# ASPECTOS DE SEGURIDAD INFORMÁTICA EN LA UTILIZACIÓN DE CLOUD COMPUTING

LUIS FELIPE GONZÁLEZ HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATÍCA
CÚCUTA
2016

# ASPECTOS DE SEGURIDAD INFORMÁTICA EN LA UTILIZACIÓN DE CLOUD COMPUTING

LUIS FELIPE GONZÁLEZ HERNÁNDEZ

Monografía de grado para optar el título de
Especialista en Seguridad Informática

Asesor
Esp. Ing. Freddy Enrique Acosta

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATÍCA
CÚCUTA
2016

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

San José de Cúcuta, Marzo 22 de 2016

## DEDICATORIA

Antes que todo quiero agradecer a Dios, por darme la vida y las fuerzas necesarias, para continuar mi recorrido profesional, superando todos los obstáculos que se me presentaron a lo largo de este proceso.

A mis padres porque siempre me motivaron por mejorar día tras día, buscando siempre conseguir todos los objetivos que me trace.

Luis Felipe González Hernández

## AGRADECIMIENTOS

Luis Felipe González Hernández expresa sus agradecimientos a:

Esp. Ing. Freddy Enrique Acosta por su importante orientación metodológica en el desarrollo de este proyecto monográfico; donde deseo destacar su disponibilidad, comprensión y conocimiento el cual sin duda alguna ha enriquecido el trabajo realizado.

Esp. Ing. José Miguel Herrán Suárez por su amable disposición y colaboración en todos los temas logísticos y administrativos, sin los cuales no hubiese podido llegar a buen puerto este proyecto debido a los distintos inconvenientes presentados en el camino.

Mag. Eduardo Buitrago, por su colaboración en las asesorías acerca de Cloud Computing y el diligenciamiento de la encuesta de valoración de amenazas.

Ing. Yesenia Arias, por compartir sus experiencias en el manejo de Cloud y brindarme de su tiempo para el diligenciamiento de la encuesta.

Ing. Argenis Gamboa, Ing. Uriel Claro, Ing. Leonardo Mora, Ing. Andrés Suarez, Ing. Juan Quiñones que me brindaron de su tiempo, y gestión para el diligenciamiento de la encuesta de amenazas de Cloud Computing.

A todas las demás personas que de una u otra forma contribuyeron para lograr cumplir con los objetivos trazados.

**CONTENIDO**

Pág

Pág

Pág

# LISTA DE TABLAS

## LISTA DE FIGURAS

## LISTA DE ANEXOS

## GLOSARIO

**Biometría:** es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos. En las tecnologías de la información (TI), la «autentificación biométrica» o «biometría informática» es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autentificación, es decir, "verificar" su identidad.[1]

**Datos sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.[2]

**Hipervisor:** el hipervisor, también llamado monitor de máquina virtual (VMM), es el núcleo central de algunas de las tecnologías de virtualización de hardware más populares y eficaces, entre las cuales se encuentran las de Microsoft: Microsoft Virtual PC, Windows Virtual PC, Microsoft Windows Server e Hyper-V.

Los hipervisores son aplicaciones que presentan a los sistemas operativos virtualizados (sistemas invitados) una plataforma operativa virtual (hardware virtual), a la vez que ocultan a dicho sistema operativo virtualizado las características físicas reales del equipo sobre el que operan.
Los hipervisores también son los encargados de monitorizar la ejecución de los sistemas operativos invitados.[3]

**Infostealer:** es un caballo de Troya, especialmente creado para robar información susceptible de los sitios Web bancarios. Se sabe que el Infostealer.Bancos se disfraza de Banco brasileño para secretamente obtener las contraseñas de los usuarios escogidos, y que se propaga a través de adjuntos contaminados en el correo electrónico que supuestamente proviene de Symantec. La empresa Symantec no está de ninguna manera involucrada con el Infostealer.Bancos[4]

---

[1] Goitchile, Biometría [online], Septiembre 2013, Disponible desde Internet: http://www.goit.cl/biometria.html
[2] LEY ESTATUTARIA 1581 DE 2012, Artículo 5 [online], Disponible desde Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
[3] Cloud Computing, Ángel Serran, Diapositiva 65 [online], Octubre 2013, Disponible desde Internet: http://es.slideshare.net/unhellsv/cloud-computing-26830463
[4] EnigmaSoftware, Infostealer.Bancos Descripción, [online], Disponible desde Internet: http://www.enigmasoftware.com/es/infostealerbancos-eliminar/

**Multi-Tenant:** se refiere a un principio en la arquitectura de software donde una única instancia del software se ejecuta en un servidor y al servicio a múltiples clientes (los arrendatarios).[5]

**Transport Layer Security:** seguridad de la Capa de Transporte. Consiste en un protocolo criptográfico que proporciona comunicaciones seguras a través de Internet. TLS es un protocolo independiente que permite a los protocolos de niveles superiores actuar por encima de él de manera transparente. Basado en SSL de Netscape 3.0, TLS supone la evolución de su predecesor, si bien no son operables entre sí.[6]

Trojan Horse (Caballo de Troya): los troyanos son una de las armas más fáciles que los piratas informáticos, en particular los script-kiddies, se pueden utilizar para hacer estragos en Internet. Un caballo de Troya es una herramienta destructiva que opera bajo la apariencia de un valioso programa o de entretenimiento. Caballos de Troya pueden ser virus o programas de control remoto que proporcionan un acceso completo a la computadora de la víctima, pueden ser instalados en un ordenador a través de un adjunto de correo electrónico destinado a ser abierto por la víctima[7].

**Secure Shell:** intérprete de órdenes segura. Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.[8]

**Secure Sockets Layer:** protocolo de Capa de Conexión Segura. Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.[9]

---

[5] Arquitecturas Multi-Tenant, Gravitar - Nora Macias [online], Octubre 2010, Disponible desde Internet: http://gravitar.biz/tecnologia-negocios/arquitecturas-multi-tenant/

[6] María Carmen España Boquera. (2003). Servicios avanzados de Telecomunicación 291-294 P., Recuperado de: https://books.google.com.co/books?id=yTSoYCiXYAAC&printsec=frontcover&dq=inauthor:%22Mar%C3%ADa+Carmen+Espa%C3%B1a+Boquera%22&hl=es&sa=X&ved=0ahUKEwiikZf_tqXLAhXGqx4KHdxNBYAQ6AEIGzAA#v=onepage&q&f=false

[7] SANS Institute, Crapanzano, Jaime, Deconstructing SubSeven, the Trojan Horse of Choice [online], 2003, Disponible desde Internet: https://www.sans.org/reading-room/whitepapers/malicious/deconstructing-subseven-the-trojan-horse-of-choice-953

[8] Marckoo Kroneer Raap, Tipos de Protocolos [online], Septiembre 2014, pp 12, Disponible desde Internet: http://www.ecured.cu/SSH

[9] Expresión Binaria, Seguridad en el protocolo SSL-TLS [online], Noviembre 2011, Disponible desde Internet: http://www.expresionbinaria.com/seguridad-en-el-protocolo-ssl-tls/

**Virtualización:** es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución.[10]

**Virtual Private Network:** una red privada virtual es una red privada que se extiende, mediante un proceso de encapsulación y en algún caso de encriptación, desde los paquetes de datos a diferentes puntos remotos, mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por un túnel definido en la red pública.[11]
**Zeus:** virus troyano Zeus v3 se ha dirigido a cuentas bancarias online.

[10] Luis Fernando Rodríguez, Virtualización, hacia el CPD inteligente de nueva generación [online], Julio 2010, Disponible desde Internet: http://www.techweek.es/virtualizacion/opinion/1006988005901/virtualizacion-cpd-generacion.1.html
[11] Universidad de Valencia, Qué es una red privada virtual (VPN)[online], Disponible desde Internet:http://www.uv.es/uvweb/servicio-informatica/es/servicios/generales/red-comunicaciones/red-privada-virtual-vpn-/-es-vpn-1285903202284.html

## RESUMEN

Esta monografía desarrolla a través de diferentes metodologías de investigación (búsqueda de documentación, entrevistas, entre otras) la identificación de las principales amenazas y vulnerabilidades a las cuales se está expuesto cuando se utiliza Cloud Computing, además de plantear estrategias de seguridad para la protección de los servicios en la nube, este desarrollo se enfocada hacia los profesionales de seguridad informática y personas en general interesadas en el tema de la seguridad brindada en Cloud Computing.

Igualmente resalta la importancia de la protección de los datos utilizando criptografía, ya que cuando utilizamos la nube como un sistema de almacenamiento de datos se recomienda emplear un nivel de cifrado adecuado para aquellos datos sensibles que vayan a ser depositados allí.

Por último teniendo en cuenta que Cloud Computing al igual que el manejo de los servicios TI locales, debe mantener la disponibilidad, confidencialidad e integridad de la información, por lo tanto se realiza una descripción de la normatividad existente en Colombia, resaltando la Ley 1581 de 2012 que regula los aspectos relativos al tratamiento de los datos personales y la libre circulación de los datos, buscando de esta manera brindar una orientación a las personas sobre los derechos que poseen al momento que se contratar esta tecnología.

## ABSTRACT

This document develops through different research methods (desk research, interviews, etc.) the identification of the main threats and vulnerabilities which are exposed when Cloud Computing is used, besides to raise security strategies for protection of cloud services, this development is focused on computer security professionals and the general public interested in the issue of security provided cloud computing.

Also the importance of data protection using encryption is highlighted, because when we use the cloud as a data storage system it is recommended that an appropriate level of encryption for sensitive data those that are to be deposited there.

Finally considering that Cloud Computing as the management of local IT services to maintain availability, confidentiality and integrity of information, therefore a description of the existing regulations in Colombia is made, highlighting the Law 1581 2012 which regulates aspects of the processing of personal data and the free movement of data, thereby seeking to give guidance to people about the rights they have when this technology contract

## INTRODUCCIÓN

Partiendo de la premisa que información es el activo más importante de toda organización no precisamente por su valor en los libros de contabilidad (puesto que no está contabilizada), sino por lo que representa la información, ya que esta, es indispensable para soportar la toma de decisiones, el control y el manejo de las operaciones de negocio de las organizaciones y como tal debe protegerse[12].
Esta monografía pone en contexto la seguridad brindada en la arquitectura Cloud Computing, resaltando las amenazas y vulnerabilidades a las cuales se expone, buscando brindar a los profesionales de la seguridad informática en general pautas de cómo mejorar los niveles de confianza al momento de utilizar esta arquitectura.

Es de resaltar que una de las amenazas más importantes que enfrenta la sociedad hoy en día con el avance tecnológico, es la pérdida del derecho a la intimidad[13], el interés del ser humano por mantener su vida personal de manera privada se ha incrementado de una manera exorbitante en los últimos años, debido al mal uso que se le ha dado al sin número de redes sociales que hoy se tienen a la disposición, es por esto que el gobierno colombiano ha establecido reglas que fundamentan y reglamentan la privacidad (intimidad), donde se establece que: "Nadie puede acceder a mis datos sin mi autorización para que los conozcan" (*Ley 1581 de 2012, Ley General de Protección de Datos Personales*).

Uno de los grandes retos que tiene hoy en día la sociedad, es la administración de la información que tiene bajo su poder, pero este desafío se incrementa aún más

---

[12] INTELCO, (2014, julio 22), SGSI 01 - Conceptos básicos sobre la Seguridad de la Información, [Archivo de Video], Disponible desde Internet: https://www.youtube.com/watch?v=oaRfwsj-jpk

[13] Derecho a la intimidad: Articulo 15 Constitución Política de Colombia establece lo siguiente:"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.
Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.
Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley."

cuando se utilizan servicio en la nube proporcionada por terceros. Por ello está monografía genera pautas para identificar las falencias que se están teniendo en el manejo de información, señalando las brechas de seguridad que pueden presentarse, tales como: riesgos de suplantación, APIs poco seguras, amenaza interna, fuga de información, desconocimiento y otras conductas que pueden llegar a comprometer el patrimonio de las personas afectadas.

Solo basta con observar el incremento en la utilización de Cloud Computing, esta viene creciendo a pasos acelerados y desde el punto de vista legal surgen un sinnúmero de temas y de interrogantes que se estudian dentro de esta monografía, todo con el propósito de conocer el entorno regulatorio en nuestro país y de esta manera poder exigir sobre los desarrollos y actividades realizadas en el manejo de esta tecnología, por porte de las empresas que brindan dicho servicio.

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1. PLANTEAMIENTO DEL PROBLEMA

El Global Cloud Index plantea aumento exponencial de servicios de almacenamiento en la nube por popularidad de apps y dispositivos móviles, por lo tanto en los próximos cinco años del tráfico de información en la nube en todas las regiones del mundo crecerá 30%, por lo que dejará de ser una tendencia y se convertirá en una solución mundial.

Los resultados del Cisco Global Cloud Index 2015-2019 indican que con el rápido crecimiento de la nube, el volumen de datos llegará a 507.5 zettabytes en 2019; 42.3 zettabytes producidos por mes, lo que sería 49 veces más de lo proyectado para data centers en 2019. [14]

Esto ha permitido establecer soluciones en el área de almacenamiento de información, además también admite la utilización de aplicaciones como por ejemplo Sistemas Operativos (OS), permitiéndoles eliminar la dependencia de servidores y aplicaciones locales, para almacenar información directamente en internet.

Los beneficios que ofrece este modelo son claros y muy atractivos: acceder a un servicio integral, eliminar las inversiones, diferir algunos costos y eliminar otros, incrementar la agilidad de las áreas de TI (Tecnología de Información), aumentar la movilidad de los usuarios, y mejorar la disponibilidad de los servicios[15].

Pero los males del crecimiento también se hacen sentir, en especial en un área tan sensible como es la seguridad. Hoy en día es cada vez más común oír hablar sobre las vulnerabilidades en este tipo de arquitecturas, por ejemplo uno de los problemas detectados radica en que un proveedor Cloud de software-as-a-service (SaaS)[16] necesita ver la información para lograr llevar a cabo sus operaciones.

Situaciones como por ejemplo, una aplicación de procesamiento de textos en línea debe ser capaz de leer el documento para poder ofrecer capacidades de corrección ortográfica, o un proveedor de almacenamiento en línea debe ser capaz de leer los documentos guardados para permitir a los usuarios buscar y encontrar lo que

---

[14] MARCO BUSTAMANTE, Crecimiento acelerado de servicios de nube, observa Cisco [online], octubre 2015, Disponible desde Internet: http://www.infochannel.info/crecimiento-acelerado-de-servicios-de-nube-observa-cisco

[15] K35, Una guía para entender qué es el "Cloud Computing" [online], 24 de mayo 2010, Disponible desde Internet: http://grupok35.blogspot.com.co/2010/05/una-guia-para-entender-que-es-el-cloud.html

[16] CIO AMERICA LATINA, Protegiendo la nube después de las filtraciones de la NSA [online], Disponible desde internet: http://www.cioal.com/2013/11/25/protegiendo-la-nube-despues-de-las-filtraciones-de-la-nsa/

necesitan. Este tipo de falencias puede originar que cualquier empleado, hacker o incluso una agencia gubernamental puedan sustraer una copia del documento.

Es importante tener en cuenta que atrás quedó el tiempo en que las amenazas informáticas eran producto y obra de muchachos rebeldes trabajando desde el garaje de la casa de sus padres, hoy el cibercrimen, no sólo pretende conseguir un beneficio principalmente económico, sino que también abarca el dominio de Internet como ataques con fines políticos, programas informáticos maliciosos, etc.[17]

La seguridad de la información es siempre uno de los puntos más importantes para tener en cuenta, especialmente en momentos de intensa transformación. Pero se observa que existe al tipo de desconocimiento por parte de algunos de los actores que utilizan esta arquitectura con relación a las amenazas que enfrentamos al utilizar Cloud Computing y se desestiman las vulnerabilidades que esta ha venido presentando en estos últimos años, lo cual generaría la imposibilidad de crear alternativas de protección y mitigación de riesgos, ocasionando brechas en la seguridad, que pueden generar la pérdida del activo más valioso de cualquier organización *"La Información"*[18].

