Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación


# ANÁLISIS DE LOS RIESGOS TÉCNICOS Y LEGALES DE LA SEGURIDAD EN CLOUD COMPUTING

**TRABAJO FIN DE MÁSTER**

**Carla Melaños Salazar**

2013

Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

**Máster Universitario en**
**Ingeniería de Redes y Servicios Telemáticos**

**TRABAJO FIN DE MÁSTER**

# ANÁLISIS DE LOS RIESGOS TÉCNICOS Y LEGALES DE LA SEGURIDAD EN CLOUD COMPUTING

Autor
**Carla Melaños Salazar**

Director
**Víctor Villagra**

Departamento de Ingeniería de Sistemas Telemáticos

2013

## Resumen

En la actualidad, el desarrollo de las Tecnologías de la Información está cambiando hacia el uso del Cloud Computing, el cual ha crecido rápidamente gracias a la diversidad de los beneficios que proporcionan sus servicios, sin embargo se han dejado de lado las consideraciones de seguridad de esta tecnología, que hoy en día es clave al tomar la decisión de externalizar datos y aplicaciones. La evolución del Cloud Computing debe darse mayormente en el área de Seguridad, que tiene gran importancia en el despliegue de este entorno, para garantizar la confidencialidad, la disponibilidad y la integridad de los datos.

El presente proyecto abarca un resumen de la investigación realizada por varios grupos especializados con respecto a los riesgos, amenazas y vulnerabilidades de la Seguridad de la Información en un entorno de Nube, con el propósito de suministrar una guía que minimice los riesgos, para los profesionales de IT que desean adoptar estos servicios en sus organizaciones.

Por otro lado, este proyecto incluye un análisis del cumplimiento normativo necesario para la implantación de modelos de Computación en la Nube. El método de análisis está basado en los planteamientos sugeridos por la Cloud Security Alliance (CSA) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) acerca de los aspectos que deberían ser regulados a nivel mundial, tomando en cuenta la posición del cliente y del proveedor, para que la expansión de los servicios se lo haga de forma estandarizada. El desarrollo de este campo legal se considera en estado incipiente, por lo que cada país interpreta el tratamiento de estos servicios en base a una adaptación de su legislación.

De igual forma, se ha profundizado en la revisión de las leyes ecuatorianas actuales, con el objetivo de compararlas con las recomendaciones europeas y verificar que parámetros han sido cubiertos y cuáles deben ser reformulados en una nueva legislación que contribuirá a la Seguridad de la Información en la Nube.

Finalmente, la aportación de este estudio es promover una visión general de los aspectos positivos, y mayormente de los puntos perjudiciales que afectan a la Seguridad al adoptar este ambiente tecnológico, que pueden afectar severamente la seguridad en estos ambientes virtuales.

## Abstract

Nowadays, Information Technology (IT) development is changing towards implementing Cloud Computing, which due its wide range of benefits, shows significant increment of the use of its services; however, such benefits do not take into account security constrains inherent of this technology, considerations that might be critical when decisions are taken to outsource data and IT applications. With this in mind, Cloud Computing should evolve mainly in information security area, a key sector for technology deployment on virtual environments, as data privacy, data availability and data integrity must be granted.

Based on this requirement for Cloud Computing, this dissertation project summarizes risks, threats and vulnerabilities of information security in a Cloud environment from investigations conducted by several specialized groups. The final goal of this project is to provide guidance to IT professionals to minimize security constrains when they were to consider implementing Cloud Computing in their organizations.

This study includes an analysis of required compliance of norms and regulations for implementing Cloud Computing models. The method of analysis was based on suggested approach by the Cloud Security Alliance (CSA) and the European Network and Information Security Agency (ENISA) about aspects that should be regulated globally, taking into consideration customer and provider position; however, the development of legal area is considered primitive and undeveloped; therefore, each country should understand regulations of Cloud services and should include amendments to their legislation.

On this context, this project has extended into an analysis of current Ecuadorian legislation (candidate original country), to compare with European recommendations and to verify which parameters have been covered and which must be reformulated in a new law that will contribute to Cloud Computing Information Security.

Finally, this project will help to promote a general overview of not only positive areas but also negative ones, which could be often overlooked, but might severely affect data security on virtual environments.

*Dedicado a mis padres Terecita y Carlos,*

*por su infinito amor y apoyo incondicional.*

# Índice general

## Contenido

# Índice de figuras

# Índice de Tablas

## Siglas

| | |
|---|---|
| API | Application Programming Interface |
| CEO | Chief Executive Officer |
| CPU | Central Processing Unit |
| CRM | Customer Relationship Managment |
| CSA | Cloud Security Alliance |
| DMTF | Distributed Management Task Force |
| ENISA | Agencia Europea de Seguridad de Redes e Información |
| GPU | Graphics processing unit |
| HP | Hewlett-Packard |
| IaaS | Infraestructure as a Service |
| IdP | Identity Provider |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISO | International Organization for Standardization |
| ITIL | Information Technology Infrastructure Library |
| ITSM | IT service management |
| ITU- T | Telecommunication Standardization Sector |
| JMV | Java virtual machine |
| LDAP | Lightweight Directory Access Protocol |
| NIST | National Institute of Standards and Technologies |
| PaaS | Platform as a service |
| PDA | Personal digital assistant |
| QoS | Quality of Service |
| SaaS | Software as a service |

| | |
|---|---|
| SAML | Security Assertion Markup Language |
| SLA | Service Level Agreement |
| SOAP | Simple Object Access Protocol |
| TI | Tecnologías de la Información |
| VPN | Virtual Private Networks |
| XACML | eXtensible Access Control Markup Language |
| XML | Extensible Markup Language |

# 1 Introducción

Actualmente vivimos una nueva era para las comunicaciones y la informática, notándose un cambio entre la tendencia de adquirir la última tecnología en equipamiento hacia la modalidad de delegar nuestra arquitectura tecnológica a un proveedor especialista del área, particularidad que ha dado inicio al uso masificado de servicios en la Nube.

Es muy posible que los próximos diez años las Tecnologías de la Información sufran más cambios que en toda la etapa de su desarrollo, por lo que se habrá saltado de vivir en la era de computadoras a la era del Cloud Computing. Se ha calculado que para el año 2020 nuestro universo estará digitalizado entre 30 y 40 veces más que en nuestros días, es por esto que el manejo de toda esta información debe realizarse de manera ordenada, sistemática y utilizando las mejores infraestructuras, es aquí donde la Computación en la Nube juega un factor determinante, puesto que se calcula que para el año 2030 se constituirá en el lugar donde se residirán un tercio de los datos a nivel global.

Se puede argumentar a favor del uso de los servicios de Cloud Computing que es una forma de aprovechar el conocimiento especializado por parte del proveedor, pero a la vez se debe tomar en cuenta un argumento surgido por los detractores, de que si la propia empresa no tiene una organización perfecta para la información, como se puede esperar que el proveedor lo vaya a tener? Es en este sentido donde el proveedor de servicio debe mostrar todas las garantías necesarias para persuadir a sus clientes de que Cloud Computing es una alternativa favorable.

El proveedor de Cloud debe estar organizado de tal manera, que proyecte confianza a sus clientes, ya que un incidente con alguno de ellos puede dejar huella sobre su profesionalidad y su imagen, y a la vez acarrear inconvenientes irreparables para el cliente. Por otro lado, los casos de éxito en la ejecución de los servicios será una muestra de que las soluciones tecnológicas ofrecidas son confiables, característica ayudará a dar credibilidad a sus clientes.

Vivimos en un mundo virtual, que nos facilita y automatiza varios procesos dentro de una empresa, sin descartar que también conlleve inconvenientes si se pierde de vista la gestión de dichos procesos. En este mismo concepto se puede situar la externalización de los servicios de las tecnologías de la información, dejando la Seguridad de la Información fuera de vista, pudiendo potenciar los riesgos, las vulnerabilidades y las amenazas. Por esta razón cuando un cliente va a elegir un proveedor de servicios de Cloud Computing debe realizar una elección acertada y

saber a quién está delegando el manejo de su información, ya que no cualquiera podría hacerlo adecuadamente.

Todos los procesos de innovación tecnológica atraviesan por las etapas de introducción, crecimiento y maduración, y esto no es ajeno al Cloud Computing, que puede decirse que al momento se encuentra en la fase de crecimiento, cuando se da un crecimiento exponencial y una maximización de las prestaciones, de los beneficios y de las ventajas, perdiendo de vista los problemas que podrían venir asociados. En este contexto, la presente investigación se enfoca en analizar los aspectos no tan atractivos de la Nube, que a la vez son fundamentales tomarse en cuenta antes de contratar un servicio, o cuando ya se lo tiene y se deba verificar el desempeño del proveedor en este campo. De la mano de estudios especializados de varias organizaciones, se pretende plantear un conjunto de alertas, sugerencias y buenas prácticas que colaboren a evitar los huecos de la Seguridad de la Información tanto en la parte técnica como en la legal.

## 1.1 Objetivos

### 1.1.1 Objetivo General

Realizar un análisis exhaustivo de todos los riesgos potenciales en el área técnica y legal que sufre la Seguridad de la Información al hacer uso de servicios de Cloud Computing, el cual sirva como una guía de buenas prácticas en el manejo de la información en proveedores de servicio y clientes de la Nube, específicamente en el territorio ecuatoriano, donde se carece de lineamientos específicos debido a la reciente aparición del Cloud Computing en el país.

### 1.1.2 Objetivos Específicos

- Examinar exhaustivamente la investigación realizada por las Organizaciones CSA, ENISA y NIST con respecto a los riesgos, amenazas y vulnerabilidades técnicas que presenta una infraestructura de Cloud Computing.
- Investigar cuáles son las normativas Europeas que están dando cobertura a los servicios de Cloud Computing.
- Comparar la legislación Ecuatoriana existente con la normativa Europea para establecer las diferencias y los puntos que se deben proponer como mejora de la normativa.

## 1.2 Estructura del Documento

En el Capítulo 1, se presenta un marco introductorio para posicionarse en el entendimiento del nuevo paradigma de Cloud Computing y la visión que ha provocado este cambio a nivel global.

En el Capítulo 2, se define todos los conceptos asociados al Cloud Computing, con un breve análisis sobre el entorno y los beneficios que presenta en el ámbito técnico,

económico y estratégico para los posibles clientes de la Nube. A continuación, se describe las ventajas y desventajas que pueden venir asociadas al adoptar este tipo de servicios. Se muestra además, los Modelos de Implantación de acuerdo al tipo de Nube y los Modelos de Servicio que se ofrecen en el Cloud Computing ya sea un modelo IaaS con énfasis en servicios de Infraestructura, un modelo PaaS encaminado a los servicios de Plataforma o un modelo SaaS referente a los servicios de Software.

Una vez revisada la introducción, en el Capítulo 3, se estudia la Seguridad en Cloud Computing, que constituye la parte esencial de este trabajo de investigación, para ello se menciona proyectos de varios organismos como la ITU, el NIST, OASIS entre otros, que han profundizado en el estudio de ésta temática y han publicado sus respectivos aportes.

En el Capítulo 4, se profundiza el estudio de los riesgos y vulnerabilidades que un servicio de Cloud Computing debe enfrentar, tomando como base los documentos generados por la CSA sobre las siete principales amenazas para el Cloud Computing y la guía sobre áreas críticas donde se revisa los trece dominios de Cloud. Por otro lado, el análisis de la ENISA además de ahondar el estudio de los riesgos y las vulnerabilidades, se encamina hacia un "Análisis del Riesgo" basado en la técnica planteada por la Norma ISO 27005:2008, examinando riesgos políticos y organizativos, técnicos, legales y riesgos no específicos a la Nube. Posteriormente utilizando como base el informe "Guías para Seguridad y la Privacidad en Cloud Computing" del NIST, se considera los nueve aspectos clave para la Seguridad de la Información en la Nube.

El Capítulo 5, comprende una revisión de las Recomendaciones Legales que ha planteado la CSA en el reporte "Cloud Compliance Report" y la ENISA en el documento "Beneficios, riesgos y recomendaciones para la Seguridad de la Información", tomando como base la normativa de la Directiva 95/46/CE de aplicación en el Espacio Económico Europeo y las Leyes Españolas: Ley Orgánica de Protección de datos de carácter personal 15/1999 (LOPD) y el Real Decreto 1720/2007-Reglamento de desarrollo de la Ley Orgánica 15/1999 (RLODP).

Finalmente, en el Capítulo 6, se revisa la situación actual del Ecuador en el ámbito legal con respecto a la protección de datos personales y el desarrollo de los nuevos servicios tecnológicos, con el fin de efectuar una comparativa de las leyes existentes como la Ley del Sistema Nacional de Registro de Datos Públicos y la Ley de comercio electrónico, firmas electrónicas y mensajes de datos, en base a los lineamientos de las normativas Europeas, todo esto con el propósito de plantear una propuesta de los puntos que podrían incluirse en un nuevo marco regulatorio ecuatoriano que dé cobertura específica a los servicios de Cloud Computing.

# 2 Cloud Computing

El concepto de Cloud Computing ha sido difundido y estudiado en los últimos tiempos, a partir de lo que varias organizaciones han establecido el suyo propio como es el caso del NIST que lo ha definido así: "Computación en la Nube es un modelo para permitir el acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos de red configurables, que pueden ser provistos rápidamente y liberados con un mínimo esfuerzo de administración e interacción con el proveedor del servicio". [1]

La CSA también ha establecido su concepto, mencionando: "La Nube es un modelo a la carta para la asignación y el consumo de computación, a través de la cual se puede utilizar una serie de servicios, aplicaciones, información e infraestructura compuesta por reservas de recursos de computación, redes, información y almacenamiento. Estos componentes pueden orquestarse, abastecerse, implementarse y desmantelarse rápidamente, y escalarse en función de las dimensiones para ofrecer unos servicios de tipo utilidad." [2]

A partir de estas dos definiciones, se obtiene un concepto más básico que puntualiza al Cloud Computing como un medio para suministrar recursos de IT como servicios. Todos los servicios ofrecidos van a ser proporcionados a través de la Nube, interpretada como una red de telecomunicaciones pública, generalmente la Internet, con lo cual el acceso a los servicios informáticos se lo hace de forma independiente a los sistemas físicos o ubicación real de los equipos.

El uso de servicios de Cloud Computing permite a los profesionales de IT minimizar el tiempo que les toma realizar actividades de diseño, implementación y mantenimiento de sus sistemas de cómputo y/o telecomunicaciones, y de éste modo centrar su atención en actividades estratégicas y funcionales, que colaboren a procesos administrativos y comerciales de sus propias empresas.

Hoy en día, son varias las empresas que están apostando por el Cloud Computing como el caso de Google o Amazon que han sido pioneras en sacar a la luz el concepto de la Nube. Amazon inició ofreciendo el servicio S3[1], el cual ofertaba a las compañías, grandes espacios de almacenamiento por una fracción del costo de tener discos duros físicos. La estrategia que ahora utilizan estos proveedores es introducir en el cliente la idea de que sería grandioso comprar recursos computacionales el momento que se necesite y con la capacidad que se requiera, sin invertir en equipamiento excesivo. [3]

[1] S3: Simple Storage Service. Amazon S3 es almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores la informática a escala web.

Otro concepto estratégico es el que ha introducido Jeff Bezos CEO de Amazon, al mencionar que: "Si las personas no generan su propia electricidad, por qué deben generar sus propios servicios de computación? ¿No es mejor delegarlos a los especialistas? " [4].

Cisco también incursiona en este mercado, al ofertar a sus clientes, que mayormente serán los proveedores de servicio, el equipamiento necesario para que desplieguen este tipo de servicios. Los Centros de Datos son su principal objetivo, ya que ésta entidad viene a constituir la unidad básica del Cloud Computing, a través de la cual se extenderán cualquier tipo de servicio IaaS, PaaS o Saas.

Otro factor relacionado con el Cloud Computing, es la red asociada a las comunicaciones de los usuarios. Ésta red debe estar preparada para soportar aplicaciones, ser convergente para datos, voz y video, tener múltiples configuraciones de QoS, tener un gran ancho de banda, poseer simetría y baja latencia, ser redundante y segura, en pocas palabras contar con todas las características para ser el mejor aliado de los servicios en la Nube.

Cloud Computing se convierte poco a poco en una herramienta diaria, que ya ha sido usada desde hace varios años, por miles de personas desde sus computadores, teléfonos inteligentes y tabletas, pero que no se lo había conceptualizado, ahora poco a poco irá transformando el modo en como los usuarios empresariales e individuales hacen uso de la tecnología, para crear mejores y mayores oportunidades.

Pero cuál es el motivo por el que las compañías pueden mostrarse renuentes a utilizar este tipo de servicios? El activo más preciado de una organización son sus datos, traducida en información general de la empresa y la información confidencial y sensible relacionada con el núcleo del negocio, como en una industria financiera o de salud, que nadie desea ponerla fuera de su vista y peor aún en terceros que no garanticen seguridad, disponibilidad, e integridad de sus datos.

Según la Empresa Gartner[2], líder mundial en investigación y consultoría de Tecnologías de la Información, en el 2011 se tuvo un crecimiento en el uso de servicios de la Nube superior al 20% con respecto al 2010. Para el 2015, se prevé un incremento del 200%, llegando a una inversión aproximada de $177.000 millones. En la Figura 1, se observa la tendencia de crecimiento en la inversión en servicios de Cloud Computing desde el 2010 hasta el 2015.

[2] Gartner: http://www.gartner.com/technology/initiatives/cloud-computing.jsp

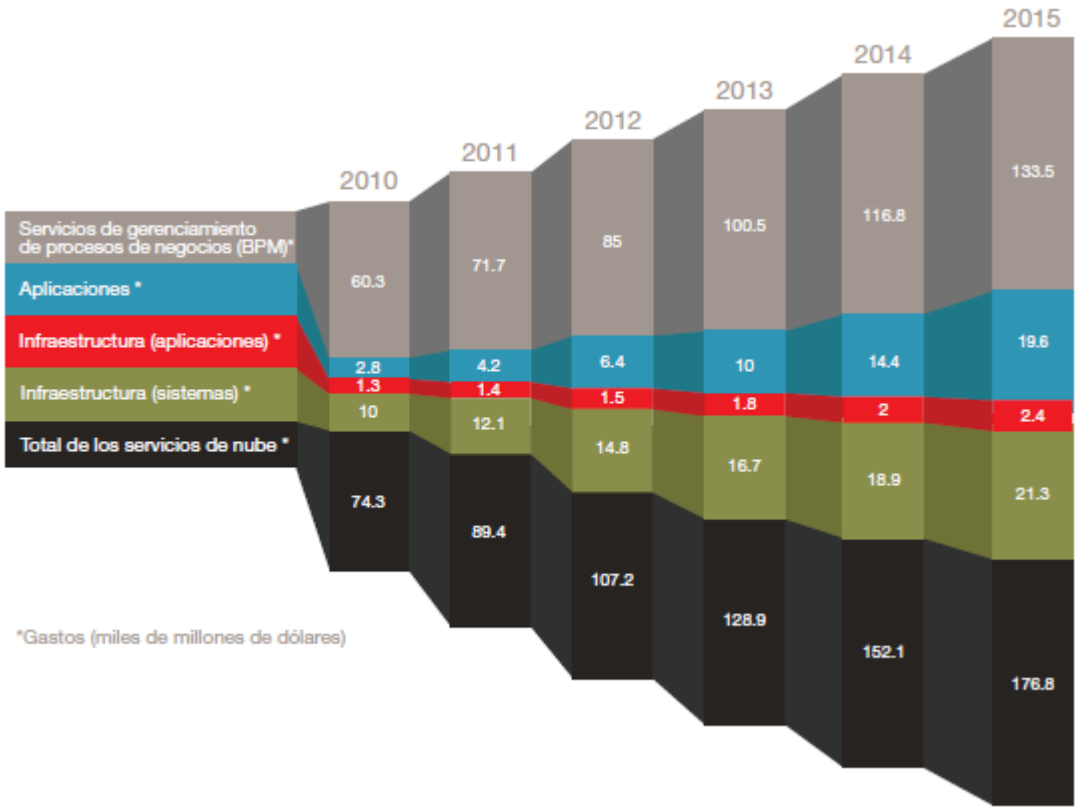


Figura 1. Estadísticas de Crecimiento de la inversión de Cloud Computing

Cómo confirmación de la importancia del Cloud Computing en la actividad científica y de investigación, la IEEE ha creado el portal web IEEE CLOUD COMPUTING[3], el cual se ha convertido en una fuente de información para todo lo relacionado a este tema. Aquí se puede encontrar artículos, conferencias, guías, estándares de interoperabilidad y las últimas innovaciones presentadas, lo cual se ha tomado como una fuente bibliográfica para el desarrollo de este proyecto.

## 2.1 Características del Cloud Computing

De acuerdo al NIST, en su definición de Cloud Computing [1], se tienen cinco características esenciales:

a) Auto servicio bajo demanda: Un usuario puede utilizar los recursos cuando considere necesario, ampliando o disminuyendo el tamaño de acuerdo a sus requerimientos momentáneos, sin precisar la interacción humana con el proveedor de servicios.
b) Acceso amplio a la red: Disponibilidad de los recursos de red para acceder desde cualquier dispositivo, sea un computador, un teléfono móvil o una Tablet, mediante el uso de mecanismos estandarizados.

[3] IEEE Cloud Computing: http://cloudcomputing.ieee.org.

c) Recursos en grupo: Debido a la variación del uso de recursos computacionales, se plantea la opción de que se lo haga agrupando múltiples usuarios y que éstos puedan ajustarse en base a la demanda de los mismos, evitando así el desperdicio.
d) Escalabilidad: Los recursos ofrecidos por el proveedor se adaptan a los requerimientos del cliente, por ejemplo las capacidades solicitadas por un usuario pueden ser rápida y dinámicamente aprovisionadas, en algunos casos hasta de forma automática, dando la percepción al usuario que el proveedor tiene recursos ilimitados y están siempre disponibles.
e) Servicio a la medida: Los sistemas de Cloud Computing controlan y optimizan automáticamente el uso de los recursos, aprovechando la capacidad de medición que hace posible que los mismos puedan ser monitoreados, controlados y emitan informes, lo que brinda transparencia del servicio ante el proveedor y el usuario.

## 2.2 Ventajas del Cloud Computing

Las ventajas que Cloud Computing ofrece a los usuarios de este nuevo servicio se las puede agrupar en los siguientes ámbitos [5, 6]:

### 2.2.1 Ventajas Técnicas

- Soporte técnico 24x7x365 en problemas eventuales que se den en cualquiera de los servicios contratados.
- Incremento o disminución de la capacidad contratada, realizando mediciones o pruebas de rendimiento en caliente, lo cual evita compras innecesarias de equipamiento.
- Elimina los problemas de seguridad al contar con herramientas y especialistas para brindar la protección necesaria a los datos y a los sistemas de los clientes.
- La empresa cliente se despreocupa de contar con un sistema de respaldo de datos, puesto que el proveedor de servicios de Cloud se encargará de replicar la información crítica y mantener actualizados sus sistemas de backup.
- Desaparecen las limitaciones de almacenamiento, de acceso a la información y de respaldos de energía eléctrica, los equipos críticos pasan a ser manejados por el proveedor de Cloud, quien usará potentes plataformas de computación de alta disponibilidad.
- Alta confiabilidad, disponibilidad e integridad de los datos de la empresa cliente, al no tener que ser almacenados en equipos de la propia compañía.
- Uso de virtualización en la mayoría de los sistemas y plataformas.

### 2.2.2 Ventajas Sociales, Económicas y Estratégicas para el usuario

- Implementación de sistemas con menor riesgo debido al respaldo del proveedor de servicios de Cloud, que a su vez mantiene otros clientes probando el mismo sistema y en procesos de mejora continua.
- Minimiza el tiempo de implementación de un nuevo sistema, que en la actualidad representa uno de los problemas más significativos en el desarrollo de nuevas aplicaciones.
- Proporciona una ventaja financiera sustancial al no requerir una gran inversión para la puesta en marcha de una nueva solución tecnológica, reduce notablemente los costos y no necesita la adquisición de equipamiento propio para utilizar tecnología sofisticada.
- Modalidad de Pay-as-you-go[4], la cual consiste en pagar únicamente por lo que se utiliza.
- Elimina los gastos asociados al tema de adquisición de software y licencias, aspectos como la renovación, el mantenimiento y las horas de soporte técnico desaparecen, ya que será parte de los costes que sufraga el proveedor de Cloud, quien incluye en el costo del servicio todos estos agregados.
- Proporciona personal especializado en sistemas informáticos quien está a cargo de los servicios en la Nube, por lo que la empresa cliente no necesita incorporar nuevo personal para la administración y funcionamiento de estos sistemas. En la actualidad las empresas recurren a terceros para solicitar asesoría y gestión dentro de su compañía.
- Introduce y refuerza el concepto de teletrabajo, permitiendo el acceso a todos los sistemas de la empresa desde lugares remotos, así los empleados de la empresa cliente pueden trabajar de forma no presencial desde donde deseen, brindando a la vez una sensación de bienestar, disminuyendo el estrés y aumentando la productividad.
- Optimización del uso de recursos físicos, computacionales, humanos y básicamente financieros.

## 2.3 Desventajas del Cloud Computing

A la vez que se han mencionado varias de las ventajas de implementar una solución de Cloud Computing, es necesario hacer una revisión de las desventajas que presenta, a continuación se menciona las más importantes [7, 8] :

- Dependencia de la red de acceso para ingresar en la plataforma donde se encuentran alojadas las aplicaciones.

[4] Pay-as-you-go: Pago según el uso.

- Contratación de un mayor ancho de banda en la empresa cliente e implementación de políticas de calidad de servicio, para evitar problemas de cuellos de botella en el acceso a las aplicaciones, o accesibilidad lenta que puedan poner en juego el desempeño de las aplicaciones.
- Desconfianza de los clientes, al no tener en su propiedad la información de su empresa y pasar a manos de terceros. Se puede percibir un sentimiento de que la información que está en la Nube ya no le pertenece.
- Desconfianza del desempeño del equipamiento, puesto que hasta los equipos más confiables han tenido fallos, de lo que tampoco estarían exentos los proveedores de servicios de Cloud. Ningún dispositivo es infalible y puede tener problemas.
- Al perder el control de la ubicación de servidores y equipos en general, puede provocar cadenas de intermediarios, que al momento de suscitarse un problema causen entorpecimiento en el tiempo de respuesta de la solución del inconveniente y esto empeore la calidad del servicio.
- Existirá una dependencia indiscutible hacia el proveedor de servicios de Cloud Computing, por ejemplo si el desarrollo de una aplicación o sistema es realizada por el proveedor, éste no proporcionará el código fuente, y así el cliente está ligado a dicho proveedor quien será el único que pueda ofrecerle mejoras.
- Si la empresa cliente desea cambiar de proveedor de servicios de Cloud, el proceso de migración puede ser una tarea muy complicada para el departamento de IT.
- Y el problema más importante es el uso inadecuado de la información almacenada en el proveedor, pues éste podría revelar información confidencial acerca de sus estrategias, planes futuros o simplemente sobre el desarrollo de la empresa, recursos que son útiles para la competencia y que podría estar riesgo.

## 2.4 Modelos de Implantación

Una infraestructura de Cloud Computing puede funcionar en cualquiera de los siguientes modelos expuestos:

- Nubes públicas
- Nubes privadas
- Nubes híbridas

### 2.4.1 Nube Pública

La infraestructura y los recursos computacionales se encuentran disponibles para el público en general a través de la red pública de Internet. Está manejada por un proveedor que a la vez puede mezclar diferentes clientes en los servidores, sistemas de almacenamiento y la infraestructura general de la Nube. Esto es adecuado si el cliente no tiene inconvenientes al compartir espacio con otros usuarios.

