Cloud Computing or CSP provider. However, for many, this model can be risky, either due to technical ignorance of the operation of Cloud Computing, or because the stored data that are part of the organization's daily life are extremely delicate.

Computer security for companies is a vital aspect, since it can directly compromise sensitive data, both from the organization and from customers. For this reason, the technological infrastructure used to exchange information must be determined and focused to avoid incidents, such as interception and / or alteration of data, impersonation or denial of service.

This monograph, by reviewing different documentary sources, seeks to be a reference that allows analyzing security aspects in the implementation of Cloud Computing services in small and medium-sized Colombian companies, as a strategy to determine whether or not the use of This type of infrastructure in the management of sensitive information.

Keywords: Cloud Computing, IaaS, SaaS, PaaS, Computer Security

INTRODUCCIÓN

Hoy en día, el uso del internet se ha hecho vital para prácticamente todas las actividades que se realizan a diario: comunicaciones, educación, transacciones financieras y comerciales, intercambio de archivos de distinta índole, etc. La penetración de este tipo de tecnología en ámbitos corporativos ha sido de gran impacto, siendo importante por ejemplo para romper los límites geográficos en temas de publicidad, mercadeo y ventas; centralización de múltiples sucursales mediante el establecimiento de canales óptimos de comunicación, reduciendo errores, tiempo y sobrecosto en el tratamiento y almacenamiento de la información.

La masificación del uso de internet en los ámbitos empresariales ha permitido que se acuñe un paradigma relacionado con la nueva forma de dar acceso a los recursos informáticos para que una empresa lleve a cabo su actividad económica, sin hacer uso de una arquitectura tecnológica tradicional (servidores y conectividad física custodiada dentro de la organización, o infraestructura 'On Premise'), sino contratando una infraestructura virtual a la que se accede vía internet, almacenada en los servidores de algún proveedor de Cloud Computing o CSP, este paradigma es conocido como Cloud Computing o Computación en la Nube.

Cloud Computing se caracteriza por el suministro vía internet de servidores y redes virtuales, donde se puede disponer de infraestructura, bases de datos, ambientes de prueba y producción, entre otros aspectos vitales para el funcionamiento de la organización; a los cuales se puede acceder sin restricción de Sistema Operativo o ubicación. Esta nueva forma de hacer uso de la infraestructura tecnológica ha penetrado de forma importante el mercado empresarial, ya que trae múltiples ventajas. El informe del Observatorio de Economía Digital del Ministerio de las Tecnologías de la Información y las Comunicaciones, emitido en diciembre de 2017[1], ubica el uso de la computación en la nube en el 19.1% de las empresas a nivel nacional en temas como computación, redes, almacenamiento, y uso de aplicaciones y servicios por demanda.

Pero aún quedan grandes vacíos en cuanto a la conceptualización y al funcionamiento del Cloud Computing y la certeza de la aplicabilidad de este modelo en los distintos sectores empresariales, específicamente en lo referido a la seguridad informática, ya que es un paradigma poco explorado y aun en crecimiento y consolidación en el país. Esta falta de perspectiva en cuanto a la seguridad informática dentro de la implementación de Cloud Computing genera la necesidad de consolidar la presente monografía, con la cual se busca dar el panorama

[1] KATZ, Raúl. Informe del Observatorio De La Economía Digital De Colombia [en línea]. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones. 2017., 44 p. Disponible en https://www.mintic.gov.co/portal/604/articles-61929_recurso_4.pdf p.30.

adecuado sobre la potencialidad, beneficios, limitaciones y riesgos que ofrecen las nuevas tecnologías en asuntos de seguridad informática.

“Análisis de los Componentes de Seguridad Informática en la Implementación de Cloud Computing en Pequeñas y Medianas Empresas Colombianas” busca ser una base de conocimiento de las necesidades de seguridad informática para las pequeñas y medianas empresas colombianas, así como ser un referente en cuanto a mecanismos y herramientas de seguridad informática suministrados por Cloud Computing y de la idoneidad del modelo en el sector empresarial colombiano. Para lograr esto se hace un análisis de los aspectos técnicos y conceptuales asociados, así como de los aspectos normativos y legales que apliquen, y de las herramientas y configuraciones específicas a la seguridad informática suministradas por los distintos proveedores de Cloud Computing o CSP.

1. PLANTEAMIENTO DEL PROBLEMA

La seguridad informática para cualquier pequeña o mediana empresa es un aspecto vital para la operación, ya que puede comprometer directamente datos delicados, tanto de la organización como de los clientes; por lo cual, la arquitectura de los sistemas de información implementados para el almacenamiento e intercambio de los datos debe estar diseñada muy especialmente para evitar incidentes como la interceptación o alteración de datos, la suplantación de identidad o la denegación del servicio.

Estos aspectos de seguridad informática, sumados al incremento de la cantidad de datos procesados e intercambiados entre los distintos sistemas de información, la masificación del acceso a los productos y servicios empresariales a través de Internet, y la necesidad de garantizar condiciones óptimas de integridad, disponibilidad y confidencialidad, hacen necesario que se piense en la implementación de nuevos modelos de infraestructura tecnológica que satisfagan estas necesidades, y una alternativa a esto pueden ser los servicios computacionales en la nube.

En ese orden de ideas, Cloud Computing es un nuevo paradigma de infraestructura tecnológica que representa una forma diferente de dar acceso los recursos informáticos para que una empresa lleve a cabo su actividad económica, sin hacer uso de una arquitectura tradicional (servidores y conectividad física custodiada dentro de la organización, o infraestructura ‘On Premise’), sino contratando una infraestructura virtual, almacenada en un servidor de algún proveedor de Cloud Computing o CSP. La computación en la nube se caracteriza por el suministro de servidores y redes virtuales, donde se puede disponer de infraestructura, bases de datos, ambientes de prueba y producción, entre otros aspectos vitales para el funcionamiento de la organización; a los cuales se puede acceder sin restricción de Sistema Operativo o ubicación geográfica y sin las limitaciones físicas que tienen los sistemas ‘On Premise’ (riesgos ambientales, altos costos para la escalabilidad y mantenimiento a nivel de hardware y software, etc.).

Se debe mencionar que cualquier solución tecnológica debe dar importancia a la seguridad informática, y Cloud Computing no es la excepción. Una plataforma o servicio de Cloud Computing debe estar en la capacidad de demostrar que posee los medios y procedimientos necesarios para proteger la integridad, la disponibilidad y la confidencialidad de la información que procesa, y que está realmente en la idoneidad de cumplir con las reglas de negocio de cualquier empresa. Todo esto nos lleva a la necesidad de determinar cuáles son los aspectos de seguridad para tener en cuenta dentro de la implementación de sistemas de información en una infraestructura de computación en la nube para una pequeña o mediana empresa, ya que existe incertidumbre sobre las garantías de Seguridad del Cloud Computing en el desarrollo de las distintas actividades operativas en las organizaciones.

FORMULACIÓN DEL PROBLEMA:

¿Cuáles son los aspectos de seguridad informática que se deben tener en cuenta en la implementación de Cloud Computing en una pequeña o mediana empresa colombiana?

2. JUSTIFICACIÓN

Cloud Computing es un paradigma que ha venido penetrando el mercado tecnológico en el país por la gran cantidad de ventajas que representa para las empresas. El informe del Observatorio de Economía Digital del Ministerio de las Tecnologías de la Información y las Comunicaciones, emitido en diciembre de 2017[2], ubica el uso de la computación en la nube en el 19.1% de las empresas a nivel nacional en temas como computación, redes, almacenamiento, y uso de aplicaciones y servicios por demanda. En este aspecto, existen CSP que ofrecen amplias gamas de productos, que van desde infraestructura (como Google Cloud, Amazon Web Services o Microsoft Cloud), o servicios especializados (como el CRM de Salesforce o G-Suite de Google).

En consecuencia, se puede afirmar que la puesta en marcha de una infraestructura de Cloud Computing representa para las pequeñas y medianas empresas colombianas múltiples beneficios, como por ejemplo la reducción de costos (ya que el modelo de pagos es por demanda, y realmente no se generan costos por escalabilidad, administración o mantenimiento de hardware y software), y optimización de la efectividad de las operaciones (mediante múltiples herramientas de desarrollo, gestión o análisis de la información, y protocolos que aseguran la confidencialidad, la disponibilidad y la integridad de los datos). Pero aún quedan grandes vacíos en cuanto al funcionamiento y certeza de la aplicabilidad de este modelo en los distintos sectores empresariales, específicamente en lo referido a la seguridad informática, ya que es un paradigma poco explorado y aun en crecimiento y consolidación en el país.

Esta falta de perspectiva en cuanto a la seguridad informática dentro de la implementación de Cloud Computing genera la necesidad de consolidar la presente monografía, con la cual se busca dar el panorama adecuado sobre la potencialidad, beneficios, limitaciones y riesgos que ofrecen las nuevas tecnologías en asuntos de seguridad informática. Entre otras, las ventajas de la construcción de un documento con tal análisis son:

- Ser una base de conocimiento de las necesidades de seguridad informática para las pequeñas y medianas empresas colombianas

- Ser un referente en cuanto a mecanismos y herramientas de seguridad informática suministrados por Cloud Computing

[2] Ibíd., p. 30

- Determinar si hay un límite a la aplicabilidad de Cloud Computing en proyectos tecnológicos para las pequeñas y medianas empresas colombianas.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar los componentes asociados con la seguridad informática en la implementación de Cloud Computing en las pequeñas y medianas empresas colombianas.

3.2 OBJETIVOS ESPECÍFICOS

- Estudiar los componentes técnicos y regulatorios de Cloud Computing
- Identificar los mecanismos de seguridad informática ofrecidos por una infraestructura Cloud Computing
- Reconocer los riesgos asociados a la implementación de Cloud Computing
- Determinar el nivel de conveniencia de la implementación de Cloud Computing en proyectos tecnológicos en pequeñas y medianas empresas colombianas

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL Y TEÓRICO

4.1.1 Computación en la Nube o Cloud Computing

Computación en la Nube o Cloud Computing hace referencia al paradigma de infraestructura tecnológica, donde los servidores, procesadores y demás elementos están virtualizados y almacenados en centros de datos remotos propiedad de un Proveedor de Cloud Computing o CSP, al cual el usuario final accede mediante internet desde cualquier dispositivo. El uso de esa infraestructura puede ser gratuito, o generar un fee mensual o un pago por consumo, dependiendo del tipo de servicio o condiciones pactadas con el CSP. Los servicios disponibilizados por Cloud Computing van desde aplicaciones ofimáticas y correo electrónico, hasta espacio de almacenamiento de información, despliegue de aplicaciones o análisis y procesamiento de datos.

Se han acuñado oficialmente varias definiciones de lo que es la Computación en la Nube o Cloud Computing. Por ejemplo:

La legislación mexicana, en su Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, define que "por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente"[3].

The Nist (National Institute of Standards and Technology) define Cloud Computing como "La computación en la nube es un modelo para permitir el acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo de gestión o Interacción del proveedor de servicios."[4]

La Mesa Sectorial sobre Cloud Computing en Colombia acepta como definición "Cloud Computing es un modelo para habilitar el acceso a un conjunto de servicios computacionales (e.g. Redes, servidores, almacenamiento, aplicaciones y servicios) de manera conveniente y por demanda, que pueden ser rápidamente

[3] ESTADOS UNIDOS DE MÉXICO. CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Reglamento De La Ley Federal De Protección De Datos Personales En Posesión De Los Particulares. (21, diciembre, 2011). Cámara de Diputados. México D.F., 2011., art. 52.

[4] GRANCE, Timothy y MELL, Peter. The NIST Definition of Cloud Computing. En: NIST. Special Publication 800-145., Septiembre, 2011., p. 8.

aprovisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor del servicio mínimos"[5]

Finalmente, Fernández consolida una definición de Cloud Computing, así: "En resumen, la computación en la nube proporciona un modelo de relación proveedor-consumidor en sustitución de la relación «vendedor de tecnología de información usuario». En la primera se compran y se venden servicios; mientras que, en la segunda, los usuarios adquieren tecnología de un vendedor y deben desplegarla e integrarla en la infraestructura existente"[6].

4.1.2 Características Esenciales de Cloud Computing

El autor García del Poyo[7] en su artículo "Cloud Computing: Aspectos Jurídicos Clave Para la Contratación de Estos Servicios" describe tres características generales de la computación en la nube:

- Multisesión: La arquitectura de Cloud Computing se basa en que los datos de un cliente están almacenados permanente en data-centers, a los cuales puede acceder mediante una conexión a internet, pero esa infraestructura de almacenamiento y comunicación vía internet no es exclusiva para un solo cliente, de modo que el acceso a la infraestructura se hace manera concurrente por parte de varios clientes del CSP.

- Acceso a los Servicios de Manera Personalizada: El usuario final puede acceder a su información mediante cualquier conexión a internet, haciendo uso de cualquier Navegador Web. Con lo anterior logra abastecerse unilateralmente de datos, procesamiento, comunicaciones y demás elementos contratados, de manera rápida y autoescalable.

- Optimización y Control Bilateral: Todos los productos y servicios suministrados por un CSP se controlan y optimizan de forma automática, ya que cuentan con métricas y elementos de monitoreo, seguimiento y notificación, con lo cual la prestación del servicio resulta transparente para las partes.

[5] CASTRO, Jorge. Cloud Computing: Una Perspectiva Para Colombia. En: Mesa Sectorial Cloud Computing. Versión 1.0.0., Abril, 2010., p. 8.
[6] FERNÁNDEZ, Froilán. Un Salto A La Nube La Computación En Los Cielos Virtuales. En: DEBATES IESA. Vol. XV., No 1 Enero, 2010., p. 43.
[7] GARCÍA DEL POYO, Rafael. Cloud Computing: Aspectos Jurídicos Clave Para la Contratación de Estos Servicios. En: Revista Española de Relaciones Internacionales. Núm. 4. ISSN 1989-6565., 2012., p. 49-50.

El Observatorio Nacional de las Telecomunicaciones y la SI[8] describe los siguientes conceptos claves, en su documento 'Cloud Computing: Retos y Oportunidades':

- Pago por Uso: El pago de un servicio de Cloud Computing se basa en el consumo, lo que quiere decir que el valor facturado por el CSP al cliente varía en función al uso que este último dé al producto contratado.

- Abstracción: Es la capacidad de que, mediante la virtualización, se entregue un servicio de procesamiento informático al cliente, pero manteniendo aislados los recursos informáticos propiedad del CSP. Por ejemplo, el Cliente puede acceder a servicios de almacenamiento sin tener contacto con un dispositivo de almacenamiento.

- Escalabilidad: Consiste en poder aumentar o disminuir las capacidades de los servicios ofrecidos al cliente, en función de sus necesidades o demanda de manera automática, omitiendo ajustes contractuales o intervención manual para el cambio en la asignación de recursos. Algunos autores, como Bruno[9], se refieren a esta característica como 'Elasticidad rápida'.

- Multiusuario: Es la capacidad de que múltiples usuarios puedan compartir recursos e información.

- Autoservicio bajo Demanda: Consiste en que el usuario pueda acceder a los distintos servicios y recursos, sin necesidad de interacción humana con el administrador de los recursos.

- Acceso sin restricciones: Corresponde a la posibilidad de acceder a un recurso o servicio, sin restricción de lugar, momento, tipo de dispositivo. El acceso a los servicios se hacer mediante una conexión a internet y un navegador de internet estándar.

Cloud Computing tiene implícitas las siguientes características, de acuerdo con lo descrito por Grace y Mell[10] para The Nist:

- El usuario puede aprovisionar para su infraestructura las capacidades de cómputo de manera unilateral (asignación de memoria y procesadores, por ejemplo), según su necesidad y sin que sea obligatoria la interacción con el CSP.

---

[8] ONTSI. Cloud Computing: Retos y Oportunidades [en línea]. Madrid: Observatorio Nacional de las Telecomunicaciones y la SI. 2012., 55 p. Disponible en https://www.ontsi.red.es/ontsi/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf p. 15 - 16

[9] BRUNO, Gaston. Cloud computing en la industria financiera. En: Revista de Ciencia y Tecnología. Vol. 13., 2013., p. 72.

[10] GRANCE y MELL, Op. cit., p. 6.

- Amplio acceso al servicio, ya que la infraestructura esta disponibilizada a través de internet y se accede mediante mecanismos estándar que promueven el uso de la plataforma desde dispositivos de tecnologías heterogéneas (como celulares, computadores de escritorio, tablets, etc.)

- La infraestructura tecnológica del CSP se pone a disposición de múltiples consumidores finales, a través de diferentes recursos virtualizados y asignados dinámicamente según la demanda del usuario.

- El usuario final no tiene control ni conocimiento sobre la ubicación física exacta de los data-centers, ni sobre las características técnicas de esos recursos asignados, pero si se puede exigir al CSP informar la ubicación de los data-centers en un nivel alto de abstracción, como el país o región.

- Las capacidades y recursos asignados a cada usuario pueden ser aprovisionadas y liberadas flexiblemente, para escalar rápidamente de acuerdo con la demanda. El usuario tiene la percepción de que los recursos son ilimitados y pueden ser escalados en cualquier momento.

- Los CSP monitorean e informan automáticamente sobre el uso de la infraestructura al tener una capacidad de medición acorde con cada tipo de servicio (almacenamiento, procesamiento, transaccional, etc.), dando transparencia de la operación y de la facturación, tanto para el CSP como para el usuario final.

Otras características que valen la pena resaltar son:

- Un elemento virtualizado de infraestructura, dentro de Cloud Computing, corresponde realmente a una abstracción de un dispositivo tecnológico de la vida real (procesador, disco duro, memoria RAM, etc.) el cual es construido mediante software, y que, para fines operacionales, cumple con la funcionalidad asociada al elemento homónimo en una arquitectura física tradicional.

- Para el usuario final es totalmente transparente el nivel de complejidad que pueda llegar a tener la tecnología que usa el CSP para la prestación del servicio. Aspectos como lenguajes de programación o arquitectura no le son relevantes, ya que sólo interactúa con la capa del servicio contratada.

- Los recursos físicos provistos por el CSP son compartidos por distintos clientes, pero cada uno de ellos tiene restringido el acceso a únicamente los recursos que le competen.

- Otros aspectos que también resultan transparentes para el usuario serian por ejemplo los mecanismos y estrategias implementadas para recuperación

ante desastres, y planes de continuidad del negocio implementados por el CSP. Si bien la seguridad informática es un tema de interés prioritario para el cliente, el CSP debe garantizar que tiene los recursos suficientes para cumplir con los SLA acordados.

4.1.3 Cloud Computing Como Arquitectura SOA

Arquitectura SOA, o Service Oriented Architecture, en español se traduce como Arquitectura Orientada a Servicios, es un framework de arquitectura de desarrollo e implementación de sistemas de información interoperables y con orientación a servicios, guiado por estándares y procedimientos internacionalmente aceptados, lo que permite a la organización unir los objetivos organizacionales con la infraestructura tecnológica con la finalidad de mejorar los resultados operacionales, la transversalidad de los servicios y la disponibilidad de la información para los procesos.

Castillo Jaime[11] define que una arquitectura SOA es un estilo de arquitectura de software que permite la construcción de software distribuido que cumple con determinadas características. Provee soluciones a las necesidades organizaciones actuales, tales como la integración de múltiples sistemas de información desarrollados en distintas tecnologías, y un enfoque basado en los procesos propios del negocio, con lo que busca reducir las incompatibilidades entre los objetivos organizaciones y el área de TI.

Esta arquitectura se caracteriza por:

- Las características del sistema se orientan hacia las necesidades de la organización, y tiene en cuenta la transversalidad e interoperabilidad de los procesos, datos o servicios.
- Orientado a Servicios, no a un proveedor o a un software en particular. Esto permite que se puedan sustituir elementos del sistema, sin interrumpir o alterar el servicio.
- Permite la desagregación de los servicios en pequeños elementos, con lo cual se busca poder recomponer nuevos servicios a la medida de las necesidades de cada operación.

[11] CASTILLO JAIME, Oswaldo Augusto. Planteamiento de un modelo basado en la arquitectura SOA en el gobierno de TI de las empresas de contact center. Trabajo de grado Magíster en Gobierno de Tecnologías de Información. Lima: Universidad Nacional Mayor de San Marcos., 2017., p. 43-44.

- Gran capacidad para la adaptación al entorno, flexibilidad y reutilización de los servicios, de forma simple y estandarizada.

Las características de una Arquitectura SOA concordantes con un modelo de Cloud Computing, según lo descrito por Arévalo Navarro[12] son:

- Los modelos de negocio tienden a la tercerización, entregando aspectos técnicos específicos y servicios a proveedores expertos.
- Facilidad para implementar modelos de colaboración (entre distintas unidades de negocio de la organización, socios o proveedores), tanto a nivel de datos, desarrollo de software o infraestructura.
- Posibilidad de remplazar, migrar o ajustar elementos del sistema sin interrumpir la operatividad del servicio.
- La arquitectura, diseño, y lenguaje de programación de un sistema de información son transparentes para el usuario final, ya que el nivel de abstracción está a nivel del servicio o funcionalidad del sistema.

4.1.4 Infraestructura 'On Premise'

Contrario a Cloud Computing, una Infraestructura ´On Premise' (o en local) es una arquitectura tecnológica tradicional, donde los servidores y conectividad están custodiados físicamente dentro de la organización. Andrade Delgado[13] describe las características de este modelo de infraestructura de la siguiente manera:

- Las aplicaciones, bases de datos e infraestructura tecnológica están alojadas en las instalaciones de la empresa; y la construcción, administración y mantenimiento es gestionada por funcionarios de esta misma.
- La existencia de este tipo de infraestructura está asociada a empresas que buscan el máximo nivel de control al ser los administradores de los recursos e información, evitando riesgos físicos o filtración de información.

