UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"Cómputo en la nube: Seguridad en el gestionamiento de la información"

TESIS

Para obtener el título de:

Ingeniera en computación

PRESENTA:

Natali Jasso Guadiana

DIRECTORA DE TESIS:

M.C. Cintia Quezada Reyes

Agradecimientos

A mis padres:

Por su esfuerzo realizado para brindarme la oportunidad de estudiar una carrera universitaria.
Gracias por estar en los bellos y en los malos momentos junto a mí, por todos sus cuidados, consejos y la educación recibida.

A mis hermanos:

Por su apoyo incondicional en estos años de mi vida.

A mi novio:

Por formar parte de mi vida, por su comprensión, apoyo y ánimo para la realización de mis metas.

A mi asesora:

Por transmitirme su conocimiento, por su tiempo y apoyo en la realización de este trabajo. Gracias profesora Cintia Quezada Reyes.

A la UNAM:

Por las experiencias adquiridas y por la fortuna de pertenecer a la mejor Universidad.

Índice

Lista de Tablas 1

Lista de Figuras 2

Introducción 4

Objetivo 8

1. Fundamentos de Seguridad 7

1.1 Definición y objetivos de Seguridad Informática 14

1.2 Definición de amenaza y vulnerabilidad 16

1.2.1 Tipos de amenazas 17

1.2.2 Tipos de Vulnerabilidades 20

1.3 Arquitectura de Seguridad OSI. 22

1.3.1 Servicios de seguridad 22

1.3.2 Mecanismos de seguridad 25

1.3.3 Ataques de seguridad 28

1.4 Metodología para brindar protección 31

2. Cómputo en la nube 31

2.1 Definición de cómputo en la nube 38

2.1.1 Tipos de servicios 43

2.1.2 Tipos de infraestructura 46

2.2 Ventajas y desventajas del cómputo en la nube 48

2.3 Diferencias entre el cómputo tradicional y el cómputo en la nube 51

2.4 Estadísticas y ejemplos del cómputo en la nube en la actualidad. 52
3. Implicaciones de seguridad en la nube 72
3.1 Situación actual 74
3.1.1 Retos de seguridad 84
3.2 Privacidad de la información en el cómputo en la nube 90
3.3 Vulnerabilidades y amenazas 94
3.4 Riesgos 98
3.5 Riesgos técnicos 99
3.6 Riesgos legales 101
4. Empleando Cómputo en la nube 104
4.1 Factores a considerar antes de migrar la información a la nube…… 106
4.2 Recomendaciones de seguridad 109
4.2.1 Gestión de la seguridad 112
4.2.2 Buen manejo y control de los servicios basados en la nube 118
4.2.3 Control de acceso 119
4.2.4 Disponibilidad-Recuperación 120
4.2.5 Integridad 120
4.2.6 Confidencialidad/Privacidad 121
4.2.7 Requisitos y exigencias legales 124
4.2.8 Auditorías 124

4.3 Cumplimiento regulatorio y auditoría..... 126
Conclusiones 132
Referencias..... 138
Anexo A: Cuestionario – Cómputo en la nube 152
Glosario de términos..... 160

Lista de Tablas

No. Tabla	Título de la Tabla	Pág.
Tabla 1.1	Servicios de Seguridad	23
Tabla 2.1	Tipos de servicios en el cómputo en la nube	43
Tabla 2.2	Ventajas del cómputo en la nube	48
Tabla 2.3	Desventajas del cómputo en la nube	50
Tabla 2.4	Diferencias entre las características del modelo tradicional y del modelo de cómputo en la nube	51
Tabla 3.1	Retos de seguridad	86
Tabla 3.2	Amenazas en el cómputo en la nube	95
Tabla 3.3	Características de los modelos de despliegue del cómputo en la nube	102

Lista de Figuras

No. Figura	Título de la Figura	Pág.
Figura 1.1	Principios básicos de la seguridad de la información.	15
Figura 1.2	Ejemplos de mecanismos de seguridad según su función.	26
Figura 2.1	Representación visual de la definición de NIST del cómputo en la nube.	40
Figura 2.2	Conocimiento del término cómputo en la nube.	53
Figura 2.3	Recomendación del uso de cómputo en la nube en la empresa.	55
Figura 2.4	Adopción de soluciones de cómputo en la nube.	56
Figura 2.5	Tipo de infraestructura recomendada.	57
Figura 2.6	Razones de la empresa para migrar a los servicios de la nube.	58
Figura 2.7	Obstáculos en la adopción de cómputo en la nube.	59
Figura 2.8	Competividad empresarial al usar cómputo en la nube.	61
Figura 2.9	Conocimiento de estándares en la nube.	62
Figura 2.10	Evolución de cómputo en la nube en México	63
Figura 3.1	Riesgos al migrar servicios a la nube	77
Figura 3.2	Seguridad en el almacenamiento en la nube.	79
Figura 3.3	Responsabilidad de la seguridad en la nube.	80
Figura 3.4	Importancia de la seguridad para cumplir objetivos de TI.	82

Figura 3.5	Competitividad empresarial	83
Figura 3.6	Porcentaje de los recursos destinados a la seguridad en el cómputo en la nube.	84
Figura 3.7	Ciclo de vida que siguen los datos procesados en la nube.	92
Figura 4.1	Temas a tomar en cuenta en las recomendaciones de seguridad	110
Figura 4.2	Responsables en el servicio IaaS	113
Figura 4.3	Responsables en el servicio PaaS	115
Figura 4.4	Responsables en el servicio SaaS	116

Introducción

Cada vez son más las personas que tienen acceso a Internet y lo usan; la revolución inalámbrica le ha dado un enfoque móvil y cada vez es más común que personas puedan y quieran acceder desde cualquier lugar donde se encuentren.

Aún cuando se puede acceder a Internet casi desde cualquier lugar, se necesita llevar consigo un dispositivo de hardware para acceder. En este dispositivo se debe encontrar la información y paquetería necesaria para visualizarla. ¿Y qué pasa si no se lleva consigo este hardware? Aún teniendo la posibilidad de acceder a Internet desde otro dispositivo, si éste no cuenta con las características necesarias y aunado a esto, no se tiene acceso a la información, no se puede trabajar.

A partir de lo anterior, se puede decir que si se logra almacenar en Internet la información, las aplicaciones y los servicios necesarios, desde cualquier equipo con acceso a Internet se podrían ejecutar las aplicaciones y acceder a la información. De esta idea surge el concepto de “Cloud Computing” o “Cómputo en la nube”, tomando evidentemente a la nube como una metáfora de Internet.

Hoy es una realidad la utilización del cómputo en la nube. Un ejemplo claro de ello es Microsoft Office, una de las paqueterías más populares ya está “en las nubes”, esto quiere decir que con cualquier dispositivo con un navegador web y acceso a internet, no importando si se cuenta con Office instalado, se pueden visualizar los documentos, editarlos y guardar una copia.

Sin embargo, una cosa es tener clara la idea y otra llevarla a la práctica de forma exitosa. Por ello y a pesar de muchos casos actuales de cómputo en la nube, no se ha cruzado el nivel de madurez necesario para que sea del todo aceptado y usado por las empresas. Cada día el cómputo en la nube evoluciona a mayor velocidad y es evidente que se adoptará.

Pareciera que el cómputo en la nube es algo fabuloso, y en realidad lo es, pero como todo tiene sus ventajas y desventajas.

Un punto preocupante para las empresas al evaluar y tomar la decisión de querer o no adoptar este modelo, es la seguridad de su información, siendo éste el activo de mayor importancia a resguardar. Por lo cual la seguridad en la nube es el foco central del trabajo de investigación que se presenta a lo largo de los capítulos de este escrito.

El motivo del presente escrito es definir qué es el cómputo en la nube, identificar los servicios ofrecidos en la nube y explorar las consideraciones relacionadas con el aseguramiento de la información, para desarrollar un estudio de las implicaciones en seguridad que se tienen actualmente en la transición del modelo tradicional al modelo en la nube en lo referente al gestionamiento de la información.

Por otra parte, debido a la necesidad y al interés de las empresas en el cumplimiento de leyes, regulaciones o normas, se presentan los factores a tomar en cuenta en el cómputo en la nube para el cumplimiento regulatorio. Así mismo se hará

mención de los tipos de auditoría que las empresas pueden solicitar para auditar la actividad del proveedor o para la validación del cumplimiento, pues vale la pena saber cómo se debe dar tratamiento a dichos temas.

Finalmente se pretende que este trabajo ayude a: 1) concientizar al usuario sobre la importancia de la seguridad de la información, y 2) orientar en la forma de gestionar los datos en la nube y al mismo tiempo que sea vista como una alternativa de resguardo y manejo de la información.

Es por esto que en este trabajo se espera concientizar a las empresas sobre los riesgos de seguridad que conlleva el uso del cómputo en la nube, desarrollando recomendaciones de seguridad que servirán de ayuda o referencia a las empresas para analizar cuándo es prudente usar el cómputo en la nube y cuándo es mejor prescindir de este modelo.

Objetivo

Se observa una tendencia marcada en el creciente uso del cómputo en la nube, por lo cual el presente trabajo tiene por objetivo dar a conocer los términos necesarios para entender el cómputo en la nube, enfocándose en presentar las consideraciones generales de seguridad a tomar en cuenta al hacer uso de algún servicio de cómputo en la nube.

De manera puntual los objetivos que se persiguen son:

- Dar a conocer las definiciones referentes a cómputo en la nube.

- Realizar un análisis de las implicaciones de seguridad que conlleva el uso de internet como medio de transmisión de la información.

- Realizar recomendaciones de seguridad para el mejor aprovechamiento de cómputo en la nube.

- Dar a conocer los principios del cumplimiento regulatorio en el cómputo en la nube.

Para alcanzar los objetivos señalados, en el capítulo I se dan a conocer los conceptos y principios básicos de la seguridad de la información. También se mencionan los objetivos que persigue, con la finalidad de entender la importancia de la seguridad de la información, en este caso, cuando la empresa (cliente) solicite al proveedor algún servicio de cómputo en la nube.

En el capítulo II se define el cómputo en la nube, los modelos de servicios y de despliegue de esta nueva forma de entrega de servicios, las ventajas y desventajas de su uso. Por último se muestran los resultados de una encuesta realizada al personal de pequeñas y medianas empresas, cuya finalidad es conocer la situación actual y la perspectiva que se tiene sobre el tema.

En el capítulo III se presentan estadísticas sobre los puntos de seguridad que preocupan a las empresas, las vulnerabilidades, las amenazas, los riesgos y los retos de seguridad al hacer uso de cómputo en la nube, los cuales se identificaron a lo largo de la investigación.

En el capítulo IV se describen una serie de recomendaciones de seguridad a tomar en cuenta para el mejor aprovechamiento del cómputo en la nube, dirigidas a aquellas empresas que decidan hacer uso de los servicios basados en este modelo.

Finalmente, después del trabajo realizado se dan a conocer las conclusiones.

Capítulo I

Fundamentos de Seguridad

Debido al uso de las nuevas tecnologías de la información y al creciente uso de Internet, la seguridad informática ha adquirido un gran auge y se debe dar trascendencia al tema.

En las empresas se permite el acceso a los sistemas de información al personal de la empresa, así como a los proveedores de servicios; por lo tanto, es elemental saber qué recursos de la misma necesitan protección, cuáles necesitan un control de acceso y cuáles deben ser los permisos de los usuarios del sistema de información, entre otros. Esto hace que sea importante conocer las bases de la seguridad informática para identificar los elementos a tomar en cuenta en el aseguramiento de la información y de los recursos.

1.1 Definición y objetivos de Seguridad Informática

En muchas ocasiones se piensa que seguridad informática y seguridad de la información tienen un mismo significado, no es así, pero persiguen un mismo objetivo: proteger la confidencialidad, integridad y disponibilidad de la información.

Cuando se habla de seguridad informática se hace referencia a todas aquellas medidas y controles que se deben establecer para el aseguramiento de los sistemas informáticos, impidiendo la actuación de procedimientos no autorizados sobre éstos.

La seguridad informática abarca aspectos generales incluyendo dentro de éstos a la seguridad de la información, que se define de acuerdo al estándar actual ISO 27002, como: "la preservación de su confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran), así como de los sistemas implicados en su tratamiento, dentro de una organización" [1]. Para que un sistema se pueda definir como seguro debe cumplir con los tres principios básicos de la seguridad de la información que se muestran en la figura 1.1

Figura 1.1 Principios básicos de la seguridad de la información

Objetivos de la seguridad Informática

Entre los principales objetivos de la seguridad informática se encuentran:

- ✓ Asegurar la confidencialidad, integridad y disponibilidad en los sistemas informáticos.
- ✓ Proteger los activos informáticos valiosos de la empresa: información, hardware y software.
- ✓ Detectar las vulnerabilidades y amenazas a la seguridad con el fin de minimizar y gestionar los riesgos.
- ✓ Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- ✓ Lograr la adecuada recuperación del sistema en caso de un incidente de seguridad.
- ✓ Cumplir con el marco normativo y legal.

1.2 Definición de amenaza y vulnerabilidad

Una amenaza se puede definir como el peligro latente de que ocurra un suceso que provoque daños, o la pérdida de los activos (información).

Las amenazas se consideran como exteriores a cualquier sistema, y aunque es imposible eliminarlas, sí es posible establecer medidas de protección que reduzcan la posibilidad de consumación de éstas.

Una vulnerabilidad es una debilidad interna de un sistema que origina la exposición de éste a las amenazas existentes, las cuales pueden ser explotadas (aprovechadas) por un atacante para violar la seguridad. Las vulnerabilidades son consecuencia de la falta de mantenimiento, de errores de planeación, de personal sin conocimientos adecuados de los sistemas informáticos e incluso de limitaciones en la tecnología.

Por lo tanto, se entiende que las amenazas explotan las vulnerabilidades, ocasionando ataques. Luego entonces, un ataque es la culminación de una amenaza.

1.2.1 Tipos de amenazas

Las amenazas provienen de 5 fuentes principalmente:

1. **Desastres naturales:** Afectaciones a la sociedad a raíz de un fenómeno natural. Algunos ejemplos son:

a. *Incendios:* Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el incorrecto almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de

las computadoras ya que puede destruir fácilmente los archivos de información y programas. Desgraciadamente algunos sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos.

b. *Inundaciones***:** Se define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Ésta es una de las causas de mayores desastres en centros de cómputo. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

c. Fenómenos Naturales: Normalmente se reciben por anticipado los avisos de tormentas, tempestades, huracanes y catástrofes similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

d. *Terremotos*: Estos fenómenos pueden ser tan débiles que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas y recursos materiales como dispositivos de almacenamiento de información.

2. Errores de Hardware: Se refieren a posibles fallas físicas totales o parciales en cualquiera de los dispositivos, incluyendo los dispositivos que los componen. Los errores en el hardware

pueden deberse a fallas en el diseño, errores de fabricación, al desgaste normal o al descuido o mal uso de las personas que lo utilizan. Los errores de hardware no siempre producen fallas detectables inmediatamente en el sistema. Un pequeño error de hardware es posible que no se detecte hasta que cause errores más graves.

3. Problemas de Software: Posibles fallas debido a incorrectas implementaciones en sistemas operativos, software mal desarrollado, mal diseñado o mal implementado, además de los códigos maliciosos (malware).

4. Errores de red: Pueden presentarse problemas debido al mal diseño, uso o implementación de la red. Las dos principales amenazas a la red son la no disponibilidad y la extracción de información a través de ella. Ejemplos de éstos son: La mala implementación de los estándares existentes como los de cableado estructurado; la incorrecta elección de la topología de red a utilizarse, la falta de planeación a futuro en cuestiones como escalabilidad y crecimiento de la red, entre otros.

5. Humana. Este tipo de amenazas puede deberse principalmente a tres causas:

a. *Ignorancia.* Los avances tecnológicos no se detienen y estar actualizado no siempre es una tarea sencilla, por lo que la ignorancia informática es algo tan común como peligroso. Una medida muy importante para resolver este problema es el principio del mínimo privilegio, el cual establece que cualquier

entidad (programa, administrador, etcétera) debe tener únicamente los niveles de acceso mínimos que le sean necesarios. Pero sin duda la solución está principalmente en la educación informática, necesaria y hasta el momento escasa.

b. *Diversión:* Muchos de los problemas informáticos se deben a personas que se entretienen buscando herramientas y documentación de aplicaciones hechas por otros. La mayoría de estas personas no tiene idea de las consecuencias que puede alcanzar su "curiosidad" y lamentablemente hoy en día cualquiera tiene acceso a esta información; la solución aquí sigue siendo la educación tanto informática como cívica.

c. *Descuido:* Es algo que no se puede erradicar con ninguna aplicación o mecanismo de seguridad por más complejo que éste sea.

1.2.2 Tipos de Vulnerabilidades

1. Física: Este tipo de vulnerabilidades está relacionado con el acceso físico a los sistemas en donde la información se está almacenando y manejando. Se pueden presentar por la falta de identificación de personas y equipos, pudiendo éstos últimos ser utilizados para el robo de la información.

2. Humana: Es una de las vulnerabilidades que se presenta a menudo ya que es la más difícil de controlar, llegando a describir a las personas como el eslabón más débil en la cadena de la seguridad. Los puntos débiles, como la falta de conciencia y la

falta de capacitación, que se presentan en las personas, puede que sean intencionales o no.

3. Software: Son todos aquellos errores de programación o de diseño presentes en los sistemas operativos, paquetería o programas desarrollados por usuarios, permitiendo accesos indebidos a los sistemas y de la misma manera a la información.

4. Hardware: La vulnerabilidad se presenta cuando el hardware falla, ya sea por mal uso, descuido, deficiencias en el diseño en su fabricación o porque la configuración de los equipos pueden alterarlos, llegando al punto de que dejen fuera de operación a los sistemas.

5. Naturales: Este tipo de vulnerabilidad está relacionada con las condiciones de la naturaleza, tales como humedad, polvo, temperaturas indebidas, desastres naturales, etcétera. Las vulnerabilidades aquí se refieren al grado en que el sistema se puede ver afectado debido a la falta o deficiencia de las medidas que prevengan estas situaciones; por ejemplo, por la falta de un respaldo de la información en algún otro sitio, plantas de energía eléctrica alterna, un sistema de ventilación en el área, etcétera.

6. Red: Abarca la transmisión de información en una red de equipos que se encuentran conectados entre sí ya sea por el medio cableado, satelital, fibra óptica u ondas de radio, por lo que se es vulnerable a ataques a la red en los que se puedan penetrar a uno de los equipos y de ahí expandirse a los demás o ataques en los que la información sea interceptada.

1.3 Arquitectura de Seguridad OSI.

Es indispensable hacer uso de recomendaciones para lograr que la comunicación entre las empresas, así como que el intercambio de información, se realice de forma segura.

La arquitectura de seguridad OSI está fundamentada en el RFC 2828 y en la recomendación X.800, enfocándose en las siguientes tres categorías:

- Servicios de seguridad
- Mecanismos de seguridad
- Ataques de seguridad

1.3.1 Servicios de seguridad

Los servicios de seguridad se necesitan para poder brindar seguridad, son servicios que mejoran la seguridad en un sistema informático y el flujo de información de una organización. Los servicios de seguridad son la esencia de la seguridad; son los objetivos que desea alcanzar la seguridad informática, son las características que se desean mantener en el manejo, creación, resguardo y flujo de la información. Los servicios de seguridad se muestran en la Tabla 1.1.