No obstante se resalta que nuestro país cuente con normatividad debidamente establecida para el manejo de la información por parte de las empresas prestadoras de los servicios de Cloud, sin embargo la mayoría de las personas tienen un desconocimiento real sobre los derechos que tienen, y las garantías reales que ofrecen las leyes en cuanto a la manipulación de la información.

## 1.2. FORMULACIÓN DEL PROBLEMA

¿Se tiene un conocimiento efectivo de las principales amenazas y vulnerabilidades a los que nos enfrentamos al momento de utilizar Cloud Computing? ¿Podemos proteger la información al utilizar este servicio? ¿Tenemos conocimiento de la regulación –Normatividad y/o Leyes- existente en el país para Cloud Computing?

## 1.3. JUSTIFICACIÓN

La historia dicta que el hombre ha resguardado y protegido con celo sus conocimientos debido a la ventaja y poder que éste le producía sobre otros hombres o sociedades. En la antigüedad surgieron las bibliotecas, lugares donde se podía resguardar la información para trasmitirla y para evitar que otros la obtuvieran, dando así algunas de las primeras muestras de protección de la información.

---

[17]Discovery, El Cibercrimen, un crimen muy bien organizado [online], Disponible desde Internet: http://id.tudiscovery.com/el-cibercrimen-un-crimen-muy-bien-organizado/

[18] Tarazona Cesar H, Amenazas informáticas y seguridad de la información [online], Octubre 2013, Disponible desde Internet: http://es.slideshare.net/mariorafaelquirozmartinez/amenazas-informaticas-27228153

SunTzuenen el arte de la guerra y Nicolás Maquiavelo en el Príncipe, señalan la importancia de la información sobre los adversarios y el cabal conocimiento de sus propósitos para la toma de decisiones. Durante la Segunda Guerra Mundial se crean la mayoría de los servicios de inteligencia del mundo con el fin de obtener información valiosa e influyente, creándose grandes redes de espionaje y como forma de protección surge la contrainteligencia.[19]

En la actualidad un ataque bien organizado por un grupo de hackers puede afectar la infraestructura informática de un país o una organización. Donde podemos identificar amenazas en los siguientes sistemas:

- Transporte: Caos. La irrupción de hackers en sistemas aeroportuarios podría desbordar las operaciones aéreas y facilitar atentados

- Defensa: Vulnerabilidad. El robo de datos y la interrupción de sistemas de defensa pueden debilitar a un país ante un ataque real.

- Sistema financiero: Fraude. Existen riesgos de parálisis en los mercados y de comisión de fraude mediante el robo de datos bancarios.

- Utilities: Cortes en el suministro. La infiltración informática en los sistemas de una compañía de electricidad o de gas podría dejar en a ciudades enteras sin suministro[20]

Lo anterior conlleva a determinar que la seguridad siempre ha sido uno de los principales problemas en el ámbito de la transmisión de datos, y esto no ha sido la excepción el ámbito de la computación. Con la aparición del Cloud Computing y a medida que crece la popularidad de servicios en la Nube, dicho aspecto (seguridad) se ha convertido en un punto especialmente relevante, pues los datos del usuario pasan a estar almacenados en servidores ajenos, gestionados por proveedores que en un principio pueden no brindarnos un cien por cien de garantías en confiabilidad.[21]

Por lo tanto, en vista de la necesidad y para que todo profesional en el tema de seguridad cuente con una herramienta que pueda utilizar como base para

---

[19]Tescari, Jesus, Definición y Características de la Seguridad de la Información [online], 24 de Abril de 2011, Disponible desde Internet:http://749jesus.blogspot.com.co/2011/04/definicion-y-caracteristicas-de-la.html

[20] Marketing &Communications Specialist, Logicalis, seguridad informática en tiempos de Cloud Computing [online], Marzo 2011, Disponible desde Internet: http://www.br.promonlogicalis.com/globalassets/latin-america/logicalisnow/revista-13/2011-02-11-entrega18-logicalis-now-n13.pdf

[21]Gradiant, Seguridad y privacidad en cloud computing [online], Septiembre 2010, Disponible desde Internet: http://www.gradiant.org/es/actualidad/noticias/249-seguridad-y-privacidad-en-cloud-computing.html

determinar las vulnerabilidades de un servicio Cloud Computing y sus amenazas asociadas, y de esta forma aplicar una mejor y más aterrizada evaluación de sus riesgos.

Para tal efecto el desarrollo de una monografía que sirva de consulta tanto a los especialistas en el tema de seguridad, como a cualquier persona en general que utilice Cloud Computing. Esta podrá servir de base para establecer las principales amenazas, vulnerabilidades y algunas alternativas viables de protección y mitigación de riesgos, además de ilustrar las bases legales sobre las cuales podremos ampararnos, y lograr de esta manera señalar cuales son las obligaciones que deben cumplir los proveedores de este tipo de tecnología, en cuanto a los aspectos de seguridad y salvaguarda de la información.

Por ultimo vale la pena recordar que la seguridad de cualquier sistema se mide por el nivel de fragilidad del eslabón más débil, si no educamos a las personas, ni les damos las bases mínimas que deben tener en cuenta para el manejo de este tipo de servicio no se habrá hecho ninguna labor porque tendremos una gran puerta abierta hacia la perdida de nuestro activo más valioso ***"La Información"***.

## 1.4. OBJETIVOS

### 1.4.1. Objetivo General

Identificar las principales amenazas, vulnerabilidades y las alternativas para la protección de la información cuando se utiliza Cloud Computing.

### 1.4.2. Objetivos Específicos

- Determinar las principales amenazas y vulnerabilidades de inicio de sesión, y de acceso a los recursos asignados en Cloud Computing.
- Plantear estrategias de seguridad para la protección de los servicios en la nube que sirvan como guía para disminuir el riesgo a ataques de ingeniería social.
- Dar a conocer la legalidad y responsabilidad en cuanto a la información, a la que se encuentran sujetas las empresas prestadoras del servicio de Cloud Computing

## 1.5. ALCANCES Y LIMITACIONES

### 1.5.1 Alcances

Este proyecto está enfocado hacia los profesionales de seguridad informática y personas en general interesadas en el tema de la seguridad brindada en Cloud Computing, desarrollando un documento monográfico en el cual se encontraran los

ataques más relevantes (phishing, ingeniería social, explotación de las vulnerabilidades de software, Malicious Insiders), y vulnerabilidades de esta arquitectura, también se señalará la normatividad vigente en Colombia para la regulación y salvaguarda de la información por parte de las empresas prestadoras de este servicio.

### 1.5.2 Limitaciones

Aun cuando existe una gran cantidad de material relacionado con Cloud Computing una posible limitación que se prevé es el bajo nivel de información de calidad respecto a este tema particular. Es de señalar que el desarrollo de este proyecto es documental, por lo tanto no se realizaran pruebas de los distintos ataques que se puedan presentar en Cloud Computing.

## 1.6. DISEÑO METODOLÓGICO

La investigación se basa en el análisis de la seguridad brindada en el manejo de la arquitectura Cloud Computing, para el cumplimiento de los objetivos del proyecto se requerirá el planteamiento de una metodología de análisis que permita la extracción de conclusiones y recomendaciones a partir del estudio de fuentes y literatura existente en la materia, del análisis de opiniones expertas y de los resultados de una exploración realizada a diferentes entidades.

El enfoque metodológico que se presenta a continuación incluye, a modo de síntesis, los principales parámetros técnicos que se adoptaran para la realización del estudio. Se llevarán cabo tres procesos de análisis que aportan diferentes fuentes de información complementarias:

- Investigación documental de fuentes secundarias. El análisis de fuentes documentales nacionales e internacionales existentes sobre seguridad en Cloud Computing para permitir enfocar los conceptos clave del estudio y obtener información de relevancia para el desarrollo del presente trabajo.

- Investigación cualitativa. Realizar entrevistas en profundidad a expertos de seguridad, profesionales pertenecientes a diferentes entidades y con cargos de responsabilidad en el ámbito de seguridad informática.

- Investigación cuantitativa. Indagar acerca de las principales preocupaciones de seguridad que acarrea la implementación de la arquitectura Cloud Computing en las diferentes empresas.

Los resultados obtenidos a partir de las tres fuentes de información utilizadas permitirán obtener reflexiones, hipótesis y conclusiones, con los cuales se

estructurarán los principales apartados del informe. Así, el estudio constituirá una visión precisa de la percepción y estado de la seguridad del Cloud Computing.

### 1.6.1. Etapa 1: Análisis Documental

Con carácter previo al despliegue de los instrumentos metodológicos utilizados para la realización del trabajo de campo, se analizarán las principales fuentes bibliográficas, revistas especializadas, noticias, blogs de opinión e información en la red relativa al contexto y fundamentos de la seguridad en Cloud Computing a nivel nacional e internacional. El análisis documental previo se encaminará de la siguiente forma:

Precisar los conceptos fundamentales, términos y aspectos básicos de seguridad en Cloud Computing y consolidar un glosario de términos y conceptos que se utilizarán en todo el ámbito del estudio.

Analizar estudios internacionales realizados acerca de la materia de estudio, con objeto de identificar los principales ejes de seguridad valorados por otros autores y expertos.

Conocer la normatividad nacional e internacional para el manejo de la información en la arquitectura de Cloud Computing.

Identificar prácticas comunes en cuanto al manejo de la seguridad en Cloud Computing.

Conocer la perspectiva y opiniones de los profesionales en seguridad, a cerca delas amenazas, vulnerabilidades y alternativas de seguridad Cloud Computing: informes prospectivos de empresas de consultoría, afirmaciones de responsables de la protección de Datos, etc.

### 1.6.2. Etapa 2: Entrevistas a Profesionales y Expertos

En esta fase se buscará la opinión de agentes con amplio conocimiento en la materia de seguridad informática, con los que se seguirá una metodología de investigación cualitativa basada en la realización de entrevistas. Todos los expertos buscados serán aquellos que conozcan a profundidad los temas relacionados con la seguridad en Cloud Computing, además de aquellos que tengan experiencias reales y efectivas sobre el análisis, diseño o implantación de alternativas de seguridad en Cloud.

### 1.6.3. Modelo de Recopilación y Explotación de la Información Resultante

La obtención de la base de datos definitiva tras las etapas de trabajo de campo y tratamiento previo de la información (depuración, codificación y validación) será el punto de partida para su análisis estadístico de cara a la obtención de resultados que contribuyan a esclarecer todas las cuestiones planteadas al inicio del proceso de la investigación.

Finalmente, los datos resultantes del proceso de análisis serán sintetizados y representados a través de modelos gráficos, indicadores simples y estadísticos que facilitarán la interpretación de los resultados y la formulación de hipótesis y conclusiones.

Entre los principales elementos de representación estadística que se utilizarán se encuentran las tablas de distribución de frecuencia y representaciones gráficas.

# 2. MARCO REFERENCIAL

El contenido de este marco se focaliza en una descripción de Cloud Computing específicamente orientada a la perspectiva concreta de los profesionales de seguridad y de networking TI.

## 2.1. MARCO TEORICO

### 2.1.1. Cloud Computing

La computación en nube (Cloud Computing) es un sistema informático basado en Internet y centros de datos remotos utilizados para gestionar servicios de información y aplicaciones. Los usuarios de este servicio tienen acceso de forma gratuita o paga, dependiendo del servicio que se necesite usar.

El término “nube” se utiliza como una metáfora de Internet y se origina en la nube utilizada para representar Internet en los diagramas de red como una abstracción de la infraestructura que representa.

El término es una tendencia que responde a múltiples características integradas. Uno de los ejemplos de está “nube” es el servicio que presta Google Apps que incorpora desde un navegador hasta el almacenamiento de datos en sus servidores. Los programas deben estar en los servidores en línea y puedas acceder a los servicios y la información a través de internet.

La computación en nube permite que los consumidores y las empresas gestión en archivos y utilicen aplicaciones en cualquier computadora con acceso a Internet sin necesidad de instalarlas.

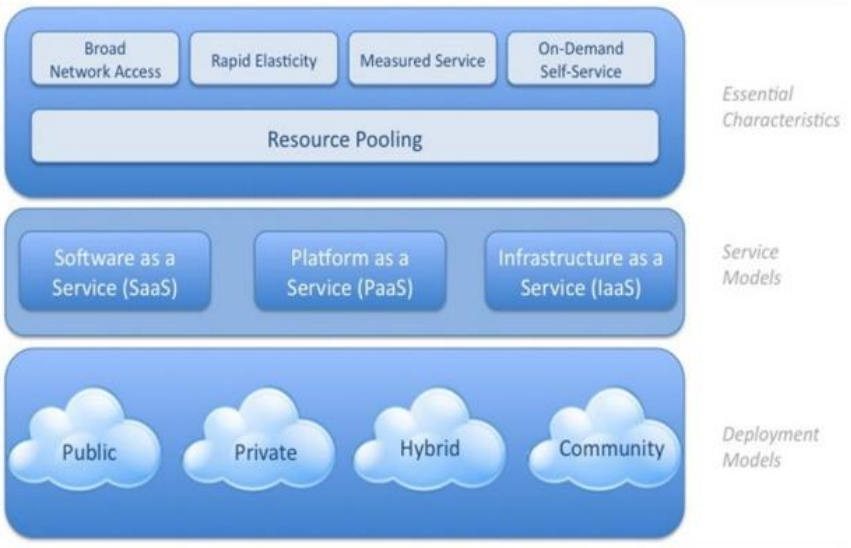
Esta tecnología ofrece un uso mucho más eficiente de recursos, como almacenamiento, memoria, procesamiento y ancho de banda, al proveer solamente los recursos necesarios en cada momento.

El servidor y el software de gestión se encuentran en la nube (Internet) y son directamente gestionados por el proveedor de servicios. De esta manera, es mucho más simple para el consumidor disfrutar de los beneficios. En otras palabras: la tecnología de la información se convierte en una servicio, que se consume de la misma manera que consumimos la electricidad o el agua[22]

[22] CENTRO DEL VALLE, Que Es La Computación En La Nube?, [online], 2015, Disponible desde Internet: http://centrodelvalle.com/webs/homepage/index.php/blog/item/16-que-es-la-computacion-en-la-nube

El NIST (National Institute of Standards and Technology) define Cloud Computing mediante la descripción de cinco características esenciales, tres modelos de servicio en Cloud y cuatro modelos de despliegue para Cloud[23]. Figura 1.

Figura 1. Modelo definición Cloud Computing del NIST.




Fuente. Cloud Security Alliance.[24]

La principal característica de Cloud Computing es el acceso ubicuo (desde cualquier lugar) a los datos. Solo se necesita un navegador web y conexión a Internet para disfrutar de los servicios en la nube, no hace falta tener un sistema operativo determinado o instalar un software específico en cada cliente. Se puede utilizar un portátil, un teléfono móvil o una videoconsola conectado a la red para acceder a las aplicaciones de la nube en cualquier momento.[25]

### 2.1.2. Características Esenciales de Cloud Computing

- **Auto-servicio por demanda:** Un consumidor puede aprovisionar de manera unilateral capacidades de cómputo, tales como tiempo de servidor y almacenamiento en red, en la medida en que las requiera sin necesidad de interacción humana por parte del proveedor del servicio.

[23] Timothy Grance, Peter Mell, The NIST Definition of Cloud Computing [online], Septiembre 2011, Disponibledesde Internet: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[24]Cloud Security Alliance, Guías de Seguridad de áreas Críticas en Cloud Computing [online], 2011, Disponible desde Internet: https://www.ismsforum.es/ficheros/descargas/guia-csa1354629608.pdf
[25]INTECO, seguridad y privacidad del Cloud Computing [online], 2011, Recuperado desde Internet: http://www.inteco.es/file/2KMNG7mbyKb6gqdnJquPKw

- **Acceso amplio desde la red:** Las capacidades están disponibles sobre la red y se acceden a través de mecanismos estándares que promueven el uso desde plataformas clientes heterogéneas, pesadas o livianas, como el PC, un teléfono móvil o un navegador Internet.[26]

- **Conjunto de recursos:** Los recursos computacionales del proveedor se habilitan para servir a múltiples consumidores mediante un modelo "multi-tenant", con varios recursos tanto físicos como virtuales asignados y reasignados de acuerdo con los requerimientos de los consumidores. Existe un sentido de independencia de ubicación en cuanto a que el consumidor no posee control o conocimiento sobre la ubicación exacta de los recursos que se le están proveyendo aunque puede estar en capacidad de especificar ubicación a un nivel de abstracción alto; por ejemplo, país, estado o centro de datos.