[12] ARÉVALO NAVARRO, José Manuel. Cloud Computing: fundamentos, diseño y arquitectura aplicados a un caso de estudio. Trabajo de grado Máster Oficial en Tecnologías de la Información y Sistemas Informáticos. Madrid: Universidad Rey Juan Carlos., 2011., p. 14-18.

[13] ANDRADE DELGADO, Wilman Ernesto. Estudio de factibilidad para la migración de servicios IT On-Premise a Cloud Computing de la vertical financiera de Cooperativas de Ahorro y Crédito (COAC) del Ecuador. Caso de aplicación. Trabajo de grado Magister en Gerencia de Sistemas y Tecnologías de Información. Quito: Universidad de las Américas., 2014., p. 4 - 5.

- Este modelo de arquitectura tecnológica significa que los servicios tecnológicos están soportados por inversiones y compras propias, e impactados por la depreciación, desgaste y obsolescencia.

En cuanto a los inconvenientes inherentes a la infraestructura 'On Premise', se pueden enumerar los siguientes:

- La construcción, administración y mantenimiento también abarca todos los elementos propios de un Plan de Continuidad del Negocio, dedicados a proteger esa infraestructura (planta de abastecimiento eléctrico, sistema de seguridad perimetral, backups, etc.). Lo anterior, desde un punto de vista financiero, resulta negativo, ya que incrementa los costos de implementación y mantenimiento del sistema.

- La capacidad de la infraestructura puede llegar a estar sobreestimada o subestimada. Si se implementa una infraestructura de mayor capacidad a la necesaria, se traduce en que el gasto incurrido fue mayor al necesario. Caso contrario, si se implementa una infraestructura con menor capacidad a la necesaria, se entiende que será necesario hacer nuevas inversiones para mejorar la capacidad del sistema.

- El uso de activos físicos propensos a la depreciación y a la obsolescencia representa a futuro nuevos gastos e inversión para mantener el sistema en funcionamiento. Del lado del software, la inversión se materializa por la necesidad constante de mantener al día las licencias de software requeridas para el funcionamiento del sistema.

- Una infraestructura 'On Premise' vuelca toda la responsabilidad de la seguridad, la disponibilidad y la gestión del riesgo a la propia empresa y sus colaboradores.

4.1.5 Modelos de Servicio de Cloud Computing

Fernández también identifica los tres modelos básicos de Servicio Cloud, dependiendo del tipo de servicio o capa de servicio que se virtualice en la nube o la estrategia establecida para gestionar la tecnología (infraestructura, plataforma o software)[14]:

[14] FERNÁNDEZ, Op. cit., p. 43.

4.1.5.1 Software Como Servicio (Software as a Service – SaaS)

Corresponde al uso del software de usuario final que provee el CSP. SaaS provee tanto el software como el hardware donde se ejecuta. Un uso generalizado que se da a la computación en la nube es el correo electrónico, como Hotmail o Gmail. En esta categoría también se puede nombrar el uso de aplicaciones ofimáticas y de productividad, alojadas en servidores propiedad del CSP, a las que se accede por medio de un navegador de internet, y que libera al usuario final de hacer mantenimiento y actualizaciones periódicas del software. Las actualizaciones de software se ejecutan en los servidores por parte del prestador del servicio, y son completamente transparentes para el usuario final.

Bruno[15] define las siguientes características y beneficios del modelo SaaS:

- Experiencia del usuario consistente ya que se trata de herramientas populares y estables.
- Arquitectura del software y modelo de datos común para cualquier tipo de negocio.
- Flexibilidad al poder suplir de forma sencilla los requerimientos complejos.
- Adaptabilidad al permitir realizar cambios en cualquier momento.

4.1.5.2 Plataforma Como Servicio (Platform as a Service – PaaS)

Corresponde a la utilización de infraestructura informática remota para el desarrollo, la prueba y el uso en ambientes de producción de las aplicaciones. El uso de una plataforma como servicio, o PaaS, significa que el cliente puede desplegar sus aplicaciones en la infraestructura de un CSP. Los usuarios de la empresa cliente acceden a su software desde cualquier dispositivo a través de Internet, teniendo autonomía en temas de desarrollo y uso de las aplicaciones, pero sin preocuparse por infraestructura, sistemas operativos o aprovisionamiento de recursos. Los sistemas operativos, capacidad de procesamiento y almacenamiento son definidos por el requerimiento del cliente, pero no tiene autonomía para la administración de estos.

Arévalo Navarro[16] define estas características de PaaS:

- Al entorno de desarrollo se accede desde un navegador Web.

[15] BRUNO, Op. cit., p. 72 - 73.
[16] ARÉVALO NAVARRO, Op. cit., p. 25 26.

- Se puede desplegar de manera sencilla la aplicación en desarrollo.
- El servicio PaaS contratado provee sus propias herramientas de monitoreo y gestión, lo cual es una herramienta importante para la liquidación de los pagos por consumo.

4.1.5.3 Infraestructura Como Servicio (Infrastructure as a Service – IaaS)

Los recursos de procesamiento, almacenamiento y redes virtuales son administrados por el cliente de manera dinámica. Desde una consola suministrada por el CSP, como Google Cloud Platform, el cliente puede definir las características de cada proyecto, en términos de asignación de cantidad de procesadores, espacio de almacenamiento, sistema operativo, reglas de seguridad en la red, etc. Una infraestructura como servicio ofrece un nivel alto de administración sobre los recursos, presentándolos con una apariencia similar a la acostumbrada en entornos de trabajo tradicionales.

Algunos ejemplos de soluciones existentes en el mercado son: Servicios de computación (Compute Service), Servicios de almacenamiento (Storage Service) y Servicios de copia de seguridad (Backup Service). Bruno[17], en cuanto a los costos, define que la ventaja que ofrece IaaS es la posibilidad de llevar los costos de infraestructura a su mínimo tamaño, ya que es un modelo de pagos por demanda, esto es, que se paga solo por el recurso tecnológico que se consume efectivamente (espacio de disco duro utilizado, memoria RAM empleada, etc.).

En distintas fuentes documentales se acuñan los siguientes tipos de funciones, que también corresponden a servicios administrados provisionados al cliente final de manera similar a los tres modelos de servicios anteriormente descritos:

4.1.5.4 Todo Como Servicio (Everything as a Service – XaaS)

XaaS, o Todo como Servicio, es un término global que hace referencia a la entrega de cualquier cosa como servicio. Esto incluye la gran variedad de servicios tecnológicos que un CSP puede ofrecer a través de internet dentro de su portafolio: Plataforma, Software, Infraestructura, Bases de Datos etc. XaaS surge de la evolución de los servicios en la nube, en donde se puede disponibilizar cualquier tipo de producto de forma económica y eficiente. Si bien el término en general hace referencia a los servicios en la nube, también se puede mencionar el HWaaS, o Hardware as a Service, que incluiría por ejemplo el alquiler de hardware, donde el prestador del servicio se encargaría del mantenimiento y la administración.

[17] BRUNO, Op. cit., p. 73.

Según Toesland[18], la implementación de cualquier tipo de servicio XaaS, se puede traducir en múltiples beneficios para el usuario final, que van desde la escalabilidad, la reducción de costos e inversión, la simplificación de la infraestructura tecnológica y la eficiencia para llevar iniciar una operación y ejecutar las actividades operacionales del cliente.

4.1.5.5 Backend Como Servicio (Backend as a Service – BaaS)

Del Vecchio, Paternina y Miranda[19] adicionan este tipo de servicio a su definición de computación en la nube, que consiste en la necesidad de suministrar los anteriores tipos de servicios (almacenamiento, infraestructura, software) a los desarrolladores web, otorgándoles espacio en la nube para almacenar los servicios analíticos para sus aplicaciones (SDK, librerías, bases de datos, gestión de usuarios, desarrollo y pruebas, integración con otros servicios, despliegue, etc.). BaaS se puede considerar como la evolución de los servidores de aplicaciones 'in situ', en donde se ofrece la posibilidad de dejar de lado la necesidad de un back-end para las aplicaciones, aumentando la eficiencia en el desarrollo y optimizando los costos.

4.1.5.6 Cache Como Servicio (Cache as a Service – CaaS)

Assila, Kobbane, Ben-Othman y Koutb[20] se refieren a Cache como Servicio (CaaS) como un modelo orientado al servicio, para el almacenamiento en caché de la información y contenidos para redes móviles basadas en la nube. Los contenidos se pueden distribuir y almacenar en función de la demanda de los consumidores finales de la información. Este concepto surge como respuesta a la demanda de contenido en Internet, donde es más rápido y eficiente para una aplicación acceder a memoria cache, que a una base de datos.

[18] TOESLAND, finbarr. C XAAS MODEL RESHAPES THE FUTURE OF OUTSOURCING. En: Computer Weekly., junio 2019., p. 27.

[19] DEL VECCHIO, José Francisco; PATERNINA, Fabián José y MIRANDA, Carlos. La computación en la nube: un modelo para el desarrollo de las empresas. En: Revista Prospectiva. Vol. 13., Julio – Diciembre, 2015., p.83.

[20] ASSILA, Bouchaib; KOBBANE, Abdellatif; BEN-OTHMAN, Jalel y KOUTBI, Mohammed El. Caching as a Service for 5G Networks: A Matching Game Approach for CaaS Resource Allocation. En 2018 IEEE Symposium on Computers and Communications (ISCC). 01193-01198J., Junio, 2018., p. 1.

4.1.5.7 Función Como Servicio (Function as a Service – FaaS)

Manner, Endreb, Heckel,y Wirtz[21] definen que Función Como Servicio es el grupo de servicios de Cloud Computing que consisten en proporcionar una plataforma para que los clientes puedan desarrollar, ejecutar y administrar las funciones de una aplicación sin mantener la infraestructura para ello. Contrario a PaaS, FaaS no requiere que se esté ejecutando constantemente ningún proceso del Servidor y solo se paga por el tiempo de ejecución de la función (y no por el tiempo de inactividad del proceso). Esta definición también es aceptada bajo el nombre de Funciones sin Servidor o Serverless Computing, en donde los desarrolladores desarrollan sus proyectos sin necesidad de contratar explícitamente un servidor para ello.

4.1.5.8 Escritorio Como Servicio (Desktop as a Service – DaaS)

Anderson[22] describe el Escritorio Como Servicio, como la virtualización de escritorios remotos a través de la computación en la nube. Escritorio como servicio (DaaS) proporciona un nivel alto de automatización y multitenencia real, reduciendo el coste de la tecnología. El CSP del servicio DaaS hospeda y mantiene la infraestructura de la computadora, el almacenamiento y el acceso, así como las aplicaciones y licencias de software de aplicaciones necesarias para proporcionar el servicio de escritorio a cambio de una tarifa mensual establecida. Los usuarios aún pueden obtener una experiencia de PC a través de un cliente ligero, pero el sistema operativo de la PC se ejecuta de forma remota en un servidor virtual alojado en la nube, donde la administración del software corre por cuenta del CSP.

4.1.5.9 Datos Como Servicio (Data as a Service – DaaS)

Abe y Ustundaug[23] se refieren a que Datos Como Servicio, se basa en el concepto de que productos ya procesados como los datos, se pueden proveer al cliente bajo modelos de distribución por demanda. Datos como Servicio permite que exista la separación de los costos y uso de los datos, del costo de un entorno de almacenamiento o plataforma de software empleada para su manipulación. DaaS trae la noción de que la calidad, el mantenimiento y el almacenado de los datos (tanto texto, como imágenes o video) es ajeno a la entidad que los necesita y el uso que esta les dé.

---

[21] MANNER, Johannes; ENDREB, Martin; HECKEL, Tobias y WIRTZ, Guido. Cold Start Influencing Factors in Function as a Service. En 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion). 181-188., Diciembre, 2018., p. 1.

[22] ANDERSON, Tim. How to Make Sense of Desktop as a Service. En: Computer Weekly., 2013., p. 15.

[23] ABE, John Olorunfemi y USTUNDAUG, Burak Berk. A Data as a Service (DaaS) Model for GPU-based Data Analytics. En: IEEE IFIP NTMS Workshop on Big Data and Emerging Trends WBD-ET 2018., Febrero, 2018., p. 2.

4.1.5.10 Red Como Servicio (Network as a Service – NaaS)

Los autores Nadaf, Rath, Arun Kumar, Shailendra, y Simha[24] describen el concepto Network as a Service (NaaS) como los servicios para conectividad de transporte de red, que implican la optimización de las ubicaciones de recursos al considerar los recursos de red y computación como un todo unificado. También incluye la prestación de un servicio de red virtual por parte de los propietarios de la infraestructura de red a un tercero, o la virtualización de la red, donde se puede controlar fácilmente la asignación de ancho de banda, o el acceso a los recursos. También incluye protocolos de seguridad de red personalizados. Con lo anterior, el cliente se puede despreocupar por la administración y la seguridad de las redes.

4.1.5.11 Seguridad Como Servicio (Security as a Service – SecaaS)

Futaro, Garro y Tundis[25] referencian Seguridad Como Servicio, como la provisión de aplicaciones y servicios de seguridad (antivirus, control de autenticación, pentesting, gestión de eventos de seguridad, etc.) a través de la nube a la infraestructura y al software basados en la nube o desde la nube. Los beneficios de un modelo de SecaaS se traducen en reducción de costos por actualización del software de seguridad, tercerización de la administración, parametrización y tareas rutinarias, etc.

Se pueden diferenciar los siguientes tipos de servicios de seguridad:

- Identity and Access Management (IAM): Administración y control de accesos al Sistema
- Data Loss Prevention (DLP): Procesos enfocados en garantizar la seguridad, protección y monitoreo de los datos que se intercambian
- Web Security (WS): Protección mediante la aplicación de políticas al tráfico web
- EMail Security (EMS): Control de seguridad sobre el correo electrónico, protege el entorno empresarial del phishing o ficheros adjuntos maliciosos
- Intrusion Management (IM): Detección y bloqueo de eventos inusuales

[24] NADAF, Shameemraj; RATH, Hemant; ARUN KUMAR, A V; SHAILENDRA, Samar y SIMHA, Anantha. An open source based network as a service (NaaS) platform for cloud provisioning. En 2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)., Diciembre, 2015., p. 1.

[25] FUTARO, Angelo; GARRO, Alfredo y TUNDIS, Andrea. Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing. En: 2014 International Carnahan Conference on Security Technology (ICCST)., Octubre, 2014., p. 1 -2.

- Intrusion Detection Systems (IDS): Sistemas de detección de intrusos
- Intrusion Prevention Systems (IPS): Sistemas de prevención de intrusos
- Business Continuity and Disaster Recovery (BCDR): Procesos que garantizan la capacidad de recuperación ante un evento
- Encryption Services: Protección de datos aplicaciones mediante cifrado
- Network Security (NS): Servicios de monitoreo y protección de los recursos de red
- Security Information and Event Management (SIEM): Monitorea los eventos de seguridad, generando informes y alertas.

4.1.6 Modelos de Despliegue de Cloud Computing

Existe una clasificación de los tipos de nubes, relacionada con la propiedad, la cobertura y el acceso a los servicios. Varela, Portella y Pallares[26] resumen esta clasificación así:

4.1.6.1 Nube Pública

Una nube pública es administrada por un CSP dueño de una infraestructura tecnológica importante y muy sofisticada, el cual puede tener varios clientes. Entre los distintos usuarios no es posible saber quién más usa la misma aplicación o servicios, tampoco es posible acceder física o lógicamente a los ficheros de otros usuarios. Los clientes tampoco pueden saber cómo se ejecutan los procesos, o exactamente en qué servidores se almacena su información. La principal ventaja de este modelo de despliegue es la gran capacidad de procesamiento y almacenamiento que puede ofrecer el CSP, el cual tiene una infraestructura física robusta capaz de garantizar niveles adecuados de disponibilidad y seguridad en sus data-centers.

4.1.6.2 Nube Privada

Es implementada por la misma organización que usa el servicio, o por un tercero o terceros contratados para gestionar un data-center de uso exclusivo. La empresa propietaria es dueña de su nube, y es quien decide sobre las políticas y

[26] VARELA, Carlos; PORTELLA, Jorge y PALLARES, Luis. Computación en la nube: un nuevo paradigma en las tecnologías de la información y la comunicación. En: Revista Electrónica Redes de Ingeniería. edición especial., enero - junio 2017., p. 138-146.

procedimientos de administración y seguridad que se pueden aplicar. Tiene elementos comunes con la nube pública, como el uso de máquinas virtuales, a pesar de que se trata de una gran infraestructura 'On Premise'. Es conveniente en grandes organizaciones que buscan niveles de seguridad y control muy elevados. Los inconvenientes de una nube privada son los mismos de una infraestructura 'On Premise', donde los costos de construcción, administración y mantenimiento pueden llegar a ser elevados.

4.1.6.3 Nube Hibrida

Consiste en un modelo de despliegue que reúne varias nubes a la vez: nube privada y nube pública, o nube privada y nube comunitaria, o dos nubes privadas pero independientes entre sí, lo cual permite que se compartan datos y aplicaciones entre las distintas nubes. También se puede, por ejemplo, alojar aplicaciones en nubes privadas, y ser accedidas por los usuarios desde nubes públicas, de modo que se puede tener control sobre aspectos críticos de las aplicaciones aprovechando a la vez las ventajas de procesamiento ofrecidas por la nube pública. Un ejemplo de nube hibrida puede ser Guao, de la Empresa de Telecomunicaciones de Cuba[27], el cual provee un software que permite la creación de entornos basados tanto en la nube publica como en la privada, según la necesidad del proyecto.

4.1.6.4 Nube Comunitaria

Este tipo de nube es aquella infraestructura tecnológica implementada por un grupo de entidades u organizaciones, con la que se busca suplir un problema o necesidad en común. Puede ser implementada en los data-center de alguna de las empresas participantes, o puede ser externa o administrada por un tercero. Un miembro del grupo puede acceder a su infraestructura, o a la infraestructura de otros miembros mediante los canales de comunicación y protocolos establecidos. Una de las grandes ventajas de este modelo de despliegue, es que los costos son compartidos entre las distintas organizaciones involucradas.

4.1.7 Orquestación del Servicio de Cloud Computing

The Nist[28] define la orquestación del servicio de Cloud Computing, como la abstracción de los componentes del sistema usados por el CSP para disponibilizar y gestionar los recursos necesarios para proporcionar los distintos servicios en la nube al cliente final. El modelo plantea una distribución de los elementos en capas,

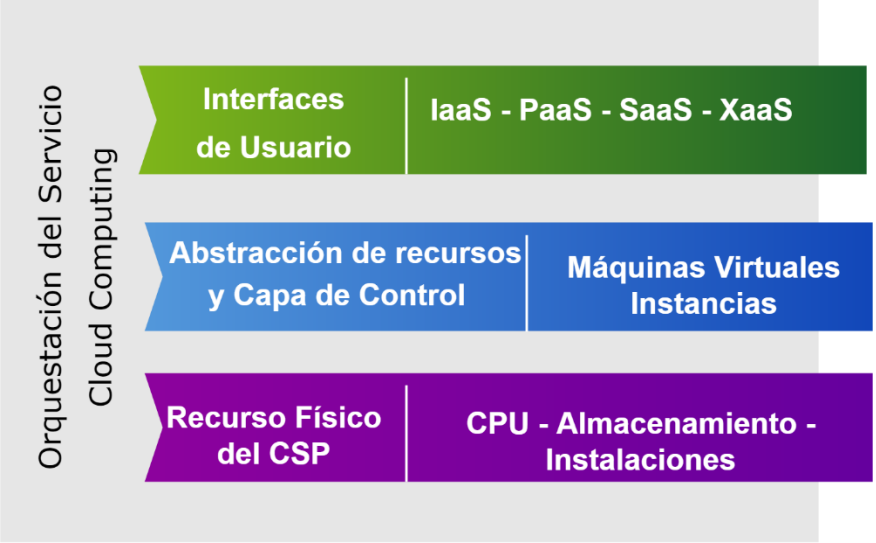
[27] ALFONSO FERRER, Eduardo. Wow! On the Road to the Cloud. En: Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A. Vol. 10 Issue 2., 2013., p. 8-13

[28] LIU, Fang; TONG, Jin; MAO, Jian; BOHN, Robert; MESSINA, John; BADGER, Lee y LEAF, Dawn. NIST Cloud Computing Reference Architecture. En: NIST. Special Publication 500-292., Septiembre, 2011., p. 13.

en donde la capa superior corresponde a las interfaces con las cuales interactúa el cliente, que varían dependiendo del modelo de servicio contratado (Servicio, Infraestructura, Plataforma, etc.). Una capa intermedia corresponde a la abstracción de recursos físicos y la capa de control, la cual contiene los elementos correspondientes a la administración y asignación de recursos suministrados por el CSP, y son básicamente a máquinas virtuales, instancias y cualquier elemento que represente un elemento virtualizado del hardware, con lo que se garantiza el uso eficiente, dinámico, seguro, mesurado y controlado de la infraestructura física por parte del cliente final. Finalmente, la capa inferior del modelo corresponde a los recursos físicos reales del CSP, lo que incluye CPU, memoria, elementos de red, elementos de almacenamiento y todos elementos de apoyo (instalaciones, sistema de refrigeración, suministro energético, etc.), Esta última capa soporta toda la operación del servicio, sin ser gestionada ni intervenida por el usuario final.

La orquestación del servicio de Cloud Computing, tal como la describe The Nist, se puede resumir en la figura 1:

Figura 1. Orquestación del Servicio de Cloud Computing



Fuente: El Autor

4.1.8 Virtualización

En el documento de Arévalo Navarro[29] se describe el concepto de virtualización como una abstracción clave para el Cloud Computing, ya que es lo que le permite

[29] ARÉVALO NAVARRO, Op. cit., p. 26.

el acceso ubicuo, o sea la capacidad que tiene un sistema de integrarse con la realidad de los usuarios finales, de forma que este no se perciba como un elemento con características diferenciadas, con capacidad de ser accesado desde cualquier lugar y en cualquier momento.

