DEFINICIÓN DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA COMPUTACIÓN EN NUBES PRIVADAS Y COMUNITARIAS.

PROYECTO DE GRADO

ANDRES FELIPE CHACÓN HURTADO
JUAN FEDERICO MAYA SUDUPE

Asesor
ARMANDO ENRIQUE CARVAJAL RODRÍGUEZ
Msc Seguridad de la Información

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

DEFINICIÓN DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA COMPUTACIÓN EN NUBES PRIVADAS Y COMUNITARIAS.

ANDRES FELIPE CHACÓN HURTADO
JUAN FEDERICO MAYA SUDUPE

Trabajo de grado para optar al título de
Maestría en Gestión de Tecnología Informática y Telecomunicaciones

Asesor
ARMANDO ENRIQUE CARVAJAL RODRÍGUEZ
Msc Seguridad de la Información

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, Junio 21 de 2012

CONTENIDO

pág.

RESUMEN **11**

1. INTRODUCCIÓN **13**

1.1 CONTEXTO DE TRABAJO *14*

1.2 PLANTEAMIENTO DEL PROBLEMA *15*

1.3 OBJETIVOS *17*

1.3.1 Objetivo General. 17

1.3.2 Objetivos Específicos: 17

1.4 RESUMEN DEL MODELO PROPUESTO *18*

1.5 RESUMEN DE RESULTADOS OBTENIDOS *21*

1.6 ORGANIZACIÓN DEL DOCUMENTO *22*

2. MARCO TEÓRICO. **23**

2.1 MARCO HISTÓRICO. *23*

2.2 DEFINICIÓN DE COMPUTACIÓN EN LA NUBE. *25*

2.2.1 Características esenciales de la computación en la Nube. 26

2.2.2 Modelos de Servicios. 27

2.2.3 Modelos de Implementación. 28

2.3 VIRTUALIZACION. *29*

2.3.1 Multiposesion. 29

2.3.2 Componentes de la Virtualización. 30

2.4 PREOCUPACIONES POR LA SEGURIDAD DE LA INFORMACION EL LA NUBE. *30*

2.4.1 Desventajas de la Computación en la Nube. 31

2.4.2 Ventajas y Desventajas de Cada Modelo frente a la Seguridad 31

2.5 ESTANDARES Y NORMAS DE SEGURIDAD DE LA INFORMACION 32

2.6 INICIATIVAS DE SEGURIDAD DE LA INFORMACION PARA LA COMPUTACION EN LA NUBE 34

2.6.1 Cloud Security Alliance 34

2.6.2 ISO/IEC NP 27017-2 34

3. MODELO PROPUESTO 36

3.1 LEVANTAMIENTO DE INFORMACION 36

3.2 SELECCIÓN DE RIESGOS 38

3.3 EVALUACION DEL RIESGO 41

3.4 DIVISION DE RESPONSABILIDADES 43

3.4.1 Responsabilidad por la Seguridad por Parte del Proveedor 44

3.4.2 Responsabilidad por la Seguridad por Parte del Cliente 45

3.5 RIESGOS 45

3.5.1 Gestión 46

3.5.2 Centro de Datos 47

3.5.3 Hardware y Redes de Computación 47

3.5.4 Capa Virtual 48

3.5.5 Aplicaciones 48

3.5.6 Información y servicios 49

4. VALIDACIÓN DE LA PROPUESTA 50

5. RESULTADOS OBTENIDOS 52

5.1 CONTROLES 55

5.1.1 Controles de Gestión 55

5.1.2 Controles de Centro de Datos o Infraestructura 63

5.1.3 Controles de Hardware de Red y Computación. 64
5.1.4 Controles de Capa Virtual 65
5.1.5 Controles de las Aplicaciones 66
5.1.6 Controles de la Información y Servicios 68

6. CONCLUSIONES Y FUTURO TRABAJO 70

BIBLIOGRAFIA 72

GLOSARIO 75

ACRONIMOS 76

ANEXOS 768

LISTA DE CUADROS

pág.

Tabla1. Modelos de Despliegue de la Computación en la Nube.....28

Tabla 2. Responsabilidad por Parte del Proveedor.....45

Tabla 3. Resumen Controles vs Marcos de Seguridad… 55

LISTA DE FIGURAS

pág.

Figura 1. Uso de la Computación en la Nube. 13
Figura 2. Principales Amenazas de la Nube. 15
Figura 3. Razones para no usar Computación en la Nube. 16
Figura 4. Tiempo de Adopción de la Computación en la Nube. 17
Figura 5. Dominios del Modelo de Seguridad de Computación en la Nube. 19
Figura 6. Taxonomía de la Computación en la Nube. 25
Figura 7. Características, Modelos de Servicios y Despliegue de la Computación en la Nube. 26
Figura 8. Multiposesion. 29
Figura 9. Modelo de Computación en la Nube. 32
Figura 10. Modelo de Levantamiento de Información. 38
Figura 11. Dominios del Modelo de Seguridad de Computación en la Nube. 39
Figura 12. Modelo de Evaluación de Riesgos. 42
Figura 13. Actores Responsables de la Seguridad 43
Figura 14. División de Responsabilidades para Cada Modelo de Servicios 44
Figura 15. Validación Promedio del Modelo 51
Figura 16. Validación de Resultados por Juicio de Expertos 51
Figura 17. Clasificación Riesgos y Controles por Dominio. 52
Figura 18. Clasificación Riesgos y Controles Dominio de Gestión 53
Figura 19. Controles por Marcos de Referencia 54

LISTA DE ANEXOS

pág.

Anexo 1. Hoja de Evaluación. 78

RESUMEN

En los últimos años, la computación en la nube ha tenido un incremento en su utilización. Se espera que dentro de los próximos 5 a 10 años este modelo de despliegue de servicios esté en una fase de producción, y que no sea de uso exclusivo de expertos en tecnologías de información y comunicaciones, sino también de académicos, empresarios y personas comunes que se vean atraídos por las ventajas ofrecidas por este modelo. La seguridad de la información es uno de los aspectos que más preocupan a los directivos de TI para migrar sus aplicaciones e información a la nube, debido a que están confiando sus datos privados a un tercero. Por este motivo, las organizaciones toman medidas que garanticen el control de su información y que minimicen los riesgos que la pueden impactar, basándose en estándares de seguridad pensados para la computación tradicional. Existen iniciativas y marcos de trabajo, tales como PCI o CSA, que pueden aportar información, pero al no haber un modelo completo de seguridad para la computación en la nube, existe la posibilidad de no hacer consciencia de los diferentes riesgos, o tratarlos de forma inadecuada.

La computación en la nube se puede caracterizar de varias formas: una, según el modelo de servicio que puede ser software como servicio (SaaS), plataforma como servicio (PaaS) o infraestructura como servicio (IaaS); otra, según el modelo de implementación, que puede ser público, privado, comunitario o híbrido. Se diferencian en el uso que se les da y el tipo de cliente que tienen.

El modelo propuesto en este trabajo se basa en implementaciones de computación en nubes privadas y comunitarias sin importar el modelo de servicio, aunque dependiendo del modelo, las responsabilidades sobre la aplicación de los controles cambian y se deben analizar individualmente.

Los riesgos fueron elaborados con el método de estructura de división de riesgo – RBS (HILLSON, 2002). Los riesgos principales fueron asociados a las características de la información como la disponibilidad, integridad y confidencialidad (ISO, ISO/IEC 27001, 2005), lo que implica riesgos de acceso no autorizado a la información a través de las diferentes capas del modelo, por la no independencia de los sistemas, la multiposesión, y por información residual mal manejada. Otra clase de riesgos que se encuentran son los relacionados con los servicios, en ellos los impactos más importante son la disponibilidad y los umbrales de aceptación.

Para tratar estos riesgos se definieron unos dominios que agrupan los diferentes controles que son los de gestión, aspectos legales, cumplimiento, control de acceso, gestión de la continuidad del negocio, operación del servicio, centro de

datos, hardware y redes de computación, capa virtual, aplicaciones, e información y servicios.

1. INTRODUCCIÓN

El término “Computación en la nube” es muy utilizado hoy en día, pero, ¿en qué consiste? Es un nuevo paradigma cuya madurez aún está en estado de desarrollo (Ver Figura 1), que está cambiando el modelo de la computación tradicional y ha migrado a lugares etéreos los datos, el procesamiento y las aplicaciones.

Básicamente es un conjunto de recursos de hardware y software, que pueden ser entregados para su uso de una manera rápida y sin necesidad de una gran administración.

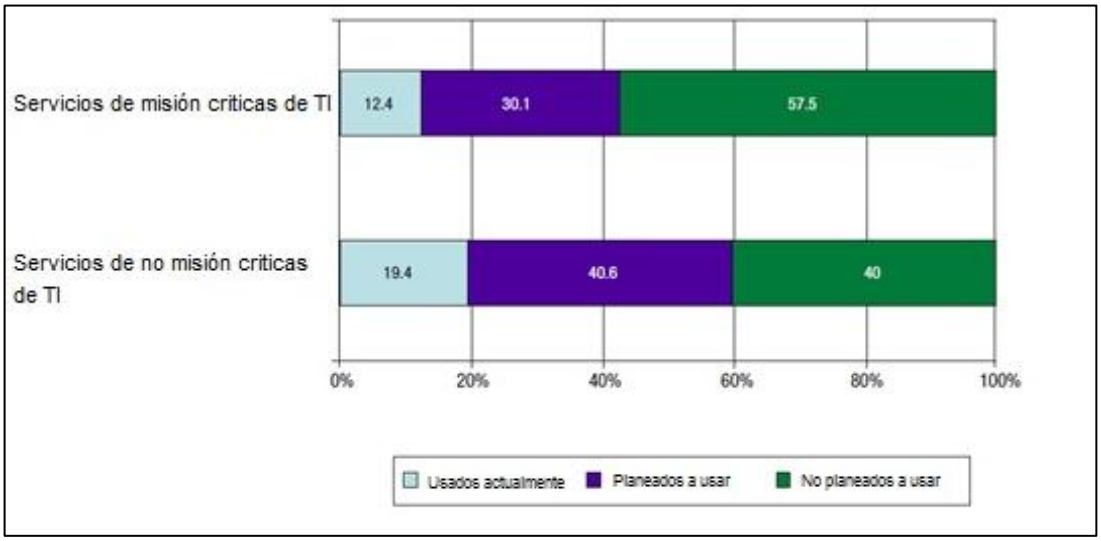


Figura 1. Uso de la Computación en la Nube. (ISACA, 2011)

Se espera que dentro de los próximos 5 a 10 años, este modelo de despliegue de servicios este en una fase de producción, y que no sea de uso exclusivo de expertos en tecnologías de información y comunicaciones, sino también de académicos, empresarios y personas comunes que se vean atraídos por las ventajas ofrecidas por este modelo (GARTNER, 2011).

Durante los últimos 50 años hemos visto la evolución acelerada de la informática, que en sus comienzos centralizaba la información a través de mainframes que manejaban grandes cantidades de datos. Después aparecen arquitecturas cliente-servidor (Años 90), modelo en el cual las capacidades de procesamiento se distribuyen, los servidores se encargaban del procesamiento de datos sensibles o de las aplicaciones que demandaban mas recursos, y las computadoras personales se encargaban de realizar tareas básicas. Posteriormente aparecen las arquitecturas colaborativas donde un número variable de computadores trabajan de forma colaborativa para solucionar problemas que individualmente no podrían hacerlo (computación distribuida), y finalmente aparece el modelo de computación

en la nube, que aunque no sustituye a las arquitecturas anteriores, consigue cambiar la forma en que se entregan servicios y aplicaciones, aprovechando los beneficios de los avances en las comunicaciones, en nuevas tecnologías como la virtualización y las arquitecturas orientadas al servicio.

El desarrollo actual de la computación en la nube tiene dos actores fundamentales. El primero lo constituyen empresas del sector de Tecnología que desarrollan implementaciones propietarias enfocadas en la tercerización de centros de cómputo, y el segundo es la comunicad académica y científica que está desarrollando implementaciones abiertas enfocadas en investigar las ventajas y complejidades del modelo (ROSALES ROSERO, 2010), sin embargo la exploración de aspectos de seguridad de cara al cliente aun no está muy explorado (TANIMOTO, 2011) dejando una sensación de falta de control sobre quién tiene acceso a la información. Esto hace que las compañías que quieran migrar a la nube no lo hayan hecho por temor a la pérdida de integridad, confidencialidad o disponibilidad de sus activos de información.

Las principales preocupaciones respecto a la computación en la nube se centran en la confidencialidad de la información y en la responsabilidad derivada de incidentes con terceros (proveedores) (ENISA, 2009). Para que este modelo alcance su máximo potencial, debe ofrecer solidez en la seguridad de la información. Por lo pronto, las organizaciones o clientes necesitan que los proveedores apliquen prácticas adecuadas de seguridad para mitigar los riesgos a los que se enfrentan, dicho de otra forma buscan garantía con respecto a la información, servicios y aplicaciones que se hospedan en las instalaciones de terceros.

Este trabajo de maestría constituye un modelo de seguridad de la información que intenta abordar estas preocupaciones de seguridad con respecto a los diferentes modelos de servicios (**S**oftware como Servicio, **P**lataforma como Servicio e **I**nfraestructura como Servicio o SPI) para implementación en nubes privadas o comunitarias en las instalaciones de un tercero. Las fuentes para la implementación del modelo de seguridad fueron los requerimientos de seguridad de la información respecto a los riesgos más comunes investigados, el cumplimiento basado en los requerimientos contractuales entre cliente y proveedor; y las mejores prácticas de seguridad de diferentes marcos de referencia tales como ISO 27001:2005, ISO 27002:2005, ISO/IEC 20000:2005, PCI DSS versión 2.0 y otros.

1.1 CONTEXTO DE TRABAJO

Con el advenimiento y la creciente aceptación de servicios de TI basados en la nube, ha surgido la preocupación de las organizaciones por la seguridad de la

información, por garantizar la integridad, confidencialidad y disponibilidad de la información en ambientes de computación en la nube debido a deslocalización y dependencia de terceros (TOWNSEND, 2009), e implicaciones de privacidad de los datos tales como aspectos jurídicos, acceso de terceros, medidas de seguridad, limitaciones en uso y retención, y el cumplimiento de normas legales vigentes (Johnston, 2011), por lo cual es necesario gestionar y controlar la información durante su ciclo de vida y el riesgo asociado a través de normas y/o estándares.

El Uso de computación en la nube es una apuesta que están haciendo las grandes empresas de tecnología como Amazon con Elastic Compute Cloud (EC2), Google con Google Apps, Apple con iCloud y Microsoft con Windows Azure. Incluso IBM ha invertido más de USD 3.000 millones en la adquisición de nuevas empresas y la puesta en marcha de diferentes soluciones para brindar servicios de computación en la nube (LANCHE, 2011), esto indica que los operadores se están alistando para los servicios que van a ofrecer y que los clientes ya están utilizando los servicios ofrecidos; más de un 60% de las grandes empresas de países desarrollados y un 15% en países de Latinoamérica (HIGUERA, 2011). El objetivo principal y la máxima preocupación de las empresas, es la seguridad de la información cuando piensan en la nube y las nuevas amenazas inherentes al modelo (SYMANTEC, 2011).

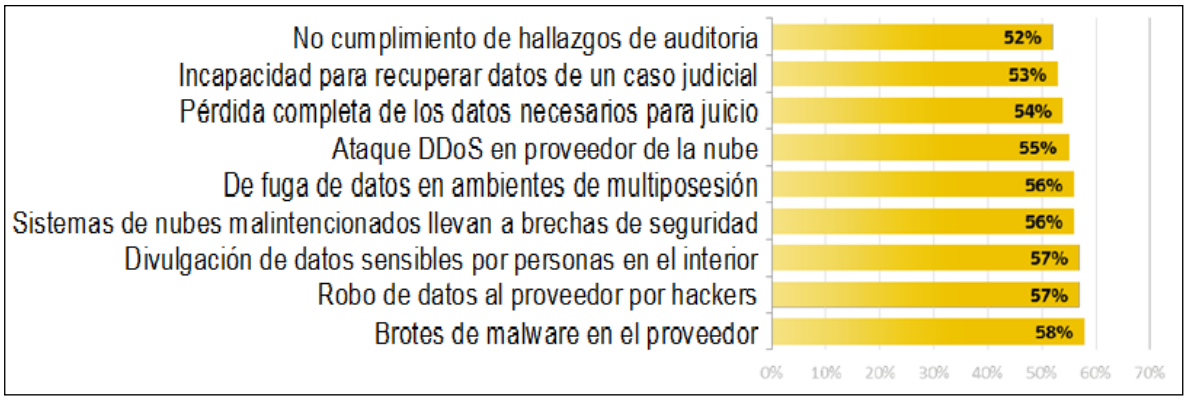


Figura 2. Principales Amenazas de la Nube. (SYMANTEC, 2011)

1.2 PLANTEAMIENTO DEL PROBLEMA

Dado que la seguridad de la información es uno de los aspectos que más preocupan a los directivos de T.I para migrar sus aplicaciones e información a la nube, al confiar sus datos privados a un tercero (Ver Figura 3), las organizaciones toman medidas que garanticen el control de su información y que minimicen los riesgos que la pueden impactar.

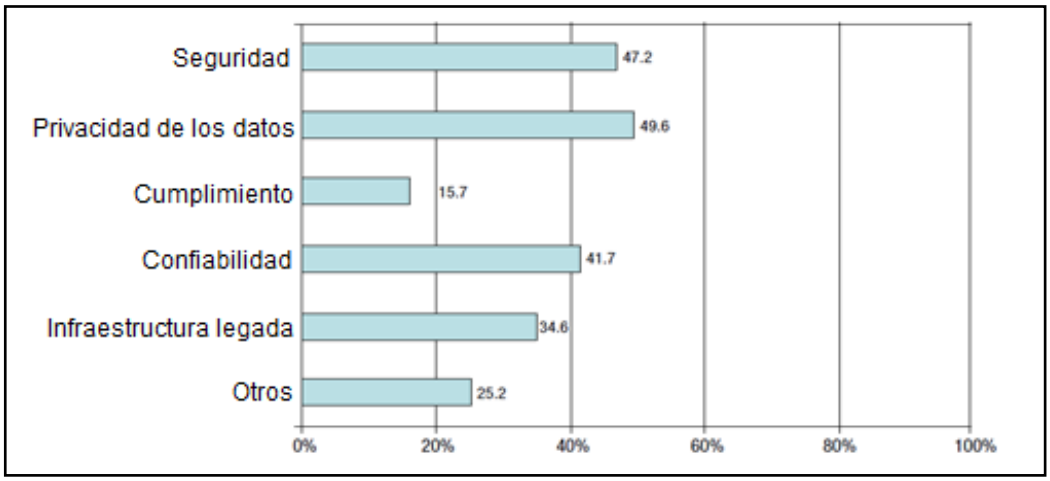


Figura 3. Razones para no usar Computación en la Nube. (ISACA, 2011)

Para ello utilizan herramientas o marcos de trabajo tales como ISO/IEC 27001:2005, ISO 27002:2005, ISO/IEC 20000:2005, entre otros, que fueron pensados originalmente para evaluar recursos de tecnología internos o alojados localmente, y que brindan la preservación de la confidencialidad, integridad y la disponibilidad de la información, asegurando controles de seguridad que protejan los activos de información y brinden confianza. Sin embargo, en el modelo de computación en la nube, tanto los procesos como la infraestructura y la información pueden estar alojados en las instalaciones de un tercero (Proveedor), cambiando el arquetipo de seguridad basado en los marcos de trabajo mencionados. Es necesario, por tanto, ajustar la utilización de estos marcos de trabajo a los nuevos requerimientos del modelo de computación en la nube. En este sentido, los marcos de trabajo que se emplearán desempeñan un papel muy útil para definir lo que debería hacerse, así como proporcionar los aspectos de la gestión de servicios y un marco de control que conduzcan a un modelo de referencia de seguridad de la información más robusto aplicable para organizaciones que quieren adoptar el modelo de computación en la nube.