- **Rápida elasticidad:** Las capacidades pueden ser rápidamente y elásticamente aprovisionadas, en algunos casos automáticamente, para escalar hacia fuera rápidamente y también rápidamente liberadas para escalar hacia dentro también de manera veloz. Para el consumidor, estas capacidades disponibles para aprovisionar a menudo aparecen como ilimitadas y pueden ser compradas en cualquier cantidad en cualquier momento.

- **Servicio medido:** Los sistemas en la nube controlan automáticamente y optimizan el uso de recursos mediante una capacidad de medición a algún nivel de abstracción adecuado al tipo de servicio; por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas. El uso de estos recursos puede ser monitoreado, controlado y reportado, proporcionando transparencia tanto para el proveedor como para el consumidor por el servicio utilizado.[27]

### 2.1.3. Modelos de Servicio en la Nube

- **Infrastructure as a Service (IaaS):** Ofrece una infraestructura computacional (normalmente un entorno de virtualización de plataforma) como un servicio, junto con almacenamiento puro y gestión de la red. En lugar de comprar servidores, software, espacio en el CPD, o equipos de red,

---

[26] Sandetel, Cloud Computing [online], 2012, Disponible desde Internet:http://www.juntadeandalucia.es/presidencia/portavoz/resources/files/2013/1/4/1357297921586analisis_cloud_computing.pdf

[27]Reyes G, Marco A., Ernesto González G,Manual de Arquitectura y Estándares de Tecnología de Información y Comunicaciones [online], Julio 2014, Disponible desde Internet:http://dgsei.edomex.gob.mx/sites/dgsei.edomex.gob.mx/files/files/C%C3%B3mputo%20en%20la%20nube%20V%201%203.pdf

los clientes compran esos recursos como un servicio totalmente externalizado.[28]

- **Software as a Service (SaaS):** La capacidad de cómputo proporcionada al usuario, es el uso de las aplicaciones del proveedor que se encuentran en ejecución en la infraestructura Cloud. Las aplicaciones son accesibles desde varios dispositivos de usuario a través de interfaces sencillas, como un navegador web (ej. Web mail), o una aplicación de escritorio. El usuario no administra o controla la infraestructura subyacente sobre la cual se ejecuta, como hardware, servidores, sistemas operativos, almacenamiento o capacidades de control sobre la aplicación; con la posible excepción de preferencias de configuración de la aplicación para específicas para el usuario.

- **Platform as a service (PaaS):** La capacidad de cómputo proporcionada al usuario es la de despegar aplicaciones adquiridas o creadas por el usuario, usando lenguajes, librerías, servicios y herramientas soportadas por el proveedor. El usuario no administra o controla la infraestructura subyacente sobre la cual se ejecuta, incluyendo redes, servidores, sistemas operativos o almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente sobre las preferencias de configuración del entorno de ejecución de la aplicación.[29]

### 2.1.4. Modelos de Implementación

- **Cloud Pública**. La infraestructura Cloud está a disposición del público en general o a disposición de un grupo industrial grande y es propiedad de una organización que comercializa servicios Cloud.

- **Cloud Privada**. La infraestructura Cloud es operada únicamente por una sola organización. Puede ser gestionada por la organización o por un tercero y puede estar ubicada en las instalaciones o fuera de ellas.

- **Cloud Comunitaria**. La infraestructura Cloud es compartida por varias organizaciones y da soporte a una comunidad específica que ha compartido preocupaciones (por ejemplo, misión, requisitos de seguridad, política o consideraciones de cumplimiento legal). Puede ser gestionada por las

[28]Cloud Security Alliance, Guías de Seguridad de áreas Criticas en Cloud Computing [online], 2011, Disponible desde Internet: https://www.ismsforum.es/ficheros/descargas/guia-csa1354629608.pdf

[29]Diaz Carreño, Emmanuell. Modelo y prototipo de servicios de computación en la nube para estudiantes y profesores de la escuela de ingeniería de sistemas e informática de la Universidad Industrial de Santander. Trabajo de Grado Ingeniero de Sistemas. Bucaramanga: Universidad Industrial de Santander. Facultad de Ingenierías Físico-Mecánicas, 2012. 28-29 p.

organizaciones o por un tercero, y puede estar ubicada en las instalaciones o fuera de ellas.

- **Cloud Híbrida**. La infraestructura Cloud es una composición de dos o más Clouds (privada, comunitaria o pública) que siguen siendo entidades únicas pero están unidas por tecnología estandarizada o propietaria que permite la portabilidad de datos y de la aplicación (por ejemplo, proliferación de Clouds para balanceo de carga entre Clouds).[30]

### 2.1.5. Ventajas y Desventajas del Cloud Computing

Entre las ventajas de Cloud Computing puedo mencionar:

- Acceso a la información y los servicios desde cualquier lugar. El sistema en nube está diseñado para ser utilizado a distancia, así que el personal de la empresa tendrá acceso a la mayoría de los sistemas en cualquier lugar donde se encuentre.

- Rápido: Los servicios más básicos de la nube funcionan por sí solos. Para servicios de software y base de datos más complejos, la computación en nube permite saltarse la fase de adquisición de hardware y el consiguiente gasto, por lo cual es perfecta para la creación de empresas.

- Actual: La mayoría de los proveedores actualizan constantemente su software, agregando nuevas funciones tan pronto como están disponibles.

- Empresas con facilidad de escalabilidad: Adaptable rápidamente a negocios en crecimiento o de picos estacionales, ya que el sistema en nube está diseñado para hacer frente a fuertes aumentos en la carga de trabajo. Esto incrementa la agilidad de respuesta, disminuye los riesgos y los costos operacionales, porque sólo escala lo que crece y paga sólo lo que usa.

- Mínima inversión en infraestructura: El proveedor ofrece servicios a varias empresas, las cuales se benefician de compartir una infraestructura compleja y pagan solamente por lo que realmente utilizan.

- Actualizaciones automáticas que no afectan negativamente a los recursos de TI. Si actualizamos a la última versión de la aplicación, nos veremos obligados a dedicar tiempo y recursos (que no tenemos) a volver a crear nuestras personalizaciones e integraciones. La tecnología de "Cloud Computing" no le obliga a decidir entre actualizar y conservar su trabajo,

[30] ICIC, Que es el Cloud Computing, [online], Disponible desde Internet: http://www.internetsano.gob.ar/archivos/cloudcomputing_empresas.pdf

porque esas personalizaciones e integraciones se conservan automáticamente durante la actualización.[31]

Entre las desventajas se pueden mencionar:

- La centralización de las aplicaciones y el almacenamiento de los datos originan una interdependencia de los proveedores de servicios.

- La disponibilidad de las aplicaciones está ligada a la disponibilidad de acceso a Internet.

- Los datos "sensibles" del negocio no residen en las instalaciones de las empresas por lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.

- La confiabilidad de los servicios depende de la "salud" tecnológica y financiera de los proveedores de servicios en nube. Empresas emergentes o alianzas entre empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.

- Seguridad. La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que estos requieren.

- Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio[32].

### 2.1.6. Seguridad para Cloud Computing

En su mayor parte, los controles de seguridad en Cloud Computing no son diferentes de los controles de seguridad en cualquier entorno de TI. Sin embargo, debido a los modelos de servicios Cloud utilizados, los modelos operativos y las tecnologías que se utilizan para habilitar servicios Cloud, pueden presentar riesgos para una organización diferentes a los de las soluciones de TI tradicionales.

---

[31] ONTSI, Cloud Computing Retos y Oportunidades [online],Mayo 2012, Disponible desde Internet: http://www.ontsi.red.es/ontsi/sites/default/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

[32] Centro i-CREO. Cloud Computing, [online], 2013, Disponible desde Internet: http://www.femeval.es/informesymanuales/Documents/i-CREO%20CLOUD%20COMPUTING/files/cloud%20computing.pdf

La utilización de los servicios en la nube conlleva un cambio en la forma de entender la seguridad informática. Deja de existir la imagen tradicional en la que todos los servicios de la empresa están en el sótano del edificio donde solo pueden acceder los administradores informáticos.
Al hacer uso del Cloud Computing una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.[33]

### 2.1.7. Virtualización y Cloud Computing

Sistemas de virtualización: Hypervisores

Hypervisor o Virtual Machine Monitor (VMM) es una tecnología que está compuesta por una capa de software que permite utilizar, al mismo tiempo, diferentes sistemas operativos o máquinas virtuales (sin modificar o modificados en el caso de para virtualización) en una misma computadora central. Es decir es la parte principal de una máquina virtual que se encarga de manejar los recursos del sistema principal exportándolos a la máquina virtual

El VMM (Virtual Machine Monitor) crea una capa de la abstracción entre el hardware de la maquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), de tal forma que maneja los recursos de las maquinas físicas subyacentes (designadas por el computador central) de una manera que el usuario pueda crear varias máquinas virtuales presentando a cada una de ellas una interfaz del hardware que sea compatible con el sistema operativo elegido.

Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. En la actualidad todos los fabricantes tanto de Software como de Hardware están trabajando para mejorar, ayudar al Hypervisor (VMM) y así poder llegar a una virtualización completa, fiable y robusta.[34]

La Virtualización es un elemento fundamental del Cloud Computing y ayuda a darle valor al Cloud Computing" explica Adams "El Cloud Computing consiste en la entrega de recursos informáticos compartidos a través de software o datos y que son entregados como un servicio de demanda a través de Internet".[35]

---

[33]INTECO, seguridad y privacidad del Cloud Computing [online], 2011, Recuperado desde Internet: http://www.inteco.es/file/2KMNG7mbyKb6gqdnJquPKw
[34] El Magazine de la Virtualización & Cloud Computing, VIRTUALIZACION [online], 2004, Disponible desde Internet: http://www.virtualizacion.com/hypervisor/
[35] Guilarte, María, 2014, Virtualización y cloud computing [online], Disponible desde Internet: http://muycloud.com/2014/01/21/virtualizacion-cloud-computing/

## 2.2. MARCO LEGAL

### 2.2.1 Ley Regulatoria Colombia

Cloud Computing tiene su principal fundamento en la gestión remota de la información. Las organizaciones transfieren gran cantidad de información, en algunos casos sensible, en servidores pertenecientes a terceros.

La Ley 1581 de 2012 regula los aspectos relativos al tratamiento de los datos personales y la libre circulación de los datos[36]. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejerce la vigilancia para garantizar que en el Tratamiento de datos personales, se respeten los principios, derechos, garantías y procedimientos previstos en esta ley.

El Decreto 886 DE 2014[37]. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo Régimen General de Protección de Datos Personales. El Ministerio de comercio, industria y turismo, como autoridad de protección de las bases de datos personales establece en el registro nacional de bases de datos información adicional, tales como:

- Datos de identificación de los responsables y encargados del tratamiento de las bases de datos.
- Canales para que los titulares ejerzan sus derechos.
- Forma de tratamiento.
- Política de tratamiento de la información ya sea manual o automatizada.

El Decreto 1377 de junio de 2013[38] tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros:

- El anuncio como tal (y a los cinco días siguientes de la comunicación, enviar carta comunicándole al respecto a la Superintendencia de Industria y Comercio).

---

[36] LEY ESTATUTARIA 1581 DE 2012 [online], Disponible desde Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[37] DECRETO 886 DE 2014 [online], Disponible desde Internet: http://www.gesdatos.co/wp-content/uploads/DECRETO-886-DEL-13-DE-MAYO-DE-2014.pdf

[38] DECRETO 1377 DE 2013 [online], Disponible desde Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0

- Formato de autorización para que si lo desean lo diligencien los titulares de datos recolectados previamente.

- Determinación de canal electrónico y físico para recibir las autorizaciones.

- Política de tratamiento de la información personal (pues esta se debe indicar en el anuncio).

- Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión.

### 2.2.2 Leyes Regulatorias en Argentina

En Argentina, en Junio del 2008 se promulgó la ―Ley No 26388‖ (56) con reformas al Código Penal modificando delitos existentes e incluyendo el alcance de los términos documento, firma, suscripción, instrumento privado y certificado, y de esta manera contemplar el uso de nuevas tecnologías. Esta reforma contempló los siguientes delitos: La pornografía infantil mediante el uso de internet u otros medios digitales, el robo y acceso no autorizado de información almacenada digitalmente, fraude y sabotaje informático, interferencias en comunicaciones.[39]

### 2.2.3 Leyes Regulatorias en Chile

Es el primer país latinoamericano en expedir una ―Ley contra los delitos informáticos, Ley 19223 del 28 de Mayo de 1993, la cual consta de cuatro artículos en los que se castigó conductas ilícitas como: la inutilización o destrucción de un sistema de tratamiento de información o sus componentes afectando el correcto funcionamiento del sistema, al igual que la interferencia, intercepción o acceso a un sistema de información con el fin de apoderarse de datos almacenados en el mismo, también sancionó el daño o destrucción de datos, así como la revelación o difusión de datos contenidos en un sistema de una manera malintencionada.[39]

### 2.2.4 Leyes Regulatorias España

Ley de Protección de Datos (LOPD)

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal regula los aspectos relativos al tratamiento de datos personales y su libre circulación. En nuestro país existe la AEPD que es la Agencia Española de Protección de Datos, el órgano de control que se encarga de garantizar el cumplimiento de la normativa.

[39] Calderón R, Guzmán G, Salinas J. (2011). Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario. Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

Si la empresa contratada va a trabajar con datos personales de la empresa o persona contratante, debe cumplir con una serie de obligaciones que marca la LOPD:

- Inscripción de ficheros.
- Deberes relacionados con la información en la recogida, el consentimiento y la calidad de los datos.
- Garantía de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
- Adopción de medidas de seguridad.

Ley de Servicios de la Sociedad de la Información (LSSI)

Las empresas que se dedican a temas relacionados con el Cloud Computing son prestadores de servicios de la sociedad de la información por lo que deben cumplir una serie de requisitos marcados por la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI).

Así pues, según la LSSI, los proveedores de servicios relacionados con la sociedad de la información deben informar a sus clientes de forma fácil, directa y gratuita sobre los siguientes temas:

- Los medios empleados para garantizar y aumentar la seguridad de la información del cliente, tales como programas antivirus, anti espías y filtros de correo electrónico si fueran necesarios.

- Las medidas de seguridad que se aplican en el servicio prestado.

- Las herramientas que existen para el filtrado y/o la restricción del acceso a determinados contenidos y servicios de Internet no deseados por el cliente.

- Las responsabilidades en que se puede incurrir por el uso ilícito de la Red.[40]

### 2.2.5 Leyes Regulatorias Estados Unidos

Normas como la Children's Online Privacy Protection Act (COPPA), la Gramm-Leach-Bliley Act (GLBA) y el Computer Fraud and Abuse Act (CFAA) entre otras regulaciones aplicables en función del mercado o sector económico en el cual se utilizan los datos, aseguran la jurisdicción basadas en la ubicación del titular de la información, a quien se le debe proteger su información personal, así esta fuese

[40]MakeSoft, Marco legal del Cloud Computing: la Ley de Protección de Datos, [online], Disponible desde Internet: http://www.makesoft.es/es/marco-legal-del-cloud-computing-la-ley-de-proteccion-de-datos/

trasferida de servidores localizados en Estados Unidos a territorio extranjero a partir de la tecnología Cloud Computing (Reingold, Mrazik, D´Jaen, Febrero 2010, p. 3). De este modo, se sigue que la información que fuera entregada a una compañía en Estados Unidos, sin importar donde se encuentre en ese momento, deberá ser protegida bajo las normas de los Estados Unidos.

Ahora bien, la posición anteriormente expuesta presenta problemas en el efectivo cumplimiento de la jurisdicción, en el supuesto que los datos se encuentren fuera del territorio de los Estados Unidos. Esto se debe a que sólo cuando un proveedor tenga activos físicos en una jurisdicción las autoridades de ésta podrán ejercer de forma efectiva la competencia judicial o administrativa en contra del proveedor (Kyer, & Stern, 2011, p. 7). En caso contrario, sería muy complejo para los ejecutores de la ley, resultando necesaria la implementación de tratados internacionales con el fin de proteger los datos personales (Reingold, Mrazik, D´Jaen, Febrero 2010, p. 4)[39].