La virtualización es asignar un nombre de un recurso físico a un elemento lógico (software), el cual puede cumplir las mismas funciones que dicho recurso físico, pero de manera más fácil y dinámica (ya que no posee las limitaciones de capacidad propias del hardware tradicional). Esta abstracción corresponde a la creación de una versión basada en software de un elemento de hardware. El concepto de virtualización se puede aplicar a Sistemas Operativos, dispositivos de almacenamiento, procesadores, redes, etc.

4.1.9 Servicios Administrados

Para Fernández[30], los servicios administrados son los ofrecidos por un Proveedor de Servicios Administrados o MSP, que conservan algunas características de Cloud Computing (como el acceso al servicio vía internet), pero que se diferencian en que son completamente administrados por el proveedor, quitando al usuario final el trabajo operativo y optimizando los costos ya que son facturados por uso efectivo. Ejemplos de estos servicios: gestión de la seguridad, del almacenamiento, de la red, entre otros.

4.2 MARCO LEGAL Y NORMATIVO

4.2.1 Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos[31] corresponde a la regulación promulgada por la Unión Europea, en 2016, para unificar la legislación relacionada con Protección de Datos Personales en los distintos países miembros de la Unión. Entre otras cosas, estipula:

- Cuáles son los requisitos que deben cumplir las empresas que operan en Europa en cuanto a protección de datos personales.
- Cómo se deben almacenar y procesar los datos personales.
- Cuáles son las multas aplicables a los incumplimientos de la norma.

[30] FERNÁNDEZ Op. cit., p. 45.

[31] UNIÓN EUROPEA. PARLAMENTO EUROPERO Y EL CONSEJO. Reglamento General de Protección de Datos. (4, mayo, 2016). Diario Oficial. Unión Europea, 2016. No. L 119/1.

Las empresas que se acogen a esta normatividad para poder operar en Europa deben demostrar:

- Que tienen implementados mecanismos que evidencian el cumplimiento del reglamento (políticas, procedimientos, documentos, etc.). Estos mecanismos deben ser de libre acceso a los consumidores en general.
- Deben establecer mecanismos para documentar de manera explícita el consentimiento de sus clientes para poder tratar datos personales.
- Que el cumplimiento del reglamento comienza desde el diseño de la empresa, producto o servicio que implique el uso de datos personales dentro de su operación.
- Que demuestran el cumplimiento de las distintas legislaciones y reglamentos de forma pública y transparente.

4.2.2 Leyes y Regulaciones Colombianas

A partir del año 2000, el Estado Colombiano, así como los distintos países latinoamericanos, han promulgado distintas leyes asociadas con la protección de datos personales basados en la Directiva de Protección de Datos de la Unión Europea de1995 (la Directiva 95/46/CE sobre protección de datos del 24 de octubre de 1995 fue sustituida por el Reglamento General de Protección de Datos – RGPD que entró en vigencia el 25 de mayo de 2016), tal como lo afirman Gutiérrez y Korn[32]. El común denominador de estas normas es la protección de datos personales, el control y las restricciones propias de la trasmisión y almacenamiento de la información en los distintos sistemas de información.

4.2.2.1 Ley 1266 de 2008

Ley Estatutaria 1266[33] de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Fue dictada por el gobierno nacional para proteger el derecho que tienen los individuos a conocer,

[32] GUTIÉRREZ, Horacio y KORN, Daniel. Facilitando “the cloud”: la regulación de la protección de datos como motor de la competitividad nacional en América Latina. En: Revista La Propiedad Inmaterial no. 18., Universidad Externado de Colombia., Noviembre, 2014., p. 85-118.

[33] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. No 47219. p. 1-24.

actualizar o rectificar la información que exista sobre cada uno en las distintas bases de datos recolectadas, tanto por entidades públicas como privadas.

4.2.2.2 Ley 1273 de 2009

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Esta ley también es conocida como la ley de Delitos Informáticos en Colombia. En su artículo 269F, regula la tenencia y transmisión de datos personales en los distintos sistemas de información sin previa autorización del propietario o titular de la información:

> Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.[34]

4.2.2.3 Ley 1341 de 2009

La Ley 1341[35] de 2009, por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Esta ley atribuye al Ministerio de Tecnologías de la Información y las Comunicaciones, autonomía para diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones, así como capacidad para promover el uso y acceso a nuevas tecnologías.

---

[34] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2011. No. 47223. p. 1-4.

[35] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2011. p. 1-34.

4.2.2.4 Ley 1581 de 2012

La Ley Estatutaria 1581[36] de 2012, también conocida como La ley de Protección de Datos Personales. Protege el derecho de todas las personas naturales a autorizar o denegar el uso, transmisión o almacenamiento de sus datos personales en los sistemas de información de las empresas o entidades. Esta ley delimita los derechos de los dueños o titulares de la información:

- Derecho a conocer, actualizar y rectificar los datos personales en manos de los responsables del Tratamiento (empresas o entidades).
- Derecho a saber cuál es el uso que se le da a la información.
- Derecho a solicitar copia de la autorización de uso de la información suministrada a los responsables del Tratamiento.
- Derecho a revocar la autorización de uso de la información suministrada a las distintas empresas o entidades.

El ámbito de aplicación de esta ley corresponde "al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales", tal y como se describe el Articulo 2. En su análisis, Gutiérrez y Korn[37] comparan la Ley 1581 colombiana con sus equivalentes en la legislación argentina y uruguaya (todas estas basadas y compatibles con las regulaciones de la Unión Europea), y se concluye que ninguna de estas permite la transferencia de información a países que no tengan regímenes de protección de datos adecuados, salvo que exista autorización explícita del dueño de la información.

4.2.2.5 Acuerdo Marco de Servicios de Nube Pública III

El Gobierno de Colombia, mediante la Agencia Nacional de Contratación Pública-Colombia Compra Eficiente, establece instrumentos para la regulación de precios y contratación de servicios por parte de las entidades públicas. Estos instrumentos son denominados Acuerdos Marco, y son específicos a cada tipo de producto o servicio ofertado. El Acuerdo Marco de Servicios de Nube Pública da herramientas a las entidades estatales para realizar compras de servicios de Cloud Computing

[36] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2013. No 48587. p. 1-301.

[37] GUTIÉRREZ, y KORN, Op. cit., p. 85 - 118.

(nube pública, nube privada y servicios profesionales) a partir de procesos de contratación más rápidos de productos estandarizados y de calidad.

La versión actual del Acuerdo Marco sobre Cloud Computing es conocida como 'Acuerdo Marco de Servicios de Nuble Pública III'[38] se encuentra vigente para el periodo Octubre 25 - 2019 hasta Octubre 25 - 2021, y su objeto es establecer:

- Las condiciones para la contratación de Servicios de Cloud Computing
- Las condiciones de la prestación del servicio por parte de los CSP
- Las condiciones bajo las cuales las Entidades Públicas se vinculan al Acuerdo Marco y adquieren Cloud Computing
- Las condiciones para el pago de los servicios de Cloud Computing.

El Acuerdo Marco para la Prestación de Servicios de Nube Pública se divide en dos catálogos: Catálogo de Servicios de Computación en la Nube (SaaS, PaaS y IaaS) y Catálogo de Servicios Complementarios (Capacitación, Servicios Profesionales, Servicios de Migración, Soluciones y Soporte). Los catálogos son suministrados y actualizados por los CSP y los proveedores que actualmente se acogen a las condiciones descritas por el Acuerdo Marco y que pueden prestar la totalidad de sus servicios a las entidades públicas colombianas, directamente o por medio de sus partners son: Amazon Web Services, Google Cloud, Microsoft Azure y Oracle Cloud.

4.2.3 Estándares y Normas Internacionalmente Aceptadas

4.2.3.1 CSA STAR

CSA STAR[39] o Cloud Security Alliance, es una organización sin ánimo de lucro que se encarga de promover las buenas prácticas para buscar que la computación en la nube sea segura (mantiene el Registro de Seguridad, Confianza y Garantía - STAR). Se vale de tres niveles (autoevaluación, auditoría de terceros y supervisión continua) para que los clientes de Cloud Computing puedan evaluar a sus proveedores. Mantiene un registro público y gratuito donde los CSP pueden publicar sus evaluaciones.

[38] COLOMBIACOMPRA. Nube pública III [en línea]. Bogotá: Colombia Compra Eficiente., Disponible en https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/nube-publica-iii

[39] CLOUD SECURITY ALLIANCE. About. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://cloudsecurityalliance.org/

4.2.3.2 FedRAMP

FedRAMP[40] o Programa Federal de Administración de Autorizaciones y Riesgo, es un programa de los Estados Unidos creado para brindar un enfoque estándar sobre la evaluación de la Seguridad, la Autorización y la Supervisión en servicios de Cloud Computing. Fue publicado en 2011 por Office of Management and Budget buscando la implementación metódica de computación en la nube dentro de las distintas oficinas gubernamentales de Estados Unidos.

4.2.3.3 ISO/IEC 20000-1:2011

ISO/IEC 20000-1:2011[41] Information technology - Service management - Part 1: Service management system requirements. Es una de las normas de la familia ISO/IEC 20000, que especifican los requisitos para la certificación de los servicios de soporte y gestión e TI. Está enfocada en los proveedores de servicios de TI, buscando que los servicios estén alineados con las necesidades de los usuarios de los servicios, asegurando calidad, optimizando costos y garantizando seguridad y mejora continua. Contiene 217 requisitos, los cuales se agrupan en cinco bloques: Provisión del Servicio, Control, Entrega, Resolución y Relaciones.

4.2.3.4 ISO/IEC 22301:2012

ISO/IEC 22301:2012[42] Societal security - Business continuity management systems - Requirements. Esta norma específica los requisitos para implementar un Sistema de Gestión de Continuidad del Negocio. Busca ayudar a las empresas a minimizar el riesgo de interrupción de las operaciones, y determinar la mejor manera de recuperarse de las interrupciones en el momento en que sucedan. Esta norma determina requisitos genéricos, aplicables en cualquier entorno empresarial.

4.2.3.5 ISO/IEC 27000:2018

ISO/IEC 27000:2018[43] Information technology - Security techniques - Information security management systems -- Overview and vocabulary, corresponde al conjunto de normas internacionales enfocados a la Seguridad Informática. ISO 27000 abarca un grupo o familia de estándares complementarios entre sí, define la terminología

[40] FEDRAMP. About Us. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.fedramp.gov/about/

[41] ISO-IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements.

[42] ISO-IEC 22301:2012 Societal security - Business continuity management systems – Requirements.

[43] ISO-IEC 27000:2018, Information technology - Security techniques - Information security management systems -- Overview and vocabulary.

necesaria para entender las demás normas asociadas. Entre estas normas asociadas se puede destacar: ISO 27001 correspondiente a la certificación de Sistema de Gestión de la Seguridad de la Información (SGSI); ISO 27002 describe las buenas prácticas a seguir para la seguridad en la información; o ISO 27004 que describe cómo implementar métricas o indicadores para medir la gestión en la seguridad de la información.

4.2.3.6 ISO/IEC 27001:2013

ISO/IEC 27001:2013[44] Information Technology - Security Techniques - Information Security Management Systems – Requirements. Es una de las normas de la familia ISO/IEC 27000. Ésta en particular describe los requisitos que debe cumplir una empresa para implementar y obtener la certificación en los Sistemas de Gestión de la Seguridad de la Información (SGSI). En esta norma se deben delimitar, por ejemplo, el campo de aplicación del SGSI dentro de la organización, el soporte o recursos destinados a mantener el sistema, planes de mejora, etc.

4.2.3.7 ISO/IEC 27002:2013

ISO/IEC 27002:2013[45] Information Technology - Security Techniques - Code Of Practice For Information Security Management. Este estándar describe catorce dominios principales y 114 controles de seguridad informática, de aplicación general (existen normas específicas para ciertos sectores, como la ISO/IEC 27011 aplicable a Telecomunicaciones, o la ISO/IEC 27017 aplicable a Computación en la Nube).

4.2.3.8 ISO/IEC 27017:2015

ISO/IEC 27017:2015[46] Information Technology — Security Techniques — Code Of Practice For Information Security Controls Based On ISO/IEC 27002 For Cloud Services. Proporciona los controles para los CSP y clientes de los servicios de Cloud Computing Esta norma aclara las funciones y responsabilidades de ambas partes para lograr que la computación en la nube sea tan segura como el resto de los datos incluidos en un Sistema de Gestión de Seguridad Informática. Esta norma se basa en la norma ISO/IEC 27002 e incluye 37 controles aplicables a clientes y proveedores de computación en la nube.

---

[44] ISO-IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements.

[45] ISO-IEC 27002:2013, Information Technology - Security Techniques - Code Of Practice For Information Security Management.

[46] ISO-IEC 27017:2015, Information Technology — Security Techniques - Code Of Practice For Information Security Controls Based On ISO/IEC 27002 For Cloud Services.

4.2.3.9 ISO/IEC 27018:2019

ISO/IEC 27018:2019[47] Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Es una de las normas de la familia ISO/IEC 27000. Esta norma establece objetivos, controles y pautas comúnmente aceptados para implementar medidas de protección de la información personal de acuerdo con los principios de privacidad la norma ISO/IEC 29100: Protección de Información de Identificación Personal (PII), aplicables en el contexto de los entornos de riesgo de seguridad informática de un proveedor de servicios de nube pública.

Fernández y Recio[48] describen este estándar como el primero sobre la privacidad y la protección de datos personales de aceptación internacional, y está redactado a la luz de la legislación de la Unión Europea (RGPD - Reglamento General de Protección de Datos). Establece pautas para determinar si un CSP ha adoptado adecuadamente medidas en cuanto a protección de datos personales, las cuales deben ser auditables y verificables. Esta norma complementa a la ISO/IEC 27001:2013 en cuanto a la identificación e implementación de controles especializados en privacidad. Servirá al CSP como marco de referencia para la implementación de buenas prácticas y esquemas de autorregulación en cuanto a protección de datos se refiere.

4.2.3.10 ISO/IEC 29100:2011

ISO/IEC 29100:2011[49] Information technology -- Security techniques -- Privacy framework. Proporciona un marco de trabajo en relación con la protección de datos personales contenidos dentro de las Tecnologías de la información y la Comunicación. Su finalidad orientar a las organizaciones a implementar los mecanismos de protección de datos personales.

4.2.3.11 PCI DSS

PCI DSS[50] es el estándar de seguridad de datos específico para la protección de las tarjetas de crédito. Fue creado por un consejo conformado por las franquicias de tarjetas de crédito más importantes (Visa, MasterCard, American Express) y determinan las buenas prácticas e indicaciones de seguridad en los sistemas, que

[47] ISO-IEC 27018:2019, Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

[48] FERNÁNDEZ, Carlos y RECIO, Miguel. Privacidad Elevada a la Nube [en línea]. Madrid: AENOR. 2015., p. 20 - 23. Disponible en https://portal.aenormas.aenor.com/revista/pdf/nov15/20nov15.pdf

[49] ISO-IEC 29100:2011, Information technology -- Security techniques -- Privacy framework.

[50] PCI SECURITY STANDARDS COUNCIL. ABOUT US. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.pcisecuritystandards.org/about_us/

deben cumplir los proveedores de servicios para proteger la información de los clientes.

4.2.3.12 SOC 1

SOC 1 - SOC for Service Organizations: ICFR[51]. Es un informe que documenta los controles internos que pueden ser pertinentes a la información financiera, tanto en su procesamiento como en su almacenamiento. Este tipo de auditorías son necesarias en aquellas organizaciones que administran o ejecutan procesos que afectan información financiera de clientes.

4.2.3.13 SOC 2

SOC 2 - SOC for Service Organizations: Trust Services Criteria[52] se creó a partir de los criterios de auditoría del AICPA (Instituto Americano de Contables Públicos Certificados) con el fin de establecer mecanismos para evaluar los controles a los sistemas informáticos en términos de seguridad, disponibilidad, integridad y confidencialidad. La guía SOC 2 fue actualizada el 1 de enero de 2018.

4.2.3.14 SOC 3

SOC 3 - SOC for Service Organizations: Trust Services Criteria for General Use Report[53]. Es un informe diseñado con el fin de establecer mecanismos para evaluar los controles a los sistemas informáticos en términos de seguridad, disponibilidad, integridad y confidencialidad, pero con necesidades más básicas de información que SOC 2. Se puede acceder a este tipo de informe libremente.

4.2.4 Prestación del Servicio del Cloud Computing

Algunos conceptos clave para entender el modelo de contratación aplicable a Cloud Computing son:

---

[51] AICPA. SOC 1 - SOC for Service Organizations: ICFR. [en línea]. [Consultado el 19 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html

[52] AICPA. SOC 2 - SOC for Service Organizations: Trust Services Criteria. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

[53] AICPA. SOC 3 - SOC for Service Organizations: Trust Services Criteria for General Use Report. [en línea]. [Consultado el 19 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc3report.html

4.2.4.1 Actores del Cloud Computing

Dentro de Cloud Computing se pueden diferenciar distintos tipos de actores que cumplen determinadas funciones y roles dentro de la prestación de los servicios, a saber:

Cloud Service Client – CSC
The Nist, en su documento Cloud Computing Reference Architecture[54] define al consumidor o Cliente de Cloud Computing como una persona u organización que mantiene una relación comercial con CSP. Es quien recibe el servicio y se le puede facturar por el servicio prestado, y debe efectuar los pagos correspondientes. El CSC puede escoger libremente el proveedor más adecuado a sus necesidades y especifica mediante el SLA los requisitos técnicos y de servicio. El Consumidor es el principal actor en la relación comercial establecida, ya que es quien conociendo el portafolio de servicios y precios del CSP solicita un servicio apropiado, establece contratos con el CSP y negocia los SLA apropiados para su necesidad tecnológica, en términos de calidad del servicio, la seguridad y escalamientos por fallas en el servicio.

Dependiendo del modelo de servicio contratado, un consumidor tiene las siguientes características:

- Un cliente SaaS es aquel que brinda a sus miembros acceso a software configurado para ser empleado por usuarios finales. El cobro se genera en función de usuarios o licencias contratados, tiempo de uso o volumen de datos almacenados.

- Un cliente IaaS es aquel que tiene acceso a máquinas virtuales, dispositivos de almacenamiento y otros tipos de elementos tecnológicos virtualizados donde puede implementar o ejecutar herramientas libremente. La facturación se genera según el tiempo o cantidad de recursos informáticos utilizados, volumen de información almacenada, etc.

- Un cliente PaaS utiliza las herramientas y recursos suministrados para desarrollar, testear, e implementar su software. El cobro a un cliente PaaS se genera según procesamiento, almacenamiento, recursos consumidos o duración del uso de la plataforma.

[54] LIU, TONG, MAOBOHN, MESSINA, BADGER y LEAF, Op. cit., p. 5.

Cloud Service Provider – CSP

Moreno Gómez[55] define que un CSP, es el prestador del servicio de Computación en la Nube. Corresponde a una organización que, a través de internet, pone a disposición de sus clientes el uso sus data-centers para guardar información o desarrollar y ejecutar software, usar aplicaciones propias del CSP, o permitir la utilización de su infraestructura para suplir necesidades de infraestructura tecnológica de terceros.

Las principales obligaciones del CSP son descritas por Grunfeld y Schcolnik[56] así:

- El CSP se compromete a mantener la disponibilidad del servicio, generalmente definidos en porcentajes de tiempo de actividad del servicio y acordes con el SLA contratado.
- El CSP no debe vender, licenciar o revelar datos del cliente, salvo autorización expresa del titular de dicha información.
- El CSP es el encargado de garantizar seguridad física y lógica, encriptación de datos y disponibilidad de los servicios contratados.
- El CSP es responsable de sus data-centers, así como de proveer la custodia y copias de seguridad de los datos almacenados.
- La prestación del servicio está enmarcada por el cumplimiento de un SLA o acuerdo de nivel del servicio.

Auditor de la Nube

The Nist[57] define al auditor de la nube como una entidad u organización externa que vela y certifica por que el CSP cumpla con las leyes, estándares y normas de aceptación general, a través de la ejecución de auditorías para la revisión de evidencia, revisión de controles informáticos o validar el cumplimiento de la normatividad asociada con seguridad o calidad.

Agente de la Nube

La función de un agente la nube corresponde a la de intermediación entre el Cliente y el Proveedor. También es referenciado como Cloud Broker y es quien se encarga de la implementación del servicio, de la administración del y medición uso, de la gestión del acceso, del rendimiento, del cumplimiento de los SLA y de la negociación

[55] MORENO GOMEZ, Gonzalo Andrés. Jurisdicción Aplicable En Materia De Datos Personales En Los Contratos De Cloud Computing: Análisis Bajo La Legislación Colombiana. En: Revista de Derecho, Comunicaciones y Nuevas Tecnologías. No 9., Julio, 2013., p. 6.

[56] GRUNFELD, Bárbara y SCHCOLNIK, Alan. ¿Cloud computing?. En: IEEM Revista de Negocios., Junio, 2015., p. 66-67.

[57] LIU, TONG, MAOBOHN, MESSINA, BADGER y LEAF, Op. cit., p. 8.

comercial entre las partes, mejorando la experiencia de usuario al prestar servicios más personalizados. La Agencia Española de Protección de Datos[58] se refiere al Agente de la Nube como socio o partner del CSP, y su función dentro de la prestación del servicio en la nube es la intermediación entre el cliente y el proveedor, ejerciendo distintas figuras contractuales como reseller, vendedor, etc.

4.2.4.2 Service Level Agreement (SLA)

También conocido como ANS o Acuerdo de Nivel de Servicio, es un acuerdo que muestra cual el nivel de servicio que espera un cliente por parte de un proveedor, en términos de operación del servicio en la nube contratado, tiempos de respuesta a los requerimientos, disponibilidad de recurso humano, documentación y herramientas para garantizar el correcto funcionamiento del producto contratado.