Actualmente se están llevan desarrollando iniciativas no estandarizadas de modelos de seguridad de la información en el modelo de computación en la nube: La matriz de control en la nube (Cloud Control Matrix, CMM) desarrollada por Cloud Security Alliance y la ISO/IEC NP 27017-2. (MAUNY, 2011).

Según los estudios de GARTNER (GARTNER, 2011) los estándares de seguridad en la nube están comenzando a tener una gran expectativa en el mercado, pero solo estarán listos dentro de 5 a 10 años, dejando un vacío que los estándares o mejores prácticas actuales no cubren (ver Figura 4).

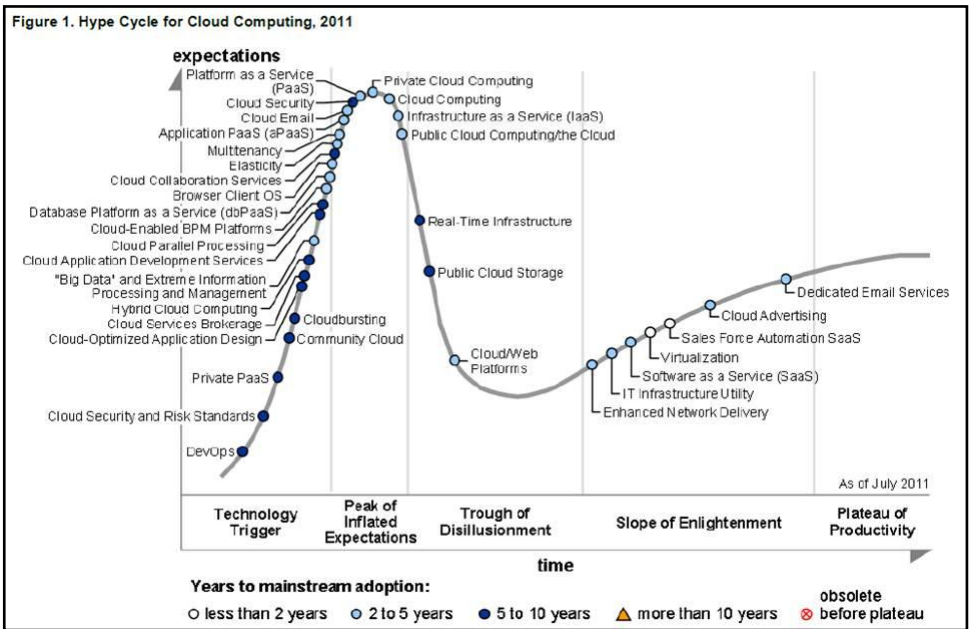


Figura 4. Tiempo de Adopción de la Computación en la Nube. (GARTNER, 2011)

Al identificar entonces que no existe un modelo de referencia estandarizado para la seguridad de la información, y la preocupación que tienen las organizaciones por los riesgos asociados a ella con la adopción del modelo de computación en la nube, existe una oportunidad de complementar el estado del arte y ofrecer una propuesta con los conocimientos adquiridos durante la maestría en informática y telecomunicaciones.

1.3 OBJETIVOS

1.3.1 Objetivo General.

Definir un modelo de referencia en seguridad de la información para la computación en nubes privadas y comunitarias tomando como referencia los marcos de trabajo ISO/IEC 27001:2005, ISO 27002:2005, ISO/IEC 20000:2005 y PCI.

1.3.2 Objetivos Específicos:

1) Analizar y seleccionar los dominios y controles que componen los marcos de trabajo ISO/IEC 27001:2005, ISO 27002:2005, ISO/IEC 20000:2005 y PCI enfocando su impacto en la seguridad de la información en las nubes privadas y comunitarias.

2) Alinear consistente e integradamente los dominios y controles de los marcos de trabajo ISO/IEC 27001:2005, ISO 27002:2005, ISO/IEC 20000:2005 y PCI en el modelo de referencia propuesto, que apliquen a la seguridad de la información para la computación en nubes privadas y comunitarias.

3) Complementar los controles existentes en el modelo de referencia propuesto.

4) Validar por medio de juicio de expertos el modelo de referencia propuesto.

1.4 RESUMEN DEL MODELO PROPUESTO

La computación en la nube es un modelo cada vez más utilizado y ofrecido debido a su elasticidad de cómputo, su cambio de modelo de gasto donde no se invierte grandes cantidades de capital, pero sí se paga una renta periódica y donde algunos de los riesgos de computación tradicional son transferidos al proveedor.

Los riesgos de la computación en la nube deben evaluarse con la misma rigurosidad que se hacen en la computación tradicional, esto conlleva a que en este nuevo esquema de servicios los riesgos aumenten en contraprestación, algunos de los riesgos transferidos son mitigados de una mejor manera por parte del proveedor.

Debido al aumento de los riesgos, la popularización del modelo y el déficit de un modelo para asegurar la información que está en la nube, existen riesgos que no se están tratando correctamente, y otros que merecen tener controles diferentes a los que se aplican con estándares como ISO/IEC 27001:2005 o ISO/IEC 27002:2005.

El modelo propuesto está dividido en dominios (ver figura 5), los cuales tienen una capa transversal que es la gestión que se debe hacer sobre las otras capas, el marco de seguridad es un conjunto de controles que dan respuesta a los riesgos encontrados, siguiendo una metodología propuesta basada en el levantamiento de información de diferentes estándares, normas y guías de seguridad de la información, seleccionando y evaluando los riesgos que se ajustan al modelo propuesto y efectuando la división de responsabilidades de cara al cliente y al proveedor para cada uno de los modelos de servicio.

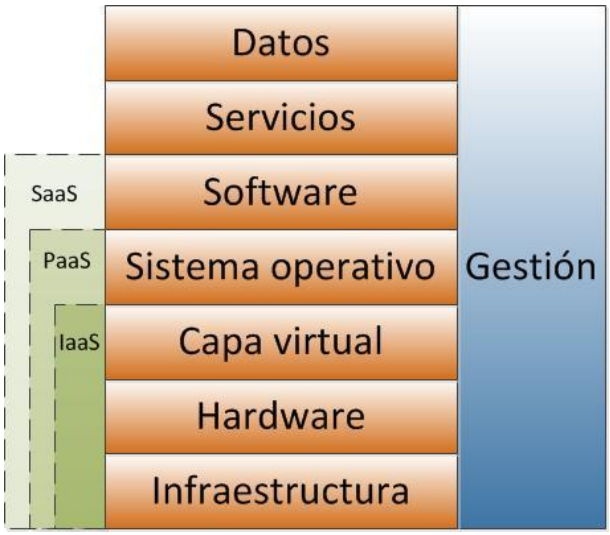


Figura 5. Dominios del Modelo de Seguridad de Computación en la Nube.

Dominio de Gestión:

La gestión implica un compromiso por parte de la dirección a liderar, desarrollar y mantener las políticas de seguridad de la información, gestión continua del riesgo y su tratamiento.

Aspectos Legales
Los aspectos legales son la base de los controles del servicio de computación en la nube, debido a que éstos presentan formalmente los acuerdos entre las partes. En este dominio se encuentran controles de confidencialidad, acuerdos de niveles de servicio, umbrales y cláusulas de cumplimiento del contrato.

Cumplimiento
El Objetivo es evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad. Se debe tener en cuenta que los servicios de computación en la nube pueden alojarse o ser accedidos desde otros países, lo que hace que el cumplimiento deba revisarse cuidadosamente.

Control de Acceso
Los controles de acceso son los que más impactan la seguridad de la información, debido a que validan identidades de múltiples fuentes. Los permisos de acceso los da el proveedor de servicio, la distribución de claves entre el cliente y proveedor podría interceptarse, el proveedor podría obtener acceso a la información dándole permisos a su usuario, al existir

más capas en el modelo tales como la capa virtual, existen más puntos de acceso a los recursos o simplemente la identificación de usuarios.

Gestión de Continuidad del Negocio.
La gestión sobre la continuidad del negocio se da como un hecho en el modelo de servicios en la nube, pero esto no siempre es cierto, se deben tener en cuenta aspectos como la continuidad del negocio del cliente y del proveedor, control sobre la información que se replica en lugares externos y control de seguridad en el momento en que se active un plan de recuperación ante desastres.

Operación del Servicio.
Los servicios usualmente pasan por un mínimo de tres etapas: una de planificación, otra de operación y por último una de finalización del servicio, la operación se enfoca en dos aspectos básicos: el primero es la disponibilidad de los servicios, esto se logra a través de los acuerdos de niveles de servicio y los umbrales; la segunda es la que se encarga de recopilar la información que serviría para un análisis forense de seguridad de la información.

Dominio de Centro de Datos o Infraestructura:

Los centros de datos son custodiados por las empresas prestadoras del servicio en todos los modelos de servicio de computación en la nube, esto hace que los riesgos sean transferidos al proveedor sin que esto implique que se estén controlando correctamente. Se deben tener contratados acuerdos de niveles de servicio para comprometer la disponibilidad de los sistemas, y el principal rol del cliente es implementar controles de auditoría para garantizar que estos acuerdos se cumplan y que los riesgos se estén mitigando correctamente. Se podrían utilizar normas internacionales para centros de datos como la TIA-942 (Telecommunications Infrastructure Standard for Data Centers) o la GR-3160 (NEBS Requirements for Telecommunications Data Center Equipment and Spaces) para garantizar el correcto diseño, uso, operación y gestión.

Dominio de Hardware y Redes de Computación:

Los recursos de hardware en todos los modelos de entrega de computación en la nube son propiedad del proveedor de servicios, por el contrario los recursos de red usualmente los provee el cliente para así acceder a los recursos. Los controles implementados son de auditoría debido a que los riesgos son transferidos al proveedor pero no necesariamente tratados por éste.

Dominio de Capa Virtual:

Los servicios en la nube son a menudo, pero no siempre, utilizados en conjunto con, y habilitados por, tecnologías de virtualización. No hay ningún requisito al respecto, sin embargo los lazos de abstracción de recursos a tecnologías de virtualización y muchas ofertas de virtualización por hipervisor o S.O no son empleadas (CSA, 2009). La capa virtual genera un conjunto de riesgos que no se tenían en el modelo tradicional de computación como la facilidad de extraer información, inyectar código en las máquinas virtuales, entre otros, además de tener un componente de multiposesión que implica que otros clientes comparten recursos y de no ser segmentados correctamente se podría llegar a acceder a la información y servicios alojados en la nube

Dominio de las Aplicaciones:

Cuando se mueven las aplicaciones a la nube, todos los controles tradicionales ya no son lo suficientemente eficaces para protegerlas, las aplicaciones ya no residen en una red de confianza en donde los controles tradicionales de seguridad perimetral las protegían, ahora las aplicaciones podrían residir con otras aplicaciones (agrupación de recursos) de otras organizaciones en las instalaciones de un tercero, y se pueden acceder desde cualquier tipo de dispositivo. Esto cambia la naturaleza de los requisitos de seguridad para aplicaciones en la nube y por supuesto los controles que las protegen.

Dominio de Información y servicios:

La información y los servicios son los únicos puntos donde, sin importar el modelo de despliegue, la responsabilidad de su gestión es de la organización pero estando en manos del proveedor, por esto se deberían generar controles que permitan a la organización mitigar riesgos como el acceso no autorizado a la información, borrado efectivo de la información cuando se solicite o la devolución de los activos cuando se termine el contrato de servicios.

1.5 RESUMEN DE RESULTADOS OBTENIDOS

Los resultados obtenidos consisten en una documentación completa sobre las definiciones de la computación en la nube, los modelos de despliegue y de servicio, la lista de riesgos relacionados, las responsabilidades de cada uno de los actores involucrados y los controles para tratar estos riesgos clasificados por dominio para el modelo utilizado de computación en la nube.

El marco de trabajo presentado es una herramienta que consta de 95 controles y 69 riesgos, que permite a las empresas asegurar sus activos de información y

ofrece un entendimiento más amplio de los riesgos y las responsabilidades dependiendo del modelo de servicio cuando migren sus servicios a la nube.

1.6 ORGANIZACIÓN DEL DOCUMENTO

Este documento de trabajo de grado elaborado para optar a la maestría de Informatica y telecomunicaciones tiene por objeto establecer una línea de base estable y segura para las operaciones de las nubes privadas y comunitarias; se debería considerar una fuente de información para empresas que pretendan migrar sus datos, servicios, aplicaciones e incluso hasta su infraestructura a la nube. También se describen una gran cantidad de aspectos de seguridad de la información, tales como riesgos y controles para cada uno de los diferentes modelos de servicio y la asignación de responsabilidades entre el cliente y el proveedor del servicio de computación en la nube.

El documento consta de 6 capítulos descritos a continuación:

En el capítulo 2 se presenta el marco teórico de la computación en la nube, su definición, sus modelos de servicio y modelos de implementación, también se abordan aspectos relacionados con la virtualización, que es un componente esencial mas no necesariamente indispensable de la computación en la nube, además se describen las preocupaciones por la seguridad de la información en la nube, los estándares y normas en seguridad, y finalmente algunas iniciativas actuales que se están convirtiendo en el punto focal para los estándares de seguridad a nivel mundial.

En el capítulo 3 se presenta la metodología detallada para obtener los controles del modelo de referencia en seguridad de la información para la computación en nubes privadas y comunitarias.

En el capítulo 4 se cubre la validación del modelo mediante encuestas a través de rúbricas a personal idóneo en el tema tratado durante el desarrollo de este documento.

En el capítulo 5 se pormenorizan, bajo la óptica de los estándares de seguridad, los resultados obtenidos mediante gráficas y todos los controles obtenidos al desarrollar la metodología y se clasifican por dominio según el modelo utilizado de computación en la nube.

En el capítulo 6 se presentan las conclusiones del trabajo y recomendaciones futuras a desarrollar tomando como base este trabajo de grado.

2. MARCO TEÓRICO.

"Sun Tzu, en El arte de la guerra, señala la importancia de la información sobre los adversarios y el cabal conocimiento de sus propósitos para la toma de decisiones"

Para entornos empresariales en donde las áreas de tecnología e información están consolidándose como un elemento impulsor, que busca convertirse en un activo importante de la organización, proporcionando y gestionando la implementación de herramientas tecnológicas que apoyen, integren y faciliten el desarrollo, distribución y la comercialización de productos o servicios, permitiéndole así obtener mayores ventajas competitivas frente a sus competidores, surge un nuevo modelo en la forma de entregar recursos de computación denominada computación en la nube, diferente al modelo tradicional de tecnología, que entre otras ventajas le permite a las empresas pasar de un modelo de gastos de capital (Capex) a un modelo de gastos operativos (Opex).

Este cambio radical en las tecnologías de información reduce costos, aumenta la competitividad, habilita la generación de nuevos ingresos y permite la flexibilización del negocio.

2.1 MARCO HISTÓRICO.

Los comienzos de la computación en la nube se remontan a 1961 cuando John McCarthy sugirió que los avances en la informática y las comunicaciones conducirían a que "algún día la computación se organizaría como un servicio público" igual que el modelo de negocio del agua o la electricidad (INTENCO, Instituto Nacional de Tecnologías de la Comunicaciones, 2011).

En el año 1969, Leonard Kleinrock, quien fue uno de los científicos a cargo del proyecto de ARPANET, indicó que las redes de computadoras estaban en su infancia y que a la medida que crezcan y se vuelvan más sofisticadas veríamos como los servicios de computación llegarían a nuestros hogares y oficinas como un servicio (Kleinrock, 1969). Estas visiones se anticipaban a la aparición de nuevos paradigmas, y acompañados con el fortalecimiento tecnológico condujeron al nacimiento de nuevos modelos para entregar servicios de computación.

En 1999, se fundó la compañía **Salesforce.com**, aplicando tecnologías desarrolladas por compañías como Google y Yahoo! a diversas aplicaciones de negocios. Se fortaleció la entrega de servicios bajo demanda, particularmente SaaS, viéndose respaldados por miles de clientes y negocios exitosos (Salesforce.com, 2011)

A inicios del año 2000, Yahoo! y Google anunciaron la prestación de servicios de computación en la nube a cuatro de las más grandes universidades de Estados Unidos: la Universidad de Carnegie Mellon, la Universidad de Washington, la Universidad de Stanford y el Massachusetts Institute of Technology (MIT).

Por esa misma época, los técnicos de Amazon se dieron cuenta que tenían una gran infraestructura y que sólo utilizaban una pequeña parte de su capacidad (Entre el 10-15%), vieron entonces la posibilidad de ofrecer estos servicios a usuarios para hacer mayor utilización de las capacidades disponibles, y en 2006 presentaron los servicios Web de Amazon (INTENCO, Instituto Nacional de Tecnologías de la Comunicaciones, 2011), ofreciendo el modelo IaaS con capacidades básicas de procesamiento y almacenamiento a través de Internet. La estrategia consistía en la ejecución personalizada de máquinas virtuales con sistema operativo Linux bajo la demanda de los usuarios, permitiéndoles eliminar los costos de inversión en infraestructura y permitiéndoles aumentar o disminuir capacidades de cómputo para satisfacer las fluctuaciones en la demanda y pagar únicamente la capacidad consumida.

Durante los años 2007 y 2008, grandes empresas como Google e IBM se aliaron con universidades norteamericanas e iniciaron investigación a gran escala sobre la computación en la nube. El resultado fue EUCALYPTUS, una plataforma de código abierto que proporciona interfaz única y permite a los usuarios el acceso a recursos de infraestructura (máquinas, red y almacenamiento) disponibles en nubes privadas o híbridas y es compatible con los servicios Web de Amazon (Eucalyptus, 2012).

En los últimos años, diversas e importantes empresas tales como IBM Corp, Microsoft, Oracle, Intel, Google, etc., han comenzado a desplegar servicios de computación en la nube. Algunos ejemplos de ellos son: Amazon EC2/S3, Google Apps, Windows Azure, entre otros.

La siguiente figura ilustra la taxonomía más amplia de soluciones de computación en la nube separadas en cuatro categorías (Servicios de infraestructura, servicios de plataforma y servicios de software que se dividen en dos: para el uso de la computación en la nube y las soluciones personalizadas).