**La Ley SOPA (Stop Online Piracy Act)**

Es un proyecto de ley que extiende las competencias del Departamento de Justicia de Estados Unidos para combatir el tráfico online de contenidos.

El Stop Online Piracy Act (Alto a la piratería en línea) también conocido como Ley SOPA o Ley H.R. 3261; es un proyecto de ley presentado en la Cámara de Representantes de los Estados Unidos el 26 de octubre de 2011 por el representante Lamar S. Smith, y un grupo de copatrocinadores bipartidario formado inicialmente por 12 miembros.

El proyecto de ley extiende las competencias del Departamento de Justicia de los Estados Unidos y amplía las capacidades de los propietarios de derechos intelectuales para combatir el tráfico online de contenidos y productos protegidos, ya sea por derechos de autor o de propiedad intelectual.

Entre estos se pueden contar, por ejemplo, música o canciones, películas, libros, obras artísticas y productos copiados o falsificados que no tributan las correspondientes tasas a los propietarios de sus derechos de autoría o invención.
El proyecto de ley originalmente propuesto permite que tanto el Departamento de Justicia de los Estados Unidos, como los propietarios de derechos intelectuales, puedan obtener órdenes judiciales contra aquellos sitios de Internet que permitan o faciliten la violación de los derechos de autor. Dependiendo de quién sea el que solicite la orden judicial, las acciones previstas contra el sitio web podrían incluir:

- Restricción al acceso a empresas que brindan un servicio de facilitación de pago tales como PayPal o que ofrecen dinero a cambio de colocar publicidad online.

- Restricción en los buscadores que vinculan con tales sitios.

- Requerimiento a los proveedores de internet, para que bloqueen el acceso a tales sitios.

El proyecto de ley convierte en un crimen al streaming no autorizado de contenidos protegidos por copyright (derecho de copia), y prevé una pena máxima de cinco años de prisión por cada diez piezas musicales o películas descargadas dentro de los seis meses desde su estreno.

El proyecto además brinda inmunidad a todos aquellos proveedores de Internet que voluntariamente lleven a cabo acciones contra tales sitios haciendo además responsable al sitio web infractor de cualquier daño producido al titular de los derechos, incluso sin tener que demostrarlo[41].

**La PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, también conocida como PIPA)**

Es un proyecto de ley que tiene por objetivo declarado el brindar al gobierno de los Estados Unidos y a los titulares de derechos de autor herramientas adicionales para restringir el acceso a aquellos «Pícaros sitios web dedicados a infringir o falsificar bienes», en especial aquellos sitios registrados fuera del territorio de los Estados Unidos.

El proyecto fue introducido el 12 de mayo de 2011, por el Senador demócrata Patrick Leahy (político) y un grupo bipartito de 11 promotores. La Oficina Presupuestaria del Congreso estimó que la implementación del proyecto de ley podría haberle costado al gobierno de los Estados Unidos una suma estimada hasta finales del 2016 de 47 millones de dólares; esta suma se habría utilizado para cubrir los costos de ejecución y para la contratación y capacitación de 22 nuevos agentes especiales y 26 empleados de apoyo. El Comité Judicial del Senado de los Estados Unidos aprobó la ley, pero el Senador Ron Wyden logró ponerla en suspenso.

La ley PIPA es una versión reescrita del proyecto Combating Online Infringement and Counterfeits Act (COICA) que no logró ser aprobada en el 2010. Un proyecto similar fue presentado ante el Congreso de los Estados Unidos el 26 de octubre del 2011, la Stop Online Piracy Act (SOPA).

El proyecto define como conducta infractora a la distribución de copias ilegales, bienes falsificados, o tecnología que permita evadir las protecciones anti copia. La

[41] Ayala Acero, Angie, Informática Jurídica Y Derecho Informático, , Marzo 2015 [online], Disponible desde Internet: http://ayalaaceroangie.blogspot.com.co/2015/03/ley-sopa-ley-pipa-cierre-de-upload-y.html

infracción existe si «los hechos o circunstancias sugieren que -el medio o mecanismo- es utilizado, primariamente como medio para participar, permitir o facilitar las actividades descritas». El proyecto de ley dice que no altera las leyes de copia o productos registrados existentes.

El proyecto está pensado para proveer «mejoras en la aplicación contra sitios web operados y registrados en el extranjero» y autoriza al Departamento de Justicia de los Estados Unidos a obtener órdenes judiciales in rem (de restitución) contra sitios web dedicados a actividades infractoras, si es que por medio de una debida diligencia, no fuera posible localizar a un individuo que conste como propietario u operador del sitio.

El proyecto requiere que el Fiscal general de los Estados Unidos notifique al demandado. Una vez que la corte publique una orden, esta puede ser utilizada para requerir a los proveedores de servicios financieros, servicios de avisos publicitarios en Internet, proveedores de servicios de Internet y herramientas para localizar información, que cesen de realizar transacciones financieras con el sitio infractor y remuevan los enlaces que vinculan con el mismo.[42]

### 2.2.6 Leyes Regulatorias Alemania

La ley federal de protección de datos especifica la adquisición, procesamiento y almacenamiento de datos personales. En dicha norma los datos personales sólo podrán ser trasmitidos a países que tengan igual o mayor protección sobre los datos, con la característica específica de que si se traslada la información a un tercero, se le debe comunicar directamente a los involucrados (Doelitzscher, Reich & Sulistio, 2010, p. 931)[43].

## 2.3. ESTADO DEL ARTE

Serrano Latorre, Jairo D Heymann Pignolo, Elisa, César Galo bardes, Eduardo, UniversidadAutónoma De Barcelona. Departament D'Arquitectura De Computadors I Sistemes Operatius, Septiembre 30 de 2013, Vulnerability Assessment for Complex Middleware Interrelationships in Distributed Systems, Este estudio revela la rápida adaptación de Cloud Computing, y como esta ha llevado a un incremento veloz en la tasa de amenazas de las tecnologías de la información. Se demuestra cómo el objetivo de estas nuevas amenazas cubren desde sistemas distribuidos a

[42] Ayala Acero, Angie, Informática Jurídica Y Derecho Informático, , Marzo 2015 [online], Disponible desde Internet: http://ayalaaceroangie.blogspot.com.co/2015/03/ley-sopa-ley-pipa-cierre-de-upload-y.html

[43] Moreno Gómez, Gonzalo Andrés, Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana, Junio 2013 [online], Disponible desde Internet: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Jurisdiccion-y-cloud-Gonzalo-Moreno-2013.pdf

gran escala, tal como el Gran Colisionador de Partículas del CERN, hasta sistemas industriales (plantas nucleares, de electricidad, petróleo, etc.) distribuidos, es decir sistemas interconectados SCADA, y como el uso de herramientas automáticas para el análisis de vulnerabilidades es realmente atractivo, pero mientras que estas herramientas pueden encontrar problemas comunes en el código fuente de un programa, estas no detectan un número significativo de vulnerabilidades críticas y complejas. [44]

María de los Ángeles López, Diana Ester Albánese, Marisa Analía Sánchez, Universidad Nacional del Sur, Abril 12 de 2013, Gestión de riesgos para adopción de la computación en nube en entidades financieras de la República Argentina, En este estudio analiza que la utilización de estas arquitecturas es fundamental considerar los nuevos riesgos a los que se exponen los entes; esto permite desarrollar estrategias de gestión destinadas a identificarlos, evaluarlos y buscar el modo de minimizar sus efectos. Se muestra la utilidad de las herramientas como la Risk Breakdown Structure (RBS), una estructura de jerarquización de fuentes de riesgos que simplifica y sistematiza el análisis. En este trabajo diseña una RBS para la identificación y descripción jerárquica de las fuentes de riesgos vinculados a la implementación de la computación en nube.

Serrano Pérez, Sergio, Universidad Politécnica De Catalunya. Departament D'arquitectura De Computadors, 2011, Uso de servicios de seguridad y confianza desde la nube: TrustedX y la Plataforma Azure de Microsoft, Este documento investiga, experimenta, desarrolla componentes y construyó un prototipo demostrador que ilustra cómo desarrollar y albergar una aplicación en la nube (en concreto Azure de Microsoft) para que esta i) pueda ser accedida de forma segura mediante el uso de tecnologías de federación (Interidy IdP, InfoCards, SAML) con autenticación única (SSO Single Sign-On) entre todos los sistemas y aplicaciones, y ii) pueda incluir mecanismos de seguridad, como la firma electrónica, que también se ofrecen como servicio (TrustedX). [45]

---

[44] Serrano Latorre, Jairo D Heymann Pignolo, Elisa, César Galobardes, Eduardo, Universitat Autònoma De Barcelona. Departament D'Arquitectura De Computadors I Sistemes Operatius, Vulnerability Assessment for Complex Middleware Interrelationships in Distributed Systems, Septiembre 30 de 2013 [online], Disponibledesde Internet: http://www.tdx.cat/bitstream/handle/10803/129506/jdst1de1.pdf?sequence=1

[45] Serrano Pérez, Sergio, Universitat Politécnica De Catalunya. Departament D'arquitectura De Computadors, Uso de servicios de seguridad y confianza desde la nube: TrustedX y la Plataforma Azure de Microsoft, 2011 [online], Disponible desde Internet: http://upcommons.upc.edu/bitstream/handle/2099.1/12401/74186.pdf?sequence=1&isAllowed=y

# 3. ANÁLISIS PRINCIPALES AMENAZAS Y VULNERABILIDADES DE ACCESO DE SESION Y DE CLOUD COMPUTING

Para el caso de estudio se consulta diversos materiales que se encuentran en la red y en la investigación realizada se lograron determinar las principales amenazas y vulnerabilidades de seguridad de Cloud Computing.

## 3.1 ANÁLISIS PRINCIPALES AMENAZAS

En *marzo del 2010 La Cloud Security Alliance* (CSA) publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud, las cuales sirvieron como punto de partida para esta investigación, entre las que encontramos las siguientes las cuales fueron complementadas con referencias bibliográficas:

### 3.1.1 Abuso y mal uso del Cloud Computing

La facilidad de registro y contratación casi anónima de servicios principalmente de IaaS (Infrastructure as a Service) y PaaS (Platform as a Service) facilita a criminales y hackers la utilización de infraestructuras de terceros para la conducción de sus actividades. Es decir, cualquiera con una tarjeta de crédito válida (dinero electrónico) puede acceder al servicio, por lo cual son conocidos los casos de proveedores de IaaS que fueran hosts de botnets tales como Zeus y trojan horses como InfoStealer. Los usuarios propios y de otros pueden saturar los servicios de Cloud.[46]

### 3.1.2 Interfaces y API poco seguros

Generalmente los proveedores de servicios en la nube ofrecen una serie de interfaces y API (Application Programming Interface) para controlar e interactuar con los recursos. De este modo, toda empresa, realiza a través de estos API o interfaces, el control, la provisión y la monitorización de los servicios Cloud.

Ejemplos:

- Permitir acceso anónimo, reutilización de tokens, autenticación sin cifrar, etc.

[46]Ing. Peña Ibarra, José Ángel, Cloud Computing, Conferencia Anual ISACA Monterrey 2011 pp 14 [online], Disponible desde Internet:http://www.isaca.org/chapters7/Monterrey/Events/Documents/20111202%20Cloud%20Computing.pdf

- Limitaciones a la hora de gestión de logs (registros de actividad) y monitorización[47]

### 3.1.3 Amenaza interna

Como en todos los sistemas de información, la amenaza que suponen los propios usuarios es una de las más importantes, dado que tienen acceso de forma natural a los datos y aplicaciones de la empresa. En un entorno Cloud esto no es en absoluto diferente ya que se pueden desencadenar igualmente incidentes de seguridad provocados por empleados descontentos y accidentes por error o desconocimiento[48].

Además, en muchos casos, es el propio proveedor del servicio el que gestiona las altas y bajas de los usuarios, produciéndose brechas de seguridad cuando el consumidor del servicio no informa al proveedor de las bajas de personal en la empresa.

### 3.1.4 Problemas derivados de las tecnologías compartidas

Esta amenaza afecta a los modelos IaaS, ya que en un modelo de Infraestructura como Servicio los componentes físicos (CPU, GPU –unidad de procesamiento grafico-, etc.) no fueron diseñados específicamente para una arquitectura de aplicaciones compartidas. Se han dado casos en los que los hipervisores de virtualización podían acceder a los recursos físicos del anfitrión provocando, de esta forma, incidentes de seguridad.[47]

### 3.1.5 Pérdida o fuga de información

Existen muchas formas en las que los datos se pueden ver comprometidos. Por ejemplo, el borrado o modificación de datos sin tener una copia de seguridad de los originales, supone una pérdida de datos.

En la nube, aumenta el riesgo de que los datos se vean comprometidos ya que el número de interacciones entre ellos se multiplica debido a la propia arquitectura. Esto deriva en pérdida de imagen de la compañía, daños económicos y, si se trata de fugas, problemas legales, infracciones de normas, etc.

La pérdida de datos se puede dar de distintas maneras. La eliminación pura y simple de información asociada a falta de backups adecuados, almacenaje en sistemas

---

[47] CSI, Top Threats to Cloud Computing V1.0 [online], Disponible desde Internet: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[48] Albaladejo, José María, Seguridad frente a los riesgos y amenazas de la Nube, Noviembre 2012 [online], Disponible desde Internet: http://www.computing.es/seguridad/informes/1064348002501/seguridad-frente-riesgos-amenazas-nube.1.html#sthash.eLHYry3F.dpuf

poco fiables, pérdidas de claves de encripción, etc. Estos episodios pueden traer importantes impactos negativos en los negocios de los clientes de los servicios en la nube[43].

### 3.1.6 Secuestro de cuenta/servicio

El concepto de secuestro de cuentas es bastante conocido: modelos de fraude como phishing y la explotación de fallas de seguridad de las aplicaciones permiten a los hackers tener acceso a datos confidenciales de los usuarios. Para servicios en modelo Cloud este tipo de amenaza sigue presente, sobre todo a través del robo de credenciales de usuarios internos de las empresas.

En un entorno en la nube, si un atacante obtiene las credenciales de un usuario del entorno puede acceder a actividades y transacciones, manipular datos, devolver información falsificada o redirigir a los clientes a sitios maliciosos[49].

### 3.1.7 Riesgos por desconocimiento

Uno de los pilares de las infraestructuras Cloud es reducir la cantidad de software y hardware que tienen que adquirir y mantener las compañías, para así poder centrarse en el negocio. Esto, si bien repercute en ahorros de costes tanto económicos como operacionales, no puede ser motivo para el deterioro de la seguridad por falta de conocimiento de esta infraestructura.

Para asistir en la toma de decisiones sobre las medidas de seguridad que se han de implantar en un entorno Cloud es conveniente conocer, al menos en parte, la información técnica de la plataforma. Datos como con quién se comparte la infraestructura o los intentos de acceso no autorizados pueden resultar muy importantes a la hora de decidir la estrategia de seguridad. La carencia de información de este tipo puede derivar en brechas de seguridad desconocidas por el afectado.[50]

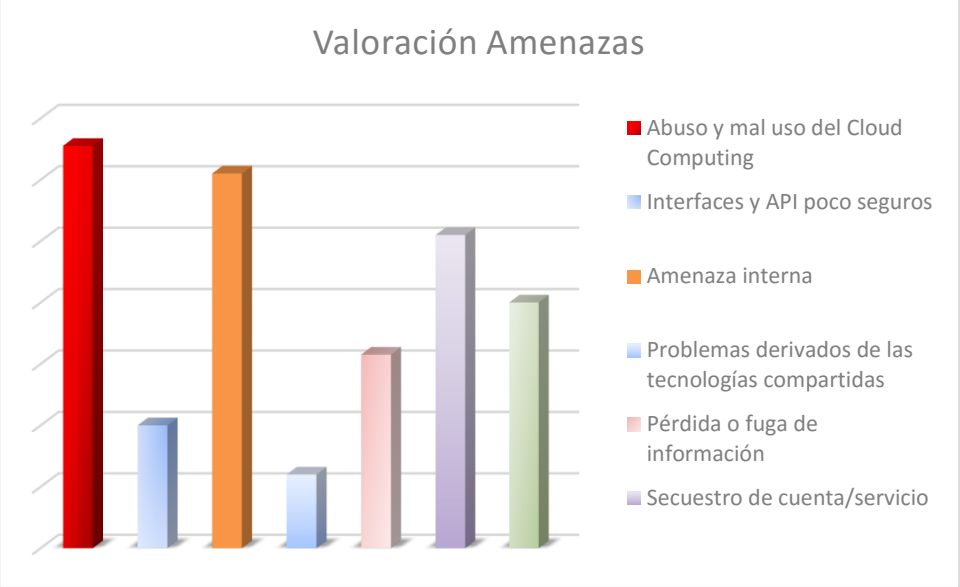
Tomando como sustento las amenazas seleccionadas anteriormente se procedió a realizar un análisis cuantitativo con base a las opiniones proporcionadas mediante encuestas (ver Anexo A.) de las cuales se determinó lo siguiente.