Tabla 1.1. Servicios de Seguridad

Servicio	Definición
Autenticación	En el área de las redes éste es uno de los servicios más importantes debido a la falta de presencia física; es decir, en las redes, tanto los dispositivos como los usuarios tienen una presencia virtual, siendo reconocidos, en la mayoría de los casos, por los mensajes que envían. Así el riesgo de suplantación es elevado. Con este servicio se garantiza que la identidad del que crea el mensaje no es falsa. Por otro lado está la autenticidad de los equipos al conectarse a una red.
Integridad de los datos	Se refiere a que la información pueda ser modificada sólo por las entidades autorizadas desde su creación o durante su transmisión por la red y que sobre esta modificación se tengan controles, por ejemplo, registros previos y posteriores a ella. De esta forma la integridad garantiza que los datos enviados coinciden exactamente con los datos recibidos.
Confidencialidad de los datos	Con este servicio se garantiza que los mensajes transmitidos, o que están

	dentro de un sistema informático, solo podrán ser accedidos por entidades previamente autorizadas (destinatario).
No repudio	Mediante este servicio se demuestra la autoría y envío de un mensaje; previene que un emisor niegue haber emitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). Esto se verifica ante un tercero para evitar la negación.
Disponibilidad	El término disponibilidad hace referencia a la probabilidad de que un servicio funcione adecuadamente en cualquier momento. La disponibilidad se expresa con mayor frecuencia a través del *índice de disponibilidad,* un porcentaje que se mide dividiendo el tiempo durante el cual el servicio está disponible entre el tiempo total. Como servicio de seguridad, la disponibilidad es la característica de la información y de los recursos informáticos de encontrarse a disposición de las entidades autorizadas que requieran acceder a ellos, ya sean personas,

	procesos o aplicaciones, en el momento que se requiera.

1.3.2 Mecanismos de seguridad

Son aquellos controles y herramientas que se utilizan para fortalecer los principios básicos de la seguridad (servicios de seguridad). Los mecanismos se requieren para ofrecer (implementar) los servicios de seguridad.

La clasificación, según su función, es la siguiente (Figura 1.2):

- ***Preventivos.*** Este tipo de mecanismos detiene agentes no deseados, actuando antes de que ocurra un hecho, protege vulnerabilidades.

- ***Disuasivos.*** Toman acción en momentos anteriores al ataque, con el objetivo de reducirlo o evitarlo.

- ***Detectores.*** Identifican agentes no deseados en el sistema enviando alertas o avisos de lo ocurrido. A diferencia de los preventivos éstos actúan después de que un hecho ocurra.

- ***Correctivos.*** Actúan cuando ya ha ocurrido el hecho para eliminar el daño.

Figura 1.2 Ejemplos de mecanismos de seguridad según su función.

La clasificación de los mecanismos con base en su necesidad son:

a) Requeridos

Son mecanismos basados en políticas, las cuales determinan si una operación sobre un objeto (dispositivos lógicos, servicios y ficheros) realizada por un sujeto (usuarios, grupos, roles, procesos y equipos) está o no permitida, basándose en los atributos de ambos. Los permisos de acceso son definidos por el sistema operativo.

Todos los controles en esta categoría pueden ser definidos con base en una o más reglas escritas. La clasificación de los datos almacenados y procesados en un sistema o red y su modo de operación determinan qué reglas aplicar, y éstas indican cuáles son los controles requeridos.

b) Discrecionales

Son mecanismos basados en los propietarios y grupos a los que pertenece un objeto (dispositivos lógicos, servicios y ficheros). Un sujeto (usuarios, grupos, roles, procesos y equipos) puede transmitir sus permisos a otro sujeto; los permisos de acceso los controla y configura el propietario de cada objeto.

Este tipo de controles es elegido por los administradores. En muchos casos los controles requeridos no reducen el nivel de vulnerabilidad a un nivel aceptable, por lo que se deben elegir e

implementar este tipo de controles para ajustar el nivel de vulnerabilidad a un nivel aceptable.

Los mecanismos de seguridad ayudan a fortalecer los servicios de seguridad. Los tipos de mecanismos según el servicio que implementan son:

a) Mecanismos de autenticación
b) Mecanismos de integridad de datos
c) Mecanismos de control de acceso
d) Mecanismos de confidencialidad
e) Mecanismo de no repudio
f) Mecanismo de disponibilidad

Es importante mencionar que no hay un mecanismo que provea todos los servicios de seguridad.

1.3.3 Ataques de seguridad

Un ataque informático consiste en aprovechar una o más debilidades o fallas en el hardware, software y sobre todo en las personas que forman parte de la empresa, eludiendo servicios y políticas de seguridad y comprometiendo la seguridad de la información de la empresa. El objetivo del ataque es obtener beneficio económico, espionaje, diversión, entre otros, causando daños o problemas a un sistema informático o red.

Los ataques suelen afectar principalmente a internet, redes de área local de empresas, redes Wi-Fi, redes de telefonía, etcétera.

Existen dos tipos de ataques. Los ataques pasivos y los ataques activos.

a) Ataques pasivos

El objetivo de este tipo de ataques es la intercepción de datos y el análisis de tráfico; en una comunicación ésta no se altera sino que únicamente es escuchada o monitoreada por el atacante. Los ataques pasivos no provocan alteración en los bienes y por ello son difíciles de detectar. Para tratar estos ataques es preferible hacer énfasis en la prevención más que en la detección.

b) Ataques activos

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. A diferencia de los ataques pasivos, los ataques activos son difíciles de prevenir, ya que son detectados hasta que fueron llevados a cabo. Por consiguiente, la meta es detectarlos y rápidamente recuperarse de cualquier daño causado por ellos.

Los ataques también pueden clasificarse dentro de cuatro categorías:

a) Interrupción (Tipo de ataque: activo)

Se habla de un ataque de interrupción cuando un recurso del sistema es destruido, no llega a estar disponible o se inutiliza. Éste es un ataque contra la disponibilidad. Algunos ejemplos de este ataque son la destrucción de un elemento de hardware,

como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

b) Modificación (Tipo de ataque: activo)

En este tipo de ataques una entidad no autorizada no solamente gana acceso al recurso sino que además altera el contenido. Éste es un ataque contra la integridad. Algunos ejemplos son los cambios de valores en un archivo de datos, alterar un programa para que funcione de forma diferente o modificar el contenido de los mensajes que se transmiten en una comunicación.

c) Intercepción (Tipo de ataque: pasivo)

Se refiere al tipo de ataques que trata de interceptar cierta información que es enviada a través de la red, es decir, una entidad no autorizada consigue acceso a un recurso o a la misma información. Éste es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son intervenir una línea para recabar datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos) o bien la lectura de las cabeceras de paquetes para conocer la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

d) Suplantación o falsificación (Tipo de ataque: activo)

En este caso una entidad no autorizada envía mensajes haciéndose pasar por un usuario legítimo. Éste es un ataque contra la autenticidad. Algunos ejemplos de este ataque son la inserción de mensajes falsificados en una red o añadir registros a un archivo.

1.4 Metodología para brindar protección

Para tratar de minimizar los efectos de un problema de seguridad se responde a las tres preguntas siguientes, las cuales ayudan a determinar el nivel de seguridad que se tiene o se desea en la empresa:

1) Identificar los activos. ¿Qué es lo que se quiere proteger? Para la mayoría de las empresas el principal activo es la Información.

   Para responder a esta primera pregunta se deben identificar todos los activos cuya integridad pueda ser amenazada de cualquier forma. Por ejemplo:

- ✓ *Hardware (Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, ordenadores personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers, entre otros.)*

- ✓ *Software (Códigos fuente y objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación).*

- ✓ *Información (En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos).*

- ✓ *Personas (Usuarios, operadores).*

- ✓ *Accesorios (Papel, cintas, tóner, etcétera.).*

Ya identificados los activos se obtiene una lista que incluirá todo lo que se necesita para proteger la empresa.

2) Identificar las amenazas y vulnerabilidades. ¿De qué se desea proteger? En este caso la respuesta se enfoca en los intrusos y los riesgos que pueden generar.

   Una vez identificados los activos se procede a la identificación de las vulnerabilidades y amenazas que se presentan en contra de los mismos, así como la identificación de los atacantes que intenten violar la seguridad.

   No siempre se debe tratar a los ataques como actos intencionados contra el sistema pues también pueden ser ocasionados por accidentes internos no intencionados en la empresa; por ejemplo un operador que derrama una taza de café sobre una terminal, un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, entre otros.

3) Definir la arquitectura de seguridad a utilizarse ¿Cómo se pueden proteger los activos?

Para dar respuesta a esta pregunta se deben cuantificar los daños que causan las posibles vulnerabilidades. Para hacerlo se puede partir de hechos sucedidos en la empresa.

La clasificación de los riesgos es una parte que hay que tratar para definir una arquitectura de seguridad, ésta se hace basada en un estudio, tomando en cuenta el nivel de importancia del daño causado y a la probabilidad de que ese daño se convierta en realidad; es decir, no se debe gastar más dinero en la implementación para proteger al activo del valor del activo.

Los activos en cuya evaluación presenten un riesgo (probabilidad de que una amenaza se lleve a cabo, ocasionando pérdidas de información o daños en los activos) mayor serán a los que se les deba implementar medidas de protección, es muy probable que sean atacados, causando pérdidas importantes.

Existe un tipo de riesgos llamados inaceptables, los cuales se deben tratar con mucho cuidado para que los sistemas informáticos funcionen correctamente; su prevención es crucial.

Finalmente, cuando ya se ha realizado el análisis se debe presentar un reporte a los responsables de la empresa teniendo en cuenta que el gasto de proteger un recurso ante una amenaza debe ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad.

Los riesgos se pueden minimizar, mas no eliminarlos completamente. Es recomendable planear tanto la prevención ante un problema, como la recuperación si el mismo se produce.

Capítulo II

Cómputo en la nube

Cuando proveedores dedicados a la entrega de servicios, como Google, Amazon AWS y otros construyeron su propia infraestructura, emergió una arquitectura a la que se le conoce como un sistema de recursos distribuidos horizontalmente; es decir, un conjunto de computadoras que se encuentran separadas físicamente pero que están conectadas entre sí a través de una red. El término de cómputo en la nube se inició con esta arquitectura, introduciendo servicios virtuales de TI. Este modelo de arquitectura está en crecimiento y cada vez son más los servicios a los cuales se puede acceder a través de la nube, aún cuando no se esté consciente de ello, en la actualidad es frecuente su uso.

2.1 Definición de cómputo en la nube

El cómputo en la nube (cloud computing) es un modelo de entrega de servicios, los cuales son suministrados a través de Internet, basándose en centros de datos remotos para gestionar los servicios de información y aplicaciones.

El término “nube” se utiliza para hacer referencia a la flexibilidad del servicio, pues éste puede tomar diferentes formas como las nubes, siendo una metáfora de Internet, ésta tiene origen en la nube utilizada para representar Internet en los diagramas de red, como una abstracción de la infraestructura que representa.

Permite que los consumidores y las empresas gestionen archivos y utilicen aplicaciones sin necesidad de instalarlas en cualquier computadora con acceso a Internet. Esta tecnología ofrece un

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

Existen varias definiciones para este término y vale la pena mencionar las siguientes:

a) Definición de la IEEE (Institute of Electrical and Electronics Engineers)

Es un nuevo paradigma de computación cuyo objetivo es proporcionar información fiable, personalizada, así como de calidad de servicio, garantizada en entornos informáticos dinámicos para los usuarios finales.

b) Definición de NIST (National Institute of Standards and Tecnology -USA-)

El cómputo en la nube es un modelo que permite un cómodo y conveniente acceso, red bajo demanda, a un grupo compartido de recursos informáticos configurables, (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente proveídos y liberados con un mínimo de esfuerzo en gestión para proveer servicios de interacción.

La figura 2.1 es una representación de la definición de cómputo en la nube dada a conocer por el NIST, en la que se incluyen las tres áreas clave para describir y entender el modelo:

Figura 2.1 Representación visual de la definición de NIST del cómputo en la nube.

1. *Características esenciales*. Los servicios en la nube se basan en cinco características fundamentales:

    a) Amplio acceso a la red. Los recursos, tales como almacenamiento, procesamiento, memoria y máquinas virtuales, entre otros, están disponibles a través de la red. Se accede a ellos por medio de

dispositivos como teléfonos, laptops, PDAs, tabletas etcétera.

b) Elasticidad y rapidez. Los recursos pueden crecer de manera rápida en cualquier momento que se necesite e incluso hacerse de manera automática, el usuario puede llegar a tener la percepción de que este crecimiento es ilimitado.

c) Servicio supervisado. Los sistemas en la nube controlan y optimizan los recursos asignados de manera automática, dependiendo del servicio que se proporcione, esto puede reportarse tanto al usuario como al proveedor, lo cual permite transparencia a ambas partes.

d) Autoservicio a la carta. El usuario puede proveerse de los recursos que necesite de forma automática y unilateral; es decir, no se necesita la interacción humana con cada proveedor de servicios.

e) Reservas de recursos en común. Los usuarios que opten por un modelo de multiposesión harán uso de recursos puestos en reservas en común de acuerdo en la demanda.

2. *Modelos de servicios.* Son tres los modelos y sus combinaciones derivadas que describen la prestación de

servicios en la nube. Hay tres maneras de ofrecer servicios a través en la nube, los cuales se explicarán más adelante:

a. Software como servicio (Sotware as a service – SaaS)

b. Plataforma como servicio (Plataform as a service – Paas)

c. Infraestructura como servicio (Infraestructure as a service – IaaS)

3. *Modelos de despliegue*. Independientemente del modelo de servicio utilizado (SaaS, PaaS, IaaS), hay cuatro formas principales en los que se despliegan los servicios en la nube y se caracterizan con modelos de despliegue adicionales que afrontan requisitos específicos, los cuales son:

a. Público

b. Privado

c. Híbrido

d. Comunidad

2.1.1 Tipos de servicios

El cómputo en la nube se compone de tres modelos de servicio:

a) Software
b) Plataforma
c) Infraestructura

Cada pilar cumple un propósito diferente en la nube y cubre distintas áreas de productos y servicios para empresas y particulares de todo el mundo.

En la tabla 2.1 se da a conocer un breve resumen de lo que es cada uno de los servicios ofrecidos en el cómputo en la nube , así como a quiénes va dirigido y en seguida una explicación más amplia de los mismos.

Tabla 2.1 Tipos de servicios en el cómputo en la nube

Servicio	Descripción	Cliente
SaaS	Modelo de distribución de software donde una empresa mantiene el derecho de uso y factura al cliente por el tiempo que haya utilizado el servicio.	Cliente final: Particulares, empresas y administraciones.
PaaS	Modelo de alquiler de entornos de desarrollo y ejecución de aplicaciones o de parte de ellas.	Desarrolladores de aplicaciones informáticas.
IaaS	Modelo de alquiler de infraestructura de computación o de alguna de sus partes:	Va dirigido hacia el cliente final y a los desarrolladores.

	capacidad de almacenamiento, procesamiento. Entrega de servicio de equipamiento informático.	

a) Software como servicio (SaaS)

Consiste en un despliegue de software en el cual las aplicaciones y los recursos computacionales se han diseñado para ser ofrecidos como servicios de funcionamiento bajo demanda. De esta forma se reducen los costos tanto de software como hardware, así como los gastos de mantenimiento y operación.

Las consideraciones de seguridad son controladas por el proveedor del servicio. El suscriptor del servicio únicamente tiene acceso a la edición de las preferencias y a unos privilegios administrativos limitados.

En el segmento de software, el cómputo en la nube ha demostrado ser útil como un modelo de negocio. Ejecutando el software mediante servidores centralizados en Internet en lugar de servidores locales, los costos se reducen enormemente. Por otra parte, al eliminar los gastos de mantenimiento, de licencias y de hardware necesario para mantener servidores locales, las empresas son capaces de ejecutar aplicaciones de forma mucho más eficiente desde el punto de vista informático.

b) Plataforma como servicio (PaaS)

La plataforma de cómputo en nube ("*Platform as a Service (PaaS)*") permite a los usuarios acceder a aplicaciones en servidores centralizados, sustentándose en la infraestructura de la nube. De esta manera, permite el funcionamiento de las aplicaciones en nube, facilitando la implementación de las mismas sin el costo y la complejidad de mantener múltiples capas de hardware y software como ha ocurrido hasta ahora.

Éste es el modelo de plataforma como servicio o PaaS en el cual el servicio se entrega bajo demanda, desplegándose el entorno (hardware y software) necesario para ello. De esta forma, se reducen los costos y la complejidad de la compra, el mantenimiento, el almacenamiento y el control del hardware y el software que componen la plataforma.

El suscriptor del servicio tiene control parcial sobre las aplicaciones y la configuración del entorno ya que la instalación de los entornos dependerá de la infraestructura que el proveedor del servicio haya desplegado. La seguridad se comparte entre el proveedor del servicio y el suscriptor.

c) Infraestructura como servicio (IaaS)

El último segmento del cómputo en la nube, la infraestructura ("*Infrastructure as a Service (IaaS)*"), representa en gran medida la columna vertebral de todo el concepto. La infraestructura es la

que permite a los usuarios crear y usar el software y las aplicaciones.

En lugar de mantener centros de datos o servidores, los clientes compran los recursos como un servicio completamente externo. Los proveedores cobran los servicios según la base establecida y por la cantidad de recursos consumidos.

Es un modelo en el cual la infraestructura básica de cómputo (servidores, software y equipamiento de red) es gestionada por el proveedor como un servicio bajo demanda, en el cual se pueden crear entornos para desarrollar ejecutar o probar aplicaciones.

El principal fin de este modelo es evitar la compra de recursos por parte de los suscriptores, ya que el proveedor ofrece estos recursos como objetos virtuales accesibles a través de una interfaz de servicio.

El suscriptor mantiene generalmente la capacidad de decisión del sistema operativo y del entorno que instala. Por lo tanto, la gestión de la seguridad corre principalmente a cargo del suscriptor.

2.1.2 Tipos de infraestructura

Dependiendo de las necesidades de cada empresa, el tipo de servicio ofrecido y la forma en cómo se implementa hace que existan diversos tipos de nube:

a) Nubes públicas

En este tipo de nube la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet. La infraestructura y los servicios que se ofrecen a los usuarios suelen ser gestionados por un proveedor. Éstas pueden tener un modelo gratuito, en algunas oportunidades, o pagado en otras, todo dependiendo del servicio que se brinde.

b) Nubes privadas

En este tipo de nube la empresa es la encargada de la implementación tecnológica, los gastos de mantenimiento, la seguridad y disponibilidad de los datos. Sus funciones están enfocadas a un grupo de usuarios que requieran uno o más servicios.

c) Nube comunitaria

En este tipo de nubes existe una alianza entre dos o más organizaciones. La característica más importante es que la infraestructura tiene que estar orientada a objetivos similares, con un marco de seguridad y privacidad común.

d) Nubes híbridas

Cuando un tercero brinda un servicio de apoyo a alguna empresa, ya sea Saas, Paas o Iass, se habla de nubes híbridas. En este caso la utilización de varias infraestructuras a la vez es un

punto clave; pueden mantenerse como entidades separadas pero están unidas por la tecnología estandarizada o propietaria.

En este caso las ventajas e inconvenientes son los mismos que los relativos a los tipos de nube que incluya la infraestructura.

2.2 Ventajas y desventajas del cómputo en la nube

Las ventajas del cómputo en la nube así como una breve descripción de las mismas se muestran en la tabla 2.2.

Tabla 2.2 Ventajas del cómputo en la nube

Ventaja	Descripción
Rápido	Los servicios más básicos de la nube funcionan por sí solos. Para servicios de software y base de datos más complejos, el cómputo en la nube permite saltarse la fase de adquisición de hardware y el consiguiente gasto, por lo cual es perfecta para la creación de empresas
Actualizaciones	La mayoría de los proveedores actualizan constantemente su software, agregando nuevas funciones tan pronto como están disponibles.
Elástico	Adaptable rápidamente a negocios en crecimiento o de picos estacionales, ya que el sistema en la nube está diseñado para hacer frente a fuertes aumentos en la carga de trabajo. Esto incrementa la agilidad de respuesta, disminuye los riesgos y los costos operacionales, porque sólo escala lo que crece y paga sólo lo que usa.

Móvil	El sistema en nube está diseñado para ser utilizado a distancia, así que el personal de la empresa tendrá acceso a la mayoría de los sistemas en cualquier lugar donde se encuentre.
Mínima inversión en infraestructura	El proveedor ofrece servicios a varias empresas, las cuales se benefician de compartir una infraestructura compleja y pagan solamente por lo que realmente utilizan.
Bajo costo	En una computadora central es mucho más sencillo y más barato organizar el mantenimiento y la seguridad, por ejemplo, ya no tenemos que estar constantemente actualizando los programas antivirus porque ya está incluido en la conexión.
Ayuda al ambiente	Con una computadora central se necesita mucho menos energía que una computadora personal y por lo tanto es mucho más barato (ventajas para el consumidor).

