



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES**

**TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES**

AUTOR:

YESSENIA RELICA RELICA

**TEMA: “ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE
CALIDAD EN SERVICIOS CLOUD COMPUTING EN EL
ECUADOR”**

DIECTOR: ING. DARWIN AGUILAR

CODIRECTOR: ING. RODRIGO SILVA

SANGOLQUÍ 2014

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: *ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE CALIDAD EN SERVICIOS CLOUD COMPUTING EN EL ECUADOR*, ha sido desarrollado en su totalidad por la señorita *YESSENIA PAULINA RELICA RELICA*, bajo nuestra dirección.

Atentamente

Ing. Darwin Aguilar

DIRECTOR

Ing. Rodrigo Silva

CODIRECTOR

AUTORIA DE RESPONSABILIDAD

YESSENIA PAULINA RELICA RELICA

DECLARO QUE:

El proyecto denominado “ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE CALIDAD EN SERVICIOS *CLOUDCOMPUTING* EN EL ECUADOR”, ha sido desarrollado en base a una investigación exhaustiva, respetando los derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, 27 Febrero 2014

Yessenia Paulina Relica Relica

AUTORIZACIÓN

YESSENIA PAULINA RELICA RELICA

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo “ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE CALIDAD EN SERVICIOS *CLOUD COMPUTING* EN EL ECUADOR”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 27 Febrero 2014

Yessenia Paulina Relica Relica

DEDICATORIA

A mi madre porque es la persona más importante que tengo en la vida, mi inspiración, pues gracias a ti soy la profesional que siempre soñé ser, tú me enseñaste que tengo que ser responsable pues como no agradecer por tus abrazos por cuidarme cuando me enfermado, por enseñarme que la vida está llena de sacrificios y pues el nuestro ha valido la pena, por ser mi amiga, apoyo, por enseñarme el valor de tener una familia unida, pues mi logro va dedicado a ti mi gran amor mío mi madre.

A mis tíos, tías, primos y primas, pues como no dedicarles mí esfuerzo ya que de una u otra forma me han ayudado, brindándome su apoyo incondicional, pues me siento realmente feliz de tener la mejor familia, unida que jamás me dejaron sola.

Finalmente mamita me siento feliz de decirte que me siento privilegiada de tenerte a mi lado y que esto es el comienzo de un futuro muy prospero para las dos siempre juntas mamita eres la mejor te amo con toda mi vida.

AGRADECIMIENTO

Agradezco a Dios por ser mi guía, maestro, mi mayor inspiración para luchar por mis sueños y así conseguir que se hagan realidad con esfuerzo y dedicación, pues aprendí que debo ser fuerte y nunca rendirme, me has enseñado que las cosas hechas con amor son más llevaderas, a ti Virgencita del Cisne madre mía gracia también por cada una de tus enseñanzas de tu ternura, pues mi corazón late de emoción por lograr mi gran sueño y todo te lo debo a ti Dios Te Amo con todo mi Corazón.

Como no agradecer a la mujer que me dio la vida mi Madre, eres la persona quien debo todo lo que soy hoy en día, tu esfuerzo, ejemplo, apoyo, amor, ternura, comprensión, gracias mami por creer en mi por dejarme volar sola como alguna vez me lo dijiste, porque cada vez que te he necesitado has estado ahí, aunque la distancia nos ha separado ya sea para llorar como para reír siempre estabas conmigo, como no agradecer a Dios por la madre que me regalo, no pudo darme mejor regalo que tu mami, pues tu trabajo nos ha llevado a ser lo que hoy en día somos ingenieras nuestro sueño cumplido, mami sin más que decirte TE AMO, eres mi vida mi todo felicidades para ti porque, tú esfuerzo se ve reflejado el día de hoy.

A mis tías como no agradecerles su apoyo, cariño, atención, gracias a mi Ayanara por las llamadas, por consentirme más que a ti mismo a pesar de la distancia, por el cariño que me regalas con cada palabra, por los momentos de llanto telefónicos gracias por ser más que mi tía mi hermana. Anabela a ti también te agradezco por tu atención por cuidarme cada día por tratarme como tu hija, por acogerme en tu casa a mi tía María a quien a pesar de que se encuentre lejos siempre estuvo pendiente de

mi pues como no agradecerle por el apoyo que me brindo, y pues el hecho que hayan creído en mi es más que suficiente las quiero montones. A mi tío Jhoffre, Pao gracias por su apoyo y estar pendientes de mí, a ti Wilson gracias por todo por ser mi amigo, cariño, comprensión, por consentirme como lo haces por las llamadas y por tu apoyo eres una de las personas que quiero muchísimo.

A mi Cami, Fer y Javi gracias pequeños por su apoyo también su cariño y a mi hermosa Maite pues los quiero mucho este esfuerzo también va por ustedes gracias por confiar en que lo podía lograr gracias.

A mis gordas Ale y July como no agradecerles cada momento de risa de llantos, por las amanecidas constantes por ser como mis hermanas, me ayudaron en cada momento y circunstancia desde que las conocí las cosas fueron diferentes entendí que puedo tener las mejores amigas porque a pesar de las peleas seguimos siendo las grandes amigas las quiero mucho mis locas.

En fin quiero gradecer a cada una de las personas que me brindaron su apoyo y me guardan aprecio pues sé que a mí alrededor tengo grandes amigos que de una u otra manera me enseñaron a vivir la vida pues de cada tropiezo, uno aprende a sobrellevar las dificultades que se presentan. Y gracias por estar presente en mi vida pues sé que llegaron en el momento preciso.

A mis queridos Ingenieros orientadores de tesis, Ing. Darwin Aguilar e Ing. Rodrigo Silva, porque me brindaron la confianza para poder llevar a cabo mi tema de tesis y culminar con éxito mi tesis. Para ustedes mi más sincero agradecimiento y aprecio.

INDICE DE CONTENIDOS

GLOSARIO.....	xiii
CAPÍTULO I	1
ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE CALIDAD EN SERVICIOS CLOUD	
COMPUTING EN EL ECUADOR	1
1.1 ANTECEDENTES.....	1
1.2 JUSTIFICACIÓN E IMPORTANCIA.....	2
1.3 OBJETIVOS.....	4
1.4 ALCANCE DEL PROYECTO.....	5
CAPÍTULO II	7
MARCO TEÓRICO	7
2.1. CLOUD COMPUTING.....	7
2.1.1 CARACTERÍSTICAS DE CLOUD COMPUTING	10
2.1.2 VENTAJAS Y DESVENTAJAS.....	11
2.1.3 TIPOS DE INFRAESTRUCTURA.....	13
2.2. MODELOS DE IMPLEMENTACIÓN DE CLOUD COMPUTING.....	14
2.2.1. NUBE PÚBLICA	16
2.2.2. NUBE PRIVADA.....	18
2.2.3. NUBE HÍBRIDA.....	19
2.3. LOS NIVELES DE SERVICIO DE CLOUD COMPUTING	20
2.4. ESTADO DEL ARTE	23
2.4.1. DETALLE DE LOS SERVICIOS IaaS,PaaS,SaaS.....	23

2.5. MOVILIDAD	33
CAPÍTULO III	35
ESTÁNDARES DE CALIDAD	35
3.1. NORMAS DE SEGURIDAD DE INFORMACIÓN ISO/ICE27001	35
3.1.1 VENTAJAS	36
3.2 SEGURIDAD DEL <i>CLOUD COMPUTING</i>	38
3.2.1 RIESGOS DEL <i>CLOUD COMPUTING</i>	39
3.2.2 PRINCIPIOS PARA LA PROTECCIÓN DE LA NUBE	44
CAPÍTULO IV	48
SERVICIO <i>CLOUD COMPUTING</i> EN EMPRESA LOCAL TELCONET	48
4.1. DATA CENTER O SERVIDORES VIRTUALES (NUBE)	48
4.2. INVERSIÓN DE TELCONET EN EL <i>CLOUD COMPUTING</i>	49
4.3. UBICACIÓN ESTRATÉGICA	51
4.4. NIVELES DE SERVICIO DE DATA CENTER	52
4.5. RESUMEN DE CARACTERÍSTICAS DE LOS TIER	52
FUENTE (TELCONET, 2013)	54
4.6. RESUMEN DE CARACTERÍSTICAS DE SEGURIDAD DE LA NUBE	55
4.7. NORMA TIA-942	60
4.8. DISPONIBILIDAD	61
CAPITULO V	65
PARÁMETROS DE CALIDAD EN SERVICIOS <i>CLOUD COMPUTING</i>	65

5.1	VIRTUALIZACIÓN	65
5.2	ESCALABILIDAD	66
5.3	INFRAESTRUCTURA COMO SERVICIO	67
5.4.	PARAMETROS TECNICOS	67
5.4.1.	NIVEL DE SERVICIO IAAS	67
5.4.2.	NIVEL DE SERVICIO PAAS.....	69
5.4.3.	NIVEL DE SERVICIO SAAS.....	70
5.4.4.	CARACTERÍSTICAS GENERALES.....	71
5.5.	PARÁMETROS ECONÓMICOS	80
5.5.1.	NIVEL DE SERVICIO IASS	80
5.5.2.	NIVEL DE SERVICIO PAAS	81
5.5.3.	NIVEL DE SERVICIO SAAS.....	81
5.6.	PARAMETROS LEGALES	82
5.6.1.	NIVEL DE SERVICIO IASS.....	82
5.6.2.	NIVEL DE SERVICIO PAAS.....	82
5.6.3.	NIVEL DE SERVICIO SAAS.....	83
5.6.4.	CARACTERÍSTICAS GENERALES.....	83
CONCLUSIONES Y RECOMENDACIONES		89
REFERENCIAS BIBLIOGRAFÍA		91

TABLA DE FIGURAS

<i>FIG. 2.1.1. Cloud Computing</i>	7
<i>FIG. 2.2.1. Modelo de Implementación</i>	14
<i>FIG. 2.2.2. Nube Pública</i>	16
<i>FIG. 2.2.3. Nube Privada</i>	18
<i>FIG. 2.2.4. Nube Híbrida</i>	19
<i>FIG. 2.3.1. Niveles de Servicio</i>	21
<i>FIG. 2.4.1.1. Servicio IaaS</i>	23
<i>FIG. 2.4.2.3 Servicio PaaS</i>	26
<i>FIG. 2.4.3.5. Servicio SaaS [6]</i>	29
<i>FIG. 2.5.1. Movilidad del Cloud Computing</i>	33
<i>FIG. 3.2.1. Seguridad de la Nube</i>	38
<i>FIG. 4.1.1. Distribución del Data Center</i>	49
<i>FIG. 4.4.1. Niveles Estratégicos</i>	52
<i>FIG. 4.8.1. Disponibilidad</i>	61

INDICE DE TABLAS

<i>Tabla 1. Resumen de Modelos de Implementación.....</i>	<i>15</i>
<i>Tabla 2. Mecanismo de Seguridad.....</i>	<i>46</i>
<i>Tabla 3. Características de los Tier.....</i>	<i>52</i>
<i>Tabla 4. Arquitectura de los Tier [9].....</i>	<i>53</i>
<i>Tabla 5. Energía los Tier [9].....</i>	<i>53</i>
<i>Tabla 6. Ambiente de los Tier [9].....</i>	<i>54</i>
<i>Tabla 7. Resumen de Características de Seguridad de los Tier.....</i>	<i>55</i>
<i>Tabla 8. Tipos de Conectividad y Servicios.....</i>	<i>57</i>
<i>Tabla 9. Soporte de Servicio [10].....</i>	<i>62</i>
<i>Tabla 10. Entrega de Servicio [10].....</i>	<i>63</i>

GLOSARIO

- SLA** Un acuerdo de nivel de servicio o Service Level Agreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.
- PDA** Un ordenador de bolsillo, organizador personal o una agenda electrónica de bolsillo, (PDA) (asistente digital personal), es una computadora de mano originalmente diseñada como agenda electrónica
- APIs** Es una interfaz de programación de aplicaciones (IPA) o API (del inglés Application Programming Interface) es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas.
- CPD** Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización

- LSA** (Light Summary Algorithm), Algoritmo Ligero de Resumen es un algoritmo de reducción criptográfico de 64 bits.
- ERP** Un sistema de planificación de recursos empresariales, por sus siglas en inglés (Enterprise Resource Planning), sistemas informáticos destinados a la administración de recursos en una organización.
- CRM** es un modelo de gestión de toda la organización, basada en la orientación al cliente (u orientación al mercado según otros autores), el concepto más cercano es marketing relacional.
- CAPEX** Inversiones en bienes de capitales, son inversiones de capital que crean beneficios. Un CAPEX se ejecuta cuando un negocio invierte en la compra de un activo fijo o para añadir valor a un activo existente con una vida útil que se extiende más allá del año imponible.
- HTML5** Es la quinta revisión importante del lenguaje básico de la World Wide Web, HTML. HTML5 especifica dos variantes de sintaxis para HTML: un «clásico» HTML, la variante conocida como HTML5 y una variante XHTML conocida como sintaxis XHTML5 que deberá ser servida como XML
- SGSI** Un Sistema de Gestión de la seguridad de la Información es, como el nombre lo sugiere, un conjunto de políticas de administración de la

información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza

- SPAM** Correo basura, mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, enviados en grandes cantidades (masivas) que perjudican de alguna o varias maneras al receptor.
- VPN** Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada
- TCO** Es el costo total de propiedad, es un método de cálculo diseñado para ayudar a los usuarios y a los gestores empresariales a determinar los costos directos e indirectos, así como los beneficios, relacionados con la compra de equipos o programas informáticos
- ITSM** Es una práctica basada en el proceso destinado a alinear la entrega de tecnología de la información (TI) con las necesidades de la empresa, haciendo hincapié en los beneficios para los clientes. ITSM implica un cambio de paradigma de la gestión de las TI como pilas de componentes individuales para centrarse en la prestación de servicios de extremo a extremo utilizando las mejores modelos de procesos de la práctica

DDoS Conocido como Ataque de denegación de servicios. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios

MALWARE También llamado badware, código maligno, o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

PHISHING Es un término informático que denomina un tipo de delito dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso

RESUMEN

En el presente trabajo se pretende determinar los parámetros de calidad óptimos, que deben ser considerados para la prestación eficiente de los servicios Cloud Computing, en el cual se vean los beneficios tanto para el usuario como para proveedor. La virtualización, escalabilidad e infraestructura son unas de las principales características, para la determinación de los parámetros de calidad según el acuerdo que se dé entre el cliente y el proveedor brindando la información suficiente sin olvidar que hay que tener presente la norma ISO/CEI 27001, en la que hace referencia en proteger los activos de información y ofrecer confianza a los clientes y así conseguir que dicho servicio sea de buena calidad. Presentaremos recomendaciones de cómo realizar la contratación del mismo, ya que en la actualidad no existe en el Ecuador normativa vigente que regule la prestación de este tipo de servicios por lo que las cláusulas deben ser claras y concisas.