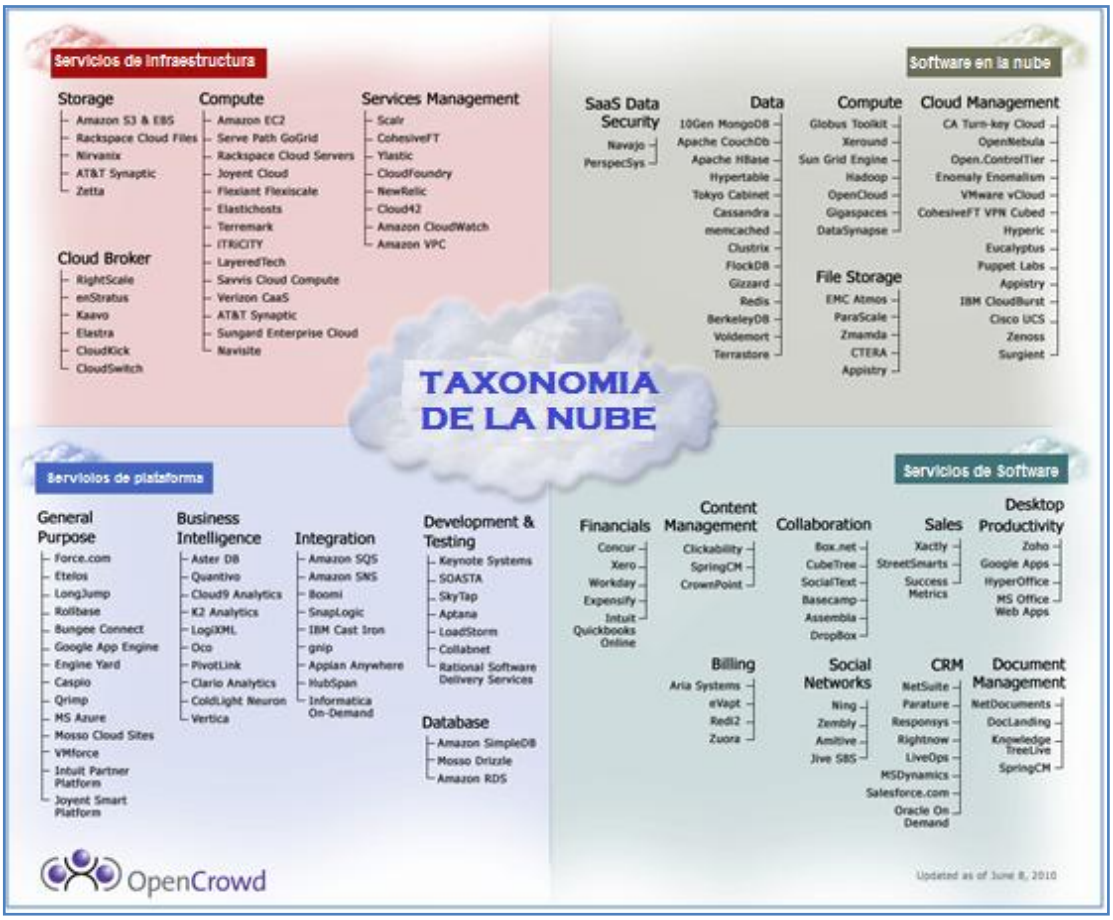


Figura 6. Taxonomía de la Computación en la Nube. (CSA, 2011)

2.2 DEFINICIÓN DE COMPUTACIÓN EN LA NUBE.

Para la definición del modelo de computación en la nube, utilizaremos la propuesta realizada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, NIST (NIST, 2011) en la cual establece que no es una tecnología nueva *per se* sino que se trata de un modelo de prestación de servicios, que permite a las empresas obtener las siguientes ventajas (MALL & GRACE, 2011)

- ✓ Acceder a un catálogo de servicios estandarizado.
- ✓ Acceder bajo demanda a un conjunto compartido de recursos informáticos configurables (Redes, servidores, centros de almacenamiento, aplicaciones y servicios).
- ✓ Obtener economías de escala.
- ✓ Flexibilización en los costos en función del consumo (Costos fijos pasan a ser variables).
- ✓ Un alto grado de automatización.

- ✓ Una rápida movilización de los recursos y aprovisionamiento.
- ✓ Alto grado de optimización de los recursos.
- ✓ Una elevada capacidad de adaptación.
- ✓ Un esfuerzo mínimo de gestión o interacción.
- ✓ Contribuye con el uso eficiente de energía por la concentración masiva de recursos.
- ✓ Acorta tiempo para desarrollo de nuevas aplicaciones o implementación de nuevos negocios
- ✓ Acceso ubicuo a la información para responder a las necesidades actuales del negocio.

El modelo de computación en la nube consta de cinco características esenciales, tres modelos de servicios y cuatro modelos de despliegue, la siguiente figura Ilustra el modelo.

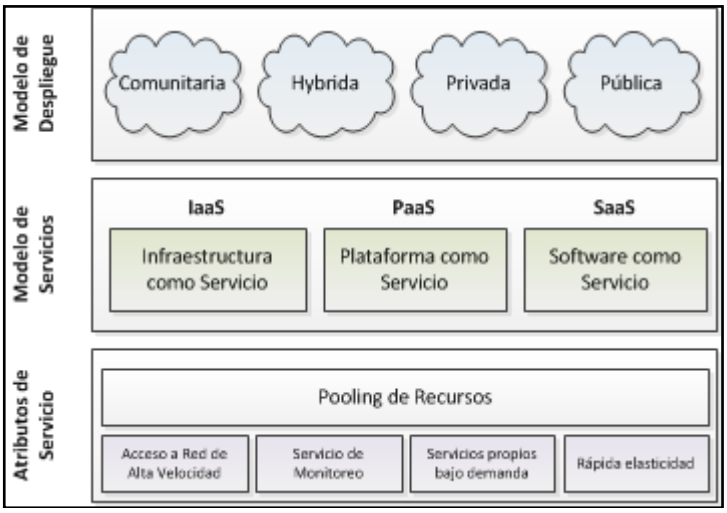


Figura 7. Características, Modelos de Servicios y Despliegue de la Computación en la Nube. (NIST, 2011)

2.2.1 Características esenciales de la computación en la Nube.

1) **Autoservicio bajo demanda**: Le permite al cliente aprovisionar las capacidades de computación, horarios, según sea necesario sin la necesidad de la interacción humana con el proveedor de servicios.

2) **Acceso a través de Internet**: Las capacidades están disponibles para acceso a internet y promueve el uso de plataformas heterogéneas (acceso a través de dispositivos móviles, portátiles o estaciones de trabajo a través de un navegador).

3) **Agrupación de recursos**: Se accede a un conjunto de recursos físicos y virtuales dinámicamente asignados según la demanda del cliente utilizando el modelo de multiposesión, que permite el uso de los mismos recursos para uno o varios clientes haciendo uso de mecanismos de segmentación y aislamiento como la virtualización.

4) **Rápida elasticidad**: Los recursos de computación pueden ser abastecidos o desabastecidos rápidamente y en algunos casos de forma automática.

5) **Medición del servicio**: Monitoreo, control e informes del uso de los recursos utilizados por el cliente.

2.2.2 Modelos de Servicios.

1) **Software como Servicio (SaaS)**: Entrega de Software que se ejecuta en la infraestructura del proveedor, como un servicio a través de Internet mediante un cliente ligero. El cliente no administra, ni controla la infraestructura de nube subyacente incluyendo las redes, servidores, sistemas operativos, centros de almacenamiento y las aplicaciones individuales. Proporciona un entorno de trabajo autónomo que se utiliza por entregar al usuario contenido, presentación, aplicación y capacidad de gestión.

2) **Plataforma como Servicio (PaaS)**: Permite al cliente despliegue en la infraestructura del proveedor aplicaciones creadas o adquiridas, librerías, servicios, etc. El cliente no controla la infraestructura de nube subyacente incluyendo las redes, servidores, sistemas operativos, centros de almacenamiento, pero si tiene control sobre las aplicaciones instaladas y su configuración. Ofertas de PaaS facilitan el despliegue de aplicaciones sin costo y la complejidad de la compra y la gestión del software y hardware subyacente y aprovisionamiento de las capacidades de alojamiento. Añade capa adicional al modelo IaaS de integración con marcos de desarrollo de aplicaciones, capacidades de middleware y funciones como bases de datos, mensajería y manejo de colas.

3) **Infraestructura como Servicio (IaaS)**: Ofrece al cliente capacidades de almacenamiento, redes, procesamiento y otros recursos informáticos, en donde el cliente implementa y ejecuta sus aplicaciones. El cliente no administra ni controla la infraestructura de nube subyacente pero tiene el control sobre los sistemas operativos, centros de almacenamiento, aplicaciones desplegadas y posiblemente el control limitado de componentes de red (firewalls). Incluye la pila completa de recursos de

infraestructura desde las instalaciones, las plataformas de hardware que residen, capacidades de abstracción de recursos, conectividad física y lógica de dichos recursos y proporciona un conjunto de APIs que permiten que le cliente final administre la infraestructura e interactúe con ella.

2.2.3 Modelos de Implementación.

1) **Nube Pública**: Es de uso abierto al público y la propiedad, gestión y operación de los servicios están en manos de terceros. Permite el acceso de múltiples usuarios que utilizan una misma infraestructura.

2) **Nube Privada**: La infraestructura en la nube privada es de uso exclusivo de una sola organización, La propiedad, gestión y operación pueden ser efectuadas por la misma organización o por un tercero. Puede estar en las instalaciones de la organización o por fuera de ellas. Garantiza una mejora en cuanto a la seguridad de la información, porque los datos sensibles y servicios de procesamiento no se comparten con usuarios diferentes a los de la organización o el tercero que la gestiona.

3) **Nube Comunitaria**: Infraestructura para el uso de una comunidad o clientes que comparten requisitos de seguridad y políticas de cumplimiento. Puede ser propietaria, gestionada y operada por una de las organizaciones clientes de la comunidad o por un tercero. Es una variación del modelo de nube privada.

4) **Nubes Híbridas**: Están dispuestas según dos o más modelos de despliegue de computación en la nube

Modelo Despliegue	Infraestructura Manejada por	Infraestructura propietaria	Localización Infraestructura	Usuarios
Nube Publica	Proveedor	Proveedor	Fuera de las Instalaciones	No Confiables
Nube Privada / Comunitaria	Organización Proveedor	Organización Proveedor	En las Instalaciones Fuera de las Instalaciones	Confiables
Nube Híbrida	Ambas Organización Proveedor	Ambas Organización Proveedor	Ambas En las Instalaciones Fuera de las Instalaciones	Confiables No Confiables

Tabla 1. Modelos de Despliegue de la Computación en la Nube. (CSA, 2011)

2.3 VIRTUALIZACIÓN.

Un elemento clave de la computación en la nube son las tecnologías de virtualización que permiten la abstracción lógica de los recursos. La virtualización separa aplicaciones, máquinas, redes, datos y servicios de sus limitaciones físicas.

Entre los beneficios de la virtualización podemos destacar los siguientes:

- ✓ Mejor utilización del servidor.
- ✓ Útil en la consolidación de centros de datos.
- ✓ Mayor densidad de máquinas virtuales en un mismo servidor, lo que significa mayores márgenes, disminución en inversiones de hardware y mayor eficiencia operativa.
- ✓ Permite implementar la característica de multiposesión.

2.3.1 Multiposesión.

No es una característica esencial de la computación en la nube según NIST (NIST, 2011), pero sí lo es según CSA (CSA, 2011). Implica el uso de los mismos recursos físicos pero no lógicos para una misma organización o para varias organizaciones. Permite abstraer los recursos de una máquina física y crear una máquina virtual con una fracción del total de recursos, pudiendo operar en diferente Hardware y junto con otras máquinas virtuales en un mismo hardware físico.

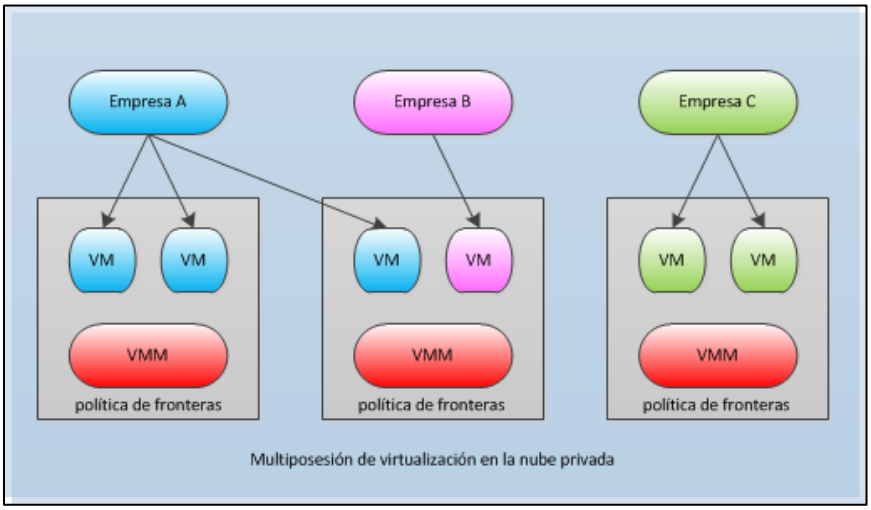


Figura 8. Multiposesion. (CSA, 2011)

2.3.2 Componentes de la Virtualización.

Los componentes de un sistema virtual son los siguientes:

- ✓ Hipervisor: Software responsable de la organización y gestión de las máquinas virtuales.

- ✓ Máquina Virtual: Es un entorno de trabajo autónomo que se comporta como un equipo independiente.

- ✓ Dispositivos Virtuales: Es una imagen de software pre-empaquetado que ofrece funciones específicas como enrutadores, switches o firewalls.

Existente diferentes tipos de virtualización, tales como: virtualización de sistema operativo, de hardware o plataforma, de red, de almacenamiento de datos, y de memoria.

La oferta de servicios de la computación en la nube, se entregan a través de un conjunto de recursos interconectados, generalmente utilizando tecnologías de virtualización que son orquestados y gestionados a través de un hipervisor, ello permite un rápido aprovisionamiento de recursos, obtener economías de escala y de densidad, y una rápida movilización de los recursos entre otros beneficios. Debe notarse que el uso de estas nuevas tecnologías involucra nuevos vectores de ataque y mayor desconocimiento de los riesgos que en las tecnologías tradicionales, y sugiere un enfoque en el diseño hacia la segmentación y el aislamiento de recursos.

2.4 PREOCUPACIONES POR LA SEGURIDAD DE LA INFORMACION EL LA NUBE.

Con el advenimiento y la creciente aceptación de servicios de TI basados en la nube, ha surgido la preocupación de las organizaciones por la seguridad de la información, por garantizar la integridad, confidencialidad y disponibilidad de la información en ambientes de Computación en la nube debido a deslocalización y dependencia de terceros (TOWNSEND, 2009) e implicaciones de privacidad de los datos tales como aspectos jurídicos, acceso de terceros, medidas de seguridad, limitaciones en uso y retención y el cumplimiento de normas legales vigentes (JOHNSTON, 2011), por lo cual es necesario gestionar y controlar la información durante su ciclo de vida y el riesgo asociado a través de normas y/o estándares.

Entender las relaciones y dependencias entre los modelos de computación en la nube es fundamental para comprender los riesgos de seguridad asociados. Para

ello haremos las siguientes consideraciones (CSA, 2011): IaaS es el fundamento de todos los servicios en la nube, PaaS está construido sobre IaaS y SaaS está construido sobre PaaS y IaaS, por lo tanto al igual que se heredan las capacidades, también se heredan los riesgos y los problemas de seguridad en la información.

2.4.1 Desventajas de la Computación en la Nube.

- ✓ Se genera interdependencia con los proveedores del servicio.
- ✓ La confiabilidad de los servicios depende del proveedor del servicio.
- ✓ La información sensible de la organización, no reside en las instalaciones físicas de la misma, se encuentra alojada en la infraestructura de un tercero, siendo más propensa al fraude o robo.
- ✓ La disponibilidad de los servicios está ligada a los servicios de red que intercomunican con las instalaciones del proveedor.
- ✓ La información debe recorrer muchos nodos, cada uno de ellos es un foco adicional de inseguridad, si se utilizan protocolos seguros la velocidad de acceso y la distribución de la información disminuye por sobrecarga.
- ✓ La confiabilidad de los servicios depende de la salud tecnológica y financiera de los proveedores de servicios en nube.

2.4.2 Ventajas y Desventajas de Cada Modelo frente a la Seguridad (CSA, 2011).

- ✓ SaaS ofrece mayor funcionalidad, con mayor capacidad de ampliación para el cliente y un nivel alto de seguridad integrado (por lo menos el proveedor tiene la responsabilidad de la seguridad).

- ✓ PaaS tiene por objeto permitir a los desarrolladores crear sus propias aplicaciones en la parte superior de la plataforma. Como resultado, tiende a ser más extensible que SaaS, a expensas de características de seguridad, donde las capacidades incorporadas son menos completas, pero hay más flexibilidad a la capa de seguridad adicional.

- ✓ IaaS tiene extensibilidad enorme, capacidades de seguridad menos integradas y funcionalidades más allá de proteger la propia infraestructura. Este modelo requiere que los sistemas operativos, aplicaciones y contenido deben ser gestionado y garantizado por los consumidores de nubes.

En la parte baja de la pila de los modelos de computación en la nube, los proveedores disminuyen las capacidades de seguridad y los administradores de los clientes son los responsables por implementarla y gestionarla.

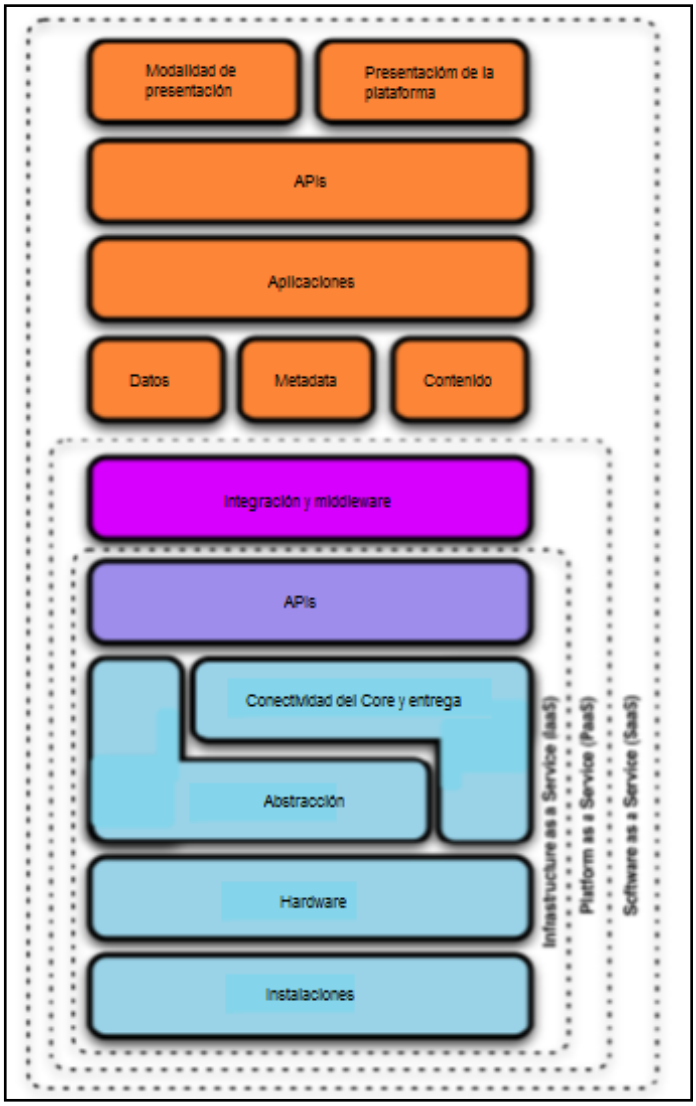


Figura 9. Modelo de Computación en la Nube. (CSA, 2011)

2.5 ESTÁNDARES Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN

¿Qué es un estándar? Los estándares son buenas prácticas que normalizan un conjunto de criterios con base al conocimiento de expertos que deben transformarse en una herramienta de valor o de diferenciación para convertirse en referencia o estándar “de facto”. (CAO AVELLANEDA, 2009)

¿Qué es un estándar de Seguridad de la información? Es un modelo para establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la Información cuyo diseño e implementación están influenciados por necesidades y objetivos, requisitos de seguridad, los procesos empleados, el tamaño y la estructura de la Organización, para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza en las partes interesadas. (ISO, ISO/IEC 27001, 2005).