Como todo, el cómputo en la nube también tiene desventajas, las desventajas se muestran en la tabla 2.3.

Tabla 2.3 Desventajas del cómputo en la nube

Desventaja	Descripción
Dependencia de terceros.	Para el usuario particular, si Internet no está disponible cuando el proveedor está sobrecargado, se paralizara todo el sistema. Para las empresas el problema es menos grave, ya que por razones de seguridad, suelen disponer de varios accesos a la red.
Falta de conexión	No se está conectado en todo momento a Internet, pues actualmente existen muchos lugares donde no se tiene conexión, y en este caso el cómputo en la nube no serviría.
Pérdida de gobernabilidad	Al hacer uso de servicios basados en cómputo en la nube, las empresas comparten con el proveedor la administración de sus activos.
Cuestiones administrativas	Ante una situación en la que se necesiten nuevos servicios se ha de recurrir a una renegociación de los términos de contrato o acudir a otra empresa. Además muchos contratos tienen clausulas como evasión de responsabilidades y cesión de propiedad de datos. Es muy importante leer bien los contratos antes de exponer los datos o los de la empresa a un tercero.

2.3 Diferencias entre el cómputo tradicional y el cómputo en la nube.

Prácticamente desde el surgimiento de las redes de computadoras existe el modelo de trabajo en red, donde "terminales tontas" establecen conexión con un servidor y es en éste donde todas las aplicaciones y recursos se encuentran.

El modelo de trabajo en red ha ido evolucionando hasta poder utilizar Internet como medio para acceder a múltiples recursos y aplicaciones Web desde cualquier equipo usando únicamente un navegador. Los equipos que se conectan son los clientes y el trabajo se realiza a través de la nube en uno o más servidores.

A pesar de su semejanza, el uso de Internet le da grandes diferencias al cómputo en la nube las cuales se muestran en la tabla 2.4.

Tabla 2.4 Diferencias entre las características del modelo tradicional y del modelo de cómputo en la nube

	Modelo Tradicional	Cómputo en la nube
Modelo de compra	Compra activos y construye arquitectura técnica	Compra Servicios
Modelo de negocio	Paga activos fijos y administrativos	Pago con base en su uso

Modelo de acceso	De la red interna al escritorio corporativo	En Internet a cualquier dispositivo
Modelo técnico	Arrendamiento individual, no compartido, estático	Escalable, elástico, dinámico, multiusuarios

2.4 Estadísticas y ejemplos del cómputo en la nube en la actualidad.

Con la finalidad de conocer la situación actual y la perspectiva que se tiene en las pequeñas y medianas empresas mexicanas sobre el cómputo en la nube, se realizó una encuesta[1] al personal de 13 empresas[2] dedicadas a las tecnologías de la información (TI), quienes ocupan puestos de analistas de sistemas (31%), oficiales de seguridad (25%), administradores de servidores (13%), programadores (25%) y administradores de proyectos (6%), obteniendo algunos resultados que se mencionarán a continuación.

En los últimos años el cómputo en la nube ha tenido auge en el uso de aplicaciones conocidas como de productividad, entre las cuales se encuentran:

- Correo

[1] Ver Anexo A.

[2] Por motivos de confidencialidad no se mencionan los nombres de las empresas.

- Web
- Aplicaciones de oficina
- Administración de documentos

De alguna manera el personal de las empresas ya está utilizando cómputo en la nube, pero como se indica en la figura 2.2, el 27 % de los encuestados dice no conocer el término.

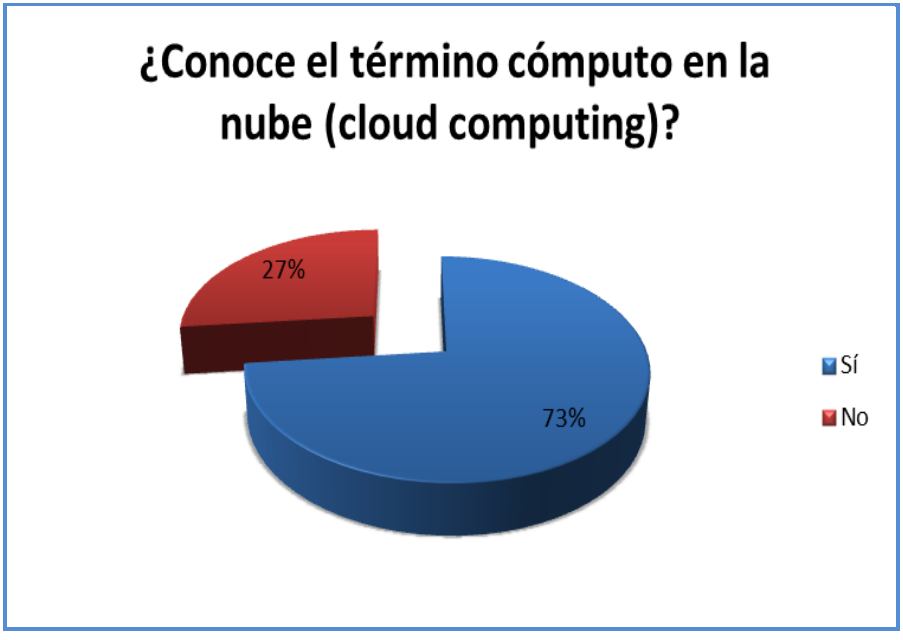

Figura 2.2 Conocimiento del término cómputo en la nube.

Como se observa en la figura 2.3, el 91% del total de los encuestados recomiendan el uso del modelo de cómputo en la nube en la empresa en que trabajan, pues aseguran que son varias las ventajas que tiene este nuevo modelo, por ejemplo:

- Reducción de costos.
- Eficacia y eficiencia en la entrega de servicios.
- Compatibilidad y distribución en los sistemas desarrollados.
- Reducción en tiempo e inversión durante la implementación.
- Acceso a la información en todo momento.

Con un porcentaje menor, la contraparte indica que debido a la falta de madurez y soporte que actualmente se tiene, aún no piensa en la adopción del modelo como una alternativa.

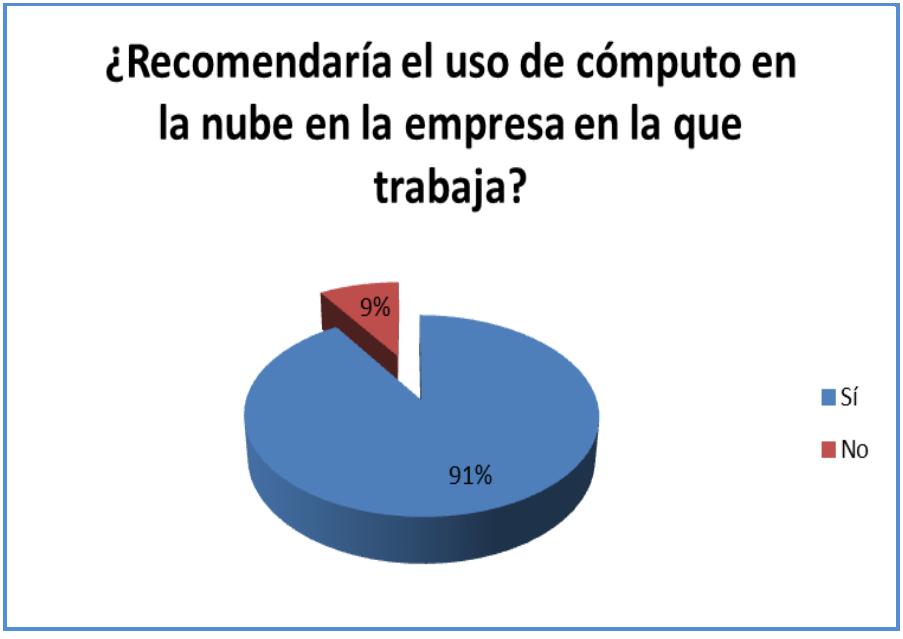

Figura 2.3 Recomendación del uso de cómputo en la nube en la empresa.

Mucho se habla de las ventajas de adopción de soluciones o servicios basados en la nube, de acuerdo con la figura 2.4, el 18% de las empresas ya están adoptando soluciones de cómputo en la nube, otras empresas (27%) migrarían sus servicios a la nube en uno o dos años aproximadamente, sin embargo, para la mayoría no es una de sus principales prioridades y no la adoptarían en un futuro próximo.

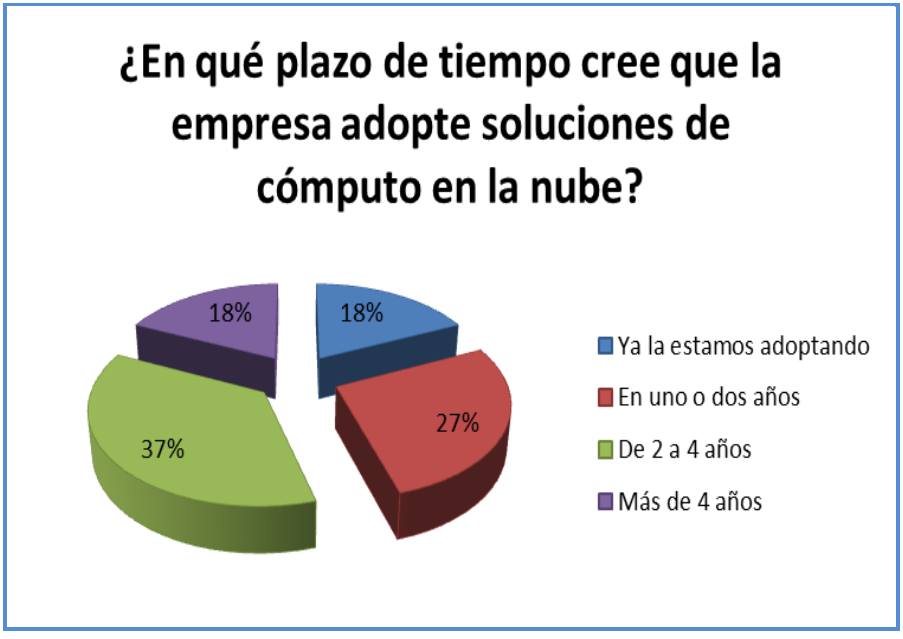

Figura 2.4 Adopción de soluciones de cómputo en la nube.

Al momento de tomar decisiones acerca de la nube, surge duda sobre cuál es el tipo de infraestructura a implementar. De acuerdo con la figura 2.5, ninguno de los encuestados recomendaría el uso de nube pública, tan solo el 18% recomiendan el uso de nube privada indicando que se tendría mayor control del entorno de red y de las medidas de seguridad para salvaguardar los activos de la empresa.

El mayor porcentaje de las personas encuestadas coincide en las razones por las cuales recomiendan el uso de la nube híbrida, éstas se mencionan a continuación:

a) Proporciona flexibilidad.

b) La información, servicios e infraestructura crítica de la empresa deberá mantenerse dentro de la organización a través de una nube privada.

c) En la nube pública se deberían tener todos aquellos servicios no críticos.

Tan solo el 9% de los encuestados desconoce el tipo de infraestructuras.

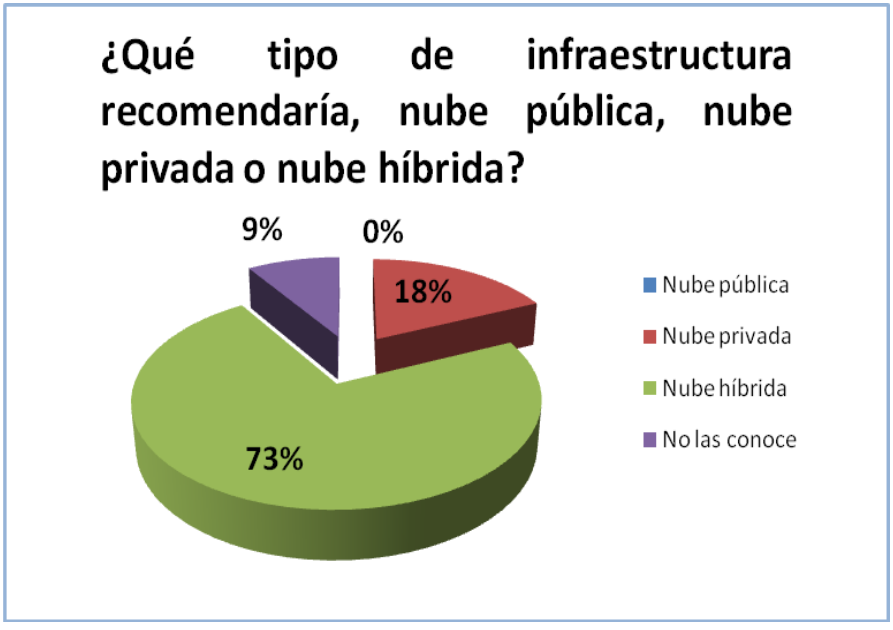

Figura 2.5 Tipo de infraestructura recomendada.

Son diversas las razones por las cuales una empresa usa o usaría cómputo en la nube, pero se puede observar en la figura 2.6 que el mayor porcentaje se debe a la reducción de costos que

implicaría su uso, siguiendo con el incremento en la eficiencia, derivándose en mejorar el servicio del cliente y la rápida implementación del cliente.

No se ven como razones principales el cumplimiento normativo, como opción para mejorar la seguridad e incrementar la flexibilidad y la capacidad de elegir.

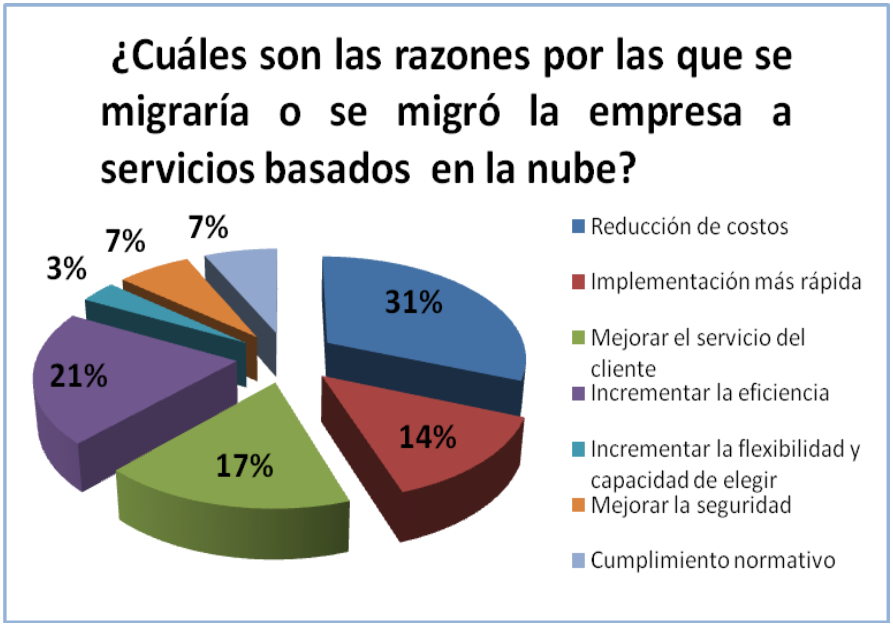

Figura 2.6 Razones de la empresa para migrar a los servicios de la nube.

Como se puede observar en la figura 2.7 un gran número de empresas tienen la preocupación de perder seguridad y el control de la administración de sus recursos e información al migrarse a la nube, que como se mencionó, no se considera una

de las principales razones para la adopción de los servicios basados en la nube, sobre todo por no conocer la localización geográfica de los servidores, control de accesos a los mismos y a la información contenida en éstos.

Los encuestados también consideran como obstáculo a Internet por el escaso acceso que se tiene a la banda ancha en México, así como la falta de servicio de Internet en varias comunidades a nivel nacional.

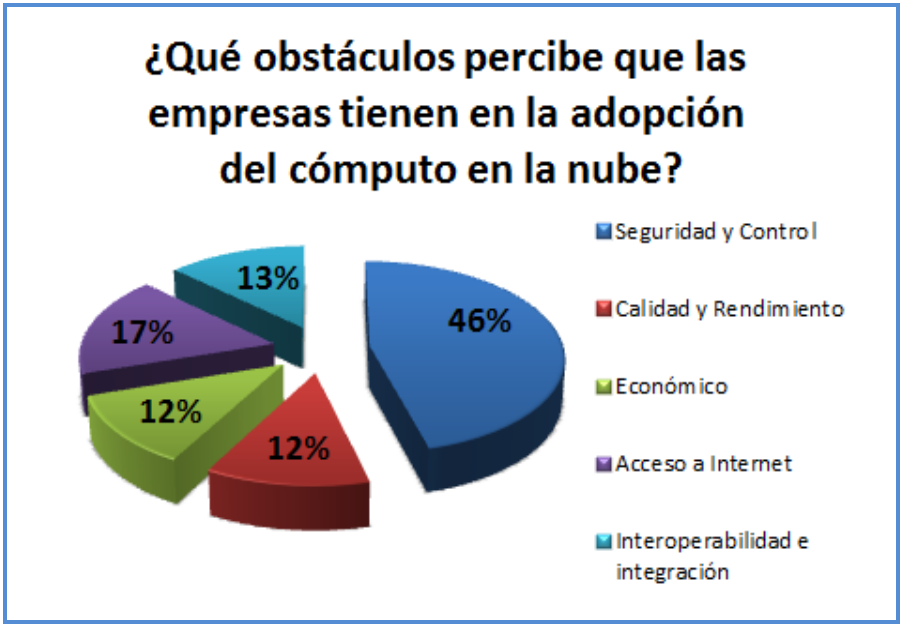

Figura 2.7 Obstáculos en la adopción de cómputo en la nube.

El mayor porcentaje de las personas encuestadas, como se muestra en la figura 2.8, considera que al migrar servicios a la

nube se generará una mayor competividad en las empresas en las que laboran, pues habrá:

- Reducción de costos.
- Incrementará la productividad.
- Inminentemente habrá mayor eficiencia.

La contraparte indica que es como cualquier otra forma de entrega de servicio y que las pequeñas empresas están compitiendo a bajo nivel, sin embargo, la realidad es otra, pues las pequeñas y medianas empresas podrán tener herramientas de gestión tan robustas y rápidas como las que hasta ahora pagan las grandes empresas, por otro lado se minimizarían los riesgos financieros en el lanzamiento de nuevos servicios o desarrollos y los gastos fijos se pueden convertir en variables.

Figura 2.8 Competividad empresarial al usar cómputo en la nube.

Como se presenta en la figura 2.9, la diferencia de porcentajes entre las personas que conocen o no los estándares con los que deberían operar o cumplir los proveedores de servicios es abismal, esto se puede deber a las siguientes causas:

- Falta de interés en la estandarización, pues aún no usan el cómputo en la nube.

- Falta de difusión de la estandarización o normativas que regulen el cómputo en la nube.

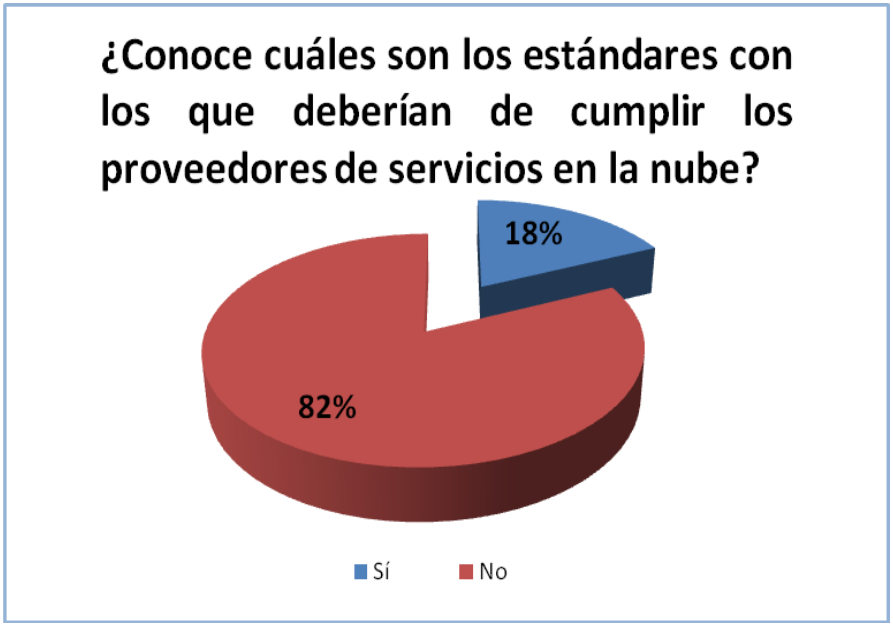

Figura 2.9 Conocimiento de estándares en la nube.