Como ejemplo de Nubes públicas se mencionan a: IMB Smart Cloud[5], SunCloud[6], Google AppEngine[7], Amazon Elastic Compute Cloud (Amazon EC2)[8], Microsoft Windows Azure[9], entre otros.

### 2.4.2 Nube Privada

Una Nube privada es aquella que permite el acceso a una sola organización la cual puede ser administrada por el proveedor de servicios o por la misma empresa. La infraestructura y los recursos computacionales son propios de la empresa y pueden estar alojados en el propio perímetro de la organización conocida como una Nube privada In-Situ o a la vez colocada en las instalaciones del proveedor la cual sería una Nube privada externa. El beneficio que representa para las empresas es que tienen dominio total sobre las aplicaciones desplegadas y mayor seguridad en lo referente la información y datos propios, pero también tiene el problema de los sistemas tradicionales que es la ampliación de los recursos.

### 2.4.3 Nube Híbrida

Este tipo de infraestructura corresponde a una fusión de los dos modelos anteriormente mencionados. Esto se traduce en un nuevo modelo en el que la organización es propietaria de cierta parte (áreas en las cuáles se maneje información sensible y confidencial) y aprovechar los servicios ofertados por una Nube pública en aquellas áreas donde pueda resultar más adecuado.

Posiblemente este modelo sea uno de los más utilizados en adelante por las compañías, quienes no quieren poner en riesgo el tema de la Seguridad de la Información.

## 2.5 Modelos de Servicio

Existen tres modelos que describen la prestación de los servicios de Cloud Computing, los cuales se detallan a continuación [9] :

[5] IBM Smart Cloud: http://www.ibm.com/cloud-computing/us/en.
[6] SunCloud: http://www.suncloudoptics.com.
[7] Google AppEngine: ttps://cloud.google.com/products.
[8] Amazon Elastic Compute Cloud (Amazon EC2): http://aws.amazon.com/es/ec2.
[9] Windows Azure: http://www.windowsazure.com/en-us.

### 2.5.1 IaaS – Infrastructure as a Service

El proveedor de servicios de Cloud Computing entrega al cliente la infraestructura básica de computo con recursos como procesamiento, almacenamiento, y equipamiento de red con la finalidad de que la empresa haga uso de estos recursos para desplegar y ejecutar software, sistemas operativos y aplicaciones. Los servicios que se pueden levantar en esta infraestructura son: base de datos, alojamiento Web, entornos de desarrollo de aplicaciones, servidores de aplicaciones, streaming de video y otros.

La ventaja al utilizar este modelo es que el cliente evita la adquisición de los recursos, puesto que el proveedor los ofrece como objetos virtuales (entorno virtualizado) los mismos que son accesibles a través de una interfaz de usuario, así no hay desaprovechamiento de recursos, y su utilización es eficiente y bajo demanda.

Un proveedor de IaaS al hacer uso de la tecnología de virtualización ofreciendo desplegar máquinas virtuales rápidamente, que reducen significativamente el tiempo de ejecución de un proyecto, y garantizando su funcionamiento gracias a las medidas que implementa el proveedor en su centro de almacenamiento, con características ambientales adecuadas, respaldos eléctricos, sistemas de prevención y extinción de incendios, sistemas de protección de la seguridad física, etc., que normalmente la empresa cliente no posee en sus instalaciones y que al querer implementarlo representaría un costo elevado. Se debe recordar que es el proveedor quien está a cargo de la Infraestructura, pero es el cliente quien está a cargo de las aplicaciones, por lo tanto él deberá encargarse de la seguridad lógica de sus datos y de sus sistemas.

Un ejemplo de Proveedor de IaaS es Amazon Web Services[10] que de acuerdo a su definición es "Un conjunto completo de servicios de infraestructuras y aplicaciones que le permiten ejecutar prácticamente todo en la Nube, desde aplicaciones empresariales y proyectos de grandes datos hasta juegos sociales y aplicaciones móviles".

En la Figura 2 se muestra el sitio Web de Amazon Web Services, donde promocionan las características más importantes de contratar este servicio: bajo coste, elasticidad al instante, accesibilidad y flexibilidad y seguridad.

[10] Amazon Web Services: http://aws.amazon.com.

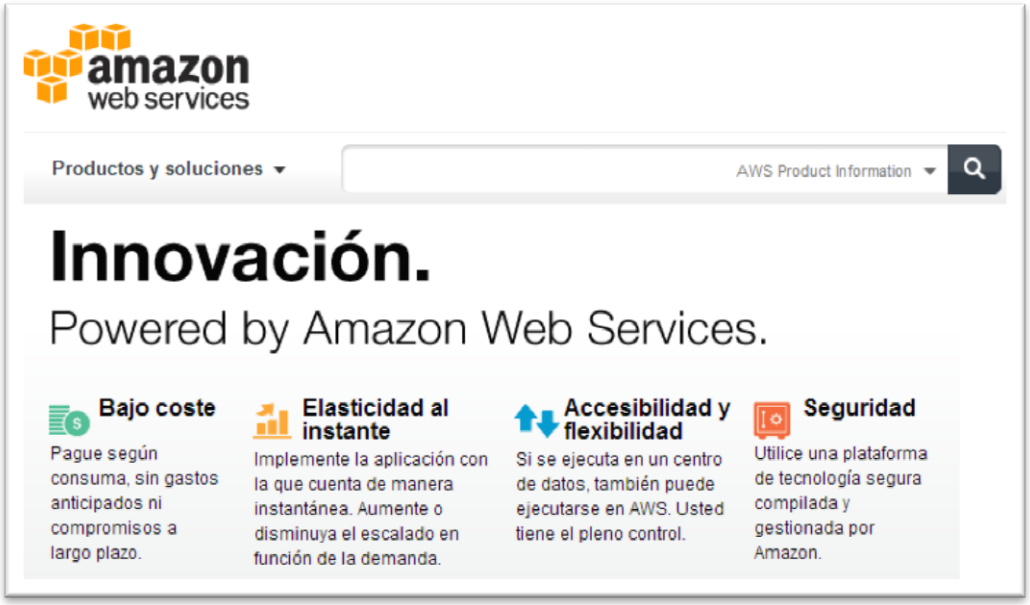


Figura 2. Presentación del Servicio de Amazon Web Services

Ejemplos de clientes que usan servicios IaaS son: Harvard Medical School y Virgin Atlantic Airways.

### 2.5.2 PaaS – Platform as a Service

El modelo PaaS propone ofrecer al cliente un conjunto de herramientas y SDKs[11] para el desarrollo de software y aplicaciones Web, es así como el mismo cliente realiza el despliegue de sus aplicaciones, tal como construir una aplicación en un tercero.

El modelo anterior evita la adquisición de hardware como servidores, respaldos eléctricos, equipos de seguridad, para este caso también prescinde de la instalación de sistemas operativos, sistemas de bases de datos y servidores de aplicaciones, ya que todo esto viene incluido en la plataforma que el proveedor brinda a sus usuarios. El usuario no gestiona la infraestructura donde corren sus aplicaciones, pero si tiene un total dominio sobre ellas, así la administración de las aplicaciones situadas en un entorno PaaS es más sencilla que en un entorno tradicional.

La principal ventaja de este servicio es que los desarrolladores de software pueden tener fácil accesibilidad a la programación de las aplicaciones, independientemente de la ubicación geográfica, debido a que el acceso se lo realiza mediante la Internet. PaaS viene a remplazar al hosting tradicional.

Casos de éxito que han aparecido en el mercado son: Google App Engine, SalesForce y Azure de Microsoft. Google App Engine [10] es el más sobresaliente en ésta categoría y está dándose a conocer por permitir el desarrollo y el alojamiento de

[11] SDKs: Software Development Kit.

aplicaciones web en su extensa infraestructura, en primera instancia de forma gratuita, utilizando varios lenguajes de programación como Java estándar que incluye JVM, servlets Java y lenguaje de programación Java, o cualquier otro lenguaje que utilice un compilador basado en JVM como JavaScript o Ruby[12]. También ofrece la opción de utilizar Python[13] que incluye un rápido intérprete y la biblioteca estándar Python. Posteriormente, la aplicación se ejecuta en la infraestructura de Google sin necesitar ningún servidor adicional.

El servicio gratuito de Google App Engine tiene una capacidad de 500 MB de almacenamiento, si se necesitara un incremento, hay la opción de ampliarlo de acuerdo a los recursos que la aplicación utilice tanto en almacenamiento como en ancho de banda, pagando a Google una tarifa en base a los gigabytes necesitados. La Figura 3 muestra la Web perteneciente al servicio de Google App Engine.

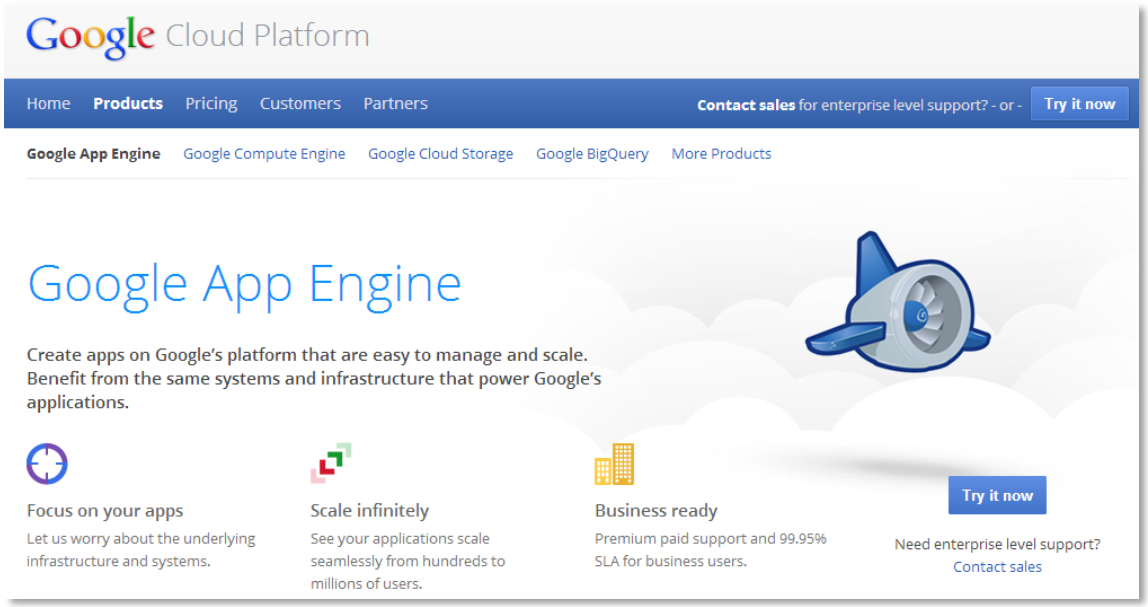


Figura 3. Captura de la Web de Google App Engine

### 2.5.3 SaaS – Software as a Service

SaaS es un modelo que consiste en un despliegue de software, específicamente una aplicación informática propietaria del proveedor que es ofrecida como un servicio. El cliente no gestiona ni servidores, sistemas operativos ni temas de almacenamiento; únicamente debe configurar ciertos parámetros, editar preferencias y ejecutar una administración con privilegios limitados para finalmente hacer uso de la aplicación.

[12] Ruby: http://www.ruby-lang.org/es.
[13] Python: http://www.python.org.

Todos los recursos computacionales e infraestructura necesaria donde se despliega la aplicación es propiedad del proveedor, evitando así que el cliente implemente software o hardware, y realice mantenimiento o procesos de actualización. Los parámetros de seguridad son controlados por el proveedor de servicio.

Este tipo de servicio se diferencia de uno en entorno convencional porque elimina en su totalidad la adquisición de software y licencias por cada usuario, por lo contrario en las aplicaciones SaaS el costo está basado en el uso bajo demanda y no en el número de usuarios.

Una aplicación SaaS puede ser accesible a través de la Internet, independizando a los usuarios de la ubicación física, y aporta a la organización una mayor flexibilidad y evita el uso de tecnologías más complejas de comunicaciones como las redes privadas virtuales.

Ejemplos de aplicaciones de servicios SaaS son: aplicaciones para almacenamiento de datos: SugarSync[14], aplicaciones de correo electrónico que es el servicio más extendido: Gmail, Yahoo, Hotmail; aplicaciones para compartición de ficheros: Windows SkyDrive[15], aplicaciones como gestores de contenidos multimedia: Flickr, aplicaciones para gestionar la relación con el cliente: CRM[16] que son ofertadas por Oracle, Salesforce, etc. y en general una amplia variedad de aplicaciones que están disponibles como Google Apps[17] que es un servicio de Google que reúne varios productos como Google Calendar, Talk, Docs, Sites, entre otras. Estas aplicaciones son gratuitas para usuarios personales y académicos, mientras que para usuarios empresariales se debe pagar un valor anual. En la Figura 4 se observa un extracto de la presentación de la Web de Google Apps para empresa.

[14] SugarSync: https://www.sugarsync.com.
[15] Windows SkyDrive: http://windows.microsoft.com/es-ES/skydrive/download.
[16] CRM: Customer Relationship Management.
[17] Google Apps: http://www.google.com/intl/es/enterprise/apps/business.


Figura 4. Extracto Web Google Apps

Finalmente, en la Figura 5 se muestra un diagrama esquemático con la agrupación de cada una de las plataformas propuestas en Cloud Computing (IaaS, PaaS y SaaS).

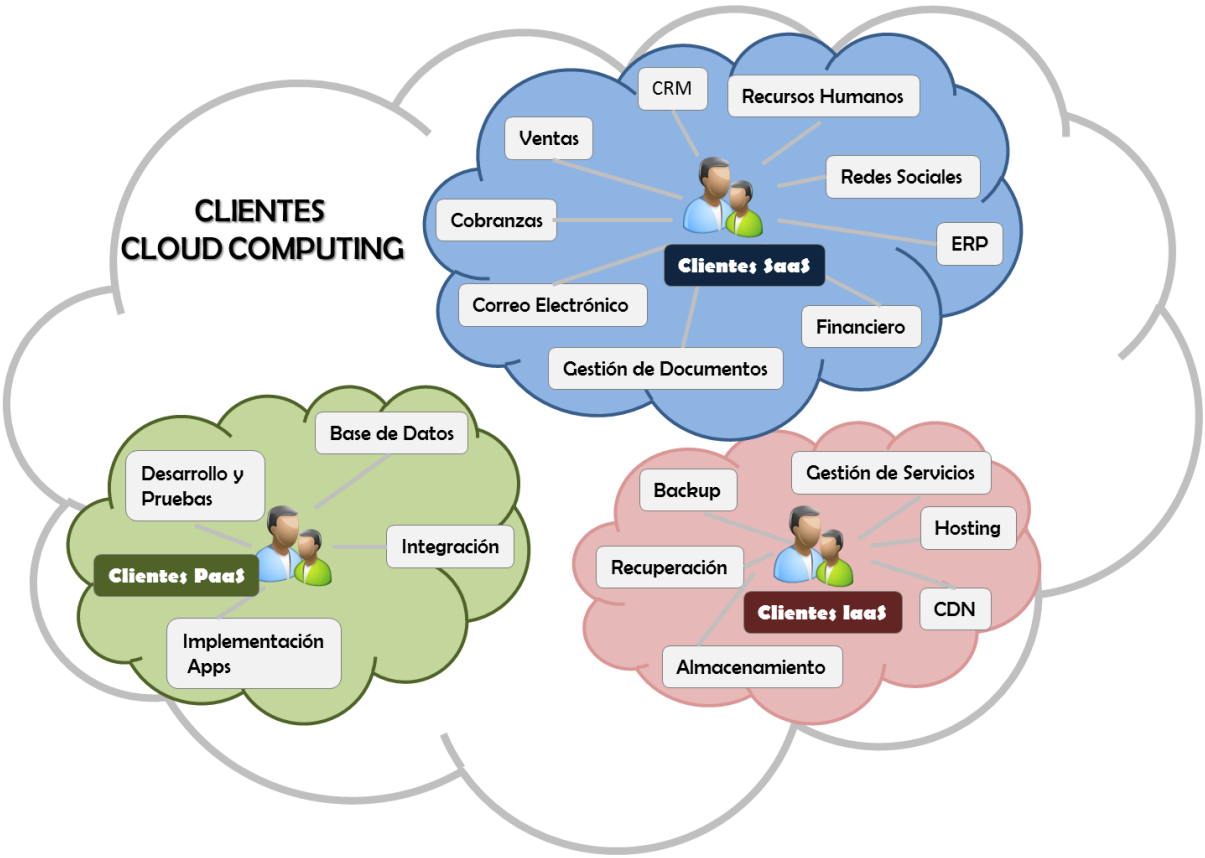


Figura 5. Esquema de los Servicios de Cloud Computing

# 3 Seguridad en Cloud Computing

## 3.1 Descripción

La seguridad es un factor clave y determinante en el diseño e implantación de soluciones de Cloud Computing. En la actualidad, la externalización de los servicios ha hecho necesario que se incrementen y reformulen las medidas de seguridad, para así garantizar que el manejo de la información en la Nube sea totalmente seguro. También se debe resaltar que la Seguridad de la Información es un tema relevante debido a que el medio para establecer la comunicación será en la mayoría de los casos a través de la Internet, que a menudo ha presentado mayores vulnerabilidades.

Un escenario de Cloud Computing puede ser visto como un entorno favorable y con opciones variadas, y a la vez ser considerado un entorno perjudicial por todos los problemas que puede acarrear. La concentración de datos en un solo lugar crea un punto muy atractivo para los atacantes, de ahí que la Nube puede considerarse un blanco perfecto para atacar simultáneamente a varios sitios o destinos [11].

Un potencial cliente se plantea varias interrogantes antes de contratar un servicio en la Nube; éstas podrían ser: Quién más verá su información? Cómo se garantiza la privacidad de los datos? Qué control de acceso se utilizará? Los datos están protegidos contra fallos? Qué pasa si la plataforma de la Nube se daña? El proveedor cuenta con sistemas de respaldos?. Con las inquietudes mostradas se ha concluido que el principal nerviosismo de los usuarios de la Nube es la privacidad, la confidencialidad, la integridad y la disponibilidad de la información. Una empresa necesita que el proveedor de servicio de Cloud Computing que pretende manejar sus aplicaciones, su información sensible o sus sistemas críticos, le garantice que está utilizando prácticas adecuadas de seguridad para mitigar los riesgos que conlleva la utilización de servicios de este tipo; es por esto que el cliente debe ser muy cuidadoso en la elección de un proveedor, esperando que el servicio que se le otorgue tenga garantías y una alta calidad. Una forma de que una compañía pueda confiar en su proveedor es respaldándose en el contrato que firmarán en conjunto, este documento es conocido como el SLA[18], que consiste en un Acuerdo de Nivel de Servicio, donde estarán explícitamente cubiertas todas las inquietudes del cliente y servirá para garantizar, tal como su nombre lo indica, los niveles de servicio en función de una serie de parámetros.

Los clientes a quienes van enfocados los servicios de Cloud Computing incluyen una variedad de clientes, desde usuarios particulares, clientes PYMES, clientes corporativos así como también clientes gubernamentales, quienes ahora son uno de los

[18] SLA: Service Level Agreement.

principales interesados en la utilización de Cloud, para reducir costos e implementar plataformas más eficientes, pero siempre garantizando que los datos estén protegidos por las normas más rigurosas, debido al tipo de información que se maneja en éste ámbito.

Los aspectos de seguridad relevantes que deben tomar en cuenta un proveedor de servicios de Cloud Computing son: seguridad física, seguridad lógica y las implicaciones legales, políticas y técnicas. Adicional, se debe considerar aspectos puntuales de seguridad como la autenticación, autorización, disponibilidad, confidencialidad, administración de identidades, integridad, auditoría, monitoreo y administración de políticas.

Para garantizar un control adecuado de la seguridad en un ambiente de Cloud, el proveedor necesita apoyarse en el cumplimiento de normas y estándares que permitan un buen manejo, control y gestión de toda la información que el cliente coloca en sus manos. Dichos estándares le permitirán evaluar su aptitud y calidad como proveedor de Cloud Computing, lo cual representa su carta de presentación hacia sus clientes, mostrándose como un proveedor con garantías en el mercado. En la actualidad no se cuenta con un estándar que certifique específicamente los servicios de Cloud Computing, sin embargo se puede hacer uso de los estándares más destacados que permiten certificar el correcto manejo de la información, entre ellos están:

- **SAS 70 [12]**

  Statement on Auditing Standards Nº 70 es un estándar de auditoría ampliamente reconocido, desarrollado por el Instituto Americano de Contadores Públicos Certificados (AICPA). Consiste en un informe sobre la estructura de control interno de la organización que presta servicios a terceros, especialmente los que afecten la estructura de control interno de la organización usuaria.

  Se pueden realizar dos tipos de informes:

  - Reporte Tipo I: Detalla la descripción de controles de la organización en un punto específico de tiempo.
  - Reporte Tipo II: Incluye la descripción de controles de la organización así como un testing detallado de los controles de la organización en un determinado período de tiempo, que al menos debe ser de seis meses.

- **SysTrust [13]**

  Permite tener un informe de auditoría sobre la fiabilidad del sistema en base a la disponibilidad, seguridad, integridad y confidencialidad de la información. No proporciona información de los controles que utiliza la organización.

- **ISO 27000 [14]**

  Las normas ISO 27000 son una serie de estándares de seguridad publicados por la ISO (International Organization for Standardization), con las mejores prácticas para el manejo de la Seguridad de la Información. A partir de ellas una compañía puede implementar un Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de minimizar el riesgo que puedan sufrir los activos de información de dicha compañía, reduciéndolos a niveles mínimos y aceptables. A través de la implantación de un SGSI, la ISO 27000 busca la preservación de la confidencial, integridad y disponibilidad de la información, y de todos los sistemas implicados en su tratamiento dentro de una determinada organización.

El análisis de la Seguridad en Cloud Computing necesita distinguir el modelo que se está utilizando, ya que cada uno de ellos tiene diferentes necesidades y elementos que supervisar, por lo tanto las consideraciones de seguridad son diferentes para un servicio IaaS, PaaS o SaaS, lo único que es semejante en cualquiera de los modelos es que la seguridad es compartida entre el cliente y el proveedor de servicio, en mayor o menor grado, pero con responsabilidades divididas. En la Tabla 1 se muestra una propuesta realizada por la ENISA[19] con respecto a la división de responsabilidades Cliente/Proveedor para cada modelo de Cloud [15].

| SOFTWARE AS A SERVICE – SaaS | |
|---|---|
| ***Cliente*** | ***Proveedor*** |
| • Cumplimiento de la legislación sobre protección de datos en relación con los datos de clientes recogidos y procesados.<br>• Manejo del sistema de Gestión de Identidades<br>• Mantenimiento del sistema de Gestión de identidades.<br>• Gestión de la Plataforma de autenticación. | • Soporte de la Infraestructura (instalaciones físicas, racks, energía, refrigeración, cableado, etc.)<br>• Seguridad y disponibilidad de la Infraestructura física (servidores, almacenamiento, ancho de banda, etc.)<br>• Gestión de parches en los sistemas operativos.<br>• Configuración de la plataforma de Seguridad.<br>• Sistemas de Monitoreo.<br>• Mantenimiento de la plataforma de Seguridad (Firewall, Host, antivirus, filtrado de paquetes).<br>• Monitoreo de Registros (Logs). |

[19] ENISA: Agencia Europea de Seguridad de Redes e Información.

| PLATFORM AS A SERVICE – PaaS | |
|---|---|
| ***Cliente*** | ***Proveedor*** |
| • Manejo del sistema de Gestión de Identidades<br>• Mantenimiento del Sistema de gestión de identidades.<br>• Gestión de la Plataforma de autenticación. | • Soporte de la Infraestructura (instalaciones físicas, racks, energía, refrigeración, cableado, etc.)<br>• Seguridad y disponibilidad de la Infraestructura física (servidores, almacenamiento, ancho de banda, etc.)<br>• Gestión de parches en los sistemas operativos.<br>• Configuración de la plataforma de Seguridad.<br>• Sistemas de Monitoreo.<br>• Mantenimiento de la plataforma de Seguridad (Firewall, Host, antivirus, filtrado de paquetes).<br>• Monitoreo de Registros (Logs). |
| **INFRASTRUCTURE AS A SERVICE – IaaS** | |
| ***Cliente*** | ***Proveedor*** |
| • Manejo del sistema de Gestión de Identidades<br>• Mantenimiento del sistema de Gestión de identidades.<br>• Gestión de la Plataforma de autenticación.<br>• Gestión de parches del Sistema Operativo huésped.<br>• Configuración de la plataforma de Seguridad huésped.<br>• Monitoreo del sistema huésped.<br>• Mantenimiento de la plataforma de Seguridad (Firewall, Host, antivirus, filtrado de paquetes).<br>• Monitoreo de Registros (Logs).<br>• Sistemas de Monitoreo. | • Soporte de la Infraestructura (instalaciones físicas, racks, energía, refrigeración, cableado, etc.)<br>• Seguridad y disponibilidad de la Infraestructura física. (servidores, almacenamiento, ancho de banda, etc.)<br>• Gestión de parches en los sistemas operativos. |

**Tabla 1. Delegación de responsabilidades Cliente/Proveedor según ENISA**

## 3.2 Iniciativas Existentes

Gracias al crecimiento del Cloud Computing en los últimos años, varias organizaciones de gran influencia en el sector de las Tecnologías de la Información, las telecomunicaciones y la Seguridad de la Información, han sumado esfuerzos en realizar estudios con especialistas de cada área, con el fin de obtener información que sea de ayuda a quienes estén interesados en la adopción de servicios en la Nube. Empresas como HP, Microsoft, IBM, British Telecom, Google participan en varios de estos proyectos, colaborando con sus especialistas para potenciar la investigación en este campo.

Las iniciativas más reconocidas a nivel internacional son:

- CSA – Cloud Security Alliance
- ENISA - Agencia Europea de Seguridad de las Redes y de la Información
- NIST - Instituto Nacional de Normas y Tecnología
- DMTF – Distributed Management Task Force
- ITU- T SG 17
- OASIS

### 3.2.1 Cloud Security Alliance - CSA

La Cloud Security Alliance (CSA de aquí en adelante) es una organización Europea sin fines de lucro formada por expertos en varias disciplinas, con el objetivo de promover buenas prácticas, sobre el uso adecuado de Cloud Computing y las soluciones de seguridad respectivas. También se encargan de promover programas de formación, así como campañas de concienciación en todo lo que respecta el Cloud Computing y los requisitos de seguridad en este tipo de ambientes.

Los expertos de la CSA han debatido y posterior a ello han liberado documentación importante que sirven como guía para el manejo adecuado de este tipo de plataformas.

A su vez la CSA cuenta con un capítulo español, especialistas en el área de "Cumplimiento en la Nube", con tres grupos de trabajo, investigando sobre temas específicos como: Privacidad y cumplimiento normativo en la Nube, Sistemas de Gestión de Seguridad de la Información y Gestión de Riesgos en la Nube; y contratación evidencias electrónicas y auditoría en la Nube.

Entre los reportes publicados por la CSA está "Amenazas principales en Cloud Computing V1.0" que consiste en una identificación de las siete amenazas, que ayude a las organizaciones a entender de mejor manera los riesgos asociados al adoptar tecnologías de Cloud Computing, y la forma en cómo mitigarlos.

Otro de los reportes importantes de la Agencia es la "Guía para Seguridad en áreas críticas, de atención en Cloud Computing", que abarca una lista de recomendaciones muy útil para los profesionales o empresas que deseen adoptar servicios de Cloud Computing, ya que pueden encontrar información relevante con respecto a la seguridad, confidencialidad, disponibilidad, protección de los datos, e incluso aspectos de la parte jurídica.