Actualmente muchas organizaciones decidieron gestionar y mejorar la seguridad de la información mediante un sistema de gestión de seguridad de la información basado en el estándar ISO 27001, con el apoyo del resto de estándares de esta familia, sin embargo la adopción de un nuevo modelo de nube conlleva la existencia de un nuevo proveedor de servicios que debe ser incluido entre los elementos del sistema de gestión, y que no puede ser regulado exclusivamente por un contrato de prestación de servicios y acuerdos de niveles de servicio debido a que no son suficientes para resolver todas las necesidades especiales que se derivan de la nube, trasladando al proveedor estas necesidades especificas, además por que la implantación de un SGSI se basa en resultados de actividades de análisis de riesgo desarrolladas por la Organización.

A continuación se citan cada uno de los estándares, normas, guías y/o buenas prácticas utilizadas para el desarrollo del marco arquitectónico del modelo de seguridad de la nube y para el desarrollo en la selección, análisis y extracción de riesgos y controles para el marco de seguridad de la información para nubes privadas con centros de datos alojados en las instalaciones del proveedor.

ISO/IEC 27001:2005: Norma o estándar para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información, con un enfoque basado en procesos. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones. La norma define los controles que deben implementarse para la adopción de un sistema de seguridad pero no indica cómo; la ISO 27001:2005 es una norma certificable (ISO, ISO/IEC 27001, 2005).

ISO/IEC 27002:2005: Estándar de seguridad que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. No es certificable. Tiene los mismos controles de la ISO 27001:2005 pero esta norma además incluye guía de implementación de los controles (ISO, ISO/IEC 27002, 2005).

ISO/IEC 20000:2005: Estándar que recoge las mejores prácticas para el proceso de GSTI (Gestión de Servicios de T.I) identificando SLA's (Services Level Agreement) basados en métricas de seguridad que sean relevantes para medir y monitorear el desempeño de seguridad de los servicios de computación en la nube en consonancia con el marco ISO/IEC 27001:2005

El estado del arte de modelos de seguridad de la información que garanticen las tres características principales de la información (Confidencialidad, Integridad y Disponibilidad) en nubes privadas son iniciativas no estandarizadas, citamos los casos más representativos como CSA (CSA, 2009) e ISO/IEC NP 27017-2.

2.6 INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COMPUTACIÓN EN LA NUBE

Algunas iniciativas adicionales de estandarización de los servicios en la nube que involucran la seguridad de la información son las siguientes: Open Grid Forum (OGF), Cloud Computing Interoperability Forum (CCIF), Distributed Management Section 3 Task Force (DMTF), Open Cloud Consortium (OCC), ETSI, OASIS, Object Management Group (OMG), Storage Networking Industry Association, ITU-T, GICTF, IETF, NIST, Open Cloud Manifesto & Cloud Computing Use Cases Group, TM Forum, W3C, CCF, CloudAudit, KCSA, Open Group Cloud Work Group, Study Group on Smart, Cloud (Japan), etc.

2.6.1 Cloud Security Alliance (CSA, 2009)

Cloud Security Alliance es una organización sin fines de lucro con la misión de promover el uso de mejores prácticas para ofrecer garantías de seguridad en la nube, y para proporcionar educación sobre los usos de la computación en nube.

Es la principal organización del mundo focalizada exclusivamente en seguridad en la nube y en conjunto con la IEEE, líder mundial en el desarrollo de estándares buscan establecer la base sobre la utilización actual y previsto de la computación en la nube servicios, así como las necesidades, actitudes y comportamientos en torno a estándares de seguridad en la nube. (GORMAN, 2011)

CSA propuso la guía de seguridad para áreas críticas enfocadas en seguridad en la nube en abril del 2009, la cual se encuentra dividida en 14 dominios que fueron concebidos y revisados por expertos en la industria y que están alineados con los estándares y buenas prácticas en seguridad. Consta de tres secciones: arquitectura, gobierno y operación; sus dominios se enfatizan en la seguridad, estabilidad y privacidad, y ofrece una guía de implementacion práctica y efectiva y recomendaciones sobre la reducción del riesgo para quienes deseen adoptar el paradigma de computacioón en la nube de forma segura.

CSA también diseño la *Cloud Security Alliance Controls Matrix (CCM)* específicamente para proporcionar los principios fundamentales de seguridad a los proveedores de nubes, así como, ayudar a los clientes potenciales de nubes en la evaluación del riesgo para la seguridad global de los proveedores de computación en la nube.

CCM proporciona un marco de controles que ofrece conceptos y principios de seguridad, que quedan alineados en 13 dominios. Estos fundamentos tienen en consideración otras normas de seguridad aceptadas por la industria, las regulaciones y marcos de control, tales como ISO 27001/27002, COBIT de ISACA, PCI, NIST, Jericho Forum y NERC CIP. (CSA, 2009)

2.6.2 ISO/IEC NP 27017-2

La organización internacional de estándares (ISO) está desarrollando el estándar ISO/IEC NP 27017-2 que se dividirá en dos partes:

- Técnicas de Seguridad para la computación en la nube y sistema de gestión de la privacidad.

- Y Controles de Seguridad que incluirá directrices para los controles de seguridad de información para el uso de servicios de computación en la nube basado en la ISO / IEC 27002.

3. MODELO PROPUESTO

Actualmente grandes empresas están empezando a centrar su atención en la computación en la nube como resultado de la necesidad de cambio en el paradigma computacional actual, escenario en donde la infraestructura, las aplicaciones y los datos estaban gestionados por las empresas y por su recurso humano, a otro escenario en donde un tercero (proveedor) confiable brinda servicios de infraestructura, uso de aplicaciones y gestión compartida de la información alojada en sus instalaciones. Sin embargo, aún no existe un desarrollo maduro de este modelo de prestación de servicios. Los factores son varios, entre otros consideramos que aún hay mucho terreno por explorar en cuanto a lo relacionado con la seguridad de la información. Cuando se va a migrar la información sensible para que esté en la infraestructura de un tercero, surgen muchas interrogantes en cuanto al acceso, localización, normas o buenas prácticas aplicadas, regulaciones y consideraciones legales de propiedad de los datos, riesgos y las relacionadas con la continuidad del negocio, acuerdos de niveles de servicio, etc.

Debido a esto surge la necesidad de tener un marco de seguridad de la información propio al modelo de computación en la nube, principalmente para los modelos de implementación privado y comunitario cuya infraestructura se encuentre en las instalaciones de un tercero, en donde se tengan en cuenta las consideraciones de seguridad como controles, de cara a valorar los riesgos de la computación en la nube.

3.1 LEVANTAMIENTO DE INFORMACIÓN

Como ningún marco de trabajo existente en la actualidad satisface por completo las necesidades de seguridad de la información en el modelo de computación en la nube (Actualmente esta en desarrollo la ISO/IEC NP 27017-2 que posiblemente cubra este vacío), se propone un marco de trabajo de seguridad en la información basado en algunos de los marcos ya existentes para lograr el convencimiento por parte de los clientes de que los entornos de computación en la nube son un espacio seguro en el cual operar y al cual trasladar información sensible, y que sus servicios de procesamiento de información no estarán expuestos a riesgos inaceptables.

Para el proceso de levantamiento de información, lo primero que se debía conocer y establecer era el modelo de computación en la nube que se emplearía. Se encontró el modelo según la NIST 800-145 (NIST, 2011) en la cual define la computación en la nube como un modelo para permitir el acceso desde cualquier lugar, de forma cómoda y bajo demanda, a conjuntos compartidos de recursos

informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente aprovisionados y desplegados con un mínimo esfuerzo de gestión o de interacción por parte del proveedor de servicios. Esta definición reconocida por clientes y proveedores del servicio de computación en la nube también es utilizada para el desarrollo de la guía de seguridad en áreas criticas de la computación en la nube (CSA, 2011), además también establece que hay tres modelos de entrega de servicio (SPI) y 4 tipos de implementación, de las cuales sólo se hará énfasis en nubes privadas o comunitarias, en las que la infraestructura se encuentra en las instalaciones de un tercero, teniendo como consecuencia que los riesgos y mecanismos de seguridad (Controles) deben considerarse como un trabajo colaborativo entre las dos partes.

Con un marco arquitectónico para la computación en la nube ya definido, se debieron hallar los riesgos y controles que se incluirían en este modelo, sin embargo se halló que los riesgos definidos como vulnerabilidades explotadas por amenazas sólo se abordan a través de profundas investigaciones aisladas de los grandes proveedores de servicio (AUTY, CREESE, GOLDSMITH, & HOPKINS) y por consiguiente se consideró adecuado abordar los riesgos y controles a través de normas, estándares y guías de seguridad para la computación en la nube, además de abundante bibliografía en Internet donde se generalizan conceptos de seguridad.

Este análisis se realiza tomando como base normas de la familia ISO 27000, tales como la ISO 27001:2005 y la ISO 27002:2005, las cuales definen un listado detallado de controles, procesos y procedimientos para garantizar la seguridad de la información, sin embargo estas normas fueron pensadas originalmente para evaluar recursos internos de tecnología; sin embargo muchos de los controles distribuidos en sus dominios puede utilizarse para el escenario de la computación en la nube.

Otros estándares de la ISO como lo son la ISO 20000-2:2005 que define las buenas prácticas para la gestión de un área de T.I sirvieron de apoyo para abordar controles de cumplimiento, contratación y acuerdos de niveles de servicio; y el estándar ISO 27031:2011 permitió obtener un panorama mas amplio para controles de gestión para la continuidad del negocio.

Estas normas de la familia de la ISO brindaron un listado detallado de controles técnicos, operativos y de gestión respecto a las tecnologías tradicionales, pero no cubrieron el vacío dejado por las nuevas herramientas utilizadas por la computación en la nube, tales como la virtualización, en donde los riesgos son menos conocidos. Para cubrir este vacío se empleó el estándar PCI Data Security Standard (PCI DSS) versión 2.0 (PCI, 2011), norma de seguridad de datos utilizada para la industria de las tarjetas de crédito en entornos virtualizados.

Se pudo recolectar información valiosa de la guía de seguridad para áreas criticas enfocadas en la seguridad en la nube, publicada por la Cloud Security Alliance en Abril del 2009, debido a que CSA se está convirtiendo en el punto focal para estándares de seguridad en la computación en la nube a nivel mundial, además ofrece una guía de recomendaciones para la reducción de riesgo en la nube.

Finalmente, se tomó información de ENISA y su documento (no es un estándar) en cuanto a beneficios, riesgos y recomendaciones para la seguridad de la información en ambientes de computación en la nube.

La siguiente figura ilustra el proceso de levantamiento de información y las fuentes utilizadas.

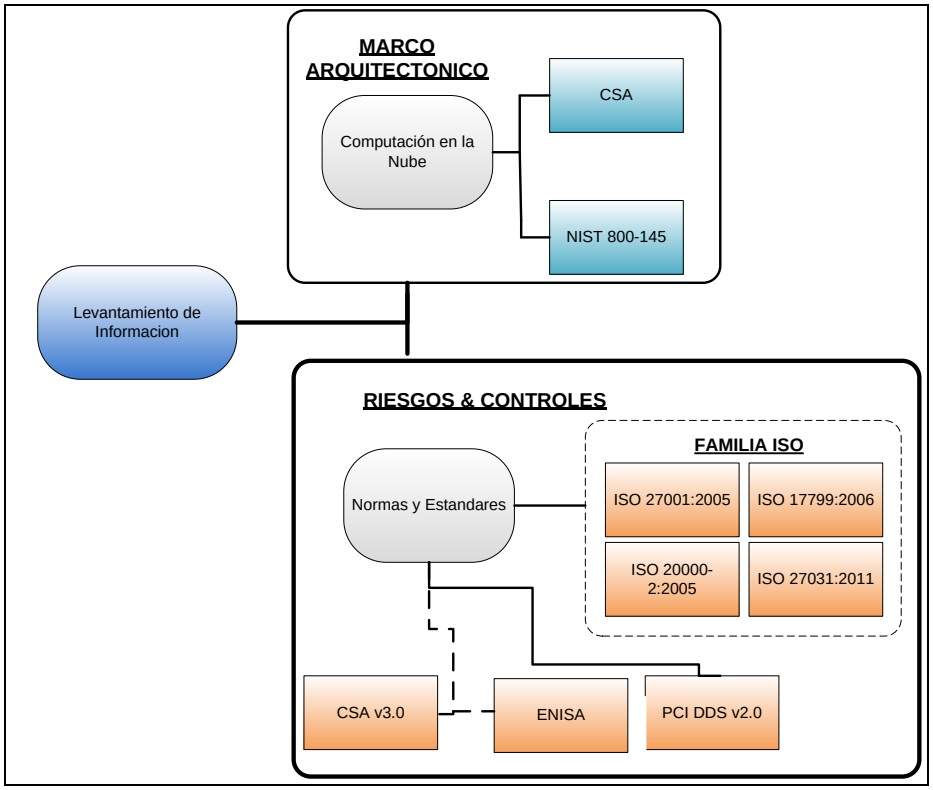


Figura 10. Modelo de Levantamiento de Información.

3.2 SELECCIÓN DE RIESGOS

La computación en la nube se ha centrado más en el lado del servicio (SPI), que en el lado de la seguridad o los riesgos asociados, sobre todo de cara al cliente (TANIMOTO, 2011). Los riesgos para los clientes que adoptan este modelo han sido vagamente investigados, a pesar de ser considerados como un factor crítico de decisión para empresas que desean migrar sus servicios.

Para el proceso de extracción y análisis (Selección), se empleó el método de estructura de división de riesgo (RBS) (HILLSON, 2002) para hacer una representación organizada de los riesgos por dominios o capas del modelo de computación en la nube. Las fuentes para este proceso son: la investigación de la computación en la nube, referencias sobre la seguridad de la información y los riesgos, y las normas y estándares descritos en la sección anterior.

Para definir el modelo de división, se emplearon como base las capas que comprenden el modelo de computación en la nube según CSA organizadas por dominio según su funcionalidad (ver Figura 11)

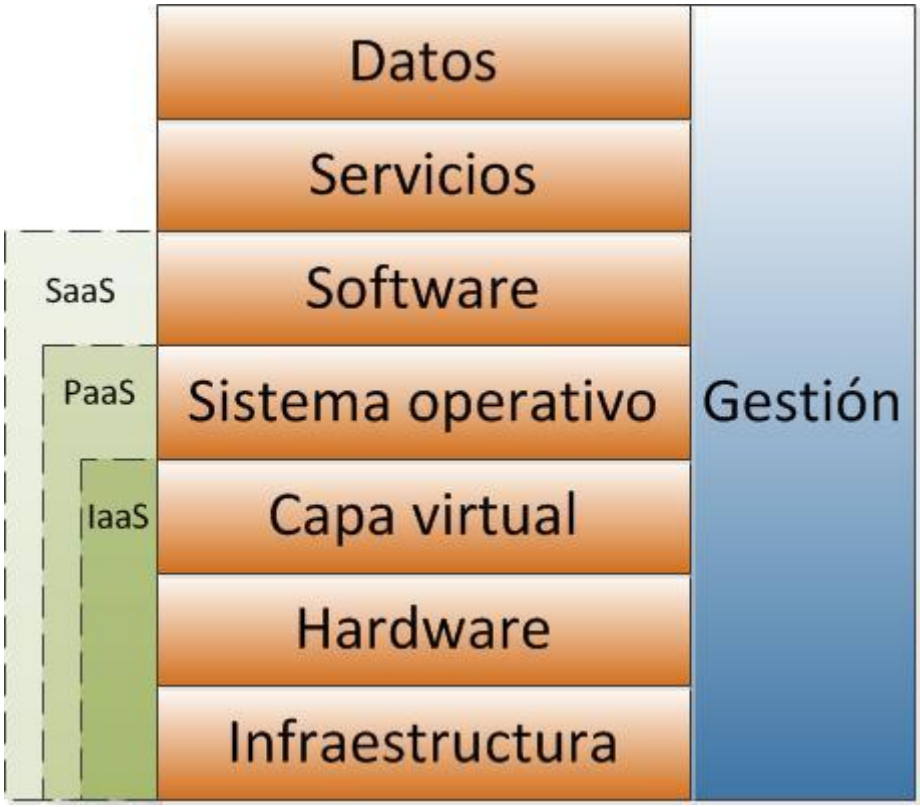


Figura 11. Dominios del Modelo de Seguridad de Computación en la Nube.

La capa de infraestructura generalmente comprende las instalaciones físicas del centro de datos, los servicios o suministros para su funcionamiento (agua, energía eléctrica, aires acondicionados, etc.) y los controles para amenazas del entorno o externas, tales como detectores de incendios, barreras perimetrales, controles biométricos de acceso.

La capa de hardware comprende los componentes físicos básicos de un sistema informática, tales como la memoria, la unidad de procesamiento, dispositivos de

almacenamiento y componentes de comunicación, que en conjunto componen el sistema de procesamiento de información.

La capa virtual esta compuesta según la NIST (NIST, 2011) por elementos tales como el hipervisor, máquinas virtuales y dispositivos virtuales. Como su nombre lo indica, se trata de un componente lógico sobre un componente físico, es la encargada de ofrecer algunos de las ventajas mas significativas de la computación en la nube, como lo son el acceso a un conjunto de recursos, rápida elasticidad, obtención economías de escala, una rápida movilización de los recursos y aprovisionamiento.

Las siguientes capas, tales como la capa de sistema operativo, software y servicios, son la que suministran la base lógica para el alojamiento de servicios de procesamiento de información. Los sistemas operativos gestionan los recursos de hardware y proveen servicios al software o a las aplicaciones para que ellas ofrezcan un conjunto de servicios a los usuarios. La capa de datos no tiene función, es simplemente de presentación y representativa para identificar los activos de información sensible que será procesada a través de todo un sistema que puede ser abarcado durante todo su ciclo de vida desde la creación, almacenamiento, uso, archivado y destrucción.

Por ultimo la capa de gestión es transversal a todas las capas del modelo de computación en la nube, y su principal función es gestionar el sistema de seguridad de la información. Se puede dividir en las siguientes funciones: control de acceso, gestión de la continuidad del negocio, operación del servicio, cumplimiento y aspectos legales y los aspectos relacionados con los recursos humanos.