De acuerdo con un informe de la Asociación Internacional de Auditoría y Control de Sistemas de Información (ISACA), en México el 26% de las empresas utilizan cómputo en la nube como un socio de negocios en la estrategia corporativa brindando una mejor gestión de la información.

De las empresas usuarias, el 13% lo hace para servicios esenciales como e-mail y almacenamiento de acuerdo con la encuesta. Sin embargo, a pesar de la creciente adopción, el tema de seguridad de la información es la principal preocupación para las organizaciones en el uso de este modelo.

Se puede observar en la figura 2.10 que el nuevo esquema de cómputo en la nube en México estará evolucionando,

incrementándose el número de servicios bajo este esquema, así como que las grandes, pequeñas y medianas empresas migrarán parte de su infraestructura a la nube.

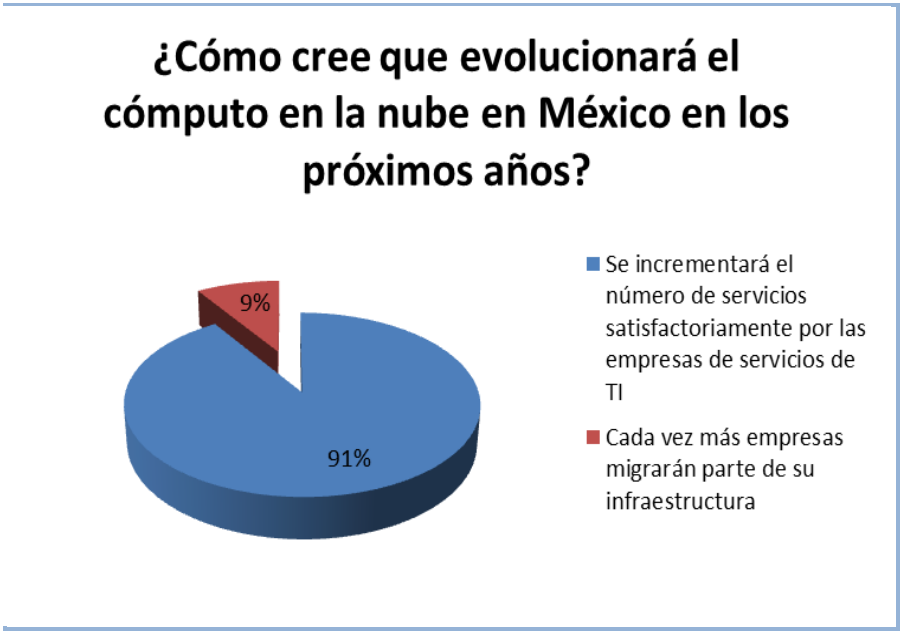

Figura 2.10 Evolución de cómputo en la nube en México.

La evolución del cómputo en la nube en las empresas depende de factores como el tamaño, la madurez y la inversión que se realiza en TI.

Existen países en los que ya se reconocen los beneficios del almacenamiento en la nube, la utilización de aplicaciones en ésta, ahorros en infraestructura y energía, como en el caso de empresas españolas y del norte y sur de América Latina, por mencionar algunas.

a) Cómputo en la nube en España.

De acuerdo con el estudio de Avanade (proveedor de servicios de tecnología) de junio de 2011, la nube privada será adoptada por el 70% las empresas españolas por motivos de seguridad. Para el 43 % de las empresas se vuelve importante la adopción de los servicios de cómputo en la nube para ahorrar costos y para un 23% por la innovación y crecimiento empresarial.

Actualmente un 40% utiliza servicios en la nube privada, el 75% de los que no la están usando ya se encuentra en su estrategia de negocio.

Las principales aplicaciones que las empresas españolas utilizan en la nube son el correo electrónico, herramientas de ofimática (Google Drive y Office Web Apps), CRM (Customer Relationship Management o Administración basada en la Relación con los Clientes.) y aplicaciones de finanzas.[3]

b) Cómputo en la nube en norte y sur de América Latina.

Según la encuesta encomendada por Symantec y realizada por Applied Research sobre "Virtualización y evolución hacia la nube 2011" a empresas ubicadas en Estados Unidos, Canadá, Argentina, Chile, Uruguay, Paraguay, entre otros, en abril de 2011, se exploró el modo en que las empresas trasladarían sus aplicaciones críticas de negocio a entornos de cómputo en la nube híbridos y virtualizados, por lo que se puede visualizar que las empresas tienen interés y están implementando servicios

[3] http://www.avanade.com/es-es/about/avanade-news/press-releases/Documents/NP_Avanade_Estudio_Cloud_Spain-julio2011.pdf

basados en la nube. De acuerdo con la encuesta, el tipo de aplicaciones que se están implementando o considerando implementar en un futuro próximo, entre otras, son:

- Aplicaciones Web.
- Administración de base de datos, correo electrónico y ERP.
- Administración de documentos.
- Inteligencia de negocios, aplicaciones de recursos humanos, aplicaciones Office.
- Administración de proyectos.
- Contables, financieros o CRM.

Además la mayoría de estas empresas sigue el mismo camino para dar paso a la adopción del cómputo en la nube, primeramente las empresas implementan la virtualización en los servidores, después virtualización en el almacenamiento y los equipos de escritorio y por último implementan el almacenamiento privado como servicio y/o una nube privada o híbrida.

Es posible observar ejemplos del cómputo en la nube en la actualidad. El cómputo en la nube se puede aplicar en casi cualquier entorno: desde el pequeño comerciante que necesita

un sitio Web de comercio electrónico de forma rápida y barata, aplicaciones individuales de negocios, como el cálculo de impuestos, rentas o contribuciones, hasta grandes compañías que requieren gran poder de cómputo como la externalización informática de alto rendimiento para complejos diseños en 3D, películas de cine o investigación científica.

El cliente puede en todo momento decidir qué aplicaciones usar y elegir entre aquellas que son gratuitas y las que no lo son. En el caso de las aplicaciones de pago, el costo irá en función de diversas variables, como el servicio contratado, el tiempo que se ha usado ese servicio, el volumen de tráfico de datos utilizado, etcétera.

Varias son las grandes empresas que se han dedicado a ofrecer estos servicios promoviendo el fácil acceso a la información, los bajos costos, la escalabilidad, y muchas características que hace pensar en la comodidad que brindan. Entre ellas se mencionan:

a) Amazon EC2 (Infraestructura como plataforma)

Amazon Elastic Compute Cloud (Amazon EC2) es un servicio Web que se ha diseñado con el fin de que la informática Web resulte más sencilla a los desarrolladores, proveyendo capacidades de cómputo elásticas, disponibles a través de una infraestructura cloud diseñada con la finalidad de proveer computación escalable a entornos Web bajo demanda, siguiendo un modelo comercial de pago por uso. (Amazon Web Services, LLC).

Amazon EC2 presenta un entorno informático virtual, que permite utilizar interfaces de servicio Web para iniciar instancias con distintos sistemas operativos, cargarlas con su entorno de aplicaciones personalizadas, gestionar sus permisos de acceso a la red y ejecutar su imagen utilizando los sistemas que desee. La sencilla interfaz de servicios Web de Amazon EC2 proporciona un control completo sobre los recursos informáticos y permite ejecutarse en el entorno informático acreditado de Amazon.

b) Salesforce.com (Software como servicio)

Salesforce.com ofrece la utilización del software como servicio, incluyendo aplicaciones para ventas, servicio, soporte y comercialización.

c) Force.com (Plataforma como servicio)

Force.com presta la utilidad de plataforma como servicio permitiendo a los desarrolladores externos crear aplicaciones

adicionales que se integran en las aplicaciones de CRM (Customer Relationship Management o gestión de las relaciones con el cliente).

d) Google App Engine (Plataforma como servicio)

Google App Engine es una plataforma para la creación y alojamiento de aplicaciones Web utilizando la infraestructura de Google.

Google Apps es un conjunto de aplicaciones en la nube que incorpora varias aplicaciones y la posibilidad de añadir aplicaciones de terceros. En conclusión, es un contenedor de aplicaciones útiles, ofreciendo herramientas eficaces para la manipulación, gestión y personalización de utilidades para dominios o nombres de Internet. Como por ejemplo: Google Apps permite gestionar el correo electrónico de los dominios (a través de Gmail), mensajería instantánea entre miembros de la organización o red (Google Talk), calendario en línea (Google Calendar), edición de documentos en línea (Google Drive) y creación de sitios Web profesionales (Google Sites).

Google Apps ofrece tres planes distintos de servicio, enfocados precisamente a tres principales tipos de clientes. Asimismo, dentro de cada plan se ofrecen diferentes escalas del servicio:

- Empresas y empleados. Estándar (Gratuita) y Premier (de Pago).

- Centros Docentes y Estudiantes. Estándar (Gratuita), Premier (de Pago) y Educación (Sólo para instituciones estudiantiles sin ánimo de lucro).

- Organizaciones y Miembros. Mismos planes que la edición de Centros Docentes y Estudiantes.

Una de las mejoras que se han integrado recientemente a Google Apps, son las novedosas herramientas de Seguridad de Postini, empresa que Google adquirió en el año 2007. Esta tecnología incluye una gestión centralizada de la política de los mensajes salientes y entrantes, así como para los filtros anti-spam, el bloqueo de correos electrónicos que intenten enviar o difundir información sensible de la empresa u organización, así como un novedoso y potente anti-virus Web completamente personalizable según el grado de las necesidades.

e) Microsoft (Software como servicio, Plataforma como servicio e Infraestructura como servicio)

Además del modelo tradicional que se conoce de instalar en el disco duro de una PC y comprar una licencia para dicho equipo, Microsoft Office también se encuentra como un servicio en la nube. En abril de 2011 Microsoft anunció la versión beta de su office “en la nube” denominado office 365 y cuya versión final se dio a conocer a finales de junio de 2011. Ahora solo bastará tener un equipo con conexión a internet para poder utilizarlo.

Pero Microsoft Office es solo un ejemplo del nivel al que ha llegado la nube, también cuenta con otras muchas aplicaciones que usan la nube, algunas de ellas son:

1. Windows Azure: Un sistema operativo como servicio en línea. Es una plataforma de servicios en la nube, los cuales se alojan en centros de datos de Microsoft, ofreciendo el sistema operativo y un conjunto de servicios de desarrollo que pueden ser utilizados individualmente o en conjunto.

2. Microsoft SQL Azure: Solución completa de base de datos cloud relacional.

3. Plataforma AppFabric de Windows Azure: Conecta servicios en la nube y aplicaciones internas.

4. Almacenamiento en la nube de X-box Live: Está disponible en algunas regiones y con ciertos Arcades.

5. Microsoft Live@edu: Ofrece una plataforma extensible que promete control, mayor seguridad y otras funciones esenciales para las instituciones de nivel primario y secundario.

6. Windows Live: Es un conjunto de servicios y productos de software, la mayoría de estas aplicaciones Web son accesibles desde un navegador, pero también hay aplicaciones binarias que necesitan ser instaladas en la PC del usuario. Windows Live ofrece sus servicios de tres

maneras: aplicaciones de Windows Live Essentials, servicios Web y servicios móviles.

f) Apple (Software como servicio)

En iCloud el contenido se almacena en Internet y desde ahí los equipos de cómputo obtienen la información. Las propias aplicaciones recogerán los datos que necesiten directamente, todo disponible vía WiFi y 3G, desde cualquier equipo Mac e incluso PC.

Capítulo III

Implicaciones de seguridad en la nube

Se vuelve importante en esta nueva forma de entrega de servicios (cómputo en la nube) la identificación de las vulnerabilidades, amenazas y riesgos a los que están expuestos los activos donde se procesa y almacena la información, esto con el propósito de definir e implementar medidas adecuadas de seguridad para resguardar y proteger a los mismos de accesos no autorizados, modificación de la información, etcétera.

La principal preocupación de las pequeñas y medianas empresas en el uso y adopción de los servicios del cómputo en la nube son los riesgos en la seguridad de la información, así como la falta de definición de políticas, leyes y estándares.

3.1 Situación actual

Aunque se sabe que existen y se tienen claras las ventajas obtenidas del uso de los servicios de cómputo en la nube, como se indicó en el capítulo anterior, uno de los obstáculos y tema que preocupa a la mayoría de las empresas (y por lo cual temen adoptar el cómputo en la nube), es la seguridad y control de sus activos. Pero la realidad es que ningún sistema informático está exento de los riesgos actuales o de otros riesgos que puedan surgir por las características propias de la computación en la nube.

Cabe mencionar que debido al auge que ha empezado a tener este modelo, los servicios en la nube se han vuelto un tema de atención para los atacantes, tal es el caso de PlayStation, la

empresa de mercadotecnia Epsilon y Amazon, que han sido víctimas de robo de información personal de hasta 77 millones de usuarios, del robo de 250 millones de correos electrónicos y de la caída de servidores ocasionando la falta de disponibilidad del servicio a páginas que utilizan su herramienta, respectivamente.

A pesar de esto y de acuerdo con la encuesta titulada "Encuesta sobre virtualización y evolución hacia la nube 2011" (encargada por Symantec a Applied Research) y cuyos resultados se basan en las respuestas otorgadas por empresas ubicadas en países del sur de América Latina incluidos Argentina, Chile, Uruguay y Paraguay, se dice que actualmente las empresas se están moviendo con precaución para disfrutar de los servicios de la virtualización o tecnologías en la nube.

Primeramente las empresas suelen utilizar entornos de pruebas y desarrollo para obtener cierta experiencia. Cuando se sienten cómodos con la tecnología, están más dispuestos a poner aplicaciones sensibles en un entorno virtualizado / en la nube. Entre las empresas que actualmente están implementando la virtualización, las aplicaciones críticas empiezan ahora a ser el centro de atención. Las empresas están más dispuestas a virtualizar las aplicaciones de bases de datos, administración de documentos y también de correo electrónico. [3]

Sin embargo, más de la mitad de ellas planean implementar la virtualización el próximo año para aplicaciones críticas, como las relacionadas con recursos humanos y contabilidad, lo que

demuestra que se están acostumbrando a incorporar la tecnología al negocio. Sin embargo, las empresas son más cautelosas frente a la implementación de nubes híbridas/privadas. Los encuestados informaron que en promedio solamente el 33 por ciento de estas aplicaciones críticas como planeación de recursos (ERP), contabilidad y manejo de relaciones con los clientes (CRM) están en entornos híbridos/privados en la nube, pues están preocupados porque el servicio o el tráfico de datos sea interceptado o secuestrado, pérdida de control físico de datos y la recuperación ante desastres. [3]

Como complemento de la información anterior y derivado de los resultados obtenidos de la encuesta[4] realizada, a continuación se muestran estadísticas sobre puntos específicos que preocupan actualmente a las empresas sobre la seguridad del cómputo en la nube, así como la perspectiva e importancia que las empresas otorgan al tema de seguridad informática o de la información.

Los encuestados consideran y así mismo tienen identificados riesgos de seguridad que una empresa posee o tendría al migrar sus servicios a la nube.

A continuación se describen los riesgos que resultaron con mayor ponderación:

[4] Ver Anexo A

❖ Información comprometida. La información es el activo más importante de las empresas, por lo cual la pérdida de ésta es una de las principales preocupaciones que se tiene, pues las empresas necesitan asegurar la privacidad de la misma.

❖ Disponibilidad. Las personas o empresas temen que al contratar los servicios en la nube y al requerir tener acceso a su información o servicios, éstos no se encuentren disponibles en todo momento.

Sin embargo, los riesgos que aparecen en la figura 3.1 también se presentan en el modelo tradicional.

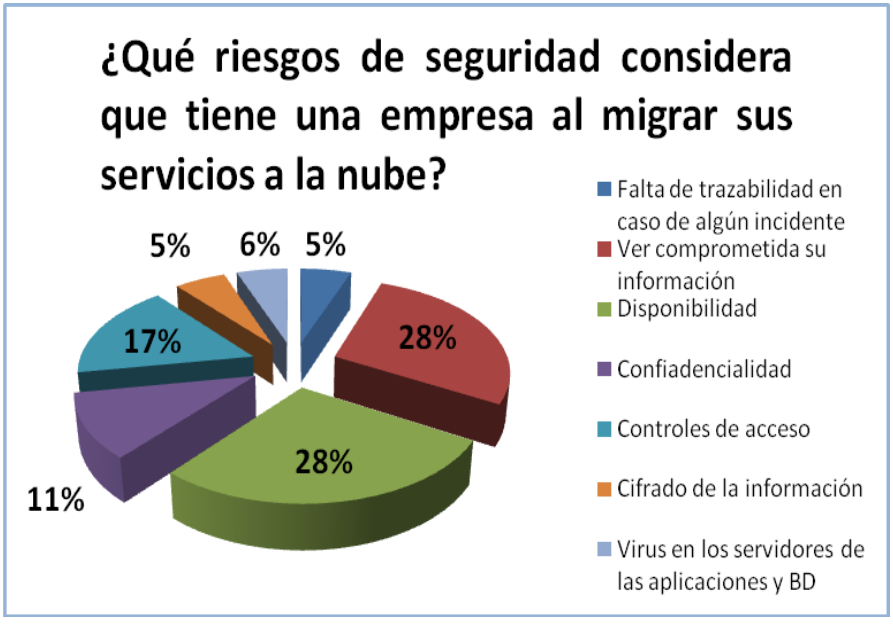

Figura 3.1 Riesgos al migrar servicios a la nube.

La mayoría de las respuestas otorgadas por los encuestados a la pregunta "¿Qué tan segura cree que esté la información almacenada en la nube?" fue segura, a pesar de que anteriormente se mencionaba por los mismos como un riesgo que la información se viera comprometida. La minoría opina que almacenar la información en la nube no es seguro, puesto que aún no se cuenta con los mecanismos de seguridad adecuados para resguardarla.

Otros más dicen no conocer a ciencia cierta si estará o no segura (Figura 3.2).

Sin embargo, la seguridad de la información en la nube mucho dependerá del tipo de control de accesos que se tenga o se implemente, de la decisión del dueño de la información acerca del tipo de información que crea conveniente se almacene en la nube, cifrado de la misma, controles de seguridad en el desarrollo de las aplicaciones, procedimientos y políticas de seguridad que lleven a cabo los administradores de los servidores.

Aunque se tomen en cuenta todas las medidas de seguridad, nunca serán completamente seguras y confiables.

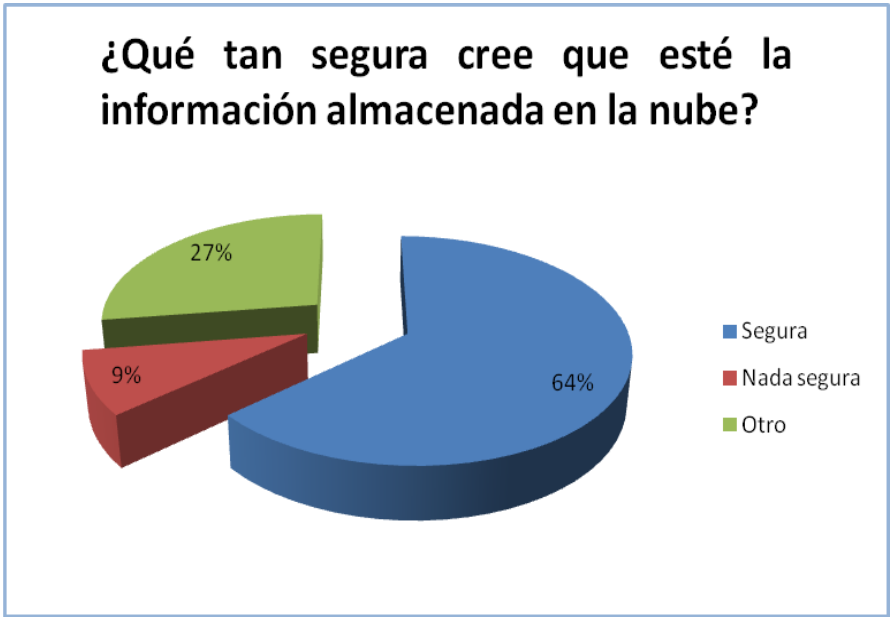

Figura 3.2 Seguridad en el almacenamiento en la nube.