Arévalo Navarro[59] describe las características básicas de este elemento del contrato de Cloud Computing:

- Un SLA es un elemento de mutuo consentimiento entre el cliente y el CSP, sobre aspectos vitales como tiempos de respuesta, disponibilidad de atención, herramientas y documentos de apoyo, o sea que define como va a ser la relación entre las dos partes.
- Debe indicar claramente las características técnicas del producto contratado, unidades de medida, métricas, herramientas de monitoreo y auditoria y niveles de escalamiento.
- Debe delimitar claramente cuáles son las necesidades del cliente y la capacidad del CSP para atender esas necesidades, proporcionando un marco de consenso y entendimiento sobre las prioridades, responsabilidades y garantías, reduciendo los conflictos por desacuerdo. Los SLA también deben tener claros como penalizar el no cumplimiento de alguno de los compromisos adquiridos por alguna de las dos partes.
- Los resultados del acuerdo deben ser medibles, ya sea en términos de satisfacción del cliente como la cantidad de atenciones realizadas, tiempo de primera respuesta, o tiempo de gestión de la solicitud; o en términos de rendimiento de la infraestructura como procesamiento de datos en la unidad de tiempo, uso de espacio de almacenamiento o memoria utilizada.

[58] AEPD. Guía para clientes que contraten servicios Computing [en línea]. Madrid: Agencia Española de Protección de Datos. 2018., 25 p. Disponible en https://www.aepd.es/media/guias/guia-cloud-clientes.pdf p. 6

[59] ARÉVALO NAVARRO, Op. cit., p. 18 - 20.

4.2.4.3 Generalidades de la Contratación de Servicios Cloud Computing

La Agencia Española de Protección de Datos[60] describe algunos aspectos generales para tener en cuenta al momento de contratar servicios de Cloud Computing:

- El cliente del servicio en la nube debe verificar junto con el CSP si el contrato ofrece las condiciones adecuadas en términos de cumplimiento de políticas de seguridad, garantías de calidad, protección de derechos del usuario, y obligaciones legales en cuanto a tratamiento de información acordes con la normatividad del país en donde se firma el contrato de prestación de servicios. A nivel de contrato, también deben quedar claros los derechos y deberes, tanto del CSP como del cliente, así como del alcance de los terceros que intervengan en la prestación del servicio.

- Pese a que los principales CSP operan como multinacionales, con infraestructura distribuida en distintos países, no se debe desconocer el cumplimiento de la reglamentación local en cuanto a protección de datos personales, ya que el dueño y responsable primario de la información es el cliente del servicio en la nube.

- El CSP debe garantizar que existen herramientas de portabilidad de datos, esto es que esté en la capacidad de integrarse fácilmente a sistemas heredados, a servicios locales y a servicios en otras nubes (e incluso la migración hacia otras nubes o arquitecturas cuando se dé por terminada la relación comercial entre el CSP y el Cliente), con el fin de disponibilizar los datos y dar continuidad al servicio, mediante el uso de lenguajes estándar y cualquier mecanismo propio de una arquitectura SOA.

- El cliente debe tener claro el tipo de nube que está contratando (pública, privada, híbrida), los distintos modelos de servicio (IaaS, PaaS, SaaS, etc.) y cual se adapta más a sus necesidades operativas.

- El CSP debe manifestar claramente que no dará ningún manejo a los datos distinto al contratado con el cliente. Igualmente, debe garantizar que posee las políticas y procedimientos de seguridad informática para garantizar Confidencialidad, Integridad y Disponibilidad de la información. Así mismo. el cliente puede exigir que le sean informados cuáles son los mecanismos, herramientas y estrategias de seguridad con las cuales el CSP afronta todo lo relacionado con la seguridad y el cifrado de información, así como conocer cuáles son los estándares internacionales en cuanto a seguridad que respaldan la operación del CSP.

[60] AEPD. Op. cit., p. 14 – 19.

A la luz de la legislación colombiana, tal como lo describen Preciado y Vargas[61], cuando se contrata Cloud Computing es importante tener en cuenta:

- Debe quedar especificada cual es la jurisdicción legal que aplica al contrato, teniendo en cuenta que el CSP puede ser de una nacionalidad, el cliente de otra, y los data-centers pueden estar en un tercer país. En cuanto a la transferencia de información a otros países, se debe tener en cuenta que la Ley 1581 de 2012 restringe la transferencia de información a países en donde la normatividad no garantice los niveles adecuados de seguridad informática. Se considera que los países que cuentan con niveles adecuados de seguridad informática son aquellos que tienen normatividad específica para la protección de datos personales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley 1581 de Colombia, etc.

- En consecuencia con el anterior punto, la Circular Externa 002 de 2018 de la Superintendencia de Industria y Comercio - SIC[62], presenta un listado de países que cumplen con las regulaciones internacionales, y a donde se puede realizar transferencia de información sin inconvenientes: Albania, Alemania, Argentina, Austria, Bélgica, Bulgaria, Canadá, Chipre, Costa Rica, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estonia, España, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Lituania, Luxemburgo, Malta, México, Noruega, Nueva Zelanda, Países Bajos, Perú, Polonia, Portugal, Reino Unido, República Checa, República de Corea, Rumania, Serbia, Suecia, Suiza y Uruguay. Para los data-centers ubicados en países que no se encuentran identificados en la circular de la Superintendencia de Industria y Comercio, es válido que el Responsable del Tratamiento de la información (o sea quien decide sobre la información, en este caso el Cliente) evalúe si el país destino ofrece las condiciones necesarias para el tratamiento de datos personales, según lo descrito en el numeral 3.1 de la circular en mención[63]:

    - Legislación aplicable a la protección de datos personales.

[61] PRECIADO, Martha y VARGAS, Magna Luz. Guía de Contratación de Servicios en la Nube Para Empresas Públicas y Privadas en Colombia que Garantice un Correcto Análisis Forense Cuando se Presenten Incidentes se Seguridad. Trabajo de grado Especialización en Seguridad Informática. Bogotá: Universidad Piloto de Colombia, 2016., p. 34 – 37.

[62] COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Externa 002 de 2018. (23 de marzo de 2018). Por medio de la cual se modifica el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única. SIC. Bogotá, D.C., 2018. No. 50544. p. 3.

[63] Ibíd., p. 2.

- Aplicación de los principios básicos del tratamiento de datos: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulaci6n restringida, seguridad y confidencialidad.
- Delimitación de derechos de los Titulares de la información.
- Definición de Responsables y Encargados del tratamiento de la información.
- Existencia de herramientas legales para la protección de los derechos de los Titules, y para el cumplimiento de la ley.

- El cliente es dueño y responsable de los datos personales, y como tal debe cumplir la normativa de su país. Para el caso de la legislación colombiana, se debe actuar en conformidad a: Ley 1266 de 2008, Ley 1273 de 2009, Ley 1581 de 2012, y demás disposiciones complementarias.

5. COMPONENTES DE SEGURIDAD DE CLOUD COMPUTING

5.1.1 Esquema de Responsabilidad Compartida

En el documento de Arquitectura de Referencia de Cloud Computing de The Nist[64], se precisa como el CSP y el consumidor de la nube pueden tener distintos niveles de acceso y control sobre la infraestructura y datos asociados a un servicio de Cloud Computing. Contrario a los modelos de infraestructura 'On Premise' donde la organización tiene control total sobre la tecnología, la infraestructura, los datos, el recurso humano; en Cloud Computing el CSP y el consumidor del servicio diseñan, implementan, operan y monitorean la infraestructura Cloud Computing de manera colaborativa. De modo que ambas partes comparten la responsabilidad de proporcionar las medidas de seguridad a la infraestructura de Cloud Computing.

Amazon Web Services[65] delimita ese nivel de responsabilidad a las capas de la arquitectura en la cual interactúa cada actor:

- Responsabilidad del CSP con la seguridad en Cloud Computing: El CSP debe velar por la seguridad de la infraestructura física y lógica que ejecuta todos los servicios provistos. Tal infraestructura corresponde al hardware, el software, los elementos de redes y las instalaciones.

- Responsabilidad del cliente final con la seguridad en Cloud Computing: La responsabilidad del cliente está definida por los servicios contratados, ya que dependiendo de este se determina el alcance a nivel de configuración a cargo del cliente y con esto sus responsabilidades de seguridad informática. Por ejemplo, cuando se contrata un servicio IaaS (como una máquina virtual), el cliente puede realizar todas las tareas de administración y configuración de seguridad necesarias (actualizaciones de software, configuración de las reglas del firewall, etc.), o para un cliente que contrata un servicio SaaS (correo electrónico, por ejemplo) la responsabilidad recae en gestionar adecuadamente las políticas de autenticación de los usuarios finales de las cuentas de correo electrónico.

En la siguiente figura, se muestra la relación de los niveles de responsabilidad del Cliente y el CSP, y como varían entre un modelo de despliegue y otro:

---

[64] LIU, TONG, MAOBOHN, MESSINA, BADGER y LEAF, Op. cit., p. 16.

[65] AMAZON WEB SERVICES. Modelo de responsabilidad compartida. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/shared-responsibility-model/

Figura 2. Niveles de Responsabilidad del Cliente y el CSP

Fuente: El Autor

5.1.2 Infraestructura Física y de Seguridad de los Principales CSP

Un data-center corresponde a un ambiente acondicionado especialmente para alojar una serie de elementos de hardware y software, con el fin de almacenar datos y dar soporte al procesamiento de información. Puede corresponder a una pequeña infraestructura privada que soporta la operación de una empresa, o a una conexión de múltiples servidores y demás elementos debidamente organizados que proveen los servicios de nube publica a diversos clientes. Para el caso de un servicio de Cloud Computing, el data-center como mínimo debe tener las siguientes características:

- Redundancia energética, lo cual corresponde a tener múltiples fuentes energéticas que garanticen la constante operación del sistema y disponibilidad de la información.
- Implementación de medidas de seguridad adecuadas, para proteger los equipos de riesgos ambientales y acceso físico indebido.

- Planes de respaldo adecuados que permitan proteger los datos almacenados en los data-centers.

Las infraestructuras físicas de Google Cloud, Amazon Web Services y Microsoft Cloud cuentan las siguientes características generales:

5.1.2.1 Google Cloud Platform

Google es una de las marcas más representativas de la compañía norteamericana Alphabet Inc. Tal como lo describe Pedraza[66], lo que comienza en los años 90's como un motor de búsqueda en internet, evoluciona a la prestación de múltiples tipos de servicios en la nube, que van desde correo electrónico, mapas, video, hosting, hasta la consolidación de su propia plataforma de servicios en la nube: Google Cloud Platform en 2008.

La infraestructura física de Google Cloud Platform está compuesta por recursos físicos (servidores, discos duros, red privada, etc.) agrupados en los llamados 'centros de datos', que se encuentran ubicados a lo largo y ancho del planeta, organizados jerárquicamente en regiones y zonas. Para Google[67], una región es un área geográfica independiente que consta de zonas, mientras que una zona es el área de implementación, de comportamiento independiente en relación con las demás zonas. Actualmente, existen 20 regiones con 61 zonas, en territorio de más de 200 países o territorios. Las regiones y zonas se interconectan mediante una robusta red privada de fibra óptica.

Una característica especial de las zonas, en relación con la tolerancia a errores y la disponibilidad de este CSP, es que cada zona se considera como un dominio con fallos únicos dentro de la región. Esto quiere decir que la no disponibilidad de una zona no afecta a las demás zonas de la misma región, garantizando con esto que el cliente final tenga siempre acceso a sus datos. La siguiente figura muestra a grandes rasgos las regiones que componen la infraestructura física de Google Cloud Platform:

[66] PEDRAZA, Jacobo. Google no quiere que te hagas viejo [en línea]. En: El País. Bogotá, noviembre 15 de 2016. [Consultado el 20 de noviembre de 2019]. Disponible en: https://elpais.com/elpais/2016/11/14/talento_digital/1479123254_229531.html

[67] GOOGLE CLOUD. Geografía y regiones. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/docs/geography-and-regions?hl=es-419

Figura 3. Regiones Google Cloud Platform

Fuente: GOOGLE CLOUD. Ubicaciones GCP [imagen]. En: About Google Cloud. [Consultado: 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/about/locations/?hl=es#regions-tab

Google [68] describe el diseño de seguridad de su infraestructura de la siguiente manera:

A nivel de Hardware, los Centros de Datos son diseñados bajo modelos de seguridad por capas, que abarca desde el control de accesos a los alojamientos físicos de los data-centers, hasta la infraestructura del hardware usado en cada parte de la prestación de un servicio. Tales capas son las siguientes:

Seguridad Operacional: Abarca todos los aspectos físicos de la locación de los data-centers, y los elementos de hardware diseñados específicamente para Google. Google diseña y construye sus data-centers, y vela por la implementación de elementos de seguridad física (control de acceso estricto mediante uso de tecnología biométrica, detectores de metales, circuitos cerrados de televisión, etc.). A nivel de hardware, tanto las placas de servidor como el equipo de red, y los chips de seguridad están diseñados a medida de las necesidades de Google. Los chips de seguridad permiten identificar el hardware de Google.

Comunicación por Internet: Google implementa medidas para proteger las comunicaciones, tanto locales como entre zonas, regiones y con usuarios finales.

[68] GOOGLE CLOUD. Descripción general del diseño de seguridad de infraestructura de Google. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/infrastructure/design/

Google implementa redes privadas de fibra óptica, con elementos de seguridad y cifrado de comunicación avanzados (Cloud InterConnect y VPN administradas), con lo que se busca que los datos en tránsito permanezcan el menor tiempo posible en la Internet pública.

Servicios de Almacenamiento: Los servicios de almacenamiento se pueden configurar para usar claves de cifrado de datos antes de estos que lleguen al dispositivo de almacenamiento físico. Con esto se reducen posibles amenazas en los niveles más bajos de almacenamiento, como por ejemplo un disco duro infectado con algún software malicioso. Todos los dispositivos de almacenamiento se encuentran cifrados y la destrucción de los elementos que terminan su ciclo de vida se hace siguiendo protocolos estrictos, de modo que no se pueda recuperar el contenido (llegando a métodos físicos de eliminación, como trituración o magnetización por ejemplo). Todos los datos almacenados cuentan con backups encriptados y fragmentos en distintas zonas de una misma región, con lo que se garantiza la disponibilidad como la integridad de la información.

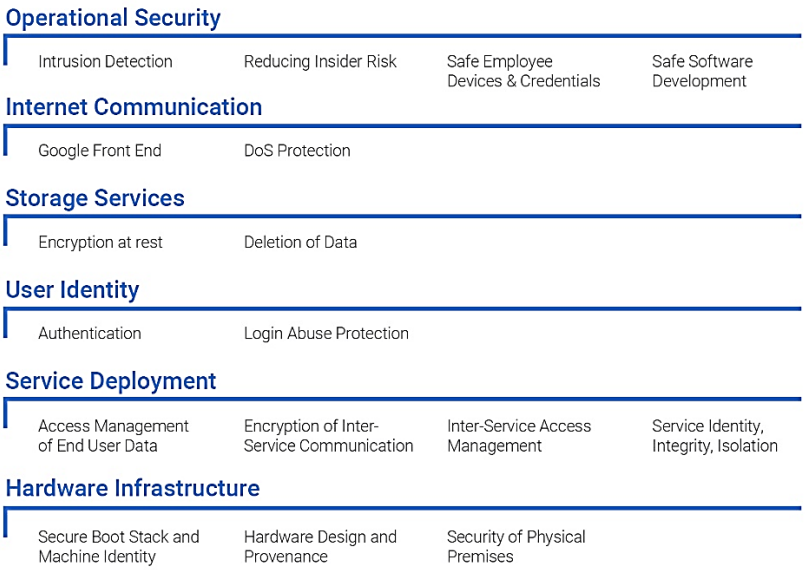
Identidad de Usuario: Esta capa de seguridad corresponde a los servicios de identidad central, e interactúa con los usuarios finales mediante las páginas de inicio de sesión. Adicional a nombre de usuario y contraseña, este servicio puede analizar patrones de inicio de sesión, como uso de un mismo dispositivo o una misma ubicación geográfica en varias ocasiones (con lo cual se identifican inicios de sesión sospechosos). Este servicio también permite la implementación de verificación en dos pasos, para asegurar el acceso a los servicios por parte del usuario final.

Despliegue de Servicios: Un servicio se puede desplegar en varias máquinas que ejecutan copias del mismo servicio, con lo que se logra manejar la carga de trabajo. Todos los servicios que se ejecutan son administrados por un servicio de orquestación de clúster llamado Borg, pero los servicios se mantienen aislados entre ellos, cuando se hace necesaria la comunicación entre servicios, se hace mediante autenticación criptográfica (implementación de tokens de seguridad, por ejemplo). También se implementan técnicas de aislamiento para proteger un servicio de otros servicios que se ejecutan en la misma máquina.

Infraestructura de Hardware: En los data-center se implementa hardware con firmas criptográficas en los elementos de bajo nivel como la BIOS, el gestor de arranque o el kernel de los sistemas operativos. Con esto se logra validar cada arranque o actualización de software. Se implementan chips de seguridad en cada dispositivo, y microcontroladores que ejecutan scripts de seguridad exclusivos de Google.

La siguiente figura resume cuáles son las capas de Seguridad de Infraestructura de Google Cloud:

Figura 4. Capas de Seguridad de Infraestructura de Google Cloud



Fuente: GOOGLE CLOUD. Descripción general del diseño de seguridad de infraestructura de Google [imagen]. En: Security Google Cloud. [Consultado: 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/infrastructure/design/

Adicional a las capas de seguridad que se implementan a nivel físico, existe monitoreo continuo de las actividades de los empleados con acceso a la infraestructura. El acceso de los funcionarios de Google a la información del usuario final se puede registrar sobre infraestructura de bajo nivel, en donde los datos están encriptados. También se implementan políticas y herramientas de detección de intrusiones, prevención de posibles incidentes, administración de vulnerabilidades, prevención de software malicioso, etc.

5.1.2.2 Amazon Web Services

Amazon Web Services es un grupo de productos de computación en la nube, de la compañía norteamericana Amazon.com, Inc. Amazon Web Services[69] surge en 2006 ofreciendo servicios de infraestructura de TI para empresas (bajo el modelo de infraestructura o plataforma como servicio), expandiéndose a lo largo de los años, hasta llegar a tener presencia comercial en 190 países.

[69] AMAZON WEB SERVICES. Acerca de AWS. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/about-aws/

La infraestructura física de Amazon Web Services está compuesta por recursos físicos (servidores, discos duros, red privada, etc.) agrupados en los llamados 'centros de datos', que se encuentran ubicados a lo largo y ancho del planeta, organizados jerárquicamente en regiones y zonas de disponibilidad. Para Amazon Web Services[70], una región es un espacio global extenso que consta de zonas de disponibilidad (generalmente tres zonas de disponibilidad por región), mientras que una zona de disponibilidad es una parte aislada de la infraestructura de Amazon Web Services, de comportamiento independiente en relación con las demás zonas y conformada por lo general por tres data-centers. Actualmente, existen 22 regiones geográficas con 69 zonas de disponibilidad implementadas por todo el mundo. Todas las zonas están interconectadas con redes de fibra óptica privada y totalmente redundante. Esta infraestructura es suficiente como para llevar a cabo la replicación sincrónica entre las zonas de disponibilidad, dando al cliente alta disponibilidad de sus datos. La siguiente figura muestra a grandes rasgos las regiones que componen la infraestructura física de Amazon Web Services:

Figura 5. Regiones Amazon Web Services

Fuente: AMAZON WEB SERVICES. Infraestructura global [imagen]. En: About AWS. [Consultado: 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/about-aws/global-infrastructure/

[70] AMAZON WEB SERVICES. AZ y regiones de infraestructuras globales. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/about-aws/global-infrastructure/regions_az/

Amazon Web Services[71] describe el diseño de seguridad de su infraestructura de la siguiente manera:

Los centros de datos de Amazon Web Services son diseñados y construidos por el mismo CSP, y son protegidos mediante la implementación de controles a distintos niveles:

Capa Perimetral: Corresponde a la seguridad física del centro de datos de Amazon Web Services, incluyendo el acceso físico y la ejecución de tareas sobre los servidores de manera remota. En cuanto al acceso por parte de los funcionarios, se implementan políticas de seguridad que limitan en gran medida el acceso físico a las instalaciones. El acceso físico es un proceso controlado mediante sistemas de autenticación multifactor y monitoreado mediante cámaras de seguridad. Adicional a las capas de seguridad que se implementan a nivel físico, existe monitoreo continuo de las actividades de los empleados con acceso a la infraestructura.

Capa de Infraestructura: Corresponde al edificio, hardware y equipamiento que conforman el centro de datos. Incluye los sistemas de suministro energético, sistemas de climatización y control de riesgos ambientales. Los suministros de electricidad, telecomunicaciones, el agua y la conectividad local se diseñan de manera redundante, con el fin de mantener el funcionamiento continuo en caso de emergencia. Esta capa también incluye toda la infraestructura tecnológica que soporta la operación de Amazon Web Services (servidores, dispositivos de almacenamiento, redes locales, infraestructura de respaldo.)

Capa de datos: Se implementan procedimientos para lograr la autorización para entrar a la capa de datos por parte de los funcionarios. De manera automática se implementan sistemas de detección de amenazas y de intrusiones electrónicas, las cuales generan alertas de amenazas o actividades sospechosas. Los dispositivos de almacenamiento se tipifican como críticos y tienen trato especial durante toda su vida útil. Existen procedimientos estrictos para dar de baja a alguno de estos dispositivos.