PALABRAS CLAVES

SEGURIDAD

NORMAS ISO/CEI 27001

EFICIENCIA

VIRTUALIZACIÓN

CALIDAD DE LA INFORMACIÓN

ABSTRACT

In the present paper is to determine the optimal parameters of quality to be considered for the efficient delivery of cloud computing services, which benefits both the user and provider to see. Virtualization, scalability and infrastructure are some of the main features for the determination of quality parameters according to the agreement between the clients and give the supplier providing enough information without forgetting that we must remember the ISO / IEC 27001, which refers to protect information assets and give confidence to customers and thus get that service is of good quality. Present recommendations on how to make the hiring thereof, as at present does not exist in Ecuador existing rules governing the provision of such services so that the clauses must be clear and concise

KEYWORDS

SECURITY

ISO / IEC 27001 STANDARDS

EFFICIENCY

VIRTUALIZATION

QUALITY OF INFORMATION

CAPÍTULO I

ANÁLISIS Y EVALUACIÓN DE PARÁMETROS DE CALIDAD EN SERVICIOS CLOUD COMPUTING EN EL ECUADOR

1.1 ANTECEDENTES

Cloud Computing (Computación en la nube) no es un concepto muy novedoso, Sin embargo, las empresas más conocidas en el campo de las Tecnologías de la Información ofrecen a corto plazo servicios de *Cloud Computing* a un rango de clientes desde organizaciones de todos los tamaños e incluso a individuos en forma independiente.

Los más grandes y más conocidos proveedores de *Cloud Computing* como son *Amazon con EC2, Microsoft con Azure* y *Google con Google Apps* (p.ej. *Gmail, Google Docs, Google Calendar*). El *Cloud Computing* es una plataforma tecnológica que le permite acceder de manera rápida y segura al *software* y el *hardware* que su empresa requiere, sin la preocupación de tener que gestionar su actualización y mantenimiento. Los usuarios de este servicio tienen acceso de forma gratuita o de pago, todo depende del servicio que el usuario requiera.

Los servicios de *Cloud Computing* han empezado a tener gran impacto en las empresas en el Ecuador. Proveedores de servicios de tecnologías de la información como IBM, Level 3, Telconet, CNT, *New Access*, etc. están ofreciendo servicios de basados en la nube.

Los modelos más utilizados actualmente son los de Infraestructura en las cuales se ofrece arrendamiento de equipos, espacios, servicios y aplicaciones de valor agregado. Si bien, las mencionadas empresas presienten que existe un gran mercado potencial en el Ecuador, en base a las experiencias del mercado global, este mercado no ha sido analizado bajo parámetros de niveles de calidad que deben cumplirse en *Cloud Computing* ni el tipo de normas por las cuales se debe regir dicho servicio en nuestro país.

1.2 JUSTIFICACIÓN E IMPORTANCIA

El *Cloud Computing* es una tendencia que cada vez va ganando más fuerza entre las empresas que prestan servicios a través de la web y usuarios que acceden a ellos a través de Internet.

El aumento en el uso de la computación en la nube se debe entre otras a que no hay necesidad de conocer la infraestructura detrás de ésta, ya que pasa a ser una nube donde las aplicaciones y servicios pueden fácilmente crecer (escalable), funcionar rápido y casi nunca falla.

Adicionalmente que las empresas se centralizan en el objetivo propio de su negocio, a más de no incurrir en gastos de equipamiento en infraestructura que luego de poco tiempo (5 años aproximadamente) dejan de prestar servicios de tecnología acorde con los requerido por la empresa.

El *Cloud Computing* se constituye, cada vez más, como tierra de oportunidades para empresas de diversas industrias. Es claro que estamos migrando de la era de la PC (toda la información almacenada y disponible en un solo lugar) a la era del *Cloud* (información que se mueve y a la que se accede desde cualquier lugar y dispositivo); y en el proceso que este cambio requiere.

A medida que se van disipando las dudas y temores, muchos proveedores de TI comienzan a ver las ventajas de la nube no sólo para los negocios sino para los consumidores.

La virtualización de escritorios permite obtener beneficios relacionados al control de los costos, a una mejor experiencia del usuario, mejor performance, movilidad y calidad de vida para los empleados. El *Cloud Computing* permite tener un retorno de inversión más que favorable en un tiempo no mayor a 3 años.

Gran importancia tiene la descripción del objeto y causas del contrato SLA (*Service Level Agreement*) como preámbulo de los derechos y obligaciones suscrito entre Proveedor-Cliente que inicia la prestación del servicio, sin embargo en el país no existen normativas, ni normas jurídicas para sustentar el compromiso suscrito.

Al mismo tiempo, una buena descripción detallada del servicio, permite una correcta calificación del contrato que constituye una labor insertada dentro de la interpretación del mismo y mostrar el fin jurídico que los contratantes pretenden alcanzar. Por la naturaleza propia del modelo *Cloud Computing*, es fundamental a los efectos de estricta seguridad jurídica, aquí mostramos algunos de los puntos que se deben tomar en cuenta.

- Ubicación del prestador del servicio.
- Localización de los servicios.
- Emplazamiento de las infraestructuras donde vayan a estar desplegadas las máquinas y plataformas.
- Tipo de servicios contratados.
- Capacidad de respaldo de información
- Costos por la prestación de servicios
- Plataforma ofertada
- Infraestructura
- Tiempo de respuesta ante fallos

1.3 OBJETIVOS

OBJETIVO GENERAL

- Analizar y evaluar los parámetros de calidad que deben considerarse en las empresas que prestan servicios de *Cloud Computing* con el estudio, ciudad de Quito.

OBJETIVOS ESPECÍFICOS

- Analizar la arquitectura de una red *Cloud Computing* dentro de las empresas locales.
- Analizar las normativas y regulaciones existentes en Ecuador y a nivel internacional para la prestación de servicio de *Cloud Computing*. Por medio de las normas de seguridad de información ISO/CEI 27001.
- Investigar los servicios *Cloud Computing* prestados para empresas locales.
- Evaluar los parámetros de calidad que existen en Telconet para brindar el servicio de *Cloud Computing*.
- Determinar los parámetros de calidad óptimos, que deben ser considerados para la prestación eficiente de los servicios *Cloud Computing* en Ecuador.

1.4 ALCANCE DEL PROYECTO

El alcance del presente proyecto se orienta a realizar una revisión de las arquitecturas del *Cloud Computing* desarrolladas durante un periodo de cinco años atrás para determinar las ventajas y desventajas existentes, así como la disponibilidad, escalabilidad y normas de seguridad de información ISO 27001.

Procederemos a la investigación de servicios que son prestados a empresas locales, como parte de este estudio tenemos como auspiciante la empresa TELCONET, la cual actualmente se encuentra brindando el servicio de *Cloud Computing* y aportando con datos reales podremos realizar un extenso análisis de los parámetros de calidad, flexibilidad, seguridad, arquitectura con la que se realiza este servicio. En este contexto el rol de TELCONET será importante para lograr una adopción mucho más masiva de la nube y para encontrarle nuevos usos de la mano de las necesidades de los usuarios., diversificar su oferta y adoptar nuevos modelos de negocio.

A partir del estudio realizado determinar los parámetros de calidad óptimos, que deben ser considerados para la prestación eficiente de los servicios Cloud Computing, en el cual se vean los beneficios tanto para el usuario como para proveedor de dicho servicio, ya que el usuario está constantemente en la búsqueda de formas más efectivas de almacenar su información y el acceder a sus datos desde cualquier lugar y dispositivo.

CAPÍTULO II

MARCO TEÓRICO

2.1. CLOUD COMPUTING

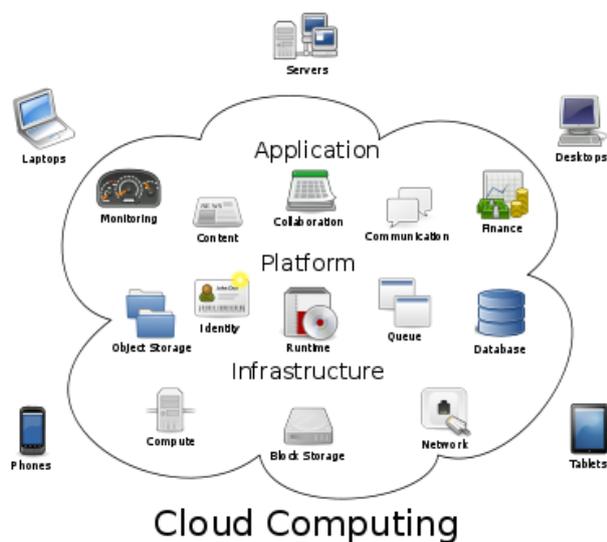


FIG. 2.1.1. Cloud Computing

FUENTE (Gomez, 2011)

Cloud Computing es conocida como una nueva tecnología que permite ofrecer servicios de computación a través de Internet, es decir, servicios que sean solicitados

por usuarios como almacenamiento, correo, aplicaciones, etc, que estén disponibles en la nube de internet. (Gomez, 2011)

Permite una mayor agilidad y eficiencia de costos en la gestión de la información digital de cualquier organización o empresa, a través de una implantación sencilla y flexible. Esencialmente, la computación en nube consiste en la gestión y suministro de aplicaciones, información y datos como un servicio. Estos servicios se proporcionan a través de la nube, ya que es un modelo basado en el consumo del servicio sin que el cliente compre la infraestructura para mantener el servicio.

Así, *Cloud Computing* proporciona de forma eficiente el acceso a servicios informáticos, independientemente de los sistemas físicos que utilizan o de su ubicación real, siempre y cuando se disponga de acceso a Internet.

Pues la información ya no tendrá que almacenarse necesariamente en los dispositivos informáticos de la empresa, sino en los sistemas proporcionados por el proveedor que brinda el servicio. Además, el *Cloud Computing* hace que no sea necesario instalar aplicaciones informáticas en los sistemas de la organización, sino que éstas se ejecutarán en la nube a través de Internet. Esto permite liberar varios recursos, de la empresa. (Cerde, 2012)

Pues la nueva propuesta a disposición de los clientes como es la infraestructura tecnológica a través de Internet, de modo que recursos informáticos dispuestos en red sean compartidos por varios usuarios y a través de distintos dispositivos, pudiendo trabajar conjuntamente sobre el mismo contenido.

Como ya hemos comentado, la implantación de *Cloud Computing* en la actualidad se ha extendido de manera considerable, en gran medida a la expansión de Internet. Uno de los ejemplos más claros es el uso y difusión del correo electrónico en Internet, el cual además le ofrece la posibilidad de enviar y recibir información a través de la red mediante un conjunto de funcionalidades.

Existen otros ejemplos de *Cloud* con los que muchos usuarios están ya familiarizados y que ofrecen una gran cantidad de servicios, tales como la plataforma de *Google Apps*, *Zoho*, *Peepel* y *Opengoo*, los cuales integran herramientas de procesamiento de textos, calendarios, aplicaciones de intercambio de fotos o herramientas de creación de sitios *Web*. Todas las herramientas mencionadas son de acceso gratuito, tanto de propiedad privada como pagadas y para uso profesional. (Daniele.catteddu, 2009)

El Cloud Computing permite ofrecer de manera conveniente, recursos y servicios altamente disponibles. Permite a los usuarios acceder a unas amplias herramientas de servicios, respondiendo a las necesidades del negocio de forma flexible y permitiendo adaptarse a las demandas de los usuarios en el tiempo.

Su principal característica es el uso de recursos compartidos y la independencia de la infraestructura, lo cual permite al usuario disponer siempre de los mismos servicios independientemente donde este se encuentre ubicado.

2.1.1 CARACTERÍSTICAS DE CLOUD COMPUTING

Presentamos a continuación algunas características esenciales del Cloud Computing y de las cuales nos vemos beneficiados los usuarios para recibir un buen servicio.

- **AUTO-SERVICIO BAJO DEMANDA**

El consumidor podrá aprovisionar recursos computacionales en forma unilateral, según lo requiera, y sin requerimiento de interacción humana con el proveedor del servicio.

- **ACCESO DESDE LA RED (PÚBLICA, PRIVADA, HÍBRIDA, COMUNITARIA)**

Todos los recursos que ofrece la nube están disponibles en la red, y el consumidor no sólo puede acceder a ellos de una sola manera, sino que también mediante plataformas como teléfonos móviles, laptops, PDAs, etc.

- **RECURSOS SEGÚN CARACTERÍSTICAS DE SERVICIO**

Los recursos del proveedor estarán agrupados para servir a múltiples consumidores, utilizando un modelo que le permita una confiable seguridad una vez asignados. Estos recursos pueden ser físicos o virtuales y deben tener todos componentes necesarios para brindar un servicio completo, entendiéndose que éste

podrá incluir recursos de almacenamiento, conectividad, procesamiento, elementos de *software*, políticas, métricas, etc. conservando las pautas de seguridad.

- **CAPACIDAD DE RÁPIDO CRECIMIENTO**

Las unidades de capacidad pueden ser rápidas y fácilmente aprovisionadas en algunos casos en forma automática. Para el consumidor, estos recursos suelen parecer ilimitados, y pueden ser adquiridos en cualquier cantidad y momento.

- **SERVICIO MEDIDO**

Los sistemas de la nube controlan de forma automática y optimizada la utilización de los recursos. Este uso de los recursos puede ser monitoreado y controlado, además, es posible realizar reportes para ambas partes, a fin de establecer la facturación del servicio. (Leon, 2010)

2.1.2 VENTAJAS Y DESVENTAJAS

Pues al ser una tecnología que ofrece flexibilidad, reducción de costos y una eficiencia presentamos a continuación algunas ventajas

- Reducción de Costos considerando que los proveedores de *Cloud Computing* utilizan infraestructuras altamente eficiente y con alto índice de utilización, reduciendo el costo de operación y mantención de la infraestructura, entre todos los clientes a los que se presta el servicio.

- La Infraestructura facilita las labores de dimensionamiento, eliminando la complejidad de calcular las proyecciones de crecimiento del negocio, permitiendo un escalamiento de la plataforma *on-demand*, según las necesidades del negocio.
- Mayor eficiencia en el uso de utilizar sistemas que se encarguen de monitorear el uso de los recursos y administrarlos de manera eficiente.
- Pues cada cliente paga por lo que está realmente utilizando, y no por toda una infraestructura que con el pasar del tiempo se vuelve obsoleta y es un gasto innecesario para la empresa, pues se nos da la facilidad de arrendar un espacio en el Datacenter.
- Calidad de Servicio permite contar con niveles de servicio (SLA) con mayores tiempos de disponibilidad. Es posible contar con diferentes niveles de servicio dependiendo del cliente y su negocio.
- Automatiza la gestión de la infraestructura mediante *scripts* u otras soluciones, permitiendo desplegar nuevas aplicaciones, o gestionar recursos de manera automática apalancando las APIs incluidas en la infraestructura.
- La escalabilidad sea en forma automática o en forma manual, es posible escalar en forma dinámica y *on-demand*. Adicional es posible realizar escalamiento de recursos de forma proactiva para atender aumentos de la

demanda a través de predicciones basadas en patrones históricos de uso de los servicios.

- La movilidad tiene una independencia del dispositivo y la ubicación, lo que permite que los usuarios puedan acceder a los sistemas usando un navegador de Internet independiente de su ubicación geográfica y del sistema operativo o computador.
- La disponibilidad, la infraestructura y arquitectura de un Data Center diseñado como una Cloud, nos brinda una alta redundancia para asegurar la Continuidad Operacional y del Negocio. Además, es posible usar la amplia distribución geográfica de un proveedor de *Cloud Computing*.