Al hacer uso de los servicios basados en la nube y debido a que se involucra tanto el cliente como el proveedor de servicios, se lleva a cambios en la manera de entender la seguridad de la información, pues recaen responsabilidades sobre cada actor que deben llevar a cabo.

Como se muestra en la figura 3.3, el mayor porcentaje se otorga a que la responsabilidad de la seguridad en la nube recae sobre el cliente, después por ambas partes (cliente y proveedor de servicios) y al final con menor porcentaje se encuentra al proveedor.

Para lograr una entrega de servicios eficiente es necesaria la participación y compromiso por ambas partes.

Los mecanismos de seguridad que se pueden aplicar para proteger los datos alojados en la nube deben considerarse como un trabajo colaborativo entre ambas partes, ya que la realización de auditorías de seguridad conjuntas es una buena práctica para revisar que todo el sistema está protegido frente a posibles amenazas. [2]

Figura 3.3 Responsabilidad de la seguridad en la nube

Proteger la información de la empresa, así como a sus recursos del impacto que es provocado por la divulgación de información confidencial, corrupción o pérdida de información o interrupción de los procesos críticos del negocio es de suma importancia. La implementación de seguridad informática desempeña un papel muy importante en este proceso.

La seguridad informática les brinda confianza a las empresas que cada vez lo toman más en cuenta. Es un tema primordial en estos días, ya que una enorme cantidad de datos sensibles viajan por la red. Se mantendría un mejor control de la empresa y se conocerían y corregirían las vulnerabilidades para hacer frente a ellas; se tendría un mejor panorama general de la empresa.

La pérdida parcial o total de la misma podría resultar catastrófica para las empresas.

Como se indica en la figura 3.4, el personal de la empresa indica que la seguridad de la información se toma en cuenta para cumplir con los objetivos de TI.

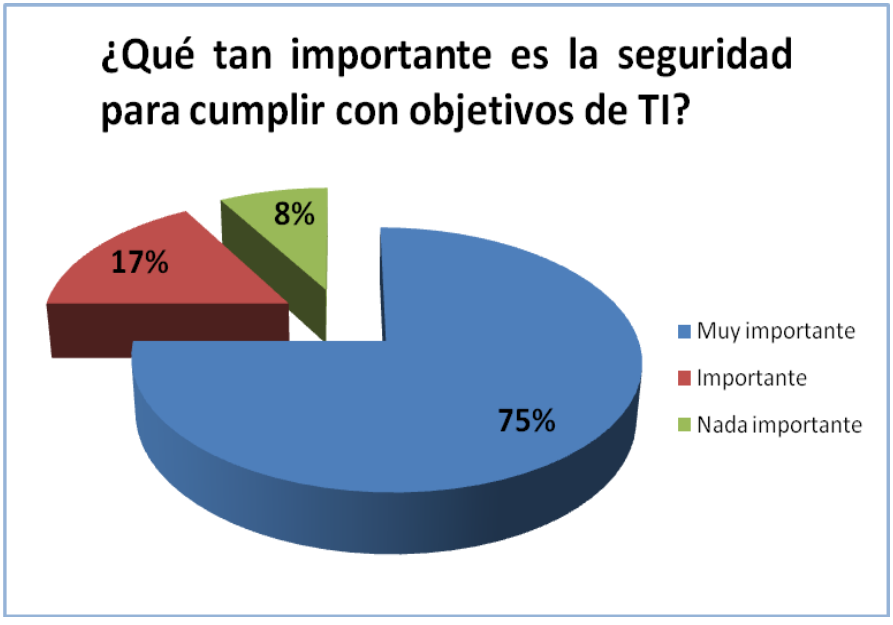

Figura 3.4 Importancia de la seguridad para cumplir objetivos de TI.

Una empresa posee una ventaja competitiva cuando tiene alguna característica diferencial respecto de sus competidores, que le confiere la capacidad para alcanzar unos rendimientos superiores a ellos, de manera sostenible en el tiempo.

La mayoría de los encuestados creen que la seguridad informática genera una mayor competividad empresarial (Véase figura 3.5)

Lo anterior es cierto, ya que la seguridad informática forma parte de las ventajas competitivas en las empresas, pues éstas al tener mejores respuestas en sus sistemas de información y al brindar la confianza necesaria para el resguardo de la misma

puede dar como resultado una buena imagen, por ejemplo. Así mismo comprueban el cumplimiento de la legislación o normatividades, protección de datos de carácter personal, propiedad intelectual, etcétera.

Figura 3.5 Competitividad empresarial

Aunque la seguridad de la información es considerada como importante por los integrantes de las empresas, el porcentaje de los recursos asignados a este tema es mínimo como se muestra en la figura 3.6, lo cual se debe a que lo ven como un gasto y no como una inversión a largo plazo.

Las empresas deben tomar en cuenta el gasto o pérdida de credibilidad que implicaría no contar con los mecanismos de

seguridad adecuados para el resguardo de la información comparado con una cifra (presupuesto óptimo) siendo esto igual o mayor gasto.

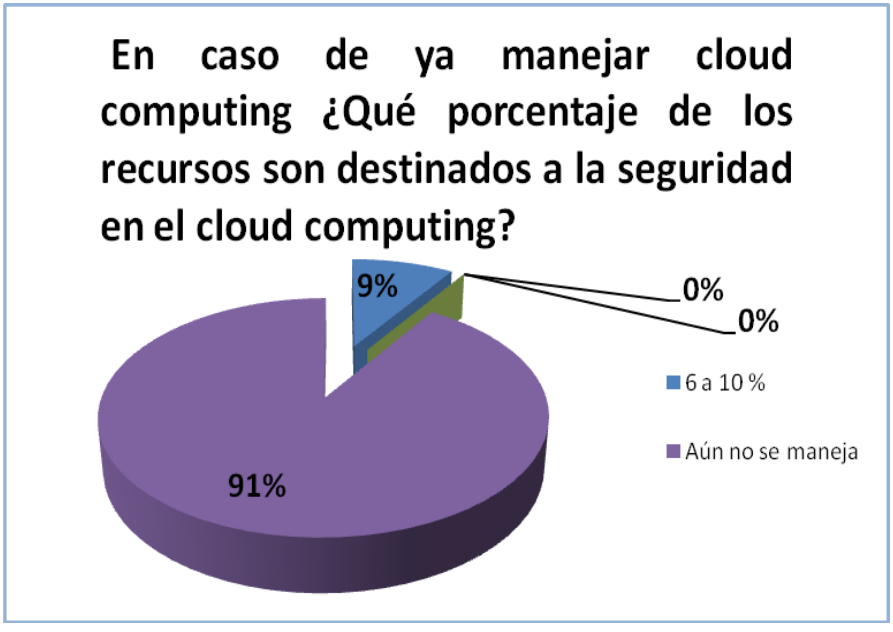

Figura 3.6 Porcentaje de los recursos destinados a la seguridad en el cómputo en la nube.

3.1.1 Retos de seguridad

Como se ha venido explicando a lo largo de los capítulos, el cómputo en la nube al ser un nuevo modelo que se está o se quiere implementar en las empresas, presenta desafíos o retos en los que se debe poner énfasis para obtener el éxito esperado

del nuevo modelo, principalmente al hacer uso de servicios en la nube pública.

A partir del estudio realizado, los retos de seguridad que se consideran en la computación en la nube se enlistan a continuación:

a) Localización geográfica de los datos y de la información.

b) Propiedad y control de los datos que se almacenan, procesan, generan o transmiten a través de los servicios en la nube.

c) Privacidad.

d) Disponibilidad, integridad y confidencialidad en la información.

e) Viabilidad y madurez en el mercado del modelo.

f) Cumplimiento regulatorio, estandarización y legislación.

g) Cifrado.

h) Procedimientos para la migración a la nube.

i) Planes de recuperación de desastres.

j) Soporte para análisis forense (técnico y legal)

En la tabla 3.1 se encuentra la descripción de cada uno de los retos mencionados.

Tabla 3.1 Retos de seguridad

Reto de seguridad	Descripción
a) Localización geográfica de la información.	Al hacer uso de servicios de cómputo en la nube no se conoce en que país el proveedor tiene alojada la información, por lo que su localización geográfica es inquietante para aquellas empresas que están alineadas al cumplimiento de leyes, pues representan desafíos reglamentarios al encontrarse en un sitio diferente al natal debido a que se pueden regir por diferentes legislaciones.
b) Propiedad y control de los datos que se almacenan, procesan, generan o transmiten a través de los servicios en la nube.	Es necesario conocer quién maneja los datos a través de los servicios en la nube, pues al realizar el procesamiento de datos sensibles fuera de las

	instalaciones de la empresa conlleva un riesgo inherente. Los datos en los entornos de nube comparten infraestructura con datos de otros clientes. El proveedor debe garantizar el aislamiento de los datos de los clientes.
c) Disponibilidad, integridad y confidencialidad en la información.	La integridad y confidencialidad de los datos es crítica, pues los datos son transferidos constantemente entre los servicios en la nube y distintos usuarios acceden a ellos, así mismo es importante tenerlos disponibles cuando se quiera hacer uso de los mismos.
d) Viabilidad y madurez en el mercado del modelo.	De manera ideal los proveedores de servicios de cómputo en la nube deben ofrecer un servicio de calidad y de alta disponibilidad continuamente. Sin embargo,

	el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos.
e) Cumplimiento regulatorio, estandarización y legislación.	Algunas regulaciones basadas en cuestiones de privacidad restringen de manera explícita la exportación de cierto tipo de datos hacia países que no tienen regulaciones equivalentes, tal es el caso de PCI.
f) Cifrado.	Como medida de protección de la información, es importante la implementación de cifrado para el acceso a la interfaz de control de recursos de la red, cifrado administrativo de acceso a las instancias de sistemas operativos, cifrado de acceso a las aplicaciones, cifrado de los datos de las aplicaciones.

g) Planes de recuperación de desastres.	Se vuelve importante que los proveedores de servicio cuenten con un esquema de alta disponibilidad, es decir, que la información sea replicada en múltiples infraestructuras evitando caer en fallas completas. Por otro lado deben contar con un plan o políticas de recuperación de datos en caso de desastre.
h) Procedimientos para la migración a la nube.	Generar procedimientos para la migración de servicios a la nube, tomando en cuenta el tipo de información que las empresas manejan.
i) Soporte para análisis en caso de incidentes	Se vuelve complicada la investigación de actividades sospechosas o ilegales, al compartir infraestructura entre diferentes clientes, ya que los datos y los logs de varios

	clientes pueden estar mezclados o en varios servidores y centros de datos, principalmente en la nube pública, hibrida y comunitaria.
j) Seguridad y privacidad de la información.	Al utilizar alguno de los 4 modelos de despliegue de cómputo en la nube el mayor reto es que exista privacidad y seguridad de la información, sobre todo en la nube pública, híbrida y comunitaria, ya que el privado está más apegado al modelo tradicional.

3.2 Privacidad de la información en el cómputo en la nube.

Una de las áreas que es afectada por el cómputo en la nube es la privacidad. Aunque el control de la privacidad en el cómputo en la nube tiene muchas amenazas y vulnerabilidades en común con el modelo tradicional, también tiene problemas únicos de seguridad.

Por ejemplo, una explotación exitosa de robo de identidad puede resultar en una pérdida de privacidad que tiene un gran impacto

en la empresa. La organización puede sufrir a corto plazo las pérdidas debido a la rehabilitación, investigación, y los costos de la restitución. También se puede incurrir en problemas a largo plazo para la organización debido a la pérdida de credibilidad, confianza y la publicidad negativa.

En la actualidad el intercambio de datos entre personas y empresas es de gran volumen en Internet, pues poco a poco se ha extendido el uso de servicios desde la red. El cómputo en la nube al tratarse de una arquitectura de sistema abierto en el que los datos y aplicaciones de los clientes se encuentran en posesión del proveedor (en el caso de la nube pública e híbrida) y en los dos restantes modelos de despliegue (nube privada y nube comunitaria), la seguridad juega un papel importante, cuyo objetivo es proteger el conjunto de datos, así como las aplicaciones de amenazas, vulnerabilidades para finalmente minimizar los riesgos, por lo que es importante conocer el ciclo de vida que siguen los datos.

De acuerdo con un estudio realizado por European Network and Information Security Agency (ENISA) [2], el ciclo de vida que siguen los datos procesados en la nube son 4, como se indica en la figura 3.7 y se describen a continuación:

1. Se adapta a un formato o se crea un fichero que contenga toda la información necesaria para que pueda ser procesada en la nube.
2. La transferencia del usuario final hacia la nube se realiza mediante un correo electrónico, una aplicación específica para

importarlos o la transferencia de la copia de seguridad obtenida de un servidor en la empresa.

3. Los datos son procesados en la nube desde su almacenamiento hasta el cálculo de complejas operaciones matemáticas. Dichos datos pueden almacenarse en copias de seguridad en la nube para facilitar fututos accesos.

4. Una vez terminado el procesamiento de los datos, el resultado se muestra al usuario con el valor añadido de la información generado en la nube.

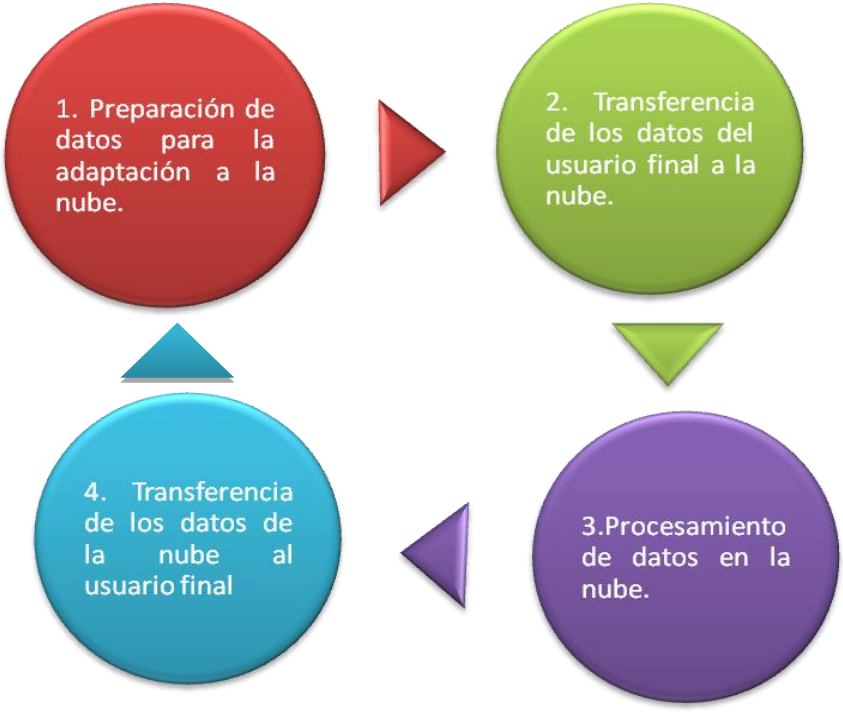

Figura 3.7 Ciclo de vida que siguen los datos procesados en la nube.

Unos de los principales problemas que pueden pensarse existen, es la pérdida del nivel de control sobre la información, que podría llegar a ser confidencial. La información es el activo más importante que poseen las empresas, por lo que el control de acceso a la misma se vuelve trascendental al utilizar servicios de computación en la nube, pues en la mayoría de los modelos utilizados en la nube el ciclo de vida que sigue la información, como se puede observar en la figura 3.7, sale de la empresa, lo que puede constituir un riesgo desde el punto de vista de la privacidad. El riesgo es que un usuario malintencionado podría interceptar los datos mientras están siendo transferidos por Internet o si están siendo almacenados y procesados en una infraestructura informática fuera de la empresa.

Los temas de privacidad que surgen en relación al cómputo en la nube son:

- Pérdidas de información.

- Penas convencionales, daños y perjuicios.

- Políticas aplicables, regulaciones estándar, contratos y políticas de intercambio.

- Metodologías de borrado, modificación, copia y acceso a la información.

- Seguridad en la transferencia y almacenamiento de la información.

- Segregación de la información. Están los datos separados de los de otros clientes.

- La información dispuesta a través de servidores y aplicaciones externos.

- La metodología con la que la información es puesta en la nube.

- Asegurar que se cumpla el ciclo de vida que siguen los datos procesados en la nube.

3.3 Vulnerabilidades y amenazas

Se han generado preocupaciones entorno a las vulnerabilidades, amenazas y riesgos al hacer uso de servicios en la nube, detectando que se tiene mayor inquietud sobre los temas de disponibilidad y seguridad de la información.

Como se ha venido estudiando, se tienen cuatro modelos en los que se pueden desplegar los servicios en la nube: Público, Privado, Híbrido y Comunitario. Cada uno de ellos tienen características específicas y algunas otras coinciden, por lo que al momento de revisar los puntos débiles y amenazas, éstas no difieren en gran medida de un modelo a otro. Por ejemplo, las

empresas suponen que en una nube pública se tiene la falta de gobernabilidad, gran número de usuarios y el compartir recursos y la negociación con el proveedor de la nube en la definición del contrato. Por otro lado, se tiene que las empresas al utilizar una nube privada deben estar preparadas para enfrentarse a amenazas como lo es la alta volatilidad en la utilización de los recursos, lo cual podría verse reflejado en escalar servicios a una nube pública, por lo cual se tendrían que redefinir nuevas políticas de seguridad. [4]

En la tabla 3.2, se hace mención de amenazas para el cómputo en la nube pública.

Tabla 3.2 Amenazas en el cómputo en la nube

Amenaza	Descripción
Fraude	Algunos ejemplos de fraude incluyen la manipulación de los datos y cualquier otra alteración de su integridad con la finalidad de obtener ganancias.
Robo de información /Fuga de datos	El robo de información o de secretos comerciales, se puede dar por la divulgación no autorizada, ya sea por personal interno o externo o por el robo físico del hardware.
Ataques externos	Dentro de los ataques externos

	se incluyen los escaneos hacia la infraestructura de la nube o la inserción de un código malicioso.
Delincuentes informáticos	Los delincuentes informáticos pueden planear sus ataques contratando servicios en la nube y ejecutarlos posteriormente, dificultando la persecución a los mismos, pues los recursos que se utilicen se borrarán una vez que concluya el ataque. También pueden contratar servicios de almacenamiento para guardar datos maliciosos o robados, dificultando de igual manera que las autoridades puedan acceder a esta información para actuar contra los atacantes.
Robo/Fallo de hardware Fallo en suministro de energía Desastres naturales	En caso de los desastres naturales, no se pueden predecir ni controlar su ocurrencia, las fallas en el suministro de energía y de hardware, así como el robo de este último pueden ser controlables.

Intercepción de datos.	Intercepción de datos durante la migración o actualización periódica de datos en la nube y/o modificación del tráfico de red.
Errores del proveedor de servicios en la nube (errores humanos).	Este tipo de amenazas se puede deber principalmente a la ignorancia o desconocimiento que se tenga sobre la manera de operar del cómputo en la nube, o por descuido o diversión por parte del personal encargado de la entrega de servicios.
Ingeniería social	La ingeniería social se busca a través del engaño y de la confianza del usuario al hacer clic en algún enlace o al utilizar interfaces de administración falsas, las cuales entregarán información crítica al atacante, como nombre de usuario, contraseña, por ejemplo.