Capa Medioambiental: Corresponde a los mecanismos y estrategias implementadas para lograr data-centers sostenibles ambientalmente hablando. Tiene en cuenta los factores del entorno donde se ubican las instalaciones, para mitigar los riesgos medioambientales, como los desastres naturales y los incendios. Se implementan sensores y demás equipos que permitan proteger los datos. Así mismo, las zonas de disponibilidad se diseñan de modo tal que los centros de datos queden separados físicamente entre sí, pero conectados mediante redes privadas, con lo que se logra garantizar la disponibilidad de los datos. El diseño de los centros de

[71] AMAZON WEB SERVICES. Seguridad en la nube de AWS. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/security/

datos es sostenible, esto quiere decir que implementan fuentes de energías renovables (eólica y solar), estrategias de reducción de emisiones de carbono, etc.

A nivel general, en cuanto a la seguridad en la infraestructura, Amazon Web Services implementa firewalls de red integrados en las Nubes Privadas Virtuales (VPC) y las capacidades de firewall para las aplicaciones web existentes, lo que permite implementar redes privadas y controlar el acceso a la información. También implementa cifrado en tránsito con TLS controlado por el cliente en todos los servicios, permite establecer opciones de conectividad con lo que se pueden configurar conexiones privadas o exclusivas en un entorno local. Sobre la seguridad de la información, se implementa cifrado automático de la totalidad del tráfico en las redes regionales y entre los data-centers de Amazon Web Services. Este CSP implementa técnicas de cifrado en reposo, lo que adiciona una capa de seguridad a los datos almacenados en los data-centers, la gestión de dicho cifrado se administra mediante servicios de almacenamiento de claves criptográficas dedicado y basado en hardware llamado CloudHSM.

En relación con la autenticación de usuarios, Amazon Web Services tiene múltiples herramientas para la administración del acceso a la infraestructura en la nube información, como por ejemplo: AWS Identity and Access Management (IAM) (define cuentas de usuario individuales y niveles de acceso) o AWS Multi-Factor Authentication (incluye opciones para autenticación basados en hardware).

5.1.2.3 Microsoft Azure

Microsoft Azure es un grupo de productos de computación en la nube especializados en servicios de Infraestructura o Plataforma, propiedad de Microsoft Corporation. Microsoft Azure[72] surge en 2010, bajo el concepto plataforma de Cloud Computing diseñada para crear, desarrollar y administrar aplicaciones, software y servicios haciendo uso de los data-centers de Microsoft.

La infraestructura física de Microsoft Azure está compuesta por recursos físicos (servidores, discos duros, red privada, etc.) agrupados en los llamados 'centros de datos', que se encuentran ubicados a lo largo y ancho del planeta, organizados jerárquicamente en regiones y zonas de disponibilidad. Para Microsoft Azure[73] una región es un conjunto de centros de datos dentro de un perímetro geográfico delimitado por las fronteras nacionales, mientras que una zona de disponibilidad es una ubicación separada físicamente dentro de una región y está compuesta por varios data-centers. Actualmente, existen 54 regiones geográficas a lo largo de 140

[72] MICROSOFT CLOUD. Introducción a la informática en la nube. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/overview/

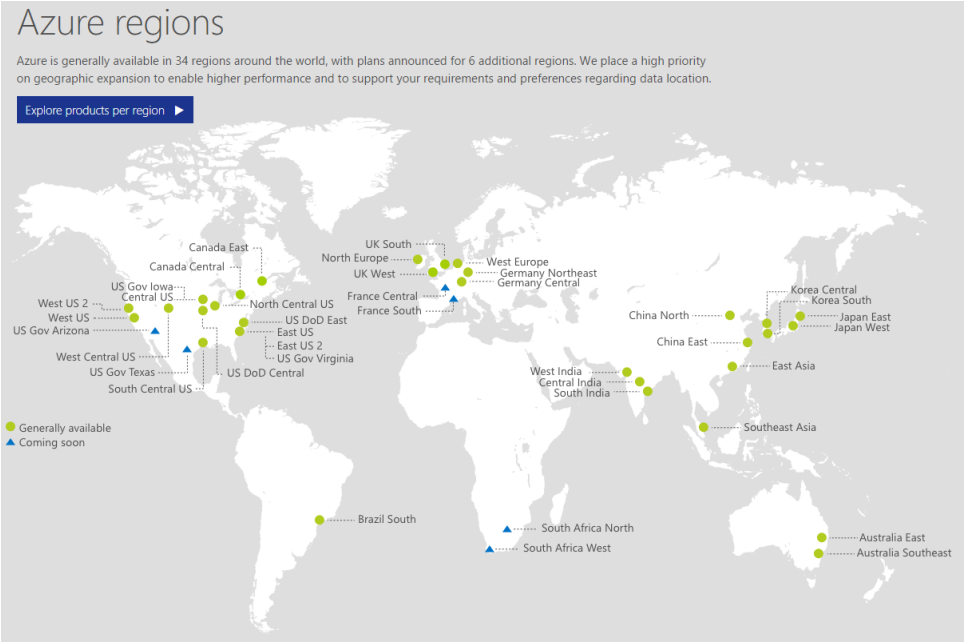
[73] MICROSOFT CLOUD. Regiones de Azure. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/global-infrastructure/regions/

países. Todas las zonas de disponibilidad están interconectadas con redes de fibra óptica privada y totalmente redundante. Esta infraestructura es suficiente como para llevar a cabo la replicación de información entre las zonas de disponibilidad, dando al cliente alta disponibilidad de sus datos.

En relación con las zonas de disponibilidad, cada una de ellas consta de uno o varios centros de datos equipados, suministro energético y de comunicaciones independiente. La separación física de las regiones y zonas de disponibilidad es la estrategia de Microsoft Azure para proteger los datos mediante la redundancia y backups encriptados.

La siguiente figura muestra de manera general las regiones que componen la infraestructura física de Microsoft Azure:

Figura 6. Regiones de Microsoft Azure



Fuente: MICROSOFT CLOUD. Microsoft Azure: Services availability by region [imagen]. En: Microsoft Azure. [Consultado: 20 de noviembre de 2019]. Disponible en: https://blogs.msdn.microsoft.com/kaushal/2014/06/06/microsoft-azure-services-availability-by-region/

Microsoft Azure[74] describe el diseño de seguridad de su infraestructura de la siguiente manera:

Los servicios suministrados por Microsoft Azure se basan en el modelo de Seguridad de Confianza Cero, en donde se debe verificar explícitamente la identidad del usuario que accede a un producto, igual que su ubicación, el dispositivo, el servicio a usar, la clasificación de datos y las anomalías. Al igual, se debe velar por que el usuario tenga el acceso menos privilegiado a los datos o herramientas, en donde se concede acceso solo a los datos que necesita y durante el tiempo suficiente. Adicional, todas las comunicaciones están encriptadas de extremo a extremo por defecto.

La identificación de nuevas amenazas se realiza por medio de servicios que utilizan inteligencia de seguridad en la red que funciona en tiempo real sobre toda la infraestructura. Esta inteligencia artificial se alimenta del comportamiento de páginas web, correos, uso de dispositivos y demás y es analizada en Microsoft Intelligent Security Graph. Permite que Azure pueda reaccionar oportunamente a comportamientos atípicos.

5.1.3 Cumplimiento Normas Internacionales de los Principales CSP

El cumplimiento de los estándares, normas y metodologías de aceptación internacional, espacialmente sobre Seguridad Informática, por parte de los CSP, son un instrumento clave para generar confianza por parte del consumidor final de los servicios. La siguiente tabla contiene algunas normas y estándares asociados con Seguridad Informática que cobijan las operaciones de los tres principales proveedores de servicios de Cloud Computing con presencia en Colombia, Google Cloud, Amazon Web Services y Microsoft Cloud:

[74] MICROSOFT CLOUD. Refuerce su seguridad con Azure. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/overview/security/

Tabla 1. Cumplimiento Normas Internacionales de los Principales CSP

Norma o Estándar	Google Cloud Platform	Amazon Web Services	Microsoft Azure
ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems – Requirements	Cuenta con Certificación[75], el documento actualizado aparece público en la página web, vigente hasta 13 de abril de 2021	Cuenta con Certificación[76], el documento actualizado aparece público en la página web, vigente hasta 7 de noviembre de 2022	Cuenta con Certificación[77], el documento actualizado aparece público en la página web, vigente hasta 19 de junio de 2020
ISO/IEC 27017:2015 Information Technology - Security Techniques - Code Of Practice For Information Security Controls Based On ISO/IEC 27002 For Cloud Services	Cuenta con Certificación[78], el documento actualizado aparece público en la página web, vigente hasta 13 de abril de 2021	Cuenta con Certificación[79], el documento actualizado aparece público en la página web, vigente hasta 7 de noviembre de 2022	Cuenta con Certificación[80], el documento actualizado aparece público en la página web, vigente hasta 10 de agosto de 2021
ISO/IEC 27018:2019	Cuenta con Certificación[81], el	Cuenta con Certificación[82], el	Cuenta con Certificación[83], el

[75] GOOGLE CLOUD. ISO 27001. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://cloud.google.com/security/compliance/iso-27001/

[76] AMAZON WEB SERVICES. ISO/IEC 27001:2013. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/iso-27001-faqs/

[77] MICROSOFT CLOUD. Microsoft and ISO/IEC 27001. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001

[78] GOOGLE CLOUD. ISO 27017. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://cloud.google.com/security/compliance/iso-27017/

[79] AMAZON WEB SERVICES. Conformidad con ISO/IEC 27017:2015[en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/iso-27017-faqs/

[80] MICROSOFT CLOUD. Microsoft y la norma ISO/IEC 27017. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://www.microsoft.com/es-xl/TrustCenter/Compliance/ISO-IEC-27017

[81] GOOGLE CLOUD. ISO 27018. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://cloud.google.com/security/compliance/iso-27018/

[82] AMAZON WEB SERVICES. Conformidad con ISO/IEC 27018:2014[en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/iso-27018-faqs/

[83] MICROSOFT CLOUD. Microsoft y la norma ISO/IEC 27018. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://www.microsoft.com/es-xl/TrustCenter/Compliance/ISO-IEC-27018

Norma o Estándar	Google Cloud Platform	Amazon Web Services	Microsoft Azure
Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	documento actualizado aparece público en la página web, vigente hasta 13 de abril de 2021	documento actualizado aparece público en la página web, vigente hasta 7 de noviembre de 2022	documento actualizado aparece público en la página web, vigente hasta 19 de junio de 2020
Reglamento General de Protección de Datos – RGPD	Cumple los requisitos[84], tiene publica la documentación	Cumple los requisitos[85], tiene publica la documentación	Cumple los requisitos[86], tiene publica la documentación
SOC 1 - SOC for Service Organizations: ICFR	Implementa el informe[87], solo está disponible para clientes, mediante acuerdo de confidencialidad	Implementa el informe[88], solo está disponible para clientes, mediante el producto AWS Artifact	Implementa el informe[89], solo está disponible para clientes, mediante acuerdo de confidencialidad

[84] GOOGLE CLOUD. Google Cloud y el Reglamento General de Protección de Datos. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/gdpr/?hl=es

[85] AMAZON WEB SERVICES. Reglamento General de Protección de Datos (RGPD). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/gdpr-center/

[86] MICROSOFT CLOUD. Protege la privacidad individual con Microsoft Cloud. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://www.microsoft.com/es-es/trust-center/privacy/gdpr-overview

[87] GOOGLE CLOUD. SOC 1. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/compliance/soc-1/

[88] AMAZON WEB SERVICES. SOC. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/soc-faqs/

[89] MICROSOFT CLOUD. Oferta de cumplimiento: controles de organización de servicios (SOC). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc

Norma o Estándar	Google Cloud Platform	Amazon Web Services	Microsoft Azure
SOC 2 - SOC for Service Organizations: Trust Services Criteria	Implementa el informe[90], solo está disponible para clientes, mediante acuerdo de confidencialidad	Implementa el informe[91], solo está disponible para clientes, mediante el producto AWS Artifact	Implementa el informe[92], solo está disponible para clientes, mediante acuerdo de confidencialidad
SOC 3 - SOC for Service Organizations: Trust Services Criteria for General Use Report	Implementa el informe[93], aparece público en la página web	Implementa el informe[94], aparece público en la página web	Implementa el informe[95], aparece público en la página web
PCI DSS	Cuenta con Certificación[96], solo está disponible para clientes, mediante acuerdo de confidencialidad	Cuenta con Certificación[97], solo está disponible para clientes, mediante el producto AWS Artifact	Cuenta con Certificación[98], solo está disponible para clientes, mediante acuerdo de confidencialidad

[90] GOOGLE CLOUD. SOC 2. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/compliance/soc-2/

[91] AMAZON WEB SERVICES. SOC. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/soc-faqs/

[92] MICROSOFT CLOUD. Oferta de cumplimiento: controles de organización de servicios (SOC). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc

[93] GOOGLE CLOUD. SOC 3. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/compliance/soc-3/

[94] AMAZON WEB SERVICES. SOC. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/soc-faqs/

[95] MICROSOFT CLOUD. Oferta de cumplimiento: controles de organización de servicios (SOC). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-soc

[96] GOOGLE CLOUD. PCI DSS. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/compliance/pci-dss/

[97] AMAZON WEB SERVICES. PCI DSS. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/pci-dss-level-1-faqs/

[98] MICROSOFT CLOUD. Oferta de cumplimiento: Estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-pci-dss

Norma o Estándar	Google Cloud Platform	Amazon Web Services	Microsoft Azure
CSA STAR	Cuenta con Certificación[99], solo está disponible para clientes, mediante acuerdo de confidencialidad	Cuenta con Certificación[100], solo está disponible para clientes, mediante el producto AWS Artifact	Cuenta con certificación[101], solo está disponible para clientes, mediante acuerdo de confidencialidad
ISO/IEC 20000-1:2011 Information technology - Service management - Part 1: Service management system requirements	No informado	No informado	Cuenta con Certificación[102], el documento actualizado aparece público en la página web, vigente hasta 19 de agosto de 2021
ISO/IEC 22301:2012 Societal security - Business continuity management systems - Requirements	No informado	No informado	Cuenta con Certificación[103], el documento actualizado aparece público en la página web, vigente hasta 15 de septiembre de 2022

[99] GOOGLE CLOUD. CSA STAR. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/compliance/csa-star/

[100] AMAZON WEB SERVICES. Cloud Security Alliance (CSA). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/csa/

[101] MICROSOFT CLOUD. Compliance offering: Cloud Security Alliance (CSA) STAR certification. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-csa-star-certification

[102] MICROSOFT CLOUD. Compliance offering: ISO/IEC 20000-1:2011 Information Technology Service Management. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en : https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-20000-1-2011

[103] MICROSOFT CLOUD. Compliance offering: ISO 22301:2012 Business Continuity Management Standard [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-iso-22301

Norma o Estándar	Google Cloud Platform	Amazon Web Services	Microsoft Azure
FedRAMP	Cumple con los requerimientos[104], la documentación está disponible para las Entidades Públicas de Estados Unidos y contratistas	Cumple con los requisitos[105], la documentación técnica solo está disponible para clientes, mediante el producto AWS Artifact	Cumple con los requisitos[106], hay documentación disponible

Fuente: El autor

5.1.4 Aspectos de Seguridad Abordados por los Principales CSP

Una infraestructura basada en Cloud Computing debe tener en cuenta requisitos de seguridad mínimos en aspectos como autenticación, confidencialidad, integridad, auditoría o disponibilidad, para generar confianza entre sus clientes finales. A continuación, se analiza cómo pueden ser abordados algunos de estos aspectos de seguridad con las herramientas y productos de los tres CSP con presencia en Colombia mencionados en el apartado anterior:

Tabla 2. Aspectos de Seguridad Abordados por los Principales CSP

Aspecto	Google Cloud Platform	Amazon Web Services	Microsoft Azure
Autenticación, o demostrar que el usuario es quien dice ser	Implementa verificación en dos pasos para acceder a cualquier producto[107]. Combina el uso de la	Implementa verificación en dos pasos para acceder a	Implementa Azure Multi-Factor Authentication[109]. Combina el uso de la contraseña

[104] GOOGLE CLOUD. FedRAMP. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security/compliance/fedramp/

[105] AMAZON WEB SERVICES. FedRAMP. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/compliance/fedramp/

[106] MICROSOFT CLOUD. Oferta de cumplimiento: Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-fedramp

[107] GOOGLE CLOUD. Verificación en dos pasos. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://www.google.com/intl/es-419/landing/2step/#tab=why-you-need-it

[109] MICROSOFT CLOUD. La experiencia de inicio de sesión con Azure Multi-Factor Authentication [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-mfa-mfasettings

Aspecto	Google Cloud Platform	Amazon Web Services	Microsoft Azure
	contraseña tradicional, con mensaje de texto, llamada de voz, notificación de una aplicación, o llave física.	cualquier producto[108]. Combina el uso de la contraseña tradicional, con mensaje de texto, llamada de voz o notificación de una aplicación.	tradicional, con mensaje de texto, llamada de voz o notificación de una aplicación.
Administración y control de acceso al Sistema	Implementa Gestión de Identidades y Accesos de Cloud (Cloud IAM)[110]. Permite gestionar los permisos y roles de los usuarios y grupos sobre los recursos.	Implementa AWS Identity and Access Management (IAM)[111]. Permite gestionar los permisos y roles de los usuarios y grupos sobre los recursos.	Implementa Administración de identidad y acceso (IAM)[112]. Permite gestionar los permisos y roles de los usuarios y grupos sobre los recursos.
Prevención de perdida de datos, o asegurar la protección y monitoreo de los datos que se intercambian	Implementa Cloud Data Loss Prevention (Cloud DLP)[113], permite inspeccionar y tipificar la información, de modo que se puede encriptar por defecto los datos tipo 'sensibles'	Implementa varias herramientas:[114] DLP de Symantec, McAfee Total Protection para DLP, que se pueden usar tanto en instancias como en aplicaciones o servicios en la nube.	Implementa Azure Information Protection[115], clasifica y protege los datos según su nivel de confidencialidad. Automatiza el proceso según reglas definidas.

[108] AMAZON WEB SERVICES. Activar la Verificación en dos pasos. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://www.amazon.es/gp/help/customer/display.html?nodeId=202073820

[110] GOOGLE CLOUD. Gestión de Identidades y Accesos de Cloud. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/iam/?hl=es

[111] AMAZON WEB SERVICES. AWS Identity and Access Management (IAM). [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/iam/

[112] MICROSOFT CLOUD. Administración de identidad y acceso (IAM). [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://azure.microsoft.com/es-es/product-categories/identity/

[113] GOOGLE CLOUD. DLP. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/dlp/docs/?hl=es

[114] AMAZON WEB SERVICES. Prevención de pérdida de datos de AWS: herramientas y estrategias. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.netapp.com/blog/aws-data-loss-prevention-tools-and-strategies

[115] MICROSOFT CLOUD. Azure Information Protection. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/services/information-protection/

Aspecto	Google Cloud Platform	Amazon Web Services	Microsoft Azure
Seguridad Web o protección de tráfico y aplicaciones web	Implementa Cloud Security Scanner[116], que identifica vulnerabilidades de las aplicaciones web.	Implementa AWS WAF[117], un firewall para aplicaciones web, protegen contra ataques que puedan afectar la disponibilidad del servicio	Implementa Azure Web Application Firewall (WAF)[118], un firewall para aplicaciones web, evitan ataques que puedan afectar la disponibilidad del servicio
Continuidad del negocio o procesos que garantizan la capacidad de recuperación ante un evento	Cloud Storage (almacenamiento en la nube) permite crear tareas programadas de copia de seguridad, desde consola con el comando gsutil[119]	Implementa herramientas para la recuperación de desastres, como CloudEndure Disaster Recovery[120], útil tanto en entornos virtuales o físicos, independiente del sistema operativo o aplicación alojada en la instancia.	Azure SQL Database permite recuperación automática ante errores, mediante copias de seguridad incluso cada 5 minutos, tablas temporales que permiten reversar cambios, múltiple replicación geográfica, etc.[121]
Servicios de encriptación o protección de datos o	Implementa Cloud Key Management Service[122], es un servicio de	Implementa AWS Key Management Service[123], permite administrar y crear	Implementa Azure Key Vault[124], permite administrar las claves criptográficas a usar

[116] GOOGLE CLOUD. Cloud Security Scanner. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security-scanner/docs/

[117] AMAZON WEB SERVICES. AWS WAF. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/products/security/#AWS_WAF

[118] MICROSOFT CLOUD. Azure Web Application Firewall (WAF). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/blog/azure-web-application-firewall-waf-generally-available/

[119] GOOGLE CLOUD. Situaciones de recuperación ante desastres para datos. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/solutions/dr-scenarios-for-data?hl=es-419

[120] AMAZON WEB SERVICES. Recuperación de desastres. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/disaster-recovery/

[121] MICROSOFT CLOUD. Introducción a la continuidad empresarial con Azure SQL Database. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://docs.microsoft.com/es-es/azure/sql-database/sql-database-business-continuity

[122] GOOGLE CLOUD. Gestión de claves criptográficas. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/kms/?hl=es

[123] AMAZON WEB SERVICES. AWS Key Management Service (KMS). [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/kms/

[124] MICROSOFT CLOUD. Key Vault. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/services/key-vault/

Aspecto	Google Cloud Platform	Amazon Web Services	Microsoft Azure
aplicaciones mediante cifrado	administración de claves criptográficas, permite generar, usar, rotar y eliminar claves.	claves criptográficas para los distintos servicios de AWS	en las demás aplicaciones
Monitoreo y administración de los eventos de seguridad	Implementa Cloud Security Command Center[125]. Evalúa el estado general de seguridad y actividad de las instancias, redes virtuales y unidades de almacenamiento	Implementa Amazon CloudWatch[126], que monitorea el estado general del sistema, genera alertas ante comportamientos atípicos	Implementa Azure Monitor[127], muestra alertas a las anormalidades en la operación a nivel de aplicaciones o red

Fuente: El autor

[125] GOOGLE CLOUD. Cloud Security Command Center. [en línea]. (s.f). [citado en 20 de noviembre de 2019]. Disponible en: https://cloud.google.com/security-command-center/?hl=es

[126] AMAZON WEB SERVICES. Amazon CloudWatch. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://aws.amazon.com/es/cloudwatch/

[127] MICROSOFT CLOUD. Azure Monitor. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es/services/monitor/

6. CLOUD COMPUTING EN PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS

6.1.1 Colombia Frente al Índice de Conectividad Global

El Índice de Conectividad Global o CGI[128], es una clasificación de referencia que evalúa a 79 países en relación con su desempeño en 40 indicadores que rastrean el impacto de las Tecnologías de la Información y la Comunicación en la economía nacional, la competitividad y el crecimiento. Esos 40 indicadores están construidos para evaluar a los habilitadores tecnológicos claves que conforman los pilares de la economía digital: Banda Ancha, Computación en la Nube, Centros de Datos e Internet de las Cosas. Dicha medición es liderada por países como Estados Unidos, Singapur y Suecia. Los cuatro pilares del índice GCI son: Oferta, Demanda, Experiencia y Potencial. Estos pilares miden:

- Oferta: Niveles actuales de suministro e inversión en productos y servicios.
- Demanda: Indica la necesidad de los productos y servicios por parte de los consumidores.
- Experiencia: Mide las variables necesarias para determinar la experiencia de los usuarios finales en los productos o servicios.
- Potencial: Muestra los indicadores a futuro del desarrollo de los productos o servicios.