---

[49] Intelco, Riesgos y Amenazas en Cloud Computing 2011 [online], Disponible desde Internet: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

[50] CSI, Top Threats to Cloud Computing V1.0 [online], Disponible desde Internet: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Figura 2. Valoración cuantitativa de las amenazas




Fuente. Propiedad del Autor

Tabla 1. Análisis Valoración Cuantitativa Amenazas

| Amenazas | Valoración Cuantitativa | Ranking |
|---|---|---|
| Abuso y mal uso del Cloud Computing | 131 | 1 |
| Interfaces y API poco seguros | 40 | 6 |
| Amenaza interna | 122 | 2 |
| Problemas derivados de las tecnologías compartidas | 24 | 7 |
| Pérdida o fuga de información | 63 | 5 |
| Secuestro de cuenta/servicio | 102 | 3 |
| Riesgos por desconocimiento | 80 | 4 |

Fuente. Propiedad del Autor

En la tabla 1 se puede observar los resultados del análisis cuantitativo, resaltando que a cada una de las amenazas que fueron tomadas del estudio de la CSA[51], se dio un peso de 7 a la que en opinión de los encuestados tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

De acuerdo con la descripción anterior, los resultados de la encuesta realizada a 20 personas conocedoras del tema de Cloud Computing se señala que, la principal amenaza a la cual se encuentra expuesta la tecnología de Cloud Computing es el abuso y mal uso de la misma la cual obtuvo un peso de 131, debido al desconocimiento e Inadecuado control del otorgamiento de permisos de los

[51] CSA significa Cloud Security Alliance

servicios en la nube, atrayendo personas mal intencionado que puede afectar el funcionamiento y aumentar el tráfico que puede terminar en el colapso del servicio en la nube.

También se determina que la segunda amenaza con mayor peso es la que presenta el personal interno de la compañía, debido a que estos tienen acceso de forma natural a los datos y aplicaciones de las empresas y esto puede desencadenar en incidentes de seguridad provocados por empleados descontentos y accidentes por error o desconocimiento.
Además, en muchos casos es el propio proveedor del servicio el que gestiona las altas y bajas de los usuarios, produciéndose brechas de seguridad cuando el consumidor del servicio no informa al proveedor de las bajas de personal en la empresa [48].

Como tercera amenaza de peso es el Secuestro de cuenta/servicio, debido a los ataques de ingeniería social que pueden sufrir los usuarios del servicio, e indudablemente si un atacante obtiene las credenciales de un usuario del entorno puede acceder a actividades y transacciones, manipular datos, devolver información falsificada[48].

Como se observa en la figura 1, la amenaza menos representativa es la correspondiente a los problemas derivados de las tecnologías compartidas ya que esta amenaza afecta solo a los modelos IaaS y cada vez es menos común que se presenten errores en el adecuado aislamiento de aplicaciones compartidas.

## 3.2 ANÁLISIS VULNERABILIDADES DE CLOUD COMPUTING

El modelo de Cloud Computing es relativamente nuevo y por lo tanto el perfil de riesgo asociado a el no es todavía lo suficientemente claro. ¿Con quién comparte determinado usuario la infraestructura? ¿Cómo está diseñada la arquitectura de seguridad del proveedor de servicios? ¿Hay información disponible sobre pruebas de intrusión y ataques? Estos aspectos dan cuenta de información sensible que pocos proveedores están dispuestos a compartir, pero que son importantes para que una corporación entienda con claridad a qué riesgos se expone al adoptar un determinado modelo de gestión de TIC[52]

La lista siguiente de vulnerabilidades no abarca todas las posibles vulnerabilidades existentes, sin embargo, sí resulta suficientemente detallada para el propósito de este trabajo. Contiene informaciones sobre vulnerabilidades de seguridad, tanto específicas de Cloud como de carácter general.

[52]Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2009, Beneficios, riesgos y recomendaciones para la seguridad de la información [online], Disponible desde Internet: https://www.enisa.europa.eu/activities/risk-management/files/.../file

### 3.2.1 Vulnerabilidades Autenticación, Autorización y Auditoría (AAA)

Un sistema pobre de autenticación, autorización y auditoría podría facilitar el acceso no autorizado a recursos, aumento de privilegios, imposibilidad de rastrear el uso indebido de recursos e incidentes de seguridad, entre otros, a través de:

- Almacenamiento inseguro de las credenciales de acceso a la nube por parte del cliente

- Funciones disponibles insuficientes

- Credenciales almacenadas en un equipo transitorio. Además, la nube hace que los ataques de autenticación basados en contraseñas (práctica fraudulenta que utiliza un troyano para robar contraseñas corporativas) tengan un impacto mucho mayor, ya que las aplicaciones corporativas ahora están expuestas en Internet. Por tanto, la autenticación basada en contraseñas llegará a ser insuficiente y será necesaria una autenticación más robusta o de dos factores para acceder a los recursos en nube.[52]

### 3.2.2 Vulnerabilidades del Alta de Usuarios

- El cliente no puede controlar el proceso de altas.

- La identidad del cliente no se verifica de manera adecuada en el registro.

- Aparecen retrasos en la sincronización entre los componentes del sistema en nube (temporales y del contenido del perfil).

- Se realizan copias múltiples y no sincronizadas de datos de identidad.

- Las credenciales son vulnerables a la intercepción y a la copia.[53]

### 3.2.3 Vulnerabilidades de la Baja de Usuarios

Los usuarios dados de baja aún son válidos debido a posibles demoras en la realización de la anulación de dichos usuarios.

[53]ENISA, 2009, Beneficios, riesgos y recomendaciones para la seguridad de la información [online], Disponible desde Internet: https://www.enisa.europa.eu/activities/risk-management/files/.../file

### 3.2.4 Acceso Remoto a la Interfaz de Gestión

En teoría, esto permite que las vulnerabilidades en equipos terminales comprometan la infraestructura en nube (cliente individual o proveedor en nube), mediante, por ejemplo, una autenticación débil de las respuestas y las solicitudes.

### 3.2.5 Vulnerabilidades del Hipervisor

Los ataques a la capa del hipervisor son muy atractivos: el hipervisor, de hecho, controla totalmente los recursos físicos y los equipos virtuales que se ejecutan sobre el, así que cualquier vulnerabilidad en esta capa es extremadamente crítica. Explotar una vulnerabilidad del hipervisor equivale potencialmente a explotar todos los equipos virtuales.

La primera prueba de concepto de un ataque contra un hipervisor desde una capa inferior la ofrecieron King (y otros) en su artículo Implementando malware con máquinas virtuales[54], en el que los autores introducen el concepto de rootkit basado en un equipo virtual.

Un escenario habitual que permite la explotación de una vulnerabilidad del hipervisor es el llamado «guest to host escape», ejemplo del cual es el «cloudburst», una vulnerabilidad del VMware. Otro escenario es el «VM hopping»: en el que el atacante accede ilegalmente a un equipo terminal utilizando algún método estándar y entonces, explotando alguna vulnerabilidad del hipervisor, pasa a controlar otros equipos virtuales que estén ejecutándose en el mismo hipervisor[55]

### 3.2.6 Ausencia de Aislamiento de Los Recursos

El uso de recursos por un cliente puede afectar al uso de recursos por otro cliente. Las infraestructuras de computación en nube IaaS dependen en su mayoría de diseños de arquitectura en los que los recursos físicos se comparten entre múltiples equipos virtuales, y por consiguiente, múltiples clientes.

Las vulnerabilidades en el modelo de seguridad del hipervisor pueden conducir a un acceso no autorizado a estos recursos compartidos. Por ejemplo, los equipos virtuales del cliente A y el cliente B tienen sus discos duros virtuales guardados en el mismo LUN (número de unidad lógica) compartido dentro de una red de área de almacenamiento (SAN). El cliente B puede ser capaz de mapear el disco duro virtual del cliente A en su equipo virtual, además de ver y/o utilizar los datos que contiene.

---

[54] T King, Samuel, Peter M Chen, Yi-Min Wang, Chad Verbowsk, Helen J Wang, Jacob R LorchSubVirt: Implementing malware with virtual machines. 2006 [online], Disponible desde Internet: http://web.engr.illinois.edu/~kingst/spring2007/cs598stk/slides/cs598stk-subvirt.pdf

[55] Ormandy, Tavis [online], Disponible desde Internet: http://taviso.decsystem.org/virtsec.pdf

Los hipervisores utilizados en nubes IaaS ofrecen API integradas, que el proveedor en nube utiliza para desarrollar una interfaz de gestión de la propiedad, de provisión y de información que está expuesta a sus clientes. Las vulnerabilidades en el modelo de seguridad del hipervisor o en las «interfaces de gestión» pueden llevar a un acceso no autorizado a la información del cliente.

Al mismo tiempo, una vulnerabilidad en este nivel puede permitir a un atacante manipular los recursos de una instalación en nube, provocando una denegación de servicio (por ejemplo, apagado de equipos virtuales en ejecución), fuga de datos, datos comprometidos.

Es de destacar que la falta de herramientas para hacer cumplir un término de servicio (ToS) o un Acuerdo de nivel de servicio (SLA) más específico, como la calidad de servicio (CdS) o los productos de planificación de recursos distribuidos (DRS) podrían permitir a un cliente monopolizar el uso de la nube, con impactos a otros clientes en forma de denegación de servicio o rendimiento pobre.

### 3.2.7 Falta de Aislamiento de la Reputación

Las actividades de un cliente pueden afectar a la reputación de otro cliente.

### 3.2.8 Vulnerabilidades en la Codificación de la Comunicación

Estas vulnerabilidades se refieren a la posibilidad de leer datos en tránsito, por ejemplo, ataques con intermediarios (MITM), autenticación pobre, aceptación de certificados autofirmados.

El ataque Man In The Middle puede incluir algunos de los siguientes sub-ataques:

- Intercepción de la comunicación (eavesdropping), incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos (plaintext) conocidos.
- Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.
- Ataques de sustitución.
- Ataques de repetición.
- Ataque por denegación de servicio (denial of service). El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes.[56]

[56]Ataque man in-the-middle, Mexico DF, 5 de septiembre2013, pp 4 [online], Disponible desde Internet: en:http://es.slideshare.net/Tensor/ataque-man-inthemiddle-25926293

### 3.2.9 Falta o Debilidad En La Codificación De Archivos y Datos En Tránsito

El no codificar los datos en tránsito, los datos mantenidos en archivos y bases de datos, las imágenes de equipos virtuales sin montar, las imágenes y datos forenses, los registros importantes y otros datos estáticos pone en riesgo los datos. El coste de poner en marcha la gestión de claves y los de procesamiento deben ser considerados en relación con el riesgo que se genera para la empresa.[53]

### 3.2.10 Imposibilidad de Procesar Datos Codificados

La codificación de datos estáticos no es difícil, pero a pesar de los avances recientes en codificación homomórfica[57] no hay indicios de un sistema comercial capaz de mantener esta codificación durante el procesamiento. En un artículo, Craig Gentry considera que realizar una búsqueda de Internet con palabras clave codificadas —una aplicación perfectamente razonable de este algoritmo— incrementaría el tiempo de computación aproximadamente un billón de veces[58]. Esto quiere decir que, durante un largo tiempo, los clientes de Cloud Computing que realicen cualquier actividad diferente a almacenar información en la nube deben confiar en el proveedor Cloud.

### 3.2.11 Procedimientos Insuficientes de Gestión de Claves

Las infraestructuras de computación en nube requieren la gestión y el almacenamiento de muchos tipos distintos de claves, entre los que, por ejemplo, se incluyen claves de sesión para proteger datos en tránsito (entre ellas están las claves SSL), claves de codificación de archivos, pares de claves para identificar proveedores en nube, pares de claves para identificar clientes, símbolos de autorización y certificados de revocación. Debido a que los equipos virtuales no tienen una infraestructura de hardware fija y el contenido basado en Cloud tiende a estar distribuido geográficamente, es más difícil aplicar controles estándar, como el almacenamiento HSM (módulo de seguridad hardware), en las infraestructuras Cloud. Por ejemplo:

- Los HSM tienen necesariamente una fuerte protección física (contra robos, escuchas y falsificaciones). Esto hace que sea muy difícil distribuirlos a lo largo de las múltiples ubicaciones utilizadas en las arquitecturas en la nube (es decir, distribuidos geográficamente y con un alto grado de replicación). Las normas de gestión de claves como PKCS#10 y las normas asociadas

[57] MIT, Technology Review,2011, Re Cifrado homomórfico [online], Disponibledesde Internet: en:https://www.technologyreview.es/informatica/37710/tr10-cifrado-homomorfico/
[58] Schneier, Bruce, Homomorphic Encryption Breakthrough [online], Disponibledesde Internet: https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html

como PKCS#11[59] no ofrecen entornos normalizados para interactuar con sistemas distribuidos.

- Las interfaces de gestión de claves accesibles a través de la Internet pública (incluso indirectamente) son más vulnerables, ya que la seguridad se reduce en el canal de comunicación entre el usuario y el almacenamiento de claves de nube y los mecanismos de autenticación remota mutua utilizados.

- Los nuevos equipos virtuales que necesitan autenticarse a ellos mismos deben ser creados con cierta confidencialidad. La distribución de esos secretos puede presentar problemas de escalabilidad. La rápida escalada de autoridades de certificación que emiten pares de claves se logra fácilmente si se determinan los recursos por anticipado, pero la escalada dinámica y sin planificar de las autoridades de responsabilidades jerárquicas es difícil de lograr debido al gasto de recursos para crear nuevas autoridades (registro o certificación, autenticando nuevos componentes y distribuyendo nuevas credenciales).

- La revocación de claves en una arquitectura distribuida también es costosa. La revocación efectiva implica esencialmente que las aplicaciones comprueben el estatus de la clave (un certificado, normalmente) de acuerdo con un límite temporal conocido que determina la ventana de riesgo. Aunque existen mecanismos distribuidos para conseguir esto, constituye un reto asegurar que las diferentes partes de la nube reciban un nivel equivalente de servicio para que se asocien a niveles de riesgo diferentes. Las soluciones centralizadas, como los OCSP, son caras y no reducen necesariamente el riesgo, a no ser que la autoridad de certificación y la lista de revocación de certificados estén estrechamente conectados.[53]

### 3.2.12 Falta de Tecnologías y Soluciones Estándar

Esto significa que los datos pueden estar «ligados» a un proveedor. Es un riesgo importante si el proveedor cesa sus operaciones.

Esto puede frenar el uso de servicios de gestión de seguridad y tecnologías de seguridad externa como la gestión federada de la identidad (FIM).

Cada proveedor de servicios Cloud tiene sus propias herramientas de gestión desarrolladas para que el usuario pueda administrar sus servicios: software, sistema operativo, hardware. Aquellas empresas que tengan un único proveedor Cloud sólo

[59] RSA, PKCS #11 v2.30: Cryptographic Token Interface Standard [online], Disponible desde Internet: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf

necesitan el sistema de gestión que les facilite dicho proveedor, por lo tanto no les importa que el sistema se adecúe a estándares.[60]

### 3.2.13 Ausencia de Un Acuerdo de Depósito de Fuentes

La falta de un depósito de fuentes significa que si un proveedor PaaS o SaaS quiebra, sus clientes no están protegidos.