2.1.3 TIPOS DE INFRAESTRUCTURA

La infraestructura de la nube está compuesta de un conjunto de elementos y recursos que proporcionan servicios que los usuarios pueden usar según sus necesidades, esta infraestructura se la puede categorizar en modelos de despliegue que describen el tipo de servicio que se está brindando, es decir cómo se crea y se la pone en funcionamiento y en modelos de servicios que puede proporcionar la nube, como *software*, plataforma o infraestructura. (Hogan, Liu, Sokol, & Tong, 2011)

2.2.MODELOS DE IMPLEMENTACIÓN DE *CLOUD COMPUTING*



FIG. 2.2.1. Modelo de Implementación

FUENTE (Gomez, 2011)

Existen varios modelos de implantación de sistemas que hacen uso del *Cloud Computing*, los cuales se dividen en sistemas basados en nubes públicas, privadas o híbridas, cada uno con sus ventajas e inconvenientes.

Se ha de elegir el modelo más adecuado para resolver el inconveniente presentado. Por ejemplo, el modelo más recomendable para el despliegue de una aplicación que se utilizará de manera temporal o provisional, probablemente sería en nubes públicas, ya que evita la necesidad de instalar equipos adicionales para su uso.

Del mismo modo, la implantación definitiva de esa misma aplicación podría requerir un despliegue en nubes privadas o híbridas si se deben garantizar ciertos requisitos de calidad de servicio o de localización de los datos gestionados.

Tabla 1. Resumen de Modelos de Implementación

NUBES	UTILIZACIÓN	CARACTERÍSTICAS
Nube pública	Despliegue de una aplicación de forma provisional. Adecuado cuando a la empresa no le importa compartir espacio con otros usuarios de la nube.	Cuentan con un tamaño y expansión mayor.
Nube privada	Despliegue de una aplicación de forma definitiva. Adecuado cuando no se prevé aumentar los recursos a corto plazo.	Normalmente se implantan en una empresa. Tienen un diseño específico para ella.
Nube híbrida	Adecuado si no se quiere compartir espacio con otros usuarios. Útil si se prevé aumentar los recursos a corto plazo.	Utiliza infraestructura física privada. Aprovecha posibilidades de ampliación públicas.

FUENTE (Relica, 2014)

2.2.1. NUBE PÚBLICA

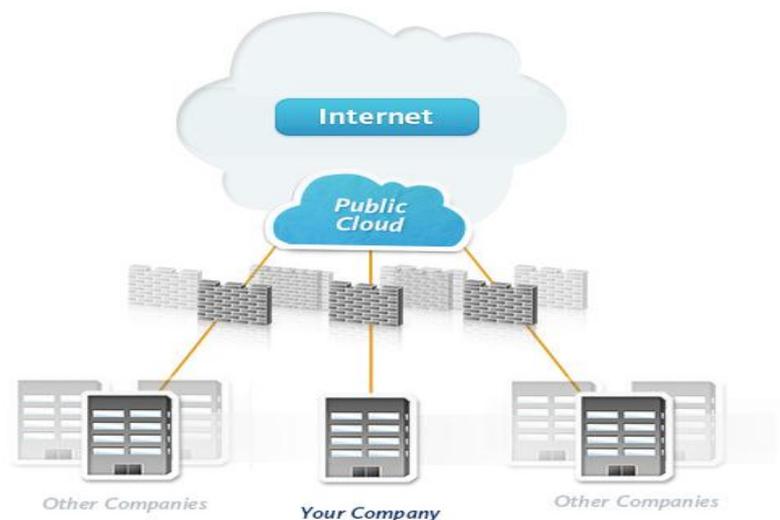


FIG. 2.2.2.Nube Pública
FUENTE (Gomez, 2011)

La denominación de Nube Pública hace referencia al modelo estándar de *Cloud Computing*, en el que el prestador de servicios pone a disposición de cualquier usuario en Internet su infraestructura (*software o hardware*) de forma gratuita o mediante el abono de cierta cantidad relacionada con el volumen o tiempo de uso de los mismos. Así, los servicios de las nubes públicas son ofrecidos en general a grupos de varias organizaciones, y su propietario es el proveedor de servicios. Las aplicaciones e información se almacenan en servidores externos y el servicio se ofrece a través de Internet.

El uso de nubes públicas permite ampliar fácilmente los recursos necesitados, ya que éstas suelen tener más tamaño que las nubes privadas, normalmente implantadas en una única organización.

Sin embargo, también presentan ciertos aspectos a vigilar y carencias respecto al resto de modelos que es necesario tener en cuenta:

- No es posible tener localizados los datos aportados a los servicios de la nube físicamente ni en todo momento.

La información aportada a la nube se almacena con aquella de otros usuarios de los servicios, esto hace que la empresa que contrata el servicio deba ser muy cuidadosa en los requisitos exigidos en el acuerdo con el proveedor de servicios en lo referente a:

- Protección de datos, control de la propiedad de la información e imposición de restricciones sobre su ubicación.
- Condiciones para que el usuario pueda inspeccionar su información en cualquier momento.
- Garantías sobre posibles pérdidas de información o falta de disponibilidad de la misma.

Algunos ejemplos de nubes públicas son *Amazon Elastic Compute Cloud (EC2)*, *IBM Blue Cloud*, *Sun Cloud*, *Google AppEngine* y *Microsoft Windows Azure Services Platform*.

2.2.2. NUBE PRIVADA



FIG. 2.2.3. Nube Privada

FUENTE (Gomez, 2011)

Actualmente existe una importante tendencia en grandes empresas a la implementación de esta nube dentro de su estructura utilizando la red privada de la misma.

Hacen referencia a redes o centros de procesamiento de datos propietarios que utilizan tecnologías y características de *Cloud Computing*, tales como la virtualización. Así, parten de los principios del *Cloud Computing* tradicional y ofrecen los mismos servicios dentro en la propia estructura de la compañía.

Se suelen diseñar específicamente para un usuario, proporcionando un control óptimo de la información gestionada, de su seguridad y de la calidad de servicio ofrecida. Habitualmente, el usuario es también propietario de la infraestructura de la nube privada, y tiene control total de las aplicaciones desplegadas en ella.

Esto obliga a adquirir nuevos sistemas antes de hacer uso de ellos, contrariamente a lo ofrecido por las nubes públicas, donde ampliar los recursos se reduce a contratarlos con el proveedor de servicios.

Como ventaja de este tipo de nubes, a diferencia de las nubes públicas, destaca la localización de los datos dentro de la propia empresa, lo que conlleva a una mayor seguridad de estos.

2.2.3. NUBE HÍBRIDA



FIG. 2.2.4. Nube Híbrida

FUENTE (Gutiérrez, 10 junio del 2013)

El modelo híbrido combina los modelos anteriormente descritos, sobre nubes públicas y privadas, de manera que se aprovecha la ventaja de localización física de la información gestionada por las nubes privadas con la facilidad de ampliación de recursos de las nubes públicas.

Las nubes híbridas consisten en combinar las aplicaciones propias de la empresa con las consumidas a través de la nube pública, entendiéndose también como la incorporación de servicios de *Cloud Computing* a las aplicaciones privadas de la organización.

Esto permite a una empresa mantener el control sobre las aplicaciones críticas para su negocio y aprovechar al mismo tiempo las posibilidades ofrecidas por los servicios ofertados por la nube en aquellas áreas donde resulte más adecuado.

Parece que actualmente este tipo de nubes está teniendo buena aceptación en las empresas, por lo que se están desarrollando *software* de gestión de nube que permita controlar la nube privada e incorporar al mismo tiempo recursos y servicios de proveedores públicos de *Cloud Computing*. (Hogan, Liu, Sokol, & Tong, 2011)

2.3.LOS NIVELES DE SERVICIO DE *CLOUD COMPUTING*

Los servicios ofrecidos por la nube se distribuyen entre todas las capas tradicionales de un sistema informático, desde la capa de *hardware* hasta la capa aplicación *software* propiamente dicha.

En la práctica, los proveedores de servicios de la nube tienden a ofrecer servicios que pueden ser agrupados en tres categorías:

- *IaaS* (Infraestructura como servicio).
- *PaaS* (Plataforma como servicio)

- *SaaS* (*Software como servicio*).

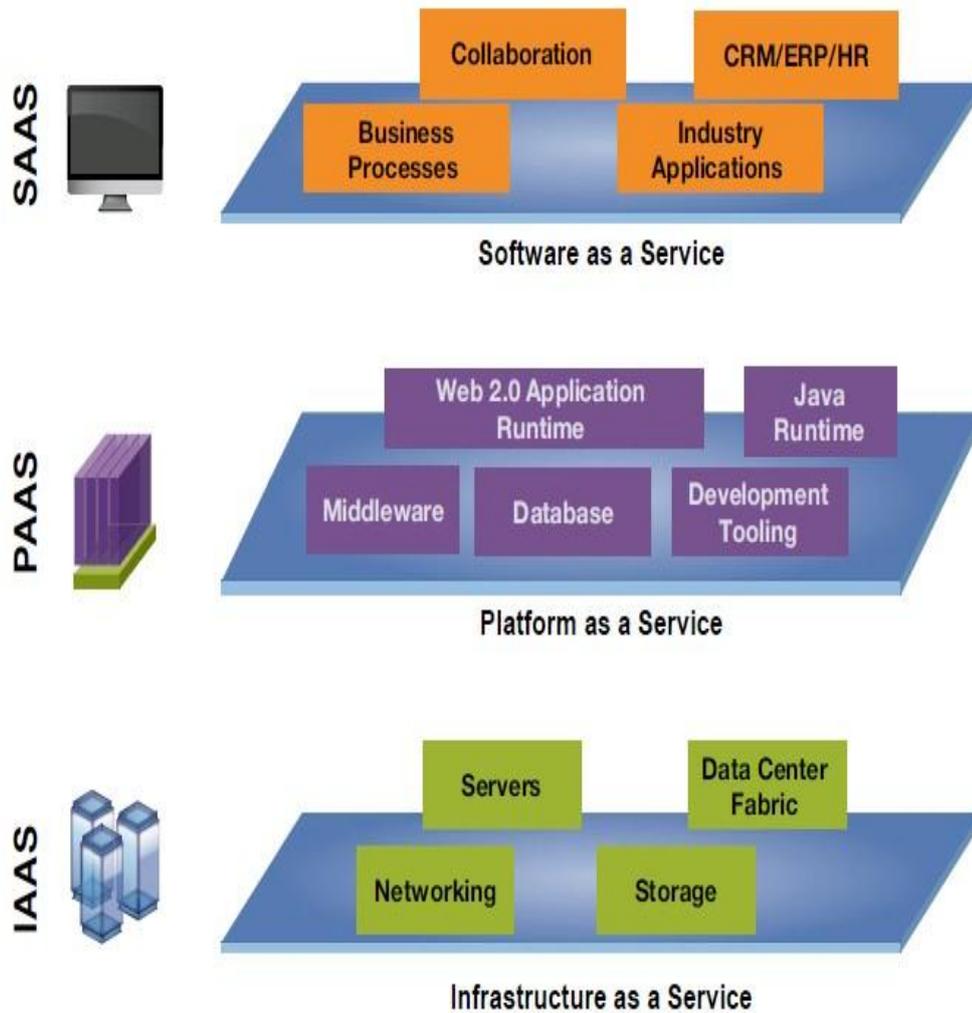


FIG. 2.3.1. Niveles de Servicio

FUENTE (Gomez, 2011)

Tal y como se indica en la figura, cada uno de los niveles de *Cloud Computing* se sostiene sobre los niveles inferiores, de forma que los servicios *SaaS* en muchas ocasiones son soportados sobre plataformas *PaaS* y consumen indirectamente infraestructura en forma de servicio (*IaaS*).

Así, una empresa que contrate una aplicación en Cloud Computing a través de un servicio *SaaS*, frecuentemente contará con el soporte y mejora continua que garantizarán la actualización y optimización de la aplicación para la seguridad de la información. Por otra parte, dicho cliente contrata indirectamente la infraestructura como son servidores, bases de datos, etc. Es necesario ejecutar las aplicaciones, del mismo modo como que se lo hiciera a través de servicios *IaaS*.

En cuanto a los usuarios pueden utilizar los tres tipos de servicios según las necesidades que se presenten.

- Empresas que quieran contratar cualquier tipo de aplicación *software* a través de servicios *SaaS*.
- Empresas TIC cuyo núcleo de negocio sea el desarrollo *software* y quieran contratar plataformas o entornos de programación en *Cloud Computing* ofrecidas por *PaaS*.
- Empresas que necesiten ampliar los recursos *hardware* para sus aplicaciones como es el espacio de almacenamiento, capacidad de procesamiento, etc. y lo resuelvan a través de servicios *IaaS*.

2.4.ESTADO DEL ARTE

2.4.1. DETALLE DE LOS SERVICIOS IaaS,PaaS,SaaS

2.4.1.1. IaaS (INFRAESTRUCTURA COMO SERVICIO)

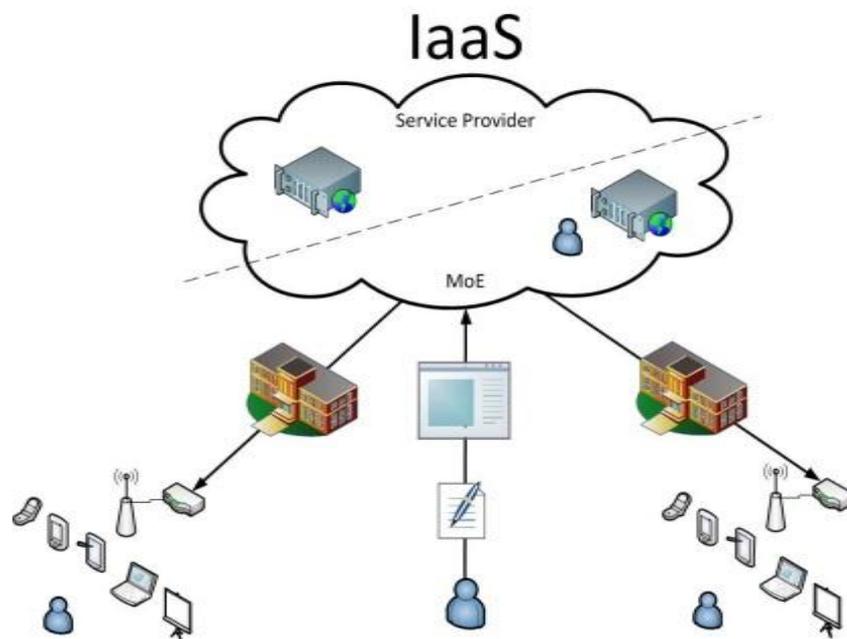


FIG. 2.4.1.1. Servicio IaaS

FUENTE (Gomez, 2011)

IaaS, o Infraestructura como Servicio, describe los sistemas *hardware* que se le ofrecen a un usuario en forma de servicios para que éste pueda situar en ellos sus aplicaciones informáticas o su información.

Los servicios que se ofrecen habitualmente abarcan desde capacidad de procesamiento o de almacenamiento ya sea alquilando servidores, discos duros,

procesamiento en un CPD, etc. Hasta la capacidad de transmisión de información en forma de redes de comunicaciones de alta capacidad.

IaaS está dirigido a cualquier empresa que desee delegar la implantación de sus sistemas *software* y aplicaciones en la infraestructura *hardware* de un proveedor externo a un fenómeno conocido tradicionalmente como *hosting*, ya sea que requiera de servicios de almacenamiento externo, copias de seguridad de sus datos, cálculos complejos que requieran software de elevadas prestaciones, etc. El proveedor les permitirá gestionar dichos sistemas en un entorno virtualizado.