Toda la información respecto a la CSA se encuentra disponible en su sitio web: https://cloudsecurityalliance.org.

### 3.2.2 Agencia Europea de Seguridad de las Redes y de la Información - ENISA

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), es una organización creada en el 2004 por la Unión Europea con el objetivo de mejorar la Seguridad de las redes y de la Información, en cuanto a la prevención, la reacción y la gestión de los problemas, a través de asesoría y el intercambio de conocimientos. Los involucrados son los países miembros de la Comunidad y un grupo seleccionado de expertos gubernamentales, catedráticos y especialistas del área de las compañías líderes en el mercado.

Debido a la rápida propagación de la tecnología, el uso constante de las redes y las tecnologías de la información en las actividades diarias tanto empresariales como personales, la ENISA se ha encargado de estudiar minuciosamente todos los aspectos relacionados a la seguridad en cada uno de los campos de aplicación por ser una preocupación creciente de la sociedad, cumpliendo así su función de informar y asesorar sobre las medidas que deban adoptarse para brindar seguridad en las redes y en los sistemas de información.

El caso de Cloud Computing no se diferencia del resto de Tecnologías de la Información, que ha tenido un boom con un crecimiento exponencial, por los beneficios que presenta, pero que a la vez es motivo de preocupación por las amenazas a las cuales se ven expuestos los datos, es así que la ENISA ha colocado su atención en un estudio minucioso y dar sus respectivas directrices.

El reporte más significativo en materia de Cloud Computing es "Beneficios, riesgos y recomendaciones para la Seguridad de la Información", el cual es ampliamente consultado y leído a nivel mundial. En este informe incluye un resumen de criterios técnicos, implicaciones jurídicas y un marco de recomendaciones concretas de cómo tratar los riesgos. La herramienta principal utilizada es el Análisis y Evaluación del Riesgo para examinar los problemas de seguridad encontrados.

Información adicional acerca de la ENISA se puede consultar en su sitio web: http://www.enisa.europa.eu/.

### 3.2.3 Instituto Nacional de Normas y Tecnología - NIST

El Instituto Nacional de Normas y Tecnología (NIST) es una entidad perteneciente al Departamento de Comercio de los Estados Unidos de América, tiene como objetivo la búsqueda de la innovación en los ámbitos de metrología, normas y tecnología como aporte para el mejoramiento de la calidad de vida, en las áreas de biotecnología, nanotecnología, Tecnologías de la Información y fabricación avanzada.

El programa de Cloud Computing fue creado en el 2010 para ayudar al gobierno de los Estados Unidos a incorporar esta tecnología en los sistemas gubernamentales dónde más convenga su uso. El objetivo es proveer un claro entendimiento del Cloud Computing y los servicios que presta.

El programa está formado por cinco grupos de trabajo que proveen orientación técnica y una guía basada en estándares para la implementación de Cloud Computing. Los grupos de trabajo son:

- Cloud Computing Target Business Use Cases
- Cloud Computing Reference Architecture and Taxonomy
- Cloud Computing Standards Roadmap
- Cloud Computing SAJACC
- Cloud Computing Security

En el capítulo de Seguridad en Cloud Computing, el NIST ha publicado varios informes como "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing", en el que se presenta una lista de los controles de seguridad que deben ser tomados en cuenta para mitigar grandes o pequeños impactos en una infraestructura.

Otra de las publicaciones importantes que ha desarrollado este grupo, es el informe "Guía para la seguridad y privacidad en Cloud Computing Público", en el que se coloca una visión general de los desafíos de la seguridad y la privacidad, y menciona las consideraciones que deben tomarse por parte de una organización en cuanto a la decisión de colocar sus datos, aplicaciones e infraestructura en un entorno de Nube pública.

Para más información publicada, se puede consultar el sitio web: http://www.nist.gov/itl/cloud.

### 3.2.4 Distributed Management Task Force – DMTF

El DMTF es una asociación de compañías que desarrolla estándares para la gestión de sistemas en entornos empresariales de IT. Debido a que el Cloud Computing y la virtualización son tecnologías que se están adoptando rápidamente en el sector

empresarial, el DMTF ha visto la necesidad de que exista una gestión interoperable de la infraestructura, entre proveedores de servicio, clientes y desarrolladores, y aunque su estudio no va específicamente dirigido hacia el área de seguridad, tiene varios trabajos relacionados con esta temática, que tienen vital importancia el momento de la interoperabilidad.

La iniciativa específica para Cloud Computing está dividida en cuatro grupos de trabajo:

- Cloud Management Working Group (CMWG)
- Cloud Auditing Data Federation Working Group (CADF)
- Software Entitlement Working Group (SEWG)
- System Virtualization, Partitioning, and Clustering Working Group (SVPC)

La aportación más sobresaliente para el área de seguridad es la del grupo Cloud Auditing Data Federation que en colaboración con la CSA han desarrollado una ontología con métricas y medidas que pueden ser expresadas a través de un protocolo de auditoría para Cloud, utilizado para satisfacer las obligaciones de nivel de servicio.

También cuenta con un grupo "Open Cloud Standards Incubator" que establece protocolos de gestión de recursos en la Nube, formatos para el empaquetado y mecanismos de seguridad para ayudar a que se facilite la interoperabilidad.

El sitio web al que se puede acceder para obtener mayor información es: http://dmtf.org/standards/cloud.

### 3.2.5 ITU-T SG17

El ITU-T SG17 es un grupo perteneciente a la Unión Internacional de Telecomunicaciones (ITU), dedicado al estudio de la seguridad en Cloud Computing en las telecomunicaciones, cuya tarea es la identificación de necesidades y el desarrollo oportuno de recomendaciones de seguridad, que posteriormente serán divulgadas con fines de asesoramiento y formación en este amplio sector.

El grupo está formado a su vez por cuatro grupos de trabajo para revisar las siguientes áreas:

- Guía para Cloud Computing en las Telecomunicaciones.
- Requisitos de seguridad y estructura de un servicio de telecomunicaciones basado en Cloud.
- Requisitos funcionales de seguridad para software como servicio (SaaS).
- Requisitos de la gestión de la identidad en Cloud Computing.

El SG17 desarrolla su investigación en torno al monitoreo continuo de la seguridad utilizando técnicas de CYBEX[20] con aplicación en entornos de virtualización y de Cloud Computing.

Adicionalmente, el SG17 considera que los controles de seguridad que deben ser aplicados en la Nube deben basarse en la norma ISO/IEC 27002 y en la UIT-T X.1051. Este tópico se ha convertido en un tema de discusión en conjunto con la CSA.

Para información adicional sobre el trabajo que ejecuta este grupo en el sitio web: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx.

### 3.2.6 OASIS - Identity in the Cloud TC

El grupo de OASIS Identity in the Cloud TC desarrolla perfiles de estándares abiertos para la implementación de la identidad, el aprovisionamiento y la gestión en Cloud Computing.

Su objetivo es abordar los problemas de seguridad que plantea la gestión de la identidad en la computación en la Nube, buscando los huecos o lagunas que los estándares de gestión de la identidad no hayan cubierto.

Mediante el planteamiento de casos de estudio, este grupo busca la interoperabilidad de los estándares actuales, el análisis de riesgos y amenazas, y la elaboración de directrices que mitiguen las vulnerabilidades.

En el informe "Identity in the Cloud Use Cases" se incluye el análisis de veinte y nueve casos de estudio, mostrando una descripción breve, el propósito, los aspectos a tomarse en cuenta y finalmente un flujo del proceso que debe seguirse para mitigar los problemas que puedan presentarse en el caso estudiado.

Los casos de estudio engloban temas de: Virtualización y seguridad en la Nube, aprovisionamiento de la identidad, auditoría de la identidad, Single Sign-On[21] federado y atributos compartidos, entre otros.

Se puede encontrar información adicional en el sitio web: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud.

[20] CYBEX: Cybersecurity Information Exchange
[21] Single Sign-On: SSO, Autenticación que posibilita al usuario el acceder a varios sistemas con una sola de identificación.

# 4 Análisis de los Riesgos y Vulnerabilidades en Cloud Computing

Los riesgos potenciales que trae el uso de un entorno de Cloud Computing se han propagado como una preocupación del sector, surgiendo varias versiones sobre ello; para enfrentar esta polémica, varias organizaciones influyentes en la Seguridad de la Información, han realizado una investigación especializada para dar a conocer los resultados como recomendaciones, que pudieran ser utilizadas por los involucrados de la Nube como proveedores, clientes y auditores de los servicios.

Para el siguiente análisis se ha tomado como línea base las iniciativas consideradas con mayor importancia y notabilidad en materia de Seguridad de la Información, especialmente en el espacio Europeo donde el uso de Cloud Computing está intensificado. Los proyectos seleccionados son:

- Cloud Security Alliance (Proyecto Europeo).
- Agencia Europea de Seguridad de las redes y la información (Proyecto Europeo).
- Instituto Nacional de Normas y Tecnología (Proyecto Norteamericano)

## 4.1 Análisis realizado en base a la Cloud Security Alliance (CSA)

Para el estudio de los riesgos y amenazas que se presentan en la Nube, se ha tomado de guía los reportes generados por la CSA, especialmente los informes "Top Threats to Cloud Computing V 1.0"[16] y la "Guía para la Seguridad en áreas críticas de atención en Cloud Computing". Estos reportes constituyen el marco de trabajo para realizar un análisis minucioso de su contenido, el cual se presenta a continuación.

### 4.1.1 Principales Amenazas para el Cloud Computing

Una solución convencional de IT, presenta sus propios riesgos, que afectan a la disponibilidad, el rendimiento y principalmente a la Seguridad de la Información. Al introducir una solución de Cloud Computing, se van a mantener estos riesgos, a la vez que varios de ellos van a ser maximizados, por la característica que tiene la Nube de concentrar los datos un solo lugar.

En la Seguridad, Cloud Computing también presenta los mismos problemas que los sistemas propios (infraestructura no externalizada), pero adicionalmente han aparecido nuevos riesgos como resultado del uso de nuevas tecnologías implementadas, como es la virtualización, las arquitecturas orientadas a servicios o las nuevas aplicaciones en la Web 2.0.

Si en una infraestructura tecnológica propia, las organizaciones colocan énfasis en resguardar la seguridad y privacidad de su información, con mayor razón en Cloud

Computing, al sentir desconfianza de que sus datos y aplicaciones residan en proveedores externos con parcial o total control de la plataforma.

Las inquietudes que se ponen de manifiesto en la seguridad en Cloud Computing se centran en la privacidad, la confidencialidad e integridad de los datos, la autenticación, la localización de los datos y otros puntos más que se detallarán a continuación:

| AMENAZA | CONCEPTO |
|---|---|
| *Amenaza 1* | Abuso y uso inadecuado del Cloud Computing. |
| *Amenaza 2* | Interfaces y APIs[22] inseguras. |
| *Amenaza 3* | Amenazas internas malintencionadas. |
| *Amenaza 4* | Inconvenientes debido a las tecnologías compartidas. |
| *Amenaza 5* | Pérdida o fuga de datos. |
| *Amenaza 6* | Secuestro de sesión o de servicio. |
| *Amenaza 7* | Riesgos por desconocimiento. |

**Tabla 2. Listado de amenazas descritas por la CSA.**

### ❖ Amenaza 1: Abuso y uso inadecuado del Cloud Computing

El acceso a las plataformas de Cloud Computing debe seguir un proceso riguroso de identificación y ser un servicio restrictivo por defecto. Un ejemplo de esto, es lo que sucede actualmente sucede cuando se quiere utilizar un servicio de Cloud de aquellos que se colocan en la Web con versiones gratuitas o con pago, pero que el único requisito que se solicita es tener una tarjeta de crédito válida, para efectuar el pago o la identificación, de este modo se puede mantener el anonimato, que es una característica que usan los delincuentes informáticos para usar la plataforma para actividades maliciosas como spammer, código malicioso u otros.

Un ejemplo es el caso de Botnets[17] alojadas en servicios IaaS, spam o bloques completos de direcciones Ip de infraestructuras Cloud que han sido publicadas en listas negras.

Las soluciones planteadas para mitigar esta amenaza son:

[22] APIs: Application Programming Interface.

- Procesos de validación y de registro muy estrictos donde se confirme los datos del usuario de forma rigurosa.
- Coordinación adecuada con la entidad que procesa los datos de la tarjeta de crédito, para verificar la identificación y evitar problemas de fraude.
- Monitoreo de las listas negras de cada bloqueo de direcciones Ip de un proveedor de Cloud Computing.

### ❖ Amenaza 2: Interfaces y APIs inseguras

Los proveedores de servicios de Cloud Computing ponen a disposición del usuario un conjunto de interfaces o APIS que pueden convertirse en un riesgo para la organización en cuanto al tema de seguridad, a la integridad, a la confidencialidad y a la disponibilidad de la información, ya que dichas APIs pueden ser el medio propicio para causar daño intencionado o problemas surgidos de modo accidental; por ello se necesita que el diseño de éstas interfaces sea realizado para proteger la seguridad de los datos que son circulan a través de ellas en aspectos como la autenticación, el acceso o el cifrado de datos.

Ejemplos de esta amenaza se dan en los accesos anónimos, o cuando el proceso de autenticación o la transmisión de contenidos se dan en texto claro, o en el caso de autorizaciones indebidas.

Las soluciones planteadas son:

- Analizar el modelo de seguridad de las interfaces del proveedor de Cloud.
- Asegurarse que se esté utilizando un método robusto de autenticación y control de acceso[18], tomando en cuenta principalmente que se haga cifrado de datos.

### ❖ Amenaza 3: Amenazas internas malintencionadas

Los usuarios internos representan uno de los problemas más conocidos de Seguridad de la Información que tiene cualquier organización, ya que ellos tienen libre acceso a todos los datos y aplicaciones que se manejan. De este modo personas maliciosas pudieran optar por esta estrategia para llegar a situarse dentro de una organización. Las compañías deben desarrollar procesos de contratación más rigurosos para precautelar que alguna persona con intenciones ocultas como un hacker, algún integrante de crimen organizado, una persona dedicada al espionaje o infiltrados del gobierno se adentren en la organización con el fin de obtener información confidencial, que en el caso de un proveedor de servicios de Cloud Computing es más sensible aún puesto que no sólo corresponde a los datos propios sino a la data confidencial de cada uno de sus clientes.

El proveedor de servicios de Cloud Computing debe revisar los procedimientos internos con respecto a los accesos físicos, los accesos a plataformas virtuales, políticas de cumplimiento y en general todas aquellas actividades donde intervenga un empleado con los datos de un cliente.

Las soluciones planteadas para esta amenaza son:

- El área de Recursos Humanos de un proveedor de servicios de Cloud debe establecer cláusulas legales y de confidencialidad en los contratos laborales.
- Exigir al proveedor transparencia en lo referente a los procedimientos usados para el manejo y la Seguridad de la Información, lo cual refleja el prestigio del proveedor y su calidad.

### ❖ Amenaza 4: Inconvenientes debido a tecnologías compartidas

Esta amenaza afecta directamente a los servicios IaaS, ya que componentes físicos como discos duros particionados, CPU y GPU no fueron diseñados con propiedades de aislamiento en el caso de ser usado en arquitecturas compartidas. Para evitar este inconveniente el hipervisor de virtualización intermedia el acceso entre los recursos computacionales físicos del anfitrión y el sistema operativo huésped, pero aún con esta estrategia se han tenido casos en los que el hipervisor ha permitido el acceso a los recursos físicos del anfitrión, involucrando incidentes de seguridad.

Los inconvenientes de tener infraestructura compartida pueden ser frenados a través de un sistema de defensa sólido que garantice a cada usuario de forma individual no causar impacto en las operaciones de ningún otro usuario que esté corriendo sobre la misma Nube del proveedor, así ninguno de los clientes pueden tener acceso a activos o a tráfico de red que no le pertenezca.

Ejemplos de esta amenaza son los casos de exploits[23] o malware que acceden a los recursos del dispositivo anfitrión, uno de ellos fue el exploit Red and Blue Pill de Joanna Rutkowska[24] o CloudBurst desarrollado por Kortchinsky Kostya que encontró fallos en las herramientas de virtualización como VMware.

Soluciones para mitigar esta amenaza son:

- Implementar buenas prácticas de seguridad para la instalación y la configuración de servicios IaaS.
- Monitorear el entorno para detectar cambios en la actividad anormal.

[23] Exploits: Software, fragmento de datos o secuencia de comandos y/o acciones.
[24] Blue Pill: http://unaaldia.hispasec.com/2009/03/otro-blue-pill-de-joanna-rutkowska.html

- Proporcionar control de acceso y autenticación robusta para el acceso de administración y de operaciones.
- Realizar auditorías y análisis de vulnerabilidades.

### ❖ Amenaza 5: Pérdida o Fuga de datos

El tratamiento de la información se ve incrementado en un entorno de Cloud debido al número de interacciones, por esto los proveedores deben tomar acciones para que los datos de sus clientes no sean manipulados, borrados o extraídos, pues la pérdida constituye un grave impacto en cualquier organización que causa perjuicios en las operaciones, desventajas económicas o problemas legales. El procedimiento de backup debe ser una acción ineludible que ayude a garantizar la integridad de los datos y así mantener la imagen y la reputación del proveedor en el mercado como un proveedor de Cloud Computing que presta garantías en sus operaciones.

Las alternativas de solución para esta amenaza son:

- Implementar APIs robustas para el control de acceso.
- Protección y cifrado de los datos en tránsito.
- Análisis de la protección de datos durante todos los tiempos de ejecución.
- Establecer mecanismos robustos para la generación de claves, almacenamiento y manejo de la información así como para la destrucción de la misma.
- Definir mediante el contrato cliente/proveedor de servicio, que la destrucción de los datos se la realice antes de que algún dispositivo de almacenamiento del proveedor sea dado de baja.
- Especificar mediante contrato las políticas de respaldo y de conservación de datos.

### ❖ Amenaza 6: Secuestro de sesión o servicio

Esta amenaza consiste en un atacante que se coloca en medio de dos máquinas y se apodera de una sesión establecida. Debido al riesgo que representa esta acción se la considera como una amenaza superior, y que en la Nube debe colocarse mayor atención para evitar que un intruso obtenga credenciales o contraseñas y luego se mantenga escondido manipulando la información, realizando transacciones o peor aún re-direccionando clientes del proveedor de servicio hacia sitios ilegítimos. En esta instancia la reputación del proveedor puede verse gravemente comprometida.

Las soluciones planteadas para esta amenaza son:

- Prohibir la compartición de credenciales entre los usuarios y los servicios.
- Implementación de técnicas de autenticación de doble factor[19], para garantizar que el proceso sea lo más seguro posible.

- Realizar un monitoreo proactivo que pueda detectar cualquier actividad no autorizada.

❖ **Amenaza 7: Riesgos por desconocimiento**

El motivo principal para que una organización tome la iniciativa de contratar un servicio de Cloud Computing es la reducción económica y de procesos de IT al no adquirir directamente hardware o software que demanden una atención personalizada del área de comunicaciones de dicha organización y demande mucho tiempo al realizar tareas que no corresponden a la línea del negocio, sin embargo esta alternativa no puede constituir un pretexto para que el cliente pierda de vista todo lo relacionado con su plataforma o infraestructura, es decir todos los aspectos técnicos.

Es conveniente que el cliente conozca datos relevantes para la seguridad como la información de que otros clientes comparten la plataforma, así puede detectar compañías que son vulnerables y que representen un peligro para su propia seguridad, o también solicitar al proveedor un registro de los intentos no autorizados que hayan sido direccionados hacia su red.

Las alternativas de solución para esta amenaza son:

- Acceso a los logs respectivos de los sistemas que está usando el cliente.
- Conocimiento parcial o total de los factores técnicos de la infraestructura.
- Monitoreo de alarmas cuando se realicen acciones con los datos críticos.

### 4.1.2 Guía para la Seguridad en áreas críticas de atención en Cloud Computing

El reporte está estructurado en trece áreas denominadas dominios, realizados con el fin de proporcionar asesoramiento en las operaciones y en la gestión de la seguridad Cloud Computing.

| | DOMINIO | CONCEPTO |
|---|---|---|
| 1 | Marco de la Arquitectura de Cloud Computing | Conceptos generales asociados a Cloud Computing. |
| 2 | Gobierno y gestión de riesgos de las empresas | Marco de gestión para la Seguridad de la Información en entornos de Nube. |
| 3 | Cuestiones legales y e-Discovery[25] | Puntos legales importantes en un entorno de Cloud Computing. |
| 4 | Cumplimiento normativo y Auditorías | Chequeo de la normativa existente y su adaptación a un entorno de Nube. |

[25] e-Discovery: Procedimiento en un pleito civil sobre el intercambio de información en formato electrónico.

| | | |
|---|---|---|
| **5** | Gestión del ciclo de vida de la Información | Conocimiento del ciclo de vida de la información y de los datos. |
| **6** | Portabilidad e interoperabilidad | Aspectos para realizar la migración a otro proveedor sin sufrir pérdidas. |
| **7** | Seguridad tradicional, continuidad del negocio y recuperación de catástrofes | Recomendaciones que garanticen mayor seguridad que en los entornos actuales. Continuidad de las operaciones. |
| **8** | Operaciones del centro de datos | Características y procedimientos del centro de datos. |
| **9** | Respuesta ante incidencias, notificación y subsanación | Procedimientos para la gestión de incidencias entre un cliente y su proveedor de Cloud. |
| **10** | Seguridad de las Aplicaciones | Amenazas de seguridad en las aplicaciones. Chequeo en cada capa de las aplicaciones. |
| **11** | Cifrado y gestión de claves | Tipo de cifrado de datos y aspectos para la gestión de claves. |
| **12** | Gestión de acceso e identidades | Funciones de la gestión de identidades y recomendaciones para una adecuada gestión. |
| **13** | Virtualización | Problemas de la virtualización, recomendaciones para evitar dichos inconvenientes. |

### ❖ Dominio 1: Marco de la Arquitectura de Cloud Computing

El primer dominio consiste en un resumen general de las definiciones, características, modelos de servicio y modelos de despliegue del Cloud Computing, temática que ya fue abordada en este proyecto en el Capítulo 2.

### ❖ Dominio 2: Gobierno y gestión de riesgos de las empresas

La organización y el proveedor de servicio deben contar con un marco de gestión de Seguridad de la Información, que les permita llevar procesos diseñados y desarrollados para la seguridad, que sean repetibles, medibles, sostenibles, defendibles y con mejora continua. La gestión de riesgo necesita identificar e implementar estructuras, procesos y controles organizativos adecuados que permitan realizar acciones sobre el gobierno y la gestión de la Seguridad de la Información en cada organización.

En esta área se tienen las siguientes recomendaciones:

- Examinar en forma detallada las capacidades de seguridad del proveedor así como los parámetros de seguridad de las aplicaciones en uso.
- Realizar auditorías minuciosas y detalladas con el fin de verificar que se estén cumpliendo todos los requisitos.
- Aun cuando el cliente y el proveedor cuenten con SGSIs, dichos sistemas deben trabajar de forma colaborativa y marcar objetivos alineados a la misión del

negocio de la organización y en concordancia con la Seguridad de la Información.

- El cliente debe evaluar los procesos del proveedor de servicio y los suyos propios con respecto a la Seguridad de la Información, para examinar si son los más óptimos y si obtienen el propósito deseado.
- Involucrar al departamento de Seguridad de la empresa cliente en el establecimiento del contrato de Nivel de Servicio (SLA), para garantizar que se estén cumpliendo todos los requisitos de seguridad. El contrato de Nivel de Servicio debe incluir:
    - ✓ Resultados de los planes de tratamiento del riesgo.
    - ✓ Métricas y estándares de la gestión de la Seguridad.
    - ✓ Evaluación y gestión del riesgo del proveedor de servicio de Cloud.
- Establecer métricas de gestión de la seguridad, que sean aplicadas antes y después de una migración a un servicio en la Nube, para evaluar los resultados y medir la efectividad del cambio.
- Elegir al proveedor de servicio en base a la apertura que tenga para compartir información y colabore con el cliente, ya que será mejor si está dispuesto a satisfacer los requisitos en cuanto a la Seguridad de la Información, caso contrario el cliente está en libertad de seleccionar otro proveedor, con el que pueda alinearse con mayor facilidad a sus objetivos de seguridad.
- Un servicio de Cloud Computing, acarrea una relación directa entre el cliente y el proveedor, pero también con terceras partes, aun cuando sea de forma indirecta, esto implica que el análisis de la seguridad se lo debe realizar a la cadena de suministro y no como un ente independiente.
- Para que el cliente tenga cubiertos todos los campos de seguridad debe desarrollar los siguientes procedimientos:
    - ❖ Gestión y evaluación del riesgo enfocado hacia el servicio contratado:
        - ✓ Tasación de activos.
        - ✓ Identificación de amenazas y vulnerabilidades.
        - ✓ Impacto que pueden sufrir los activos.
        - ✓ Análisis de la probabilidad de eventos.
        - ✓ Niveles y criterios de aceptación que se han aceptado en la gestión del riesgo
        - ✓ Planes de tratamiento de riesgo con múltiples opciones.
    - ❖ Aceptación de riesgos residuales derivados del uso de un servicio de Cloud.
    - ❖ Plan de continuidad del negocio y recuperación de catástrofes: Especificación de escenarios, en los cuales se contemple la pérdida del

servicio del proveedor de Cloud, así como de los proveedores de terceras partes del dicho proveedor.

### ❖ Dominio 3: Cuestiones legales y e-Discovery

La aparición del Cloud Computing hace que las organizaciones coloquen mayor interés al tratamiento de los datos, más aún en el caso de la presencia de un tercero como lo es el proveedor de servicios de la Nube.

Dada la importancia del manejo de los datos, el cliente de un servicio de Cloud debe realizar un análisis prolijo y completo de todos los aspectos legales involucrados en el servicio. En el análisis legal se considera tres tipos de dimensiones, en primer lugar dimensiones funcionales en las que se debe distinguir que servicios específicos tienen implicaciones legales, en segundo lugar las dimensiones jurisdiccionales relacionadas con el gobierno y el modo en que se administran las leyes y la normativa para el uso de servicio de Cloud Computing y finalmente dimensiones contractuales en lo referente al contrato en sí, la estructura que éste deba tener para la gestión de disputas legales y de los aspectos de seguridad.

Las implicaciones legales de un servicio de este tipo, son diferentes a las de un servicio con infraestructura tradicional, sobresaliendo características como el anonimato de la identidad de los proveedores de servicio y el anonimato de la localización de los servidores involucrados en el servicio.

En necesario resaltar que el tratamiento de aspectos legales en Cloud Computing es relativamente nuevo y no cuenta con un historial legal, lo cual puede causar inquietudes mientras se llegue a procesos maduros y asertivos. Este punto se profundizará en el Capítulo 5.

Las siguientes recomendaciones están delineadas para el tratamiento de los temas legales:

- Establecer una responsabilidad compartida en relación con el e-Discovery [20, 21] entre el cliente y el proveedor de servicio.
- El proveedor debe garantizar que los datos del cliente van a recibir la misma atención y manejo cauteloso, que si estuvieran en manos del propietario.
- Implantar un proceso metódico para la devolución y la enajenación segura de los activos entregados por parte del cliente.
- Conocer específicamente donde hospedará el proveedor los datos entregados, para estar al tanto del cumplimiento de las leyes locales y de las cláusulas relacionadas con la restricción del flujo de datos fronterizo.
- El cliente debe asegurarse que la información que ha entregado al proveedor de servicio se encuentra en su formato original y es autenticable.