### 3.2.14 Modelado Inadecuado Del Uso De Recursos

Los servicios en nube son particularmente vulnerables al agotamiento de recursos debido a que no se provisionan estadísticamente. Aunque muchos proveedores permiten que los clientes reserven recursos con antelación, los algoritmos de provisión de recursos pueden fallar debido a:

- Modelado inadecuado del uso de recursos, que puede llevar a un exceso de reserva o de provisión (lo que, a su vez, lleva a un derroche de recursos por parte del proveedor en nube). Token Bucket, Fair Queuing y Class Based Queuing son algoritmos reputados de asignación de recursos. Estos algoritmos son vulnerables a distorsiones de equidad.

- Fallo de los algoritmos de asignación de recursos debido a eventos extraordinarios (por ejemplo, eventos de noticias remotas para la entrega de contenido).

- Fallo de los algoritmos de asignación de recursos que utilizan clasificación de tareas o paquetes, debido a que los recursos están clasificados de manera insuficiente.

- Fallo en la provisión general de recursos (en oposición a las sobrecargas temporales).[61]

### 3.2.15 Falta de Control en el Proceso de Evaluación de Vulnerabilidad

Las restricciones al escaneado de puertos y los test de vulnerabilidad son una vulnerabilidad importante que, en combinación con una condición de uso que haga

[60] García Martínez, Pablo, ¿Necesitamos estándares en los servicios de cloud computing?, 29 de septiembre de 2011 [online], Disponible desde Internet:http://blog.virtualizamos.es/2011/09/29/%C2%BFnecesitamos-estandares-en-los-servicios-de-cloud-computing/

[61]RSA, PKCS #11 v2.30: Cryptographic Token Interface Standard [online], Disponible desde Internet: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf

responsable al cliente de asegurar los elementos de la infraestructura, constituye un problema grave de seguridad.[52]

### 3.2.16 Posibilidad de Que se Realice Un Análisis Interno de la Red (En Nube)

Los clientes en nube pueden llevar a cabo escaneados de puertos y otras pruebas en otros clientes dentro de la red interna[51].

### 3.2.17 Posibilidad de Que Se Realicen Comprobaciones de Corresidencia

Los ataques por vía alternativa que aprovechan una falta de aislamiento de los recursos permiten a los atacantes determinar qué recursos están compartidos por qué clientes.

### 3.2.18 Ausencia de Disponibilidad Experta

A pesar de que la nube tiene el potencial de mejorar la disponibilidad experta, muchos proveedores no ofrecen servicios y términos de uso apropiados para permitirlo. Por ejemplo, los proveedores SaaS normalmente no permiten el acceso al registro de IP de los clientes que acceden a contenidos. Los proveedores IaaS pueden no ofrecer servicios expertos como equipos virtuales recientes e imágenes de disco.[62]

### 3.2.19 Limpieza de Medios Sensibles

La tenencia compartida de recursos de almacenamiento físico significa que puede haber fuga de datos sensibles debido a que bien las políticas de destrucción de datos aplicables al final de un ciclo de vida pueden ser imposibles de aplicar debido a que, por ejemplo, los medios no pueden ser destruidos físicamente porque un disco está todavía en uso por otro propietario o no puede localizarse, bien no hay un procedimiento aplicable.[53]

### 3.2.20 Sincronización de las Responsabilidades o las Obligaciones Contractuales Externas A La Nube

Frecuentemente, los clientes en nube no son conscientes de las responsabilidades que asumen en las condiciones de servicio. Hay una tendencia a atribuir erróneamente al proveedor en nube la responsabilidad de actividades como la codificación de archivos, incluso aunque esté claramente señalado en los términos

[62]RSA, PKCS #11 v2.30: Cryptographic Token Interface Standard [online], Disponible desde Internet: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf

del contrato entre las dos partes que no se ha asumido ninguna responsabilidad de ese tipo.[63]

### 3.2.21 Aplicaciones Inter-Nube Que Crean Dependencia Oculta

En la cadena de suministro (dependencias intra y extra nube) existen dependencias ocultas y la arquitectura del proveedor en nube no ofrece operaciones continuas desde la nube cuando las terceras partes implicadas, subcontratistas o la compañía cliente, han sido separadas del proveedor del servicio y viceversa.[52]

### 3.2.22 Cláusulas Service Level Agreement (SLA) Con Compromisos En Conflicto Para Con Diferentes Partes

Las cláusulas SLA (Acuerdo de Nivel de Servicios) también pueden estar en conflicto con compromisos enunciados en otras cláusulas o en cláusulas de otros proveedores.

Errores más frecuentes en la implantación:

- Definir niveles de servicio inalcanzables
- Regulación excesiva
- Error en la definición de prioridades
- Complejidad técnica
- Irrelevancia (si un SLA no tiene ningún efecto sobre el cliente, el objetivo no tiene sentido).[64]

### 3.2.23 Cláusulas SLA Que Contienen Un Riesgo De Negocio Excesivo

Los SLA pueden acarrear demasiado riesgo de negocio para un proveedor, dado el riesgo real de fallos técnicos. Desde el punto de vista del cliente, los SLA pueden contener cláusulas que resulten ser perjudiciales; por ejemplo, en el terreno de la propiedad intelectual, un SLA puede especificar que el proveedor en nube posee los derechos de cualquier material almacenado en la infraestructura en nube.[52]

### 3.2.24 Auditoría o Certificación No Disponible Para Los Clientes

El proveedor de Cloud no puede ofrecer ninguna garantía al cliente vía una certificación de auditoría.

---

[63]Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2009, Beneficios, riesgos y recomendaciones para la seguridad de la información [online], Disponible desde Internet: https://www.enisa.europa.eu/activities/risk-management/files/.../file

[64]Acuerdo de Nivel de Servicio en Contratación (SLA), PORTALEY nuevas tecnologías, S.L, [online], Disponible desde Internet:http://www.contratosinformaticos.com/sla/

Por ejemplo, algunos proveedores en nube están utilizando hipervisores de código abierto o versiones adaptadas de los mismos, lo que constituye un requisito fundamental para algunas organizaciones por ejemplo las agencias del Gobierno de EE.UU.

Es importante tener en cuenta que no se está afirmando que exista una correlación directa entre certificación y nivel de vulnerabilidad (dado que no existe suficiente información sobre la protección de perfiles y los objetivos de seguridad de los productos certificados).[63]

### 3.2.25 Ausencia de Políticas de Limitación De Recursos

Si no existe un modo flexible y configurable para que el cliente y/o el proveedor en nube establezcan límites sobre los recursos, puede haber problemas cuando el uso de recursos sea impredecible.

### 3.2.26 Almacenamiento de Datos En Jurisdicciones Múltiples Y Falta De Transparencia Sobre Este Punto

Los servicios de datos en espejo para su entrega a través de redes de proximidad y almacenamiento redundante sin información en tiempo real sobre dónde se almacenan los datos disponible para el consumidor introduce un nivel de vulnerabilidad. Las empresas pueden incumplir las normas inconscientemente, especialmente si no se ofrece información clara sobre la jurisdicción del almacenamiento.

### 3.2.27 Falta de Información Sobre Jurisdicciones

Los datos pueden almacenarse y/o procesarse en jurisdicciones de alto riesgo, donde son vulnerables a la confiscación por medio de una entrada forzada. Si esta información no se encuentra disponible para los clientes en nube, no pueden tomar medidas para evitarlo.

### 3.2.28 Vulnerabilidades No Específicas De La Tecnología Cloud

Durante el análisis de la información recopilada, se han identificado las siguientes vulnerabilidades que no son específicas de la computación en nube pero que, sin embargo, deben tenerse en cuenta al evaluar un sistema típico planteado en Cloud.

### 3.2.29 Ausencia De Conciencia De Seguridad

Los clientes en nube no son conscientes de los riesgos que podrían afrontar al migrar hacia la nube, en particular aquellos riesgos generados a partir de amenazas específicas de la nube, es decir, pérdida de control, cierre de la empresa

proveedora, agotamiento de recursos del proveedor en nube, etc. Esta falta de conciencia también podría afectar al proveedor en nube, que puede no ser consciente de las medidas que debería tomar para mitigar estos riesgos.

### 3.2.30 Falta de Procesos de Investigación

Dado que pueden existir funciones de alto privilegio en los proveedores en nube, debido a la escala implicada, la ausencia de, o una inadecuada investigación sobre el perfil de riesgo del personal con dichas funciones es una vulnerabilidad importante.

### 3.2.31 Funciones y Responsabilidades Confusas

Estas vulnerabilidades se refieren a la atribución inadecuada de funciones y responsabilidades en la organización del proveedor en nube.[65]

### 3.2.32 Aplicación Deficiente de Las Definiciones de Funciones

En el proveedor en nube, una separación inadecuada de funciones puede conducir a roles excesivamente privilegiados que pueden convertir a los sistemas muy grandes en vulnerables. Por ejemplo, ninguna persona debería tener privilegios de acceso a toda la nube[52].

### 3.2.33 No Aplicación Del Principio De «Need-To-Know»

Éste es un tipo especial de vulnerabilidad relativa a los roles y las responsabilidades, no debería darse un acceso a los datos innecesarios a las partes.

La información es un recurso corporativo, un activo de gran valor para la organización. El objeto de la información es aportar el conocimiento necesario para poder actuar con seguridad, eficacia y oportunidad, tanto en el cumplimiento de la misión como en el proceso de toma de decisiones o consultas. Existe una responsabilidad individual y colectiva de que la información esté accesible, disponible y utilizable para aquellas entidades que requieran dicha información para acometer sus tareas y servicios oficiales.[66]

---

[65] Morocho Llivicota, Guillermo Oswaldo, Tesis, Modelo de gestión de riesgos de infraestructura como servicios (IaaS) de Cloud Computing para empresas del sector público Ecuatoriano, Pág.50 [online], Disponible desde Internet: http://bibdigital.epn.edu.ec/bitstream/15000/12556/1/CD-6652.pdf

[66] Autoridad Nacional para la protección información clasificada, Seguridad de la Información, Edición 3/Diciembre 2012, Pág. NS/04 – 8 [online], Disponible desde Internet: http://www.cni.es/comun/recursos/descargas/NS-04_Seguridad_de_la_Informacion.pdf

### 3.2.34 Configuración Deficiente

Esta clase de vulnerabilidades incluye: aplicación inadecuada de una línea base de seguridad y procedimientos de aumento de la resistencia a los fallos, error humano y administrador no formado.[67]

### 3.2.35 Vulnerabilidades De La Aplicación o Gestión De Parches Insuficiente

Esta clase de vulnerabilidades incluye: errores en el código de la aplicación, procedimientos de parcheado conflictivos entre el proveedor y el cliente, aplicación de parches no examinados, vulnerabilidades en los navegadores.

### 3.2.36 Lista Complementaría De Vulnerabilidades

- Vulnerabilidades del sistema o del sistema operativo
- Software que no es confiable
- Ausencia de plan continuidad del negocio y de recuperación de desastres
- Falta de inventario de activos (o incompleto o inadecuado)
- Selección de proveedores insuficiente, no se indaga en el mercado las posibilidades existentes
- Vulnerabilidades en el consumo de recursos
- Incumplimiento del acuerdo de no divulgación por el proveedor
- Responsabilidad por pérdida de datos
- Falta de políticas o procedimientos insuficientes para la recopilación y retención de registros
- Recursos de filtrado inadecuados o mal configurados

[67]RSA, PKCS #11 v2.30: Cryptographic Token Interface Standard [online], Disponible desde Internet: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf

# 4. ESTRATEGIAS DE SEGURIDAD PARA LA PROTECCION DE LOS SERVICIOS EN LA NUBE– CLOUD COMPUTING

Utilizar los servicios en la nube conlleva un cambio en la forma de entender la seguridad informática. Deja de existir la imagen tradicional en la que todos los servidores de la empresa están en el sótano del edificio donde solo pueden acceder los administradores informáticos. Al hacer uso del Cloud Computing una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.[68]

Retomando el análisis realizado, en el cual se determinaron una serie de amenazas y en donde se evidenció que la principal amenaza a la que se encuentra expuesta Cloud, se presenta a continuación una serie de recomendaciones a tener en cuenta para la reducción del riesgo de dichas amenazas, estas están organizadas de acuerdo a la prioridad dada en el análisis anteriormente mencionado.

## 4.1. RECOMENDACIONES PARA REDUCCIÓN DEL RIESGO

### 4.1.1 Abuso y mal uso del Cloud Computing

- Implementar un sistema de registro de acceso más restrictivo, siempre y cuando las medidas de seguridad más restrictivas no impacten negativamente en la satisfacción del cliente, deberían resultar rentables y cuantificables, a través de la reducción del riesgo del personal, ingresos, reputación y valor de los accionistas.[23]
- Coordinar y monitorear el fraude en tarjetas de crédito
- Monitorizar el tráfico de clientes para la detección de posibles actividades ilícitas
- Comprobar las listas negras públicas para identificar si los rangos IP de la infraestructura han entrado en ellas

### 4.1.2 Interfaces y API poco seguros

Dado que todo (autenticación, acceso, cifrado de datos, etc.) se realiza a través de estas herramientas, se hace necesario que los interfaces estén diseñados de forma segura, evitando así los problemas de seguridad, tanto los que son intencionados como los que se producen de forma accidental.[68]

- Analizar los problemas de seguridad de las interfaces de los proveedores de servicio

[68]Inteco, Octubre 2011, Guía para empresas: seguridad y privacidad del cloud computing [online], Disponible desde Internet: http://www.genbetadev.com/seguridad-informatica/inteco-publica-una-guia-para-seguridad-y-privacidad-en-el-cloud-computing

- Asegurarse que la autenticación y los controles de acceso se implementan teniendo en cuenta el cifrado de los datos

### 4.1.3 Amenaza interna

- Especificar cláusulas legales y de confidencialidad en los contratos laborales
- Determinar los posibles problemas en los procesos de notificación

### 4.1.4 Problemas derivados de las tecnologías compartidas

Para evitar este tipo de incidentes se recomienda implementar una defensa en profundidad con especial atención a los recursos de computación, almacenamiento y red. Además, se ha de generar una buena estrategia de seguridad que gestione correctamente los recursos para que las actividades de un usuario no puedan interferir en las del resto.[68]

- Diseñar buenas prácticas para la instalación y configuración
- Monitorizar los entornos para detectar cambios no deseados en las configuraciones o la actividad
- Proporcionar autenticación fuerte y control de acceso para el acceso de administración
- Adecuar los acuerdos de nivel de servicio para controlar el parcheado y la corrección de vulnerabilidades

### 4.1.5 Pérdida o fuga de información

- Implementar API potentes para el control de acceso
- Proteger el tránsito de datos mediante el cifrado de los mismos
- Analizar la protección de datos tanto en tiempo de diseño como en tiempo de ejecución
- Proporcionar mecanismos potentes para la generación de claves, el almacenamiento y la destrucción de la información
- Definir, por contrato, la destrucción de los datos antes de que los medios de almacenamiento sean eliminados de la infraestructura, así como la política de copias de seguridad

### 4.1.6 Secuestro de cuenta/servicio

- Prohibir, mediante políticas, compartir credenciales entre usuarios y servicios
- Aplicar técnicas de autenticación de doble factor siempre que sea posible
- Monitorizar las sesiones en busca de actividades inusuales

### 4.1.7 Riesgos por desconocimiento

- Tener acceso a los logs (registros de actividad) de aplicaciones y datos
- Estar al corriente, total o parcialmente, de los detalles de la infraestructura
- Monitorizar y recibir alertas sobre el uso de información crítica[68]

Los mecanismos de seguridad que se pueden aplicar para proteger los datos alojados en la nube deben considerarse como un trabajo colaborativo entre las dos partes (proveedor de servicios en la nube y cliente), ya que ambas deben asumir unas responsabilidades. La realización de auditorías de seguridad conjuntas es una buena práctica para revisar que todo el sistema está protegido frente a posibles amenazas.