En el análisis de riesgos cualitativo asociamos los riesgos dependiendo de su impacto y área de incidencia a cada una de las capas independientes del modelo de servicios de la computación en la nube, sin embargo la responsabilidad por la implementación de los controles en la parte del proveedor o del cliente depende de estos modelos (Ver división de responsabilidades) o de acuerdos establecidos durante la etapa de contratación.

Las opciones para el tratamiento de los riesgos que se utilizarán en la selección de controles de seguridad en el modelo de computación en la nube son las siguientes:

- **Transferencia del Riesgo:** Los controles contra los riesgos transferidos son la vigilancia del proveedor (a través de contratos, auditorias y acuerdos de niveles de servicio) y la garantía de cumplimiento por parte del proveedor de servicios.

- **Prevención del Riesgo:** La implementación de controles para la prevención del riesgo son ejecutados por el proveedor, el cliente o conjuntamente. Los riesgos generalmente son causados por especificaciones del servicio de computación en la nube

En un proceso de evaluación y tratamiento de los riesgos, estos también pueden ser mitigados (especificaciones del proveedor se ajustan como medidas para hacer frente a un riesgo) y aceptados (basados en factores externos) (ISO, ISO/IEC 27002, 2005), sin embargo estas consideraciones no serán determinantes para la selección de controles que harán parte del marco de seguridad para la computación en la nube.

3.3 EVALUACIÓN DEL RIESGO

Este proceso debe ser realizado por la organización o cliente interesado en mover un activo de información a cualquiera de los diversos modelos de la computación en la nube. Los riesgos durante el proceso de migración no son considerados.

Este proceso puede efectuarse similarmente a la evaluación de riesgos de seguridad para la computación tradicional según la ISO/IEC 27002:2005 pero se deben considerar la gestión de un tercero y el modelo de servicios en la nube. El proceso es un método rápido para determinar dependiendo del servicio en la nube, qué controles debe implementar para la prevención del riesgo. Los siguientes son los pasos que deben considerarse (ver figura 12)

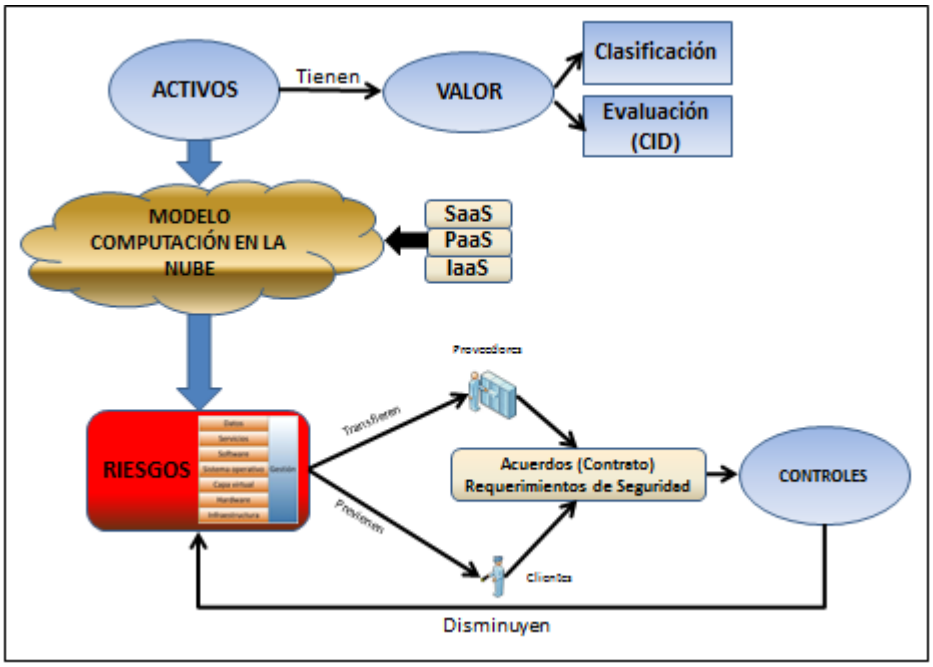


Figura 12. Modelo de Evaluación de Riesgos.

1. Identificar activo (Información, servicio, aplicación)
2. Clasificar el activo.
3. Evaluar los criterios de confidencialidad, integridad y disponibilidad de los activos (Valorar los activos).
4. Identificar en qué modelo de servicio de la computación en la nube se halla el activo.
5. Seleccionar los riesgos para cada uno de los dominios del modelo de computación en la nube, de acuerdo con el modelo de servicio.
6. Determinar el grado de control y responsabilidades, dependiendo de los requisitos de seguridad y los acuerdos establecidos con el proveedor del servicio (transferencia de los riesgos).
7. Seleccionar los controles correspondientes a los riesgos asociados al activo, de acuerdo con su valoración, impacto, frecuencia y costo de implementación (Si el impacto es mínimo por la pérdida en las características de alguna de las propiedades de los activos y el costo es alto, se efectúa un análisis costo vs. beneficio para la consideración de la implementación de control).
8. Mejora continúa basada en los resultados de la implementación de controles y la mitigación del riesgo.

3.4 DIVISIÓN DE RESPONSABILIDADES

Existen dos actores principales responsables de la seguridad del sistema al hacer uso de la computación en la nube: Proveedor de servicios en la nube y el cliente (NIST, 2011). El proveedor de servicios en la nube dispone de la infraestructura alojada en sus instalaciones físicas para hospedar los servicios, aplicaciones y datos del cliente, el cliente es la organización o empresa que contrata los servicios en la nube, paga por ello y a su vez ofrece servicios a usuarios internos o clientes de la organización. En la siguiente figura se ilustran dichos conceptos.

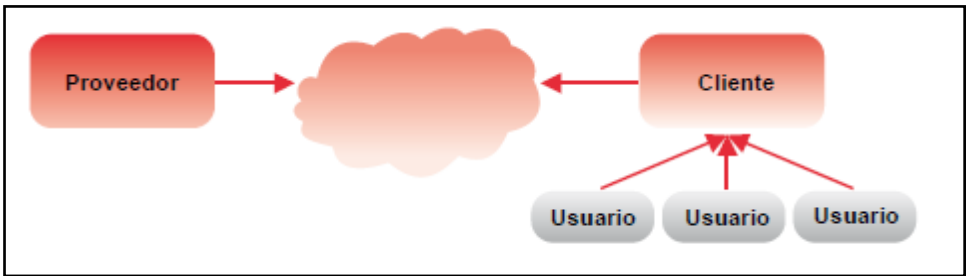


Figura 13. Actores Responsables de la Seguridad

Los controles y medidas de seguridad para la protección de la información sensible hospedada en la nube debe considerarse como un trabajo colaborativo entre los dos actores debido a que ambas partes deben asumir responsabilidades individuales; sin embargo, el estándar PCI recomienda que todos los servicios ofrecidos por la computación en la nube deben ser individualmente revisados para determinar las responsabilidades entre los actores (cliente-proveedor). La siguiente figura ilustra la responsabilidad por parte de los interesados, se identifica que la responsabilidad varía, dependiendo del tipo de servicio o modelo de despliegue, por ejemplo se puede evidenciar que en el modelo de Infraestructura como servicio (IaaS) el proveedor tiene más responsabilidad por los controles que en el modelo de Software como servicio (SaaS).

Figura 14. División de Responsabilidades para Cada Modelo de Servicios

En esta gráfica se observa cómo se dividen las responsabilidades en la implementación de controles para cada uno de los dominios.

3.4.1 Responsabilidad por la Seguridad por Parte del Proveedor (ENISA, 2009)

El proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesamiento de datos, debe impedir el acceso físico no autorizado a sus instalaciones, también debe garantizar el mantenimiento y actualización a nivel de hardware y equipos de comunicaciones (En todos los modelos de servicios de la computación en la nube) y sus responsabilidades varían dependiendo del modelo de servicios. A continuación la siguiente tabla resume en forma general las responsabilidades del proveedor para cada uno de los modelos de servicios de la computación en la nube.

SaaS	PaaS	IaaS
Controles de inicio de sesión y logs de auditoría.		
Seguridad de configuración de la plataforma (reglas de firewall, IDS/IPS, etc.)		
Seguridad de mantenimiento de la plataforma (firewall, IDS e IPS , Antivirus, Filtrado de paquetes).		
Procedimientos de aseguramiento (Hardening) de servidores.		
Gestión de Actualizaciones de Sistema operativo y Aplicaciones.		
Sistemas de Monitoreo.		
Seguridad de la infraestructura física y disponibilidad servidores, centros de almacenamiento, ancho de banda de red, etc)		
Seguridad capa de virtualización (Hipervisor, dispositivos virtuales, etc.)		
Infraestructura de soporte (Energía, refrigeración, cableado, suministros, etc.)		

Tabla 2. Responsabilidades por Parte del Proveedor

3.4.2 Responsabilidad por la Seguridad por Parte del Cliente

Las responsabilidades en la implementación de los controles es básicamente el marco de seguridad que se desarrolló durante este trabajo de maestría. El conjunto de controles ofrecidos son de cara al cliente. Estos controles también dependen del modelo de servicio de la computación en la nube y se clasifican por dominios según el modelo de la nube, por ejemplo en el modelo Software como servicio, en donde la gran parte de los controles están del lado del proveedor, el cliente u organización debe únicamente implementar controles de gestión tales como cumplimiento, control de acceso entre otros sobre la información alojado en los servicios de la nube.

3.5 RIESGOS

Los riesgos de la computación en la nube son innumerables, al igual que en la computación tradicional, este es un conjunto de riesgos que ayudan a entender la problemática de este nuevo modelo de servicio y proporcionará una base para la implementación de controles enfocados al manejo de los riesgos.

Los riesgos se pueden tratar de cuatro formas: aceptándolos, mitigándolos, transfiriéndolos o evitandolos (ISO, ISO/IEC 27005, 2008). Cuando una compañía pasa sus servicios locales a un modelo de computación en la nube se tiende a pensar que los riesgos se transfieren y por este motivo no deben ser atendidos, lo que realmente pasa es que el control que se debe tomar al transferirlos es

diferente para poder tratarlos, por otro lado existen nuevos riesgos que aparecen y se deben tener en cuenta.

3.5.1 Gestión

1. Una baja frecuencia de actualización en el análisis y gestión, los riesgos deben revisarse periódicamente ya que pueden cambiar o aparecer nuevos.
2. Explotación de las vulnerabilidades del sistema por insuficiente análisis de vulnerabilidades y pruebas de penetración.
3. El proveedor puede no cumplir las expectativas de mitigación de los riesgos transferidos a él.

Aspectos Legales

1. Fuga de información.
2. Auditorías hechas por personas no independientes a lo auditado.
3. Disminución o no disponibilidad de los servicios e información sin que esto genere una reacción por parte del proveedor para restablecerlos.
4. Las políticas y procedimientos del cliente y el proveedor no están alineados.
5. No existan incentivos para la resolución de incidentes o aplicar cambios por parte del proveedor de servicios en un tiempo corto.

Cumplimiento

1. Debido a la capacidad de prestar los servicios de cómputo o almacenamiento de información en diferentes países, las leyes de cada país aplican como una sola.
2. La necesidad hacer mantenimientos reactivos o proactivos, el proveedor sólo informa y no solicita una ventana de mantenimiento.

Control de Acceso

1. El acceso a la plataforma, aplicaciones o datos puede darse desde cualquier lugar y cualquier persona que conozca el usuario y clave.
2. Los accesos dados por el proveedor implican que él puede sobrepasar los controles de acceso establecidos.
3. Las aplicaciones expuestas en internet puede incrementar los riesgos de acceso no autorizado.
4. La Suplantación, debido a que no se cuenta con autenticación de doble factor
5. Se pueden interceptar las claves que son distribuidas desde el proveedor hacia los clientes

Gestión de la continuidad del negocio

1. El proveedor de servicios no cuenta con un plan de continuidad de negocio
2. El plan de recuperación ante desastres no está asegurado.

Operación del servicio

1. Débil gestión y manejo de incidentes
2. Débil cadena de custodia en Investigación Forense

3.5.2 Centro de Datos

1. Acceso físico a personal no autorizado
2. El personal autorizado para ingresar al centro de datos no depende del cliente
3. Falla en los servicios de suministros del proveedor, como energía eléctrica o agua
4. Daño o interferencia en las Instalaciones
5. Amenazas externas (Incendio, terremoto, incendio, explosión, manifestaciones sociales y otras formas de desastre)
6. Amenazas o peligros del entorno
7. Fuga de información
8. Funcionamiento inadecuado de los sistemas de alarma
9. Falla de los equipos por falta o inadecuado mantenimiento.

3.5.3 Hardware y Redes de Computación

1. Intercepción de la información
2. Expansión de recursos de computo, almacenamiento o de redes no es eficiente
3. Sistemas con un único punto de falla
4. Otras personas pueden acceder a la información por redes físicas, lógicas o de monitoreo, por una mala segmentación de los discos o procesamiento
5. Actividades de Procesamiento no deseadas
6. Falta de disponibilidad de los recursos
7. Fuga de información
8. Acceso no autorizado a Sistemas y aplicaciones
9. Falla en la gestión de las capacidades y recursos del sistema
10. No disponibilidad de los servicios de comunicación

3.5.4 Capa Virtual

1. El hipervisor puede tener vulnerabilidades o problemas de seguridad (CSA, 2009)
2. Acceso ilimitado a los recursos e información del administrador del hipervisor.
3. Existe la posibilidad de un ataque de punto ciego
4. Robo de máquinas virtuales o de sus imágenes
5. La multiposesión de recursos puede tener como resultado que se pueda acceder a recursos no deseados
6. La información que está en los centros de datos del proveedor no es regresada al cliente después de terminar el contrato de prestación de servicios.
7. Las máquinas virtuales y las imágenes son vulnerables al robo o modificación (CSA, 2009)
8. Máquinas virtuales que necesitan ser borradas efectivamente no lo son.
9. Único punto de falla del hipervisor
10. Existen múltiples puntos de acceso a los sistemas desde la plataforma virtual
11. Alojamiento en máquinas virtuales de diferentes niveles de confianza.
12. Falta de separación de funciones de los administradores
13. Software malintencionado que pretenda burlar las protecciones del hipervisor para tener acceso a otras máquinas virtuales o incluso al sistema anfitrión.
14. Protección inadecuada de las máquinas virtuales (CSA, 2009)
15. Máquinas virtuales de zona de confianza y con los controles tradicionales de seguridad basados en red convencional (CSA, 2009)
16. Problemas de rendimiento que surgen de la CPU y memoria utilizada para la seguridad y operaciones complejas (CSA, 2009)
17. Las máquinas virtuales preformadas no son aseguradas para cada cliente
18. Diferentes tipos de datos pueden mezclarse en una misma máquina física y comparten un mismo común denominador de seguridad (CSA, 2009)
19. Mala configuración de imágenes o manipuladas antes de inicializarse (CSA, 2009)
20. El movimiento de máquinas virtuales entre servidores físicos no deja rastro para auditorias y supervisión de seguridad (CSA, 2009).

3.5.5 Aplicaciones

1. Instalación de aplicaciones no autorizadas
2. Procesamiento correcto de las aplicaciones

3. Interoperabilidad de las aplicaciones en ambientes virtuales
4. Aplicaciones, interfaces y APIs inseguras

3.5.6 Información y servicios

1. Protección de datos sensibles ya que el proveedor no conoce que información es confidencial, de uso interno, público o secreto
2. Borrado seguro de los datos del cliente, inclusive las copias de seguridad (TANIMOTO, 2011)
3. El no cumplimiento de los acuerdos de niveles de servicio
4. El no pacto de umbrales puede resultar en un desempeño menor sin generar indisponibilidad
5. Datos abandonados de la organización pueden ser interceptados o pueden ser accedidos por terceros que administran infraestructura ajena
6. Robo de Información en Instalaciones del Proveedor

4. VALIDACIÓN DE LA PROPUESTA

El modelo propuesto se validó a través de un panel de expertos conformado por clientes, proveedores y auditores con experiencia en el modelo de computación en la nube.

Los clientes son jefes o gerentes de tecnología en empresas del sector real, las cuales tienen servicios alojados en nubes comunitarias desde hace algunos años con modelos de IaaS, PaaS y SaaS, las principales recomendaciones son las asociadas con la implementación de los controles por su extensión. Para este caso se debería hacer un proyecto para el manejo de riesgos, en el cual se priorizan los riesgos a mitigar de acuerdo a criterios de cada organización, para mitigar los riesgos seleccionados se pueden implementar algunos controles, aunque la ventaja del modelo de computación en la nube es que algunos controles deben ejecutarse por parte del proveedor y el cliente únicamente debería hacer auditoria si se están haciendo correctamente.

Los proveedores son gerentes o líderes de equipos de empresas que prestan servicios de computación en nubes comunitarias, las principales recomendaciones son que la computación en la nube se trata en el documento desde un punto de vista ideal y académico en el cual no se tienen en cuenta todas las posibilidades que existen en las negociaciones, las diferentes responsabilidades que los proveedores asumen o no y por ultimo el aprovisionamiento de recursos que no se hace de manera tan automática y transparente para el usuario. Debido a la variedad de modelos de servicio que se pueden ofrecer en la computación en la nube es bueno generar unos patrones y desde allí poder hacer las particularizaciones pertinentes.

Los auditores son consultores de seguridad y expertos en riesgos, quienes avalaron los diferentes marcos de trabajo utilizados aunque hicieron la salvedad de particularizar a cada empresa que quiera implementarlo.

El modelo ha servido en particular a la empresa Colombina S.A., donde se han implementado algunos controles como controles de acceso e implementado seguridad en los centro de datos alternos, además de auditorias continuas a los procesos y procedimientos acordados

En conclusión el modelo se valida teniendo en cuenta que existen particularidades que se deben revisar en cada caso.

El resultado de las validaciones se refleja en la siguiente figura (figura 15), en ella se ilustra la puntuación de uno a cinco promedio de siete ítems que nos permitan

realimentación del modelo de computación en la nube según el panel de expertos seleccionado, la figura 16 nos ofrece información individual sobre la puntuación de cada uno de los panelistas a las preguntas de validación del modelo.