Así, los proveedores de servicios son los propietarios de las máquinas físicas, y las ofrecerán como servicio a los usuarios a través de entornos que les permitan gestionarlas, por ejemplo una página *Web* para el control de las máquinas.

2.4.1.2. IAAS VS. SISTEMA TRADICIONAL

A continuación se muestra de forma esquematizada una comparación entre el uso de los sistemas informáticos tradicionales requeridos por una organización, y los cambios que puede aportar el uso de *IaaS*. (Gomez, 2011)

- **RENDIMIENTO**

En el sistema tradicional se desaprovechan recursos, mientras que en un sistema *IaaS* se consigue una mayor eficiencia en su utilización entre estos menos sistemas

informáticos desaprovechados, menor energía consumida por unidad de información gestionada, sistemas más automatizados para una mayor eficiencia.

Asimismo, los recursos físicos se gestionan de manera unificada por parte del proveedor, por lo que el tiempo necesario para adaptar los recursos de un usuario de *IaaS* a sus necesidades reales en cada momento se reduce notablemente. Así, el proveedor de servicios podrá optimizar el uso en todas sus máquinas, reduciendo así los costos por el servicio.

- **PROPIEDAD DEL SISTEMA**

Las máquinas físicas utilizadas para *IaaS* son propiedad del proveedor de servicios, con el consiguiente riesgo de que éste pudiera dejar en algún momento de ofrecer el servicio. Sin embargo, esta característica aporta importantes ventajas, por ejemplo el hecho de que el equipamiento se renueva más fácilmente debido a la economía de escala de estos sistemas y de que se siguen estándares que facilitan la interoperabilidad entre fabricantes. Por otra parte, aunque en los sistemas tradicionales la infraestructura es propiedad de la organización, tiene el inconveniente de que está asociada a sistemas que se pueden quedar obsoletos o ser incompatibles con otros.

- **FIABILIDAD Y RESPUESTA ANTE FALLOS**

El empleo de servidores virtuales dedicados, que simulan una máquina con un sistema operativo propio, permite separar esta máquina simulada del resto de

funcionalidades ofrecidas por el resto de la máquina física. Así, si la máquina física falla, se puede utilizar la máquina simulada en otra máquina física, por lo que las consecuencias de un fallo en alguna de las máquinas y el tiempo de recuperación se reducen drásticamente.

Además, estas máquinas utilizadas en *IaaS* se encuentran replicadas, y disponen de centros físicos de almacenamiento y procesamiento con ciertas características que, en el caso de ser implantadas en los centros tradicionales, tendrían unos costos demasiado elevados.

2.4.1.3. PaaS (PLATAFORMA COMO SERVICIO)

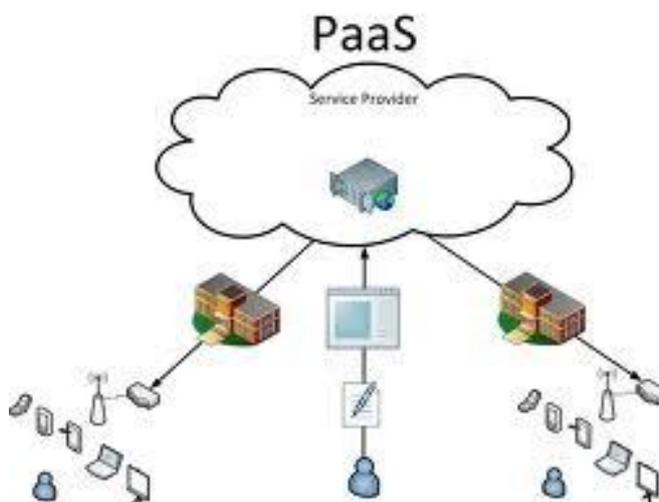


FIG. 2.4.2.3 Servicio PaaS

FUENTE (Leon, 2010)

PaaS, o Plataforma como Servicio, es un modelo orientado a equipos de trabajo que realicen proyectos de manera compartida, para lo cual proporciona un conjunto

de herramientas y funcionalidades *software* como sistemas operativos y servicios asociados a los mismos para desarrollo conjunto de *software* y aplicaciones, situados en una red de máquinas de *Cloud Computing* y accesibles a través de Internet.

Así, para proyectos relacionados con las Tecnologías de la Información y las Comunicaciones, *PaaS* permite crear aplicaciones mediante el uso de un entorno de desarrollo único que integra las principales tecnologías basadas en estándares.

Cuanto más dependan los resultados de cada miembro del equipo de los del resto de integrantes, más efectivo será el uso de *PaaS* en el rendimiento global del equipo, ya que simplifica el trabajo colaborativo, y reduce los costos en tiempo y en los sistemas necesarios para soportar la colaboración.

PaaS estará dirigido por tanto a desarrolladores *software* que requieran de un entorno de trabajo colaborativo. El establecimiento de una plataforma *Cloud* de este tipo para el desarrollo de aplicaciones informáticas permitirá que varios equipos de desarrollo distantes puedan trabajar en un mismo proyecto y en una misma máquina.

Así, se reduce el costo por el mantenimiento de varios equipos, se evitan problemas de incompatibilidad entre equipos y se disminuye el esfuerzo de creación de las aplicaciones, ya que se dispone de un sistema que unifica y centraliza de manera simple un desarrollo distribuido.

2.4.1.4. PAAS VS. SISTEMA TRADICIONAL

Al igual que en *IaaS*, el uso de *PaaS* aporta ciertas mejoras y facilidades, entre las que destacan:

- **CALIDAD FINAL**

El importante esfuerzo colaborativo realizado en aplicaciones informáticas creadas con *PaaS* hace posible que en la gran mayoría de los casos el usuario perciba una calidad final mayor que la ofrecida por aplicaciones convencionales:

A diferencia del proceso tradicional, donde se desarrolla en un entorno y posteriormente se traslada a otros para su prueba y puesta en marcha, en *PaaS* la creación de la aplicación se realiza en un entorno unificado y que será el mismo al que accederán sus usuarios finales, por lo que se reducirán los errores debidos a las diferencias entre entornos y serán más sencillos de corregir.

Por otra parte, el hecho de gestionar toda la información de manera centralizada permite obtener estadísticas de la información real accedida en cada momento, las cuales podrían reutilizarse para mejorar la aplicación u otras similares.

- **INTEROPERABILIDAD CON OTROS SISTEMAS EN LÍNEA**

Trabajar con *PaaS* facilita la conectividad a esos recursos, ya que ambos estarán diseñados específicamente para trabajar de forma conjunta, y permite actualizar automáticamente las conexiones entre los recursos, lo cual supone una ventaja respecto al desarrollo realizado en los sistemas tradicionales. Asimismo, *PaaS* utiliza frecuentemente una infraestructura *IaaS*, ya descrita anteriormente, beneficiándose de sus ventajas como ampliar o reducir los recursos físicos eficientemente.

2.4.1.5. *SaaS* (SOFTWARE COMO SERVICIO)

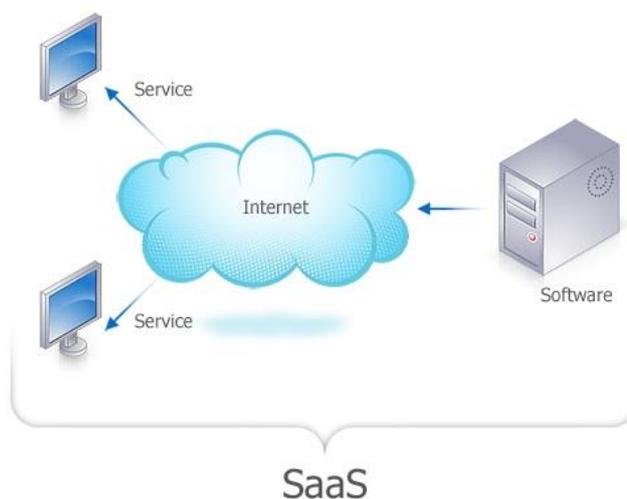


FIG. 2.4.3.5. Servicio SaaS [6]

A continuación, se describirá el último de los niveles en los que se estructura los servicios de Cloud Computing: *SaaS* (*Software As A Service*). Probablemente, se trata del sistema más extendido entre las empresas, dado el alto rango de aplicaciones que ofrece.

SaaS, o *Software* como servicio, es un modelo de despliegue de *software* donde una aplicación informática se ofrece como un servicio a través de Internet. Así, se permite que el usuario del servicio no necesite instalar o actualizar la aplicación en sus equipos.

Este modelo permite el uso de nuevo *software* sin necesidad de realizar una gran inversión inicial en adquisición de licencias o sistemas informáticos. De hecho, la inversión se realiza únicamente en función del uso de los servicios *SaaS*, cuyo costo a corto plazo suele ser bastante reducido. Una vez establecido el acuerdo de servicio o LSA con el proveedor, las aplicaciones pueden comenzar a utilizarse en un periodo de tiempo muy breve.

Así, *SaaS* está orientado principalmente a reducir el costo de implantación y uso de los sistemas informáticos asociados a la gestión de los recursos empresariales (como pueden ser los ERP y CRM) de una organización.

El costo se reduce debido a que la inversión inicial es prácticamente inexistente, y las tarifas por el uso posterior de los servicios *SaaS* son bastante reducidas debido a la economía de escala y a alta especialización de las empresas proveedoras de esos servicios.

En cuanto a los agentes destinatarios de *SaaS*, pueden ser cualquier empresa que esté interesada en alguno de los servicios ofrecidos por proveedores *SaaS*, los cuales pueden ser de muy distinto tipo desde servicios genéricos relacionados con actividades como la gestión del correo electrónico, repositorio de documentos

compartidos, hasta servicios que cubran procesos de negocio estratégicos para la organización, en los que se puede llegar a cierto acuerdo de parametrización o personalización con el proveedor de servicios *SaaS*.

En cualquiera de estas situaciones, no se debe obviar la realización de un análisis detallado de las necesidades de la empresa y del impacto que produciría la adopción de soluciones *SaaS* en el seno de la compañía.

2.4.1.6. SAAS VS. SISTEMA TRADICIONAL

En la práctica, las aplicaciones *SaaS* se diferencian de las aplicaciones tradicionales en ciertos aspectos fundamentales, varios de ellos ya comentados en las ventajas generales ofrecidas por *Cloud Computing*:

- **ADMINISTRACIÓN INFORMÁTICA**

Las organizaciones que usan *software* tradicional comúnmente necesitan un departamento de administración o una subcontratación de esas competencias a otras empresas para que se resuelvan problemas asociados a la implantación de la infraestructura informática o la resolución de problemas como la seguridad de los sistemas, la fiabilidad, el rendimiento ofrecido o problemas de disponibilidad.

Si se utiliza *SaaS*, esta administración se ve reducida considerablemente, ya que la realiza el proveedor de servicios basándose en el acuerdo de nivel de servicio.

- **INDEPENDENCIA DE LAS MEJORAS EN LAS APLICACIONES**

El proveedor de *SaaS* no sólo se encarga de la administración, como se acaba de comentar, sino que también es el que se encarga de instalar, mantener y actualizar las aplicaciones del cliente, por lo que este último podrá invertir su tiempo en las tareas propias de su negocio, utilizando sus recursos en las áreas más estratégicas.

- **INDEPENDENCIA DE ACCESO**

Las aplicaciones ofrecidas con *SaaS* son accesibles a través de Internet, independientemente del lugar físico de acceso a la red. Así, se aporta mayor flexibilidad a la organización y se evita usar tecnología más compleja para acceder a la red privada de la empresa desde el exterior (con el uso, por ejemplo, de redes privadas virtuales).

Aunque en ocasiones esto puede llegar a ser un inconveniente, ya que siempre se ha de tener conexión permanente a Internet para poder utilizarlo. Además, las aplicaciones han de gestionar un almacenamiento temporal y periódico de la información para evitar una posible pérdida en el caso de que la conexión a Internet se interrumpa. (Gomez, 2011)

2.5.MOVILIDAD



FIG. 2.5.1. Movilidad del Cloud Computing

FUENTE (Hogan, Liu, Sokol, & Tong, 2011)

No hay duda de que los servicios de *Cloud Computing* o en la nube se convertirán en los próximos años en un conductor de la innovación.

La mayor parte del valor generado por este fenómeno ha sido capitalizado por los *big-players* con sede en EE.UU., como Amazon o Google. Pero la nube ofrece oportunidades, desde *pymes* a grandes compañías que pueden aprovechar la potencialidad y flexibilidad de este nuevo modelo de negocio.

Llevar servicios a la nube permite adoptar un sistema flexible de costos adaptando los presupuestos de Tecnología de la Información a las necesidades reales de cada momento, sin grandes inversiones. Además, permite una implementación muy rápida de cualquier servicio, generando una rapidez en la respuesta a las necesidades empresariales. Y, por último, aporta una gran

escalabilidad de recursos, de manera que se utilicen éstos en función de la demanda y picos de trabajo de las propias compañías.

Durante los últimos años se está hablando mucho de las ventajas para que las empresas puedan movilizar y agilizar ciertos procesos y aplicaciones de negocio. Así, destacan algunos beneficios como el aumento de la productividad, la reducción de costos, el incremento de la satisfacción del cliente y de los empleados e incluso, la generación de nuevos modelos de negocio innovadores posibilitados por las nuevas tecnologías móviles.

Pues si bien es cierto ya son mayoritarios los sectores o ámbitos de actividad los que potencian su negocio a través de la movilidad, servicio al cliente, fuerza de ventas, trazabilidad en la entrega de productos y gestión de inventarios, gestión de rutas modificables en tiempo real o la oficina móvil, entre otros. Las posibilidades son muy amplias y algunas todavía inimaginables.

CAPÍTULO III

ESTÁNDARES DE CALIDAD

3.1.NORMAS DE SEGURIDAD DE INFORMACIÓN

ISO/ICE27001

La seguridad de la información es vital conocerla y utilizarla para el funcionamiento de cualquier organización y sobre todo para mantener siempre segura nuestra información. Disponer de la certificación *ISO/IEC 27001* ayuda a gestionar y proteger nuestros valiosos activos de información. Es una norma adecuada para cualquier organización, independientemente de su tamaño o su sector. La norma es especialmente interesante si la protección de la información es crítica.

ISO/IEC 27001 es la única norma internacional, que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI) y permite establecer una serie de controles de seguridad adecuados para proteger los activos de

información y ofrecer confianza a cualquiera de las partes interesadas y en especial a nuestros clientes.

A continuación presentamos las principales características por las que se debe regir la norma ISO/IEC 27001:

- **Confidencialidad:** Garantizar el acceso sólo a personas autorizadas.
- **Disponibilidad:** Conseguir que esté disponible cuando sea necesaria.
- **Integridad:** Mantener la exactitud y prevenir la manipulación no autorizada, la pérdida y el deterioro.
- **Autenticación:** Asegurar la identidad de quién accede o genera la información.
- **Trazabilidad:** Saber quién ha hecho qué y cuándo. (Salas, 2013)

3.1.1 VENTAJAS

- **COMPETITIVIDAD Y SUPERVIVENCIA:**

Disponer de la certificación ofrece una mayor confianza de la empresa por parte de sus clientes, lo que puede favorecer la elección frente a competidores. Pero es tal el interés y crecimiento de esta norma, por lo que puede llegar incluso a establecer la diferencia entre la supervivencia o no de una empresa.