## 4.2 ESTRATEGIAS DE SEGURIDAD

### 4.2.1 Gestión de Cambios

Se debe mantener un historial de modificaciones de los datos o ficheros almacenados en la nube. Cada modificación debe llevar asociado un sello de fecha y el usuario que lo produjo. Si se detecta que varios usuarios han modificado el recurso a la vez se puede analizar el sello de fecha para comprobar qué versión tiene validez. Del mismo modo, si se detecta un error de integridad en el recurso se puede volver a una versión anterior que sea correcta.[69]

### 4.2.2 Las copias de Seguridad

Son la última línea defensiva para garantizar la integridad de los datos. Utilizando adecuadamente las herramientas en la nube se pueden programar copias de seguridad cada cierto tiempo. Si se detecta un fallo de integridad a nivel general, la única forma de solucionarlo es volver a una versión anterior del sistema almacenada en la copia de seguridad.[70]

### 4.2.3 Control de Acceso

Cuando una empresa o entidad utiliza las capacidades de Cloud Computing, necesita que el administrador del sistema establezca un correcto control de acceso para garantizar que los usuarios solo utilizan los datos o procesos para los que han sido autorizados.[68]

---

[69] Sanabria, Juan David, Abril 2015, privacidad en la nube [online], Disponible desde Internet: https://prezi.com/lgsmtvm16yfc/privacidad-en-la-nube/

[70]Programación Integral S.A, Seguridad y privacidad del Cloud Computing [online], Disponible desde Internet:http://programacionintegral.es/tpv/75-actualidad/nos-interesa/721-seguridad-y-privacidad-del-cloud-computing

### 4.2.4 Establecer una Política de Seguridad

Una correcta política de seguridad limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y además impide que personas ajenas a la organización accedan o corrompan los datos.

### 4.2.5 Establecer Políticas de Backups

Permite recuperar los datos aun cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware. Todos los proveedores de servicios en la nube ofrecen sistemas de copias de seguridad de forma completamente transparente para el usuario. Tan solo es necesario seleccionar los activos que se quieren proteger y la periodicidad con la que se desean estas copias. La recuperación frente a un ataque puede ser tan sencilla como la restauración de un snapshot (copia instantánea de volumen) anterior de la máquina virtual.[68]

## 4.3 CRIPTOGRAFÍA

Por otra parte dentro de la industria de la seguridad hay unanimidad en que la mejor forma de proteger la información y los servicios en la nube pasa por el uso de la criptografía. No hay proveedor de servicios en la nube que no ofrezca, en su opinión, los mejores y más avanzados estándares y técnicas criptográficas en toda su infraestructura de servicios. Así la encriptación es esencial a la hora de evitar que la información sea interpretada, en caso de ser interceptada, por personas o servicios no autorizados. Es también necesaria para proteger nuestros datos en caso de pérdida.[71]

La criptografía juega un papel protagonista en el uso de los servicios en la nube. La criptografía proporciona un nivel superior de seguridad en tres aspectos principales:

### 4.3.1 Protección de las Conexiones de Red

El uso de Secure Sockets Layer (SSL) y Transport Layer Security (TLS) permiten que todos los datos que viajen desde el servidor en la nube hasta el usuario estén cifrados impidiendo su acceso a terceras personas incluso cuando se utiliza una red Wi-Fi no segura.[72]

---

[71] González, David, Cloud Computing y Seguridad, [online], Disponible desde Internet: http://recsi2012.mondragon.edu/es/programa/recsi2012_submission_35.pdf

[72] Quintero Otavo, Mónica Tatiana, Seguridad en la Nube, 9 de Abril de 2015, pp 14 [online], Disponible desde Internet: https://prezi.com/za5p6os_bqou/seguridad-en-la-nube/

### 4.3.2 Protección de Las Conexiones Entre Los Administradores Del Sistema

En este caso, el uso de Secure Shell (SSH) y Virtual Private Network (VPN) permitirá a los administradores del sistema o desarrolladores de las aplicaciones mantener un canal seguro de comunicación con los sistemas en la nube.

### 4.3.3 Protección de los Datos.

Si se utiliza la nube como un sistema de almacenamiento de datos es muy recomendable utilizar un nivel de cifrado adecuado para aquellos datos sensibles que vayan a ser depositados allí. De esta forma, si algún usuario no autorizado intercepta los datos o tiene acceso al sistema de ficheros de la nube, no podrá leer el contenido allí depositado sin conocer la clave de cifrado.

## 5. MARCO REGULATORIO DE COLOMBIA – CLOUD COMPUTING

Es importante iniciar este aspecto señalando que es la Comisión de Regulación de Comunicaciones, de acuerdo con el artículo 19 de la Ley 1341, el órgano encargado de promover la competencia, evitar el abuso de posición dominante y regular los mercados de las redes y los servicios de comunicaciones; con el fin que la prestación de los servicios sea económicamente eficiente, y refleje altos niveles de calidad[73].

La Ley de TIC 1341 de 2009, atribuye a la CRC de funciones de regulación de los mercados de las redes y servicios de comunicaciones, como son, entre otros, las redes y servicios de telefonía fija y móvil, acceso a Internet fijo y móvil, provisión de contenidos y aplicaciones, y todos los servicios que puedan enmarcarse dentro de las Tecnologías de la Información y las Comunicaciones.

Afortunadamente Colombia es uno de los países que cuenta a la fecha con un conjunto de leyes que facilitarán el desarrollo del Cloud Computing en Colombia. A continuación, se describen estas leyes y se enuncian los temas más importantes que éstas mencionan:

### 5.1 LEY 1273 DE 2009

Por medio de la Ley 1273 de 2009 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 protege a los sistemas de Información de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. La Ley penaliza, entre estos atentados, el acceso abusivo a los sistemas informáticos, la interceptación de datos, la ejecución de daños informáticos, el uso de software malicioso, la violación de los datos personales, la suplantación de sitios web para capturar datos personales, el hurto por medios informáticos y semejantes y la Transferencia no consentida de activos.

### 5.2 LEY 1221 DE 2008 - LEY DE TELETRABAJO

Por medio de esta ley, se establecen normas para promover y regular el Teletrabajo y se provee un marco de seguridad jurídica.

---

[73] CRC, Agenda Regulatoria 2015-2016 [online], Disponible desde Internet: https://www.crcom.gov.co/uploads/images/files/2014/Actividades_Regulatorias/AgendaRegulatoria20152016/Propuesta_AgendaRegulatoria_2015-2016_20141030.pdf

Esta ley define el teletrabajo en sus distintas formas, establece una política pública de fomento al teletrabajo y una red nacional de fomento al teletrabajo. De igual manera, menciona que el Gobierno Nacional pondrá en funcionamiento un sistema de inspección, vigilancia y control para garantizar el cumplimiento de la legislación laboral en el marco del teletrabajo y se proveen las garantías laborales, sindicales y de seguridad social para los tele trabajadores.

## 5.3 LEY 1266 DE 2008

La ley 1266 de 2008 Declarado Exequible mediante Sentencia C-1011 del 16 de octubre de 2008., dictan las disposiciones generales del hábeas data y 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, entre otros.

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Ley 1273 de 2009 Delitos informáticos.

Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Además, estable los principios de la administración de datos: Principio de veracidad, de finalidad, de circulación restringida, de temporalidad de la información, de interpretación integral de derechos constitucionales, de seguridad y de confidencialidad; establece los derechos de los titulares de la información, los deberes de los operadores, las fuentes y los usuarios de información, la vigilancia de los destinatarios de la ley.

## 5.4 LEY 1341 DE 2009

Por medio de esta ley, 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 de Espectro y se dictan otras disposiciones. Esta ley tiene por objeto determinar el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la

administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

Además, define los siguientes principios orientadores: prioridad al acceso y uso de las tecnologías de la información y las comunicaciones, libre competencia, uso eficiente de la infraestructura y de los recursos escasos, protección de los derechos de los usuarios, promoción de la inversión, neutralidad tecnológica, el derecho a la comunicación, la información y la educación y los servicios básicos de las tic y la masificación del gobierno en línea.

## 5.5 LEY ESTATUTARIA 1621 DE 2013

Conocida como la “Ley de Inteligencia”, permitió precisar los fines, limites, principios y controles que enmarcan la actividad de inteligencia y contrainteligencia en el sistema democrático colombiano.
En este mismo contexto, se acogieron treinta y cinco (35) recomendaciones realizadas por las Naciones Unidas el 17 de mayo de 2010, traducidas en buenas prácticas para los organismos de inteligencia desde una perspectiva de respeto por los derechos humanos y bajo unos esquemas de supervisión y control. Aspectos incorporados:

- Sistema de ponderación de derechos, que radica en la imperativa valoración de los principios y los límites de la actividad de inteligencia y contrainteligencia, frente a situaciones fácticas que determinan la obligación del Estado de actuar; esto es, asegurar la consecución de los fines esenciales del Estado, la vigencia del orden democrático, la integridad territorial, la soberanía, la seguridad y defensa de la nación.

- Identificó los organismos y dependencias del Estado encargadas de realizar actividades de inteligencia y contrainteligencia.

- Define los límites y fines de la función de la inteligencia la cual se debe regular en todo momento por el respeto de garantías o derechos fundamentales.

- Prohíbe la vinculación de menores de edad en actividades de inteligencia.

- Creación del Plan Nacional de Inteligencia que define las prioridades de Gobierno Nacional en materia de inteligencia y contrainteligencia y asigna responsabilidades.

- Creación de controles y mecanismos adicionales a los existentes de supervisión internos (Inspectores Generales) y externos (Comisión Legal Parlamentaria).

- Creación de los Centros de Protección de Datos de Inteligencia y Contrainteligencia, orientado a salvaguardar la reserva de la información y garantizar la protección de los derechos fundamentales.

- Establecimiento de mecanismos para la actualización, corrección y retiros de datos de archivos de inteligencia.

- Diferenciación entre el concepto de monitoreo e interceptación de comunicaciones.

- Reglamentación de los mecanismos de coordinación y cooperación entre organismos de inteligencia del Estado[74]

La Ley 1621 de 2013 mediante la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, se encuentra reglamentada por el Decreto Nacional 857 de 2014.

## 5.6 RESOLUCIÓN CRC 2258 DE 2009

Teniendo en cuenta que la protección del ciberespacio es un factor de trascendente importancia para preservar la seguridad de la nación y su economía, la CRC comprendió la necesidad de estudiar los cambios que se han generado sobre estos asuntos, y analizar alternativas de modificación o creación de reglas para contribuir desde la perspectiva regulatoria interna.

Con el fin de cumplir con lo descrito anteriormente se consideraron diferentes tendencias mundiales sobre la materia, así como el estado actual de redes de telecomunicaciones en el país, y los servicios y mecanismos de seguridad que son implementados en las mismas.

Por medio de esta Resolución, se incluyeron definiciones de términos asociados a la ciberseguridad en el Artículo 1.8 de la Resolución CRT 1740 de 2007:

Autenticación, Autorización, Ciberespacio, Ciberseguridad, Confidencialidad de datos, Disponibilidad, Entidad, Infraestructura crítica, Integridad de datos, Interceptación, Interferencia, Interrupción, No repudio, Pharming, Phishing, Software Malicioso (Malware), Vulnerabilidad, Por otra parte, se modificó la redacción del Artículo 2.4 de la Resolución CRT 1740 de 2007, incluyendo la

[74] Lizarazo Rojas, Manuel Felipe, El Nuevo Rol Jurídico De La Inteligencia Y Contrainteligencia En El Estado Colombiano 2014, [online], Disponible desde Internet: http://repository.unimilitar.edu.co/bitstream/10654/7148/3/INTELIGENCIA%20Y%20CONTRAINTELIGENCIA%20EN%20EL%20ESTADO%20COLOMBIANO.pdf

necesidad por parte de los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet que deben utilizar los recursos técnicos y logísticos que garanticen la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción, e interferencia del mismo. De acuerdo con los marcos de seguridad definidos por la UIT, en lo que respecta a:

- Autenticación: (Recomendaciones UIT X.805 y UIT X.811).
- Acceso: (Recomendaciones UIT X.805 y UIT X.812)
- Servicio de No repudio: (Recomendaciones UIT X.805 y X.813)
- Principio de Confidencialidad de datos: (Recomendaciones UIT X.805 y X.814)
- Principio de Integridad de datos: (Recomendaciones X.805 y X.815)
- Principio de Disponibilidad: (Recomendación X.805)

Así mismo, se modificó el Artículo 22 de la Resolución CRT 1732 de 2007, sobre inviolabilidad de la comunicaciones aclarando que los proveedores de redes y/o servicios de telecomunicaciones, deben asegurar los principios (confidencialidad, integridad y disponibilidad) y servicios de seguridad (autenticación, autorización y no repudio) de la información, requeridos para garantizar la inviolabilidad de las comunicaciones, la información que se curse a través de ellas y los datos personales de los suscriptores y/o usuarios, en lo referente a las redes y/o servicios suministrados por dichos operadores.

Por último se modificó el Artículo 23 de la Resolución CRT 1732 de 2007, sobre seguridad de los datos e informaciones, en donde los proveedores de redes y/o servicios de telecomunicaciones, deberán adoptar mecanismos que garanticen el manejo confidencial, la integridad y disponibilidad de los datos de los suscriptores y/o usuarios, los cuales sólo pueden ser intercambiados con otros proveedores para efectos de la prevención y control de fraudes en las telecomunicaciones y el cumplimiento de las obligaciones regulatorias que así lo exijan.

### 5.7 LEY 599 DE 2000

En el capítulo séptimo de esta ley se tratan aspectos sobre la violación a la intimidad, reserva e interceptación de comunicaciones, el texto de la ley cita lo siguiente:

Artículo 192. Violación ilícita de comunicaciones. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

Artículo 193. Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

Artículo 196. Violación ilícita de comunicaciones o correspondencia de carácter oficial. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años.

La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia esté destinada o remitida a la Rama Judicial o a los organismos de control o de seguridad del Estado.

La pena se aumentará de una tercera parte a la mitad cuando la conducta descrita en el inciso anterior se realice con fines terroristas.

**5.8 LEY 1288 DE 2009**

Esta Ley modificó algunos artículos del código penal referente a los delitos informáticos, los cuales quedaron de la siguiente manera:

Artículo 25. Modificación de penas para los delitos de divulgación y empleo de documentos reservados y acceso abusivo a un sistema informático. Con el objeto de garantizar la reserva legal de los documentos de inteligencia y contrainteligencia y evitar su divulgación por parte de los miembros de organismos que llevan a cabo este tipo de actividades, los artículos 194, 195, 418, 419 y 420 del Código Penal quedarán así:

"Artículo 194. Divulgación y empleo de documentos reservados. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en pena de prisión de cinco (5) a ocho (8) años, siempre que la conducta no constituya delito sancionado con pena mayor".

"Artículo 195. Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en pena de prisión de cinco (5) a ocho (8) años".

"Artículo 418. Revelación de secreto. El servidor público que indebidamente dé a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en pena de prisión de cinco (5) a ocho (8) años y multa de veinte (20) a ciento veinte (120) salarios mínimos legales mensuales vigentes, e inhabilitación para el ejercicio de funciones públicas por diez (10) años.

Si de la conducta resultare perjuicio, la pena será de cinco (5) a ocho (8) años de prisión, multa de sesenta (60) a doscientos cuarenta (240) salarios mínimos legales mensuales vigentes, e inhabilitación para el ejercicio de derechos y funciones públicas por diez (10) años".

"Artículo 419. Utilización de asunto sometido a secreto o reserva. El servidor público que utilice en provecho propio o ajeno, descubrimiento científico, u otra información o dato llegados a su conocimiento por razón de sus funciones y que deban permanecer en secreto o reserva, incurrirá en prisión de cinco (5) a ocho (8) años y pérdida del empleo o cargo público, siempre que la conducta no constituya otro delito sancionado con pena mayor".

"Artículo 420. Utilización indebida de información oficial privilegiada. El servidor público que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad pública, que haga uso indebido de información que haya conocido por razón o con ocasión de sus funciones y que no sea objeto de conocimiento público, con el fin de obtener provecho para sí o para un tercero, sea este persona natural o jurídica, incurrirá en pena de prisión de cinco (5) a ocho (8) años y pérdida del empleo o cargo público".