Los principales puntos débiles al utilizar servicios de cómputo en la nube en las empresas se enlistan a continuación:

a) Falta de aislamiento de información o servicios.
b) Pérdida de gobernabilidad.
c) Falta de Integridad y confidencialidad de la información.

d) Pérdida o compromiso de registros de seguridad (manipulación de investigación forense).
e) Autenticación y autorización.
f) Acceso remoto a la administración de interfaces.
g) Falta de mecanismos de cifrado en los canales en donde se transfiere la información.
h) Falta de cifrado de archivos de datos en tránsito.
i) Funciones y responsabilidades poco claras.

3.4 Riesgos

Aunque el cómputo en la nube ofrece oportunidades y ventajas, no está exento de riesgos, la gran concentración de datos hacen que el cómputo en la nube sea un punto atractivo para los atacantes. Por esta razón es necesario conocer los riesgos presentes en un entorno de cómputo en la nube, con el fin de tomar las medidas necesarias para que éstos no afecten a los usuarios ni proveedores de servicios.

Hay que tomar en cuenta que independientemente de que si se implementa una nube pública, privada o híbrida se tendrán riesgos, los cuales se darán en mayor o menor nivel dependiendo del tipo de información que se maneje y del giro de la empresa.

A continuación se presentan los riesgos técnicos y legales asociados al uso de servicios basado en cómputo en la nube pública.

3.5 Riesgos técnicos

Las ventajas que este nuevo modelo puede aportar a las empresas se pueden ver afectadas al no poner la atención adecuada en los aspectos de seguridad de la información. Cuando las empresas planean adquirir servicios de computación en la nube, es importante que se conozcan, se identifiquen y se evalúen los riesgos técnicos con la finalidad de proteger a sus activos frente a posibles amenazas.

A continuación se enlistan los riesgos técnicos relativos a la computación en la nube, así como una breve descripción.

a) Portabilidad e interoperabilidad de los servicios del cómputo en la nube. El problema se presenta cuando los servicios usan diferentes interfaces y lenguajes de programación. La falta de una estandarización en las interfaces y de procedimientos puede hacer difícil o cara la transferencia de información de un proveedor a otro.

b) Denegación de servicio. Un caso común es la falta de disponibilidad de la información.

c) Pérdida o robo de información. La pérdida de información en las empresas se puede llevar a cabo desde un borrado accidental o fugas internas de la misma, por los usuarios del cómputo en la nube, hasta ser eliminada por un ataque informático, lo que lleva a la mala imagen de la empresa.

Por otro lado, se tiene el riesgo de que el proveedor de servicios al tener un respaldo de la información del cliente no realice el proceso de eliminado de la misma, así como que se quede con una copia de la información.

d) Suplantación de identidad. Normalmente el nombre de usuario y la contraseña son las credenciales utilizadas para el acceso a los sistemas de información, en el cómputo en la nube puede que no sea un mecanismo de identificación robusto al ser internet el medio de acceso a la aplicación.

e) Desconocimiento del perfil del riesgo. En las empresas no se cuenta con un nivel adecuado de experiencia sobre los nuevos modelos o métodos de operar de los usuarios malintencionados.

f) Accesos no autorizados mediante APIS. Los proveedores de servicio ofrecen interfaces de programación de aplicaciones (APIS) al personal de las empresas para tener acceso a los programas o aplicaciones que se encuentran ejecutando en la nube, las cuales son la interfaz para arrancar o parar los servicios o aumentar y disminuir los servicios. Muchas de las veces las APIS se desarrollan sin las medidas de seguridad adecuadas, y siendo éstas las puertas de acceso a los programas y aplicaciones se tiene el riesgo de robo o accesos no autorizados a la información del cliente, así mismo son amenazadas por ataques de malware.

g) Accesos no autorizados por compartir recursos informáticos. El compartir recursos de almacenamiento, memoria, CPU de los servidores es una de las características del cómputo en la nube y

lo cual representa un riesgo en el almacenamiento de la información.

3.6 Riesgos legales

Dado que las leyes no se desarrollan al mismo tiempo que la tecnología, ya que ésta última va creciendo exponencialmente, la aplicación de viejas leyes a nuevas tecnologías genera incertidumbre. Actualmente no hay leyes ni tratados internacionales que regulen el cómputo en la nube, por el momento, los contratos son la respuesta a los vacíos legales, la idea es que sean justos, que no sean unilateralmente redactados, que sean negociados con los usuarios, dependiendo el giro de la empresa. Los SLA´s son los documentos en los que se deben indicar los niveles de servicio con el proveedor, así como mencionar claramente la postura de cada una de las partes.

La mayoría de los riesgos legales se deben por las características propias de cada modelo de despliegue del cómputo en la nube, en específico de la entidad encargada de gestionar la información, en la tabla 3.3 se indica que la gestión de la información y la infraestructura se encuentra en posesión del proveedor de servicios en una nube pública, a diferencia de nube privada e híbrida, por lo cual se ha generado mayor desconfianza entorno a la nube pública.

Tabla 3.3. Características de los modelos de despliegue del cómputo en la nube

Modelo de despliegue	Infraestructura en manos de	Ubicación de la infraestructura	Gestión por parte de	Comparten recursos
Público	Proveedor externo	Externa	Proveedor externo	Uno o varios clientes
Privado	Organización o proveedor externo	Interna o externa	Organización o proveedor externo	Pertenece a un cliente
Híbrido	Ambos	Interna y externa	Ambos	Uno o varios clientes

Los riesgos legales que se tienen actualmente detectados en el cómputo en la nube se enlistan a continuación:

a) Protección de datos personales. Cómo se ha venido mencionando, la flexibilidad para la entrega de servicios, es una de las características principales del cómputo en la nube, lo que podría implicar que el proveedor en cualquier momento decidiera cambiar el lugar donde puede estar tratando y almacenando la información del cliente. Legalmente, al cambiar

de país se cambiaría de jurisdicción. Por ejemplo, si la información está en un servidor Alemán, probablemente estará sujeta a las leyes alemanas, además las autoridades extranjeras podrían no solo auditar, sino eventualmente pedir la información de la empresa para alguna investigación.

b) E-discovery / Regulaciones a aplicar al cambiar los datos de un país a otro. La información en la nube pude ser almacenada en más de un domicilio legal, lo que implica tener que lidiar con diferentes consecuencias legales.

c) Sub – contratantes en la nube. Se tiene el riesgo que al contratar inicialmente servicios de cómputo en la nube con algún proveedor del que se tenga buenas referencias en la entrega de los mismos, éste en un determinado tiempo subcontrate parte del servicio y por lo tanto no se tengan los mismos niveles de seguridad, confidencialidad y servicio.

d) Pérdida de la información. Actualmente no se cuenta con recursos legales que pudieran ayudar a implantar penas por los daños ocasionados frente a la pérdida de información, ya sea por fallas en los dispositivos, por descuido o por no contar con planes de recuperación de información por parte del proveedor.

e) Auditoría. Riesgos en el cumplimiento regulatorio al depender de un tercero para la entrega de evidencia y al no implementar correctamente los controles de seguridad en los sistemas.

Capítulo IV

Empleando Cómputo en la nube

Las empresas que requieran aprovechar los beneficios de rendimiento, de tiempos de respuesta y de ahorros de costos que brinda la adopción del cómputo en la nube, deben empezar enfrentando las preocupaciones que actualmente se tienen: seguridad, administración de la información y cumplimiento normativo. También se debe considerar la creación de estrategias de seguridad durante la implementación del cómputo en la nube, tomando en cuenta el tipo de servicios a contratar, requisitos que se deben solicitar al proveedor y el tipo de nube a utilizar.

4.1 Factores a considerar antes de migrar la información a la nube.

Cuando una empresa está considerando migrar a la nube servicios o procesos de trabajo, se deben considerar factores como: la infraestructura, el diagnóstico de necesidades, la cultura organizacional y la seguridad de la información, esto con la finalidad de que resulte exitosa la migración y aporte el mayor beneficio a la empresa.

Para determinar si la empresa se puede o no beneficiar de las soluciones del cómputo en la nube, a continuación se enlistan algunas actividades previas a la migración a un modelo basado en nube:

a) Tener en cuenta las características actuales de la infraestructura de la empresa.

b) Revisar los objetivos y metas claves para la empresa, es decir, realizar un análisis de las áreas de negocio adecuadas para la migración.

c) Detectar a los usuarios que trabajan remotamente con la finalidad de conocer las necesidades y la forma de adaptación de los usuarios.

d) Tener en cuenta el número de personas que acceden por hora a algún servicio, para determinar si se requiere de un servidor dedicado o un servidor compartido.

e) Considerar si la empresa está sujeta a las distintas normas de cumplimiento que requieren la clasificación de los datos, tales como:

   - BASEL II (Basel Accords)
   - DoD (Department of Defense) Directive 8500.1
   - FISMA (Federal Information Security Management Act)
   - GLB (Gramm-Leach-Bliley)
   - HIPAA (Health Insurance Portability and Accountability Act)
   - PCI DSS (Payment Card Industry Data Security Standard)
   - SOX (Sarbanes-Oxley)

f) Definir el tipo de nube a utilizar. La empresa debe realizar un análisis DAFO (debilidades, amenazas, fortalezas, y oportunidades), con la finalidad de obtener información para la identificación del modelo de nube más apropiado.

g) Elegir al proveedor de prestación de servicios con experiencia y que permita implementar rápidamente el modelo, además de que puedan ser aplicados a las necesidades concretas de la empresa. Se debe buscar un proveedor que se adapte a sus necesidades en cualquier tipo de nube a implementar.

h) Investigar la reputación del proveedor.

i) Realizar una evaluación de los riesgos que se tendrán al implementar un modelo basado en la nube (se pueden tomar en cuenta para su evaluación los riesgos mencionados en el subtema 3.4), estudiando las causas de las posibles amenazas y las consecuencias que éstas puedan provocar. Para esto, se puede ayudar respondiendo preguntas como las siguientes:

- ¿Qué es lo que se va a migrar? Identificar los servicios críticos y aquéllos que no lo son, así como priorizar aquéllos que se adapten de mejor manera a un entorno de procesamiento en la nube.

- ¿Qué servicios debo pasar a la nube? Poner especial atención a la naturaleza y flujo de la información.

- ¿Por qué se va a migrar?

- ¿Cómo se va a migrar?

- ¿Cuánto tiempo tomará migrar y qué problemas puede traer en la entrega de servicios?

j) Desarrollar una estrategia de adopción del cómputo en la nube.

k) Capacitar al personal de las empresas sobre los cambios que implica la migración a la nube.

4.2 Recomendaciones de seguridad

Derivado de la identificación de los riesgos de seguridad en el capítulo anterior, los cuales impactan a las empresas que deseen hacer uso de los servicios basados en cómputo en la nube, se presentan a lo largo de este subtema una serie de acciones recomendadas para minimizar los riesgos asociados desde la implementación hasta la operación , cubriendo temas como autenticación, integridad de los datos, control de acceso, confidencialidad o privacidad de los datos, disponibilidad, exigencias legales, auditoría, entre otras, como se puede

observar en la figura 4.1, lo anterior con la finalidad de tener un servicio de nube confiable.

Figura 4.1 Temas a tomar en cuenta en las recomendaciones de seguridad

Antes de dar a conocer las recomendaciones, es trascendente comentar que una característica común en el cómputo en la nube es la virtualización. La virtualización es la técnica mediante la cual se crea una versión virtual de algunos recursos

computacionales (sistemas operativos, aplicaciones, dispositivos de red y plataformas de hardware) mediante el uso de software, posibilitando que una máquina física contenga una o más maquinas lógicas (máquina virtual), cada máquina virtual tiene asignados recursos como puede ser CPU, memoria, espacio de almacenamiento y conexiones de red.

Como se mencionó, el cómputo en la nube es una forma de entrega de servicios, pagando únicamente por los recursos utilizados, mientras que la virtualización es un posible servicio que puede ser entregado y que provee más servidores haciendo uso del mismo hardware. Para poder implementar servicios basados en nube se requieren sistemas virtuales, es decir, la virtualización es la base del cómputo en la nube, principalmente en el tema de plataforma.

Cabe mencionar que los recursos de hardware físicos con los que cuenta un servidor se comparten al sistema operativo instalado en una máquina virtual mediante hypervisor, ya sea del tipo nativo o host, siendo una nueva inclusión tecnológica, se ve como un nuevo vector de ataque, por lo que es de suma importancia que el hypervisor se encuentre actualizado y con controles de acceso adecuados, esto como medida de seguridad.

Otra de las características del cómputo en la nube es que requiere ser multitenancy o multiusuario, lo cual se puede lograr a través de la virtualización, pues se comparte la infraestructura

o alguna instancia de software que se esté ejecutando en los servidores, sirviendo a varios clientes a la vez.

Las empresas deben asegurar que el proveedor de servicios garantice que los datos estarán aislados entre un cliente y otro y que se lleven a cabo correctamente los procedimientos de cifrado de la información.

A continuación se emite una serie de recomendaciones de seguridad que servirán como referencia a las empresas que deseen contratar servicios de cómputo en la nube con algún proveedor y para que analicen si es prudente hacer uso del modelo o si es mejor prescindir del mismo.

4.2.1 Gestión de la seguridad

Se debe de tomar en cuenta que al utilizar los servicios en la nube se presenta una forma diferente de administración, ya que en este modelo participan tanto el proveedor de servicios en la nube como el cliente. Por lo cual se deben:

- Establecer explícitamente las responsabilidades en el SLA (por sus siglas en inglés Service Level Agreement – Acuerdos de nivel de Servicio), tanto del cliente como del proveedor.

- Implementar por ambas partes (cliente y proveedor) los mecanismos de seguridad para la protección de la

información que se encuentra en la nube, ya que cada parte deberá tomar sus propias responsabilidades.

En la figura 4.2 se muestran a los actores sobre los que recaen responsabilidades de seguridad informática en servicios de tipo IaaS. Algunos proveedores que ofrecen este servicio son: VMWare, Amazon EC2 y Rol Azure.

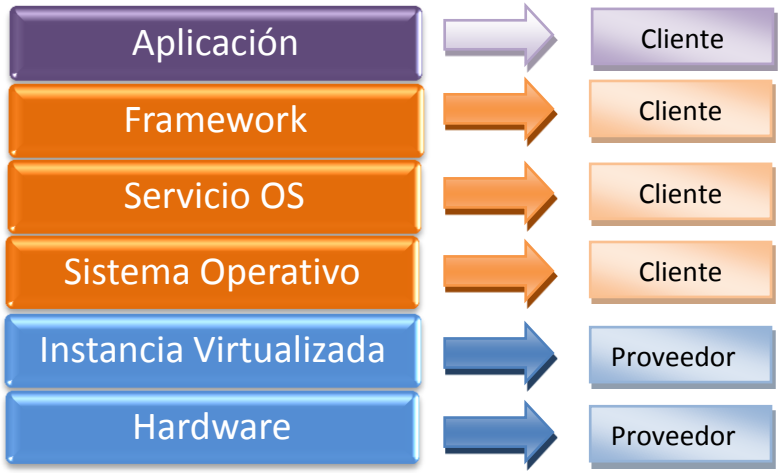

Figura 4.2 Responsables en el servicio IaaS

Si el cliente decide adquirir algún servicio de tipo IaaS, el proveedor se debe encargar de:

- Garantizar la seguridad física en sus sites.
- Cuidar accesos no autorizados a sus sites.

- Mantener actualizados los equipos para evitar que posibles amenazas exploten las vulnerabilidades de los sistemas de información.

El cliente es el responsable de:

- Mantener el sistema operativo actualizado.
- Instalar los parches de seguridad.
- Mantener políticas de seguridad tradicionales como el control de usuarios, el borrado de cuentas de usuarios que ya no se utilicen, etcétera.
- Revisión del software para comprobar que no tiene vulnerabilidades.

En la figura 4.3 se muestran a los actores sobre los que recaen responsabilidades de seguridad informática en servicios de tipo PaaS. Algunos proveedores que ofrecen este servicio son: Windows Azure y Google Appengine.

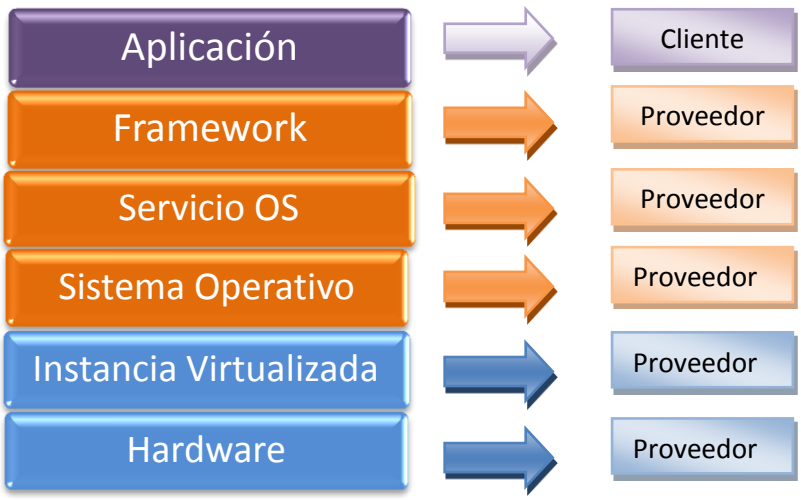

Figura 4.3 Responsables en el servicio PaaS

En la figura 4.4 se muestra a los actores sobre los que recaen responsabilidades de seguridad informática en servicios de tipo SaaS. Algunos proveedores que ofrecen este servicio son: Google Apps y Office 365.

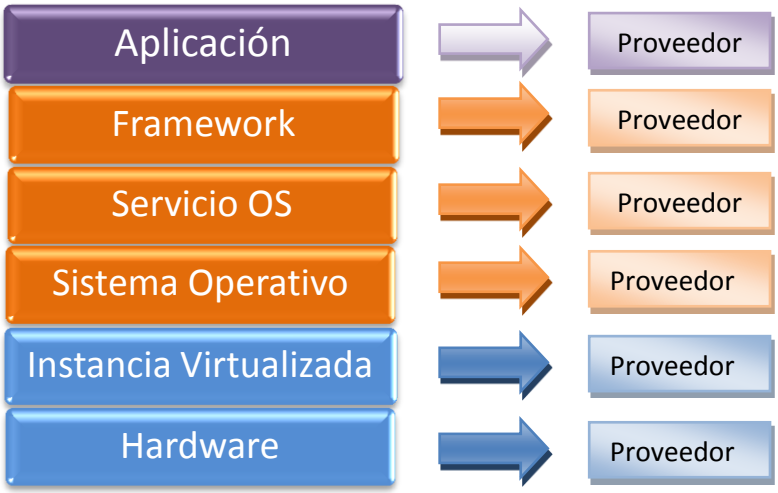

Figura 4.4 Responsables en el servicio SaaS

- Establecer e implementar mecanismos de identificación y autentificación que garanticen que terceros no autorizados puedan acceder a los servicios ofrecidos mediante el cómputo en la nube.

- Realizar supervisiones periódicas del tráfico de red para clientes.

- Analizar los modelos de seguridad en las interfaces o API´s que los usuarios utilizan para gestionar e interactuar con los sistemas. Es importante que estas API´s estén desarrolladas bajo fuertes sistemas de autenticación, de

control de acceso, de monitoreo de uso y de cifrado en la comunicación de datos que viajan a través de Internet.

- Realizar escaneos en busca de vulnerabilidades y auditar las configuraciones.

- Implementar fuerte generación de claves, almacenamiento, gestión y prácticas de destrucción de la información.

- Comprender las políticas de seguridad y utilizar un monitoreo proactivo para detectar actividades no autorizadas.

- Verificar que el proveedor de servicios cuente con herramientas de monitoreo y rendimiento de la aplicación, esto para evitar caídas de servicios, mitigación de riesgos, etc.

- Utilizar SSL/TLS al realizar conexiones de red entre los usuarios y las aplicaciones en la nube. A través del protocolo SSL se establece una conexión Web segura entre el cliente y el proveedor de servicios pudiendo enviar datos a través de un canal seguro y confiable.