- **REDUCCIÓN DE RIESGOS Y COSTOS**

La implantación de controles que obliga la norma, reduce al mínimo los incidentes de seguridad como son interrupciones de servicio, fugas de datos, etc. Y facilita la continuidad del negocio en el caso de que se produzcan, por lo que ahorra costos operativos y disminuye el lucro.

- **MÉTODO**

La implementación de un SGSI transforma la seguridad en una actividad de la gestión. Convierte un conjunto de actividades en un ciclo de vida metódico y controlado. El estándar además crea conciencia y compromiso de seguridad en todos los niveles de la empresa.

- **VISIÓN EXTERNA Y ADECUACIÓN**

La norma implica una serie de medidas de auditoría interna y externa que, por un lado, impone responsabilidad al personal de la empresa que verá auditado su ya que será controlado su trabajo y, por otro, aportará una visión externa independiente y ajena a la rutina de la empresa que siempre aportará muchas acciones de mejora. El SGSI además tiene en cuenta el marco legal, lo que ayuda a la correcta adecuación de la empresa a la normativa vigente.

- **ORGANIZAR EL NEGOCIO**

En algunos casos, especialmente cuando la empresa ha tenido un rápido crecimiento, los activos de información pueden estar dispersos o desorganizados. Esta evaluación ayudará a planificar inversiones y futuras acciones de acuerdo a su importancia dentro de la organización. (Gomez, 2011)

3.2SEGURIDAD DEL *CLOUD COMPUTING*



FIG. 3.2.1. Seguridad de la Nube

FUENTE (Cerde, 2012)

Como sabemos la seguridad siempre ha sido uno de los principales problemas en el ámbito de la transmisión de datos, con la aparición del *Cloud Computing* se tiene como objetivo principal cuidar la integridad y privacidad de la información de los usuarios.

Pues si bien es cierto el *Cloud Computing* es una tecnología que permite acceder a sus datos desde cualquier punto a través de una conexión a Internet por medio de la

gran infraestructura que posee, la posibilidad de obtener recursos adicionales bajo demanda o despreocuparse del mantenimiento del sistema son unas de las grandes ventajas, aún existen algunos puntos vulnerables y riesgos de la seguridad que es importante conocerlos para así tomar medidas de seguridad tanto para proveedores como clientes y mejorar los recursos de la nube para un mejor servicio.

3.2.1 RIESGOS DEL *CLOUD COMPUTING*

El gran crecimiento del *Cloud Computing* en el mundo empresarial, ha provocado que haya mayores amenazas sobre la infraestructura del servicio puesto que por medio de ella existen miles de estafas e invasión de información por lo que se ven afectadas muchas empresas que usan la nube como una solución tecnológica.

Pues podemos decir que los principales riesgos y amenazas en la red de internet, son los mismos que pueden darse en el *Cloud Computing*, por lo tanto las amenazas a las que se ve expuesta la nube son:

➤ ABUSO Y USO MALINTENCIONADO

Este riesgo afecta principalmente a modelos de servicio *IAAS* y *PAAS* y se relaciona con acceso a la infraestructura o plataforma con poca seguridad y restricción, ya que cualquier usuario puede acceder a la nube siempre que pague por su uso. De tal manera que los hackers y piratas informáticos pueden acceder a los recursos de la nube sin ningún inconveniente.

Por lo general, los ataques que realizan los hackers son, el robo de contraseñas, introducción de virus a manera de SPAM, ataques de negación de servicio, creación de códigos maliciosos que inhabilitan los recursos.

Como ejemplo de este tipo de riesgo en la nube, son conocidos los casos de proveedores *IAAS* que albergan *botnets* que han alojado sus centros de control en infraestructuras *Cloud*. Por ellos tenemos algunos casos.

PRIMER PROBLEMA:

En este caso un hacker envía un virus a través de internet que infecta a todas las computadoras y equipos vulnerables que se encuentren conectados a la red, esto a su vez crea una red de máquinas esclavas que son conocidas como *botnets*, que se ejecutan de manera automática y autónoma, controlando servidores y ordenadores de forma remota

SEGUNDO PROBLEMA:

Para este segundo caso, el hacker vende o alquila la *botnet* a otros hackers, quienes a su vez la usan para realizar fraude, *spamming*, ataques DDoS17 (Denegación de servicios), entre otros.

Por lo general, los hackers usan las *botnets* en *Cloud Computing* ya que al tener una nube con servicios u aplicaciones, en donde existen infinidad de máquinas virtuales, es sumamente fácil infectar las máquinas y así expandir el virus, para poder

atacar mediante varios métodos a las empresas y organizaciones que albergan su información en la nube.

Por lo tanto, una *botnet* en un entorno *Cloud* puede ser suficiente como para poner en riesgo el contenido de los datos subidos a la nube, ya que además de expandirse a través de toda su infraestructura, esta puede llevar a cabo ataques como:

- **DDoS**

Denegación de servicio distribuido en la nube que puede lanzar un ataque masivo y coordinado para impedir o reducir los servicios y aplicaciones, saturando el ancho de banda y los recursos del sistema. Como por ejemplo, inundaciones de mensajes robo de contraseñas del servicio de correo electrónico.

- **SPYWARE Y MALWARE**

Espías enviados a la nube, que pueden recompilar datos de los usuarios e información confidencial para mal uso de la misma, como por ejemplo venderla o alterar su contenido.

- **ADWARE**

Consiguen que los clientes se descarguen, instalen a través de publicidad ventanas basadas en hábitos de navegación del usuario, es decir, forzar al navegador del usuario a visitar páginas web periódicamente.

➤ PÉRDIDA DE INFORMACIÓN

Este tipo de amenaza se puede dar debido a varias causas entre las cuales están errores humanos o por acciones malogradas por parte del usuario *Cloud*. Por ejemplo se puede dar perdida de datos o modificación de los mismos sin tener una copia de seguridad.

Por esta razón, la mayoría de empresas utilizan medidas como la incorporación de cláusulas de confidencialidad en los contratos laborales, o el establecimiento de políticas de seguridad en el uso de los recursos de la nube. Los problemas más comunes son el mal uso de las claves de los usuarios, autenticación, autorización y cifrado de las claves.

Por lo que se podría implementar API's más seguras que hagan un control de acceso a los usuarios de una manera más exhaustiva, protección del tránsito de datos mediante técnicas de cifrado. Además de tener servidores de almacenamiento de información a manera de *backups* de la información original, y almacenamiento en sistemas seguros con claves encriptadas.

➤ API'S INSEGURAS

Las API's son una puerta de entrada hacia los servicios de la nube por lo que se convierten en un punto crítico de seguridad y privacidad del sistema. Los proveedores de servicios *Cloud* ofrecen interfaces y API's para controlar los recursos

de la nube, por lo tanto la monitorización y control se da por medio de una API, en donde esta tiene la potestad de dar permisos para arrancar o parar los servicios de la nube, o aumentar y disminuir los recursos de la misma.

De tal manera que si no existe una correcta política de seguridad las API's pueden sufrir ataques por parte de *malware*²³ para realizar acciones adicionales malignas que pueden afectar a los sistemas de la nube.

➤ **SUPLANTACIÓN DE IDENTIDAD**

Esta es una de las amenazas más comunes en *Cloud Computing*, ya que no todas las aplicaciones de la nube requieren al usuario introducir su nombre de usuario y la clave de acceso. Además es común el fraude mediante phishing y la explotación de fallas de seguridad para el robo y suplantación de identidad de los usuarios, como también acceder a actividades y aplicaciones a manera de virus, manipulación de datos, intercambio de información falsificada y redirigir a los usuarios a sitios maliciosos. Las investigaciones realizadas por expertos han identificado tres métodos utilizados para realizar el robo de identidad digital.

- **ATAQUE PHISING:**

Caracterizador por adquirir información confidencial de forma fraudulenta como contraseñas, tarjetas de crédito, información bancaria, etc. A menudo este tipo de ataque se propaga como SPAM en la nube y parece ser enviado por otro usuario o un tercero que pertenece a la comunidad Cloud o hace uso de la misma.

- **PHARMING**

En este ataque se aprovechan las vulnerabilidades del servidor DNS y se encuentra el nombre de dominio de un sitio web que permite al atacante redirigir un nombre de dominio a otra máquina distinta. (Salas, 2013)

3.2.2 PRINCIPIOS PARA LA PROTECCIÓN DE LA NUBE

Debido a que todos los datos terminaran en la nube, es necesario contar con distintos niveles de protección de los mismos, adicionalmente a la protección brindada por el proveedor y la implementada por los clientes. Es decir, tener niveles de seguridad para que se ajusten a la confidencialidad de los diferentes tipos de datos.

3.2.2.1 SEGURIDAD DE LA IDENTIDAD

La seguridad de la identidad preserva la integridad y la confidencialidad de los datos y aplicaciones, además de ofrecer disponibilidad inmediata a los usuarios.

Como solución de seguridad se puede considerar el mecanismo de autenticación solida de nombres de usuario y contraseñas, con la adopción de técnicas y tecnologías estandarizadas, como ya se mencionaron.

Además de un control exhaustivo por parte de la empresa en la creación y asignación de nuevos usuarios, los cuales a su vez deberían ser llevados en un control cada vez que accedan a la información.

3.2.2.2 SEGURIDAD DE LA INFRAESTRUCTURA

La nube debe ser diseñada para ser segura, como interfaces sólidas y con sistemas de evaluación de vulnerabilidades y administración de cambios con niveles de servicio que creen confianza en la empresa o usuario que desee hacer uso de la nube. En cuanto a la administración, es importante considerar el ciclo de vida de los recursos de la nube, ya las necesidades y los requerimientos de los clientes se modifican, el proveedor de servicios debe ofrecer nuevos recursos y eliminar los recursos obsoletos, tomando en cuenta que esto brindara niveles de confianza hacia los clientes.

3.2.2.3 SEGURIDAD DE LA INFORMACIÓN

Para dar seguridad a la información es necesario tener una barrera de protección que garantice la seguridad de la infraestructura a utilizar. Por lo que es necesario aislamiento de los datos en situaciones de tenencia múltiple ya que al tener varios usuarios que hagan uso de recursos compartidos, estos se ven vulnerables a ataques y robo.

Por tanto, la virtualización, la encriptación y el control de acceso son herramientas que permitirán distintos grados de separación entre las organizaciones, pequeños usuarios y usuarios independientes.

Clasificación de los datos, es decir según su importancia, para lo cual se podrá implementar políticas de seguridad en las cuales dependiendo del grado de

confidencialidad los datos podrán ser almacenados dentro de la misma empresa en un servidor exclusivo, o bajo medidas de encriptación de datos.

Buen manejo y control de cumplimiento de normas de seguridad, con la creación de información de administración y validación realizada a manera de monitoreo y auditoria del estado del manejo de la información. Brindando seguridad al documentar el acceso y denegación de acceso a los datos, y verificando que no se haya cambiado el contenido de la información. (Gomez, 2011)

Tabla 2. Mecanismo de Seguridad

MODELOS DE SERVICIO	MECANISMO DE SEGURIDAD POR PARTE DE	
	PROVEEDOR	CLIENTE
INFRAESTRUCTURA (IAAS)	Debe brindar seguridad a los equipos, programas, data center y garantizar la disponibilidad de la información.	Debe mantener el sistema operativo actualizado para que los parches de seguridad se mantengan activo.
	Garantizar que la información no se pierda, o que se acceda personal no autorizado y hacer responsable al cliente si hace uso ilícito de la nube.	Tiene la responsabilidad de la configuración del firewall, de los permisos necesarios para que puedan acceder a la red, autenticación, autorización de la nube. CONTINUA 

	Dar servicio de actualización a los equipos tanto de software como hardware y así controlar la infraestructura de red de gestión de recursos	Es responsable controlar el ingreso de usuarios y realizar copias de seguridad de los datos para garantizar que no hay pérdidas de información en caso de haber un fallo.
INFRAESTRUCTURA (PAAS)	Protección de datos y administración del acceso a las aplicaciones así como las instalaciones de malware.	El cliente crea, despliega y ejecuta una aplicación, administra los upgrades parches para todas las funciones de la misma.
	Mecanismos de control y eliminación de software para que no ingresen a la nube.	El cliente usa hojas de cálculo, procesadores de texto, copias de seguridad, cobros, procesamiento de nómina y facturación.
INFRAESTRUCTURA (SAAS)	Administración del acceso a aplicaciones específicas que se ofertan en la nube	El único control que un usuario final tiene es acceder a la aplicación del Usuario final.
	El proveedor controla los sistemas operativos, hardware, infraestructura de red, de aplicaciones y parches.	Pueden ingresar desde un desktop, laptop o teléfono móvil.

FUENTE (Relica, 2014)

CAPÍTULO IV

SERVICIO CLOUD COMPUTING EN EMPRESA LOCAL

TELCONET

4.1. DATA CENTER O SERVIDORES VIRTUALES (NUBE)

Es el área de Control Físico donde se consolida todo el equipo de procesamiento de datos. Dedicada a proporcionar un servicio ininterrumpido a las operaciones de procesamiento de datos críticos de una o varias empresas.

ASPECTOS IMPORTANTES DEL CENTRO DE DATOS

Tenemos como son energía eléctrica, el enfriamiento para mantener el control ambiental, las medidas de seguridad son las más importantes el monitoreo (NOC) es necesario para poder mantener un control del servicio Pues si bien es cierto la detección de incendios es necesario ya que en los equipos se encuentran todos los equipos y finalmente tienen una de las mejores infraestructuras de red.

La infraestructura de cableado representa menos del 5% del costo del centro de datos y normalmente es el de más bajo interés (Vazquez, 2012)

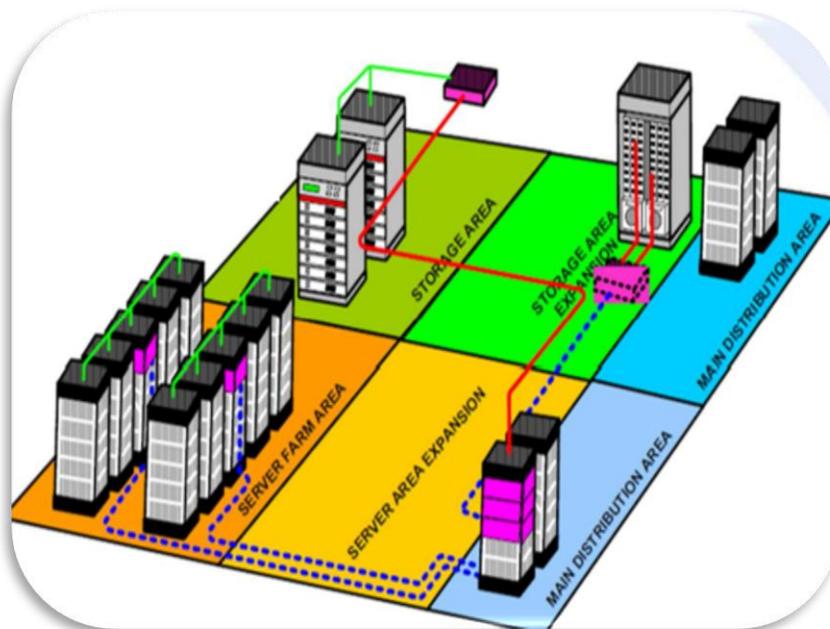


FIG. 4.1.1. Distribución del Data Center

FUENTE (TELCONET, 2013)

4.2. INVERSIÓN DE TELCONET EN EL CLOUD COMPUTING

La intención que poseen de invertir es la tendencia en el mundo que se está dando pues se encuentran apoyados por una infraestructura de redes para brindar mejores servicios hacia el mercado nacional e internacional.