Parágrafo 1°. Adiciónese un artículo 418B (revelación de secreto culposa) a la Ley 599 de 2000, el cual quedará así:

"Artículo 418 B. Revelación de secreto culposa. El servidor público que por culpa dé indebidamente a conocer documento o noticia que deba mantener en secreto o reserva, incurrirá en multa de diez (10) a ciento veinte (120) salarios mínimos legales mensuales vigentes y pérdida del empleo o cargo público".

Parágrafo 2°. Adiciónese un artículo 429B a la Ley 599 de 2000, el cual quedará así:

"La persona que bajo cualquier circunstancia dé a conocer información sobre la identidad de quienes desarrollan actividades de inteligencia o contrainteligencia, incurrirá en pena de prisión de (5) cinco a (8) ocho años siempre que la conducta no constituya delito sancionado con pena mayor".

## 5.9 LEY 1581 DE 2012

Esta Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Dentro de los contenidos mínimos que se desprenden del derecho de hábeas data se encuentra que las personas tienen la facultad de conocer – acceso – la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las mismas donde se encuentra dicha información; tienen además, el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular – salvo las excepciones previstas en la normativa –.

La Ley obliga a todas las entidades públicas y empresas privadas a revisar el uso de los datos personales contenidos en sus sistemas de información y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas, como entidad responsable del tratamiento (persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos) deben definir los fines y medios esenciales para el tratamiento de los datos de los usuarios y/o titulares, incluidos quienes fungen como fuente y usuario, y los deberes que se le adscriben responden a los principios de la administración de datos y a los derechos –intimidad y hábeas data – del titular del dato personal.

## 5.10 DECRETO 1377 DEL 27 DE JUNIO DE 2013

El Decreto tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, entre otros:

- El anuncio como tal (y a los cinco días siguientes de la comunicación, enviar carta comunicándole al respecto a la Superintendencia de Industria y Comercio).

- Formato de autorización para que si lo desean lo diligencien los titulares de datos recolectados previamente.

- Determinación de canal electrónico y físico para recibir las autorizaciones.

- Política de tratamiento de la información personal (pues esta se debe indicar en el anuncio).

- Conducto regular y canales físicos y electrónicos definidos para que el titular ejerza sus derechos de acceso, rectificación y supresión.

## 5.11 LEY 527 DE 1999

Esta ley se implementó para definir y reglamentar el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y dictar otras disposiciones.

## 5.12 PLAN NACIONAL DE TIC

El Plan Nacional de Tecnologías de la Información y las Comunicaciones es la estrategia nacional para la utilización de TICs en Colombia. Entre sus objetivos, el Plan está orientado a contribuir en el fortalecimiento de las políticas de inclusión y de equidad social y aumentar la competitividad del país, lo cual redundará en desarrollo social para los colombianos. Para esto, el Plan propone una serie de políticas, acciones y proyectos en ocho ejes principales: cuatro transversales y cuatro verticales.
Los ejes transversales cubren aspectos y programas que tienen efecto sobre los distintos sectores y grupos de la sociedad. Estos ejes son:

- Comunidad
- Marco regulatorio
- Investigación, desarrollo e innovación
- Gobierno en Línea

Los ejes verticales se refieren a programas que ayudarán a lograr una mejor apropiación y uso de las TIC en sectores. Estos ejes son:

- Educación
- Salud
- Justicia
- Competitividad empresarial.

## 5.13 DOCUMENTO CONPES 3072 DE 2000

El documento CONPES 3072 de 2000 presenta la “Agenda de Conectividad”, que es el programa del Ministerio de Tecnologías de la Información y las Comunicaciones, encargado de impulsar el uso y masificación de las Tecnologías de Información y Comunicación -TIC- como herramienta dinamizadora del desarrollo social y económico del país. En este documento se presenta como estrategia “Gobierno en Línea”, que propende por el mejoramiento del funcionamiento y la eficiencia del Estado, de la transparencia del Estado y busca fortalecer el control social sobre la gestión pública así como la función del Estado al servicio del ciudadano a través del uso de tecnologías de la información.

## 5.14 DOCUMENTO CONPES 3248 DE 2003

El Documento CONPES 3248 de 2003 define el programa de renovación de la administración pública y establece que la finalidad de la estrategia de Gobierno electrónico es “…definir una política y un conjunto de instrumentos adecuados para el manejo de la información en el sector público de modo que se garantice plena transparencia de la gestión, alta eficiencia en los servicios prestados a los ciudadanos y en las relaciones con el sector productivo y condiciones adecuadas para promover el desarrollo interno y la inserción internacional. Esta política confiere sentido a la incorporación y al uso de la tecnología informática en el desarrollo de las operaciones de las entidades estatales, tanto en sus actividades internas como en sus relaciones con otras entidades públicas y privadas, con los ciudadanos y con el sector productivo. El propósito último es facilitar las relaciones del ciudadano con la administración, e incrementar la eficiencia, la transparencia y el desarrollo territorialmente equilibrado del Estado”.[75]

[75] Mesa Sectorial Cloud Computing, Cloud Computing Una Perspectiva Para Colombia [online], Disponible desde Internet: http://cintel.co/wp-content/uploads/2013/05/16.clud_computing_Cloud-Computing-Mesa-sectorial-1.pdf

# CONCLUSIONES

Se determina que las principales amenazas a las cuales se encuentra expuesta la tecnología de Cloud Computing, son las que están directamente relacionas con acciones que incluyen a los usuarios finales que manejan los diferentes servicios de la nube.

De acuerdo a la investigación se logra deducir que los mecanismos de seguridad que pueden ser aplicados para proteger los datos alojados en la nube, deben considerarse como un trabajo colaborativo entre las dos partes (proveedor de servicios en la nube y cliente), ya que ambas deben asumir unas responsabilidades.

Los riesgos generados por las distintas amenazas de Cloud se pueden mitigar a través de la utilización de estrategias de seguridad como control de acceso, realizar copias de seguridad, establecimiento de políticas de seguridad y demás buenas prácticas descritas en esta monografía.

La criptografía es un mecanismos que juega un papel muy importante en el uso de los servicios en la nube, toda vez que la criptografía proporciona un nivel superior de seguridad en tres aspectos principales, como son: la protección de las conexiones de red entre los usuarios y las aplicaciones en la nube, protección de las conexiones entre los administradores del sistema y los servicios de la nube y protección de los datos.

Las leyes en nuestro país brindan garantías a las personas que utilizan Cloud Computing, ya que exige a los proveedores brindar garantías en el manejo de la información contenida en bases de datos, en especial la financiera, crediticia, comercial y de servicios.

## RECOMENDACIONES

No hay proveedor de servicios en la nube que no ofrezca, estándares y técnicas criptográficas en toda su infraestructura de servicios por lo cual se recomienda la aplicación de la criptografía como método para mantener la integridad de la información manejada a través de Cloud Computing.

Es importante impulsar la capacitación de las personas sobre el uso adecuado de Cloud, para disminuir las brechas de seguridad que son generadas por los usuarios.

Toda persona encargada de la seguridad de información la elaboración de políticas de seguridad Cloud que limiten la libertad de los usuarios para borrar elementos del sistema, y de esta forma protegerse ante el ataque de software malintencionado y además de impedir que personas ajenas a la organización accedan o corrompan los datos.

Es relevante conocer la normatividad existente, internacional y de Colombia para el manejo de Cloud Computing, la cual nos mostrara las garantías que brindan, y como podemos actuar en caso de presentarse alguna filtración de nuestra información al utilizar esta tecnología.

# BIBLIOGRAFÍA


Calderón R, Guzmán G, Salinas J. (2011). Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario. Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral

Díaz Carreño, Emmanuell. Modelo y prototipo de servicios de computación en la nube para estudiantes y profesores de la escuela de ingeniería de sistemas e informática de la Universidad Industrial de Santander. Trabajo de Grado Ingeniero de Sistemas. Bucaramanga: Universidad Industrial de Santander. Facultad de Ingenierías Físico-Mecánicas, 2012.

Gonzalo Andrés Moreno Gómez, Jurisdicción aplicable en materia de datos personales en los contratos de cloud computing: análisis bajo la legislación colombiana, Junio 2013, Disponible desde Internet: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Jurisdiccion-y-cloud-Gonzalo-Moreno-2013.pdf

María Carmen España Boquera. Servicios avanzados de Telecomunicación, España 2008.

Martine van der Steeg, Johannes W. van den Bent. EXIN Cloud Computing Foundation, Edición febrero 2013.

NTC 1486:2008, Documentación. Presentación de Tesis, Trabajos de Grado y Otros Trabajos de Investigación.

NTC 4490:1998, Referencias Documentales Para Fuentes de Información Electrónicas.

NTC 5613:2008, Referencias Bibliográficas.Contenido, Forma y Estructura.

Sandra Jaramillo Marín. (2011). Manual Para la Presentación de Trabajos de Grado, Recuperado de: http://docencia.udea.edu.co/metodologiaIV/ejemplo.html

Serrano Latorre, Jairo D Heymann Pignolo, Elisa, César Galo bardes, Eduardo, UniversidadAutónoma De Barcelona. Departament D'Arquitectura De Computadors I Sistemes Operatius, Vulnerability Assessment for Complex Middleware Interrelationships in Distributed Systems, Septiembre 30 de 2013 [online], Disponibledesde Internet: http://www.tdx.cat/bitstream/handle/10803/129506/jdst1de1.pdf?sequence=1

## WEBGRAFÍA


Abel Suing. 2008. Documento Las líneas de investigación. [online], Disponible desde Internet:http://www.slideshare.net/abelsuing/definicin-de-las-lneas-de-investigacin

Agencia Europea de Seguridad de las Redes y de la Información (ENISA), 2009, Beneficios, riesgos y recomendaciones para la seguridad de la información [online], Disponible desde Internet: https://www.enisa.europa.eu/activities/risk-management/files/.../file

Centro i-CREO. (2013). Cloud Computing, [online], Disponible desde Internet: http://www.femeval.es/informesymanuales/Documents/i-CREO%20CLOUD%20COMPUTING/files/cloud%20computing.pdf

CRC, Agenda Regulatoria 2015-2016 [online], Disponible desde Internet: https://www.crcom.gov.co/uploads/images/files/2014/Actividades_Regulatorias/AgendaRegulatoria20152016/Propuesta_AgendaRegulatoria_2015-2016_20141030.pdf

CSA. Marzo de 2010. Top Threats to Cloud Computing V1.0[online], Disponible desde Internet: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

DECRETO 1377 DE 2013 [online], Disponible desde Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646#0

DECRETO 886 DE 2014 [online], Disponible desde Internet: http://www.gesdatos.co/wp-content/uploads/DECRETO-886-DEL-13-DE-MAYO-DE-2014.pdf

LEY ESTATUTARIA 1581 DE 2012 [online], Disponible desde Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Luis Saiz Gimeno, Miguel A. Arroyo, Alfonso González de Lama, German Realpe, Diego Rodríguez Herrero, Seguridad informática en la nube (cloud compunting), 5 de Junio 2014 [online], Disponible desde Internet:https://www.youtube.com/watch?v=e_Mlu-z1ikA

INTECO. 2011, Seguridad y privacidad del Cloud Computing. [online], Disponible desde Internet: http://www.inteco.es/file/2KMNG7mbyKb6gqdnJquPKw

MakeSoft, Marco legal del Cloud Computing: la Ley de Protección de Datos, online], Disponible desde Internet: http://www.makesoft.es/es/marco-legal-del-cloud-computing-la-ley-de-proteccion-de-datos/

María Guilarte, 2014, Virtualización y cloud computing [online], Disponible desde Internet: http://muycloud.com/2014/01/21/virtualizacion-cloud-computing/

Mesa Sectorial Cloud Computing, abril 2010, Cloud Computing – Una Perspectiva Para Colombia [online], Disponible desde Internet: http://cintel.co/wp-content/uploads/2013/05/16.clud_computing_Cloud-Computing-Mesa-sectorial-1.pdf

MIT, Technology Review,2011, ReCifradohomomórfico [online], Disponibledesde Internet: en: https://www.technologyreview.es/informatica/37710/tr10-cifrado-homomorfico/

NIST.Special Publication 800-145, 2011, Cloud Computing. [online], Recuperado de: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Ormandy, Tavis [online], Disponible desde Internet: http://taviso.decsystem.org/virtsec.pdf

OWASP Foundation,guía de pruebas OWASP, 2008 [online], Disponible desde Internet:https://www.owasp.org/images/8/80/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf

RSA, PKCS #11 v2.30: Cryptographic Token Interface Standard [online], Disponibledesde Internet: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf

Samuel T King, Peter M Chen, Yi-Min Wang, Chad Verbowsk, Helen J Wang, Jacob R LorchSubVirt: Implementing malware with virtual machines. 2006 [online], Disponible desde Internet: http://web.engr.illinois.edu/~kingst/spring2007/cs598stk/slides/cs598stk-subvirt.pdf

Schneier Bruce, Homomorphic Encryption Breakthrough [online], Disponibledesde Internet: https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html

# ANEXOS

## ANEXO A. ENCUESTAS

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 5 |
| Interfaces y API poco seguros | 1 |
| Amenaza interna | 7 |
| Problemas derivados de las tecnologías compartidas | 2 |
| Pérdida o fuga de información | 4 |
| Secuestro de cuenta/servicio | 6 |
| Riesgos por desconocimiento | 3 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 6 |
| Interfaces y API poco seguros | 1 |
| Amenaza interna | 5 |
| Problemas derivados de las tecnologías compartidas | 2 |
| Pérdida o fuga de información | 5 |
| Secuestro de cuenta/servicio | 4 |
| Riesgos por desconocimiento | 7 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías comparticas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las maycres amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 4 |
| Amenaza interna | 5 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 6 |
| Riesgos por desconocimiento | 2 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 5 |
| Interfaces y API poco seguros | 1 |
| Amenaza interna | 7 |
| Problemas derivados de las tecnologías compartidas | 2 |
| Pérdida o fuga de información | 4 |
| Secuestro de cuenta/servicio | 6 |
| Riesgos por desconocimiento | 3 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 4 |
| Riesgos por desconocimiento | 5 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: ✓ NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 6 |
| Interfaces y API poco seguros | 3 |
| Amenaza interna | 7 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 2 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 4 |
| Riesgos por desconocimiento | 5 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: x NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las maycres amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 5 |
| Interfaces y API poco seguros | 1 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 2 |
| Pérdida o fuga de información | 4 |
| Secuestro de cuenta/servicio | 7 |
| Riesgos por desconocimiento | 3 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Clouc Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de informaciór
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de informaciór | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 6 |
| Interfaces y API poco seguros | 3 |
| Amenaza interna | 7 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 2 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |

**Proyecto de Seguridad Informática – UNAD**
**Luis Felipe González Hernández**
**Encuesta Para determinación Principales Amenazas Cloud Computing**

La Cloud Security Alliance (CSA) en 2010 publicó un informe «Top Threats to Cloud Computing V1.0» sobre las mayores amenazas de la infraestructuras Cloud las cuales son las siguientes:

- Abuso y mal uso del Cloud Computing
- Interfaces y API poco seguros
- Amenaza interna
- Problemas derivados de las tecnologías compartidas
- Pérdida o fuga de información
- Secuestro de cuenta/servicio
- Riesgos por desconocimiento

1. Está usted de acuerdo con determinar que las amenazas descritas por la CSA son las principales de la infraestructura Cloud?

SI: X NO: ___

2. De un peso cuantitativo de 1 hasta 7 (sin repetir) a cada amenaza, donde 7 será la amenaza que tiene mayor ocurrencia o probabilidad de ocurrencia y 1 a la de menor ocurrencia.

| Amenazas | Nivel de Ocurrencia |
|---|---|
| Abuso y mal uso del Cloud Computing | 7 |
| Interfaces y API poco seguros | 2 |
| Amenaza interna | 6 |
| Problemas derivados de las tecnologías compartidas | 1 |
| Pérdida o fuga de información | 3 |
| Secuestro de cuenta/servicio | 5 |
| Riesgos por desconocimiento | 4 |