- Implementar cláusulas específicas en el contrato, para establecer el compromiso del proveedor a no violar la confidencialidad de sus datos, ni hacer uso de ellos durante su relación contractual ni al verse finalizada.

### ❖ Dominio 4: Cumplimiento normativo y Auditorías

Cuando una organización decide utilizar servicios en la Nube, puede ser que este cambio implique ajustar los procedimientos, los sistemas y los requisitos normativos con los cuales manejaba la organización, lo cual se podría tornar complicado al querer alinearse a los requisitos normativos del proveedor. Aun cuando la empresa cliente cuente con un sistema de gestión relacionado con la informática es posible que quienes auditan esta norma no estén relacionados con los servicios de Cloud Computing, es por ello que el cliente debe tener en cuenta las siguientes consideraciones:

- ✓ La división de responsabilidades con respecto al cumplimiento de las normas de un sistema entre la organización y el proveedor de servicios de Cloud.
- ✓ La capacidad del proveedor de servicio para apoyar al cumplimiento normativo de la empresa cliente, al exponer evidencias para dicho cumplimiento.
- ✓ Colocarse en la posición de mediador entre el equipo de auditoría de una normativa y el proveedor de Cloud Computing.

A continuación se exponen las recomendaciones dadas respecto al cumplimiento normativo:

- Incluir los representantes del departamento Legal y de Gestión del cliente en el establecimiento del contrato, para asegurarse de que el proveedor cumpla con las obligaciones de normas y estándares.
- Establecer una cláusula en el contrato, para especificar el derecho del cliente a auditar al proveedor, especialmente cuando la organización tiene que cumplir algún requisito normativo sobre el servicio que está corriendo sobre la Nube. La auditoría podría verse sustituida si el proveedor de servicio presenta ante sus clientes alguna certificación relacionada con sistemas de gestión de seguridad, como el caso de la Norma ISO 27000.
- Analizar si la normativa existente en la organización se verá afectada por el uso de un servicio en la Nube, en caso de ser así, se debería plantear un nuevo alcance.
- Evaluar que controles de seguridad de cumplimiento normativo posee el proveedor de servicio.
- Analizar el impacto que presenta una normativa en la infraestructura del proveedor de servicio seleccionado. En este campo se puede dar el caso de

que controles que se han establecido para una infraestructura interna no se puedan aplicar para un servicio en la Nube.

- Examinar el impacto que sufrirán los procedimientos, los requisitos y las políticas de la organización en cuanto a la norma o estándar al cual esté alineada, en el momento de trasladar sus datos y aplicaciones a la Nube. Posterior al cambio es necesario almacenar las evidencias de cómo se están cumpliendo la norma en el nuevo entorno.
- Seleccionar auditores que tengan experiencia con servicios de Cloud Computing, puesto que un auditor o asesor que no esté relacionado con ésta temática desconoce todos los retos que presenta el entorno.
- Solicitar que el proveedor de servicios cuente con una certificación de auditoría como SAS 70 Type II y con la certificación ISO 27001, o a su vez que demuestre su proyecto de certificación.

### ❖ Dominio 5: Gestión del ciclo de vida de la Información

El objetivo principal de la Seguridad de la Información se basa en la protección de datos, que en un escenario de Cloud debe verse mayormente fortalecido. En este campo se deben diferenciar dos aspectos:

- ✓ **Ciclo de Vida de la Información**:
  Crear, almacenar, utilizar, compartir, archivar y destruir.

- ✓ **Ciclo de vida de los datos:**
  - Seguridad de los datos: relacionado con la confidencialidad, integridad, disponibilidad, autenticidad, autorización, autenticación y no repudio de los datos.
  - Geo-localización de los datos: Debe existir garantías de que los datos se almacenen en localizaciones que ha sido permitidas mediante el contrato.
  - Remanencia o persistencia de los datos: La eliminación de datos debe ser de forma absoluta y efectiva.
  - Mezcla de datos con otros clientes: Los datos que sean clasificados como sensibles no deben mezclarse con ningún otro cliente ni en el uso, almacenamiento o tránsito.
  - Planes de backup y recuperación de datos para la restauración: Los datos siempre deben estar disponibles y para esto deben existir procedimientos de backup y recuperación.
  - Descubrimiento de datos: Es un reto que implica aún varias revisiones técnicas y legales, en el que se debe garantizar que los datos sean recuperables en su totalidad.

- Agregación de datos e inferencia: Establecer prácticas que garanticen al cliente la protección de la información confidencial en cuanto a violaciones.

En este dominio se tienen las siguientes recomendaciones:

- Conocer qué tipo de controles se están aplicando durante el ciclo de vida de los datos.
- Estipular en el contrato que el cliente debe conocer la localización geográfica del almacenamiento de los datos.
- Solicitar que se informe con anterioridad si se da algún caso de embargo de datos, debido a problemas del proveedor del servicio con un tercero o con una entidad gubernamental.
- Determinar que usuarios y con qué tipo de privilegios tendrán acceso a sus datos tanto en la organización como en el proveedor de servicio.
- El proveedor de servicios de Cloud, debe establecer como política fundamental la "Denegación por defecto"[22].
- Cifrar los datos que se encuentren en la Nube, tanto en procesos estáticos como en procesos de tránsito.
- Implantar penalizaciones hacia el proveedor de servicio en el caso de que se registren procesos de violación de los datos.
- Ejecutar constantemente pruebas para medir los procesos de backup y recuperación de datos.

### ❖ Dominio 6: Portabilidad e interoperabilidad

El cambio de proveedor puede representar para el cliente un proceso engorroso, por lo que debe realizar un análisis exhaustivo si el potencial proveedor le brinda todas las facilidades para la portabilidad y la interoperabilidad. Estos dos aspectos deben ser incluidos en la gestión de riesgos que presenta el proveedor a sus clientes.

Razones como un incremento en los costos del servicio, un cese de actividad o un descenso inaceptable de la calidad del servicio ofrecido, puede hacer que un cliente desee cambiar de proveedor de servicio.

Ya que en el mercado no existen estándares establecidos de interoperabilidad, el proceso de migración de proveedor puede resultar traumático, con pérdidas de tiempo, esfuerzo y dinero, por lo cual se deben seguir las siguientes recomendaciones:

- Establecer en el contrato, específicamente en el programa de la Continuidad de Negocio cual será el proceso a seguir en el caso de una migración.

- Tomar en cuenta el tamaño de los datos, pues este parámetro puede ser decisivo al momento de una migración y el tiempo que tardará en restablecerse el servicio en un nuevo proveedor.
- Documentar toda la arquitectura, configuraciones y controles de seguridad, que en lo posterior facilitará la migración a un nuevo proveedor.
- En el caso específico de servicios IaaS, tener conocimiento de cómo capturar y portar las imágenes de una máquina virtual hacia un nuevo proveedor.
- Identificar las dependencias de hardware antes de realizar una migración.
- Solicitar al antiguo proveedor se facilite todos los registros del sistema del cliente que está funcionando en la Nube.
- Consultar con su primer proveedor de servicios de Cloud, la posibilidad que se pueda restablecer el servicio, en el caso de que el nuevo proveedor no cumpla con todos los servicios ofertados.
- Determinar si las APIs usadas en el proveedor antiguo pueden ser compatibles con el nuevo proveedor, por esta razón es mejor que se utilicen estándares y APIs abiertas.
- Realizar copias de seguridad continuamente.
- Tomar en cuenta que cualquier herramienta desarrollada en forma personalizada para el cliente, deberá ser desarrollada nuevamente.
- Trasladar las copias de seguridad y todos los registros hacia el nuevo proveedor para tenerlos como evidencia en caso de auditorías o requerimientos legales.
- Solicitar al nuevo proveedor un test de las aplicaciones antes de realizar una migración.

### ❖ Dominio 7: Seguridad tradicional, continuidad del negocio y recuperación de catástrofes

Los tres aspectos que se detallan en este dominio tienen especial importancia en un entorno de Cloud, si en infraestructuras internas eran vitales, hoy en día se deben mantener los principios tradicionales y darle mayor énfasis a los cambios que se vayan a realizar y su inmediata actualización.

Se recomienda lo siguiente:

- Solicitar al proveedor que restrinja el acceso hacia sus datos a la menor cantidad de colaboradores internos, disminuyendo así el mal uso de la información confidencial.
- Adoptar prácticas de seguridad estrictas que a largo plazo puedan disminuir el riesgo.
- Inspeccionar las instalaciones del proveedor de servicio.

- Revisar detenidamente los planes de recuperación de catástrofes y de continuidad del negocio del proveedor.
- Identificar las inter-dependencias físicas de la infraestructura del proveedor.
- Exigir al proveedor la documentación pertinente acerca de los controles de seguridad implementados y su relación con los estándares del sector.
- Verificar que el proveedor de servicios de Cloud cuente con un Plan de continuidad de negocio vigente, que esté aprobado, testeado y certificado por los estándares reconocidos en la rama y que se encuentren en un lugar para que sean libremente consultados.

### ❖ Dominio 8: Operaciones del centro de datos

El centro de datos es el elemento más importante para un proveedor de servicios de Cloud Computing, el cual evolucionado con el tiempo para que actualmente se lo conozca como un centro de datos de nueva generación, donde se maneja la última tecnología en materia de almacenamiento, procesamiento y seguridad de datos.

Un centro de datos debe estar operado bajo estándares como ITSM[26] o ITIL[27] para entregar a sus clientes servicios con calidad y empleando las mejores prácticas. El centro de datos debe implementar lo siguiente:

- ✓ Establecimiento de políticas y procedimientos para garantizar un ambiente seguro.
- ✓ Restricción de acceso a los activos de información.
- ✓ Implementación de sistemas de seguridad física perimetral para salvaguardar la información sensible.

Debido a la característica de Cloud Computing de brindar servicios a la carta, el proveedor debe asegurarse que el centro de datos tenga los recursos necesarios para poder suministrar al cliente las capacidades ofertadas.

Las recomendaciones en este dominio son las siguientes:

- La organización debe asegurarse que el centro de datos cuenta con procesos de manejo, buenas prácticas de gestión y software adecuado para la administración. A la vez el cliente puede utilizar medidas para asegurarse de la agilidad y la alta disponibilidad de recursos dentro del mismo.
- El proveedor de Cloud puede apoyarse en varias fuentes de información acerca de cómo realizar la construcción o remodelación de un centro de datos para servicios de Cloud. Dentro de dicha documentación se puede

[26] ITSM: Information Technology Service Management, http://www.itsm.info/ITSM.htm.
[27] ITIL: Information Technology Infrastructure Library, http://www.itil-officialsite.com.

encontrar una matriz de la CSA denominada CSA Cloud Controls Matrix [28] que ayuda en la verificación de la calidad de los servicios que se están entregando.

- Utilizar técnicas de manejo de servicios de IT para asegurar la disponibilidad, la seguridad en la entrega y la gestión de los activos de información.
- Realizar auditorías en el centro de datos, en base a los estándares de seguridad y normativas existentes en el sector, y publicar los resultados para que sean observados por los clientes.

### ❖ Dominio 9: Respuesta ante incidencias, notificación y subsanación

La respuesta a incidencias es determinante en la gestión de servicios de Cloud, donde deberá visualizarse un cambio sustancial del manejo de incidencias en una plataforma estándar con el que ahora debe darse en Cloud Computing, debido al modelo compartido entre el cliente y proveedor de servicios.

Para evitar inconvenientes en la solución de incidencias de seguridad, es necesario definir la responsabilidad de cada una de las partes, para que no se vea comprometido el proceso de gestión, en el caso de que no se tengan definidas todas las directrices.

El proveedor debe tomar en cuenta que todos sus procesos deben contar con un refuerzo de seguridad y que cualquier descuido por más simple que pueda parecer representa un riesgo potencial para la integridad de los datos alojados en sus plataformas.

Una incidencia tiene un ciclo de vida: detección, análisis y diagnóstico, corrección, resolución, retroalimentación y cierre. A cada una de estas fases, el proveedor debe darle el respectivo tratamiento.

La gestión de incidencias amerita un conocimiento técnico por parte de quienes están en el proceso de administración y solución, para ello se ha propuesto la creación de un grupo llamado SOC [23], correspondiente al Centro de Operaciones de Seguridad quienes se encargan de controlar las alertas y/o alarmas, los accesos no autorizados, la detección de intrusos, etc., para realizar la gestión sobre cada incidencia y posteriormente un análisis de indicadores de todas las incidencias suscitadas.

Las recomendaciones para este dominio son:

- Implementar una vía de comunicación apropiada entre el cliente y el proveedor, que se utilice al presentarse un evento/incidente. Para este

[28] CSA Cloud Controls Matrix: CCM, https://cloudsecurityalliance.org/research/ccm.

proceso se pueden usar estándares diseñados para facilitar la comunicación de incidentes.

- El proveedor de servicio debe permitir al cliente el acceso a la plataforma para realizar análisis forenses o recuperación de incidentes.
- Identificar los tipos de incidencias y cuáles son las más relevantes, para posteriormente diseñar estrategias para la erradicación, soporte y recuperación de incidentes.
- Revisar el historial de incidencias del proveedor.
- Apoyarse en el contrato como garantía para el soporte en incidencias por parte del proveedor.

### ❖ Dominio 10: Seguridad de las Aplicaciones

La seguridad de las aplicaciones está presente en cada uno de los modelos, sean para aplicaciones SaaS, así como PaaS o IaaS. En un entorno de Cloud Computing, la seguridad de las aplicaciones es un punto sumamente sensible, mucho más que en el ambiente tradicional, para ello se debe considerar cada una de las etapas de la vida útil de una aplicación para para así poder mitigar los riesgos que se pudieran presentar.

El ciclo de vida de desarrollo de software está formado por las etapas de: diseño, desarrollo, garantía de calidad, documentación, despliegue, gestión, mantenimiento y desmantelamiento.

Algunas de las amenazas que se pueden presentar son:

- ✓ Spoofing: Asumir la identidad de otro usuario.
- ✓ Manipulación: Modificar los datos en tránsito.
- ✓ Repudiación: Denegar el origen de la transacción.
- ✓ Revelación de Información: Revelación desautorizada de los datos.
- ✓ Denegación de Servicio: Afectación de la disponibilidad.
- ✓ Cambio de privilegios: Asumir otro rol o derecho.

Las recomendaciones para este dominio son:

- Definir requisitos funcionales y de regulación para la seguridad y la privacidad de las aplicaciones.
- Realizar un análisis del riesgo de las aplicaciones en cuanto a la seguridad y a la privacidad.
- Utilizar arquitecturas que mitiguen las amenazas, por ejemplo "Open Security Architecture"[29].

[29] OSA: http://www.opensecurityarchitecture.org/cms/index.php.

- Categorizar las vulnerabilidades de acuerdo al impacto crítico que posean y definir un proceso de remediación.
- Contar con máquinas virtuales que tengan imágenes fiables.
- Resguardar las claves secretas de cada una de las aplicaciones.
- Definir qué tipo de cifrado se utilizará.
- Precautelar los archivos utilizados para la depuración de aplicaciones.
- Tomar en cuenta que al utilizar administración externa y multiposesión, esto se puede convertir en una amenaza para la aplicación.
- Establecer métricas para medir la efectividad de la seguridad de las aplicaciones.
- Analizar qué acciones pueden tomar los intrusos malintencionados en este nuevo tipo de aplicaciones, en el caso de un hacker este podría atacar el código visible.
- Establecer en el contrato con el proveedor una cláusula que permita al cliente realizar evaluaciones de vulnerabilidad remota y de aplicaciones.

### ❖ Dominio 11: Cifrado y gestión de claves

El cifrado de datos es una acción fundamental para evitar el robo de la información. Es necesario realizar un adecuado manejo de los datos antes de moverlos hacia la Nube.

Un proveedor debe contar con mecanismos para cifrado de datos y gestión de claves. El cifrado le proporcionará protección a los recursos de sus clientes y la gestión de claves fortalecerá el acceso a dichos recursos.

El cifrado de datos se puede dar en tres instancias:

- ✓ Cifrado de datos en tránsito por las redes: Se debe proteger los datos en tránsito, aun cuando sea en la misma red interna del proveedor de servicio.
- ✓ Cifrado de datos estáticos: Se puede cifrar los datos que están almacenados o que pertenecen a una base datos, para así protegerlos de un proveedor o coposeedor mal intencionado. El cliente puede enviar su información cifrada y almacenarla de este modo, al momento que la recibe de vuelta realiza el proceso de descifrado en sus propias instalaciones.
- ✓ Cifrado de datos en soporte de backup: Se debe proteger los datos de backup contra el mal uso, pérdida o robo. Normalmente el proveedor asegura que está ejecutando dicha acción.

Con respecto a la gestión de claves, se tienen los siguientes aspectos:

- ✓ Almacenamiento seguro de claves: El almacenamiento de claves debe ser seguro y estar protegido, caso contrario se colocaría al descubierto todos los datos que ya están cifrados.
- ✓ Acceso al almacenamiento de claves: Este acceso debe ser estrictamente limitado a quienes necesiten las claves en cuestión.
- ✓ Backup y recuperación de claves: Se debe implementar mecanismos de recuperación segura de claves y de backup, ya que la pérdida de claves puede llevar a la pérdida total de los datos.

Como alternativa se puede utilizar el protocolo KMIP[30], diseñado para la comunicación entre sistemas empresariales de gestión de claves y sistemas de cifrado. También existe la posibilidad de aplicar el estándar IEEE 1619.3 (Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data)[24].

Las siguientes son recomendaciones a aplicarse para este dominio:

- Utilizar las mejores prácticas de gestión de claves cuando se use cifrado o descifrado.
- Establecer en el contrato, una cláusula sobre el uso del cifrado en los servicios, mediante estándares existentes en el sector.
- Solicitar información al proveedor de cómo está gestionando el ciclo de vida de las claves.
- Identificar si cada cliente tiene sus propias claves o si se está utilizando las mismas con todos los clientes del proveedor.
- Asegurarse de que los datos clasificados como sensibles estén utilizando cifrado en cada etapa (tránsito, estático y backup).
- Exigir al proveedor que se realice cifrado para todos los archivos y backups.

### ❖ Dominio 12: Gestión de acceso e identidades

Un servicio de Cloud Computing debe contar con un buen mecanismo de gestión de la identidad y control de acceso, que garantice su éxito en la Nube. Estos dos procesos son puntos susceptibles que necesitan especial atención para utilizar las tecnologías adecuadas para mitigar los riesgos de ataque.

Las principales funciones de la gestión de identidades y control de acceso son:

- ✓ Abastecimiento de identidades: Alta y baja de usuarios.
- ✓ Autenticación: Autenticar usuarios de forma fiable y gestionable.

[30] KMIP: Key Management Interoperability Protocol, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip#overview.

- ✓ Federación: Gestión de identidad federada utilizando un proveedor de identidad (IdP[31]).
- ✓ Gestión de perfiles de usuario y autorizaciones: Establecer perfiles de usuario con información fiable y con sus respectivas políticas de acceso.
- ✓ Soporte para el cumplimiento normativo.

En estas áreas se tienen varias recomendaciones, las más importantes son:

- Para el alta y baja de usuarios utilizar soluciones estándar y no propietarias del proveedor, ya que puede dificultar las operaciones.
- Utilizar esquemas SPML[32].
- El cliente debe considerar la opción de utilizar un Proveedor de Identidades para realizar la autenticación.
- Utilizar una conexión VPN a la par de un sistema de identidad como una solución SSO[33] o autenticación basada en LDAP.
- Utilizar OpenID [25], tomando en cuenta que los usuarios deben tener privilegios limitados.
- El proveedor puede implementar autenticación local basada en autenticación abierta OAUTH[26].
- La autenticación puede ser trasladada al cliente a través del uso de sistemas con Lenguaje SAML[34].
- Para el caso del proveedor, es una buena alternativa que utilice sistemas de autenticación robustos, como el uso de contraseñas de un solo uso, usuarios biométricos, certificados digitales, etc.
- Confirmar que el proveedor cuenta por lo menos con los estándares principales para la federación como son SAML y Web Services-Federation.
- El proveedor debe aceptar cualquier formato de federación estándar proveniente de un Proveedor de Identidad.
- Para el control de acceso, establecer modelos dependiendo del tipo de servicio.
- Establecer políticas de privacidad y evaluar su cumplimiento.

### ❖ Dominio 13: Virtualización

La virtualización es un componente fundamental del Cloud Computing, al ser la herramienta que permite a los proveedores ofrecer los recursos tan rápido como lo desee el cliente, sin que esto demande la compra del equipamiento sino únicamente de

[31] IdP: Identity Provider.
[32] SPML: Service Provisioning Markup Language, https://www.oasis-open.org/committees/download.php/4137.
[33] SSO: Single Sign-On.
[34] SAML: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

la capacidad [27]. Otra de las ventajas de usar virtualización es el poder compartir la infraestructura física y brindar servicios independientes a sus clientes, garantizando principalmente que están aislados de forma segura.

Aun cuando esta técnica aporta beneficios técnicos y económicos, también puede incrementar los problemas de seguridad, se puede decir que los inconvenientes que ya los tenía anteriormente ahora son migrados hacia la Nube, por ello necesita atención especial a las vulnerabilidades que introduce. Los problemas más sobresalientes son:

- ✓ El rápido despliegue de una máquina virtual puede introducir errores si el proveedor no tiene procedimientos adecuados para la planificación y ejecución del proceso.
- ✓ Complejidad en el uso del software de gestión, cuando se tenga en el mismo entorno para servidores y dispositivos de red.
- ✓ Debido a la encapsulación de máquinas virtuales, se puede extraer fácilmente los datos de una máquina en específico, pues sólo representa copiar un conjunto de ficheros.
- ✓ Si el servidor físico donde se están alojando las máquinas virtuales presenta problemas de configuración, su afectación va directamente a todas las máquinas virtuales, ocasionando problemas en varios clientes.
- ✓ La clonación de las máquinas virtuales en base a una plantilla puede duplicar opciones como el usuario de administración, dando a un atacante esta debilidad para acceder a la máquina virtual de otro cliente.

Se plantean las siguientes recomendaciones:

- Solicitar al proveedor la información sobre el tipo de virtualización que está utilizando y los controles de seguridad que tiene cada máquina virtual.
- Validar cualquier plantilla de máquina virtual que sea originaria del proveedor de servicio antes de ponerla en uso.
- Requerir al proveedor el acceso y control de administración del sistema operativo virtualizado.
- Incluir en la máquina virtual autenticación fuerte y la misma gestión de identidad que se maneje internamente en la empresa.
- El proveedor puede realizar una clasificación de máquinas virtuales de acuerdo al tipo de función que ejecuten y así colocarlas en zonas de seguridad de acuerdo a su importancia.
- Pedir al proveedor que se tenga un procedimiento de generación de informes que confirmen el aislamiento entre máquinas virtuales y que generen alertas cuando se de alguna violación del mismo.

## 4.2 Análisis en base a la ENISA

A través de la investigación de la ENISA se da a conocer un conjunto de buenas prácticas y consideraciones a tomarse en cuenta en el manejo de la información específicamente para servicios en la Nube; con este propósito el documento "Beneficios, riesgos y recomendaciones para la Seguridad de la Información"[28], aporta con temas como la evaluación del riesgo, y principalmente las recomendaciones enfocadas hacia la Seguridad de la Información debido a la que tiene importancia en Cloud Computing por la concentración masiva los datos, que resulta muy atractivo para los atacantes.

De acuerdo a la ENISA el modelo de Cloud está causando fuertes impactos en aspectos como: la administración de los recursos al necesitar una rigurosa gestión tanto en la parte física como lógica; en la arquitectura de las redes ya que el cliente va a esperar un servicio de calidad que a la vez viene ligado con su proveedor de comunicaciones; y en la economía de las empresas y del proveedor, que deben manejar una economía a escala, que crecerá en base a la necesidad de los recursos.

A continuación se revisan las ventajas, los riesgos y las vulnerabilidades de la Seguridad de la Información cuando se hace uso de la Nube, posteriormente se examina cómo realizar el análisis del riesgo y finalmente una revisión de cuáles deben ser los requisitos que un proveedor de servicio de Cloud Computing debe cumplir para garantizar que proporciona un tratamiento adecuado a la Seguridad.

### 4.2.1 Ventajas para la Seguridad de la Información en un entorno de Cloud Computing

- ***La Seguridad como elemento diferenciador del Mercado:*** La mayoría de clientes o potenciales clientes, tienen puesta su primera preocupación en la Seguridad, y están basando la selección en el renombre de los ofertantes, y en el nivel de confidencialidad, integridad, resistencia a fallos y soluciones que el proveedor ofrezca en pro de la Seguridad de la Información.
- ***Interfaces normalizadas para servicios de Seguridad gestionados:*** El proveedor puede utilizar interfaces abiertas y estandarizadas, que faciliten la gestión de servicios adicionales como seguridad gestionada por otro proveedor.
- ***Escalada rápida e inteligente de recursos:*** Un proveedor tiene ventajas en cuanto a la gestión de recursos, del tráfico, de la autenticación, y todos los temas relacionados puesto que cuenta con las herramientas y la infraestructura para enfrentar problemas y solucionarlos rápidamente, lo que no sucede en un ambiente normal que necesitaría adquisición de los equipos.

- ***Auditoría y recogida de pruebas:*** Acceder a un clon de la máquina virtual para realizar un análisis forense minucioso de los datos, sin tener que desconectar la infraestructura.
- ***Actualizaciones y opciones por defecto puntuales, efectivas y eficaces:*** Actualizar y reforzar con rapidez los últimos parches y configuraciones de seguridad en las máquinas virtuales de los clientes gracias a la plataforma homogénea con la que se cuenta, que no sucede en un sistema tradicional.
- ***Beneficios de la concentración de recursos:*** Abarata los costos del control de acceso físico y la perimetrización usada para proteger los centros de datos.

### 4.2.2 Principales Riesgos en términos de Seguridad

Los riesgos más significativos en la Seguridad en la Nube son:

1. ***Pérdida de Gobernanza:*** Un usuario de Cloud pierde el control de sus datos, dando paso a que sea el proveedor quien vele por la seguridad de los mismos.
2. ***Vinculación:*** La migración desde un proveedor hacia otro puede ser totalmente compleja sino se usan procedimientos estandarizados.
3. ***Fallo de aislamiento:*** Los mecanismos utilizados para separar recursos como el almacenamiento, memoria o enrutamiento pueden fallar.
4. ***Riesgos de cumplimiento normativo:*** La migración a un servicio en la Nube puede modificar los procesos de una empresa, impidiendo que cumpla los requisitos de alguna normativa, que anteriormente estaba cubierta o en proceso de certificación.
5. ***Comprometimiento de la interfaz de gestión:*** La interfaces de gestión pueden verse comprometidas al ser el punto de conexión hacia los recursos. Se tienen mayores vulnerabilidades cuando se usa la Internet como la red de conexión, o en el uso de acceso remoto, o en las debilidades propias del navegador.
6. ***Protección de datos:*** Puede resultar complicado para el cliente, comprobar si su proveedor está utilizando técnicas correctas en la gestión de los datos y que estén en conformidad con la ley. Por esta razón algunos proveedores ponen en evidencia su capacidad para gestionarlos informando sobre sus buenas prácticas, los controles que poseen o a su vez mostrando las certificaciones en el ámbito de la Seguridad como puede ser la Certificación SAS 70 o ISO 27001.
7. ***Supresión de datos insegura o incompleta***: La eliminación de datos podría resultar imposible en un ambiente de Cloud, la cual puede darse por errores en los procesos de eliminación de datos tal como se presenta en los sistemas operativos normales o por copias de la información indebidamente clasificadas.
8. ***Miembro malicioso:*** Tanto en la empresa del cliente como en el proveedor pueden existir posiciones que tengan perfiles de alto riesgo, como por ejemplo el

administrador del sistema del proveedor de Cloud Computing o el administrador de la seguridad gestionada.