- Utilizar para la protección de las conexiones entre los administradores del sistema o desarrolladores de las aplicaciones y servicios en la nube SSH o VPN, con la

finalidad de mantener un canal seguro de comunicación con los sistemas en la nube.

- Tener soporte del proveedor de servicios, para todo tipo de servicios que se utilicen, ya que puede ayudar a corregir problemas y aclarar dudas que se presenten mediante la utilización de los mismos.

- Verificar que el proveedor ofrezca respaldo de los datos ante posibles pérdidas. Lo ideal es que los respaldos se realicen en distintas ubicaciones, previendo redundancia, disponibilidad y garantizando que no haya pérdida de datos ante desastres.

- Solicitar la documentación sobre los controles de seguridad internos y externos al proveedor.

- Solicitar al proveedor la ubicación donde reside la información de la empresa, así como conocer el personal que está administrando los servicios en la nube.

4.2.2 Buen manejo y control de los servicios basados en la nube

Para lograr un buen manejo y control de los servicios basados en nube se debe:

- Evaluar los procedimientos de gestión de riesgos y monitoreo, asegurando tener visibilidad sobre las operaciones de nube.

- Crear una cultura entre el personal de la empresa de la manera de compartir información, así como del uso eficaz de los servicios de la nube, pues el personal debe estar consciente de que se están conectando a Internet, lo que implica cambios en el nivel de acceso así como en las medidas de seguridad.

- Hacer cumplir las políticas, los estándares, procedimientos y los controles de administración, así como establecer responsabilidades de las personas que usan y administran los recursos de tecnología de la información.

4.2.3 Control de acceso

Es de suma importancia controlar el acceso a la información y medios de procesamiento y almacenamiento de la información por lo cual se debe:

- Establecer controles de acceso, asegurando que los usuarios hagan uso de la información o procesos para los que han sido autorizados. Las reglas del control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.

4.2.4 Disponibilidad-Recuperación

Es importante cerciorarse de que la implementación de servicios en la nube tenga métodos de recuperación en caso de alguna falla, por lo cual se deberá:

- Verificar los planes de recuperación de desastres y de continuidad de negocio del proveedor en la nube.

- Asegurar que la implementación de servicios basados en la nube incluya métodos de recuperación, así como que la solución proporcione la escalabilidad y rendimiento necesario (disponibilidad 24x7, seguridad y confidencialidad de los datos).

4.2.5 Integridad

En el ámbito de cómputo en la nube, la integridad de los datos es especialmente crítica, pues lo datos están siendo transferidos constantemente entre los servicios en la nube y los distintos usuarios que acceden a ellos, para lo cual se tienen las siguientes recomendaciones:

- Emplear herramientas de cifrado de datos para los datos que se vayan a almacenar en la nube, de tal manera que si algún usuario no autorizado intercepta los datos, no los pueda leer sin conocer la clave de cifrado, garantizando la integridad de los mismos.

- Llevar a cabo una correcta administración de cambios para contar con el historial de modificaciones de los datos almacenados de la nube, cada modificación debe llevar asociada la fecha y el usuario que solicitó y realizó el cambio.

- Utilizar herramientas en la nube para la programación periódica de copias de seguridad.

- Controlar la integridad mediante procesos que consisten en obtener un valor para la función hash antes de mover el dato y otro cuando se ha terminado de mover. Si otros valores no coinciden es que ha habido un problema en la transacción y debe ser repetida. En el caso del cómputo en la nube no se utilizan funciones resumen solo para ficheros, sino también para máquinas virtuales completas o para las copias de seguridad.

4.2.6 Confidencialidad/Privacidad

En las nubes privadas y públicas se debe controlar el acceso y se debe proteger la información sensible salvaguardando su seguridad y privacidad, por lo que se tienen las siguientes recomendaciones:

- Evaluar la capacidad de los proveedores de servicios de nube en el cumplimiento de estándares legales.

- Garantizar la segregación física de los datos.

- Tener un enfoque de ciclo de vida hacia la administración de los datos.

- Preguntar por el tipo de certificación que posea el proveedor de servicios y conocer el tipo de seguridad que ofrecen los proveedores.

- Realizar el proceso de manera secuencial, es decir, migrar a la nube los datos o procesos considerados como no sensibles. Por ejemplo, se puede instalar un servidor Web o de correo en la nube y el servidor de base de datos mantenerlo de manera local.
  Cuando ya se hayan probado los servicios del cómputo en la nube con información no sensible y el resultado sea exitoso, se puede realizar una migración completa a la nube.

- Mantener una copia completa del modelo tradicional durante un tiempo, pues en caso de que se detecten problemas después de realizar la migración a la nube, se puede volver al modelo tradicional. De esta forma se puede trabajar en la correcta integración de las aplicaciones en el nuevo modelo de forma transparente para los usuarios.

- Realizar un procedimiento de clasificación de la información. La información que una organización procesa debe ser clasificada de acuerdo con la sensibilidad de la misma, ayudando a :

    - Identificar qué información es más sensible o vital, cuál pudiera ser pública, privada o confidencial para la empresa.

    - Identificar mecanismos de protección de acuerdo con el tipo de información.

    - Cumplir con legislaciones o regulaciones.

A continuación el procedimiento que se puede seguir para clasificar la información:

a. Identificar el administrador y custodio de la información.

b. Especificar los criterios de clasificación y etiquetado de la información.

c. Especificar y documentar cualquier excepción a la política de clasificación.

d. Especificar los controles que se aplicarán a cada nivel de clasificación.

e. Especificar los procedimientos de terminación de la desclasificación de la información o para la transferencia de la custodia de la información a otra entidad.

f. Crear un programa de sensibilización de la empresa acerca de los controles de clasificación.

4.2.7 Requisitos y exigencias legales

Se tiene que estar alerta en que los servicios basados en la nube estén regulados por contratos transparentes, con la finalidad de garantizar el funcionamiento adecuado de los servicios adquiridos por las empresas. Es de suma importancia:

- Revisar los requisitos y exigencias legales que se venían cumpliendo en cuanto al manejo y tratamiento de la información e identificar los cambios que se producirán al prestar servicios de cómputo en la nube.

4.2.8 Auditorías

Mediante las auditorías las empresas tienen la capacidad de auditar la actividad del proveedor y/o validar el cumplimiento regulatorio, por lo cual se recomienda:

- Realizar auditorías de seguridad junto con el proveedor con la finalidad de revisar que los sistemas estén protegidos frente a posibles amenazas.

- Revisar los SLA´s, para el caso específico de los SLA en la nube éstos deberán contener:

    - La lista de servicios que proporciona el proveedor y una definición completa de cada servicio.

    - Las métricas para determinar si el proveedor está suministrando los servicios tal como lo prometió y un mecanismo de auditoría para monitorear el servicio.

    - Las responsabilidades del proveedor, el consumidor y los recursos disponibles para ambos si los términos de los SLA no se cumplen.

    - Una descripción de cómo el SLA se modificará a través del tiempo.

En el siguiente subtema se darán a conocer los tipos de auditoría que se pueden incluir en el SLA.

4.3 Cumplimiento regulatorio y auditoría

Hoy por hoy, las empresas se están rigiendo por normas de supervisión con la finalidad de que las direcciones o gerencias pertenecientes a éstas se involucren y tengan visibilidad de las necesidades de gobernabilidad que las empresas deben considerar e implantar, así como identificar cualquier violación a normas o algún proceso interno.

La mayoría de las ocasiones el negocio no visualiza el beneficio que conlleva realizar una inversión en el cumplimiento regulatorio. Algo que se debe tomar en cuenta es que el incumplimiento con el marco regulatorio puede representar un riesgo, teniendo como resultado el pago de multas, así como la pérdida de credibilidad por parte de los clientes en las empresas.

Mediante el cumplimiento regulatorio se contribuye a garantizar la prestación de servicios de alta calidad y el estricto cumplimiento de las normas.

En lo que respecta al cómputo en la nube y de acuerdo con el estudio realizado en el capítulo 3, el cumplimiento regulatorio representa un reto de seguridad muy importante para hacer uso de dicho modelo. Por ejemplo, si el proveedor de servicios de cómputo en la nube no tiene la necesidad de cumplir con alguna normatividad y/o estándar, probablemente los clientes sí lo requieran, en lo cual las empresas deben prestar atención y deben especificarlo en el contrato de servicios o SLA e identificar

aquellas normas aplicables a las empresas, tanto las normas generales obligatorias, como las normas particulares que aplican por aceptar los términos de un contrato o las que se llevan a cabo de manera voluntaria con el objetivo de implementar en las empresas las mejores prácticas.

En la actualidad existen estándares que deseablemente un proveedor de cómputo en la nube debería tener implementados y acreditados, para el establecimiento de relaciones de confianza entre los clientes y los proveedores, pues a través de estos, el cliente puede confiar en que la información y/o servicios transferidos tendrán un nivel de seguridad óptimo.

Los estándares actuales son:

- **ISO 27001:2005.** Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

- **ISO 20000-1: 2011.** Especifica los requisitos de los sistemas de gestión de servicios.

- **ISO 22301:2012.** Es un marco de referencia para gestionar la continuidad del negocio.

- **SAS 70.** Por sus siglas en inglés Statement on Auditing Standards No. 70, es un estándar de auditoría, cuyo reporte consiste en una revisión centralizada por parte de

un auditor independiente de aquellos servicios tercerizados, proveyendo información a las organizaciones usuarias y a sus auditores, acerca del control interno de la organización de servicios.

Existen estándares de la familia ISO 27000 que aún están en fase de borrador, pero las cuáles son específicas para el cómputo en la nube:

- **ISO 27017.** El estándar proporcionará orientación sobre los elementos de seguridad de la información en el cómputo en la nube.

- **ISO 27018.** El estándar proporcionará una guía sobre aspectos de privacidad en nubes públicas.

Se debe preguntar el alcance de las certificaciones, pues se tienen casos en que únicamente se encuentran certificados en solo un servicio.

El cliente deberá vigilar de cerca la confiabilidad, los controles implementados por los proveedores de servicios de cómputo en la nube, posibles violaciones de seguridad y el desempeño en general.

Una de las formas de validación del cumplimiento de las normas es la realización de auditorías por parte de un ente externo a las empresas.

De acuerdo con un estudio realizado por la CSA (Cloud Security Alliance), la auditoría es uno de los factores relevantes a revisar en la contratación de servicios de cómputo en la nube, mediante ésta las empresas tendrán la capacidad de auditar la actividad del proveedor y/o validar el cumplimiento regulatorio.

A continuación se enlistan los tipos de auditorías que se pueden incluir en el contrato de servicios, así como su descripción:

a) Auditoría de cumplimiento normativo. Aquellas relacionadas con los cumplimientos legales.

b) Auditoría de cumplimiento de estándares o buenas prácticas. Se realizan con la finalidad de obtener o mantener alguna certificación.

c) Auditoría de políticas internas del cliente. Algunas empresas generan y cumplen políticas internas, tales como el uso del correo electrónico, las cuales al hacer uso de cómputo en la nube deben seguir y el proveedor debe acatar y responder a las auditorías de personal interno de la empresa.

d) Auditoría sobre puntos establecidos en el contrato. Por medio de este tipo de auditorías se verifica que se estén llevando a cabo los puntos establecidos en el SLA, lo cual ayuda a la confianza de las empresas.

Si bien los puntos anteriores a tomar en cuenta son amplios, cabe mencionar que en el mercado existen o se están desarrollando soluciones para todos los requisitos de confianza, las cuáles podrían ser de gran ayuda para una administración aceptable:

- Herramientas de seguridad para la administración, autenticación y registro completo de claves.

- Herramientas para la medición del rendimiento para acuerdos de nivel de servicio que requieren monitoreo.

- Herramientas de prevención de pérdida de datos que clasifican y restringen automáticamente el acceso a la información.

- Herramientas para verificar el cumplimiento de normas, administración del ciclo de vida de las políticas y los objetivos corporativos y análisis de riesgos.

Las empresas deben prestar atención en los aspectos de seguridad de la información al adquirir servicios de cómputo en la nube, así como en que los mecanismos de seguridad que se puedan aplicar para proteger los datos alojados en la nube se consideren como un trabajo colaborativo entre el proveedor y el cliente.

Conclusiones

En este trabajo de tesis se planteó estudiar el cómputo en la nube en cuanto a la seguridad en el gestionamiento de la información, por lo que fue importante investigar las bases de seguridad informática para identificar los elementos a tomar en cuenta en el aseguramiento de la información y de los recursos en esta nueva forma de entrega de servicios.

El tener un capítulo dedicado a los fundamentos del cómputo en la nube, resulta de gran ayuda, ya que acerca al lector a conocer y entender las características, los modelos de servicios y de despliegue del cómputo en la nube, para posteriormente orientarlo sobre los aspectos de seguridad a considerar en caso de que decidan hacer uso de éste. Cabe señalar que mediante los resultados obtenidos de la encuesta realizada al personal de las empresas dedicadas a las tecnologías de la información se observa que las empresas tienen como foco el uso de cómputo en la nube por diversas razones, por lo que se concluye que todo se irá moviendo hacia esa forma de entrega de servicios cuya adopción será en menos de cinco años. Sin embargo, no hay que obviar sus implicaciones de seguridad, por lo cual la importancia que tuvo la revisión e investigación acerca de los retos, los riesgos, las amenazas y las vulnerabilidades que estarían presentes al hacer uso del cómputo en la nube, tomando en cuenta que a diferencia del modelo tradicional, se basa en la compra de servicios, pago en base a su uso, acceso desde Internet, escalabilidad, dinámico y multiusuario.

Derivado del análisis realizado sobre las implicaciones de seguridad se concluye lo siguiente:

- Con el cómputo en la nube se tiene una nueva forma de usar los recursos de tecnología y gestión de la información, por lo que es sustancial conocer, identificar y evaluar los riesgos.

- Los riesgos se darán en mayor o menor nivel dependiendo del tipo de información que se maneje, así como del giro de la empresa.

- Se tienen amenazas y vulnerabilidades en común con el modelo tradicional.

- El cómputo en la nube es un punto atractivo para los atacantes, por lo que los mecanismos de seguridad que se pueden aplicar para proteger los datos alojados en la nube deben considerarse como un trabajo colaborativo entre el proveedor y el cliente.

- Las empresas deben poner o prestar la atención adecuada en los aspectos de seguridad de la información al adquirir servicios de cómputo en la nube.

- Se debe poner énfasis en los retos de seguridad, para obtener el éxito esperado del nuevo modelo.

Es importante señalar que para la mayor parte de las empresas la seguridad informática se ha convertido en un tema de interés, pues entre otras cosas la relacionan con poseer mayor competividad en el mercado, y para la adopción del cómputo en la nube no está siendo menos, por lo que fue importante definir los factores a tomar en cuenta para migrar la información a la nube. Una vez que realicen la evaluación y análisis de los mismos

sobre su operación, deben poner hincapié en minimizar los riesgos asociados al uso del cómputo en la nube así como seguir las recomendaciones expuestas a lo largo del último capítulo de este trabajo con la finalidad de tener servicios de nube confiable, teniendo siempre en cuenta que:

- La migración debe ser secuencial, se deben migrar a la nube los datos o procesos considerados como no sensibles. Si el resultado es exitoso, se debe continuar con la migración de los servicios críticos.

- Los SLA´s son fundamentales, por lo que se deberá prestar atención y cuidado en los que se estipula en el mismo, se debe orientar de tal manera que se llegue a contar con la confidencialidad, la integridad y la disponibilidad de la información y de los servicios contratados.

- Los proveedores de cómputo en la nube deben generar la suficiente confianza y los clientes deberán confiar en sus proveedores, lo cual se logrará con su historial de efectividad, imagen actual y el correcto funcionamiento de los servicios.

Por otro lado, se tiene que la mayor parte de los encuestados no tienen presente la parte de la estandarización, esto se atribuye a la falta de difusión de la estandarización o normativas que regulen el cómputo en la nube o a la falta de interés en la estandarización, tema de estudio relevante para que los clientes confíen en los servicios de nube a través del cumplimiento.

Mediante la investigación se pudo conocer la existencia de estándares de la familia ISO 27000 que aunque están en desarrollo serán específicos para el cómputo en la nube, pero mientras éstos sean liberados, las empresas pueden solicitar a sus proveedores que cuenten con certificaciones en los estándares ISO 27001, ISO 20000-1, 22301:2012 y SAS 70, asegurando que se cumpla con un nivel de seguridad óptimo.

El cómputo en la nube trae beneficios, pero no se pueden obviar sus implicaciones o riesgos, y se debe tener cuidado con obligaciones legales y regulatorias. A pesar de esto no deberían detenerse las iniciativas en la nube siempre y cuando se tenga identificada la manera adecuada de implementar los servicios. La adopción de nube es un camino no una única implementación y la seguridad debe ser vista como un requisito y de manera integral, recordando que no existe seguridad al 100%.

Referencias

Bibliografía

- Bloor Robin, Halper Fern, Hurwitz Judith, Kaufman Marcia. “Cloud Computing for Dummies”, Wiley Publishing Inc. Ed 2010.

- [1] Gómez Vieites, Álvaro. “Enciclopedia de la seguridad Informática”, Alfaomega. Ed 2007

- Ransome James, Rittinghouse John. ”Cloud Computing: Implementation, Management and Security”, CRC Press, Ed 2010 .

- Quezada Reyes, Cintia. “Apuntes de la materia Seguridad Informática I”, Facultad de Ingeniería - UNAM, 2005.

- Stallings, William. “Network Security Essentials Applications and Standards”, Prentice Hall. Ed 2000.

Referencias Electrónicas (Última revisión: 30-enero-2013)

- *Análisis de riesgos*

ENISA (2009).Cloud Computing Risk Assessment. Disponible en: http://www.enisa.europa.eu/act/rm/files/deliverables/ cloud-computing-risk-assessment.