Colombia, para la medición del 2019, ocupó el puesto 55 con una puntuación de 41 sobre 120 unidades posibles (mostrando un aumento de 1 punto en relación con la medición de 2018, y de 2 puntos en relación con la medición de 2017). El informe evidencia que Colombia está experimentando un auge en el uso de la nube, con una puntuación de 48 de 120 sobre este habilitador tecnológico, cifra cercana al promedio general de la medición que es 51, lo cual indica que el país es competitivo en cuanto a la oferta y la demanda de Cloud Computing en relación con los demás países medidos. Los puntajes en los otros habilitadores tecnológicos fueron: Banda Ancha 42, Centros de Datos 21, e Internet de las Cosas 33 (siendo la mejor puntuación la obtenida en Computación en la Nube, con 48 puntos).

La siguiente tabla muestra la puntuación y análisis de los Indicadores relacionados con Computación en la Nube:

[128] HUAWEI. Índice de Conectividad Global 2019. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://www.huawei.com/minisite/gci/en/

Tabla 3. Análisis del Puntaje de Colombia en el Índice de Conectividad Global sobre Cloud Computing

Indicador	Puntaje	Observaciones a la Puntuación
Oferta (Inversión en la Nube)	3 / 10	Se ha generado oferta en productos relacionados con infraestructura como servicio, procesamiento de datos y almacenamiento en la nube pública.
Demanda (Migración a la Nube)	4 / 10	La calificación está dada por el porcentaje de proyectos de software que han migrado de infraestructura tradicional a implementaciones en la nube.
Experiencia (Experiencia en la Nube)	4 / 10	Corresponde a la medición de la calidad del servicio percibida por los usuarios de internet. La calidad del servicio de internet se relaciona con la generación de nuevas oportunidades para Cloud Computing.
Potencial (Potencial de la Nube)	5 / 10	El dato se deriva de datos de encuestas sobre el potencial para el desarrollo del mercado y los beneficios económicos por la adopción de Cloud Computing

Fuente: HUAWEI. Índice de Conectividad Global 2019. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://www.huawei.com/minisite/gci/en/

6.1.2 Cloud Computing Como Servicio Exento de IVA en Colombia

Un aspecto importante a tener en cuenta sobre la penetración y fomento de Cloud Computing como nueva tecnología de la información y la comunicación en Colombia por parte del Estado, es que en la Ley 1943 de 2018 o Ley de Financiamiento[129], se incluye la Computación en la Nube dentro de los "Servicios excluidos del Impuesto a las Ventas (IVA)", siempre y cuando el modelo de servicio a implementar cumpla con las definiciones estipuladas en el Concepto 017056 de 2017[130] de la DIAN - Dirección de Impuestos y Aduanas Nacionales:

[129] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1943. (28 de diciembre de 2018). Por la cual se expiden normas de financiamiento para el restablecimiento del equilibrio del presupuesto general y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2018. No. 50820. p. 7.

[130] COLOMBIA. DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES. Concepto 017056 de 2017. (25 de agosto de 2017). Concepto Unificado Del Numeral 24 Del Artículo 187 De La Ley 1819 De 2016. Bogotá, D.C., 2017. No. 017056.

- El servicio debe cumplir las siguientes características: autoservicio bajo demanda, acceso amplio a la red, asignación común de recursos, rápida elasticidad y servicio medible

- El servicio se debe poder clasificar dentro de alguno de los Modelos Servicio de Computación en la Nube: Software como servicio (SaaS), Plataforma como Servicio (PaaS) o Infraestructura como Servicio (IaaS)

- El servicio se debe poder clasificar dentro de alguno de los Modelos Despliegue de Computación en la Nube: Nube Privada, Nube Comunitaria, Nube Pública o Nube Híbrida

6.1.3 Aspectos Generales de la Adaptación a Cloud Computing

En cuanto a la adaptación de Cloud Computing, tal como lo describe The Nist[131], la implementación de este modelo tecnológico dentro de un entorno empresarial se debe traducir en reducción de costos en infraestructura tecnológica y actualizaciones de software más rápidas. Pero dicha adopción debe ir ligada a la forma en cómo la nube puede responder a las preocupaciones de los usuarios sobre seguridad, integración e interoperabilidad. En cuanto a la interoperabilidad e integración, se espera que Cloud Computing esté en la capacidad de integrarse fácilmente a sistemas heredados, a servicios locales y a servicios en otras nubes, con el fin de disponibilizar los datos y dar continuidad al servicio. Esto quiere decir que un CSP debe proporcionar mecanismos para que los usuarios finales del servicio puedan copiar objetos desde y hacia la nube, o mecanismos para para usar sus datos y servicios desde y hacia distintos sistemas mediante interfaces basadas en estándares de común aceptación que faciliten la comunicación.

En cuanto a la seguridad, The Nist afirma que es un aspecto transversal de la infraestructura de Cloud Computing que afecta todos los elementos de la arquitectura, desde la seguridad física provista por el CSP, hasta la seguridad de la aplicación y de los datos, en donde intervienen tanto el CSP como el consumidor final del servicio. Por lo tanto, la seguridad de toda la infraestructura de Cloud Computing no es únicamente responsabilidad del CSP, sino también de los consumidores finales y otros actores relevantes. Una infraestructura basada en Cloud Computing debe tener en cuenta requisitos de seguridad mínimos en aspectos como autenticación, autorización, disponibilidad, confidencialidad, gestión de identidad, integridad, auditoría, monitoreo de seguridad, respuesta a incidentes y gestión de políticas de seguridad.

[131] LIU, TONG, MAOBOHN, MESSINA, BADGER y LEAF, Op. cit., p. 15.

Los data-centers propiedad de los CSP, que sustentan la operación de un servicio de Cloud Computing, son compartidos por varios clientes, y esto genera la percepción de que una falencia en los niveles de seguridad se puede convertir en accesos no autorizados a datos confidenciales, sin embargo, se debe tener en cuenta que los esquemas de Cloud Computing cuentan con los mecanismos necesarios que garantizan un ambiente seguro entre usuarios (procesos avanzados de autenticación y control de accesos, encriptación en varios niveles, etc.). Una vez más, es importante resaltar que el modelo de seguridad de Cloud Computing es de 'Responsabilidad Compartida', de modo que mientras que el usuario tenga una buena definición de la política de identidad y control de acceso basada en mínimos privilegios, y que el proveedor garantice las herramientas y condiciones de seguridad física requeridas; el uso de una infraestructura Cloud Computing resultante contará con los niveles de seguridad adecuados.

También es importante tener en cuenta que no es necesario migrar de inmediato ni en la totalidad los servicios de información que soportan las operaciones de una empresa. Es importante iniciar los procesos de migración a la nueva tecnología a partir del análisis de casos de éxito de otras empresas que ya tengan avances en Cloud Computing, con lo cual se logra prever el resultado de la implementación, así mismo, la adopción de Cloud Computing se debe hacer de manera gradual, e iniciando con procesos no críticos para la operación. Este abordaje permite que se mitiguen los riesgos propios de los cambios de tecnología, como resultados no esperados o variables no tomadas en cuenta en el plan inicial.

En cuanto a la protección de datos personales, en el proceso de contratación se debe especificar cuál es la jurisdicción legal que aplica al contrato, y así debe ser para evitar ambigüedades, teniendo en cuenta que el CSP puede ser de una nacionalidad, el cliente de otra, y los data-centers pueden estar en un tercer país. Para el almacenamiento de información fuera de Colombia, se debe tener en cuenta que la Ley 1581 de 2012 restringe la transferencia de información a países en donde la normatividad no garantice los niveles adecuados de seguridad informática. Se considera que los países que cuentan con niveles adecuados de seguridad informática son aquellos que tienen normatividad específica para la protección de datos personales, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley 1581 de Colombia, etc. Independiente del país en donde se almacene, los derechos de propiedad de la información y responsabilidad sobre esta, siempre recae en el propietario de la información.

Desde el punto de vista de la inversión financiera necesaria para la puesta en marcha de una infraestructura tecnológica que sustente la operación de una empresa, Fernández resalta que:

> Frecuentemente, cuando se presenta el tema de la computación en la nube a las empresas, se recurre a la metáfora de la generación de electricidad para resaltar las ventajas de un servicio público que se paga de acuerdo con su uso, con la modalidad

de suscripción, en contraste con la generación propia de electricidad, que exige grandes inversiones en equipos y personal especializado, antes de que se impusiera el concepto de un único proveedor.[132]

6.1.4 Beneficios de Cloud Computing

En relación con los beneficios para el usuario final, por la implementación de modelos de Servicios en la Nube, Moreno[133] describe los siguientes:

- Para el usuario final es transparente todo lo relacionado con actualización de versiones de software, así como la escalabilidad o aumento de capacidad de procesamiento de la infraestructura contratada.
- El CSP es responsable de sus data-centers, así como de garantizar la custodia y copias de seguridad de los datos almacenados y medidas de seguridad informática a nivel de infraestructura.
- El usuario final puede acceder a toda la infraestructura contratada, desde cualquier conexión a internet. Puede contar con una muy variada gama de servicios, como correo electrónico, almacenamiento, software, etc. La ejecución de los procesos se caracteriza por la velocidad, la escalabilidad y la simpleza, garantizando una experiencia de usuario gratificante.
- Desaparece el riesgo de perder competitividad por obsolescencia tecnológica para el tratamiento de información, ya que el CSP pondrá a disposición las actualizaciones de software necesarias y de manera oportuna.
- El pago por el uso de la infraestructura es bajo, ya que solo se factura por el uso real dado.
- La empresa cliente no incurre en gastos por adecuación física y administración de servidores de aplicaciones y demás, ni se expone a riesgos físicos o ambientales asociados a la tenencia de data-centers. Tampoco es necesario tener personal informático dedicado al soporte técnico de esa infraestructura, las funciones del proceso de T.I. de la organización se centrarían en garantizar el acceso seguro a internet y el correcto funcionamiento de los dispositivos y equipos de cómputo.

Bruno[134] en su documento 'Cloud Computing en la Industria Financiera', afirma desde una perspectiva global, que las entidades financieras que adoptan este tipo

[132] FERNÁNDEZ, Op. cit., p. 42.
[133] MORENO, Mario. Computación En La Nube. En: Documentos de Trabajo. No 566., Junio, 2015., p. 11 - 13.
[134] BRUNO, Op. cit., p. 69-82.

de infraestructura, aparte de reducir costos en el área de infraestructura tecnológica, pueden enfocar sus actividades en mejorar su operación, generando una ventaja competitiva que acelera el aumento de rentabilidad. Este autor enumera estos otros beneficios del Cloud Computing:

- La existencia de estos diferentes modelos de Cloud Computing (SaaS, PaaS, IaaS) permite que la transición hacia este tipo de infraestructura pueda ser gradual (e incluso mantenerse hibrida, migrando unos servicios a la nube, y manteniendo otros en la infraestructura tradicional, según las necesidades de la organización).

- Existe claridad para establecer mediciones de costos por el uso de la infraestructura, ya que se pueden implementar fácilmente métricas por cada software o servicio en uso.

- Se pueden reducir los gastos de infraestructura mediante el uso transversal y transparente de los recursos a través de distintas áreas de negocios.

- Cloud Computing permite mayor flexibilidad, agilidad y capacidad de escalar las incidencias, para dar pronta solución a los requerimientos operacionales.

- Mayor productividad para los usuarios finales de la información, ya que el uso de aplicaciones en tiempo real permite obtener la información necesaria al instante.

- La reducción de la infraestructura física 'On Premise' apunta al mejor aprovechamiento de los recursos energéticos y a reducción de la generación de desperdicios tecnológicos propios, lo que se traduce en que Cloud Computing apunta a ser una tecnología ambientalmente amigable.

- Las condiciones contractuales entre el CSP y la empresa usuaria denotan gran importancia al cumplimiento de los Acuerdos de Nivel de Servicio (disponibilidad del servicio de mesa de ayuda, tiempo de respuesta, capacidad de los recursos, etc.), con lo que se busca que exista mínima afectación en la operación del usuario si se llega a presentar alguna novedad en el servicio de Cloud Computing.

Gutiérrez y Korn[135] describen otros beneficios en cuanto a la implementación de Cloud Computing desde enfoques sociales:

- Creación de empleos e innovación, esto ya que, al reducir los costos del mantenimiento de la infraestructura tecnológica, las empresas pueden ampliar el presupuesto para temas de desarrollo, innovación, nuevos

[135] GUTIÉRREZ, y KORN, Op. cit., p. 85-118.

productos y mercados, factores importantes para la generación de empleo, especialmente en el sector de tecnología.

- El punto anterior va de la mano con la masificación del Teletrabajo, ya que permite que los funcionarios de las empresas puedan acceder a todas las herramientas de trabajo desde cualquier computador y conexión a internet.

- La computación en la nube es un medio de inclusión social, ya permite que las pequeñas empresas tengan acceso a herramientas de procesamiento de datos avanzadas, a costos accesibles. Estas herramientas también permiten el acceso a tecnologías de punta en temas de salud o educación en comunidades rurales o de bajos ingresos.

- Cloud Computing es una herramienta que les permite a las organizaciones adaptarse a los nuevos desafíos del mercado con mayor agilidad, otorgando rapidez en el despliegue de nuevas aplicaciones y servicios con menor riesgo e inversiones de capital, ayudando así a que pequeñas organizaciones puedan competir con productos de calidad y flexibles a la demanda.

- Cloud Computing es un medio para democratizar la seguridad en la infraestructura tecnológica. Esto es posible cuando el CSP confiere las mismas estrategias y herramientas de seguridad informática a toda la infraestructura de sus data-centers, protegiendo tanto a grandes como a pequeños clientes. Esto beneficia a la pequeña y mediana empresa, que en un contexto de infraestructura 'On Premise' no tendría los recursos necesarios para implementar controles de seguridad informática robustos o actualizar los que tiene implementados todas las veces que sea necesario.

En cuanto a la Gestión del Riesgo, la Guía de Computación en la Nube[136] señala los siguientes beneficios:

- Rápida recuperación ante desastres y fallos, ya que la infraestructura de los data-centers provistos por los CSP debe incluir planes eficientes de respaldo y recuperación ante fallos o desastres naturales. Si la eventualidad se presenta del lado del usuario final, no habría afectación en los datos almacenados en la nube, y las actividades para restablecer la operación estarían enfocados a recuperar las comunicaciones y acceso a dispositivos finales.

- Los riesgos técnicos, ambientales y del entorno social se transfieren en su mayoría a los data-centers del CSP. El proveedor es quien respalda con

[136] G.ST.02 Guía de Computación en la nube [en línea]. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones. 2018., 44 p. Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html., p.34.

tecnología de punta, la seguridad, el mantenimiento, la actualización y los procesos de mejora continua de la infraestructura física que soporta el servicio. Del lado del usuario final, la responsabilidad sobre los riesgos técnicos, ambientales y del entorno social se centra en las comunicaciones, los dispositivos finales y el acceso a las plataformas.

6.1.5 Factores Impulsores de Cloud Computing

Ya desde 2010, el documento de la Mesa Sectorial Cloud Computing en Colombia se describía como iba a ser la evolución de la Computación en la Nube en el país:

> La llegada de la crisis económica mundial desafió la competitividad de las empresas a través del recurso más económico conocido: la innovación y el ingenio, el talento humano. Cientos de empresas recurrieron a sus estructuras de personal y confiaron en su planta de TI la reducción de costos e impacto de la crisis, forzando a que la innovación afectara los rígidos y tradicionales componentes de IT hasta llevarlos a la Nube.[137]

Entre otros factores, los modelos de computación en la nube están evolucionado en las empresas colombianas, impulsados por la necesidad de reducir la inversión en tecnología e infraestructura física, mediante el uso de data-centers compartidos y de propiedad de terceros, pero sin dejar de ser competitivos en el mercado. En el documento de la Mesa Sectorial de Cloud Computing para Colombia se identifican los principios básicos a tener en cuenta, dentro de la adopción de Cloud Computing a nivel empresarial:

- Que la dirección de la organización tenga claros los conceptos, beneficios y riesgos de la implementación de Cloud Computing, así como la metodología de la adaptación de Cloud Computing a las necesidades y operaciones de la empresa.
- Todos los procesos migrados a la nube deben cumplir estándares y políticas alineadas con todos los demás procesos de la compañía.
- Implementación de procesos de transferencia del conocimiento sobre el uso de las nuevas herramientas, con el fin de alinear a toda la organización a un mismo concepto.

[137] CASTRO, Op. cit., p. 26 - 27.

- Iniciar los procesos de adopción de nuevas tecnologías a partir de casos de éxito de otras empresas que ya tengan avances en Cloud Computing, con lo cual se logra prever el resultado de la implementación.

- La adopción de Cloud Computing se debe hacer de manera gradual, e iniciando con procesos no críticos para la operación.

En cuanto a las oportunidades y amenazas en la implementación de Cloud Computing en las pequeñas y medianas empresas, la Mesa Sectorial identifica las siguientes:

Oportunidades:

- Acceso a tecnologías actualizadas

- Capacidad de tener infraestructura flexible y escalable

- Reducción de los costos en Infraestructura en TI y operacionales

Amenazas:

- Percepción de pagar por algo innecesario, porque se puede manejar en infraestructura local

- Desconocimiento de los conceptos de Cloud Computing, su funcionamiento y beneficios

- Desconocimiento de la normatividad TIC, y de los beneficios impulsados por el Estado para la implementación de nuevas tecnologías.

La Mesa Sectorial sobre Cloud Computing para Colombia[138] describe algunos factores impulsores en la implementación de los servicios de computación en la nube:

- Tercerización: Muchas organizaciones empresariales optan por entregar la operación y mantención de sus servicios a terceros. Con esto se minimizan costos y optimizan resultados, sin necesidad de prestar mucha atención al trasfondo técnico del servicio. Cloud Computing encaja dentro de este enfoque.

[138] Ibíd., p. 13.

- Tiempo de Valoración y Desempeño: La promesa de servicio de Cloud Computing se centra en entregar soluciones empresariales de alto desempeño. Técnicamente, los CSP están preparados para superar las capacidades de cualquier infraestructura 'On Premise' en términos de almacenamiento, procesamiento y disponibilidad.

- Ubicuidad: Los servicios de Cloud Computing permiten acceder a la información y herramientas de manera ubicua, o sea en cualquier momento y desde cualquier lugar. Esto permite que los colaboradores de las empresas puedan trabajar colaborativamente, desde múltiples ubicaciones y sin restricción de dispositivo tecnológico, dinamizando los procesos internos de las empresas usuarias de Cloud Computing.

- Economía: Cloud Computing permite a las empresas usuarias, la reducción en la inversión en tecnología e infraestructura física, mediante el uso de data-centers compartidos y de propiedad de terceros.

- Maduración de las tecnologías: La aparición de nuevas tecnologías para la virtualización de servicios eficientes, dinámicos y elásticos, generan oportunidades de mercado al Cloud Computing por encima de las infraestructuras tradicionales. Cloud Computing tiene como ventaja competitiva, la capacidad de ofrecer servicios complejos, accedidos bajo demanda, económicos y de fácil implementación y acceso.

6.1.6 Riesgos de Cloud Computing

Si bien Cloud Computing ofrece múltiples ventajas, también es necesario tener en cuenta los siguientes riesgos, tal y como los describe Bruno[139] en su documento enfocado al sector financiero:

- Sobre temas de seguridad, se debe tener en cuenta que el usuario final del servicio de Cloud Computing es quien debe velar por el control de acceso ya que es único dueño de los usuarios y contraseñas para acceder al servicio, mientras que el CSP es el encargado de garantizar seguridad física y lógica y encriptación de datos.

- El cliente, si bien es dueño de la información, ya no tiene control sobre ciertos aspectos, como la proliferación de los datos debido a las condiciones de respaldo de los datos. Esto se debe a que el CSP en busca de entregar servicios tolerantes a fallos puede generar distintas copias de la información, con lo que se podría aumentar la posibilidad de exposición de su información.

[139] BRUNO, Op. cit., p. 69-82.

- El dueño de la información puede desconocer completamente donde está alojada su información, así como las condiciones técnicas de procesamiento.

- La seguridad física es responsabilidad del CSP, quien debe garantizar que posee las herramientas de protección al acceso no autorizado a los datos a nivel físico o de red, entre aplicaciones que cohabiten en una infraestructura física o entre las distintas instancias de los sistemas operativos.

- A pesar de que el CSP es responsable de la estabilidad del servicio de Cloud Computing, esto no resta importancia a que la empresa usuaria tenga que establecer adecuadamente los planes de recuperación de desastres y continuidad del negocio, en aspectos como comunicaciones, energía y estado de los equipos de cómputo.