### 4.2.3 Vulnerabilidades de Seguridad

El Cloud Computing da lugar al incremento de explotar las vulnerabilidades, que vienen en mayor grado por el tipo de tecnologías que forman el núcleo de la infraestructura.

En primer lugar, es necesario distinguir la diferencia entre vulnerabilidad, riesgo y amenaza.

***Vulnerabilidad***: Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza[29].

***Amenaza:*** Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización [29].

***Riesgo:*** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. [29].

Las vulnerabilidades que ocasionan mayor daño en una plataforma de Cloud son las relacionadas a la virtualización, al cifrado y gestión claves y a la gestión de acceso, pero también se debe recordar que las vulnerabilidades ya existentes en una plataforma convencional también podrían lograr el mismo efecto, es por eso que necesitan su respectivo análisis y gestión. En base a lo mencionado la ENISA presenta un listado a detalle de las vulnerabilidades de Seguridad que engloban tanto las específicas para entornos de Cloud Computing como las generales, reiterando que a pesar de ser conocidas también necesitan dárseles tratamiento.

#### A. Vulnerabilidades de Seguridad Específicas a la Nube

a) Vulnerabilidades de AAA[35]: Sistemas pobres de Autenticación, Autorización y Auditoría que faciliten el acceso no autorizado a los recursos.
b) Procesos no controlados para el alta y baja de usuarios.
c) Acceso remoto a la interfaz de gestión comprometiendo la infraestructura en la Nube.
d) Vulnerabilidades del hipervisor, equivalente a que todos los equipos virtuales también tenga la misma vulnerabilidad.
e) Ausencia de aislamiento de los recursos de un cliente con los del resto.
f) Vulnerabilidades en la codificación de la comunicación, autenticación pobre.
g) Falta o debilidad en la codificación de archivos y datos en el tránsito.
h) Imposibilidad de procesar datos codificados.

[35] AAA: Authentication, Authorization and Accounting.

i) Procedimientos insuficientes de gestión de claves.
j) Generación de claves: Baja entropía para la generación de números aleatorios.
k) Falta de tecnologías y soluciones estándar.
l) Ausencia de un acuerdo, en el caso de quiebre de un proveedor de PaaS o de SaaS.
m) Modelado inadecuado del uso de recursos, que pudiera concluir en un agotamiento de recursos, debido a un fallo en los algoritmos de provisión de recursos.
n) Posibilidad de que se realice un análisis interno de red como un escaneo de puertos de la red, en otros clientes dentro de la Nube.
o) Posibilidad de que se realicen comprobaciones de corresidencia, que den a conocer fallos en el aislamiento y el chequeo de que recursos están compartidos por otros clientes.
p) Eliminación fallida o limpieza completa de los medios sensibles.
q) Falta de conocimiento acerca de las responsabilidades o las obligaciones contractuales del cliente al contratar servicios en la Nube.
r) Cláusulas en el contrato, que presenten un riesgo para el negocio, pues podrían entregar al proveedor demasiados derechos sobre el material almacenado.
s) Auditoría o certificación no disponible para los clientes.
t) Sistemas de Certificación no adaptados a las infraestructuras de Nube.
u) Provisión de recursos e inversiones en infraestructura inadecuadas.
v) Ausencia de políticas de limitación de recursos.
w) Almacenamiento de datos en jurisdicciones múltiples y falta de transparencia sobre este punto.
x) Falta de información sobre jurisdicciones, los datos podrían almacenarse en lugares de alto riesgo y puedan ser confiscados.
y) Falta de integridad y transparencia en los términos de uso.

### B. Vulnerabilidades de Seguridad no específicas a la Nube

a) Ausencia de conciencia de la Seguridad, tanto clientes como proveedores deben estar conscientes de los riesgos a los que se puede enfrentar la información.
b) Falta de procesos de investigación sobre el perfil de riesgo del personal que tiene funciones con cierto grado de privilegios.
c) Distribución confusa de funciones y responsabilidades, ya sea en el proveedor o en el cliente.
d) Separación inadecuada de las funciones en el proveedor, dando como resultado que hayan roles con privilegios muy altos.

e) La no aplicación del principio de "Need to Know"[36]. No dar accesos innecesarios a las partes.
f) Procedimientos de Seguridad física inadecuados.
g) Vulnerabilidades del sistema o de los sistemas operativos.
h) Uso de software poco confiable.
i) Ausencia o deficiencia de un Plan de Continuidad del Negocio y de recuperación de desastres. El plan debería estar puesto a prueba.
j) Inventario de activos incompleto, inadecuado o ausente.
k) Identificación insuficiente de los requisitos de seguridad y de cumplimiento legal.
l) Análisis insuficiente en la selección del proveedor.
m) Ausencia de redundancias
n) Gestión de parches insuficiente.
o) Vulnerabilidades en el consumo de recursos.
p) Incumplimiento del acuerdo de no divulgación por parte del proveedor.
q) Falta de políticas o procedimientos insuficientes para la recopilación y retención de registros.
r) Recursos de filtrado inadecuados o mal configurados.

### 4.2.4 Evaluación del Riesgo

La evaluación del riesgo se lo define como el proceso de comparar el riesgo estimado contra un criterio de riesgo dado, para así establecer la importancia del riesgo.

El proceso para evaluarlo se lo ha realizado a partir de una estimación del nivel de Riesgo, en función de la probabilidad de un escenario de incidentes y el impacto negativo estimado, como lo indica la Tabla 3.

El riesgo resultante se mide en una escala de 0 a 8, con la siguiente clasificación:

- Riesgo Bajo: 0 – 2
- Riesgo Medio: 3 – 5
- Riesgo Alto: 6 – 8

La estimación de los niveles de riesgo se lo ha realizado en base a lo planteado por la Norma ISO 27005:2008 [30].

[36] Need to know: Principio del mínimo conocimiento.

| | | Probabilidad del escenario de Incidentes | | | | |
|---|---|---|---|---|---|---|
| | | **Muy Baja** | **Leve** | **Media** | **Alta** | **Muy alta** |
| **Impacto** | **Muy bajo** | 0 | 1 | 2 | 3 | 4 |
| | **Leve** | 1 | 2 | 3 | 4 | 5 |
| | **Medio** | 2 | 3 | 4 | 5 | 6 |
| | **Alto** | 3 | 4 | 5 | 6 | 7 |
| | **Muy alto** | 4 | 5 | 6 | 7 | 8 |

**Tabla 3. Estimación de los niveles de Riesgo según Norma ISO 27005:2008**

La Evaluación del Riesgo realizada por la ENISA utiliza el escenario de una PYME dado que la mayoría de la industria europea se constituye de este tipo de compañías.

Para cada uno de los riesgos se analizaron los siguientes parámetros:

- Nivel de Probabilidad
- Grado de Impacto
- Vulnerabilidades
- Activos afectados
- Nivel de Riesgo

En la Tabla 4 se muestra un resumen de los riesgos encontrados en el escenario PYME, clasificados en tres grupos:

- Riesgos políticos y organizativos
- Riesgos técnicos
- Riesgos legales
- Riesgos no específicos a la Nube

| EVALUACION DEL RIESGO EN LA NUBE | | | | |
|---|---|---|---|---|
| **CATEGORIA** | **DETALLE** | **PROBABILIDAD** | **IMPACTO** | **RIESGO** |
| **Políticos y Organizativos** | Vinculación | Alta | Medio | **Alto** |
| | Pérdida de Gobernanza | Muy Alta | Muy alto | **Alto** |
| | Desafíos de Cumplimiento | Muy Alta | Alto | **Alto** |
| | Pérdida del renombre empresarial a raíz de actividades de prestación conjunta. | Baja | Alto | Medio |
| | Error o cancelación del servicio en Nube | N/A | Muy alto | Medio |
| | Adquisición del proveedor en Nube | N/A | Medio | Medio |
| | Fallo en la cadena de suministro | Baja | Medio | Leve |
| **Técnicos** | Agotamiento de recursos | Media / Leve | Medio / Alto | Medio |
| | Fallo de aislamiento | Leve (Nube privada) / Media (Nube pública) | Muy alto | **Alto** |
| | Miembros maliciosos de proveedores en Nube. Abuso de funciones privilegiadas | Media | Muy alto | **Alto** |
| | Compromiso de interfaz de gestión. (Manipulación, disponibilidad de la Infraestructura) | Media | Muy alto | Medio |
| | Interceptación de datos en tránsito | Media | Alto | Medio |
| | Fuga de datos durante la carga/descarga dentro de la Nube | Media | Alto | Medio |
| | Supresión de datos insegura o ineficaz | Media | Muy alto | Medio |
| | Distribución de denegación de servicio (DDoS) | Media/Leve | Muy alto | Medio |
| | Denegación económica de servicio (EDoS) | Baja | Alto | Medio |
| | Pérdida de las claves de codificación | Baja | Alto | Medio |
| | Realización de escaneados o detecciones maliciosas | Media | Medio | Medio |
| | Motor de servicio de compromiso | Baja | Muy alto | Medio |
| | Conflictos entre los procedimientos de refuerzo del cliente y el entorno de la Nube | Baja | Medio | Bajo |

| | | | | |
|---|---|---|---|---|
| **Legales** | Órdenes judiciales y descubrimiento electrónico | Alta | Medio | **Alto** |
| | Riesgo derivado del cambio de jurisdicción | Muy Alta | Alto | **Alto** |
| | Riesgo de la protección de datos | Alta | Alto | **Alto** |
| | Riesgos relativos a la licencia | Media | Medio | Medio |
| **No específicos de la Nube** | Brechas en la red | Baja | Muy alto | Medio |
| | Gestión de la red (Congestión de la red, fallo en la conexión, uso no óptimo) | Media | Muy alto | Alto |
| | Modificación del tráfico de la red | Baja | Alto | Medio |
| | Escalada de privilegios | Baja | Alto | Medio |
| | Ataques de Ingeniería Social (Suplantación) | Media | Alto | Medio |
| | Pérdida o compromiso de los registros operativos | Baja | Medio | Bajo |
| | Pérdida o compromiso de los registros de seguridad (Manipulación de la Investigación experta) | Baja | Medio | Bajo |
| | Pérdida o robo de las copias de Seguridad | Baja | Alto | Medio |
| | Acceso no autorizado a los locales (incluido el acceso físico a las máquinas y otras instalaciones) | Muy baja | Alto | Bajo |
| | Robo de equipos informáticos | Muy baja | Alto | Bajo |
| | Catástrofes naturales | Muy baja | Alto | Bajo |

**Tabla 4. Análisis y Evaluación del Riesgo en la Nube**

Para visualizar de mejor forma como se ha adoptado la categoría de bajo, medio o alto riesgo, en el listado, se propone el siguiente ejemplo:

Para el riesgo: "*Fallo de Aislamiento*", con una probabilidad "Media" y un impacto "Muy Alto", el resultante en un riesgo "Alto", como lo indica la Tabla 5.

| DETALLE | PROBABILIDAD | IMPACTO | RIESGO |
|---|---|---|---|
| Fallo de aislamiento | Media (Nube pública) | Muy alto | Alto |

| | | Probabilidad del escenario de Incidentes | | | | |
|---|---|---|---|---|---|---|
| *Fallo de Aislamiento* | | Muy Baja | Leve | Media | Alta | Muy alta |
| **Impacto** | **Muy bajo** | 0 | 1 | 2 | 3 | 4 |
| | **Leve** | 1 | 2 | 3 | 4 | 5 |
| | **Medio** | 2 | 3 | 4 | 5 | 6 |
| | **Alto** | 3 | 4 | 5 | 6 | 7 |
| | **Muy alto** | 4 | 5 | 6 | 7 | 8 |

Tabla 5. Evaluación del Riesgo: Fallo de Aislamiento

### 4.2.5 Requisitos de la Seguridad de la Información en un Proveedor de Cloud Computing.

Cuando un cliente va a contratar servicios en la Nube, su máxima preocupación se enfoca en la Seguridad de la Información al tener que colocarla en las manos del proveedor, por ello la ENISA ha planteado ciertos requisitos que debería cumplir los proveedores para que los servicios de Cloud Computing tengan garantizados los aspectos de Seguridad.

- ***Seguridad del Personal:*** Saber qué tipo de profesionales estarán relacionados con los datos de los clientes, por ejemplo que políticas y procedimientos se maneja para la contratación del personal, confirmación de la identidad, historial delictivo, etc.; que capacitación en cuanto a los temas de seguridad recibe un empleado, o también si los empleados tienen un proceso de evaluación continua para medir su desempeño.
- ***Aseguración de la Cadena de Suministro:*** Se relaciona a los procesos claves para la seguridad que vayan a ser contratados por parte del proveedor de servicio a un tercero, por ejemplo un proveedor de gestión de identidad. El proveedor de la Nube debe analizar qué tan confiable es a la vez su contratista, aplicándole contratos de Nivel de Servicio para garantizar los servicios que le presta, y

finalmente confirmar si sigue estándares para la Seguridad de la Información y aplica controles y políticas de Seguridad internamente.

- ***Seguridad Operativa:*** Mediante un contrato, se espera que el cliente coloque todos los puntos necesarios para contar con un servicio a su conformidad, aun así es posible que fuera de ello sea necesario realizar consultas acerca de cómo el proveedor trata la seguridad a nivel de software, la gestión de parches, el control de la arquitectura de red, el control de la arquitectura de alojamiento, el suministro de recursos, entre otros.
- ***Gestión de Accesos e Identidad:*** Verificar los procedimientos relacionados a la gestión de acceso y la identidad, y que controles se usan en la autorización, autenticación, el suministro de identidades, la gestión de datos personales, la gestión de claves, codificación, robo de credenciales, etc.
- ***Gestión de Activos:*** El proveedor debe mostrar que mantiene una lista actualizada de activos tanto de hardware como de software y de las aplicaciones que se encuentran en su control, con la respectiva clasificación de acuerdo a la sensibilidad y criticidad de cada uno de ellos. Para llevar una mejor actualización el proveedor debería utilizar un mecanismo automático para el inventario.
- ***Datos y Portabilidad de Servicios:*** El proveedor deberá mostrar procedimientos documentados para la exportación de datos desde la Nube y exponer si los formatos de exportación son universales, interoperables y que funcionarán sin ningún inconveniente en otro proveedor. Se deberá realizar el mismo proceso para el tema de aplicaciones.
- ***Gestión de la Continuidad del Negocio:*** Es mejor si el proveedor demuestra que tiene procedimientos para la recuperación de sus operaciones y garantiza la continuidad del negocio. La gestión y respuesta a incidentes es parte fundamental de la continuidad del negocio, ya que de este modo se puede prever cualquier impacto que cause un evento inesperado y dar soluciones que permitan mantener un nivel aceptable de las operaciones.
- ***Seguridad Física:*** El proveedor debe demostrar al cliente en que forma está respaldada la seguridad física de sus instalaciones, en temas como: el acceso físico, los riesgos de edificios adyacentes, control del personal que acceda a zonas susceptibles, identificación de equipos no autorizados, uso de equipos portátiles por parte del personal que puedan acceder al centro de datos, tarjetas de acceso, etc. Un buen ejemplo para controlar este punto es revisar la sección 9 de la norma ISO 27001/2.
- ***Controles Medioambientales:*** En este campo el proveedor debe evidenciar cuáles son las medidas que se tomarían en el caso de presentarse cuestiones medioambientales que provoquen la interrupción del servicio, como catástrofes

o problemas puntuales del centro de datos como la temperatura, la humedad, el impacto de rayos, los problemas eléctricos, etc.

- ***Requisitos Legales:*** Un potencial cliente de servicios de Cloud, debe considerar sus obligaciones a nivel nacional como internacional, respecto al cumplimiento reglamentario cuando fuese necesario. El cliente debe consultar con el proveedor inquietudes como: la ubicación física del proveedor, si utilizará otras compañías cuya infraestructura esté ubicada fuera del proveedor de Cloud, o la jurisdicción de los términos contractuales y de los datos, que sucederá con sus datos una vez finalizado el contrato.

## 4.3 Análisis en base al NIST

El grupo de trabajo del NIST especialistas en Seguridad en Cloud Computing, han desarrollado el reporte "Guías para Seguridad y la Privacidad en Cloud Computing"[31], del cual se extrajeron los temas de: "Aspectos claves para la Seguridad" y "Recomendaciones para la Seguridad", que contienen información relevante para la temática que se está investigando.

### 4.3.1 Aspectos Clave para la Seguridad en Cloud Computing

De acuerdo al NIST los aspectos clave para la Seguridad en Cloud Computing son los siguientes nueve puntos:

#### ❖ Gobernanza

La Gobernanza está relacionada con todos los aspectos de control y supervisión de las políticas, los procedimientos y los estándares para el desarrollo de las aplicaciones. También abarca el diseño, la implementación, las pruebas, y la monitorización de los servicios distribuidos. La diversidad de los servicios de Cloud hace necesaria una buena gobernanza, ya que si los despliegan sin ninguna regulación, se puede convertir en una mezcla inmanejable de servicios inseguros.

Colocar especial atención a los roles y responsabilidades que están repartidas entre el cliente y el proveedor, particularmente en lo referente a la gestión del riesgo. Es conveniente que el programa de gestión de riesgos esté en continua revisión y evolución.

Adicional se recomienda implementar mecanismos y herramientas de auditoría para determinar cómo se está almacenando, protegiendo y utilizando los datos; cómo se validan los servicios y cómo se cumplen las políticas empresariales.

#### ❖ Cumplimiento

El cumplimiento se refiere a la responsabilidad de la organización para operar de acuerdo a las leyes, regulación, estándares y especificaciones establecidas. Existen varios tipos de regulación y leyes, dependiendo el país, el estado o la localidad, lo cual

provoca que el cumplimiento sea un problema complejo para el Cloud Computing. En este aspecto se debe mencionar las siguientes áreas:

- **Leyes y Regulación**
  Los proveedores de servicios de Cloud están cada vez más preocupados por el tema legal y reglamentario, por lo que pueden optar por almacenar y procesar los datos en jurisdicciones específicas y aplicar garantías para la seguridad y la privacidad. De todas formas, el cliente viene a considerarse en última instancia en la responsabilidad de la seguridad y la privacidad de los datos en poder de un proveedor.

- **Localización de los datos**
  La falta de información acerca de cómo se ha implementado una solución de Cloud Computing, hace que el cliente desconozca cómo y dónde son almacenados sus datos, ni cómo están protegidos, posiblemente si el proveedor cuenta con certificaciones de normas de seguridad, el cliente tendrá más confianza en su proveedor.

  Si la información es trasladada entre diferentes países involucrará que tenga diferentes marcos legales y regulatorios, afectando al tratamiento de los datos. La preocupación surge al determinar los límites donde se debe aplicar la legislación del país que recoge los datos y cuando aplicar la legislación del país destino.

- **Descubrimiento electrónico**
  El descubrimiento electrónico consiste en la identificación, recolección, procesamiento, análisis y producción de la información almacenada electrónicamente en la fase de descubrimiento de un proceso judicial. Para este proceso se hace el análisis del correo electrónico, archivos adjuntos y otros datos almacenados en un sistema o en un medio de almacenamiento, así como de los metadatos como fechas de creación o modificación de objetos. El proveedor debe estar en capacidad de almacenar adecuadamente toda la información de sus clientes, evitando daños intencionados que afecten las evidencias en caso de un litigio.

### ❖ Confianza

Para que una organización abandone el control directo de su información y con esto la privacidad y la seguridad de la misma, demanda que tenga un alto grado de confianza en el proveedor. Los puntos clave en este ámbito son:

- **Acceso desde adentro**

  Las amenazas internas son un problema de todas las organizaciones, y en Cloud Computing no es la excepción, los propios empleados, ex-empleados, empresas asociadas o cualquier persona que tenga de alguna forma acceso a los datos, puede causar tanto daños intencionados como no intencionados, desde fraude hasta robo de información confidencial.

- **Propiedad de los datos**

  Para que el proveedor cree un marco de confianza en sus clientes, debe estipular claramente en el contrato que la propiedad de todos los datos los mantiene la organización a diferencia de lo que sucede en las redes sociales, que ha sido un motivo de discusión acerca de quién es el propietario una vez que se utiliza el servicio; además que el proveedor no utilizará su información para beneficio propio.

- **Servicios complejos**

  Un servicio de Cloud Computing puede estar formado por anidación de otros servicios, y su disponibilidad dependerá directamente de los servicios que lo componen. Si la disponibilidad de un servicio de apoyo disminuye, la disponibilidad general también se verá afectada en forma proporcional.

  En el caso que se utilice en un servicio la intervención de terceras partes, se deberá definir las responsabilidades y obligaciones para cada uno. Las garantías de responsabilidad y cumplimiento de estos servicios anexos, pueden representar un grave problema para los servicios compuestos.

- **Visibilidad**

  El monitoreo es una herramienta vital y necesaria en la vigilancia de la seguridad en los servicios de Cloud Computing, en este caso esta responsabilidad ha sido trasladada directamente al proveedor, quien será el encargado de mantener una vigilancia continua, ya que toda la información está en su lado y posee un control completo.

  Es necesario que el proveedor de servicio, sea transparente en lo referente a cómo está operando, que tipo de controles tiene implementado o que procesos utiliza para la gestión de la seguridad y la privacidad de los datos. Normalmente los proveedores suelen ser muy reservados con esta información pues lo consideran como un punto de ataque, pero es necesario que la organización tenga la visibilidad de cómo está siendo manejada su información.

- **Datos Auxiliares**
  El proveedor tiene la responsabilidad de proteger los datos auxiliares de sus clientes, no necesariamente los que se tienen almacenados, sino los datos referentes a información adicional que involucre al cliente, que de igual forma puedan ser usados con fines maliciosos.

- **Gestión del Riesgo**
  La gestión del riesgo es el proceso de identificación y evaluación de riesgo para las operaciones y los activos de la organización, y posteriormente tomar las medidas necesarias para reducirlos a un nivel aceptable. Este proceso incluye la realización de una evaluación de riesgos, la implementación de una estrategia de mitigación de riesgos, y el empleo de técnicas y procedimientos para la supervisión continua del estado de seguridad de los sistemas de información. En [32] se puede visualizar otra herramienta para la gestión del Riesgo.

### ❖ Arquitectura

La arquitectura de una infraestructura de Cloud Computing está comprendida por hardware y software; dentro del software su unidad fundamental es la máquina virtual y las APIS que permiten crear las aplicaciones. La comunicación entre todos estos elementos de la infraestructura puede ocasionar problemas de seguridad. Los puntos importantes son:

- **Superficie de Ataque**
  La inclusión del hipervisor como una capa de software, para la conexión entre el sistema operativo y los elementos de hardware usados para operar con varias máquinas virtuales va a suponer un nuevo punto de ataque. Si el hipervisor se ve comprometido podría resultar en un fallo de todos los sistemas que lo acoge.

- **Protección de la Red Virtual**
  Varias de las plataformas de virtualización tienen la capacidad de crear switches basados en software y configuraciones de red como parte del entorno virtual, permitiendo así que las máquinas virtuales puedan comunicarse de forma directa en el mismo servidor. Al realizar esta conexión el tráfico de red que se produce no puede ser monitoreado por elementos físicos de red como un cortafuegos o un sistema de detección de intrusos, razón por la que se deben extremar las precauciones de seguridad de la red, para evitar ataques internos.

- **Imágenes de Máquinas Virtuales**
  Una máquina virtual comprende una pila de software, incluida todas las aplicaciones instaladas y configuradas. Una práctica común en el entorno de

virtualización es la compartición de la imagen de una máquina virtual, pues es un método de rápido inicio, que a la vez puede introducir un problema de seguridad ya que si una organización ha creado una imagen con sus respectivos datos ésta puede ser replicada.

- **Protección del Cliente**
  En los entornos de Cloud Computing se pueden introducir brechas de seguridad con el uso de navegadores, conexiones inalámbricas o sistemas de escritorio sin sus debidas actualizaciones. Adicional, se puede tener la presencia de virus o troyanos que obtengan información confidencial o realicen monitoreo de la víctima. Para evitar estos inconvenientes, los proveedores deben buscar nuevos mecanismos de seguridad o reforzar los existentes para garantizar la protección del cliente.

### ❖ Identidad y control de acceso

Una de las principales preocupaciones de una organización es la protección y privacidad de los datos sensibles, por lo que el proveedor debe darle gran importancia a la gestión de la identidad y el control de acceso, para brindar a sus clientes garantías en la seguridad de sus datos. Una solución planteada es la federación de identidades, que puede ser implementada a través del estándar SAML o del estándar OpenID.

- **Autenticación**
  La autenticación es el proceso de establecer confianza en la identificación de usuarios. Varios proveedores de servicios de Cloud han optado por utilizar el estándar SAML, el cual proporciona un entorno para el intercambio de información para el proceso de autenticación entre dominios cooperantes, luego a través del uso del protocolo SOAP[37] son enviadas y recibidas las respuestas. Este tipo de mensajes SOAP se firman digitalmente. La autenticación mediante el uso de SOAP puede acarrear problemas de seguridad por lo que debe ser tratada con mucho cuidado. Un ejemplo de ataques es el de tipo XML Wrapping, que manipula las peticiones SOAP introduciendo información en la cabecera.

- **Control de Acceso**
  El uso del estándar SAML no es suficiente para realizar autenticación y control de acceso, es por eso que deben usarse otras opciones como XACML que complementa a SAML y que permite el control de acceso a los recursos. Sin embargo, también puede sufrir ataques los mensajes entre las entidades

[37] SOAP: Simple Object Access Protocol.

XACML, por lo que se los debe proteger contra acciones de repetición, borrado y modificación de la información.

### ❖ Aislamiento de Software

Un proveedor de Cloud Computing está enfocado en ofrecer a sus clientes servicios bajo demanda, entrega rápida y flexibilidad en el servicio y que se logra a través del uso de máquinas virtuales. Una vulnerabilidad que sufren los servicios IaaS son los ataques a las máquinas virtuales por parte alguna otra máquina virtual huésped que esté corriendo sobre un mismo servidor, es por ello que el aislamiento es fundamental en la compartición de plataformas en la Nube.

- **Complejidad del Hipervisor**

  La seguridad de un sistema computacional depende de la calidad del software que se ejecuta en el kernel[38], que controla la ejecución de los procesos. El hipervisor está diseñado para correr múltiples máquinas virtuales de modo concurrente, cada una con su sistema operativo y aplicaciones, pero proporcionando aislamiento entre unas y otras.

  El hipervisor debe ser más inteligente y menos complejo que un sistema operativo. Para mejorar la seguridad y proveer un fuerte aislamiento, se le ha añadido características adicionales que lo convierten en un elemento más complejo, similar a un sistema operativo. Para que el proveedor de Cloud pueda solucionar los problemas y comprenda los riesgos que estos elementos acarrean a su infraestructura, es necesario que conozca apropiadamente el funcionamiento y el uso de la virtualización.

- **Vectores de Ataque**

  El uso de recursos físicos compartidos mediante máquinas virtuales, es un punto propicio para que los atacantes encuentren vulnerabilidades. Entre los vectores de ataque más conocidos son:

  - Desbordamiento de buffer para ejecutar códigos arbitrarios, o fallos para realizar denegaciones de servicio.
  - Ataque "Man in the middle[39]", que modifica el código de autenticación.
  - Instalación de rootkits[40], a través de la modificación de la memoria el momento de una migración de una máquina virtual.

[38] Kernel: Núcleo de un sistema operativo.
[39] Man in the middle (MitM): Ataque en el que el enemigo tiene capacidad de leer, insertar y modificar los mensajes entre dos partes.
[40] Rootkits: Programa que da accesos a una computadora con presencia oculta al administrador para corromper el funcionamiento normal del sistema operativo.