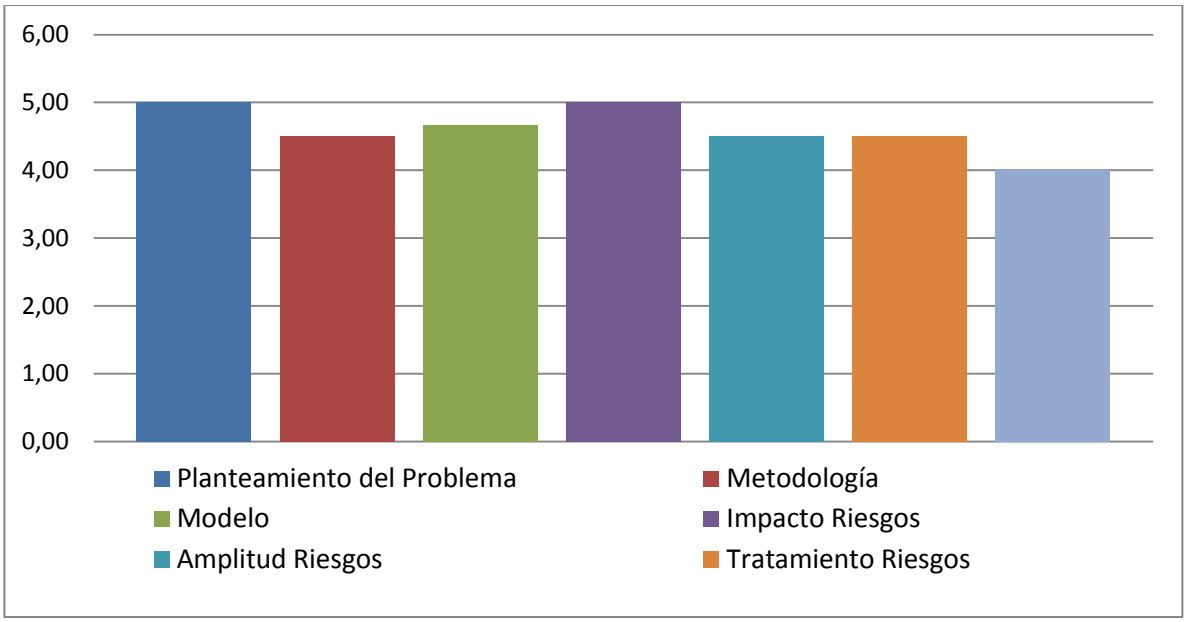


Figura 15. Validación Promedio del Modelo

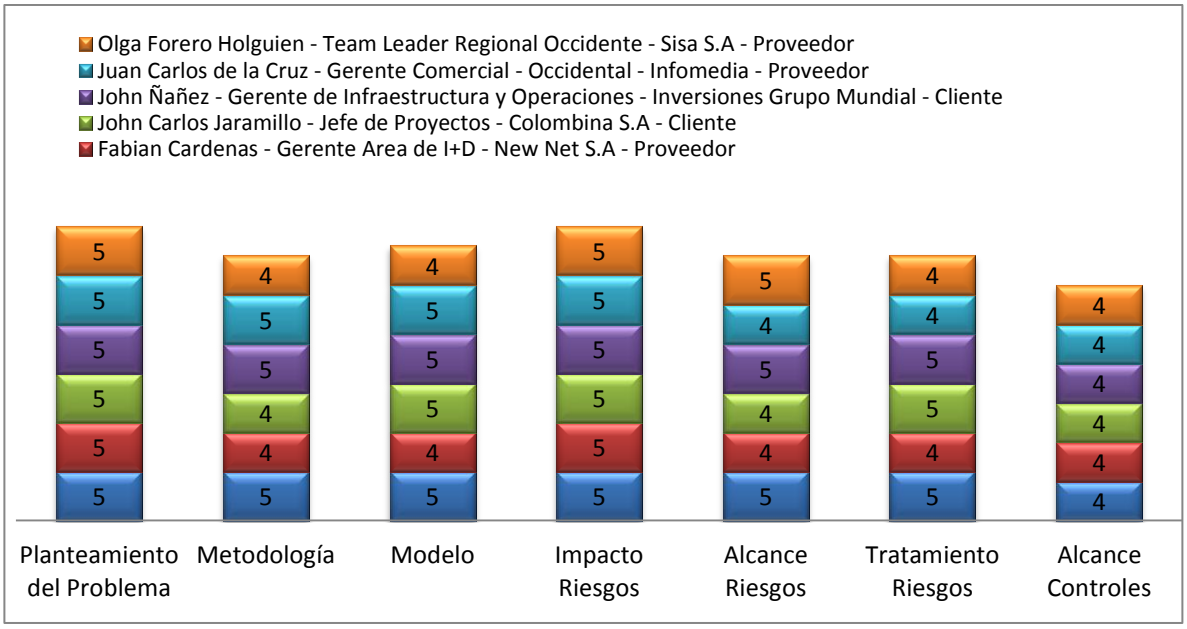
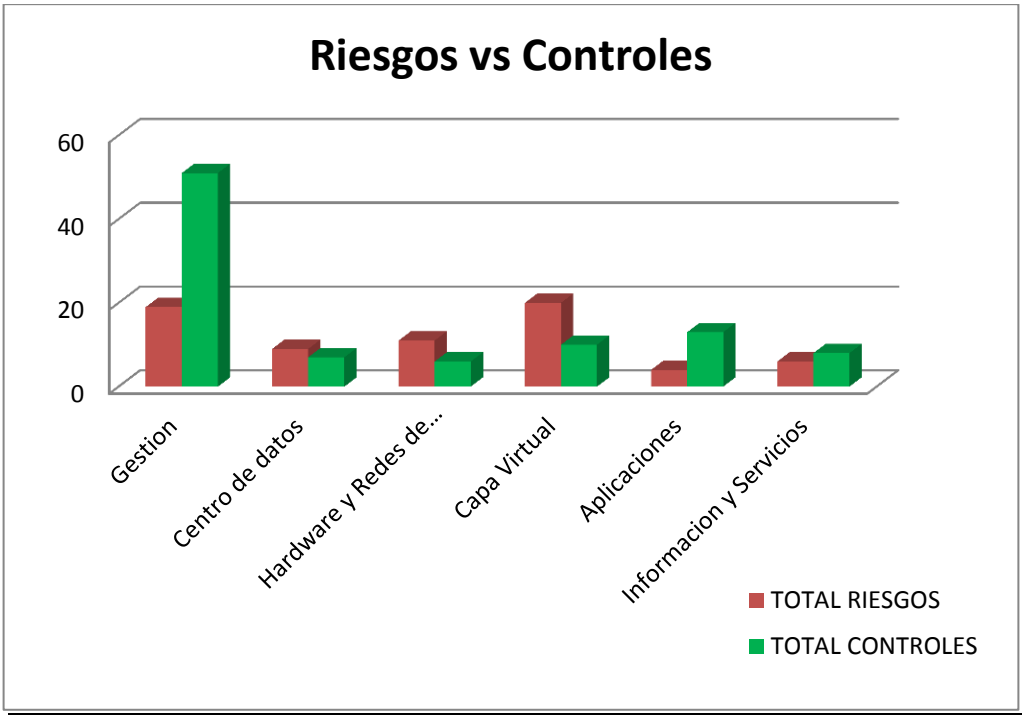


Figura 16. Validación de Resultados por Juicio de Expertos

5. RESULTADOS OBTENIDOS

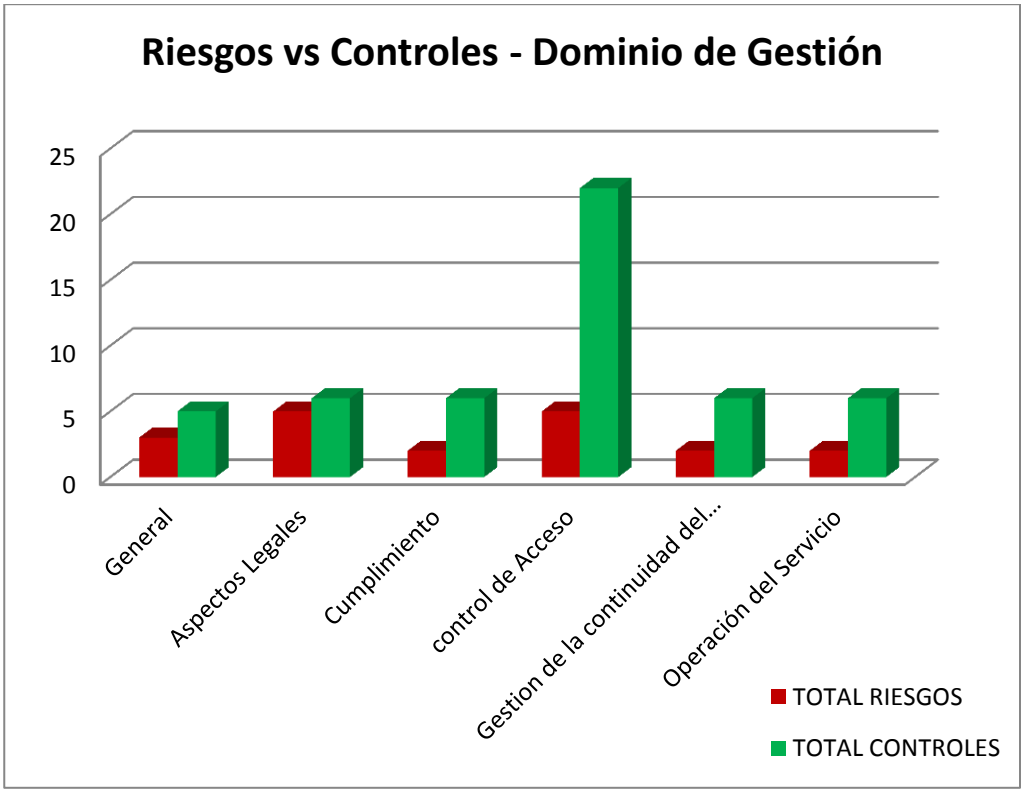
Siguiendo la metodología propuesta para hallar controles que deben ser considerados de cara al cliente para cada uno de los diferentes modelos de servicios y para los modelos de implementación privado o comunitario, donde la infraestructura física se encuentra alojada en las instalaciones del cliente, se encontró un total de 69 riesgos y 95 controles, que se clasificaron para cada uno de los dominios del modelo de computación en la nube con el que se trabajó a lo largo del desarrollo de esta investigación. (Figura 15)



DOMINIO	TOTAL RIESGOS	TOTAL CONTROLES
Gestión	19	51
Centro de datos	9	7
Hardware y Redes de Computación	10	6
Capa Virtual	20	10
Aplicaciones	4	13
Información y Servicios	6	8

Figura 17. Clasificación Riesgos y Controles por Dominio.

El dominio de gestión, debido a su complejidad operativa y extensión se subdivide para su clasificación como lo muestra la siguiente figura



DOMINIO GESTION	TOTAL RIESGOS	TOTAL CONTROLES
General	3	5
Aspectos Legales	5	6
Cumplimiento	2	6
control de Acceso	5	22
Gestión de la continuidad del Negocio	2	6
Operación del Servicio	2	6

Figura 18. Clasificación Riesgos y Controles Dominio de Gestión

La lista completa de controles no es exhaustiva y de acuerdo al modelo, la implementación o a las responsabilidades adquiridas durante la contratación pueden ser necesarios controles adicionales para evitar, prevenir, mitigar o transferir los riesgos nuevos. También destacamos que la clasificación de riesgos y controles dentro de los dominios del modelo de la nube no es rigurosa, un riesgo

puede afectar a cualquiera de los dominios, por ejemplo la fuga de información puede presentarse en cualquiera de los dominios del modelo de la nube, sin embargo se incluye únicamente en los dominios en los cuales el impacto de la materialización de riesgo puede ser crítico, esta clasificación es subjetiva y se hizo basados en los criterios y conocimientos de los desarrolladores del trabajo. Ocurre el mismo escenario para los controles, estos pueden aplicarse a varios dominios del modelo.

Los controles obtenidos, un total de 95, fueron extraídos de varias fuentes como marcos de trabajo en seguridades ya existentes y algunos estandarizados como se menciona en la metodología. A continuación la siguiente figura ilustra la distribución porcentual de los controles.

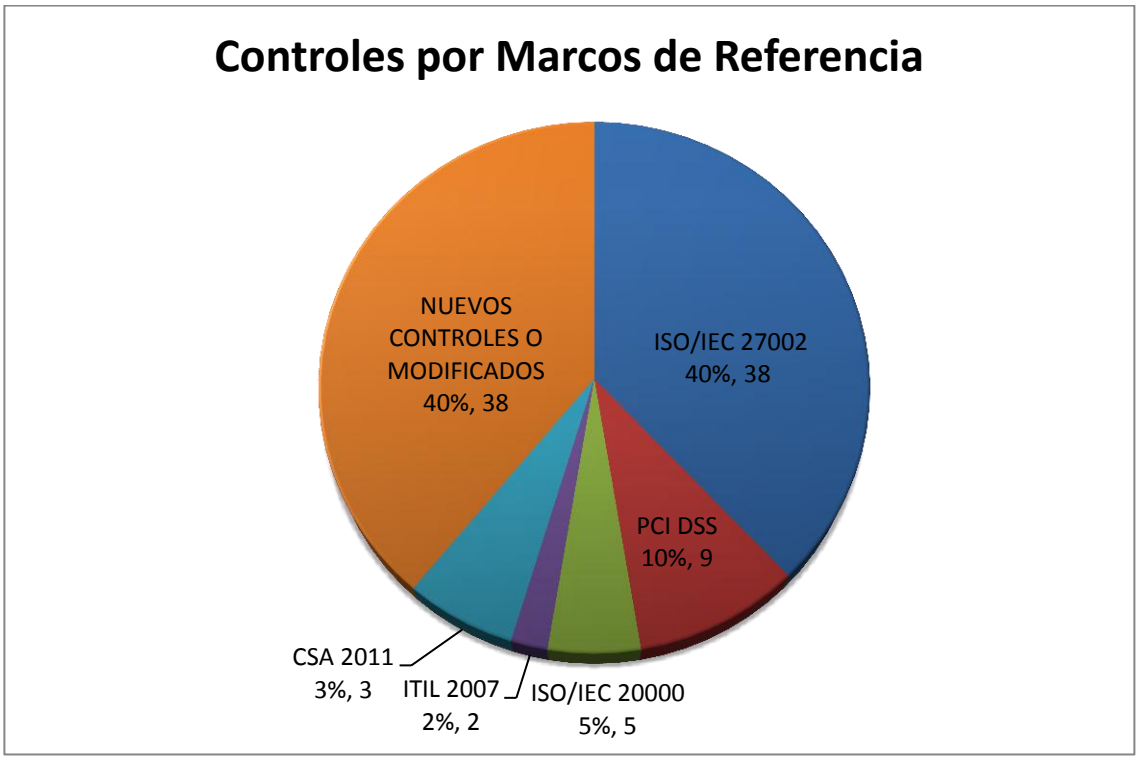


Figura 19. Controles por Marcos de Referencia

De acuerdo con la figura 17 se concluye que la norma ISO/IEC 27002:2005 constituye una base importante de controles útiles para el tratamiento de los riesgos cuando se piensa migrar los servicios a la nube privada o comunitaria en cualquiera de sus modelos de servicios. Los controles de esta norma fueron utilizados principalmente para apoyar el dominio de gestión, el cual involucra los riesgos asociados con las personas, las operaciones, la organización y otros

aspectos no tan técnicos, como sí lo hace por ejemplo el estándar PCI DSS, que ofrece principalmente este tipo de controles.

La siguiente gráfica resume el total de controles de los marcos de seguridad utilizados para cada uno de los dominios.

DOMINIOS		ISO/IEC 27002	PCI DSS	ISO/IEC 20000	ITIL 2007	CSA 2011	NUEVOS o MODIFICADOS	TOTAL
Gestión	General	3					2	**5**
	Aspectos Legales	1		1		1	3	**6**
	Cumplimiento	4					2	**6**
	Control de Acceso	11	8				3	**22**
	Continuidad del Negocio	5					1	**6**
	Operación del Servicio	1		1	2		2	**6**
Centro de datos		1		1			5	**7**
Hardware y Redes de Computación		1					5	**6**
Capa Virtual			1				9	**10**
Aplicaciones		7					6	**13**
Información y Servicios		4		2		2		**8**
TOTAL CONTROLES		**38**	**9**	**5**	**2**	**3**	**38**	**95**

Tabla 3. Resumen Controles vs Marcos de Seguridad.

Los objetivos de control y los controles se listaran en la siguiente sección 5.1. Estos están clasificados por dominio. La lista puede no ser exhaustiva y una organización que tenga sus servicios e información en nubes privadas y/o comunitarias puede considerar que son necesarios objetivos de control y controles adicionales. Los controles obtenidos en este modelo especifican el que debe hacerse, sin embargo no proporcionan orientación para la implementación de las mejores prácticas. Desarrollar un marco de seguridad para computación en la nube que incluya una guía de implementación se deja para un futuro trabajo de grado debido a la extensión y complejidad inherente a la nube.

5.1 CONTROLES

5.1.1 Controles de Gestión

Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. (ISO, ISO/IEC 27002, 2005).

1. Política de seguridad para servicios en la nube
   Control: Se debería implementar una política de gestión de la seguridad (directrices a nivel corporativo sobre uso de los servicios y recursos informáticos con el objetivo de proteger la información) documentada, revisada periódicamente y comunicada a todos los empleados y partes externas considerando los requisitos de seguridad de la organización, reglamento y leyes pertinentes y análisis de riesgos. (ISO, ISO/IEC 27002, 2005)

   La política es moldeada por estas cuatro variables:
   - ✓ Tipo de servicio de la nube (IaaS, PaaS, SaaS).
   - ✓ Si el modelo de implementación es privada o comunitaria.
   - ✓ Cuánto control se tiene sobre los sistemas operativos, software y hardware.
   - ✓ Cómo se aplica la política de umbrales (IBM, 2011)

2. Compromiso de la dirección con la seguridad de la información.
   Control: Apoyo y compromiso por parte de la dirección con la seguridad de la información asignando las responsabilidades y roles específicos y verificando la ejecución de la política de seguridad. (ISO, ISO/IEC 27002, 2005)

3. Coordinación y asignación de responsabilidades para la seguridad de la información.
   Control: La seguridad de la información debería ser coordinada por representantes de cada una de las áreas de la organización y sus responsabilidades deben ser documentadas, asignadas y comunicadas. (ISO, ISO/IEC 27002, 2005).

4. Gestión del riesgo.
   Control: Se deberían hacer análisis y gestión de los riesgos periódicamente.

5. Pruebas de penetración y hacking ético.
   Control: se deberían hacer periódicamente pruebas de penetración y de hacking ético para evaluar las vulnerabilidades del sistema.

Aspectos Legales

Los aspectos legales son el eje central de los controles de seguridad, estos son necesarios para implementar los demás controles, también es un

escenario para los temas de cumplimiento, acuerdos de niveles de servicio, umbrales y de confidencialidad.

1. Acuerdo sobre la confidencialidad.
   Control: Los acuerdos de confidencialidad y de no-divulgación deberían ser parte integral del contrato de prestación de servicios, especificando las responsabilidades y acciones por el no cumplimiento, salvaguardando la confidencialidad de la información. (ISO, ISO/IEC 27002, 2005)

2. Auditorías independientes.
   Control: Revisiones independientes y evaluaciones se efectuarán al menos una vez al año, o en intervalos planificados, para asegurar que la organización cumple con las políticas, procedimientos, normas y los requisitos reglamentarios aplicables (es decir, internos / externos auditorías, certificaciones, la vulnerabilidad y pruebas de penetración) (CSA, 2011)

3. Acuerdos de niveles y umbrales de los servicios
   Control: Los servicios prestados deberían contar con uno o más acuerdos de niveles de servicio y los umbrales permitidos, estos deberían estar estipulados explícitamente en el contrato de servicios. (ISO, ISO/IEC 20000, 2008)

4. Entrega de información
   Control: Debería ser parte del contrato los procedimientos y mecanismos para la entrega de información en el momento de terminación del contrato.