La Mesa Sectorial sobre Cloud Computing para Colombia[140] también menciona algunos obstáculos importantes dentro de la implementación de esta infraestructura:

- Percepción de la Seguridad: Existe desconocimiento acerca de las ventajas en términos de Seguridad Informática que puede ofrecer una infraestructura de Cloud Computing, por encima de un data-center privado. Aún existe la idea de que los datos están más seguros dentro una infraestructura 'On Premise' que dentro de la infraestructura de computación en la nube (a pesar de los riesgos ambientales, humanos, de obsolescencia y demás, propios de la infraestructura física privada).

- Percepción a Cerca de las Regulaciones: Debido a que los datos salen del país de residencia del cliente (incluso puede llegar a varios países, dependiendo de la fragmentación de datos propia del plan de backups implementado por el CSP), y el CSP puede ser de una nacionalidad diferente a la del cliente, no existe claridad en cuanto a que regulación normativa sobre tratamiento de datos personales y demás, pueden aplicarse efectivamente dentro de la prestación del servicio.

- Restricciones de Internet: El uso de una infraestructura de Cloud Computing depende en gran medida del acceso a una conexión a Internet, lo cual pondría en riesgo la operación de la empresa usuaria en el momento de una caída de la conectividad, tanto a nivel local como de los distintos nodos por donde se establece la comunicación hasta los data-centers del CSP.

- Pérdida de Control Sobre la Información: Existe percepción de pérdida de control sobre la información, debido a la inexistencia de la intervención a los servidores y demás elementos físicos de la infraestructura, así como por el desconocimiento de la ubicación exacta donde se almacenan los ficheros.

[140] CASTRO, Op. cit., p. 14.

Esto genera la idea de dependencia total al CSP, limitando las libertades y derechos sobre la información propias del Cliente.

6.1.7 Temores Asociados con la Implementación de Cloud Computing

Pese a las ventajas que ofrece la implementación de infraestructuras Cloud Computing, aún hay elementos que generan temor a los empresarios para incursionar en esta nueva tecnología, de los cuales se pueden resaltar los siguientes:

Tabla 4. Temores Asociados con la Implementación de Cloud Computing

Temor sobre Cloud Computing	Análisis del Temor
No disponibilidad del servicio	Para la disponibilidad del servicio se deben tener en cuenta dos aspectos: La calidad del acceso a Internet dentro de la empresa, que se ve afectado tanto por la infraestructura de la red local implementada, como por la calidad del servicio de Internet contrato. Por otra parte, los acuerdos de nivel de servicio (SLA´s) establecidos al iniciar la relación comercial con el CSP, los cuales se encuentran respaldados por la infraestructura física del CSP y sus planes de backups y redundancia de la información. Siempre que el acceso a internet dentro de la empresa sea el adecuado, y se seleccione un CSP que ofrezca Acuerdos de Nivel del Servicio sobresalientes, no se deberían presentar incidentes de disponibilidad del servicio que afecten la operación del usuario final. La calidad del servicio de internet es un factor importante para el acceso a Cloud Computing, tal como lo señala la Mesa Sectorial colombiana[141], ya que puede causar cuellos de botella en el flujo de información.
Baja integridad y confidencialidad al operar en infraestructura compartida	Tal como lo afirma la Guía de Computación en la Nube[142], los CSP ofrecen herramientas a nivel físico y lógico con las que garantizan un ambiente seguro entre usuarios (procesos avanzados de autenticación y control de accesos, encriptación en varios niveles, etc.). Con esto buscan que la operación, datos y servicios contratados de un cliente no afecten la operación de los demás.

[141] Ibíd., p. 14.
[142] G.ST.02 Guía de Computación en la nube, Op. cit., p.37.

Temor sobre Cloud Computing	Análisis del Temor
Cloud Computing es inseguro	La Mesa Sectorial sobre Cloud Computing para Colombia[143] aborda este aspecto señalando que una infraestructura en la nube es mucho más segura que una infraestructura 'On Premise'. Esto se justifica afirmando que dentro de un data-center privado los datos están expuestos a riesgos ambientales, humanos, de obsolescencia y demás, propios de la infraestructura física, mientras que un data-center de Cloud Computing cuenta con tecnología de punta para afrontar dichos riesgos. El CSP, contrario a una pequeña o mediana empresa, está en la capacidad financiera de invertir constantemente en actualización de hardware y software. Adicional, se debe tener en cuenta que el modelo de seguridad de Cloud Computing es de 'Responsabilidad Compartida', de modo que mientras que el usuario tenga una buena definición de la política de identidad y control de acceso basada en mínimos privilegios, y que el proveedor garantice las herramientas y condiciones de seguridad física requeridas; el uso de una infraestructura Cloud Computing resultante contará con los niveles de seguridad adecuados.
Poco control sobre el sistema y los datos alojados	La Agencia Española de Protección de Datos[144] describe este aspecto como la falta de control por parte del usuario final sobre la infraestructura física del data-center donde se alojan sus datos, ya que es propiedad del CSP. Pero, en cuanto a los datos, el cliente es dueño y responsable de los datos personales, y como tal debe cumplir la normativa sobre protección de datos de su país. El CSP no tiene ningún nivel de acceso a los datos, a menos que contractualmente se especifique lo contrario.
Desconocimiento de la ubicación real del Data-Center	Los CSP hacen pública la ubicación de sus centros de datos a un nivel de abstracción alta (países, regiones o zonas). El cliente tiene derecho a seleccionar las zonas donde quiere almacenar o replicar sus datos, y que esta selección quede explicita en sus Acuerdos de Nivel de Servicio y demás documentación contractual necesaria. Lo que el cliente desconoce realmente es el data-center exacto donde están sus datos, y el hardware que soporta la operación.
Falta de claridad sobre la legislación aplicable	En cuanto a la percepción del cumplimiento de las regulaciones aplicables, no existe legislación específica a Cloud Computing en Colombia, pero si hay regulaciones muy claras que definen temas sensibles que trascienden a la

[143] CASTRO, Op. cit., p. 14.
[144] AEPD, Op. cit., p. 12.

Temor sobre Cloud Computing	Análisis del Temor
	nube, como Protección de Datos personales. La Mesa Sectorial sobre Cloud Computing para Colombia[145] indica que debe existir cumplimiento por parte del CSP y del Cliente, de las distintas leyes y reglamentos asociados con el almacenamiento y tratamiento de datos personales que apliquen dentro del territorio colombiano.

Fuente: El autor

[145] CASTRO, Jorge. Cloud Computing: Una Perspectiva Para Colombia. En: Mesa Sectorial Cloud Computing. Versión 1.0.0., Abril, 2010., p. 14.

7. RESULTADOS

La implementación de Cloud Computing para una pequeña o mediana empresa colombiana, resulta conveniente desde muchos puntos de vista, ya que los modelos de negocio del mercado tienden a la tercerización, entregando aspectos técnicos específicos y servicios a proveedores expertos. Lo anterior abre la posibilidad de acceder a tecnología de punta para la ejecución de actividades diarias, haciendo una mínima inversión en infraestructura tecnológica, en donde todos los aspectos de implementación, actualización, mantenimiento, escalamiento y recuperación de desastres a nivel de hardware o software son absorbidos por el CSP. Adicional, la facilidad para implementar modelos de colaboración, tanto a nivel de datos, desarrollo de software o infraestructura, hace que los sistemas estén en la capacidad de evolucionar rápidamente y adaptarse a las necesidades del entorno. Por otra parte, y debido a su orientación a ser una arquitectura SOA, se pueden remplazar, migrar o ajustar elementos del sistema sin interrumpir la operatividad del servicio.

La computación en la nube se puede pensar como un medio de inclusión social, ya que permite que las pequeñas y medianas empresas tengan acceso a herramientas de procesamiento de datos avanzadas, con costos accesibles. También permite que dichas empresas puedan adaptarse a los nuevos desafíos del mercado con mayor agilidad, ya que otorga rapidez en el despliegue de nuevas aplicaciones con menor riesgo e inversiones financieras, ayudando así a que estas pequeñas organizaciones puedan competir con productos de calidad y flexibles a la demanda. Cloud Computing permite democratizar el acceso a la seguridad informática, esto es posible cuando el CSP da el mismo tratamiento a todos los datos almacenados en sus data-centers, protegiendo tanto a grandes como a pequeños clientes con la misma tecnología de punta. Esto beneficia a la pequeña y mediana empresa, que en un contexto de infraestructura ‘On Premise’ no tendría los recursos necesarios para implementar controles de seguridad informática robustos o actualizar su infraestructura cada vez que aparece una nueva amenaza de seguridad informática.

Desde el punto de vista financiero, quien implementa Cloud Computing no incurre en gastos de acondicionamiento físico o de administración de servidores, ni se expone a riesgos físicos y ambientales propios de la tenencia de data-centers. Tampoco es necesario tener personal de soporte técnico para esa infraestructura, las funciones del área de T.I. se centrarían en gestionar el acceso seguro a internet y el correcto funcionamiento de los dispositivos y equipos de cómputo. En cuanto al uso de la infraestructura, los CSP implementan herramientas y métricas que permiten que la facturación sea por consumo, de manera transparente para las dos partes.

El cambio a este modelo tecnológico se debe reflejar en la reducción de costos en infraestructura tecnológica y a actualizaciones de software más rápidas. Pero dicha

adopción debe ir unida a la forma en cómo el CSP aborda a las inquietudes de los usuarios sobre seguridad informática, integración e interoperabilidad. En cuanto a la interoperabilidad e integración, Cloud Computing debe proporcionar mecanismos para que los usuarios finales puedan copiar objetos desde y hacia la nube, o mecanismos para usar sus datos y servicios desde y hacia distintos sistemas mediante interfaces basadas en estándares de común aceptación que faciliten la comunicación.

En cuanto a seguridad informática, se debe tener en cuenta que es un aspecto transversal de la infraestructura de Cloud Computing, en donde intervienen tanto el CSP (quien garantiza la seguridad física y lógica) como el Cliente (quien garantiza el control de acceso a aplicaciones y datos). Por lo tanto, la seguridad de toda la infraestructura de Cloud Computing no es únicamente responsabilidad del CSP, sino también de los consumidores. Los data-centers propiedad de los CSP, que sustentan la operación de un servicio de Cloud Computing, son compartidos por varios clientes, lo cual genera la percepción de que una falla de seguridad se puede traducir en accesos no controlados a datos confidenciales. En este sentido, se debe tener en cuenta que la arquitectura de seguridad de Cloud Computing implementa los mecanismos necesarios para generar un ambiente seguro entre usuarios. Cabe resaltar que el modelo de seguridad de Cloud Computing es de 'Responsabilidad Compartida', y mientras que el usuario controle debidamente el acceso a los sistemas, y que el CSP provea las herramientas y condiciones de seguridad física ideales; el uso de Cloud Computing contará con los niveles de seguridad informática apropiados.

También se debe tener en cuenta que, para la implementación de Cloud Computing, no es obligatorio migrar inmediatamente ni en su totalidad los servicios de información que soportan las operaciones de la empresa. Se deben iniciar los procesos de migración a la nueva tecnología a partir del análisis de casos de éxito y el estudio de ofertas de los CSP, con lo cual se puede prever el resultado de la implementación. Igualmente, la adopción de Cloud Computing se debe hacer de forma gradual, partiendo de procesos de bajo impacto para la operación de la empresa. Con esto se logran reducir los riesgos inherentes a los cambios de tecnología, como los resultados no esperados o variables no previstas en el plan inicial de trabajo.

Es importante resaltar que no existen restricciones para que en Colombia se lleve información a la nube. Si bien aún es un modelo de infraestructura tecnológica que se encuentra en sus inicios, y no existe una legislación específica a Cloud Computing en el país, si hay regulaciones muy claras aplicables a temas sensibles que trascienden a la nube, como por ejemplo Protección de Datos Personales. Entre estas regulaciones tenemos: Ley 1266 de 2008 sobre Habeas Data, Ley 1273 de 2009 sobre protección de la información y de los datos, Ley 1341 de 2009 sobre Tecnologías de la Información y la Comunicación, Ley 1581 de 2012 sobre Protección de Datos personales, Acuerdo Marco de Servicios de Nube Pública III

que regula la contratación con entidades Públicas, la Circular 002 de 2018 de la Superintendencia de Industria y Comercio que complementa a la ley 1581, o la Ley 1943 de 2018 que define a Cloud Computing como un servicio exento del Impuesto a las Ventas (IVA).

8. CONCLUSIONES

La revisión de múltiples fuentes documentales para la construcción de la presente monografía permitió analizar los aspectos conceptuales básicos dentro de la implementación de servicios de Cloud Computing en pequeñas y medianas empresas colombianas; así como el conocimiento de las regulaciones legales aplicables, y del modelo de contratación y aspectos necesarios para la prestación transparente del servicio. Particularmente sobre el aspecto legal, se encontró que Colombia aún tiene un largo camino por recorrer, ya que las regulaciones existentes no son específicas a Cloud Computing. A pesar de esto, se debe resaltar que la legislación colombiana si brinda garantías a las empresas y demás demandantes del servicio que utilizan Cloud Computing, ya que los CSP deben cumplir regulaciones muy claras aplicables a temas sensibles que trascienden a la nube, como lo es la Protección de Datos Personales.

En cuanto a los mecanismos y aspectos de Seguridad Informática de la Computación e la Nube, se encuentra que este es un aspecto transversal de la infraestructura en donde intervienen tanto el CSP como el consumidor final del servicio. Por lo tanto, la seguridad informática de Cloud Computing no depende únicamente de una buena infraestructura física y lógica provista por el CSP, sino también de las buenas prácticas de los clientes y consumidores finales. La infraestructura, herramientas y procesos de los CSP más conocidos en el país, y estudiados en el presente documento, demuestran que la arquitectura de los sistemas de información que implementan para el almacenamiento e intercambio de los datos está diseñada muy especialmente para evitar incidentes como la interceptación o alteración de datos, la suplantación de identidad o la denegación del servicio, aspectos vitales para la seguridad informática de cualquier pequeña o mediana empresa. A pesar de que el CSP es el encargado de la seguridad y estabilidad del servicio de Cloud Computing, no se resta responsabilidad a la empresa usuaria en establecer adecuadamente los planes de recuperación de desastres y continuidad del negocio, en aspectos como comunicaciones, energía y estado de los equipos de cómputo, así como de implementar las medidas necesarias para prevenir el acceso no autorizado a los servicios en la nube.

Si bien Cloud Computing ofrece múltiples ventajas, también es necesario tener en cuenta algunos riesgos, ya que esta infraestructura opera de manera distinta a como funcionan en las arquitecturas físicas tradicionales. El cliente sigue siendo dueño de la información, pero Cloud Computing genera pérdida del control sobre ciertos aspectos, como por ejemplo la proliferación y fragmentación de los datos en distintos países debido a las condiciones de respaldo de los datos, o desconocimiento de dónde está alojada la información, así como de las condiciones técnicas del procesamiento. Debido a que los datos salen del país de residencia del cliente, puede faltar claridad en cuanto a qué regulación normativa sobre tratamiento de datos personales, pueden aplicarse efectivamente dentro de la prestación del servicio. El uso de una infraestructura de Cloud Computing también genera

dependencia del acceso a Internet, lo cual pondría en riesgo la operación de la empresa usuaria en el momento de una caída de la conectividad.

Cloud Computing ofrece a las pequeñas y medianas empresas la posibilidad de acceder a tecnología de punta para la ejecución de sus actividades diarias, haciendo una mínima inversión en infraestructura tecnológica, en donde todos los aspectos de implementación, actualización, mantenimiento, escalamiento y recuperación de desastres a nivel de hardware o software son absorbidos por el CSP. Adicional, la implementación de Cloud Computing busca la reducción de la infraestructura física, con lo que hay un mejor aprovechamiento de los recursos energéticos y a reducción de la generación de desperdicios tecnológicos, lo que se traduce en que Cloud Computing apunta a ser una tecnología ambientalmente amigable. Cloud Computing también impulsa formas más eficientes de laborar dentro de las empresas, como por ejemplo la masificación del Teletrabajo, ya que permite que los funcionarios puedan acceder a todas las herramientas de trabajo desde cualquier computador y conexión a internet.

9. RECOMENDACIONES

Colombia es un entorno favorable para que las pequeñas y medianas empresas piensen en la implementación de Cloud Computing, ya que desde muchos puntos de vista este paradigma es beneficioso para la operación, permitiendo por ejemplo el acceso fácil a tecnología de punta con una mínima inversión en infraestructura, y con la garantía de que los grandes proveedores de Cloud Computing con presencia en el país cuentan con la experiencia y capacidad técnica necesarias para garantizar la confidencialidad, la integridad y disponibilidad de la información, lo anterior cumpliendo con estándares y regulaciones de seguridad y protección de datos personales nacionales e internacionales.

La seguridad informática en los modelos de computación en la nube es un aspecto transversal y de responsabilidad compartida, donde interviene tanto el proveedor quien garantiza la seguridad física y lógica, como el cliente quien gestiona el control de acceso a aplicaciones y datos. La empresa usuaria del servicio de Cloud Computing debe implementar políticas y controles para garantizar la seguridad informática en redes, dispositivos de usuario final y recurso humano.

No existe una legislación específica a Cloud Computing en Colombia, ya que es un modelo de infraestructura tecnológica que se encuentra en sus inicios. Si bien se cumple con regulaciones de suma importancia como lo es Protección de Datos Personales, es importante que a futuro existan herramientas jurídicas que controlen específicamente la contratación de servicios en la nube, lo cual generaría confianza al usuario final y por ende mayor penetración en el mercado de esta tecnología.

El remplazo de los data-centers privados por el uso de Cloud Computing apunta a la reducción de riesgos físicos y ambientales, al mejor aprovechamiento de los recursos energéticos y a una menor generación de desperdicios tecnológicos, lo cual significa que Cloud Computing es ambientalmente amigable y muy oportuno en entornos empresariales donde ya es visible la responsabilidad con el medio ambiente.

REFERENCIAS

ABE, John Olorunfemi y USTUNDAUG, Burak Berk. A Data as a Service (DaaS) Model for GPU-based Data Analytics. En: IEEE IFIP NTMS Workshop on Big Data and Emerging Trends WBD-ET 2018., Febrero, 2018.

AEPD. Guía para clientes que contraten servicios Computing [en línea]. Madrid: Agencia Española de Protección de Datos. 2018., 25 p. Disponible en https://www.aepd.es/media/guias/guia-cloud-clientes.pdf

AICPA. Assurance and Advisory. [en línea]. [Consultado el 19 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/

ALFONSO FERRER, Eduardo. Wow! On the Road to the Cloud. En: Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A. Vol. 10 Issue 2., 2013.

AMAZON WEB SERVICES. AWS re: Invent. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/

ANDERSON, Tim. How to Make Sense of Desktop as a Service. En: Computer Weekly., 2013.

ANDRADE DELGADO, Wilman Ernesto. Estudio de factibilidad para la migración de servicios IT On-Premise a Cloud Computing de la vertical financiera de Cooperativas de Ahorro y Crédito (COAC) del Ecuador. Caso de aplicación. Trabajo de grado Magister en Gerencia de Sistemas y Tecnologías de Información. Quito: Universidad de las Américas., 2014.

ARÉVALO NAVARRO, José Manuel. Cloud Computing: fundamentos, diseño y arquitectura aplicados a un caso de estudio. Trabajo de grado Máster Oficial en Tecnologías de la Información y Sistemas Informáticos. Madrid: Universidad Rey Juan Carlos., 2011.

ASSILA, Bouchaib; KOBBANE, Abdellatif; BEN-OTHMAN, Jalel y KOUTBI, Mohammed El. Caching as a Service for 5G Networks: A Matching Game Approach for CaaS Resource Allocation. En 2018 IEEE Symposium on Computers and Communications (ISCC). 01193-01198J., Junio, 2018.

ASSURANCE AND ADVISORY [en línea]. AICPA. [Consultado: 10 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/

BRUNO, Gaston. Cloud computing en la industria financiera. En: Revista de Ciencia y Tecnología. Vol. 13., 2013.

CASTILLO JAIME, Oswaldo Augusto. Planteamiento de un modelo basado en la arquitectura SOA en el gobierno de TI de las empresas de contact center. Trabajo de grado Magíster en Gobierno de Tecnologías de Información. Lima: Universidad Nacional Mayor de San Marcos., 2017.

CASTRO, Jorge. Cloud Computing: Una Perspectiva Para Colombia. En: Mesa Sectorial Cloud Computing. Versión 1.0.0., Abril, 2010.

CLOUD SECURITY ALLIANCE. About. [en línea]. [Consultado: 10 de noviembre de 2019]. Disponible en: https://cloudsecurityalliance.org/

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2011.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2011.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1943. (28 de diciembre de 2018). Por la cual se expiden normas de financiamiento para el restablecimiento del equilibrio del presupuesto general y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2018.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2013

COLOMBIA. DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES. Concepto 017056 de 2017. (25 de agosto de 2017). Concepto Unificado Del Numeral 24 Del Artículo 187 De La Ley 1819 De 2016. Bogotá, D.C., 2017.

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Externa 002 de 2018. (23 de marzo de 2018). Por medio de la cual se modifica el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única. SIC. Bogotá, D.C., 2018.

COLOMBIACOMPRA. Nube pública III [en línea]. Bogotá: Colombia Compra Eficiente., Disponible en https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/nube-publica-iii

DEL VECCHIO, José Francisco; PATERNINA, Fabián José y MIRANDA, Carlos. La computación en la nube: un modelo para el desarrollo de las empresas. En: Revista Prospectiva. Vol. 13., Julio – Diciembre, 2015.

ESTADOS UNIDOS DE MÉXICO. CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Reglamento De La Ley Federal De Protección De Datos Personales En Posesión De Los Particulares. (21, diciembre, 2011). Diario Oficial. México D.F., 2011.