En el Ecuador existe una demanda insatisfecha de sitios de alta disponibilidad para que las empresas alojen sus servidores o demanden servicios de hosting y housing.

SERVICIOS QUE PROPORCIONA TELCONET COMO DATA CENTER

- **HOUSING:** es un alojamiento compartido en el cual se alquila un espacio de gabinetes cerrados (colocación), suites dedicadas (jaulas).
- **HOSTING:** son servidores virtualizado que ofrecen servicios en la nube, en un Centro de datos con las más avanzadas tecnologías en materia de seguridad física que posee vigilancia, protección anti-incendios, sistemas de alimentación eléctrica y de climatización para servicios de misión crítica

SERVICIOS QUE OFRECE A LOS CLIENTES

Entre las principales características principales es la seguridad lógica, así como el mantenimiento de sistemas, soporte manos remotas, el monitoreo dedicado, backups.

ESPACIO E INTERCONEXIONES

Posee interconexiones con más de 1500 m² de espacio técnico proyectado en los dos Centros de Cómputo como son:

- Quito: Categoría TIER III (capacidad 180 racks)
- Guayaquil Categoría TIER IV (capacidad 400 racks)

Pues posee los Data center más grandes y avanzados del Ecuador, a la vanguardia de Latinoamérica, cumpliendo las Normas TIA 942-2 y Uptime Institute. Permitiendo dar servicios a empresas del Ecuador y la Región

Tiene interconexión dentro de Ecuador desde Quito y Guayaquil hacia el mundo a través del Nap de las Américas, con altas velocidades de conexión donde convergen múltiples operadores nacionales e internacionales de telecomunicaciones posibilitando una conectividad a Internet a través de múltiples canales sin exclusividad, lo que garantiza el 100% de conectividad de los servicios hacia el mundo. [9]

4.3. UBICACIÓN ESTRATÉGICA

Construidos en instalaciones dedicadas para el efecto en Quito Sector Carretas y en Guayaquil Sector Campus Prosperina Espol, los Datacenter's proporcionan entre otros, servicios de acceso a Internet y servicios de seguridad lógica.

Estos Datacenter's estarán unidos mediante una red de fibra óptica con capacidad 2 Lambdas (20Gbps) redundante totalmente dedicadas para este propósito, lo que le permite servicios de backups en sitios distintos en caso de que así sean requeridos por tratarse de servicios de misión crítica de nuestros clientes.

4.4. NIVELES DE SERVICIO DE DATA CENTER

A continuación presentamos los niveles de escalamiento del data center



FUENTE (TELCONET, 2013)

4.5. RESUMEN DE CARACTERISTICAS DE LOS TIER

Tabla 3. Características de los Tier

CARACTERISTICAS	QUITO-TIER III	GUAYAQUIL-TIER IV
Tipo de edificio	Independiente (180 RACKS)	Independiente (400 RACKS)
• Personal	24x7x365	24x7x365
• Camino de distribución	1 activo, 1 pasivo	2 activos
• Redundancia	N+1 (Mantenimiento concurrente)	2N (Tolerante a Fallas)
• Climatización		Ininterrumpida
• Puntos únicos de fallo	1 activo, 1 pasivo	Ninguno
• Disponibilidad	Ninguno	99,995%
• Conexión entre DC's	99,982%	2 Lambdas (20Gbps)
	2 Lambdas (20Gbps)	REDUNDANT
	REDUNDANTE	

FUENTE (Vazquez, 2012)

Tabla 4. Arquitectura de los Tier [9]

ARQUITECTONICA	Quito – TIER III	Guayaquil – TIER IV
Suelo Técnico	1300 m ² - Construcción	2500 m ² - Construcción
(reforzado,	450 m ² - Área Útil	1000 m ² - Área Útil
antiestático,	180 racks de capacidad	400 racks de capacidad
antideslizante,		
antielástico).	Jaula dedicada, rack	Jaula dedicada, rack
• Separación de	dedicado, rack Compartido.	dedicado, rack
clientes	Servidores Físicos y	compartido.
	Virtuales	Servidores Físicos y
• Servidores	Espacio para oficinas,	Virtuales
• Otros espacios	aparcamiento, zona de	Espacio para oficinas,
	descarga, almacén.	aparcamiento, zona de
		descarga, almacén.

FUENTE (TELCONET, 2013)

Tabla 5. Energía los Tier [9]

ENERGIA		
• Centro de	1,5 MVA	11,5 MVA
Transformación	UPS escalables de 200 Kva en	UPS escalables de
• Sistemas de	configuración 2N+1	200 Kva en
alimentación		configuración
Ininterrumpida	Grupo de 450 Kva y cuadro	2N+1
	automático de puesta en	Grupo de 450
• Grupo electrógeno	marcha (2N)	CONTINUA 

<p>• Suministro de corriente continua</p>	<p>Grupo Rectificador + Baterías (2N)</p>	<p>Kva y cuadro automático de puesta en marcha(2N) Grupo Rectificador + Baterías(2N)</p>
--	---	--

FUENTE (Relica, 2014)

Tabla 6. Ambiente de los Tier [9]

AMBIENTE		
<p>• Parámetros de control ambiental</p>	<p>Temperatura controlada de 21°C + - 1.5°C y humedad relativa del 40% (+/-10%)</p>	<p>Temperatura controlada de 21°C + - 1.5°C y humedad relativa del 40% (+/- 10%)</p>
<p>•Refrigeración de salas</p>	<p>Aire acondicionado redundante independiente en cada sala en Configuración 2N rotativo.</p>	<p>Aire acondicionado redundante independiente en cada sala en configuración 2N rotativo.</p>

FUENTE (TELCONET, 2013)

4.6. RESUMEN DE CARACTERÍSTICAS DE SEGURIDAD DE LA NUBE

Tabla 7. Resumen de Características de Seguridad de los Tier

SEGURIDAD	Quito – TIER III	Guayaquil – TIER IV
Control de incendios	<p>Sistema de detección constituido por detectores iónicos de humos y gases de combustión.</p> <p>Zonas de detección controladas por central analógica micro procesada modular con plena autonomía de señalización, centralización de fuego y avería.</p> <p>Agente extintor ECARO – 25</p>	<p>Sistema de detección constituido por detectores iónicos de humos y gases de combustión.</p> <p>Zonas de detección controladas por central analógica micro procesada modular con plena autonomía de señalización, centralización de fuego y avería. Agente extintor ECARO – 25</p> <p>• Equipo de seguridad 24x7x365</p>
• Seguridad con personal	• Equipo de seguridad 24x7x365	• Total cobertura de zonas externas e internas
• Circuito cerrado de televisión	• Total cobertura de zonas externas e internas	<p>CONTINUA</p> 

<ul style="list-style-type: none"> • Control de accesos • Grabación digital de las imágenes Iluminación sorpresiva 	<ul style="list-style-type: none"> • Control de accesos biométricos con lectores de tarjetas de proximidad. • Registro de accesos a los Datacenters 	<p>Control de accesos biométricos con lectores de tarjetas de proximidad.</p> <ul style="list-style-type: none"> • Registro de accesos a los Datacenters
<p>Gestión del edificio</p>	<p>Sistema de seguimiento que supervisa las alarmas eléctricas, mecánicas, de temperatura, de humedad, de incendios, de seguridad, de control de accesos y de temperatura de racks de clientes</p>	<p>Sistema de seguimiento que supervisa las alarmas eléctricas, mecánicas, de temperatura, de humedad, de incendios, de seguridad, de control de accesos y de temperatura de racks de clientes</p>

FUENTE (TELCONET, 2013)

Tabla 8. Tipos de Conectividad y Servicios

CONECTIVIDAD REDUNDANTE	
<ul style="list-style-type: none"> • Conectividad • Gestión de ancho de banda 	<p>Conexiones redundantes y de gran ancho de banda a nivel interno del país y hacia el mundo apoyadas en la infraestructura CARRIER de Telconet.</p> <p>Gestión de ancho de banda flexible, escalable y basada en sistemas de alta disponibilidad.</p>
Servicios Profesionales	
<ul style="list-style-type: none"> • Soporte a la instalación • Servicio manos remotas 24x7x365 • Administración de sistemas • Copias de seguridad y recuperación 	<p>Soporte en la instalación de equipos, cableados y otros hardware pasivos</p> <p>Disponible acciones de reinicio de servidores, cambios de soportes, verificación de cables y otras actuaciones guiadas</p> <p>Equipo de administraciones de sistemas a disposición de los clientes en horario 8x5</p> <p>Servicios de back up centralizado, online backup y restauración</p>

FUENTE (TELCONET, 2013)

DISTINCIÓN

Los Datacenter's se distinguen en cuanto a servicios, disponibilidad y calidad:

- Disponibilidad máxima de servicios
- Especialización tecnológica y servicios
- Seguridad lógica y física
- Calidad en las condiciones de entorno y en la conectividad a internet.
- Flexibilidad y escalabilidad para el crecimiento de los clientes.

BENEFICIOS QUE POSEE

Como operación y Mantenimiento controlados en un Datacenter Certificado por Uptime Institute., pues posee beneficios en los diseños pre-certificados. Adicional contiene la mayor conectividad neutral, ductos construidos de acceso para otros.

El cliente tiene la posibilidad de elegir espacios en renta o servicios en cualquiera de los dos Datacenter's. Además tendrá aseguramiento de los esfuerzos técnicos comerciales de servicios dando factibilidad para que el cliente se enfoque completamente a su negocio.

RESPONSABILIDAD

Tiene la responsabilidad de operación del Negocio respecto a:

- Producción.
- Realización de todas y cada una de las tareas del negocio.
- Calidad y cantidad con la eficiencia y mejora continua.

- Administración de nuevos servicios o clientes. (Vazquez, 2012)

INFRAESTRUCTURA

Posee infraestructura que se la detalla a continuación.

- Sala de Equipos Dataroom
- Sala de Operadores
- Sala de Sistemas
- Bóveda
- Sistema de Energía Eléctrica
- Equipos de Comunicaciones
- Equipos Computacionales
- Sistemas Computacionales

SALA DE EQUIPOS DATAROOM

Para la sala de equipos tienen y es necesario:

- Piso elevado
- Cabina Aislada
- Módulos de Rack
- Cámaras de Seguridad
- Sistema de Gas Antifuego
- Sistema de Rociadores Sprinklers
- Sistema de Alarmas de Incendio
- Sistema de Climatización (TELCONET, 2013)

EQUIPOS COMPUTACIONALES EXTERNOS SERVICIO HOUSING O

SITIO CONTINGENCIA

- Servidores
- Ordenador central
- Unidad de Cintas de Respaldo
- Unidad de Storage
- Unidad de Discos Duros

SISTEMAS COMPUTACIONALES

- Sistemas Operativos (contraseñas)
- Firmware complemento del sistema operativo
- Software de Explotación
- Aplicativos de la Gestión (soporte al negocio office)
- Aplicativos del negocio Sistemas. (TELCONET, 2013)

4.7.NORMA TIA-942

Brinda los requerimientos y lineamientos necesarios para el diseño e instalación de Data Center o centros de cómputo. Aprobado por:

- TIA (Telecommunications Industry Association)
- ANSI (American National Standards Institute)

REQUERIMIENTOS DE LOS DIFERENTES ELEMENTOS DE UN DATACENTER

- Estructura
- Ubicación
- Acceso
- Protección contra incendios
- Equipos
- Redundancia

4.8. DISPONIBILIDAD

Tier	% disponibilidad	% de parada	Tiempo de parada a año.
Tier I	99.671 %	0.329 %	28.82 horas
Tier II	99.741 %	0.251 %	22.68 horas
Tier III	99.982 %	0.018 %	1.57 horas
Tier IV	99.995 %	0.005 %	52.56 minutos

FIG. 4.8.1. Disponibilidad

FUENTE (TELCONET, 2013)

PERSPECTIVA DEL CLIENTE

La perspectiva que tiene el cliente para que su servicio sea bueno es la disponibilidad de servicios, que posea confiabilidad en la infraestructura a bajos costos y que se brinde un soporte completo y de buena calidad cuando se pierde el mismo.

APRENDIZAJE Y CRECIMIENTO

- Flexibilidad en la infraestructura de la Tecnología de la Información
- Controlar los cambios de servicio e infraestructuras
- Adaptabilidad a la demanda cambiante en el negocio
- Comunicación y transferencia de conocimiento
- Productividad del negocio en relación con los costos

ITSM (GESTIÓN DE SERVICIO DE LA TECNOLOGÍA DE LA INFORMACIÓN)

Está dividido en dos áreas principales:

- **SOPORTE DE SERVICIO:** Provisión de servicios en forma efectiva.
- **ENTREGA DE SERVICIO:** Administración de los servicios de IT, garantizando proveer el servicio acordado con el cliente

Tabla 9. Soporte de Servicio [10]

SOPORTE DE SERVICIO	Administración de Configuración
	Servicio de Escritorio
	Administración de Incidentes y Problemas
	Administración de Cambios
	Administración de Release

FUENTE (Relica, 2014)

Tabla 10. Entrega de Servicio [10]

ENTREGA DE SERVICIO	Administración de Disponibilidad
	Administración de Capacidad
	Administración Continua de Servicios TI
	Administración Financiera de Servicios TI
	Administración de los Niveles de Servicios
	Administración de las Relaciones con los Clientes (CRM)

FUENTE (Relica, 2014)

NORMA ISO 17799/27001**DOMINIOS DE CONTROL**

- Política de Seguridad
- Aspectos organizacionales para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de Accesos
- Desarrollo y mantenimiento de sistemas

- Gestión de continuidad de negocio
- Conformidad con la legislación

VENTAJAS

- Aumento de la seguridad efectiva de los sistemas de información
- Correcta planificación y gestión de la seguridad
- Garantías de continuidad del negocio
- Mejora continua a través del proceso de auditoría interna
- Incremento de los niveles de confianza de nuestros clientes
- Aumento del valor comercial y mejora de la imagen de la organización

(Vazquez, 2012)

CAPITULO V

PARÁMETROS DE CALIDAD EN SERVICIOS CLOUD COMPUTING

5.1 VIRTUALIZACIÓN

La virtualización consiste en la capacidad de separar el software del sistema operativo, las aplicaciones informáticas de los sistemas físicos o hardware en los que están instalados. Esta característica aplicada al Cloud Computing se materializa en que el usuario no tiene que preocuparse por la implementación concreta de los servicios de la nube ni tener en cuenta el hardware asociado a ellos o que, supongan grandes cambios en las aplicaciones instaladas.

Por otra parte, la virtualización posibilita una optimización respecto al aprovechamiento de los recursos comunes, ya que permite que las aplicaciones sean independientes del hardware en el que se ejecutan como que varias aplicaciones pueden ejecutarse en una misma máquina o una aplicación puede usar varias máquinas a la vez.