### ❖ Protección de Datos

Los servicios de Cloud Computing están diseñados para compartir plataformas, característica que no es apreciada por los clientes al sentir desconfianza por su información confidencial, por ello el proveedor debe mostrar las garantías de sus datos están debidamente almacenados y en forma segura. El proveedor debe proteger todos los datos de los clientes ya sean aplicaciones, configuraciones o datos propiamente dichos. Adicional se debe proteger la información en cada una de las fases de uso, sea en tránsito o en descanso. Así mismo es necesario el uso de la criptografía para la transferencia de datos y para la gestión de claves.

- **Valor concentrado**

  Con la expansión de servicios de Cloud Computing, también se amplían las opciones de ataque, la infraestructura de un proveedor es un punto de valor concentrado al tener centralizada toda la información de varias organizaciones, lo cual resulta más atractivo para los delincuentes, ya que si realizan un ataque perjudican a varios clientes al mismo tiempo. La ingeniería social vuelve a tomar importancia para obtener las credenciales de administración y a partir de ellas violar la autenticación.

- **Saneamiento de datos**

  Cuando un medio de almacenamiento va a dejar de ser usado por el cliente es necesario que se garantice que la eliminación de sus datos se lo hará de forma correcta e infalible. Lo mismo debe pasar con las copias de seguridad o los datos residuales cuando se cancele el servicio. La compartición de la plataforma podría impedir realizar un proceso de saneamiento adecuado, pues podría eliminarse información de otros clientes. Otra brecha de seguridad en este campo, es la existencia de técnicas que recuperan datos en medios de almacenamiento, a pesar de que éstos hayan sido borrados, lo cual puede usarse con fines maliciosos.

### ❖ Disponibilidad

La disponibilidad puede verse afectada temporal o permanentemente. Inconvenientes como fallos en el equipamiento del proveedor, ataques de denegación de servicio o desastres naturales, ponen en peligro la disponibilidad de los servicios.

- **Fallos Temporales**

  A pesar de que los entornos de Cloud Computing se hayan diseñado para tener una alta disponibilidad, pueden experimentar fallos y caídas de desempeño. En los últimos años se han dado ejemplos como fallas en el almacenamiento, actualizaciones mal realizadas o inoportunas, o fallos en los dispositivos de red, que ha obligado a los clientes a permanecer sin servicio por aproximadamente 3

o 4 horas. Con un nivel del 99.95% al año se tendrán 4.38 horas de caída del servicio, excluyendo las ventanas de trabajo necesarias para los mantenimientos en la infraestructura del proveedor. Este es un aspecto importante para la organización y que debe estar incluido en el contrato o SLA. Por otro lado el proveedor debe presentar su plan de continuidad en el caso de fallos en el servicio y estipular los tiempos de recuperación.

- **Fallos prologados y permanentes**
  Estos inconvenientes pueden ser causados por problemas en otro ámbito como declaración de bancarrota de un proveedor, incautación de los equipos por temas legales o pérdida de los servicios de los proveedores de terceras partes. Al suscitarse un problema de esta magnitud todos los usuarios de los servicios en la Nube pueden quedar fuera por un tiempo indefinido.

- **Denegación de servicio**
  La denegación de servicio consiste en la saturación de un objetivo con varias peticiones falsas y así evitar que se respondan a las peticiones legítimas de forma oportuna. Para este ataque se utilizan varias computadoras o una Botnet[41]. Aun cuando los ataques sean exitosos, el sólo hecho de enviar peticiones ocasiona un alto consumo de los recursos en el proceso de defensa. La denegación de servicio no solamente procesa por medio de la Internet, también se realiza de internamente a servicios que gestionan la infraestructura.

### ❖ Respuesta a incidentes

La labor del proveedor de servicios de Cloud es vital en cada una de las etapas de las incidencias como: verificación, análisis, contención, recolección de evidencias, corrección del problema y restablecimiento del servicio. Tanto el cliente como el proveedor deben estar alerta y mantener una relación de colaboración para detectar y reconocer incidentes de seguridad, puesto que en plataformas de Cloud puede ser difícil su reconocimiento. En el contrato o SLA se deben establecer los procedimientos del proveedor en cuanto a la respuesta a incidentes, así el cliente conocerá con anterioridad que garantías va a tener el momento de suscitarse un incidente con el servicio.

- **Disponibilidad de los datos**
  La disponibilidad de datos referentes al monitoreo es básico y necesario para detectar a tiempo los incidentes de seguridad. Generalmente los clientes se encuentran limitados en el acceso a una fuente de información de eventos, o no

[41] Botnet: Red de equipos zombies.

tener la interfaz adecuada para el sistema de manejo de incidencias que normalmente está bajo la supervisión y restricción del proveedor.

- **Análisis y solución de incidentes**
  Para el análisis completo de una incidencia, se debe conocer el nivel de afectación, los sistemas y aplicaciones afectadas y una reconstrucción del problema suscitado. Los clientes de la Nube, pueden tener inconvenientes en el análisis de las incidencias por el desconocimiento de cómo está la arquitectura y dónde se produjo el fallo. La falta de información del evento limita al cliente para reunir y preservar los datos pertinentes como pruebas.

### 4.3.2 Resumen de Recomendaciones

En la Tabla 6, se muestra un resumen realizado por el NIST sobre las principales recomendaciones en cada una de las áreas clave mencionadas en el literal anterior.

| AREA | RECOMENDACIÓN |
|---|---|
| **Gobernanza** | • Implementar políticas, procedimientos y estándares utilizados para el desarrollo de aplicaciones y servicios de Cloud Computing.<br>• Establecer mecanismos de auditoría y herramientas de control sobre el seguimiento de las políticas organizacionales durante todo el ciclo de vida. |
| **Cumplimiento** | • Entender los diferentes tipos de leyes y regulación que imponen obligaciones se privacidad y seguridad en la organización y el impacto de las iniciativas de Cloud Computing, particularmente aquellos que involucran ubicación de datos, privacidad y controles de seguridad, gestión de registros y requisitos de descubrimiento electrónico.<br>• Evaluar las ofertas del proveedor de Cloud Computing con respecto a los requisitos organizacionales que debe cumplir y asegurar que las condiciones del contrato satisfacen adecuadamente las necesidades de la Empresa.<br>• Asegurarse de que los procesos del proveedor de Cloud Computing no ponga en riesgo la privacidad o la seguridad de los datos y de las aplicaciones del cliente. |
| **Confianza** | • Asegurarse de que los acuerdos de servicio tengan medios suficientes para permitir la visibilidad dentro de los controles de privacidad y seguridad y de los procesos usados por el proveedor de Cloud Computing y su rendimiento.<br>• Establecer derechos de propiedad claros y exclusivos sobre los datos.<br>• Monitorear continuamente el estado de seguridad del sistema de información para apoyar las constantes decisiones de gestión de riesgos |

| | |
|---|---|
| **Arquitectura** | • Comprender las tecnologías subyacentes que el proveedor de Cloud Computing utiliza para servicios de suministro, incluidas las repercusiones que los controles técnicos involucrados tienen sobre la seguridad y privacidad del sistema, a lo largo del ciclo de vida y en todos sus componentes. |
| **Identidad y Control de Acceso** | • Asegurarse de que se cuentan con las garantías adecuadas para asegurar la autenticación, autorización y otras funciones de gestión de acceso e identidad, y que éstas son adecuadas para la organización. |
| **Aislamiento de Software** | • Comprender el funcionamiento de la virtualización y de otras tecnologías de aislamiento que el proveedor de Cloud Computing utilice en la arquitectura de software multy-tenant, y evaluar los riesgos que esto puede conllevar para la organización. |
| **Protección de Datos** | • Evaluar que tan adecuadas son las soluciones brindadas por el proveedor de Cloud en lo referente a la gestión de datos, control de accesos a los datos, seguridad de los datos en reposo, en tránsito y en uso, así como la desinfección de los mismos.<br>• Tomar en cuenta el riesgo que se presenta para la organización al colocar sus datos en una plataforma compartida con otras organizaciones y tener una concentración masiva de datos.<br>• Comprender y evaluar los riesgos involucrados en la gestión de claves criptográficas. |
| **Disponibilidad** | • Entender las cláusulas del contrato y los procedimientos del proveedor de servicio en lo relacionado a la disponibilidad, el backup y la recuperación de datos, la recuperación de desastres; y asegurar que se cumple con los planes de continuidad del negocio y planificación de contingencia.<br>• Asegurarse de que en caso de interrupciones por un desastre, las operaciones críticas pueden ser inmediatamente reanudadas, y el resto de las operaciones pueden restituirse de manera oportuna y organizada. |
| **Respuesta a Incidentes** | • Entender las cláusulas del contrato y los procedimientos del proveedor de servicio en lo referente a las respuestas a incidentes y asegurarse de que se conozcan los requerimientos de la organización.<br>• Asegurarse de que el proveedor de Cloud tiene procesos de respuesta transparentes y mecanismos suficientes para compartir información durante y después de un incidente.<br>• Asegurarse de que la organización pueda responder a los incidentes de forma coordinada con el proveedor, con sus respectivos roles y responsabilidades para el entorno informático. |

**Tabla 6. Resumen de Recomendaciones según NIST**

## 4.4 Comparativa de los riesgos, de acuerdo a las tres iniciativas.

Con el estudio realizado de los riesgos y amenazas, de las tres iniciativas referidas, se ha realizado un esquema (Figura 6) para representar la relación entre cada una de ellas, con el fin de visualizar aquellos riesgos que son coincidentes, y que serían interpretados como los más sobresalientes y que necesitan mayor atención.

| CSA |
| --- |
| • Abuso y uso inadecuado del Cloud Computing<br>• Intefaces y APIs inseguras<br>• Amenazas internas<br>• Inconvenientes por tecnologías compartidas.<br>• Pérdida o fuga de datos.<br>• Secuestro de sesión o de servicio<br>• Desconocimiento |

| ENISA |
| --- |
| • Pérdida de Gobernanza.<br>• Vinculación<br>• Fallo de aislamiento.<br>• Incumplimiento normativo.<br>• Comprometimiento de las interfaces de gestión.<br>• Protección de datos<br>• Supresión de datos insegura o incompleta.<br>• Miembros maliciosos. |

| NIST |
| --- |
| • Gobernanza<br>• Cumplimiento normativo.<br>• Confianza<br>• Arquitectura<br>• Identidad y control de Acceso.<br>• Aislamiento de Software.<br>• Protección de datos.<br>• Disponibilidad.<br>• Respuesta a Incidentes. |

Tabla 7. Resumen de los riesgos según la CSA, ENISA y NIST

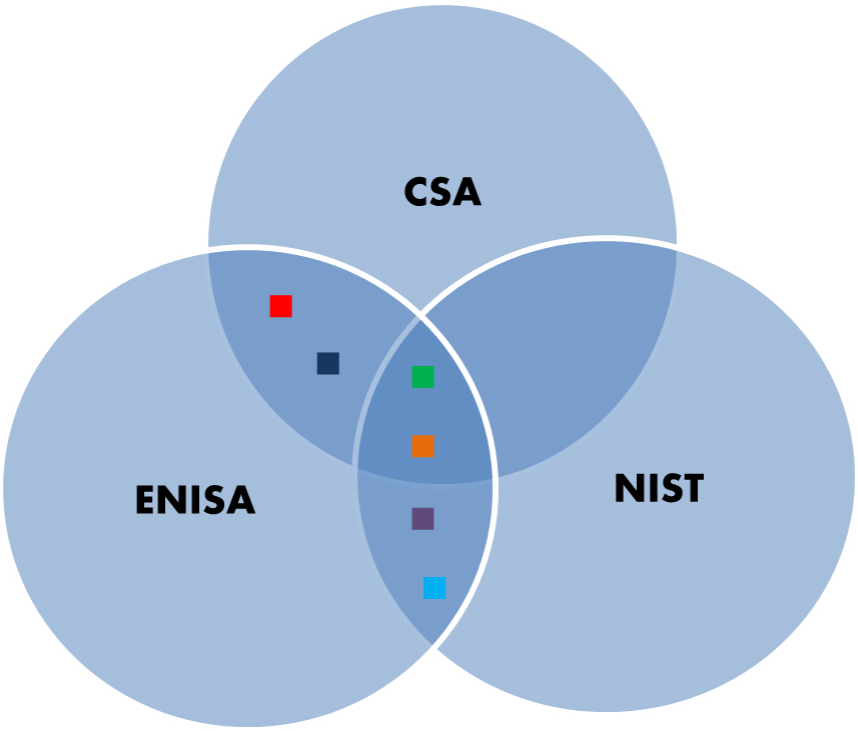


Figura 6. Esquema de comparación de los riesgos en Cloud Computing

# 5 Análisis de los Aspectos Legales en Cloud Computing

La inquietud en los aspectos legales en Cloud Computing surgen a partir del uso explosivo de servicios en la Nube y su constante crecimiento, que a la vez pone de manifiesto la necesidad de tener una legislación adecuada, y que contribuya a un despliegue adecuado de este nuevo ambiente tecnológico.

Interrogantes como: ¿Quién accede a los datos?, ¿Quién los puede ver?, ¿Qué es lo que hacen con ellos? O si se diera un incidente ¿Quién es el responsable, cómo localizarlo o cómo hacerlo responsable de sus actos? Todas estas preguntas hacen que los clientes de la Nube, se sientan intimidados antes de contratar un servicio, de ahí que los dos principales involucrados Clientes y Proveedores busquen el establecimiento de una normativa a seguirse, utilizada como respaldo y garantía para las partes.

Una de las complejidades de la buscada legislación es la ubicación de los datos, ya que éstos podrían situarse en países con una regulación y leyes diferentes a las que se apliquen a la ubicación del cliente o del proveedor. Desde la posición de cliente, éste puede perder la confianza si sus datos van a ser procesados fuera de sus instalaciones y más aún fuera del país y ser colocados en cualquier lugar del mundo.

Este tema preocupa a clientes, proveedores de servicios, y a los gobiernos, puesto que se enfrentan a desafíos legales, que no necesariamente pueden ser cubiertos con la adaptación de sus leyes vigentes, pues pueden dejar vacíos legales, que no sucederían si se propone una nueva legislación en la que se plasme todos los puntos de forma definida.

Para no detener la contratación de estos servicios, se utiliza otra alternativa que es apoyar el tema legal en contratos, en acuerdos de Nivel de Servicio (SLA) o en cualquier otro documento que se establezca entre el cliente y el proveedor. Estos documentos vienen a ser la principal herramienta jurídica para el amparo en cualquier tema legal.

Aspectos como la protección de los datos, la seguridad en el almacenamiento o en las transferencias, el acceso de las autoridades policiales, la preservación de la confidencialidad y no divulgación, deben estar estipulados en los contratos, y tenerse muy en cuenta como parte del campo legal.

En este capítulo se revisará los criterios de las dos Agencias Europeas (CSA y ENISA) en relación a este tema, que finalmente servirá como pauta para el análisis realizado en el Capítulo 6.

## 5.1 Recomendaciones Legales de acuerdo a la CSA

Actualmente se considera que los servicios de Cloud Computing no están regulados, es por ello que la revisión de la parte legal es obligatoria, que necesita igual atención que el proceso técnico de adopción de estos servicios. Lo ideal para una organización es que el departamento técnico y legal se involucren en la contratación de los servicios en la Nube, de este modo el cliente sentirá que está protegido en todos los ámbitos y no sufrirá sorpresas posteriores. Debido a esta problemática la CSA ha visto la necesidad de analizar los parámetros legales y ha realizado un documento guía para los lectores. El objetivo es abordar el cumplimiento normativo que rija el uso de los servicios de Cloud Computing y la relación que pueda tener con la aplicación de otras leyes, para este caso principalmente apoyándose en la normativa de la Directiva 95/46/CE del Parlamento Europeo[42]. Otra ley referenciada es la legislación española, debido a su rigurosidad en la protección de datos personales, considerando que si los servicios de Cloud Computing se adaptan y cumplen esta normativa, es posible que pudieran cumplir cual otra normativa existente.

En Europa, la protección de los datos, se considera un derecho fundamental de los ciudadanos, lo que no sucede en otros lugares como Estados Unidos de América.

Los siguientes puntos detallan los temas a cumplirse en el campo legal, basado en el "Cloud Compliance Report"[33] de la CSA.

### 5.1.1 Establecimiento de roles

Los involucrados directos en Cloud Computing son la empresa proveedora de servicios en la Nube y la organización que los contrata denominada cliente. A estos dos representantes se les ha asignado roles para que tenga aplicabilidad con la normativa revisada, de la siguiente forma:

*Empresa cliente* -> ***Responsable del Tratamiento***

*Empresa proveedora de servicios de Cloud* -> ***Encargado del Tratamiento***

#### 5.1.1.1 Responsable del Tratamiento

El Responsable del Tratamiento de datos en Cloud Computing, es el cliente propiamente dicho quien contrata los servicios en la Nube. Sus responsabilidades son:

- Velar para que el proveedor de servicios de Cloud implemente las medidas necesarias para el cumplimiento de la normativa de protección de datos.
- Analizar el riesgo sobre el ciclo de vida de la información, y los activos que se colocan en la Nube.

[42] Parlamento Europeo: http://www.europarl.europa.eu/news/es.

- Realizar auditorías al proveedor de servicio de forma continua, ya sean internas o externas. Para que el proveedor no se niegue a este proceso es recomendable que se incluya una cláusula de auditoría en el contrato.
- Utilizar las herramientas que el proveedor ponga a su disposición para controlar la información en todo su ciclo de vida.
- Vigilar que el proveedor adopte las medidas de seguridad necesarias de acuerdo al modelo de despliegue: IaaS, SaaS o PaaS.
- Vigilar que se pongan en marcha las medidas de seguridad aplicables al control de acceso, gestión de incidencias, copias de seguridad y recuperación, auditorías y telecomunicaciones.

#### 5.1.1.2 Encargado del Tratamiento

El concepto del Encargado del Tratamiento ha sido establecido por la normativa de protección de datos española como: Persona jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del Responsable del Tratamiento.

En la Nube, el Encargado del Tratamiento de datos es el proveedor de servicios de Cloud Computing. Entre sus responsabilidades están:

- Establecer un contrato claro y detallado, donde coloque todos los aspectos necesarios que den cobertura a la seguridad, la protección y las obligaciones de las partes.
- Indicar en el contrato si va a hacer uso de servicios subcontratados.
- Adoptar las medidas de seguridad de acuerdo al modelo de despliegue: IaaS, SaaS o PaaS.
- Tomar en cuenta las medidas de seguridad para el control de acceso, gestión de incidencias, copias de seguridad y recuperación, auditorías y telecomunicaciones.
- Proporcionar a sus clientes herramientas adecuadas de control para que puedan cumplir con sus respectivas obligaciones.
- Delimitar los países donde se podría realizar el tratamiento de los datos, para así ofrecer más confianza al cliente.

### 5.1.2 Aplicación de la Legislación

La aplicación de la legislación puede ser un tema difícil de comprender, más aún cuando se tengan diferentes lugares de ubicación del cliente, del proveedor de servicios o de los sistemas de tratamiento de datos, para esto hemos tomado como referencia la perspectiva del a CSA quienes indican que el punto clave para la aplicación de una normativa es el lugar donde se encuentra establecido el **Responsable del Tratamiento de datos (Cliente),** tomando en cuenta su ubicación y el tipo de

información que coloca en la Nube para cumplir con el Derecho nacional aplicable, es decir que la ley aplicable sólo dependerá del Estado donde esté el Responsable del Tratamiento que contrata los servicios de Cloud Computing, independientemente de donde esté localizado el proveedor de servicios de Cloud o los sistemas de tratamiento utilizados por el mismo. Un punto adicional que se debe recalcar es que el proveedor deberá tomar en cuenta también las medidas de Seguridad que su propio Estado le exija para la prestación de servicios.

Es necesario mencionar que la relación entre clientes y proveedores puede tener escenarios muy variados, como el caso en que los involucrados se establezcan en un mismo lugar, o que cada uno esté en ubicaciones diferentes, o que los dos estén en la misma ubicación pero que los sistemas de tratamiento de los datos se encuentren en otra ubicación. En el reporte de la CSA se ha dado preferencia a la mención de los casos cuando se encuentran dentro del Espacio Económico Europeo (EEE) y ciertas relaciones fuera de él. Para comprender claramente la aplicación de estos procesos, se muestra los siguientes ejemplos:

- **Caso 1:** El Responsable del Tratamiento se establece en el Estado Francés (Miembro del EEE) y el Encargado del Tratamiento se sitúa en un lugar diferente, por ejemplo España. La legislación que será aplicada para el tratamiento de los datos será la normativa francesa. Ver Figura 7.

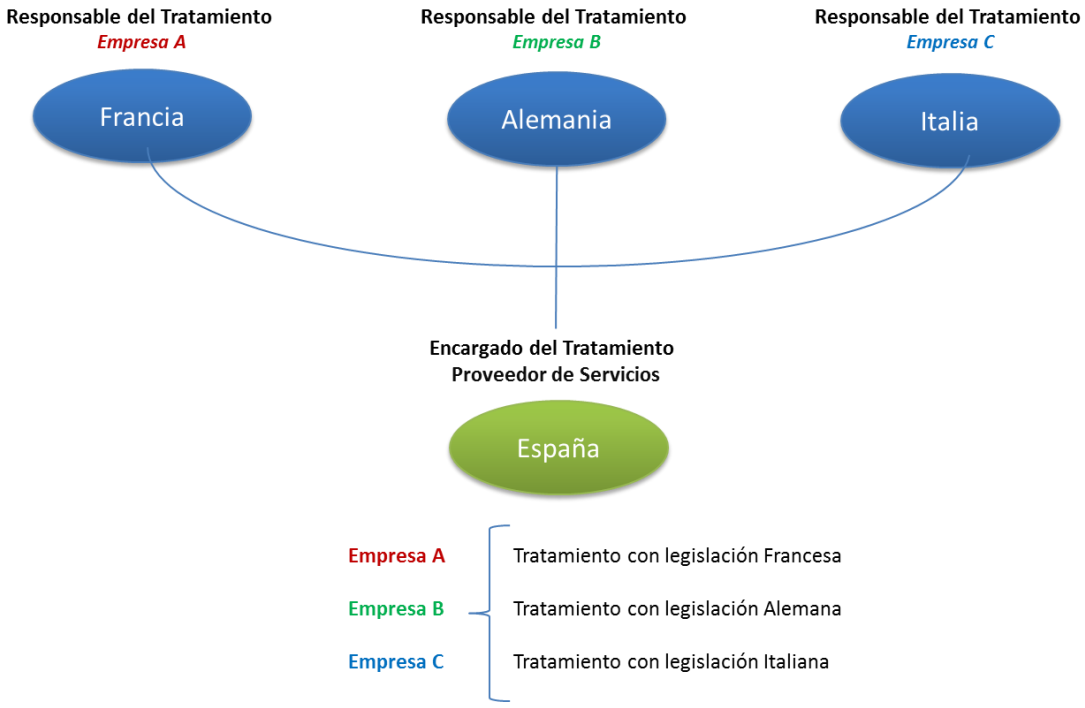


Figura 7. Esquema Caso 1

- **Caso 2:** El Responsable del Tratamiento es una empresa multinacional, establecida en una ubicación como Francia, y sus sucursales en Alemania e Italia. En Francia se realizan todas las operaciones y movimientos con los datos recogidos del resto de sucursales, por lo que la legislación a aplicarse es la legislación francesa, aun cuando los datos procedan de Alemania o Italia. Ver Figura 8.

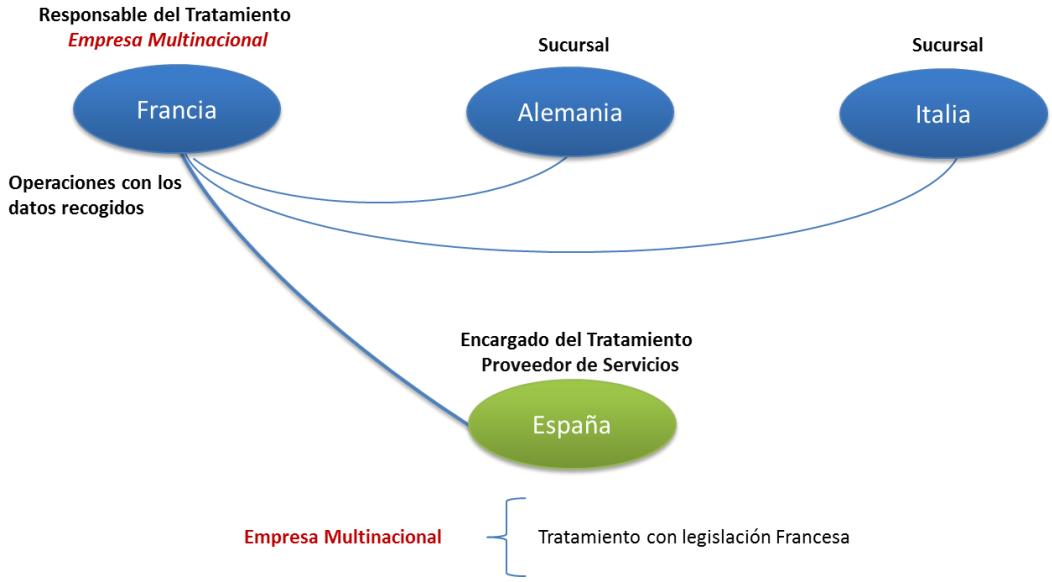


Figura 8. Esquema Caso 2

- **Caso Especial:** Si el Responsable del Tratamiento no está establecido en el EEE, pero su proveedor de servicios utiliza medios o equipos ubicados en un Estado del EEE, dicho proveedor exportará la legislación de protección de datos del Estado miembro para el tratamiento de datos personales de sus clientes. Ver Figura 9.


Figura 9. Esquema Caso Especial

### 5.1.3 Legislación Aplicable

La legislación que la CSA ha usado y que cubre los puntos del tratamiento de datos personales es la Directiva 95/46/CE [34], la cual representa un marco europeo, que sirve como guía para otras legislaciones a nivel continental, y que establece varios principios para los estados miembros con respecto a temas como: la información, el consentimiento, la finalidad, la calidad, la seguridad, los derechos de acceso, la rectificación, la cancelación y oposición, la autoridad de control independiente y la limitación a las transferencias internacionales de datos.

Las dos consideraciones tomadas en cuenta son:

- Establecimiento del Responsable del Tratamiento de datos, ubicado en un país perteneciente al Espacio Económico Europeo (EEE), y
- Si el Responsable del Tratamiento de los datos está fuera del EEE, pero hace uso de medios para el tratamiento de los datos que se localizan en el EEE.

Adicional a la Directiva 95/46/CE, en el territorio español se hace uso de:

- Ley Orgánica de Protección de datos de carácter personal 15/1999 (LOPD) [35], y
- Real Decreto 1720/2007 Reglamento de desarrollo de la Ley Orgánica 15/1999 (RLODP) [36].

A continuación se mencionan las cláusulas más destacadas de estas tres normativas, que describen los puntos relacionados y con aplicación para el tratamiento de datos personales.