FEDRAMP. About Us. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.fedramp.gov/about/

FERNÁNDEZ, Carlos y RECIO, Miguel. Privacidad Elevada a la Nube [en línea]. Madrid: AENOR. 2015., p. 20 - 23. Disponible en https://portal.aenormas.aenor.com/revista/pdf/nov15/20nov15.pdf

FERNÁNDEZ, Froilán. Un Salto A La Nube La Computación En Los Cielos Virtuales. En: DEBATES IESA. Vol. XV., No 1 Enero, 2010.

FUTARO, Angelo; GARRO, Alfredo y TUNDIS, Andrea. Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing. En: 2014 International Carnahan Conference on Security Technology (ICCST)., Octubre, 2014.

G.ST.02 Guía de Computación en la nube [en línea]. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones. 2018., 44 p. Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html

GARCÍA DEL POYO, Rafael. Cloud Computing: Aspectos Jurídicos Clave Para la Contratación de Estos Servicios. En: Revista Española de Relaciones Internacionales. Núm. 4. ISSN 1989-6565., 2012.

GOOGLE CLOUD. Descubre lo que puedes lograr con Google Cloud. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com

GRANCE, Timothy y MELL, Peter. The NIST Definition of Cloud Computing. En: NIST. Special Publication 800-145., Septiembre, 2011.

GRUNFELD, Bárbara y SCHCOLNIK, Alan. ¿Cloud computing?. En: IEEM Revista de Negocios., Junio, 2015.

GUTIÉRREZ, Horacio y KORN, Daniel. Facilitando “the cloud”: la regulación de la protección de datos como motor de la competitividad nacional en América Latina. En: Revista La Propiedad Inmaterial no. 18., Universidad Externado de Colombia., Noviembre, 2014.

HUAWEI. Índice de Conectividad Global 2019. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://www.huawei.com/minisite/gci/en/

ISO-IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements.

ISO-IEC 22301:2012 Societal security - Business continuity management systems – Requirements.

ISO-IEC 27000:2018, Information technology - Security techniques - Information security management systems -- Overview and vocabulary.

ISO-IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements.

ISO-IEC 27002:2013, Information Technology - Security Techniques - Code Of Practice For Information Security Management.

ISO-IEC 27017:2015, Information Technology — Security Techniques - Code Of Practice For Information Security Controls Based On ISO/IEC 27002 For Cloud Services.

ISO-IEC 27018:2019, Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

ISO-IEC 29100:2011, Information technology -- Security techniques -- Privacy framework.

KATZ, Raúl. Informe del Observatorio De La Economía Digital De Colombia [en línea]. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones. 2017., 44 p. Disponible en https://www.mintic.gov.co/portal/604/articles-61929_recurso_4.pdf

LIU, Fang; TONG, Jin; MAO, Jian; BOHN, Robert; MESSINA, John; BADGER, Lee y LEAF, Dawn. NIST Cloud Computing Reference Architecture. En: NIST. Special Publication 500-292., Septiembre, 2011.

MANNER, Johannes; ENDREB, Martin; HECKEL, Tobias y WIRTZ, Guido. Cold Start Influencing Factors in Function as a Service. En 2018 IEEE/ACM International

Conference on Utility and Cloud Computing Companion (UCC Companion). 181-188., Diciembre, 2018.

MICROSOFT CLOUD. Azure. Invente con un objetivo. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es

MORENO GOMEZ, Gonzalo Andrés. Jurisdicción Aplicable En Materia De Datos Personales En Los Contratos De Cloud Computing: Análisis Bajo La Legislación Colombiana. En: Revista de Derecho, Comunicaciones y Nuevas Tecnologías. No 9., Julio, 2013.

MORENO, Mario. Computación En La Nube. En: Documentos de Trabajo. No 566., Junio, 2015.

NADAF, Shameemraj; RATH, Hemant; ARUN KUMAR, A V; SHAILENDRA, Samar y SIMHA, Anantha. An open source based network as a service (NaaS) platform for cloud provisioning. En 2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)., Diciembre, 2015.

ONTSI. Cloud Computing: Retos y Oportunidades [en línea]. Madrid: Observatorio Nacional de las Telecomunicaciones y la SI. 2012., 55 p. Disponible en https://www.ontsi.red.es/ontsi/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

PCI SECURITY STANDARDS COUNCIL. ABOUT US. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.pcisecuritystandards.org/about_us/

PRECIADO, Martha y VARGAS, Magna Luz. Guía de Contratación de Servicios en la Nube Para Empresas Públicas y Privadas en Colombia que Garantice un Correcto Análisis Forense Cuando se Presenten Incidentes se Seguridad. Trabajo de grado Especialización en Seguridad Informática. Bogotá: Universidad Piloto de Colombia, 2016.

TOESLAND, finbarr. C XAAS MODEL RESHAPES THE FUTURE OF OUTSOURCING. En: Computer Weekly., junio 2019.

UNIÓN EUROPEA. PARLAMENTO EUROPERO Y EL CONSEJO. Reglamento General de Protección de Datos. (4, mayo, 2016). El Parlamento. Unión Europea, 2016.

VARELA, Carlos; PORTELLA, Jorge y PALLARES, Luis. Computación en la nube: un nuevo paradigma en las tecnologías de la información y la comunicación. En: Revista Electrónica Redes de Ingeniería. edición especial., enero - junio 2017.

ANEXOS

Anexo 1. Formato RAE

Fecha de Realización: 12/12/2019
Título: ANÁLISIS DE LOS COMPONENTES DE SEGURIDAD INFORMÁTICA EN LA IMPLEMENTACIÓN DE CLOUD COMPUTING EN PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS
Autor: TORRES GONZÁLEZ, Adriana Marcela
Palabras Claves: Cloud Computing, IaaS, SaaS, PaaS, Seguridad Informática
Descripción: Cloud Computing representa una nueva manera de disponibilizar los recursos informáticos para que una empresa lleve a cabo sus actividades económicas, mediante el uso de infraestructura tecnológica virtualizada, almacenada en un servidor de algún proveedor de Cloud Computing o CSP. Sin embargo, para muchos, este modelo puede resultar riesgoso, ya sea por desconocimiento técnico del funcionamiento de Cloud Computing, o porque los datos almacenados que forman parte del diario vivir de la organización son en extremo delicados. La seguridad informática para las empresas es un aspecto vital, ya que puede comprometer directamente datos delicados, tanto de la organización como de los clientes. Por este motivo la infraestructura tecnológica usada para almacenar e intercambiar información, debe estar diseñada y enfocada para evitar incidentes tales como la interceptación y/o alteración de datos, la suplantación de identidad o la denegación del servicio. La presente monografía, mediante la revisión de distintas fuentes documentales, busca ser un referente que permita analizar los aspectos de seguridad en la implementación de servicios de Cloud Computing en pequeñas y medianas empresas colombianas, como estrategia para determinar si es conveniente o no el uso de este tipo de infraestructura en el manejo de información delicada.
Fuentes: Para la realización de la monografía, se hizo uso de 56 referencias bibliográficas, las cuales corresponden a fuentes electrónicas. A continuación, se listará las mencionadas citas: ABE, John Olorunfemi y USTUNDAUG, Burak Berk. A Data as a Service (DaaS) Model for GPU-based Data Analytics. En: IEEE IFIP NTMS Workshop on Big Data and Emerging Trends WBD-ET 2018., Febrero, 2018. AEPD. Guía para clientes que contraten servicios Computing [en línea]. Madrid: Agencia Española de Protección de Datos. 2018., 25 p. Disponible en https://www.aepd.es/media/guias/guia-cloud-clientes.pdf AICPA. Assurance and Advisory. [en línea]. [Consultado el 19 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/

ALFONSO FERRER, Eduardo. Wow! On the Road to the Cloud. En: Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A. Vol. 10 Issue 2., 2013.
AMAZON WEB SERVICES. AWS re: Invent. [en línea]. [Consultado el 16 de octubre de 2019]. Disponible en: https://aws.amazon.com/es/
ANDERSON, Tim. How to Make Sense of Desktop as a Service. En: Computer Weekly., 2013.
ANDRADE DELGADO, Wilman Ernesto. Estudio de factibilidad para la migración de servicios IT On-Premise a Cloud Computing de la vertical financiera de Cooperativas de Ahorro y Crédito (COAC) del Ecuador. Caso de aplicación. Trabajo de grado Magister en Gerencia de Sistemas y Tecnologías de Información. Quito: Universidad de las Américas., 2014.
ARÉVALO NAVARRO, José Manuel. Cloud Computing: fundamentos, diseño y arquitectura aplicados a un caso de estudio. Trabajo de grado Máster Oficial en Tecnologías de la Información y Sistemas Informáticos. Madrid: Universidad Rey Juan Carlos., 2011.
ASSILA, Bouchaib; KOBBANE, Abdellatif; BEN-OTHMAN, Jalel y KOUTBI, Mohammed El. Caching as a Service for 5G Networks: A Matching Game Approach for CaaS Resource Allocation. En 2018 IEEE Symposium on Computers and Communications (ISCC). 01193-01198J., Junio, 2018.
ASSURANCE AND ADVISORY [en línea]. AICPA. [Consultado: 10 de noviembre de 2019]. Disponible en: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/
BRUNO, Gaston. Cloud computing en la industria financiera. En: Revista de Ciencia y Tecnología. Vol. 13., 2013.
CASTILLO JAIME, Oswaldo Augusto. Planteamiento de un modelo basado en la arquitectura SOA en el gobierno de TI de las empresas de contact center. Trabajo de grado Magíster en Gobierno de Tecnologías de Información. Lima: Universidad Nacional Mayor de San Marcos., 2017.
CASTRO, Jorge. Cloud Computing: Una Perspectiva Para Colombia. En: Mesa Sectorial Cloud Computing. Versión 1.0.0., Abril, 2010.
CLOUD SECURITY ALLIANCE. About. [en línea]. [Consultado: 10 de noviembre de 2019]. Disponible en: https://cloudsecurityalliance.org/
COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2011.
COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2011.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1943. (28 de diciembre de 2018). Por la cual se expiden normas de financiamiento para el restablecimiento del equilibrio del presupuesto general y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2018.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley Estatutaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2013

COLOMBIA. DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES. Concepto 017056 de 2017. (25 de agosto de 2017). Concepto Unificado Del Numeral 24 Del Artículo 187 De La Ley 1819 De 2016. Bogotá, D.C., 2017.

COLOMBIA. SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Circular Externa 002 de 2018. (23 de marzo de 2018). Por medio de la cual se modifica el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única. SIC. Bogotá, D.C., 2018.

COLOMBIACOMPRA. Nube pública III [en línea]. Bogotá: Colombia Compra Eficiente., Disponible en https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/nube-publica-iii

DEL VECCHIO, José Francisco; PATERNINA, Fabián José y MIRANDA, Carlos. La computación en la nube: un modelo para el desarrollo de las empresas. En: Revista Prospectiva. Vol. 13., Julio – Diciembre, 2015.

ESTADOS UNIDOS DE MÉXICO. CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Reglamento De La Ley Federal De Protección De Datos Personales En Posesión De Los Particulares. (21, diciembre, 2011). Diario Oficial. México D.F., 2011.

FEDRAMP. About Us. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.fedramp.gov/about/

FERNÁNDEZ, Carlos y RECIO, Miguel. Privacidad Elevada a la Nube [en línea]. Madrid: AENOR. 2015., p. 20 - 23. Disponible en https://portal.aenormas.aenor.com/revista/pdf/nov15/20nov15.pdf

FERNÁNDEZ, Froilán. Un Salto A La Nube La Computación En Los Cielos Virtuales. En: DEBATES IESA. Vol. XV., No 1 Enero, 2010.

FUTARO, Angelo; GARRO, Alfredo y TUNDIS, Andrea. Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing. En: 2014 International Carnahan Conference on Security Technology (ICCST)., Octubre, 2014.

G.ST.02 Guía de Computación en la nube [en línea]. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones. 2018., 44 p. Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html

GARCÍA DEL POYO, Rafael. Cloud Computing: Aspectos Jurídicos Clave Para la Contratación de Estos Servicios. En: Revista Española de Relaciones Internacionales. Núm. 4. ISSN 1989-6565., 2012.
GOOGLE CLOUD. Descubre lo que puedes lograr con Google Cloud. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://cloud.google.com
GRANCE, Timothy y MELL, Peter. The NIST Definition of Cloud Computing. En: NIST. Special Publication 800-145., Septiembre, 2011.
GRUNFELD, Bárbara y SCHCOLNIK, Alan. ¿Cloud computing?. En: IEEM Revista de Negocios., Junio, 2015.
GUTIÉRREZ, Horacio y KORN, Daniel. Facilitando "the cloud": la regulación de la protección de datos como motor de la competitividad nacional en América Latina. En: Revista La Propiedad Inmaterial no. 18., Universidad Externado de Colombia., Noviembre, 2014.
HUAWEI. Índice de Conectividad Global 2019. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://www.huawei.com/minisite/gci/en/
ISO-IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements.
ISO-IEC 22301:2012 Societal security - Business continuity management systems – Requirements.
ISO-IEC 27000:2018, Information technology - Security techniques - Information security management systems -- Overview and vocabulary.
ISO-IEC 27001:2013, Information Technology - Security Techniques - Information Security Management Systems - Requirements.
ISO-IEC 27002:2013, Information Technology - Security Techniques - Code Of Practice For Information Security Management.
ISO-IEC 27017:2015, Information Technology — Security Techniques - Code Of Practice For Information Security Controls Based On ISO/IEC 27002 For Cloud Services.
ISO-IEC 27018:2019, Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
ISO-IEC 29100:2011, Information technology -- Security techniques -- Privacy framework.
KATZ, Raúl. Informe del Observatorio De La Economía Digital De Colombia [en línea]. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones. 2017., 44 p. Disponible en https://www.mintic.gov.co/portal/604/articles-61929_recurso_4.pdf
LIU, Fang; TONG, Jin; MAO, Jian; BOHN, Robert; MESSINA, John; BADGER, Lee y LEAF, Dawn. NIST Cloud Computing Reference Architecture. En: NIST. Special Publication 500-292., Septiembre, 2011.
MANNER, Johannes; ENDREB, Martin; HECKEL, Tobias y WIRTZ, Guido. Cold Start Influencing Factors in Function as a Service. En 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion). 181-188., Diciembre, 2018.

MICROSOFT CLOUD. Azure. Invente con un objetivo. [en línea]. [Consultado el 20 de noviembre de 2019]. Disponible en: https://azure.microsoft.com/es-es
MORENO GOMEZ, Gonzalo Andrés. Jurisdicción Aplicable En Materia De Datos Personales En Los Contratos De Cloud Computing: Análisis Bajo La Legislación Colombiana. En: Revista de Derecho, Comunicaciones y Nuevas Tecnologías. No 9., Julio, 2013.
MORENO, Mario. Computación En La Nube. En: Documentos de Trabajo. No 566., Junio, 2015.
NADAF, Shameemraj; RATH, Hemant; ARUN KUMAR, A V; SHAILENDRA, Samar y SIMHA, Anantha. An open source based network as a service (NaaS) platform for cloud provisioning. En 2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)., Diciembre, 2015.
ONTSI. Cloud Computing: Retos y Oportunidades [en línea]. Madrid: Observatorio Nacional de las Telecomunicaciones y la SI. 2012., 55 p. Disponible en https://www.ontsi.red.es/ontsi/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf
PCI SECURITY STANDARDS COUNCIL. ABOUT US. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: https://www.pcisecuritystandards.org/about_us/
PRECIADO, Martha y VARGAS, Magna Luz. Guía de Contratación de Servicios en la Nube Para Empresas Públicas y Privadas en Colombia que Garantice un Correcto Análisis Forense Cuando se Presenten Incidentes se Seguridad. Trabajo de grado Especialización en Seguridad Informática. Bogotá: Universidad Piloto de Colombia, 2016.
TOESLAND, finbarr. C XAAS MODEL RESHAPES THE FUTURE OF OUTSOURCING. En: Computer Weekly., junio 2019.
UNIÓN EUROPEA. PARLAMENTO EUROPERO Y EL CONSEJO. Reglamento General de Protección de Datos. (4, mayo, 2016). El Parlamento. Unión Europea, 2016.
VARELA, Carlos; PORTELLA, Jorge y PALLARES, Luis. Computación en la nube: un nuevo paradigma en las tecnologías de la información y la comunicación. En: Revista Electrónica Redes de Ingeniería. edición especial., enero - junio 2017.

Contenido del documento:

- Resultados
- Conclusiones

Metodología:

La presente monografía está compuesta por cuatro fases, acordes con los objetivos específicos definidos. Inicialmente se realiza la introducción al concepto de Computación en la Nube, así como de los elementos y definiciones técnicas básicas que ayudan a entender la naturaleza del Cloud Computing.

Luego de entender los aspectos técnicos del Cloud Computing, se realiza el acercamiento a las normas técnicas de aceptación internacional sobre seguridad informática aplicables a la Computación en la Nube, así como de los reglamentos de Protección de Datos Personales y legislación colombiana adaptable a la prestación de un servicio de Cloud Computing dentro del territorio nacional.

En la fase número dos, se realiza análisis de los mecanismos de seguridad informática ofrecidos por una infraestructura Cloud Computing, mediante el estudio de las características propias de los tres principales proveedores de Cloud Computing con presencia en Colombia. Ahora, en la fase número tres, se analizan los aspectos del Cloud Computing en pequeñas y medianas empresas colombianas, con el fin de identificar beneficios, temores y riesgos propios de la implementación de este tipo de tecnología.

Por último, en la fase cuatro se realiza un análisis de las fases anteriores para identificar los resultados de la actividad y consolidar una conclusión sobre qué aspectos de seguridad se deben tener en cuenta para la implementación de una infraestructura en la nube.

Conceptos nuevos:

- CSP
- Multisesión
- Virtualización
- Escalabilidad y Elasticidad
- Infraestructura ‘On Premise’
- Modelos de Servicio
- Modelos de Despliegue
- Reglamento General de Protección de Datos
- Esquema de Responsabilidad Compartida
- Niveles de Seguridad
- Índice de Conectividad Global

Conclusiones:

La revisión de múltiples fuentes documentales para la construcción de la presente monografía permitió analizar los aspectos conceptuales básicos dentro de la implementación de servicios de Cloud Computing en pequeñas y medianas empresas colombianas; así como el conocimiento de las regulaciones legales aplicables, y del modelo de contratación y aspectos necesarios para la prestación transparente del servicio. Particularmente sobre el aspecto legal, se encontró que

Colombia aún tiene un largo camino por recorrer, ya que las regulaciones existentes no son específicas a Cloud Computing. A pesar de esto, se debe resaltar que la legislación colombiana si brinda garantías a las empresas y demás demandantes del servicio que utilizan Cloud Computing, ya que los CSP deben cumplir regulaciones muy claras aplicables a temas sensibles que trascienden a la nube, como lo es la Protección de Datos Personales.

En cuanto a los mecanismos y aspectos de Seguridad Informática de la Computación e la Nube, se encuentra que este es un aspecto transversal de la infraestructura en donde intervienen tanto el CSP como el consumidor final del servicio. Por lo tanto, la seguridad informática de Cloud Computing no depende únicamente de una buena infraestructura física y lógica provista por el CSP, sino también de las buenas prácticas de los clientes y consumidores finales. La infraestructura, herramientas y procesos de los CSP más conocidos en el país, y estudiados en el presente documento, demuestran que la arquitectura de los sistemas de información que implementan para el almacenamiento e intercambio de los datos está diseñada muy especialmente para evitar incidentes como la interceptación o alteración de datos, la suplantación de identidad o la denegación del servicio, aspectos vitales para la seguridad informática de cualquier pequeña o mediana empresa. A pesar de que el CSP es el encargado de la seguridad y estabilidad del servicio de Cloud Computing, no se resta responsabilidad a la empresa usuaria en establecer adecuadamente los planes de recuperación de desastres y continuidad del negocio, en aspectos como comunicaciones, energía y estado de los equipos de cómputo, así como de implementar las medidas necesarias para prevenir el acceso no autorizado a los servicios en la nube.

Si bien Cloud Computing ofrece múltiples ventajas, también es necesario tener en cuenta algunos riesgos, ya que esta infraestructura opera de manera distinta a como funcionan en las arquitecturas físicas tradicionales. El cliente sigue siendo dueño de la información, pero Cloud Computing genera pérdida del control sobre ciertos aspectos, como por ejemplo la proliferación y fragmentación de los datos en distintos países debido a las condiciones de respaldo de los datos, o desconocimiento de dónde está alojada la información, así como de las condiciones técnicas del procesamiento. Debido a que los datos salen del país de residencia del cliente, puede faltar claridad en cuanto a qué regulación normativa sobre tratamiento de datos personales, pueden aplicarse efectivamente dentro de la prestación del servicio. El uso de una infraestructura de Cloud Computing también genera dependencia del acceso a Internet, lo cual pondría en riesgo la operación de la empresa usuaria en el momento de una caída de la conectividad.

Cloud Computing ofrece a las pequeñas y medianas empresas la posibilidad de acceder a tecnología de punta para la ejecución de sus actividades diarias, haciendo una mínima inversión en infraestructura tecnológica, en donde todos los aspectos de implementación, actualización, mantenimiento, escalamiento y

recuperación de desastres a nivel de hardware o software son absorbidos por el CSP. Adicional, la implementación de Cloud Computing busca la reducción de la infraestructura física, con lo que hay un mejor aprovechamiento de los recursos energéticos y a reducción de la generación de desperdicios tecnológicos, lo que se traduce en que Cloud Computing apunta a ser una tecnología ambientalmente amigable. Cloud Computing también impulsa formas más eficientes de laborar dentro de las empresas, como por ejemplo la masificación del Teletrabajo, ya que permite que los funcionarios puedan acceder a todas las herramientas de trabajo desde cualquier computador y conexión a internet.
AUTOR: ADRIANA MARCELA TORRES GONZÁLEZ