El principal aspecto a tener en cuenta a la hora de utilizar recursos virtualizado y que las empresas que contratan servicios de Cloud deben tener en cuenta es que les deben garantizar la seguridad de la información en esos entornos. Para ello, es necesario establecer controles adecuados de acceso y gestión segura de la información en cada uno de los niveles informáticos del entorno virtualizado, que estará compartido por muchos usuarios.

En términos económicos, se dice que ambas características, virtualización y escalabilidad, aumentan la elasticidad del sistema, ya que los costos asociados al uso de los recursos se adaptan mejor a las necesidades de cada momento. (Daniele.catteddu, 2009)

5.2 ESCALABILIDAD

La escalabilidad es posiblemente la característica más destacable del Cloud Computing. Consiste en la capacidad de adaptar fácilmente los recursos a utilizar en función de las necesidades de cada momento y la variación de la demanda. Gracias a la escalabilidad, los recursos que ofrecen los proveedores de servicios a sus clientes se adaptan dinámicamente a las necesidades de la empresa, consiguiendo que el servicio sea lo más eficiente posible.

Esto permite ofrecer una mayor capacidad cuando sea necesario, permitiendo a su vez un ahorro de costos notable, ya que la ampliación y adaptación en sistemas Cloud es más económica que en sistemas tradicionales, puesto que se ahorran costos en equipos o en software propietario. (Quesada, 2011)

Así, un sistema escalable que adapte los recursos a la demanda en cada instante, permite eliminar el exceso de aprovisionamiento de recursos para los momentos de mayor intensidad de acceso, el cual sería innecesario el resto del tiempo

5.3. INFRAESTRUCTURA COMO SERVICIO

El proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero. Tal vez se pueda decir que éste es el modelo más primitivo de *nube*, que se inició con los sitios de Internet que proporcionaban capacidad de almacenamiento masivo a través de la red y los servidores de alojamiento web (Gomez, 2011)

5.4. PARAMETROS TECNICOS

5.4.1. NIVEL DE SERVICIO IAAS

El proveedor de servicios *IaaS* ofrece una infraestructura informática para determinados Sistemas Operativos y *software* como son bases de datos, alojamiento *Web*, entornos de desarrollo de aplicaciones, servidores de aplicaciones, codificación y *streaming* de vídeo, la empresa que pasara a ser nuestro usuario debe tener en cuenta que no podrá incorporar otros sistemas particulares de su solución.

- **VIRTUALIZACIÓN EN IAAS**

Los usuarios pueden desplegar máquinas virtuales en la infraestructura física de *IaaS* en muy poco tiempo, en algunos casos, en pocos minutos, por lo que se reduce significativamente el tiempo y costo puesto en marcha de nuevos sistemas. Además, la capacidad de ampliación de recursos de hardware es menos costosa y rápida que en el caso tradicional.

Por otro lado, la disponibilidad y calidad de servicio ofrecidos en *IaaS* suelen estar garantizado durante casi todo el tiempo de utilización, ofreciendo soluciones alternativas en el caso de faltar el servicio.

Así, uno de los aspectos importantes de la virtualización para que una empresa piense en optar por *IaaS* sería conseguir una reducción significativa de la inversión en recursos para garantizar la disponibilidad del sistema, que generalmente consiste en la adquisición de sistemas físicos redundantes para evitar pérdidas de servicios que habitualmente no se usan.

Otro aspecto estratégico a tener en cuenta es el hecho de que la deslocalización física del *hardware* utilizado junto con el uso de redes privadas virtuales (VPN) posibilita el acceso simultáneo y seguro de múltiples empleados de la organización a los sistemas con mayor facilidad de disponer alta velocidad de conexión. (Gomez, 2011)

5.4.2. NIVEL DE SERVICIO PAAS

A la hora de crear las aplicaciones que posteriormente se encontraran en los sistemas *PaaS*, hay que tener en cuenta que la tecnología a usar en las mismas debe ser compatible con dichos sistemas.

En general, la tecnología estará basada en estándares internacionales, pero el rango de funciones que ofrece puede ser bastante limitado en ciertos casos. Esto puede reducir el rendimiento de determinadas aplicaciones.

Por otro lado, las plataformas *PaaS* permiten ampliar fácilmente los recursos disponibles para la aplicación ya que, por ejemplo, se usan sistemas de ficheros y bases de datos específicas para ello.

Sin embargo, la gestión de la información en estos sistemas es bastante compleja, por lo que en la práctica se confía parte de ese control al proveedor de servicios. Se deberá conocer hasta qué punto la información gestionada es crítica, y qué niveles de seguridad se establecerán. Esto obliga al proveedor a suministrar información sobre la estructura de los datos.

Finalmente, la gestión de las aplicaciones una vez situadas en las máquinas de *PaaS* suele ser más sencilla que en las instalaciones tradicionales, pero se dispone de menor control de todos los sistemas.

- **VIRTUALIZACIÓN PAAS**

Con *PaaS* se ofrecen soluciones de almacenamiento y computación para los desarrolladores de software accesibles independientemente de la ubicación, adoptando así herramientas de escalabilidad y flexibilidad de configuración sin que los usuarios de la plataforma necesiten mantener la tecnología que se encuentran utilizando ni los recursos de los mismos.

5.4.3. NIVEL DE SERVICIO SAAS

Las aplicaciones informáticas *SaaS* suelen ofrecer cierta flexibilidad de configuración para su adaptación a las necesidades del cliente. Sin embargo, existen empresas que necesitan aplicaciones muy particulares, cuya adaptación es a partir de *software SaaS* que es demasiado costosa directamente para los proveedores de servicios. En esos casos, esas empresas deberán desarrollar un *software* específico.

Otro factor a considerar es el tipo y la cantidad de datos a transmitir a las aplicaciones de la empresa. Habitualmente, las redes de comunicaciones ofrecen altas velocidades de transmisión de datos en sus instalaciones, y menores velocidades en su acceso a Internet.

Si se utiliza una aplicación *SaaS*, se ha de considerar que se deberá acceder a Internet para transmitir información. Para mejorar la calidad de transmisión de la información, las aplicaciones *SaaS* sólo transmiten la información estrictamente

necesaria también llamada solución basada en caché o agrupan la información para transmitirla en el momento óptimo y seguro. (Gomez, 2011)

- **VIRTUALIZACIÓN SAAS**

En algunas empresas se presenta cierta resistencia a que las funcionalidades de gestión de la empresa se externalicen hacia sistemas en Internet. Sin embargo, se pueden realizar proyectos de prueba en los que se analicen las mejoras que puede aportar a la empresa el uso de estos sistemas *SaaS*.

Para mejor servicio los proveedores de *SaaS* ofrecen a menudo periodos de prueba para que las empresas puedan realizar estos análisis y de esta manera verificar si cubren las necesidades de dichos clientes. (Gomez, 2011)

5.4.4. CARACTERÍSTICAS GENERALES

- **SEGURIDAD EN LA GESTIÓN DE LA INFORMACIÓN**

Dado que la información de la organización se transmitirá a través de Internet, es necesario establecer un sistema seguro de comunicaciones contra posibles amenazas o corrupción de los datos.

Para garantizar la seguridad, en ciertos casos la información deberá estar encriptadas o protegida. Por otra parte, no se puede pensar que controlar los datos es sólo una cuestión técnica, también es algo procedimental: no se deben firmar

contratos de exención de responsabilidades o delegar absolutamente todo en los proveedores como la mejor forma de gestionar la seguridad.

Por otra parte, siempre se debe garantizar el acceso autorizado a la información gestionada en la nube. Para ello, los usuarios deben disponer de un inventario de la información aportada al proveedor de Cloud Computing, garantizando que esa información está correctamente clasificada. (Leon, 2010)

➤ **VENTAJAS DE LA ESCALA**

En pocas palabras, todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. Por tanto, la misma cantidad de inversión en seguridad puede obtener una mejor protección.

Aquí quedan incluidas las distintas medidas defensivas, como el filtrado, la administración de parches, el refuerzo de máquinas virtuales, los recursos humanos y su gestión y control, la redundancia de hardware y software, los sistemas de autenticación seguros, un control eficaz basado en funciones y soluciones federadas de gestión de la identidad por defecto, que también mejora los efectos de red de la colaboración de varios socios implicados en la defensa.

➤ **UBICACIONES MÚLTIPLES**

La mayoría de proveedores en nube cuentan con los recursos económicos necesarios para replicar el contenido en ubicaciones múltiples por defecto. De este

modo se aumenta la redundancia y la independencia de los errores y se proporciona un grado de recuperación de desastres listo para su uso.

- **MEJORA DEL TIEMPO DE RESPUESTA A LOS INCIDENTES**

Los sistemas a mayor escala gestionados satisfactoriamente, por ejemplo, a raíz de la detección temprana de nuevos despliegues de programas maliciosos, pueden desarrollar capacidades más eficaces de respuesta ante incidentes.

- **GESTIÓN DE AMENAZAS**

Los proveedores en nube también pueden permitirse contratar a especialistas para que se ocupen de las amenazas concretas a la seguridad, mientras que las compañías más pequeñas sólo se pueden permitir los servicios de un número reducido de profesionales generalistas. (Quesada, 2011)

- **ESCALABILIDAD RÁPIDA E INTELIGENTE DE RECURSOS**

La lista de recursos en nube que pueden ser escalados rápidamente bajo demanda ya incluye, entre otros, el almacenamiento, el tiempo de CPU, la memoria, las solicitudes de servicios web y las máquinas virtuales, y el nivel de control granular sobre el consumo de recursos aumenta a medida que las tecnologías mejoran.

Un proveedor en nube tiene potencial para reasignar recursos de manera dinámica para el filtrado, la catalogación de tráfico, la codificación, etc., con vistas a

incrementar el apoyo a las medidas defensivas (por ejemplo, frente a los ataques distribuidos de denegación de servicio (DDoS) cuando un ataque está produciéndose o puede producirse.

Cuando esta capacidad de reasignación dinámica de recursos se combina con métodos adecuados de optimización de recursos, el proveedor en nube puede limitar las posibles consecuencias de determinados ataques sobre la disponibilidad de los recursos que utilizan los servicios alojados legítimamente, así como reducir el impacto del incremento de uso de los recursos por la defensa de seguridad para hacer frente a dichos ataques.

Sin embargo, para lograr este efecto, el proveedor debe aplicar una coordinación adecuada de la autonomía para la defensa de seguridad y para la gestión y optimización de los recursos.

La capacidad de escalar dinámicamente los recursos defensivos bajo demanda posee ventajas evidentes con respecto a la resistencia a los fallos.

Además, cuanto mayor escalada de los distintos tipos de recursos individuales de manera granular sin escalar la totalidad de los recursos del sistema, más barato será responder a los picos repentinos no maliciosos de demanda. (Quesada, 2011)

➤ PORTABILIDAD DE LA INFORMACIÓN

Las soluciones que ofrecen los proveedores de *Cloud Computing* pueden clasificarse como abiertas a la portabilidad o cerradas a la misma. Se podrá considerar una solución abierta a la portabilidad cuanto mayor sea la facilidad de un usuario para transferir todos sus datos y aplicaciones desde un proveedor a otro o a los sistemas propiedad del cliente, garantizando la disponibilidad de los datos y la continuidad del servicio.

Hay que tener en cuenta que el fin de la relación con el proveedor de *cloud* puede darse no sólo en el caso de desacuerdo legal del contrato por parte del cliente sino por otras circunstancias ajenas al mismo, como podría ser el fin de la prestación de algún tipo de servicio por parte del proveedor, el cambio de su política comercial o del marco regulatorio. Es entonces un aspecto importante que debe tenerse en cuenta a la hora de utilizar servicios de *cloud*, sobre todo públicos, pues cuanto más cerrado a la portabilidad sea el proveedor mayor será la dificultad, o incluso imposibilidad, de poder realizar esa transferencia a un costo razonable que se encuentre al alcance del cliente del proveedor.

➤ LOCALIZACIÓN DEL PROCESO Y DE LOS DATOS

El proveedor de *Cloud Computing*, a la hora de implementar los servicios al usuario final, puede ser el prestador único de los mismos cuando todos los recursos para proporcionarlos pertenecen al propio proveedor. Es decir, dispone de toda la

infraestructura necesaria, que administra directamente, y no subcontrata a terceros en función de la distinta carga de trabajo que tenga.

A la hora de decantarse por la utilización de un servicio de *Cloud Computing*, hay otros condicionantes que hay que tener en cuenta desde el punto de vista de los derechos de los ciudadanos y del ejercicio de las responsabilidades del cliente de dichos servicios.

Es importante identificar qué proveedores de *Cloud* están localizados dentro del Espacio Económico Europeo o en países que de una u otra forma garanticen un nivel adecuado de protección de los datos de carácter personal. Esta localización afecta no sólo a la sede del proveedor de *Cloud*, sino también a la localización de cada uno de los recursos físicos que emplea para implementar el servicio, de forma directa o subcontratada. Y hay que enfatizar que hay que tener en cuenta la localización de todos los recursos pues, por la misma naturaleza del servicio de *Cloud*, los datos pueden estar en cualquier momento en cualquier sitio, pero los derechos y obligaciones relativos a dichos datos han de garantizarse siempre. (Gomez, 2011)

- **SEGURIDAD POR PARTE DEL PROVEEDOR**

El proveedor de servicios y recursos en la nube es el encargado de dar toda la seguridad correspondiente a la parte física y al software de cada aplicación. En lo que se refiere a la parte física, debe garantizar que los centros de procesos de datos estén protegidos ante cualquier amenaza de robo o daño, además de que deberá mantener

los equipos actualizados y con el correspondiente mantenimiento para evitar cualquier daño y por ende pérdida de información.

Para garantizar el correcto funcionamiento de los servicios en la nube, los proveedores usan mecanismo de virtualización y segmentación de datos para dar una seguridad más completa a los datos y aplicaciones de sus clientes. (Daniele.catteddu, 2009)

La virtualización da la posibilidad de tener varias máquinas virtuales ejecutando diferentes aplicaciones y servicios en un mismo servidor, y cada una ejecutando un sistema operativo diferente de forma aislada.

El espacio de memoria es controlado por un hipervisor²⁵, por lo que el proveedor debe encargarse del control y eliminación del software malintencionado que pretenda burlar la acción del supervisor para tener acceso a las máquinas virtuales. Otro punto vulnerable es la localización de los datos de los clientes, por lo que el proveedor debe utilizar mecanismos de protección como servidores de almacenamiento a manera de backups originales.

Además, en la parte de Software debe garantizar seguridad a los usuarios que hagan uso de las aplicaciones y programas; por lo tanto, como mecanismos adicionales de seguridad que el proveedor debe garantizar a los clientes tenemos. (Gomez, 2011)

- **CRIPTOGRAFÍA**

Mediante la técnica de cifrado de datos realizar la protección de las conexiones de red entre los usuarios y las aplicaciones de la nube, permitiendo que todos los datos que viajen en este canal de comunicación se encuentren cifrados, impidiendo su acceso a terceras personas.

- **CONSIDERACIONES POR PARTE DEL CLIENTE**

Como seguridad por parte del cliente, se debe considerar el tipo de nube que contrate según su necesidad:

- **CONTROL PERIMETRAL**

Mediante la instalación y configuración de un firewall para monitorizar la comunicación de los usuarios de la empresa hacia la nube o viceversa, y decidir si permite o no el paso de información, según las configuraciones realizadas.