Gestión de riesgos en ingeniería del software (2006). Disponible en: http://www.um.es/docencia/barzana/IAGP/Iagp5.html

- Cómputo y seguridad/privacidad en la nube

Akamai Technologies (2011). Leveraging Cloud Security to Weather Threatening Storms. Disponible en: http://whitepapers.itespresso.es/wps_content/papers/ leveraging_cloud_z6rgtf6y8cpgv9z.pdf

ACIS (2009). ¿Qué es la computación en la nube?. Revista: SIstemas No. 112 pag 72-80. Disponible en: http://www.acis.org.co/fileadmin/Revista_112/tres.pdf

BMC (2009). Cloud computing en perspectiva. Disponible en: http://documents.bmc.com/products/documents/78/13/107813 /107813.pdf

bSecure (2011). Acuerdos de Niveles de Servicios: factor crítico de éxito en la nube. Disponible en: http://www.bsecure.com.mx/featured/

acuerdos-de-niveles-de-servicios-factor-critico-de-exito-en-la-nube/

bsecure (2011). Explican expertos implicaciones de seguridad de la nube. Disponible en: http://www.bsecure.com.mx/enlinea/cuestionan-expertos-implicaciones-de-seguridad-de-la-nube/

bsecure (2010). The Cloud Reloaded: Seguridad en la nube. Disponible en: http://www.bsecure.com.mx/enlinea/the-cloud-reloaded-seguridad-en-la-nube/

CISCO (2011). Información básica de computación en la nube: Mejora del valor TI. Disponible en: http://www.slideshare.net/ciscolatinoamerica/informacin-bsica-sobre-computacin-en-la-nube-mejora-del-valor-de-ti

Cloud Computing una perspectiva para Colombia (2010). Disponible en: http://www.interactic.com.co/dmdocuments/clud_computing.pdf

Cloud Computing and Data Protection (2009). Disponiible en: http://www.whoswholegal.com/news/features/article/18246/cloud-computing-data-protection/

Cloud Security Alliance (2011). Primer informe sobre Cumplimiento en “la Nube”. Disponible en: http://ismsforum.es/ficheros/SIC96_052-054.pdf

Cloud Security Alliance (2009). Guía para la Seguridad en áreas críticas de atención en Cloud Computing. Disponible en: https://cloudsecurityalliance.org/guidance/csaguide-es.v2.pdf

Cloud Security Alliance (2009). Security Guidance For Critical Áreas Of Focus in Cloud. Disponible en: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Economista digital (2011). La informática 'en la nube' mejorará la competitividad de las pymes. Disponible en: http://www.economiadigital.es/es/notices/2011/07/ la_informatica_en_la_nube_mejorara_la_competitividad_de_las _pymes_21187.php

[4] ENISA (2011). Seguridad y resistencia en las nubes de la administración pública. Disponible en: http://cert.inteco.es/extfrontinteco/img/File/intecocert/ EstudiosInformes/es_governmental_clouds_enisa.pdf

Entendiendo computación en la nube (2011). Disponible en: http://www.avanet.org/ entendiendo-la-computación-en-la-nube-i.aspx

EMC^2 (2010). Creación de una nube confiable: estrategias de implementación para nubes privadas e híbridas. Disponible en: http://mexico.emc.com/collateral/emc-perspective/ h8558-cloud-trust-ep.pdf

Gallardo, S (2010). Diez años después, la seguridad en 2020,

Revista Sistemas. Disponible en:
http://www.acis.org.co/fileadmin/Revista_115/caraysello.pdf

Globe Testing (2011). Seguridad en cloud (III) http://www.globetesting.com/2011/10/seguridad-en-cloud-iii/

IBM (2009). Cloud Security Guidance. Disponible en: http://www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf

IBM (2009). Computación en nube para la empresa: Parte 1: Captura de la nube, Disponible en: http://www.ibm.com/developerworks/ssa/websphere/ techjournal/0904_amrhein/0904_amrhein.html

Guía práctica sobre la seguridad del Cloud Computing (2009). disponible en: http://www.avanade.com/ es-es/approach/research/Pages/A-practical-guide-to-Cloud-Computing-security.aspx

IBM (2010). Security and Cloud Computing. Disponible en: http://www.sit.informatik.tu-darmstadt.de/fileadmin/ user_upload/Group_SIT/Presentations/100302a%20Cloud%20Security%20Lecture.pdf

Informática en la nube: llega la tormenta (2009). Disponible en: http://www.tecnicaindustrial.es/TIFrontal/ a-2739-Informatica-nube--llega-tormenta.aspx

[2] Inteco (2011). Guía para empresas: Seguridad y privacidad del Cloud Computing. Disponible en: http://www.inteco.es/Seguridad/Observatorio/guias/Guia_Cloud

Inteco-cert (2011). Riesgos y amenazas en cloud computing. Disponible en: http://cert.inteco.es/extfrontinteco/img/File/intecocert/ EstudiosInformes/ cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Legitec (2011). Los servicios cloud y la protección de la privacidad: propuesta de “seal” de la UE para empresas de servicios “CLOUD”. Disponible en: http://www.legitec.com/blog/ los-servicios-cloud-y-la-proteccion-de-la-privacidad-propuesta- de-seal-de-la-ue-para-empresas-de-servicios-cloud/

Ponemon Institute y CA Technologies (2011). Estudio: "Security for Cloud Computing Users". Disponible en: http://blog.segu-info.com.ar/2011/06/ estudio-security-for-cloud- computing.html?utm_source=feedburner&utm _medium=feed&utm_campaign=Feed%3A+NoticiasSeguridadInfo rmatica+%28Noticias+de+Seguridad+Inform%C3%A1tica%29#axz z1Uvn47MXG

Ponemon Institute y CA Technologies (2011). Estudio "Security of Cloud Computing Providers". Disponible en: http://www.dataprix.com/empresa/recursos/ estudio-security-cloud-computing-providers-ponemon-institute-

ca-technologies

Ponemon Institute (2011). Security of Cloud Computing Providers Study. Disponible en: http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/security-of-cloud-computing-providers-final-april-2011.pdf

Protocolos efectivos de Compliance para prevenir responsabilidad penal en la empresa (2011). Disponible en: http://www.iberianlawyer.com/a-debate/2476-protocolos-efectivos-de-compliance-para-prevenir-responsabilidad-penal-en-la-empresa

Pymempresario(2011), 26% de las empresas mexicanas usan computación en nube. disponible en: http://www.pymempresario.com/2011/06/26-de-las-empresas-mexicanas-usan-computacion-en-nube/

Qualys, Sin fecha, New Requirements for Security and Compliance Auditing in the Cloud, disponible en: http://www.qualys.com/forms/whitepapers/compliance_auditing_cloud/

RCA Security Inc (2009). La función de la seguridad en cloud computing de confianza. Disponible en: http://www.rsa.com/solutions/business/wp/11021_CLOUD_WP_0209_SP.pdf

Revista seguridad (2010). Privacidad e la Información en la Nube.

Disponible en: http://revista.seguridad.unam.mx/numero-08/privacidad-de-la-informaci%C3%B3n-en-la-nube

Revista Cloud Computing (2011) El 63% de las empresas usa cloud computing, disponible en: http://www.revistacloudcomputing.com/2011/07/el-63-de-las-empresas-usa-cloud-computing/

Revista Sic (2009). De los servicios de SOC a la seguridad en la nube. Disponible en: http://www.revistasic.com/respuestassic/12/ S12_programa.pdf

RSA Security Brief (2010). Infrastructure Security: Getting to the Bottom of Compliance in the Cloud. Disponible en: http://www.vmware.com/files/pdf/cloud/vmware-cloud-solution-security-in-the-cloud-wp-en.pdf

SafeNet (2011). Guía práctica de seguridad en la nube. http://whitepapers.itespresso.es/wps_content/papers/guia_practica_de_la_seguridad_en_la_nube.pdf

Symantec (2009). Cloud Computing Security. Disponible en: http://www.symantec.com/connect/articles/cloud-computing-security

[3] Symantec (2011). Encuesta sobre la virtualización y Evolución hacia la nube. Disponible en: http://www.symantec.com/content/es/mx/enterprise/images/theme/evolution/

symantec-Encuesta-sobre-Virtualizacion-y-Evolucion-hacia-la-Nube-SOLA.pdf

Symantec (2011). Virtualization and Evolution to the Cloud Survey, Disponible en: http://www.symantec.com/content/es/mx/enterprise/images/theme/evolution/ Symantec-2011-Virtualization-and-Evolution-to-Cloud-Survey-Report_ENG.pdf

TechNet Latinoamérica. (2011). Computación en la nube para profesionales de TI (2/6): Qué es la nube http://blogs.technet.com/b/latinoamerica/archive/2011/04/07/computaci-243-n-en-la-nube-para-profesionales-de-ti-2-6-qu-233-es-la-nube.aspx

Verizon (2010). Detrás de la nube: desmitificación de las opciones de informática en la nube. Disponible en: http://www.verizonbusiness.com/resources/whitepapers/wp_detras-de-la-nube-desmitificacion-de-las-opciones-de-informatica-en-la-nube_es_xg.pdf

Vmware (2009) . A Review of Cloud Computing, Security Implications and Best Practices. Disponible en: http://www.vmware.com/files/pdf/cloud/ VMware-Savvis-Cloud-WP-en.pdf

Vmware (2009). Securing the cloud, Review of Cloud Computing, Security Implications and Best Practices: Disponible en:

http://www.vmware.com/files/pdf/cloud/
VMware-Savvis-Cloud-WP-en.pdf

Vmware (2011). Your Cloud. Accelerate IT. Accelerate Your Business. Disponible en: http://vmware.com/files/lasp/pdf/VMW_CorpBrochure_A4_LA.pdf?cf83010D37=65D7BDF4!bmphc3NvZzpjb3JwOpc7jgTl8MzaCTl3uMh0Yvc=

Wikipedia (2013). Cloud computing. Disponible en:
http://en.wikipedia.org/wiki/Cloud_computing#Privacy

- Cumplimiento

Cloud Security Alliance (2011). Cloud Compliance Report de CSA-ES. Disponible en:
https://sites.google.com/a/cloudsecurityalliance.es/csa-s/noticias/publicaciondelprimercloudcompliancereportdecsa-es

RSA Security Brief (2010). Infrastructure Security:
Getting to the Bottom of Compliance in the Cloud. Disponible en:
http://www.vmware.com/files/pdf/cloud/vmware-cloud-solution-security-in-the-cloud-wp-en.pdf

- Definición MAC/DAC

Sistemas de control de acceso: MAC Y DAC (2010), Disponible en:
http://seguinfo.wordpress.com/2010/03/15/sistemas-de-control-de-acceso-mac-y-dac/

- Riesgos y amenazas

Marzo Asesores (2010). Cloud computing riesgos y normativa. Disponible en: http://www.marzoasesores.es/index.php?option=com_content&view=article&id=86:cloud-computing-riesgos-y-normativa&catid=3:articulos&Itemid=27

Revista .seguridad (2010). Todo Depende del Cristal con que se Mire la Nube. Disponible en: http://revista.seguridad.unam.mx/numero-08/perspectivas-todo-depende-del-cristal-con-que-se-mire-la-nube

- Tipos de vulnerabilidades

UNAM. Sin fecha. Tutorial de seguridad informática, capitulo 2: Amenazas y vulnerabilidades http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

- Virtualización

Definición, Tipos e Historia de la Virtualización (2008) http://www.linuxparatodos.net/portal/article.php?story=20081016110607389

Tecnología Pyme (2009). ¿Qué es la virtualización? Disponible en: http://www.tecnologiapyme.com/software/que-es-la-virtualizacion

Anexo A: Cuestionario – Cómputo en la nube

Contesta las siguientes preguntas de manera puntual, en caso de que no conozcas la respuesta, indícalo por favor. El objetivo de este cuestionario es conocer la situación actual del cómputo en la nube en las empresas, únicamente para fines estadísticos.

1. **¿Cuál es el giro de la empresa en la que labora?**

2. **¿Cuál es el puesto que ocupa en la empresa?**

3. **¿Conoce el término cómputo en la nube (cloud computing)? En caso de que su respuesta sea positiva conteste las siguientes preguntas.**

   ☐Sí

   ☐No

4. **¿Cuál es su perspectiva respecto al cómputo en la nube?**

5. **¿En qué plazo de tiempo cree que la empresa adopte soluciones de cómputo en la nube?**

   ☐Ya la estamos adoptando
   ☐En uno o dos años

   ☐En dos a cuatro años

   ☐En más de cuatro años

6. **¿Cuáles son las razones por las que se migraría o se migró la empresa a servicios basados en la nube? Puede marcar más de una opción.**

   ☐Reducción de costos

   ☐Implementación más rápida

   ☐Mejorar el servicio del cliente

   ☐Incrementar la eficiencia

   ☐Incrementar la flexibilidad y capacidad de elegir

   ☐Mejorar la seguridad

   ☐ Cumplimiento normativo

7. **¿Qué obstáculos percibe que las empresas tienen en la adopción de cómputo en la nube? Puede marcar más de una opción.**

   ☐Seguridad y control

   ☐Calidad y rendimiento

   ☐Económico

   ☐Acceso a Internet

   ☐Interoperabilidad e integración

   ¿Por qué?

8. **¿Recomendaría el uso de cómputo en la nube en la empresa en la que trabaja?**

   ☐ Sí
   ☐ No
   ¿Por qué?

9. **¿Cree que el uso de cómputo en la nube genere una mayor competitividad empresarial?**

   ☐ Sí
   ☐ No
   ¿Por qué?

10. **¿Cree que la seguridad informática pueda generar una mayor competitividad empresarial?**

    ☐ Sí
    ☐ No
    ¿Por qué?

11. **¿Qué tan importante es la seguridad para cumplir con objetivos de TI?**

    ☐Muy importante

    ☐Importante

    ☐Nada importante

12. ¿Qué tipo de infraestructura recomendaría, nube pública, nube privada o nube híbrida?

☐Nube pública, ¿Por qué?
☐Nube privada, ¿Por qué?

☐Nube híbrida. ¿Por qué?

13. En caso de ya manejar cómputo en la nube ¿Qué porcentaje de los recursos son destinados a la seguridad en el cómputo en la nube?

☐<5%

☐6 a 10 %

☐11 a 20 %

☐30 %

Otro _____

14. ¿Qué tan segura cree que esté la información almacenada en la nube?

☐Muy segura

☐Segura

☐Nada segura

¿Por qué?

15. ¿Qué riesgos de seguridad considera que tiene una empresa al migrar sus servicios a la nube?

16. ¿De quién cree es la responsabilidad de la seguridad en la nube?

17. ¿Cómo cree que evolucionará el cómputo en la nube en México en los próximos años?

18. ¿Conoce cuáles son los estándares con los que deberían de cumplir los proveedores de servicios en la nube?

☐Sí, ¿Cuáles?
☐ No

Glosario de términos

A

Activo

Son los elementos, tales como: la información, software, hardware, usuarios, infraestructura, que tienen valor para la organización, los cuales son necesarios para el correcto funcionamiento y para alcanzar los objetivos de la misma.

Ataque

Evento exitoso o no, que atenta sobre el buen funcionamiento del sistema informático.

Amenaza

Peligro latente de que ocurra un suceso potencialmente desastroso para los activos, provocando daños.

Arcades

El término “arcade” se refiere a los videojuegos clásicos (Deportivos, Simuladores, de Carreras, de Acción, de Peleas).

APIS

Un API (Application Programming Interface o Interfaz de Programación de Aplicaciones) es un conjunto de funciones o

procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción, facilitando el intercambio de datos entre dos aplicaciones.

C

Confidencialidad

Es una de las medidas de la seguridad de la información, cuya función es la protección de los datos, garantizando que solo aquellos que estén autorizados puedan acceder a la información.

CRM

Un CRM (Customer Relationship Management o Gestión de las Relaciones con los clientes) es una estrategia de negocio centrada en el conocimiento del cliente compuesta por procesos de negocio, personas y tecnología, los cuales se deben tomar en cuenta para llevar a cabo acciones y decisiones basadas en datos, en respuesta y anticipación al comportamiento de los clientes.

Desde el punto de vista tecnológico, son los sistemas y la arquitectura requerida para capturar, analizar y compartir lo necesario en las etapas de la relación de los clientes con la empresa.

Cloud

El término “cloud” o “nube” se utiliza para hacer referencia a la flexibilidad en la entrega de servicios de negocio y tecnología, siendo una metáfora de Internet.

D

Disponibilidad

Es una de las medidas de seguridad de la información, cuya función es asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

E

ERP

Es una de las medidas de seguridad de la información, cuya función es asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Los sistemas de Planificación de Recursos Empresariales (ERP - Enterprise Resource Planning) son sistemas integrales, modulares y adaptables de gestión para la empresa, permitiendo controlar los diferentes procesos de los departamentos interrelacionados

de la empresa, por ejemplo de producción, de logística, de ventas, de inventarios, de contabilidad.

H

Hardware
Conjunto de componentes físicos (eléctricos, electrónicos, electromecánicos, y mecánicos) que conforman una computadora, como son: CPU, memoria RAM, fuente de alimentación, cables, disco duro, entre otros.

I

IaaS

Por sus siglas en inglés Infraestructure as a Service (Infraestructura como servicio). Es un modelo de servicio donde los recursos informáticos como los servidores y el equipamiento de redes son propiedad y están alojados con algún proveedor de servicios. El usuario puede proveerse de los recursos que necesite de forma automática y unilateral mediante una interfaz web, que sirve como una consola de gestión de operaciones de Tecnologías de la información.

Información
Es el conjunto de datos organizados en poder de una entidad que tienen valor para ésta más allá de la forma en que se guarde o

transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etcétera), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Integridad

Es una de las medidas de seguridad de la información, cuya función es asegurar que la información y sus métodos de proceso son exactos y completos.

IEEE

Son las siglas que corresponden a Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos). Es una asociación técnico-profesional e internacional sin fines de lucro dedicada principalmente a la estandarización, se conforma por ingenieros eléctricos, ingenieros en electrónica, ingenieros en sistemas e ingenieros en telecomunicación.

ISACA

Son las siglas que corresponden a Information Systems Audit and Control Association (Asociación de auditoría y Control de Sistemas de Información), es una asociación que provee certificaciones, así como información sobre los sistemas de

aseguramiento de la información, control y seguridad, cumplimiento y riesgos relacionados con la tecnología de la información.

L

Logs

Es un registro de actividad de un sistema durante un rango de tiempo, utilizado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué, ayudando a la identificación de problemas o incidencias de seguridad en algún dispositivo o aplicación.

N

NIST

NIST (Instituto Nacional de Estándares y Tecnología del inglés National Institute of Standards and Technology) es la unidad del Departamento de Comercio de EE.UU, que promueve y mantiene los estándares de medición. También cuenta con programas activos para alentar y ayudar a la industria y a la ciencia al desarrollo y utilización de estas normas.

O

Ofimática

Conjunto de herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

P

Paas

Por sus siglas en inglés Platform as a Service (Plataforma como servicio). Es un modelo de servicio que ofrece lo necesario para el desarrollo e implementación de aplicaciones desde Internet.

PC

Una PC (Personal Computer) es una máquina que recibe, procesa y entrega datos.

PCI

PCI (Payment Card Industry) es un estándar que ayuda a las empresas a proteger o asegurar los datos de los dueños de las tarjetas de crédito o débito, que se procesan, se almacenan o se transmiten, con la finalidad de prevenir fraudes.

R

RFC

Por sus siglas en inglés Request for Comment (Petición de comentarios), son documentos cuyo contenido es una propuesta oficial para un nuevo protocolo de Internet, con explicación detallada y con orientación técnica en la mayoría de los casos.

Riesgo

Probabilidad de que una amenaza se lleve a cabo, utilizando vulnerabilidades existentes de un activo generando pérdidas o daños.

M

Malware

Es la abreviatura de Malicious Software (Software Malicioso), término que engloba cualquier programa o mensaje susceptible a causar daños o causar un mal funcionamiento en los sistemas informáticos y en las redes, por ejemplo, virus, troyanos, gusanos, spyware, etcétera.

Mecanismo de seguridad

Son aquellas herramientas o controles que permiten implementar los servicios de seguridad.

Modelo de seguridad

Es un esquema para especificar y hacer cumplir las políticas de seguridad en un sistema informático.

S

SaaS

Por sus siglas en inglés Software as a Service (Software como Servicio). Es un modelo de servicio en el cual las aplicaciones y los recursos computacionales se han diseñado para ser ofrecidos como servicios de funcionamiento bajo demanda y a través del cual los proveedores entregan el servicio de mantenimiento, operación diaria, y soporte del software usado por el cliente. El software y los datos que maneja se almacenan en los servidores del proveedor que presta el servicio, accediendo a éste mediante un navegador web.

Seguridad de la información

Se define como la preservación de la confidencialidad, disponibilidad e integridad de la información.

Seguridad informática

Cualquier medida que ayude a impedir la ejecución de operaciones no autorizadas sobre un sistema o red informática, que pudieran comprometer la confidencialidad, integridad y disponibilidad de la información.

Servicios de seguridad

Son aquellas funciones de seguridad de la información necesarias y que se tienen que contemplar para minimizar y gestionar los riesgos, recuperar los sistemas y limitar pérdidas en caso de un incidente, entre otros.

Sistema informático

Es la unión de diversos elementos (hardware, software, soporte humano) que funcionan relacionándose entre sí con un objetivo preciso.

SLA´s

Un SLA (Service-Level Agreement) es un contrato escrito entre un proveedor de servicio y su cliente que especifica el nivel de calidad en la entrega de servicios.

Software

Conjunto de programas, instrucciones o reglas necesarios para la ejecución de tareas específicas en una computadora, que a diferencia del hardware es intangible, por ejemplo los procesadores de texto, el sistema operativo, editores de imágenes, entre otros.

V

Vulnerabilidad

Debilidad interna de un sistema que origina la exposición de éste a las amenazas existentes, las cuales pueden ser explotadas (aprovechadas) por un atacante para violar la seguridad.

W

Wi-fi

Es una abreviación del término inglés Wireless Fidelity o "Fidelidad inalámbrica", esta tecnología permite conectarse a una red de forma inalámbrica, sus características están especificadas por el estándar internacional IEEE 802.11 (ISO/IEC 8802-11)

3G

Es la abreviación de tercera generación de transmisión de voz (llamadas telefónicas) y datos (mensajería instantánea, intercambio de correos electrónicos) a través de telefonía móvil mediante el servicio universal de telecomunicaciones móviles.