De acuerdo al:

- Art. 4, de la Directiva 95/46/CE, al Art. 2 de la LOPD y al Art. 3 RDLOPD: Se proporciona las directrices para el tratamiento de los datos personales y para la protección de los mismos.
- Art. 12 de la LOPD: Establecer un contrato entre el cliente y el proveedor de servicios, específicamente se menciona que: "*El contrato es una obligación entre el responsable de los datos y el Encargado del Tratamiento, y que se debe dejar por escrito o de alguna forma que permita acreditar su celebración y contenido*".
- Art. 20.2 del RLOPD: El cliente debe vigilar el cumplimiento de medidas de seguridad por parte de su proveedor de servicios en la Nube.
- Art. 82.2 del RLOPD: El proveedor de servicios debe disponer de un Documento de Seguridad.
- Art. 88 del RLOPD: El documento de Seguridad del proveedor de servicios de Cloud debe indicar cuáles son las medidas de seguridad que se van a aplicar a los archivos que contengan datos personales de los clientes, empleados y proveedores.
- Art. 21 de la RLOPD: Si el proveedor de servicios subcontrata servicios externos, debe cumplir los siguientes requisitos:
  - ✓ Que el servicio que va a ser subcontratado, se haya estipulado en el contrato entre el proveedor y el cliente, con la respectiva explicación del servicio.
  - ✓ Que el cliente establezca indicaciones de cómo deben ser tratados sus datos.
- Art. 83 del RLOPD: El proveedor de telecomunicaciones debe conservar íntegros los datos en tránsito, y no revelar el contenido de las comunicaciones, a menos que sea solicitada por una entidad legal autorizada.
- Art. 20 a 22 del RDLOPD: Si el proveedor de telecomunicaciones ofrece servicios complementarios como hosting, se le considerará como Encargado del Tratamiento.

Por otro lado, los siguientes artículos de la RLOPD, abarcan los procedimientos más notables que tienen aplicación en el Cloud Computing.

1. Art. 117 al 119, Tutela de derechos ARCO[43].
2. Art. 120 al 129, Ejercicio de la potestad sancionadora.
3. Art. 130 al 136, Inscripción o cancelación de ficheros.
4. Art. 137 al 144, Transferencias internacionales de datos.
5. Art. 153 al 156, Exención del derecho de información al interesado.

[43] ARCO: Derechos de acceso, rectificación, cancelación y oposición.

6. Art. 157 y 158, Autorización de conservación de datos para fines históricos, estadísticos o científicos.

### 5.1.4 Transferencias Internacionales

Las transferencias internacionales son muy frecuentes en la Nube, por lo que se deben considerar las regulaciones específicas para ésta área.

Para el caso español se usa la siguiente legislación:

- Capítulo IV de la Directiva 95/46/ CE: Transferencia de datos personales a países terceros.
- Título V de la LOPD: Movimiento internacional de datos.
- Título VI del RLOPD: Transferencias internacionales de datos.

**Consideraciones:**

- ✓ Conocer si la transferencia de datos se hace a un país con un nivel de protección de datos adecuado, o por lo contrario a un país que no lo posea.
- ✓ Si el movimiento de los datos se realiza entre los 27 países miembros de la Unión Europea, y los tres países más del Espacio Económico Europeo, no necesitan ningún requisito adicional, únicamente la identificación en la notificación del fichero al Registro General de Protección de Datos.
- ✓ Se considera a Suiza, Canadá, Argentina, Jersey, Isla de Man y Estados Unidos como países que cuentan con un nivel de protección adecuado.
- ✓ Si el movimiento se lo realiza dentro de un grupo multinacional, se deberían establecer "Binding Corporate Rules"[44], que estipulen la regulación necesaria para este procedimiento.
- ✓ Si el movimiento de los datos se realiza a un país que no tiene un nivel adecuado de protección de datos, se debe solicitar autorización de la autoridad competente, en el caso de España, al Director de la Agencia Española de Protección de Datos. Para que se ejecute la aprobación, las partes (exportador e importador) deben firmar un contrato escrito donde se estipulen las garantías necesarias para el respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales.
- ✓ El cliente debe conocer la ubicación territorial de los medios que van a ser utilizados por el proveedor para dar el tratamiento a sus datos, de este modo conocerá si el país donde se localiza cuenta o no con el nivel de protección adecuado.

[44] Binding Corporate Rules: Normas corporativas vinculantes, que permiten la transferencia internacional de datos personales en empresas multinacionales.

- ✓ La infraestructura del proveedor puede cambiar de lugar físicamente sin que el cliente se entere, haciendo que sea primordial la regulación de este tema.
- ✓ El cliente debería analizar en primer lugar que tipo de datos piensa colocar en la Nube, y si el hecho de que dichos datos se encuentren en otro país pueda traerle problemas con la jurisdicción que los aplica, ya que puede ser difícil hacer cumplir derechos legales.
- ✓ Es conveniente que en el contrato se incluya, una cláusula donde se indique el lugar donde van a localizarse los datos, para que de éste modo el cliente tenga claro en qué país se situará, y a la vez colocar una referencia dependiendo del país, de que cual es la normativa aplicable en esa jurisdicción, como por ejemplo para los miembros del Espacio Económico Europeo es la Directiva Europea 95/46/CE.

### 5.1.5 Autoridades de Control

En la legislación Europea y conforme a la Directiva 95/45/CE debe existir una autoridad independiente de control, para la protección de datos personales.

De acuerdo al:

Art. 28, de la Directiva 95/45/CE, se obliga a los estados miembros del EEE a delegar autoridades encargadas de vigilar en su territorio el cumplimiento de la normativa.

Las funciones de esta entidad son:

- Tener en cuenta las peticiones y reclamos de los afectados.
- Solucionar los reclamos de tutela de los derechos ARCO.
- Inspeccionar y sancionar en caso de requerirlo.
- Realizar vigilancia de carácter preventivo.
- Ordenar el cese del tratamiento de los datos.
- Otorgar las autorizaciones que dictamine la norma.

Debido a la característica de extraterritorialidad del Cloud Computing, las autoridades de control, pudieran tener que aplicar más de una legislación para resolver algún reclamo o inconveniente.

### 5.1.6 Comunicación de datos a otras autoridades

Uno de los casos con trascendencia legal, puede darse cuando una autoridad competente solicite al proveedor de servicios de Cloud, información personal de alguno de sus clientes. Esta responsabilidad a su vez recaerá sobre el Responsable del Tratamiento, que en la Nube es directamente el cliente.

Si los datos son solicitados por una autoridad, el proveedor deberá informar al usuario que sus datos han sido requeridos y posteriormente entregados.

Si en el contrato que firman las dos partes, no queda estipulado que tipo de información el cliente está colocando en la Nube, el proveedor puede desconocer totalmente qué tipo de información se está transfiriendo hacia el proveedor, y la naturaleza de la misma.

## 5.2 Recomendaciones Legales de acuerdo a la ENISA

La ENISA considera que las cuestiones legales son un aporte clave para una expansión adecuada del Cloud Computing. Su reporte "Beneficios, riesgos y recomendaciones para la Seguridad de la Información", también examina el campo legal, usado posteriormente para una comparativa jurídica.

En su gran mayoría, los clientes colocan su preocupación en la Seguridad y en la protección a los datos. En esta instancia, es donde la presencia de la legislación tiene vital importancia, ya sea la por la protección legal que se tenga en un contrato con el proveedor o por las leyes que se dispongan en cada región.

Si el único elemento jurídico con el que cuenta el cliente es el contrato o el SLA, es necesario que este documento sea detallado y específico, para garantizarle a la organización la cobertura en los puntos trascendentales como la seguridad y la privacidad. Posterior a que el proveedor de Cloud le haga partícipe el contrato preparado, el potencial cliente debe revisar exhaustiva y cuidadosamente todo lo incluido en este documento.

De acuerdo a la ENISA se tienen cinco aspectos legales a ser cubiertos (Ver Figura 10), los cuáles no corresponden exclusivamente al Cloud Computing, y que se puede tomar como referencia el análisis legal aplicado a los servicios de Internet, siempre recordando que los servicios en la Nube van a plantear nuevos desafíos y cambios regulatorios.

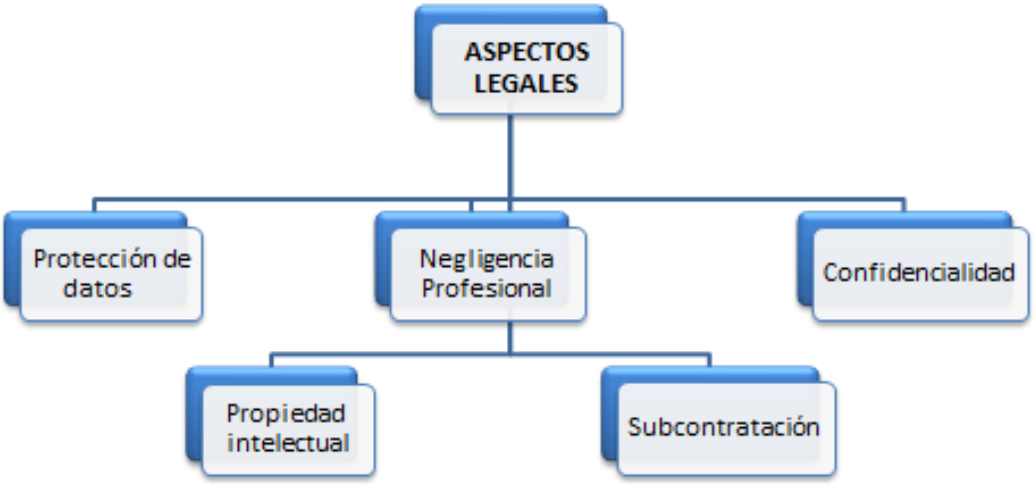


Figura 10. Aspectos Legales según la ENISA

Adicionalmente, se debe considerar el tipo de empresa con la que se está tratando a nivel del proveedor como en el caso del cliente, ya que a partir de ello se puede establecer la capacidad de negociar las cláusulas que estén contenidas en el contrato de prestación de servicios en la Nube, tal como lo muestra la Tabla 8.

| PROVEEDOR | CLIENTE | CONTRATO |
|---|---|---|
| Empresa grande | PYME | Debilidad para negociar el contrato por parte del cliente. |
| Empresa mediana | Empresa mediana | Opción de negociar por cualquiera de las dos partes. |
| PYME | Empresa grande o entidad pública | Opción de negociar por parte del cliente. |

Tabla 8. Relación cliente – proveedor de acuerdo al tipo de organización.

Una PYME que contrate un servicio con un proveedor grande, puede estar imposibilitada para realizar modificaciones o cambios al contrato, sin embargo, podría evaluar diferentes proveedores con mejores opciones en los puntos del SLA o contrato.

Si los dos integrantes del contrato son empresas medianas, están en capacidad de negociar las cláusulas desde la perspectiva de cada una de las partes.

Finalmente si el cliente es una gran empresa o pertenece al grupo de las entidades gubernamentales, pueden estar en la posición de solicitar a su proveedor el establecimiento de un contrato específico que se adapte a sus solicitudes.

### 5.2.1 Protección de datos

Las orientaciones de este punto, están basadas en el reporte de la Directiva 95/46/CE y del Consejo del 24 de Octubre de 2009 [34], en lo relacionado a la protección de personas físicas, el tratamiento de datos personales y la libre circulación de estos datos.

En primer lugar, se debe diferenciar cinco conceptos:

1. ***Datos personales:*** Toda la información referente a una persona física identificada o identificable (con un número de identidad).
2. ***Datos sensibles:*** Datos personales que revelen la raza, etnia, religión, filosofía u otro tipo de información como opiniones políticas, pertenencia a asociaciones, a partidos políticos, sindicatos o grupos religiosos, o también datos relacionados a su salud y sexualidad.
3. ***Tratamiento de datos personales:*** Conjunto de operaciones realizadas sobre los datos personales. Las operaciones están formadas por las fases de registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión u otra forma que de acceso a esta información.
4. ***Responsable del Tratamiento:*** Persona física o jurídica u organismo que determine los fines y los medios del tratamiento de datos personales.
5. ***Encargado del Tratamiento:*** Persona física o jurídica u organismo que trate datos personales por cuenta del Responsable del Tratamiento.

**Consideraciones:**

- Cualquiera de los servicios que oferte un proveedor de Cloud Computing realizará el procesamiento de datos personales, aún incluidos los datos sensibles.
- La ubicación del Responsable del Tratamiento es relevante para la aplicación de la legislación.
- La ubicación del tratamiento de datos no es relevante para la aplicación de la legislación.
- Para el caso puntual de la aplicación de la Ley de la Directiva, se la aplicará si el *Responsable del Tratamiento* está situado en la Unión Europea, y si se recurre a medios ubicados dentro del mismo territorio, un ejemplo puede ser un centro de datos.

- De acuerdo al esquema de los 5 conceptos, para un entorno de Cloud en este análisis se distinguirá al cliente como el "*Responsable del Tratamiento*" y al proveedor de servicios como el "*Encargado del Tratamiento*".
- La función del *Responsable del Tratamiento* es elegir el *Encargado del Tratamiento,* e informar a sus clientes lo relacionado sobre la transferencia de datos al proveedor de la Nube, cuáles son los fines de realizar dicha acción y que calidad de servicios está recibiendo. También se debe informar si el tratamiento de los datos y la transferencia se realizará fuera del EEE.
- Todos los involucrados en el tratamiento de los datos, deben estar al tanto de los derechos y obligaciones relacionados con el proceso, y tener muy entendido el derecho de respetar la vida privada.
- Uno de los requisitos prioritarios del cliente cuando contrata un servicio en la Nube, es la garantía de que sus datos estén disponibles e íntegros, por esto los proveedores deben reforzar las medidas de seguridad, como en los países europeos que existen requisitos obligatorios de seguridad a cumplirse previamente antes de brindar servicios, aun así el cliente debe asegurarse de que se cumplan todas las medidas.
- El cliente se considera como el único Responsable del Tratamiento de datos, aun cuando el tratamiento lo realice el proveedor de la Nube en calidad de encargado externo del tratamiento.
- El cliente debe asegurarse que en el contrato firmado con el proveedor se estipule una cláusula de protección de datos, y las funciones y las obligaciones de las partes.
- Debido a que el cliente es el responsable en su totalidad del tratamiento de los datos, y legalmente responsable de la equidad, la legalidad y la finalidad de los mismos, debe apoyarse en cláusulas que lo respalden en este propósito.
- Cuando el proveedor es una empresa grande y el cliente una PYME, será el proveedor quien establezca la cláusula de protección de datos, es ahí donde el cliente PYME debe asegurarse que dicha cláusula le aporte las garantías de un tratamiento lícito de los datos y las soluciones necesarias en caso de presentarse daños contractuales. Si las dos empresas son medianas tanto cliente como proveedor, la cláusula de protección de datos, podrá ser negociada por cualquiera de las partes, mientras que si el proveedor es pequeño y trata con empresas grandes o gubernamentales, pueden ser que estos clientes sean quienes establezcan la cláusula indicada.
- Si la ubicación del proveedor de servicios de Cloud está fuera del Espacio Europeo, la protección de datos deberá ser soportada por cláusulas contractuales.

### 5.2.2 Confidencialidad

La confidencialidad debe ser protegida por el proveedor, ya que representa un factor de riesgo para sus clientes. Ninguno de ellos se sentirá tranquilo si la confidencialidad no se ve garantizada. Si existe una fuga de información causada por el proveedor por un fallo o intencionalmente, esto repercutirá en forma dañina en la actividad o en las operaciones del cliente y en la reputación del proveedor.

**Consideraciones:**

- Un cliente PYME deberá revisar a detalle la cláusula de confidencialidad y no divulgación que el proveedor ofrezca en el contrato, determinando si cuenta con las suficientes garantías para preservar toda la información sensible y secreta que se colocará en la Nube.
- En los otros dos tipos de cliente, estas cláusulas deben negociarse y estipular una infracción si la información confidencial del cliente es divulgada.

### 5.2.3 Propiedad Intelectual

La propiedad intelectual puede ponerse en riesgo al utilizar un entorno de Cloud Computing, y que si sufre un perjuicio, será un daño posiblemente nunca revertido, aun utilizando proceso legales.

**Consideraciones**:

- Incluir una cláusula contractual específica que regule los derechos de propiedad intelectual.
- Un cliente PYME, deberá evaluar el valor de su propiedad intelectual y con este conocimiento, revisar la cláusula relacionada para verificar si le da garantías y el proveedor utiliza herramientas en pro de la protección de su información.
- Para los otros dos clientes (medianos y grandes), se negociará una cláusula que penalice al proveedor si éste violara las disposiciones colocadas acerca de la propiedad intelectual.

### 5.2.4 Negligencia Profesional

La negligencia profesional puede hacer que el cliente experimente errores en los servicios contratados, a la vez estos errores exponen a los clientes a inconvenientes con sus respectivos usuarios, y tal vez hasta el incumplimiento de temas contractuales. Otro punto de afectación está en las actividades de los empleados de la empresa cliente, puesto que si se contrata tecnología para procesos internos que sean críticos, tendrá una afectación directa sobre su propia organización.

**Consideraciones:**

- Para un cliente PYME, la cláusula de limitación/exclusión estará a favor del proveedor, por lo que el cliente deber revisar si esto es sostenible.
- Para clientes de organizaciones medianas y grandes, y con contratos de alto valor, se recomienda colocar cláusulas de limitación de la responsabilidad y cláusulas de indemnización, que coloquen responsabilidades hacia el proveedor de Cloud por los daños y perjuicios que pueda experimentar el cliente.

### 5.2.5 Servicios de subcontratación y cambios de control

La intervención de terceras partes en el servicio que presta el proveedor de Cloud Computing, puede poner en riesgo la calidad de los mismos. Un cliente puede elegirlo en base a su renombre o profesionalidad, pero puede desconfiar de la subcontratación de servicios a terceros, de quienes desconozca sus procesos y que no ofrezcan las mismas garantías que el proveedor de la Nube.

**Consideraciones:**

- Un cliente PYME, deberá determinar si su proveedor subcontrata servicios y la calidad de los mismos. Podrá solicitar al proveedor garantías relativas al funcionamiento de los servicios subcontratados.

  En los cambios de control, el cliente debe revisar si existe una cláusula que mencione el procedimiento de comunicación a seguirse cuando se dé un cambio en la organización administrativa del proveedor y estipular que el contrato pueda disolverse si no está de acuerdo con dichos cambios.

- Los clientes de organizaciones medianas, grandes y entes públicos, están en la posición de autorizar o no la subcontratación de servicios. En esta línea, el cliente debe estar informado sobre los servicios que se quiere subcontratar y quien es la empresa que los ejecuta. Como en el caso anterior el proveedor debe ofrecer las garantías relativas a los servicios subcontratados.

  Para los cambios de control, este tipo de clientes están en la posición de negociar, de que si el proveedor va a tener alguna modificación en su organización, el cliente pueda aprobarla o no, y también poder dar término al contrato o establecer una renegociación del mismo.

- Todas estas opciones deben estar claramente estipuladas en una cláusula de garantías y compensaciones, una cláusula de cambio de control y una cláusula de resolución del acuerdo.

### 5.2.6 Resumen y lista de Chequeo de las cláusulas a incluirse en el contrato o SLA.

De lo revisado en los cinco literales anteriores, se ha resaltado cuales son los puntos necesarios que un cliente debe considerar antes de firmar un contrato con un proveedor de la Nube, de este modo se protegerá aun cuando en su país no exista una legislación que ampare este tipo de servicios.

En la Tabla 9 se ha colocado un resumen de las cláusulas indispensables en un proceso de contratación de servicios de Cloud Computing, siendo muy recomendable que se analice detenidamente el documento que el proveedor pone a su disposición antes de la firma de las partes y revisar con esta lista de chequeo, que proporciona una confirmación si se está dando alcance a todos los temas antes mencionados.

| ASPECTO | DEFINICIÓN | CHEQUEO |
|---|---|---|
| 1 | Cláusula de protección de datos | ✓ |
| 2 | Cláusula de confidencialidad / no divulgación | ✓ |
| 3 | Cláusula de propiedad intelectual | ✓ |
| 4 | Cláusula de limitación de la responsabilidad | ✓ |
| | Cláusula de indemnización | ✓ |
| 5 | Cláusula de garantías y compensaciones | ✓ |
| | Cláusula de cambio de control | ✓ |
| | Cláusula de resolución del contrato | ✓ |

Tabla 9. Lista de Chequeo sobre las cláusulas legales.

# 6 Caso de Estudio: Marco Regulatorio en Ecuador

## 6.1 Situación Actual

El Ecuador es un territorio donde el Cloud Computing se encuentra en una etapa inicial e inmadura, pero en proceso de crecimiento y adaptación a las nuevas exigencias del mercado. Las Tecnologías de la Información se han convertido en un instrumento poderoso en los movimientos económicos y estratégicos a nivel mundial y también local. Es fácil ver como la informática y las telecomunicaciones son las industrias más poderosas mundialmente, gracias a su participación en todas las actividades diarias de los individuos y más aún en la intervención en el plano empresarial. Los sectores tecnológicos se encuentran en plena efervescencia y Ecuador no es un lugar ajeno a este fenómeno, el Cloud Computing es un ejemplo palpable que se pone a disposición de las organizaciones para la innovación en el sector tecnológico y permitirles ser más competitivas.

Los proveedores ecuatorianos que incursionan en los servicios en la Nube deben enfrentar el reto de saber llegar a las organizaciones, pues a pesar de ser tan beneficioso para el cliente, su principal incertidumbre se fundamentará en la Seguridad de la Información como ya se lo ha mencionado, para ello el ofrecimiento debe ser el de servicios seguros y de calidad, que permitan que el cliente deposite su confianza y se sienta cómodo en realizar la migración hacia la Nube.

Para revisar con precisión la situación actual del despliegue de los servicios de Cloud Computing en el Ecuador, es conveniente realizar un análisis FODA, mostrado en la Tabla 10, para medir la repercusión y viabilidad en la adopción de este cambio tecnológico.

| | |
|---|---|
| **FORTALEZAS** | 1. Conceptos relativamente nuevos en la región, por lo que su expansión se debe realizar de forma controlada.<br>2. Desarrollo rápido de una infraestructura de IT.<br>3. Especialistas en el área de IT realizando el manejo de los servicios.<br>4. Escalabilidad en la infraestructura tecnológica, sin nuevas inversiones.<br>5. Colaboración con las PYMES que son potenciales clientes, economizando costos en tecnología. Las PYMEs constituyen un alto porcentaje dentro de la industria ecuatoriana. |
| **OPORTUNIDADES** | 1. Permitir que las empresas ecuatorianas puedan alcanzar un nivel tecnológico de países desarrollados.<br>2. Centrar los esfuerzos de las organizaciones hacia el núcleo del negocio.<br>3. Reducir costos en la infraestructura de IT de las grandes empresas.<br>4. Permitir que las empresas cuenten con infraestructuras controladas con todos los estándares del sector.<br>5. Incremento de la seguridad en las aplicaciones. |

| | |
|---|---|
| **DEBILIDADESS** | 1. Falta de una cultura de Seguridad de la Información, en proveedores y clientes.<br>2. Falta de conocimientos de Cloud Computing, tanto de sus beneficios como de sus debilidades.<br>3. El índice de penetración de Internet no sobrepasa el 30%, por lo que el acceso a la Nube mediante la Internet puede verse limitado.<br>4. Capacidades de acceso a la Internet relativamente bajas, provocando procesos y aplicaciones lentas. |
| **AMENAZAS** | 1. Pérdida de control en los datos que manejarán los proveedores.<br>2. Proveedores que no están certificados en estándares de Seguridad de la Información.<br>3. Monopolio por parte de los pocos proveedores de servicio que pueden brindar el servicio de la Nube.<br>4. Carencia de regulación para la expansión de los servicios. |

**Tabla 10. Análisis FODA del Cloud Computing en Ecuador.**

En base al FODA mostrado, se concluye que la adopción de servicios en la Nube en Ecuador es viable, por presentar Fortalezas y Oportunidades que confirman un terreno adecuado para su despliegue, recordando que las Amenazas y las Debilidades están presentes, y que las soluciones que se adopten no permitan potenciarlas. Aun cuando el Cloud Computing puede ser considerado un paradigma, los entendidos en las Tecnologías de la Información de las empresas ecuatorianas, le apostarán a una solución robusta y a la vez beneficiosa.

En el año 2012 algunos operadores ecuatorianos han optado por incursionar en los servicios de Cloud Computing, como la empresa *Telconet*[45] que ofrece a sus clientes servicios IaaS, inaugurando dos centros de datos de alta disponibilidad más grandes del país y de Latinoamérica que cuentan con la categoría TIER III y IV. Otra compañía que apuesta por la Nube, es *Cloud Ecuador*[46] quienes ofrecen los tres modelos de despliegue IaaS, PaaS y SaaS. *Telefónica Ecuador*[47], también pone a disposición centros de datos, pero con localización en otros países como Brasil, Argentina o Estados Unidos enfocados hacia el uso de empresas multinacionales que tienen sucursales en Ecuador.

Por otro lado y tal como se menciona en las amenazas de la Tabla 10, la no existencia de una normativa que regule los servicios brindados por un proveedor de Cloud,

[45] Telconet: http://telconet.net/index.php/es/nuestros-servicios/centro-de-datos
[46] Cloud Ecuador: http://www.ecuadorcloud.com/index.html
[47]Telefónica: http://www.movistar.com.ec/site/empresas/datos-empresas/ti-y-outsourcing/hosting.html

puede acarrear problemas en el ámbito legal para los clientes y las compañías proveedoras del servicio.

Al momento existe un vacío legal de una legislación exacta para Cloud Computing, por lo que se trata de cubrir con las leyes ecuatorianas existentes, que pueden dar alcance en mayor parte al manejo de datos y la protección de datos personales, pero no con todas las especificaciones que las soluciones de la Nube demandan.

A continuación se hace una revisión de las leyes vigentes que pueden tener relación con el entorno de Cloud:

- Constitución de la República del Ecuador
- Ley del Sistema Nacional de registro de Datos Públicos
- Ley de comercio electrónico, firmas electrónicas y mensajes de datos

### 6.1.1 Constitución de la República del Ecuador

La Constitución de la República [37] constituye la legislación suprema del Ecuador y se ubica sobre cualquier otra normativa. Está considerada como el marco para la organización entre el gobierno y la ciudadanía y como la fuente de la autoridad jurídica para el gobierno. La Constitución vigente fue revisada por la Asamblea Constituyente en el 2008.

Al ser un documento enfocado a cubrir todas las áreas de interés del gobierno y los derechos de los ciudadanos, los artículos que se pueden extraer con respecto al tema en estudio son escasos. Específicamente, el artículo 66 de este documento, puede ser interpretado para la aplicación en servicios de Cloud Computing. Los literales 19, 21 y 28, manifiestan la garantía de los derechos a la identidad personal y colectiva y a la protección de datos de carácter personal, incluyendo el acceso a éstos datos y la decisión sobre la información que se proporciona. El texto original del artículo es:

***Art. 66.-*** *Se reconoce y garantizará a las personas:*

***Numeral 19.*** *El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.*

***Numeral 21.*** *El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.*

***Numeral 28.*** *El derecho a la identidad personal y colectiva, que incluye tener nombre y apellido, debidamente registrados y libremente escogidos; y conservar, desarrollar y fortalecer las características materiales e inmateriales de la identidad, tales como la nacionalidad, la procedencia familiar, las manifestaciones espirituales, culturales, religiosas, lingüísticas, políticas y sociales.*

Verificando en estos tres numerales, el objeto de esta ley es garantizar la protección de los datos personales como un derecho constitucional. Un proveedor de servicios en la Nube, debe tomar en cuenta que si no maneja adecuadamente los datos personales de sus clientes, puede estar infringiendo lo dictaminado por esta normativa.

Por otro lado, la Constitución Ecuatoriana también reconoce el derecho de Habeas Data en el Artículo 92, un recurso legal que permite a los ciudadanos conocer la existencia de una base de información o registro de datos sobre sí mismo o sobre sus bienes y acceder a ella para corregirlos, sea en una parte o en su totalidad, y así evitar que dicha información pueda causarle perjuicios. También tiene derecho a conocer el uso que pueda realizarse con dichos datos. Este derecho está muy ligado hacia la protección de datos, y les proporciona garantías procesales y judiciales.