- **IDS (INTRUSIÓN DETECCIÓN SISTEMAS)**

Instalación y configuración de un sistema de detección de intrusos, de manera que bloquee o permita conexiones de los usuarios hacia la nube contratada, de manera que puedan ser analizadas para determinar si alguna conexión es portadora de contenido peligroso para la red.

Por lo que la seguridad en la nube sigue siendo un reto tanto para las empresas como para los clientes de *Cloud Computing*. En donde se debe considerar el rendimiento, buen manejo y control de los datos para tener una administración segura de la nube y evitar que sea atacada por riesgos inminentes

- **CONDICIONES EN QUE SE PRESTA EL SERVICIO**

Debe verificarse de forma previa a la contratación las condiciones en la que se presta el servicio con el fin de determinar si ofrecen un nivel adecuado de cumplimiento.

Las condiciones ofrecidas por los proveedores se deben contrastar con una lista de control que incluya, entre otros, elementos relativos a la información proporcionada, ubicación del tratamiento, existencia de subencargados, políticas de seguridad, derechos del usuario y obligaciones legales del prestador del servicio.

Es aconsejable comparar las características ofrecidas por varios proveedores, no sólo en términos económicos sino también en relación con los contenidos de la prestación y las garantías de calidad y cumplimiento legal que cada proveedor proporciona. En cualquier caso, debe prestarse especial atención a no contratar servicios prestados en *nube* que no reúnan los requisitos legalmente establecidos.

Tener en consideración los procedimientos de salida en caso de cambio de proveedor facilitará que los procesos de retorno de datos se lleven a cabo sin merma de la integridad de los datos y con control pleno del responsable sobre su destino

ulterior. En este ámbito son de especial importancia los sistemas que el proveedor proporcione para asegurar, en todo momento, la portabilidad de esos datos. (Gomez, 2011)

Pues si bien es cierto el presente estudio pretende facilitar el cumplimiento de la normativa de protección de datos en la contratación de servicios de *Cloud Computing* ofreciendo una información práctica dirigida a, microempresas y profesionales. Asimismo se informa sobre las características específicas de la contratación en las Administraciones Públicas. (Gomez, 2011)

5.5.PARÁMETROS ECONÓMICOS

5.5.1. NIVEL DE SERVICIO IASS

El costo de utilización de los servicios *IaaS* sigue varios modelos para la prestación del mismo como son:

En el primer modelo se cobra una tarifa fija por hora y unidad de recursos utilizados. Esto es útil para aplicaciones poco probadas en las que el consumo sea impredecible.

En el segundo, se ofrece la posibilidad de disponer de un recurso reservado, con un pequeño coste, y un cobro por el uso posterior. Suele emplearse en aplicaciones con un uso predecible y que necesiten de capacidad reservada, incluyendo recuperación ante desastres.

En otros modelos, se paga en función del uso instantáneo que se haga de los recursos. Este último caso es adecuado cuando se necesita una alta flexibilidad de los recursos en determinados momentos, por ejemplo, grandes consumos en momentos determinados del día no predecibles. Habitualmente, se pueden combinar estos modelos para adaptarlos a las necesidades específicas del usuario.

5.5.2. NIVEL DE SERVICIO PAAS

Los proveedores *PaaS* habitualmente ofrecen un periodo de pruebas sin costo en los que los usuarios pueden comprobar las ventajas competitivas que pueden encontrar en *PaaS*, o pueden experimentar con nuevas aplicaciones adaptadas a ese tipo de sistemas como evaluación antes de contratarlo. Comúnmente, se ofrece un costo por uso de los recursos del sistema, es decir, se cobra una cantidad fija por cada Giga Byte de almacenamiento, por cada hora de procesamiento o por cada Giga Byte de información transmitida hacia terceros.

Asimismo, para fomentar la implantación de *PaaS* se tiende a ofrecer un servicio gratuito limitado a una cantidad diaria de uso, a partir del cual se realiza el cobro según se ha descrito. (Gutiérrez, 10 junio del 2013)

5.5.3. NIVEL DE SERVICIO SAAS

Las aplicaciones tradicionales tienen un costo inicial alto basado en la adquisición de las licencias para cada usuario. Estas licencias suelen ser abiertas, es decir, no presentan restricciones temporales a su uso.

En cambio, para las aplicaciones *SaaS* el costo se basa en el uso, no en el número de usuarios, y el gasto de mantenimiento es nulo, ya que la las aplicaciones las gestiona el propio proveedor. Un modelo más equilibrado entre ambos podría ser el uso de sistemas basados en un uso ilimitado durante un periodo de tiempo.

5.6.PARAMETROS LEGALES

Pues ya que en la actualidad no se encuentran normativas vigentes que puedan regir completamente este tipo de servicio presentamos algunos aspectos importantes legales para cada modelo para tener en cuenta como se debe realizar la contratación.

5.6.1. NIVEL DE SERVICIO IASS

El uso de *IaaS* obliga a sus usuarios a que no exijan la localización en todo momento de la ubicación física de la información gestionada. Otra característica a tener en cuenta es que algunos de los proveedores de servicios *IaaS* realizan back-ups o copias de la información que gestionan esta información. Estos dos aspectos son importantes si se gestiona información protegida de carácter personal o empresarial.

5.6.2. NIVEL DE SERVICIO PAAS

Al comenzar a usar los servicios *PaaS*, se establece un acuerdo entre el proveedor y el usuario en el que se describen las condiciones del servicio ofrecido.

Habitualmente, el usuario se compromete a no realizar un uso indebido de los sistemas que se le ofrecen. Por otro lado, el proveedor señala las condiciones de tarificación del servicio, de garantía de acceso y gestión adecuada de la información, y de las garantías legales en caso de errores o desastres en sus sistemas

5.6.3. NIVEL DE SERVICIO SAAS

Algunas organizaciones que operan en varios países están sujetas a legislaciones que exigen la obtención de informes que describan cómo gestionan la información.

Sin embargo, es posible que los proveedores de SaaS no sean capaces de proporcionar esos informes, o de utilizar sistemas de trazabilidad o seguimiento de la información que gestionan. Todo esto debe aparecer claramente especificado en el acuerdo de nivel de servicio. Asimismo, se ha de considerar la capacidad que tienen los proveedores de utilizar sistemas que garanticen la seguridad y privacidad de los datos que gestionan. (Gutiérrez, 10 junio del 2013)

5.6.4. CARACTERÍSTICAS GENERALES

➤ SUBCONTRATACIÓN

Por el contrario, puede no tratarse de un prestador final cuando el servicio que ofrece directamente al usuario se construye sobre la subcontratación a terceros de elementos necesarios para implementarlos ya sea para la parte de hardware, almacenamiento, comunicaciones. A su vez, los subcontratistas pueden subcontratar

de nuevo parte del servicio que proporcionan al prestador final a terceras y sucesivas compañías.

Este es un modelo de cadena de subcontrataciones que en teoría podría no tener fin, y cuyo objeto es redimensionar continuamente los recursos de la *nube* de forma dinámica y en función de las condiciones del mercado.

➤ **TRANSPARENCIA**

En relación al control de la localización de los datos de un usuario, un servicio de *cloud* puede ser auditable o transparente, cuando el contratista puede reclamar información precisa de dónde, cuándo y quién ha almacenado o procesado sus datos (dentro de los recursos propios del proveedor o de la cadena de subcontrataciones), y en qué condiciones de seguridad se ha producido.

En otro caso, nos encontraremos con un servicio opaco al usuario, en el que éste no tiene opción alguna de obtener información precisa de qué ha ocurrido con sus datos ni herramientas para auditar el servicio que se le está proporcionando y en el que su propia información escapa a su control.

• **LAS GARANTÍAS CONTRACTUALES**

La contratación de servicios de *Cloud Computing* se realizará a través de un contrato de prestación de servicios. Resulta imprescindible que ese contrato

incorpore entre sus cláusulas las garantías a las que obliga la Ley Orgánica de Protección de Datos.

Atendiendo a la relación contractual establecida entre el cliente y el proveedor de la *nube*, también este contrato se puede clasificar como negociado o de adhesión.

Podemos decir que un contrato entre el cliente y el proveedor es negociado si el primero tiene, o se le ofrece, la capacidad para fijar las condiciones de contratación en función del tipo de datos que se van a procesar, las medidas de seguridad exigibles, el esquema de subcontratación, la localización de los datos, la portabilidad de los mismos y cualquier otro aspecto de adecuación para la contratación correcta del servicio.

En la mayoría de los casos, sin embargo, lo que se oferta son contratos de adhesión, constituidos por cláusulas contractuales cerradas, en las que el proveedor de *cloud* fija las condiciones con un contrato tipo igual para todos sus clientes, sin que el usuario tenga ninguna opción para negociar sus términos. (Gomez, 2011)

➤ **LA ESCALABILIDAD EN LOS NIVELES DE SERVICIO.**

En pocas palabras, todos los tipos de medidas de seguridad son más baratos cuando se aplican a gran escala. Por tanto, la misma cantidad de inversión en seguridad puede obtener una mejor protección.

Aquí quedan incluidas las distintas medidas defensivas, como el filtrado, la

administración de parches, el refuerzo de máquinas virtuales, los recursos humanos y su gestión y control, la redundancia de hardware y software, los sistemas de autenticación seguros, un control eficaz basado en funciones y soluciones federadas de gestión de la identidad por defecto, que también mejora los efectos de red de la colaboración de varios socios implicados en la defensa.

➤ **RECOMENDACIONES IMPORTANTES EN LAS AREAS JURIDICAS TECNOLÓGICAS Y OPERATIVAS**

A continuación una serie de recomendaciones que sería importante que se tengan en cuenta al momento brindar el servicio basado en *Cloud Computing* implicar en la estrategia *Cloud Computing* a las áreas jurídicas, tecnológicas y operativas para elaborar instrumentos contractuales que se adapten a las necesidades de esta tecnología.

- Pues si bien es ciertos en la actualidad no hay normativas vigentes para este servicio por lo que debemos tomar en cuenta los parámetros que se presentan para la contratación de acuerdo a la necesidad del cliente
- Debe informarse sobre los tipos de *nube* (privada, pública, híbrida) y las distintas modalidades de servicios.
- Con esta información debe decidir para qué datos personales contratará servicios de *Cloud Computing* y cuáles prefiere mantener en sus propios sistemas de información.

- Desarrollar programas de colaboración público-privada y consolidar los estándares tecnológicos comunes y abiertos que permitirán la expansión de esta tecnología en todas las administraciones y organismos públicos.
- Los sectores públicos y privados deberían establecer alianzas y proyectos de colaboración que faciliten el impulso de iniciativas, destinadas a la estandarización tecnológica, la interoperabilidad y la convergencia hacia un ecosistema *Cloud*.
- En los contratos deben acordarse, de forma expresa, las medidas de seguridad aplicadas, las condiciones de acceso a la información, las medidas de contingencia, las cláusulas de subcontratación del servicio y las condiciones de finalización del contrato y devolución de los activos y servicios contratados.
- Los proveedores deben garantizar, a través del contrato o de acuerdos de nivel de servicio, el cumplimiento de políticas de seguridad basadas en estándares auditables y someterse a controles y revisiones de terceros que certifiquen el cumplimiento de estas políticas.
- Se debe garantizar mediante auditoría o certificado de destrucción/borrado que el proveedor cancela y elimina los datos pertenecientes a la Administración pública implicada en la finalización del contrato.

- El contrato debe estar sometido a cláusulas de penalización en caso de incumplimiento de los acuerdos de nivel de servicio establecidos.
- La incorporación de la obligación del proveedor de contratar un seguro de responsabilidad civil es una práctica recomendable cuando la criticidad del servicio, o de la información transferida, lo requiere.

CONCLUSIONES Y RECOMENDACIONES

A continuación detallamos algunas conclusiones importantes que debemos tomar en cuenta para la contratación del servicio de Cloud Computing.

- Concluimos que la nueva tecnología como lo es el Cloud Computing tiene un gran auge a nivel empresarial ya que permite una mayor agilidad y eficiencia de la información digital, a través de una implantación sencilla y flexible.
- Concluimos que los niveles de servicio que nos brinda el Cloud Computing es de gran ayuda para portabilidad de los datos, así como ahorro de costos en la infraestructura de una empresa.
- Se concluye que el proveedor debe garantizar la seguridad y la integridad de la información, para prevenir futuras pérdidas de datos de los clientes, y asegurar que el proveedor que brinde este servicio tenga la certificación ISO/CEI 27001
- Concluimos que actualmente no se tiene normativas vigentes en Ecuador para la contratación de Cloud Computing, sino más bien se lleva a cabo por medio un contrato donde se vean beneficiados tanto el cliente como el proveedor, adicional el contrato debe estar sometido a cláusulas de penalización en caso de incumplimiento de los acuerdos de nivel de servicio establecidos.

- Se concluye también que el proveedor es el encargado de realizar los mantenimiento de los equipos ya sea que se haya arrendado un espacio en el Data Center o sea necesario las actualizaciones de los servidores de las aplicaciones para garantizar su correcto funcionamiento.

- Se recomienda informarse acerca de los niveles de servicio que se brinda para poder elegir de mejor manera el nivel que se necesita, y cubrir la necesidad que este presentando la empresa.

- Se recomienda leer detenidamente los Términos y Condiciones del Service Level Agreement (SLA) y evaluar si corresponden con las condiciones que estamos dispuestos a aceptar que se nos brinde el servicio así como también los costos que demanden el mismo.

- Finalmente se recomienda verificar que existan cláusulas al momento de finalizar el servicio, relacionadas con la seguridad de la información involucrada y los requisitos establecidos para su disposición, borrado seguro, devolución, o a su vez el poder cambiar de proveedor.

REFERENCIAS BIBLIOGRÁFICA

- Cerda, P. (17 de Julio de 2012). *Tecnologías Aplicadas*. Obtenido de <http://patriciocerda.com/2012/01/que-es-el-cloud-computing-y-cuales-son.html>
- Daniele.catteddu. (2009). Beneficios, riesgos y recomendaciones para la seguridad de la información. *Computacion en nube*, 141.
- Gomez, M. (2011). Seguridad en Cloud Computing. *INTECO-CERT*, 45.
- Gutiérrez, R. T. (10 junio del 2013). La Tecnología como servicio. *Cloud Computing*, 68.
- Hogan, M., Liu, F., Sokol, A., & Tong, G. (16 de julio de 2011). NIST Cloud Computing. *National Institute of Standards and*, 76.
- Leon, J. d. (2010). Cloud Computing. *Estudio de Cloud Computing*, 68.
- Quesada, C. (2011). Movilidad. *Senior Manager de IT Risk & Assurance de Ernst & Young*, 2.
- Relica, Y. (27 de Febrero de 2014). Análisis Y Evaluación De Parámetros De Calidad En Servicios Cloud Computing En El Ecuador. *Análisis Y Evaluación De Parámetros De Calidad En Servicios Cloud Computing En El Ecuador*. Quito.
- Salas, G. (09 de Abril de 2013). *.securitybydefault.com*. Obtenido de http://www.securitybydefault.com/2013/04/algunos-apuntes-juridicos-sobre-los_9.html
- TELCONET. (15 de NOVIEMBRE de 2013). *PRESENTACION DE DATA CENTER*. Obtenido de <http://www.telconet.net/datacenter>

Vazquez, V. (15 de NOVIEMBRE de 2012). *TELCONET*. Obtenido de

<http://www.telconet.net/>