5. Políticas y normas de seguridad como parte integral del contrato
   Control: Las políticas de seguridad de la información del cliente deberían ser parte integral del contrato.

6. Clausulas de cumplimientos
   Control: Deberían existir penalizaciones por el no cumplimiento de los acuerdos establecidos, estas penalizaciones deberían estar estipuladas en el contrato.

Cumplimiento

El Objetivo es evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad, se debe tener en cuenta que los servicios de computación en la nube pueden alojarse o ser accedidos desde otros países lo que hace que el cumplimiento deba tener especial cuidado.

1. Derecho de auditoria

Control: Se debe garantizar por medio del contrato de servicios el derecho a hacer auditorias físicas y lógicas de los sistemas.

2. Identificación de la legislación aplicable
   Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.

3. Protección de los registros de la organización
   Control: Los registros importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio. (ISO, ISO/IEC 27002, 2005).

4. Protección de los datos y privacidad de la información personal
   Control: Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato. (ISO, ISO/IEC 27002, 2005).

5. Reglamentación de los controles criptográficos
   Control: Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes. (ISO, ISO/IEC 27002, 2005).

6. Verificación del cumplimiento técnico
   Control: Los sistemas de información se deberían verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad. (ISO, ISO/IEC 27002, 2005)

Control de Acceso

Los conceptos de identidad, derechos y control de acceso requieren un cambio fundamental respecto a la informática tradicional (Autenticación se realiza usando sistemas de autenticación local) cuando utilizamos computación en la nube (Aplicación que valida las identidades provenientes de múltiples fuentes externas junto con sus atributos para permitir el acceso al sistema, procesos y datos). (CSA, 2011)

1. Registro de usuarios.
   Control: Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. (ISO, ISO/IEC 27002, 2005).

2. Gestión de privilegios.

Control: Se debería restringir y controlar la asignación y el uso de privilegios (ISO, ISO/IEC 27002, 2005), establezca un sistema de control de acceso para los componentes del sistema con usuarios múltiples que restrinja el acceso basado en la necesidad del usuario de conocer y que se configure para negar todo, salvo que se permita específicamente. (PCI, PCI DSS (PCI Data Security Standard), 2011).

3. Gestión de contraseñas para usuarios.
   Control: La asignación de contraseñas se debería controlar a través de un proceso formal de gestión. (ISO, ISO/IEC 27002, 2005).

4. Revisión de los derechos de acceso de los usuarios.
   Control: La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios. (ISO, ISO/IEC 27002, 2005).

5. Restringir el acceso directo a las aplicaciones desde internet.
   Control: Se debería implementar formas de acceder a los servicios sin exponerlos directamente a internet como una red privada virtual (Virtual Private Network – VPN); si el servicio es nativo de internet como correo electrónico o paginas web se deberían tener controles adicionales como zonas desmilitarizadas y servidores para la interacción con los usuarios (Front-End) y servidores de procesamiento de datos (back-end). (PCI, PCI DSS (PCI Data Security Standard), 2011)

6. Uso de contraseñas
   Control: Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

7. Política de uso de los servicios en red.
   Control: Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados. (ISO, ISO/IEC 27002, 2005).

8. Autenticación de usuarios para conexiones externas.
   Control: Se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos. (ISO, ISO/IEC 27002, 2005).

9. Acceso a los sistemas de computo
   Control: No permita ninguna conexión directa de entrada o salida de tráfico entre Internet y los sistemas de computo (PCI, PCI DSS (PCI Data Security Standard), 2011)

10. Identificación y autenticación de usuarios

Control: Todos los usuarios deberían tener un identificador único (ID del usuario) únicamente para su uso personal, y se debería elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario. (ISO, ISO/IEC 27002, 2005)

11. Sistema de gestión de contraseñas
    Control: Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. (ISO, ISO/IEC 27002, 2005).

12. Uso de las utilidades del sistema
    Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación. (ISO, ISO/IEC 27002, 2005).

13. Tiempo de inactividad de la sesión.
    Control: Las sesiones inactivas se deberían suspender después de un periodo definido de inactividad. (ISO, ISO/IEC 27002, 2005).

14. Limitación del tiempo de conexión.
    Control: Se deberían utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo. (ISO, ISO/IEC 27002, 2005)

15. Restricción del acceso a la información.
    Control: Se debería restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso. (ISO, ISO/IEC 27002, 2005).

16. Computación y comunicaciones móviles
    Control: Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

17. Dispositivos y aplicaciones de prevención
    Control: Se deberían implementar dispositivos o aplicaciones tales como firewalls, detectores de intrusos (Intrusion detection system - IDS), sistemas de prevención de intrusión (intrusion prevention system- IPS) y zonas desmilitarizadas. (PCI, PCI DSS (PCI Data Security Standard), 2011)

18. Cifrado de acceso

Control: Cifre todo el acceso administrativo que no sea de consola utilizando un cifrado sólido. Utilice tecnologías como SSH, VPN o SSL/TLS para la administración basada en la web y el acceso administrativo que no sea de consola.

19. Distribución segura de claves
    Control: Verifique que los procedimientos de administración de claves se hayan implementado para solicitar la distribución de claves seguras y nunca debe enviar claves no cifrados por medio de tecnologías de mensajería de usuario final (por ejemplo, el correo electrónico, la mensajería instantánea, el chat, etc.). (PCI, PCI DSS (PCI Data Security Standard), 2011).

20. Limite el acceso a los componentes del sistema
    Control: Se debe limitar el acceso a los componentes y a los datos a aquellos individuos cuyas tareas necesitan de ese acceso. (PCI, PCI DSS (PCI Data Security Standard), 2011)

21. Cobertura de todos los componentes del sistema
    Control: Confirme que los sistemas de control de acceso se implementen en todos los componentes del sistema. (PCI, PCI DSS (PCI Data Security Standard), 2011).

22. Autenticación mediante dos o mas factores
    Control: Los usuarios deberían tener mas de un método para la autenticación en los sistemas. (PCI, Information Supplement: PCI DSS Virtualization Guidelines, 2011)

Gestión de la continuidad del negocio

Un plan de recuperación ante desastres es un documento basado en estas cinco principales actividades: prevención de incidentes, detección de incidentes, respuesta a incidentes, recuperación y mejoramiento. (ISO, ISO/IEC 27031, 2011)

1. Política de recuperación ante desastres.
   Control: Se debería contar con una política de recuperación ante desastres que demuestre el compromiso de la alta dirección, su alineamiento con los objetivos de la organización, delimitada incluyendo limitaciones y exclusiones, aprobada y firmada por la alta dirección, comunicada y revisada en intervalos de tiempo establecidos. (ISO, ISO/IEC 27031, 2011).

2. Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio.

Control: Se debiera desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización. (ISO, ISO/IEC 27002, 2005).

3. Continuidad del negocio y evaluación del riesgo.
   Control: Identificar eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información. (ISO, ISO/IEC 27002, 2005).

4. Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información.
   Control: Desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos. (ISO, ISO/IEC 27002, 2005).

5. Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio.
   Control: Los planes de continuidad del negocio debieran ser probados y actualizados regularmente para asegurar que sean actuales y efectivos. (ISO, ISO/IEC 27002, 2005).

6. Servicios e información en contingencia
   Control: Se deberían evaluar los riesgos y aplicar los controles de seguridad a la información y los sistemas de contingencia.

Operación del servicio

La gestión sobre los activos debería ser permanente en la operación del servicio ya que podría impactar fundamentalmente a la disponibilidad, esta se puede ver afectada como parte inherente a la operación y se debería tratar desde las acciones preventivas hasta las correctivas para tener el menor tiempo de solución con el menor impacto posible.

1. Reporte sobre los eventos de seguridad de la información
   Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible. (ISO, ISO/IEC 27002, 2005)

2. Capacitación a los usuarios

Control: los usuarios deberían recibir capacitaciones periódicas para poder identificar los eventos de seguridad de la información.

3. Gestión de alertas
   Control: Tener alertas que permitan detectar que se ha superado un umbral, que algo ha cambiado o que hubo un fallo

4. Gestión de incidentes
   Control: Se debería contar con un plan de acción para resolver los incidentes tan pronto como sea posible y llevar un registro para extraer información sobre los de las posibles causas. (ITIL, 2007)

5. Gestión de problemas
   Control: Se debería tener un proceso que permita prevenir problema e incidentes que han pasado, para eliminar incidentes recurrentes y minimizar el impacto de los incidentes que no pueden ser prevenidos. (ITIL, 2007)

6. Gestión de cambios
   Control: Todos los cambios deberían ser evaluados, aprobados e implementados de manera controla y deberían incluir la forma en la que se va a revertir o remediar si el cambio no tiene éxito. (ISO, ISO/IEC 20000, 2008)

5.1.2 Controles de Centro de Datos o Infraestructura

Los centros de datos son custodiados por las empresas prestadoras del servicio en todos los modelos de servicio de computación en la nube, esto hace que los riesgos sean transferidos al proveedor sin que esto implique que se estén controlando correctamente. Se deben tener contratados acuerdos de niveles de servicio para comprometer la disponibilidad de los sistemas y el principal rol del cliente es implementar controles de auditoria para garantizar que estos acuerdos se cumplan y que los riesgos se estén mitigando correctamente. Se podrían utilizar normas internacionales para centros de datos como TIA-942 (Telecommunications Infrastructure Standard for Data Centers) o GR-3160 (NEBS Requirements for Telecommunications Data Center Equipment and Spaces) para garantizar el correcto diseño, uso, operación y gestión.

1. Auditoria de control de acceso físico
   Control: se deben hacer revisiones periódicas a los procesos y procedimientos que controlan el acceso físico a los centros de datos.

2. Auditoria en el control de amenazas externas

Control: se deben hacer revisiones periódicas a los procesos y procedimientos que mitigan los riesgos de las amenazas externas.

3. Acuerdos de niveles de servicio
   Control: Se deberían firmar acuerdos de niveles de servicio con rangos de aceptación y cargas de trabajo para asegurar la disponibilidad. (ISO, ISO/IEC 20000, 2008)

4. Acuerdos de confidencialidad
   Control: Los acuerdos de confidencialidad y de no-divulgación deberían ser parte integral del contrato de prestación de servicios, especificando las responsabilidades y acciones por el no cumplimiento, salvaguardando la confidencialidad de la información. (ISO, ISO/IEC 27002, 2005)

5. Auditoria de acuerdos con terceras partes
   Control: Se debe evidenciar la gestión de los acuerdos de niveles de servicios que tiene el proveedor con sus proveedores de suministros

6. Auditoria sobre los sistemas de alarmas
   Control: Se debe evidenciar la revisión constante de los sistemas de alarma, se recomendaría un sistema de monitoreo de alarmas.

7. Auditoria sobre el mantenimiento de los equipos
   Control: Se debe evidenciar el mantenimiento continuo de los sistemas y alarmas.

5.1.3 Controles de Hardware de Red y Computación.

Los recursos de hardware en todos los modelos de entrega de computación en la nube son propiedad del proveedor de servicios y los recursos de red se tienen componentes en las instalaciones del proveedor para brindar el acceso único o compartido a los recursos y en las instalaciones del cliente para acceder a estos recursos.

1. Acuerdos de niveles de servicios sobre la expansión de recursos.
   Control: Se deberían tener acuerdos especificando los tiempos de obtención por parte del proveedor, tiempos de implementación, costos y viabilidad técnica para aplicarlos para recursos de cómputo, redes y almacenamiento.

2. Auditoria de análisis de sistemas con único punto de falla.
   Control: Se deberían efectuar análisis constantes para encontrar únicos puntos de falla.

3. Acuerdos con terceras partes.
   Control: El proveedor debería tener acuerdos de aprovisionamiento con terceras partes.

4. Acuerdos de niveles de servicios de las redes de datos.
   Control: Se deberían tener acuerdos sobre los niveles de servicios de las redes de datos, teniendo en cuenta consumo de canales, disponibilidad de estos y tiempo de solución a fallas.

5. Segmentación de la redes de datos.
   Control: Las redes de datos como las de backups y administración deberían estar físicamente separadas o en su defecto segmentadas por VLANs.

6. Acuerdos de confidencialidad.
   Control: Todas las personas que laboren para el proveedor de servicios en la nube deberían firmar acuerdos de confidencialidad con la empresa contratante y ella a vez con la empresa del cliente. (ISO, ISO/IEC 27002, 2005)

5.1.4 Controles de Capa Virtual

Los servicios en la nube son a menudo pero no siempre utilizados en conjunto con, y habilitados por, tecnologías de virtualización. No hay ningún requisito, sin embargo los lazos de abstracción de recursos a tecnologías de virtualización y muchas ofertas de virtualización por hipervisor o S.O no son utilizadas. (CSA, 2011).

1. Aislar las funciones de seguridad
   Control: Implementación en las maquinas virtuales con el mismo proceso de separación del mundo físico de ser necesario incluso mas rigurosos, por que un atacante podría comprometer varios componentes del sistema (PCI, Information Supplement: PCI DSS Virtualization Guidelines, 2011)

2. Aplicar el menor privilegio y mayor separación de deberes
   Control: Se deberían tener una metodología para garantizar el acceso de a los operadores tener los menores privilegios posibles para realizar sus labores y la mayor segregación de funciones.

3. Aseguramiento del hipervisor, las maquinas virtuales y otros componentes
   Control: Se deberían asegurar el hipervisor, las maquinas virtuales y otros componentes y evaluar su seguridad periódicamente

4. Reconocer el carácter dinámico de la capa virtual

Control: Se debería ejecutar todos los controles de seguridad a los componentes físicos en donde puedan correr los servicios de la capa virtual debido a que los componentes de esta capa como los discos virtuales, maquinas virtuales, hipervisores entre otros pueden ejecutarse en distintas maquinas físicas.

5. Multiposesion
   Control: Se deberían segmentar los recursos físicos de tal manera que los componentes de la capa virtual no puedan acceder, ni ser accedidos desde el mismo componente físico con otra capa virtual

6. Monitoreo para ataques de punto ciego
   Control: se deberían efectuar revisiones para evitar ataques desde puntos donde no se puedan monitorear como conmutadores virtuales o arreglo de discos compartidos.

7. Destrucción de datos residuales
   Control: Se deberían tener procedimientos para el manejo de datos residuales, como maquinas virtuales en desuso o terminación

8. Entrega de datos
   Control: Se debería tener un procedimiento en el cual el proveedor de servicios entregue los datos de manera completa, sin alteraciones y cifrada

9. Cifrado de maquinas
   Control: Las maquinas virtuales deberían estar cifradas en copias de respaldo, imágenes del sistema, maquinas apagadas y de ser posible en las maquinas activas.

10. Logs de auditoria
    Control: Se deberían tener y revisar periódicamente los logs de auditoria que contenga el rastro de backups, imágenes de los sistemas, accesos, entre otros.

5.1.5 Controles de las Aplicaciones

Cuando se mueven las aplicaciones a la nube, todos estos controles tradicionales ya no son lo suficientemente eficaces para protegerlas, las aplicaciones ya no residen en una red de confianza en donde los controles tradiciones de seguridad perimetral las protegían, ahora las aplicaciones podrían residir con otras aplicaciones (agrupación de recursos) de otras organizaciones en las instalaciones de un tercero y se pueden acceder desde cualquier tipo de dispositivo. Esto

cambia la naturaleza de los requisitos de seguridad para aplicaciones en la nube y por supuesto los controles que las protegen.

1. Política de seguridad de aplicaciones seguras.
   Control: Se debería contar una política de seguridad de aplicaciones apoyada por la dirección en la cual se debería incluir métricas o registros que permitan el análisis y la revisión periódica. (ISO, ISO/IEC 27002, 2005)

2. Controles contra códigos maliciosos.
   Control: Se deberían implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios. (ISO, ISO/IEC 27002, 2005)

3. Pruebas de Penetración.
   Control: Se deberían hacer pruebas que permitan evidenciar vulnerabilidades resultantes de malas configuraciones del sistema, fallas conocidas o desconocidas del hardware y software, debilidades operativas en procesos o controles técnicos

4. Gestión de Privilegios.
   Control: Se debería tener un proceso formal de autorización que permita restringir y controlar la asignación y el uso de privilegios a los usuarios de acuerdo con sus necesidades o actividades (ISO, ISO/IEC 27002, 2005)

5. Registro de Usuarios.
   Control: Se debería tener un proceso formal de registro y cancelación de usuarios, con el fin de conceder y revocar el acceso a las aplicaciones (ISO, ISO/IEC 27002, 2005)

6. Segregación de Funciones.
   Control: Distribución de funciones y aéreas de responsabilidad para reducir oportunidades de modificación o uso inadecuado de las aplicaciones, ninguna persona debe tener la responsabilidad de, o el acceso a más de una función relacionada (ISO, ISO/IEC 27002, 2005)

7. Procesamiento correcto de las Aplicaciones.
   Control: Para el control de procesamiento correcto de aplicaciones se deberían aplicar los controles del dominio de procesamiento correcto en las de la norma ISO/IEC 27002, Tecnología de la información, Técnicas de seguridad.

8. Pruebas de Interoperabilidad.

Control: Pruebas de interoperabilidad Que permita garantizar la transferencia segura de información a través de aplicaciones utilizando un conjunto común de formatos de intercambio (Protocolos).

9. Monitoreo de actividades.
   Control: Se deberían monitorear contantemente las actividades de los usuarios.

10. Registros de auditoría
    Control: Las actividades deberían dejar registro de todas las actividades de los usuarios y no deberían poderse manipular por los administradores.

11. Supervisión por la dirección
    Control: La dirección debería revisar periódicamente la segregación de funciones, permisos y controles que se hacen a los sistemas y aplicaciones.

12. Aislamiento de sistemas sensibles.
    Control: Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo. (ISO, ISO/IEC 27002, 2005)

13. Restricción del acceso a la información.
    Control: Se debería restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

5.1.6 Controles de la Información y Servicios

La información y los servicios son los únicos puntos donde sin importar el modelo de despliegue la responsabilidad de su gestión es de la organización pero estando en manos del proveedor por esto se deberían generar controles que permitan a la organización mitigar los riesgos asociados.

1. Inventario y asignación de activos de información y servicios
   Control: se deberían inventariar los activos de información y servicios que están en la nube, identificar un propietario por cada uno. (ISO, ISO/IEC 27002, 2005)

2. Uso aceptable de los activos de información
   Control: Los propietarios deberían establecer las reglas para el uso correcto de los activos y servicios. (ISO, ISO/IEC 27002, 2005)

3. Acuerdos de niveles de servicios

Control: Se deberían firmar acuerdos de niveles de servicio con rangos de aceptación y cargas de trabajo para asegurar la disponibilidad. (ISO, ISO/IEC 20000, 2008)

4. Devolución de activos
   Control: El proveedor de servicios de la nube debería devolver todos los activos propiedad de la organización dentro de un marco de tiempo definido y documentado una vez que el contrato ha sido terminado o cuando el cliente lo determine. (CSA, 2011)

5. Clasificación de la información
   Control: La información se debería clasificar en términos de su valor, las restricciones legales, restricciones contractuales, la sensibilidad, la criticidad para la organización y la obligación de un tercero para la retención y prevención de la divulgación no autorizada o uso indebido. (CSA, 2011)

6. Catalogo de servicios
   Control: Se debería definir un catalogo con todos los servicios ofrecidos en la nube con el nombre del servicio, la descripción, metas como por ejemplo el tiempo de restitución un servicio después de una falla mayor, puntos de contacto, horas de servicio y excepciones al igual que los acuerdos de seguridad. (ISO, ISO/IEC 20000, 2008)

7. Etiquetado y manejo de la información
   Control: Se debería etiquetar la información de acuerdo a su clasificación y para cada nivel de clasificación definir los procedimientos de manejo seguros, incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucción. (ISO, ISO/IEC 27002, 2005)

8. Seguridad de los recursos humanos
   Control: Para el tratamiento de las personas tales como usuarios, contratistas y terceras partes, antes, durante y después de la contratación se deberían aplicar los controles del dominio de seguridad de los recursos humanos de la norma ISO/IEC 27002, Tecnología de la información, Técnicas de seguridad.