El Habeas Data tiene la característica de carecer de autoridades de control, por lo que en el caso de haber algún inconveniente la intervención de la autoridad se da ex-post[48], es decir que su intervención se realiza luego de algún incumplimiento. En Cloud Computing, esto pudiera no resultar adecuado, en primer lugar porque si se ocasiona daños en la información esto puede ser no subsanable o recuperable, y en segundo punto pues sería adecuado que los proveedores tengan que cumplir requisitos y obligaciones previas, antes de poner en marcha los servicios, tal como se da en Europa al tener normativas ex–ante[49]

### 6.1.2 Ley del Sistema Nacional de Registro de Datos Públicos

La presente Ley [38] es una normativa publicada el 31 de Marzo de 2010 con la finalidad de regular el sistema de registro de datos públicos y su acceso, y la administración de las bases de datos que manejan entidades públicas y privadas. Además sirve para garantizar la seguridad jurídica, la sistematización e interconexión de la información y la implementación de nuevas tecnologías.

La mayoría de los artículos están redactados para el tratamiento de datos personales y datos sensibles que maneja el Estado en varios entes de orden público como el Registro Civil, el de la Propiedad Mercantil, vehicular, de patentes, Propiedad Intelectual, entre otros.

[48] Ex–post: Expresión latina con significado "Ley posterior al hecho".
[49] Ex-ante: Expresión neolatina con significado "Antes del suceso".

Específicamente son los artículos 12, 13 y del 21 al 26, donde se ha delimitado las directrices para el tratamiento de los datos personales, sin embargo si queremos acoplarlo al entorno de Cloud Computing ninguno de ellos guarda relación con los requisitos específicos que han aparecido en este modelo, más bien son una continuidad de lo que se menciona en la Constitución de la República.

El texto original de estos artículos es el siguiente:

***Art. 12.- Medios Tecnológicos.-*** *El Estado, a través del ministerio sectorial con competencia en las telecomunicaciones y en la sociedad de la información, definirá las políticas y principios para la organización y coordinación de las acciones de intercambio de información y de bases de datos entre los organismos e instancias de registro de datos públicos, cuya ejecución y seguimiento estará a cargo de la Dirección Nacional de Registro de Datos Públicos. La actividad de registro se desarrollará utilizando medios tecnológicos normados y estandarizados, de conformidad con las políticas emanadas por el ministerio sectorial de las telecomunicaciones y de la sociedad de la información.*

***Art. 13.- De los registros de datos públicos.-*** *Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes.*

***Art. 21.- Cambio de información en registros o bases de datos.-*** *La o el titular de los datos podrá exigir las modificaciones en registros o bases de datos cuando dichas modificaciones no violen una disposición legal, una orden judicial o administrativa. La rectificación o supresión no procederá cuando pudiese causar perjuicios a derechos de terceras o terceros, en cuyo caso será necesaria la correspondiente resolución administrativa o sentencia judicial.*

***Art. 22.- Control Cruzado.-*** *La Dirección Nacional de Registro de Datos Públicos se encargará de organizar un sistema de interconexión cruzado entre los registros público y privado que en la actualidad o en el futuro administren bases de datos públicos, de acuerdo a lo establecido en esta Ley y en su Reglamento.*

***Art. 23.- Sistema Informático.-*** *El sistema informático tiene como objetivo la tecnificación y modernización de los registros, empleando tecnologías de información, bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive, codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados.*

*El sistema informático utilizado para el funcionamiento e interconexión de los registros y entidades, es de propiedad estatal y del mismo se podrán conceder licencias de uso limitadas a*

*las entidades públicas y privadas que correspondan, con las limitaciones previstas en la Ley y el Reglamento.*

***Art. 24.- Interconexión.-*** *Para la debida aplicación del sistema de control cruzado nacional, los registros y bases de datos deberán obligatoriamente interconectarse buscando la simplificación de procesos y el debido control de la información de las instituciones competentes.*

*El sistema de control cruzado implica un conjunto de elementos técnicos e informáticos, integrados e interdependientes, que interactúan y se retroalimentan.*

***Art. 25.- Información física y electrónica.-*** *Para efectos de la sistematización e interconexión del registro de datos y sin perjuicio de la obligación de mantener la información en soporte físico como determinan las diferentes normas de registro, los distintos registros deberán transferir la información a formato digitalizado.*

*La Dirección Nacional de Registro de Datos Públicos definirá el sistema informático para el manejo y administración de registros y bases de datos, el cual regirá en todos los registros del país.*

***Art. 26.- Seguridad.-*** *Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública.*

### 6.1.3 Ley de Comercio electrónico, firmas electrónicas y mensajes de datos

La Ley de Comercio electrónico, firmas electrónicas y mensajes de datos [39], se la reconoce como la principal herramienta jurídica en el país para los diferentes servicios que usan medios electrónicos. Fue procesada en base a los requerimientos de la población el año 2002, debido al incremento de las tecnologías de la información y el manejo de datos personales en sus actividades cotidianas.

Se puede señalar que esta normativa es la Ley que más cercana cubrir las necesidades jurídicas en el caso de servicios de Cloud Computing que se presten en el territorio ecuatoriano, recalcando que para el momento que fue desarrollada esta tecnología no se había considerado, por lo que hay varios puntos que siguen quedándose en el aire.

En la cláusula referida a la confidencialidad, se menciona que se protegerá los datos sin importar la forma, el medio o la intención, lo cual permite que se pueda incluir dentro de este artículo los servicios de Cloud Computing. También es importante en este inciso, la presencia de las sanciones respectivas a quien incumpla lo establecido.

***Art. 5.- Confidencialidad y reserva.-*** *Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a*

*estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia [39].*

Al mencionar la protección de datos, se complementa con lo dispuesto por la Constitución de la República. No se ha proporcionado una explicación detallada de los alcances y en qué sentido se ejerce el derecho de la protección de datos, siendo esta cláusula un referente escaso para el caso de Cloud Computing, puesto que en este entorno se tienen varios escenarios para los cuales se debe garantizar la protección de los datos.

***Art. 9.- Protección de datos.-*** *Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.*

*La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.*

*No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.*

*El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.[39]*

El Artículo 50 relaciona la presente normativa con la Ley de Defensa del Consumidor, para que los usuarios que han contratado algún tipo de servicio, puedan hacer uso de sus derechos y obligaciones. Esto tiene amplia aplicación para los servicios de Cloud Computing, en base a lo revisado al no existir un marco regulador, la principal herramienta jurídica la establece el contrato firmado entre el cliente y el proveedor, que en muchas ocasiones cuando el usuario tiene quejas o inconvenientes con el servicio, no conoce la existencia de esta entidad que lo respalda y lo protege para exigir sus derechos.

***Art. 50.- Información al consumidor.-*** *En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.*

*Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.*

*En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o servicio de que se trate.[39]*

Finalmente en el Artículo 21 del Reglamento General a la Ley de Comercio electrónico, firmas electrónicas y mensajes de datos [40], precisa sobre la Seguridad de la Información en la prestación de servicios electrónicos utilizados para el envío de información personal, exigiendo al proveedor el uso de sistemas seguros en todas las etapas del proceso de la prestación del servicio. Esto puede constituirse como un requisito para el proveedor de Servicios de Cloud Computing.

## 6.2 Comparativa con las Recomendaciones Legales planteadas

Tomando como base los criterios propuestos por las Agencias Europeas antes mencionadas en el estudio legal, se obtuvo una tabla de control, que verifica las áreas que resguardan las actuales leyes ecuatorianas, y que puntos se deberían reestructurar o proponer en una Ley futura. La Tabla 11 y 12 muestra la siguiente información:

| LEY | CODIF. |
|---|---|
| Constitución de la República del Ecuador | A |
| Ley del Sistema Nacional de registro de Datos Públicos | B |
| Ley de comercio electrónico, firmas electrónicas y mensajes de datos | C |

**Tabla 11. Codificación referencial Leyes Ecuatorianas**

| DERECHO NORMADO | LEY |
|---|---|
| Protección de datos | A,C |
| Confidencialidad y no divulgación | B, C |
| Propiedad intelectual | X |
| Limitación de responsabilidades | X |

| | |
|---|---|
| Indemnización | X |
| Garantías y compensaciones | X |
| Cambio de Control | X |

**Tabla 12. Verificación de requisitos.**

De lo observado, sobresale que la protección de datos y la confidencialidad son dos áreas que se encuentran protegidas, la primera por la Constitución de la República y por la Ley de comercio electrónico, y la segunda por la Ley del Sistema Nacional de registro de Datos Públicos, pero al realizar un resumen del resto de necesidades que el Cloud Computing demanda, se verifica que no están cubiertas por ninguna otra reglamentación.

Con lo mostrado se deduce que el Ecuador tiene un vacío jurídico, al no contar con un estatuto específico para estandarizar legalmente los servicios de Cloud Computing, por lo que los servicios ofertados hoy en día, están desarrollándose sin un marco que reglamente este proceso de evolución al Cloud Computing, que está siendo rápidamente acogido por las grandes empresas y las actividades mercantiles del país.

Debido a ello, surge la necesidad de que la Asamblea Nacional Legislativa haga una revisión urgente y proponga alternativas de modificación a las leyes existentes o la creación de una nueva ley basada en referentes y recomendaciones mundiales, con el propósito de que crear una un marco legal robusto y apropiado. Así se tendrá la garantía de que los servicios ofrecidos cuentan con la correspondiente normatividad.

Una de las propuestas más cercanas hacia las necesidades actuales, se presentó el 16 de Marzo de 2010, como Proyecto de ***"Ley de Protección a la Intimidad y a los Datos personales"[41]***, que surge con el objetivo de proteger la información personal que constituye la esfera más íntima de las personas, que en los últimos años ha sufrido un tratamiento deficiente, puesto que se han dado casos en que esta información ha sido adquirida por delincuentes para manipular, controlar o hasta recibir beneficios económicos. Otro de los objetivos de esta propuesta fue frenar la correlación de datos a la que nos hemos visto expuestos, varias empresas han intercambiado información personal de sus usuarios con el fin de expandir mercados, sin la respectiva autorización de los clientes, resultando molesto y perjudicial al darnos cuenta de que la información supuestamente confidencial ha sido fácilmente obtenida.

**Características:**

- Menciona sobre los datos que manejan las instituciones públicas, y que no deberían ser revelados ni expuestos a riesgos. Relaciona las tecnologías de la Información y la Internet como un peligro para develar la información.
- Establece conceptos de los involucrados como el titular de los datos, el Responsable del Tratamiento, el Encargado del Tratamiento y varios otros, muy similar a las legislaciones europeas revisadas.
- Trata las implicaciones de las transferencias internacionales, el tratamiento realizado por terceras partes y la creación de un Órgano de Control y Dirección Nacional.
- Guarda gran similitud con la Ley de Protección de Datos Española.

A pesar de tener buenos planteamientos fue rechazada por la Asamblea Nacional el 7 de Mayo de 2012, luego de una revisión exhaustiva por parte de la Comisión, quienes argumentaron puntos en contra como que la creación del organismo introducirá más burocracia en los procesos, que la existencia del Habeas Data ya da cobertura a varias cláusulas mencionadas y que ya existen leyes que cubren los mismos puntos como la Constitución de la República.

Personalmente, considero que la propuesta contenía argumentos válidos y no repetitivos, que pudieron considerarse para hacer que la "Protección de Datos" sea más específica y no tan general como sucede con las leyes actuales.

En último lugar, se propone que los siguientes principios pueden incluirse en un nuevo marco regulatorio ecuatoriano, que abarque de forma concreta la protección de datos y norme completamente los servicios en la Nube.

a) ***Principio de Aprobación***: Considerar si el tratamiento de datos necesita el consentimiento del titular, responsable de los datos, interesado de los datos, etc.
b) ***Principio de Delimitación de responsabilidades:*** Esclarecer cuáles son las responsabilidades específicas de las partes en un servicio de Cloud Computing.
c) ***Principio de Finalidad:*** Cual será la finalidad determinada para utilizar la plataforma de Cloud Computing, y si debe o no extenderse hacia otra finalidad.
***d) Principio de Seguridad:*** Qué medidas técnicas y organizativas deben adoptarse para el tratamiento de datos en un entorno de Cloud. Si es posible establecerlo como un requisito para los proveedores de la Nube.

e) ***Principio de Transferencias Internacionales:*** Cómo debería realizarse el flujo transfronterizo de los datos personales y los niveles de protección que deben presentar los involucrados. Qué se reconoce por un adecuado nivel de protección.

f) ***Principio de intervención de terceras partes que afecten el tratamiento de los datos:*** Qué requisitos deben cumplir las terceras partes cuando intervengan en un ambiente de Nube. Comunicación al cliente de quienes intervienen en el tratamiento de datos en la Nube.

g) ***Principio de comunicación:*** Comunicación a los clientes acerca de todos los cambios y modificaciones importantes que se den en la plataforma de la Nube, que afecten el servicio, siendo claros y transparentes.

h) ***Principio de indemnizaciones, garantías y sanciones:*** Cómo retribuyen los proveedores de servicios de la Nube al cliente en el caso de provocarle daños irreparables en el tratamiento de los datos.

i) ***Principio de propiedad intelectual:*** Cómo se interpreta la propiedad intelectual de los datos colocados en una infraestructura de Nube. Qué sanciones se colocarían al mal uso o abuso de contenido con derechos de autor.

# 7 Conclusiones y Trabajos Futuros

## 7.1 Conclusiones

- La Computación en la Nube es el nuevo paradigma de las Tecnologías de la Información, que a pesar de sus detractores, cada vez son más las empresas y entes gubernamentales que ha apostado por la adopción de los servicios virtuales. Para que la expansión de esta tecnología se provea de forma adecuada se necesita realizar una capacitación masiva en el sector, propendiendo a que los involucrados comprendan ampliamente los conceptos sobre la Nube, pero también las problemáticas que conlleva. La propuesta es ofrecer Infraestructura, Plataforma y Software como servicios.

- Debido a la importancia del Cloud Computing a nivel mundial, varias organizaciones han encaminado sus esfuerzos en el estudio y análisis de un amplio conjunto de conocimientos como los modelos de servicio, los modelos de despliegue, la arquitectura y todas las tecnologías asociadas a este nuevo estilo de trabajo. En el campo de la Seguridad, existen iniciativas específicas realizando investigación detallada acerca de los riesgos asociados y cómo mitigarlos.

- La principal preocupación desde el punto de vista de los usuarios es la seguridad e integridad de los datos que va a colocarse en la Nube. Los estudios revelan que las empresas se muestran desconfiadas por aspectos como la pérdida de control sobre los datos, el tratamiento que pueda darle el proveedor o la disponibilidad de la plataforma utilizada, que causarían graves inconvenientes en las empresas clientes, poniendo en riesgo sus operaciones, los servicios que presten a sus respectivos usuarios, la imagen y reputación de la empresa y la capacidad del proveedor de Cloud para ofrecer servicios de calidad.

- La virtualización es el instrumento esencial al implementar una solución de Cloud Computing, gracias a ello se puede ofrecer servicios con escalabilidad, rapidez y económicos, lo que no sucede en un sistema tradicional que toma su tiempo en ponerse en marcha el proyecto, la proyección de recursos puede que no haya sido correctamente calculada y que la adquisición del equipamiento represente posiblemente la inversión más grande del proyecto.

- Las compañías proveedoras de servicios de Cloud, pero en mayor grado las empresas clientes deben colocar especial atención a los riesgos, vulnerabilidades y amenazas que están relacionadas a este entorno. La gestión y evaluación del riesgo puede establecerse en una herramienta que identifique cuáles son las áreas afectadas, y si el uso de esta tecnología representa una ventaja o no para el cliente.

- Los principales riesgos para la Seguridad al utilizar servicios en la Nube son: inconvenientes por infraestructuras compartidas al no tener un adecuado aislamiento, APIs o interfaces inseguras que comprometan la gestión del servicio, inadecuada protección de los datos en la Nube, permitiendo que exista fuga o pérdida de la información, amenazas internas por parte de los propios empleados, carencia de normas o estándares para estos servicios, falla del proveedor para responder rápidamente a las incidencias, y varias otros problemas, que pueden resultar peligrosos a la hora de entregar servicios de calidad.

- Si bien es cierto que la Seguridad en Cloud Computing es el campo con mayor énfasis en la investigación, también debe considerarse la importancia de los estudios en otras áreas como la gestión de la identidad, la gestión del control de acceso, la seguridad forense, la virtualización, la computación distribuida, entre otras. En la mayoría de casos la infraestructura va a ser compartida por varias empresas de las cuales se desconoce los fines o intenciones de utilizar la plataforma, por lo que la definición de políticas de control de acceso es vital para mantener a salvo los datos confidenciales.

- Las entidades reguladoras a nivel global como local, deben tomar conciencia de la rapidez con la que está evolucionando esta tecnología con la proliferación de los servicios, y preocuparse de plantear leyes aplicables al Cloud Computing, que permita tener un marco legislativo que dictamine los lineamientos para este modelo de negocio, con condiciones favorables para clientes y proveedores. La Seguridad en la Nube ve como un pilar de apoyo a la legislación asociada, puesto que en el tratamiento de datos se tienen varias implicaciones legales, que son de especial interés por parte de los dueños de la información.

- Debido a la falta de una regulación específica para la Nube, los contratos o acuerdos de Nivel de Servicio representan el principal elemento de cumplimiento, donde deben colocarse todos los requerimientos que el cliente

necesitase, las responsabilidades de cada una de las partes, las medidas de protección, los controles del servicio, las herramientas de gestión, etc. que van a ser usadas para que el tratamiento de los datos tenga un manejo adecuado. Este documento debe ser revisado y analizado cuidadosamente por el cliente, involucrando el área técnica y legal, antes de aceptar los planteamientos provistos por el proveedor. Muchos de estos acuerdos tienen la capacidad de ser negociados, dependiendo del tamaño de la empresa cliente y del tipo de proveedor con el cual se esté contratando los servicios, generalmente las grandes empresas y las entidades gubernamentales tendrán más oportunidades de adaptar los contratos de acuerdo a sus intereses. Recordar también, que este documento es el objeto jurídico con el que el cliente cuenta, bajo el podrá protegerse ante cualquier inconveniente en el ámbito legal.

- La elección del proveedor de servicios de Cloud Computing, debe realizarse de acuerdo a aquel que mejor se adapten hacia los requerimientos de la empresa cliente, recordando siempre en seleccionar aquel proveedor que cuente con modelos o estándares que garanticen el tratamiento de la Seguridad de la Información. Uno de estos estándares puede ser el tener implantando un Sistema de Gestión de Seguridad de la Información con certificación ISO 27001:2005, que muestra que el proveedor sabe cómo resguardar la información, buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma.

- En Ecuador, el Cloud Computing aún es un tema relativamente nuevo, en primer lugar porque son pocos los proveedores que han incursionado en la oferta de estos servicios y luego porque los usuarios tienen un desconocimiento total del funcionamiento de esta tecnología. Para modificar estas condiciones es necesario que los proveedores establezcan estrategias de comercialización, incluyendo una campaña de difusión que dé a conocer los beneficios y oportunidades de utilizar este entorno, y así fomentar el interés de los clientes e implementar soluciones empresariales que puedan colocarlas en un mejor nivel y estar en condiciones de competir a nivel global.

## 7.2 Trabajos Futuros

Las futuras líneas de investigación pueden abarcar las siguientes necesidades:

- Desarrollo de interfaces estandarizadas tanto para datos como para aplicaciones que permitan la interoperabilidad y la portabilidad. La capacidad del cliente está limitada a cambiar de entorno, si las interfaces son propietarias, lo que impide su independencia de modificar la infraestructura en caso de querer reversar el proceso o realizar un cambio de proveedor.

- Desarrollo de estándares de Seguridad para el Cloud Computing, que establezcan un conjunto de políticas, controles y procedimientos que aseguren que los métodos usados garantizan un entorno adecuado para los datos y las aplicaciones en un ambiente virtual. Adicionalmente se podría implantar una certificación específica para Cloud Computing.

- Establecer una entidad de acreditación para las empresas proveedores de servicios de Cloud Computing, para que a través de dicha acreditación los usuarios puedan conocer el nivel y la capacidad de manejar el tratamiento de datos del proveedor.

- Crear herramientas de monitoreo para las aplicaciones de la Nube, que sean compatibles con los sistemas internos de los clientes y que midan el desempeño de las mismas.

# Bibliografía


[1] P. Mell and T. Grance, "The NIST definition of cloud computing." *NIST Special Publication,* vol. 800, pp. 145, 2011.

[2] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing V2.1. 2009Available: https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide.v2.1.pdf.

[3] Wentao Liu, "Research on cloud computing security problem and strategy," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference On,* 2012, pp. 1216-1219.

[4] Anonymous The cloud is the computer - IEEE spectrum. *2013(2/1/2013),* Available: http://spectrum.ieee.org/computing/hardware/the-cloud-is-the-computer.

[5] M. Carroll, A. van der Merwe and P. Kotze, "Secure cloud computing: Benefits, risks and controls," in *Information Security South Africa (ISSA), 2011,* 2011, pp. 1-9.

[6] E. Sepúlveda, O. Salcedo and E. Gómez, "MANEJO DEL RIESGO Y SEGURIDAD EN EL CONSUMO DE SERVICIOS DE TI EN CLOUD COMPUTING," *REDES DE INGENIERIA,* vol. 1, pp. 10-21, 2012.

[7] Anonymous "Motivos para rechazar el Cloud Computing | Raul Lapeira," 2011.

[8] E. K. Clemons and Yuanyuan Chen, "Making the decision to contract for cloud services: Managing the risk of an extreme form of IT outsourcing," in *System Sciences (HICSS), 2011 44th Hawaii International Conference On,* 2011, pp. 1-10.

[9] J. Gibson, R. Rondeau, D. Eveleigh and Q. Tan, "Benefits and challenges of three cloud computing service models," in *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference On,* 2012, pp. 198-205.

[10] Google. Google app engine. *2012(Septiembre 12, 2012),* 2012. Available: https://developers.google.com/appengine/docs/whatisgoogleappengine?hl=es.

[11] F. Sabahi, "Cloud computing security threats and responses," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference On,* 2011, pp. 245-249.

[12] Anonymous SAS 70 service organization auditing standards. *2013(2/1/2013),* Available: http://sas70.com/.

[13] CICA. Trust services - principles and criteria, and illustrations. *2012(Septiembre 15),* 2012. Available: http://www.webtrust.org/item64428.aspx.

[14] Anonymous ISO 27000 - ISO 27001 and ISO 27002 standards. *2013(2/1/2013),* Available: http://www.27000.org/.

[15] Anonymous Cloud computing information assurance framework — ENISA. *2013(2/1/2013),* Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

[16] Cloud Security Alliance. Top threats to cloud computing V1.0. 2010Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[17] N. Hachem, Y. Ben Mustapha, G. G. Granadillo and H. Debar, "Botnets: Lifecycle and taxonomy," in *Network and Information Systems Security (SAR-SSI), 2011 Conference On,* 2011, pp. 1-8.

[18] J. Chen, X. Wu, S. Zhang, W. Zhang and Y. Niu, "A decentralized approach for implementing identity management in cloud computing," in *Cloud and Green Computing (CGC), 2012 Second International Conference On,* 2012, pp. 770-776.

[19] J. Liou and S. Bhashyam, "A feasible and cost effective two-factor authentication for online transactions," in *Software Engineering and Data Mining (SEDM), 2010 2nd International Conference On,* 2010, pp. 47-51.

[20] D. Mohamed, "Discovery of electronically stored information (ESI) or e-discovery: The law and practice in malaysia and other jurisdictions," in *Information Society (i-Society), 2012 International Conference On,* 2012, pp. 461-465.

[21] F. M. Heikkila, "E-Discovery: Identifying and Mitigating Security Risks during Litigation," *IT Professional,* vol. 10, pp. 20-25, 2008.

[22] Honggang Zhang, B. DeCleene, J. Kurose and D. Towsley, "Bootstrapping deny-by-default access control for mobile ad-hoc networks," in *Military Communications Conference, 2008. MILCOM 2008. IEEE,* 2008, pp. 1-7.

[23] A. Madani, S. Rezayi and H. Gharaee, "Log management comprehensive architecture in security operation center (SOC)," in *Computational Aspects of Social Networks (CASoN), 2011 International Conference On,* 2011, pp. 284-289.

[24] Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data, P1619.3, IEEE. Febrero 28, 2007). *P1619.3* Available: http://standards.ieee.org/about/sasb/nescom/projects/1619-3.pdf, 2007.

[25] Anonymous OpenID foundation website. *2013(2/1/2013),* Available: http://openid.net/.

[26] Anonymous OATH - initiative for open authentication | all users, all devices, all networks. *2013(2/1/2013),* Available: http://www.openauthentication.org/.

[27] A. Volokyta, I. Kokhanevych and D. Ivanov, "Secure virtualization in cloud computing," in *Modern Problems of Radio Engineering Telecommunications and Computer Science (TCSET), 2012 International Conference On,* 2012, pp. 395-395.

[28] ENISA. Beneficios, riesgos y recomendaciones para la seguridad de la información. Unión Europea. 2009Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish.

[29] Anonymous ISO27000.es - el portal de ISO 27001 en español. gestión de seguridad de la información. *2013(2/10/2013),* Available: http://www.iso27000.es/glosario.html.

[30] Anonymous ISO/IEC 27005:2008 - information technology -- security techniques -- information security risk management. *2013(2/10/2013),* Available: http://www.iso.org/iso/catalogue_detail?csnumber=42107.

[31] W. Jansen and T. Grance. Guidelines on security and privacy in public cloud computing. *NIST Special Publication* pp. 800-144. 2011.

[32] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato and A. Kanai, "Risk management on the security problem in cloud computing," in *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference On*, 2011, pp. 147-152.

[33] Cloud Security Alliance. Cloud compliance report. España. 2011Available: https://cloudsecurityalliance.org/csa-news/csa-issues-first-cloud-compliance-report-for-spain/.

[34] Parlamento Europeo y Consejo de la Unión Europea. Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995<br />relativa a la protección de las personas físicas en lo que respecta al tratamiento<br />de datos personales y a la libre circulación de estos datos. 1995. Available: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf.

[35] Jefatura del Estado de España. LEY ORGÁNICA 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *BOE núm. 298*1999. Available: http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf.

[36] Ministerio de Justicia de España. Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *BOE-A-2008-979*2008. Available: http://www.boe.es/buscar/doc.php?id=BOE-A-2008-979.

[37] Asamblea Constituyente del Ecuador. Constitución de la república del ecuador. 2008. Available: http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf.

[38] Asamblea Nacional del Ecuador. Ley del sistema nacional de registro de datos públicos<br />. 2010. Available: http://www.regprocue.gob.ec/wp-content/uploads/2012/03/ley-del-sistema-nacional-de-registro-de-datos-publicos.pdf.

[39] Congreso Nacional del Ecuador. Ley de comercio electrónico, firmas electrónicas y mensajes de datos. *Registro Oficial 557-S*2002.

[40] Presidencia de la República del Ecuador. Reglamento general a la ley de comercio electrónico, firmas electrónicas y mensajes de datos. 2002. Available: http://www.conatel.gob.ec/site_conatel/?option=com_content&view=article&catid=335:todos&id=99:-reglamento-a-la-ley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos.

[41] Asamblea Nacional del Ecuador. Proyecto a laLey de protección a la intimidad y a los datos personales. *2010-023*2010. Available: http://www.asambleanacional.gov.ec/tramite-de-las-leyes.html.