6. CONCLUSIONES Y TRABAJO FUTURO

1. En términos de seguridad de la información, las economías de escala y la flexibilidad ofrecidas por la computación en la nube privada o comunitaria puede tener impacto positivo en el caso que se requiere menor inversión en medidas de seguridad por que se distribuyen los costos y puede tener impacto negativo a que la concentración masiva de recursos y datos se convierten en un objetivo más atractivo para atacantes.

2. En modelos de computación híbrida, donde se mezclen datos, servicios, aplicaciones o infraestructura del modelo de computación tradicional con el modelo de la nube en cualquiera de sus modelos de servicios, se debe considerar efectuar una evaluación de riesgos independientes para cada uno de los escenarios. Por ejemplo para el modelo de computación tradicional podemos utilizar las medidas o controles de las normas ISO/IEC 27001:2005 o ISO/IEC 27002:2005.

3. La metodología para la obtención de riesgos y controles de la computación en la nube debe seguir un modelo PHVA que permita asegurar controles de seguridad adecuados para garantizar los activos de información.

4. Los controles debe ser examinados periódicamente para reflejar: Nuevos riesgos, disponibilidad de nuevas tecnologías, cambios en los requerimientos de seguridad y experiencia en el uso de los controles.

5. La lista de controles del marco de seguridad no es exhaustiva, por lo cual una organización podría requerir controles adicionales dependiendo de su necesidad, también para la implementación de ellos debe hacerse previa evaluación del riesgo, impacto y probabilidad de que se materialice el riesgo para conducir la estrategia a seguir de tratamiento.

6. Una de las partes fundamentales de la computación en la nube es el contrato, entre cliente y proveedor, en éste se debe prestar especial atención a los derechos y obligaciones relacionadas con el acceso, el control y otros aspectos de seguridad.

7. En cualquiera de los modelos de despliegue de computación en la nube, los datos o información sensible puede residir en cualquier parte del mundo, esto obliga a las empresas a conocer y cumplir con las normas y leyes del país donde la información se ubica físicamente, es decir se vincula a aceptar una jurisdicción concreta.

8. El marco de seguridad de la información desarrollado para nubes privadas o comunitarias no ofrece una guía de implementación sobre las medidas de control, simplemente se especifica qué debe hacer el control, pero no cómo se debe implementar. Se puede considerar para un futuro trabajo el desarrollo de las buenas prácticas para cada uno de estos controles

9. Otra consideración especial para trabajos futuros es realizar una guía de auditoría para el seguimiento en la implementación de controles.

10. El modelo de seguridad de la información para la computación en la nube es un modelo teórico, así como la asignación de riesgos y controles alojados en cada uno de sus dominios, por lo tanto dependiendo del servicio contratado y del tipo de activo se debe particularizar tanto las responsabilidades de cada uno de los actores como los riesgos y controles.

11. Los principales riesgos de seguridad de la información que afectan la computación en la nube en cualquiera de sus modelos de servicios son la privacidad de los datos confidenciales o sensibles de las organizaciones y el acceso no autorizado.

BIBLIOGRAFIA

AUTY, M., CREESE, S., GOLDSMITH, M., & HOPKINS, P. (n.d.). Inadequacies of Current Risk Controls for the Cloud. *2nd IEEE International Conference on Cloud Computing Technology and Science*, 1-8.

CAO AVELLANEDA, J. (2009, 12 9). *Microsoft dando ejemplo en la nube mediante ISO 27001*. Retrieved 11 11, 2011, from http://seguridad-de-la-informacion.blogspot.com/2009/12/microsoft-dando-ejemplo-en-la-nube.html

CSA. (2009). *Cloud Security Alliance*. Retrieved from https://cloudsecurityalliance.org/

CSA. (2011, 11 14). *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0.* Retrieved from https://cloudsecurityalliance.org/

CSA. (15 de 11 de 2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.* Recuperado el 22 de 12 de 2011, de Cloud Security Alliance: https://cloudsecurityalliance.org/

ENISA. (11 de 2009). *Cloud Computing Information Assurance Framework.* Recuperado el 17 de 02 de 2012, de Secure Applications and Services — ENISA: https://www.enisa.europa.eu/activities/application-security

Eucalyptus. (2012, 01 20). *What is Eucalyptus, Cloud Computing Software from Eucalyptus*. Retrieved from http://www.eucalyptus.com/learn/what-is-eucalyptus

GARTNER. (2011). *Cycle to Adoption for Cloud Computing.*

GORMAN, J. -M.-S. (2011). News & Events: Press Releases.

HIGUERA, J. M. (2011, 11 10). *Las empresas están entrando en la nube - Negocios | Portafolio.co*. Retrieved from http://www.portafolio.co/negocios/las-empresas-estan-entrando-%25E2%2580%2598la-nube%25E2%2580%2599

HILLSON, D. (2002, 06). *The Risk Breakdown Structure (RBS) as an Aid to Effective Risk Management.* Retrieved from http://www.risk-doctor.com/pdf-files/rbs0602.pdf

IBM. (2011, 06 23). *Craft a cloud service security policy*. Retrieved 03 21, 2012, from http://www.ibm.com/developerworks/cloud/library/cl-cloudsecurepolicy/index.html

INTENCO, Instituto Nacional de Tecnologías de la Comunicaciones. (Octubre de 2011). *Seguridad y Privacidad del Cloud Computing.* Obtenido de www.inteco.es/file/3LeSufa2tYmC_bcRKSFfbg

ISACA. (2011). *Global Status Report on the Governance of Enterprise IT (GEIT).* Recuperado el 02 de 12 de 2011, de http://www.isaca.org/Knowledge-Center/Research/Documents/Global-Status-Report-GEIT-10Jan2011-Research.pdf

ISO. (2005). *ISO/IEC 27002.*

ISO. (2005). ISO/IEC 27001. *Information security management systems*.

ISO. (2008). *ISO/IEC 20000.* Bogota: ICONTEC.

ISO. (2008). *ISO/IEC 27005.* Suiza.

ISO. (2011). *ISO/IEC 27031.* Siuza.

ITIL. (2007). *Service Operation.* Londres.

JOHNSTON, S. (2011, 10 11). *Cloud Computing and Standards - A Regulator's View.* Retrieved 11 14, 2011, from www.oasis-open.org

LANCHE, D. (2011, 11 12). *www.dinero.com*. Retrieved from http://www.dinero.com/negocios/articulo/en-3-anos-ibm-ha-invertido-us3000-millones-cloud-computing/120422

MALL, P., & GRACE, T. (2011). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology (NIST), Information Technology Laboratory*, 7.

MAUNY, C. (20 de 06 de 2011). *Normalisation ISO et Cloud Computing Cloud Computing Security and Privacy.* Obtenido de

http://www.telindus.lu/resources/20110620-sc27-tls-cloud_computing_security_and_privacy-v1.1.pdf

NIST. (2011, 07). *NIST Cloud Computing Standards Roadmap v1.0.* Retrieved from http://www.navigatingthroughthecloud.com/wp-content/uploads/2012/03/NIST-Cloud-Computing-Standard-Roadmap-2011.pdf?9d7bd4

NIST. (2011, 09). *The NIST Definition Of Cloud Computing.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

PCI. (2011). *Information Supplement: PCI DSS Virtualization Guidelines.*

PCI. (2011, 11 10). *PCI DSS (PCI Data Security Standard).*

PCI. (2011, 11). *PCI DSS (PCI Data Security Standard) v2.0.* Retrieved from PCI DSS Virtualization Guidelines: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

ROSALES ROSERO, E. E. (07 de 2010). Trabajo de Grado (Magister en Ingenieria). *UNACLOUD: INFRAESTRUCTURA COMO SERVICIO PARA CLOUD COMPUTING OPORTUNISTA*. Bogota: Universidad de los Andes. Facultad de Sistemas.Departamento de Sistemas y Computacion.

Salesforce.com, I. (2011, 12 10). *Corporate History and Milestones - salesforce.com - .* Retrieved from http://www.salesforce.com/company/milestones/

SYMANTEC. (2011). *Encuesta sobre el Estado de la Nube.*

TANIMOTO, S. (2011). Risk Management on the Security Problem in Cloud Computing. *IEEE*.

TOWNSEND, M. (2009). Managing a Security Program in a Cloud Computing Enviroment. *ACM Press*, 128–133.

GLOSARIO

Aceptar el Riesgo: De forma consciente y objetiva aceptar el riesgo residual existente.

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la compañía (materializar el riesgo).

Antivirus: Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominados malware).

Confidencialidad: Es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados (ISO, ISO/IEC 27001, 2005).

Conmutador: Es un dispositivo físico/lógico de interconexión de redes de computadoras cuya función es interconectar dos o más segmentos de red.

Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía.

Disponibilidad: Es la propiedad de la información que se refiere a que ésta sea accesible y utilizable por solicitud de una entidad autorizada, cuando así lo requiera (ISO, ISO/IEC 27001, 2005).

Enrutadores: Dispositivo de Hardware utilizado para interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar.

Evitar el Riesgo: Se entiende a cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad en particular, para asi evitar la presencia del riesgo.

Firewall: Componente de hardware y software diseñado para bloquear el acceso no autorizado y permitiendo el acceso autorizado.

Hardening: Proceso de aseguramiento de sistema mediante reducción de superficies de vulnerabilidad.

IDS: Sistema de detección de intrusos, permite detectar accesos no autorizados a un computador o a una red

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Información: La información es un activo que, como otros activos importantes del negocio u organización, es esencial para las actividades del mismo y, en consecuencia, necesita una protección adecuada. (ISO, ISO/IEC 27002, 2005)

Integridad: Se define como la propiedad de salvaguardar la exactitud y completitud de los activos de información (ISO, ISO/IEC 27001, 2005).

IPS: Sistema de prevención de intrusos. Busca detectar anomalías que indican un riesgo potencial. Puede tomar medidas protectoras.

Monitoreo: Proceso continúo de recolección y análisis de datos cualitativos y cuantitativos, con base en los objetivos planteados en un programa o proyecto, que tiene como propósito descubrir fortalezas y/o debilidades para establecer líneas de acción, permitiendo brindar correcciones y reorientaciones técnicas en la ejecución.

Reducir el Riesgo: Actividades que conllevan al mejoramiento de las medidas existentes o a la implementación de nuevas medidas que ayuden a disminuir riesgos a los niveles definidos como aceptables.

Riesgo: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Seguridad de la Información: La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio. Además se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

Transferir el Riesgo: Transferir el riesgo a terceros, por ejemplo: seguros, proveedores.

VPN: Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

ACRONIMOS

ARPANET: Advanced Research Projects Agency Network

CAPEX: CAPital EXpenditures (Gastos de capital).

CCM: Cloud Security Alliance Controls Matriz (Matriz de Control de CSA).

CSA: Cloud Security Alliance.

ENISA: European Network and Information Security Agency

EUCALYPTUS: Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems (Utilidad de arquitectura informática elástica para confiar sus programas a sistemas funcionales).

GSTI: Gestión de Servicios de T.I.

IAAS: Infrastructure as a Services (Infraestructura como Servicio).

IEEE: Institute of Electrical and Electronics Engineers

ISO: International Organization for Standarization (Organización Internacional para la Estandarización).

OPEX: OPerative EXpenditures (Gastos de Operación).

PAAS: Platform as a Services (Plataforma como Servicio).

PCI: Payment Card Industry data security standard (Estándar de Seguridad de Información para Industria de Tarjetas de Crédito).

RBS: Risk Breakdown Structure (Estructura de División de Riesgo).

SAAS: Software as a Services (Software como Servicio).

SGSI: Sistema de Gestión de Seguridad de la Información.

SLA: Service Level Agreement (Acuerdo de Niveles de Servicio).

SPI: Software, Platform, Infrastructure (Modelos de Servicio de Computación en la Nube).

VPN: Virtual Private NetWork (Red Privada Virtual).

ANEXO 1

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre:

Cargo:

Empresa:

Rol en el servicio de computación en nube (Cliente / Proveedor / Auditor):

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

PLANTEAMIENTO DEL PROBLEMA

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5

METODOLOGÍA

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5

MODELO

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5

RIESGOS

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5

CONTROLES

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

1	2	3	4	5

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5

Comentarios:

Firma: _____

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre: César Iván Rodríguez Sánchez

Cargo: Consultor en Seguridad de la Información

Empresa: NewNet S.A.

Rol en el servicio de computación en nube (Cliente / Proveedor / Auditor): Auditor

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

Planteamiento del problema

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5
				X

Metodología

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5
				X

Modelo

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5
				X

Riesgos

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

Controles

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

1	2	3	4	5
				X

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5
			X	

Comentarios:

El modelo de capas para la identificación de riesgos y responsabilidades en los diferentes modelos de servicio, me parece útil para explorar e identificar de manera detallada los componentes de un servicio en la nube. Los riesgos y controles propuestos me parecen valiosos para evaluar un servicio de computación en la nube. Me hubiera gustado encontrar en el proyecto estudios de como terceros pueden proveer confianza en el modelo de computación en la nube, tales como entes acreditados que emitan certificaciones, y aseguradoras que respondan ante incidentes de seguridad.

Firma:

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre: FABIAN CARDENAS VARELA

Cargo: GERENTE ÁREA DE I+D

Empresa: NOVASEC S.A.S

Rol en el servicio de computación en nube: PROVEDOR

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

Planteamiento del problema

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5
				X

Metodología

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5
			X	

Modelo

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5
			X	

Riesgos

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
			X	

Controles

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

1	2	3	4	5
			X	

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5
			X	

Comentarios:

Hay que hacer énfasis y dejar claro que cada empresa es responsable de realizar una identificación, evaluación y definición del tratamiento de los riesgos con un nivel mayor de detalle a nivel cualitativo y cuantitativo, utilizando como referencia el modelo de seguridad planteado. Esto debido a que la naturaleza de cada organización y el impacto de estos riesgos planteados es particular. Por esta razón los controles planteados son una referencia válida para la academia y la industria pero no son tan amplios y suficientes que apliquen a cada empresa particular. Cada empresa es responsable de analizarlos formalmente, adecuarlos, implementarlos y mantenerlos de acuerdo con sus necesidades.

Firma: Fabian Alberto Cárdenas Varela.
C.C. # 85'475.910 de Santa Marta

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre: John Carlos Jaramillo Carmona

Cargo: Jefe de Proyectos.

Empresa: Colombina S.A.

Rol en el servicio de computación en nube (Cliente / Proveedor / Auditor): Cliente

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

Planteamiento del problema

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5
				X

Metodología

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5
			X	

Modelo

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5
				X

Riesgos

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
			X	

Controles

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

1	2	3	4	5
				X

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5
			X	

Comentarios:

Se categorizaron muy bien los riesgos, identificándolos como activos de información, definiendo el custodio y el responsable de los mismos, siendo un factor critico de éxito para la correcta implementación de un sistema de gestión de seguridad tanto a nivel de infraestructura, plataforma y software o aplicaciones. El modelo describe una excelente metodología para definir y desarrollar un proyecto de seguridad informática, ya que involucra todas las capas asociadas a la computación en la nube.

Firma:

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre: John Harold Ñañez

Cargo: Gerente de Infraestructura y operaciones

Empresa: Inversiones Grupo Mundial

Rol en el servicio de computación en nube (Cliente / Proveedor / Auditor): Cliente

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

Planteamiento del problema

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5
				X

Metodología

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5
				X

Modelo

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5
				X

Riesgos

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

Controles

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

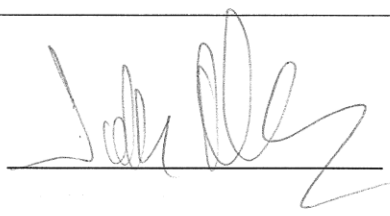
1	2	3	4	5
				X

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5
			X	

Comentarios:

Me queda la inquietud de la capacidad de la empresas para implementar todos los controles expuestos.

Firma: 

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre: Juan Carlos De La Cruz

Cargo: Gerente Comercial - Occidente

Empresa: Infomedia

Rol en el servicio de computación en nube (Cliente / Proveedor / Auditor): Proveedor

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

Planteamiento del problema

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5
				X

Metodología

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5
				X

Modelo

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5
				X

Riesgos

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				X

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
			X	

Controles

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

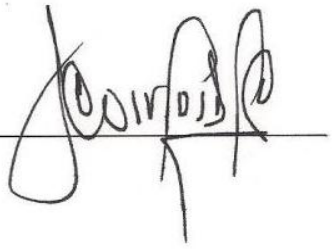
1	2	3	4	5
			X	

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5
			X	

Comentarios:

Los riesgos planteados dependen del tipo de negociación que se tiene con los clientes, lo que hace que las responsabilidades varíen.

Firma: 

HOJA DE EVALUACIÓN DEL PROYECTO DE GRADO

Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias

Nombre: Olga lucía Forero Holguin.

Cargo: Team Leader Regional Occidente.

Empresa: Sisa S.A.

Rol en el servicio de computación en nube (Cliente / Proveedor / Auditor): Proveedor

De acuerdo al documento definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias califique de 1 a 5 las siguientes preguntas siendo 1 la menor y 5 la mayor calificación.

Planteamiento del problema

¿El planteamiento del problema es pertinente para la situación de las compañías que tengan servicios alojados en nubes privadas o comunitarias?

1	2	3	4	5
				x

Metodología

¿Considera que la metodología aplicada para el levantamiento de riesgos es apropiada?

1	2	3	4	5
			x	

Modelo

¿Considera que la división por dominios del modelo de la computación en la nube permite la distribución efectiva de riesgos y controles?

1	2	3	4	5
			x	

Riesgos

¿Considera que los riesgos planteados afectan o impactan a empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				x

¿Considera que los riesgos planteados son amplios y suficientes de acuerdo a la problemática actual de las empresas que alojan sus servicios en nubes privadas o comunitarias?

1	2	3	4	5
				x

Controles

¿Considera que los controles del modelo de seguridad tratan correctamente los riesgos planteados?

1	2	3	4	5
			x	

¿Considera que los controles planteados son amplios y suficientes?

1	2	3	4	5
			x	

Comentarios:

Los modelos de Cloud no son tan estáticos como los describen, depende de cada negociación y de cada cliente, también la forma en que los proveedores asignamos los recursos dependen de factores como la viabilidad técnica, económica y las ventanas de mantenimiento para hacerlo.

Firma: