FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

PROPUESTA TÉCNICA DE SEGURIDAD PARA EMPRESAS QUE ESTAN ADOPTANDO SERVICIOS EN LA NUBE

SUSTENTADO POR:

GERSON ZABDI FLORES MALDONADO

JORGE EDUARDO HERNÁNDEZ MARTÍNEZ

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN GESTIÓN DE LAS TECNOLOGIAS DE LA INFORMACIÓN

TEGUCIGALPA, FCO. MORÁZAN, HONDURAS, C.A.

SEPTIEMBRE 2014

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR
LUIS ORLANDO ZELAYA MEDRANO

SECRETARIO GENERAL
JOSÉ LÉSTER LÓPEZ

VICERRECTOR ACADÉMICO
MARLON BREVÉ REYES

VICERRECTORA CAMPUS SPS
ANA LOURDES LAFFITE

DECANO DE LA FACULTAD DE POSTGRADO
DESIREE TEJADA

PROPUESTA TÉCNICA DE SEGURIDAD PARA EMPRESAS QUE ESTAN ADOPTANDO SERVICIOS EN LA NUBE

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE LAS TECNOLOGIAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JORGE AMADOR

ASESOR TEMÁTICO

FRANCISCO MANUEL ZELAYA

MIEMBROS DE LA TERNA

CARLOS PÉREZ

DIANA CÁRCAMO

ADALBERTO MÉNDEZ

AGRADECIMIENTOS

Agradecemos a Dios por bendecirnos día a día con su gran misericordia y proporcionarnos su amor incondicional.

A nuestras familias que siempre nos brindan su amor y cariño incondicional y nos apoyaron en este largo proceso y han sido nuestra roca fuerte en los momento más difíciles de este gran reto.

A nuestros incansables amigos, que nos han apoyado siempre con su compresión por nuestras faltas en las reuniones y porque nos han enseñado que los verdaderos amigos siempre están en las buenas y las malas.

FACULTAD DE POSTGRADO

PROPUESTA TÉCNICA DE SEGURIDAD PARA EMPRESAS QUE ESTAN ADOPTANDO SERVICIOS DE SEGURIDAD EN LA NUBE

AUTORES:

Gerson Flores Maldonado

Jorge Eduardo Hernández Martínez

RESUMEN EJECUTIVO

Este trabajo pretende demostrar el problema de seguridad de la información que enfrentan las empresas que utilizan servicios en la nube, así como también la incertidumbre que se presenta al momento de enumerar sus riesgos en una arquitectura en la nube de tipo pública.

El alcance de la investigación es meramente descriptivo con un enfoque cuantitativo, de tipo no experimental, transeccional ya que no se intervendrá directamente en las variables de investigación. Después de haber realizado la encuesta a varios usuarios de servicios en la nube se descubrió que la no adquisición de este tipo de servicios se debe a la poca información sobre este tema, si bien es cierto los clientes tienen conocimientos generales de servicios en la nube, no cuentan con información útil y real al respecto sino que la mayor parte de la información obtenida es dada por el proveedor. Es por ello que este trabajo presenta una propuesta de estrategia de seguridad para cualquier empresa que desee adquirir este tipo de servicio en la nube.

La propuesta muestra un formulario que debe ser llenado por el usuario y de acuerdo a la respuesta del mismo se podrá conocer los requerimientos mínimos necesarios. **Palabras clave:** Propuesta Técnica, Seguridad de la información, Computación en la nube, Nube pública, Seguridad en la nube,

GRADUATE SCHOOL

PROPUESTA TÉCNICA DE SEGURIDAD PARA EMPRESAS QUE ESTAN ADOPTANDO SERVICIOS DE SEGURIDAD EN LA NUBE

AUTHORS:

Gerson Flores Maldonado

Jorge Eduardo Hernández Martínez

ABSTRACT

This work aims to demonstrate the problem of information security that companies using cloud services experiments, as well as the uncertainty that occurs when listing your risks in a public cloud architecture.

The research conducted in this study is descriptive and not experimental, using a quantitative method as no variables were manipulated and the study reflects the results of a specific range of time. After having surveyed a significant portion of users cloud services the study shows that the lack of demand for these types of services can be explained by a lack of information provided to the customer, but most of the information obtained is given by the supplier. That is why this paper presents a proposal for security strategy for any company wanting to purchase this type of cloud service.

The proposal shows a form that must be filled by the user according to the response of the same will be required to meet the minimum requirements.

Keywords: Technical proposal, Information Security, Cloud Computing, Public Cloud and Cloud Security.

ÍNDICE

CAPITULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

Una frase común hoy en día en las organizaciones es: “el activo más valioso de los negocios es la información”, por lo que la necesidad de mantenerlo seguro es vital para las empresas.

La conceptualización de la computación en la nube actualmente es sinónimo de movilidad, accesibilidad, disponibilidad y control. La computación en la nube no es un concepto nuevo en estos tiempos, la disponibilidad de soluciones, emparejado con las presiones económicas para recortar presupuestos, ha motivado a muchas compañías a tomar más en serio una potencial migración de algunos de sus servicios informáticos a la nube.

La integración de la computación en la nube y la seguridad debe ser absoluta, por lo que se presentarán varios aspectos importantes a considerar en este documento. La seguridad de la información es un campo bastante dinámico, se rige por muchas variantes como ser la legislación sobre el manejo de esta información, la evolución de las tecnologías y la creciente comunidad de atacantes con propósitos lucrativos que cada vez es más sofisticada. Las empresas necesitan ser más creativas para implementar prácticas de seguridad, combinando tecnología con métricas, plantillas de manejo de riesgos y políticas internas.

En el capítulo uno, se define el problema central de estudio, destacando cuáles son sus antecedentes, se define el objetivo general y los objetivos específicos, se expone la relevancia y la necesidad de llevar a cabo esta investigación, así como su aplicabilidad práctica y metodológica.

En el capítulo dos se presenta el marco teórico, el cual muestra el porqué de la necesidad de las empresas de manejar sus datos mediante sistemas de información, el surgimiento de conceptos innovadores como la virtualización y cómo esto da lugar a la creación de la

computación en la nube, enfocándonos finalmente en el resguardo y seguridad de la información utilizada en estos servicios.

El capítulo número tres detalla la estrategia que se llevara a cabo en dicha investigación, el enfoque y método, las técnicas y las herramientas que se utilizaron para fundamentar las variables a verificar, obtener la información necesaria y contestar los objetivos del estudio.

El resultado obtenido de dicha investigación servirá como guía de lineamientos recomendados de seguridad a las empresas que decidan migrar sus servicios de TI en la nube.

1.2 ANTECEDENTES

1.2.1 SERVICIOS DE SEGURIDAD EN LA NUBE ACTUALMENTE

Se ha analizado la realidad actual de servicios en la nube que ofrece una prestigiosa empresa proveedora de servicios de internet y seguridad en Honduras, a continuación se presenta un resumen de los servicios de infraestructura y seguridad en la nube que ofrecen.

1.2.2 INFRAESTRUCTURA COMO SERVICIO (IAAS).

Esta solución provee servidores estándar, almacenamiento, equipo de red y capacidades de software consumibles bajo demanda y en escala. El modelo de IaaS libera recursos de TI que normalmente se usarían para albergar, ejecutar y mantener equipo y software.

Dentro de los servicios de Infraestructura como servicio (IaaS) que ofrece esta empresa ISP (Internet Service Provider) podemos mencionar los más relevantes como ser:

Servicios de Red:

- Switches
- Balanceo de Carga
- Firewall
- IPS

Infraestructura de Servidores:

- Windows
- Linux
- Unix
- ESX

Infraestructura de Almacenamiento y Respaldo:

- NAS (Network Attached Storage)
- SAN (Storage Area Network)
- Respaldo en la nube

Infraestructura de Monitoreo:

- Monitoreo de Hardware
- Monitoreo de Sistemas Operativos

Aplicaciones de Software:

- Base de Datos.
- Correo Electrónico.
- Aplicaciones de Office.
- Aplicaciones de Negocio (ERP, CRM, etc)

Infraestructura de escritorio en la nube:

- Virtualización de Servidores de Escritorio en arquitectura Windows Server.

Virtualización de Servidores de Escritorio en la arquitectura de preferencia del cliente (Flex).

1.2.3 SEGURIDAD COMO SERVICIO EN LA NUBE:

Ellos ofrecen servicios de seguridad perimetrales y de red interna que cubren riesgos como ser:

Perimetrales

- VPNs a través de Internet.
- Servidores públicos.
- Correo Electrónico.
- Firewall Administrable

Internos

- Usuario final.
- Sitios Alternos (DRS).
- Servidores críticos y no críticos.

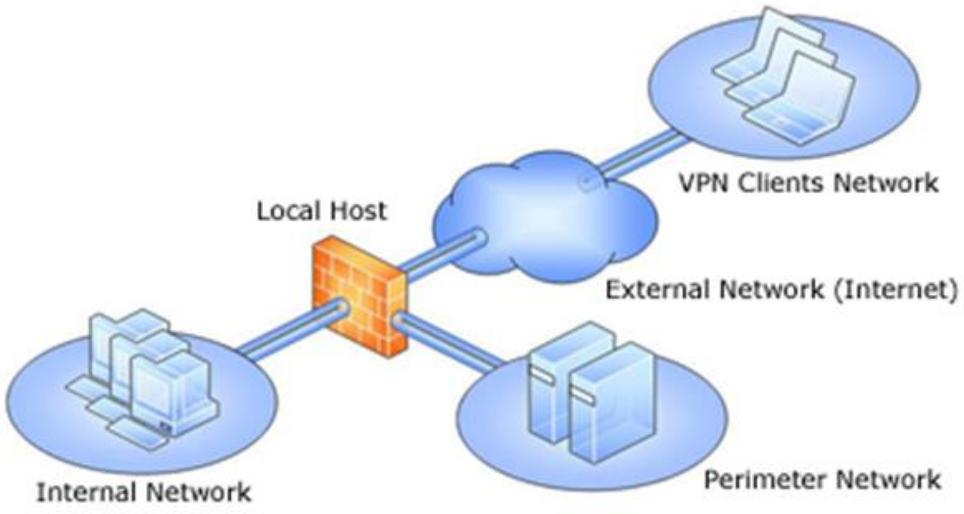

Figura 1. Esquema de red convencional que muestra una red interna, red perimetral y red externa.

1.3 DEFINICIÓN DEL PROBLEMA

En esta sección se presenta el problema de seguridad de la información que enfrentan las empresas que utilizan servicios en la nube, así como también en la incertidumbre que se presenta al momento de enumerar sus riesgos en una arquitectura en la nube de tipo pública.

Actualmente las empresas manejan grandes flujos de información prioritaria y confidencial, usando servicios en la nube, pero no presta las condiciones de seguridad necesarias para este tipo de ambiente por lo que se hace necesario poder tener estándares establecidos que orienten a las organizaciones hondureñas de que es lo más recomendable para ellas

1.3.1 ENUNCIADO DEL PROBLEMA

Las empresas que emprenden el camino hacia una arquitectura en la nube, lo hacen para satisfacer una necesidad específica, como ser movilidad, accesibilidad a sus datos, flexibilidad en sus aplicaciones o solamente buscan simplificar la administración y mantenimiento de sus infraestructuras tecnológicas, sin embargo, aparte de las facilidades que este servicio provee, también vienen acompañadas de riesgos de seguridad para la información que se maneja en estos servicios, existen amenazas latentes que necesitan ser controladas por lo tanto se deben tomar medidas preventivas para la mitigación de estas amenazas y riesgos. Por lo tanto, los clientes de servicios en la nube necesitan que se les garantice que los proveedores aplican prácticas adecuadas de seguridad para mitigar los riesgos que enfrentan ambas partes (tanto el cliente, como el proveedor).

Los clientes en nube no son conscientes de los riesgos que podrían afrontar al migrar hacia la nube, en particular aquellos riesgos generados a partir de amenazas específicas de la nube, es decir, pérdida de control, cierre de la empresa proveedora, agotamiento de recursos del proveedor en nube, etc. Esta falta de conciencia también podría afectar

al proveedor en nube, que puede no ser consciente de las medidas que debería tomar para mitigar estos riesgos. (ENISA, 2009)

La experiencia que nos ha dejado nuestro trabajo día a día es que las amenazas vienen en aumento a medida que pasa el tiempo, la motivación de los generadores de ataques en contra de la seguridad de nuestra información ha aumentado al ver una oportunidad de lucro detrás de la importancia y el valor que esta información representa.

1.3.2 FORMULACION DEL PROBLEMA DE INVESTIGACIÓN

El problema de la investigación es la constante amenaza de seguridad informática que pone en riesgo la valiosa información de empresas que manejan sus servicios, infraestructura o aplicaciones en la nube, teniendo como consecuencia, la pérdida parcial o total de sus datos debido a fallas internas o a debilidades en la seguridad de los sistemas de información. La mala elección de una estrategia adecuada de seguridad para una arquitectura en la nube específica puede tener un impacto relevante en la continuación de un negocio, un problema secundario sería también el desconocimiento de los riesgos de seguridad para la información que una arquitectura en la nube de tipo pública puede conllevar.

1.4 OBJETIVOS

En esta sección se presentan los objetivos que mostraran el rumbo de dicho proyecto de investigación.

1.4.1 GENERAL:

Determinar una estrategia integrada de seguridad para una arquitectura de servicios en la nube pública según los estándares actuales de los fabricantes líderes en seguridad.

1.4.2 ESPECÍFICOS:

- Describir estándares de estrategias de seguridad de empresas líderes para servicios en la nube pública.
- Identificar estrategias de seguridad para nubes públicas utilizadas actualmente por empresas ubicadas en la ciudad de Tegucigalpa
- Evaluar las estrategias de seguridad para nubes públicas en uso actualmente por las empresas nacionales según la determinación de los estándares de empresas líderes.
- Construir estrategias integradas de seguridad para nubes públicas basadas en la evaluación aplicada a las estrategias de seguridad.

1.5 JUSTIFICACIÓN

Los beneficios de uso de tecnologías como la computación en la nube nos brindan facilidades en la agilidad y flexibilidad de acceder a nuestra información desde cualquier parte, estas facilidades se empiezan a convertir en una necesidad con la nueva y amplia visión de los negocios actualmente, y se considera la seguridad de esta información como un pilar fundamental del éxito de esta tendencia tecnológica como es la computación en la nube.

El contar con una sólida estrategia de seguridad de información puede traerle beneficios directos a un negocio, como ser el uso de la seguridad como elemento diferenciador del mercado, ya que esta constituye una prioridad para muchos clientes, una ágil e inteligente escalabilidad de recursos, alta capacidad de reasignación dinámica de recursos, auditoría y recogida de pruebas en tiempo real con reducción considerable de tiempo para realizar inspecciones minuciosas forenses, actualizaciones puntuales, efectivas y eficaces, concentración de recursos.

CAPITULO II. MARCO TÉORICO

En este apartado se analizan las bases teóricas de la investigación, comenzando con la descripción del concepto de computación en la nube, además se ahonda en el tema de la búsqueda de seguridad de la información que es el origen y antecedente del objeto de estudio.

La computación en la nube o servicios en la nube, es un concepto que aunque relativamente nuevo, sobre todo en el mercado de América Latina, ha sido producto de las innovaciones y cambios de paradigmas que se han dado en las tecnologías de la información, y que han respondido a una necesidad de las organizaciones. Esta necesidad ha sido impulsada por un mercado globalizado, cada vez más competitivo, que requiere que una empresa pueda utilizar sus recursos de manera más eficiente.

Para eficientar los recursos las empresas deben ser capaces de manejar, administrar, y analizar la información que hace posible sus operaciones de forma rápida y confiable. Las organizaciones deben poder recolectar esta información que se origina en diferentes áreas y niveles de la empresa, y como sucede en muchos casos, en diferentes ubicaciones geográficas (ya sea nacional o internacionalmente), para luego procesarla y de ella no solamente sacar datos operativos o contables, sino algo que les permita planificar, evaluar si una estrategia está dando los resultados esperados, proyectar resultados, tomar decisiones que tendrán resultados a mediano o largo plazo, etc.

Tratar de lograr esto sin un sistema de información que pueda automatizar transacciones, almacenar grandes cantidades de información, generar reportes de forma oportuna, para una empresa mediana o grande sería muy difícil. La información sería volátil y poco confiable.

Los sistemas de información a su vez vienen acompañados de una infraestructura, en la que participan los dispositivos de usuario final como computadoras personales, y los dispositivos móviles como teléfonos y tabletas, que en los últimos años se han vuelto indispensables para muchos. Las comunicaciones también forman parte esencial en el desarrollo de estos sistemas, permitiendo la distribución de la información en redes

privadas o públicas. A su vez esta información y los servicios que permitan manipularla y visualizarla deben estar almacenados en otros medios físicos que también necesitan de administración y mantenimiento ya sea por la misma empresa o por otros proveedores. Estos dispositivos deben estar en ubicaciones que aseguren su seguridad y disponibilidad, esto es lo que se conoce como centros de datos.

La infraestructura de las tecnologías de información tiene un costo para las empresas que los utilizan, tanto en compra de equipo, en mantenimiento de centros de datos, en seguridad para resguardar los datos y en tener personal capacitado para manejarlos. Las empresas han tratado de reducir este gasto ya sea subcontratando para ahorrar en personal o virtualizando para minimizar equipos, pero sea la decisión que se tome siempre se debe tener control de la seguridad de la información resguarda en los equipos.

A continuación se profundizará en estos temas y veremos como la computación en la nube es un intento más por tener sistemas de información y aplicaciones más potentes a menor costo.

2.1 MARCO CONCEPTUAL

Para que el lector pueda comprender mejor la teoría presentada en este capítulo se incluyen ciertas definiciones de palabras técnicas que son necesarias para poder fundamentar y comprender del tema de este estudio.

1. Servidor: Es el hardware donde reside una aplicación y que es utilizado por uno o más usuarios a través de la red.
2. Tarjeta de red (NIC): es una clase de tarjeta destinada a ser introducida en la placa madre de una computadora o se conecta a uno de sus puertos para posibilitar que la máquina se sume a una red y pueda compartir sus recursos.
3. Inversor: Es un dispositivo que convierte corriente DC a AC.

4. Hub: Dispositivo de comunicación de capa 1 que consta de varios puertos a través de los cuales se repite la una señal transmitida por cualquiera los aparatos conectados a él. Todos los puertos del hub se encuentran en el mismo dominio de colisión.

5. Switch: Dispositivo de comunicación de capa 2 que consta de varios puertos cada uno representando un dominio de colisión separado. A diferencia del hub la trama transmitida no se replica a todos los puertos con la excepción de un broadcast.

6. Router: Dispositivo de comunicación que enruta paquetes entre dominios de broadcast distintos.

7. Broadcast: una trama que es replicada a través de todos los puertos de un switch.

8. Firewall: Aparato que filtra paquetes basándose en reglas y criterios como dirección o puerto de origen y destino.

9. Colisiones: Choque de tramas que ocurre cuando dos o más equipos tratan de transmitir datos al mismo tiempo.

10. Rack: Gabinete de 2 o tres postes, de altura y anchura variable que se utiliza para alojar equipos de la red como servidores, switches, routers, plantas telefónicas, etc...

11. UTP: Cable de cobre de par trenzado. Es una clase de cable que no se encuentra blindado y que suele emplearse en las telecomunicaciones.

12. Estación de trabajo: Computadora personal de escritorio.

13. Terminal tonta: Computadora que consta de monitor, teclado y tarjeta de red y es utilizada para acceder a los recursos del servidor al cual está conectada.

14. RDP: Protocolo de Windows que permite acceder a la interface gráfica (desktop) de una computadora o servidor remoto.

15. Active Directory: Aplicación utilizada en redes Windows donde se registran los usuarios y equipos que tienen acceso a recursos de la red. Es encargado también de distribuir las políticas de grupo para los ambientes basados en Windows.

16. Ethernet: Estándar con protocolos de capa 1 y 2 utilizados en la implementación de una red de área local.

17. Linux: Sistema operativo basado en Unix, que es distribuido bajo el esquema de licenciamiento GPL (Licencia pública general).

18. Windows: Sistema operativo desarrollado por Microsoft.

19. Fibra canal: Estándar para de red para conectar equipos en una SAN.

20. SAN: Storage Area Network, es una red de equipos utilizados para almacenamiento de datos.

21. UNIX: Sistema operativo que se utiliza en servidores o Mainframes. Las versiones de Unix son propietarias como por ejemplo: Unix de Hp es HP-UX, de IBM es AIX, de Sun es Solaris.

22. VNC: Aplicación que permite gestionar remotamente una computadora o servidor vía su interface gráfica.

23. Hypervisor: Software o Hardware que se utiliza para ejecutar y gestionar máquinas virtuales.

2.2 NECESIDAD DE LOS SISTEMAS DE INFORMACIÓN

El manejo de la información siempre ha sido uno de los grandes retos para las organizaciones. La complejidad de esto varía de acuerdo a un determinado grupo de variables como lo son:

- El tipo de información a manejar.
- La cantidad de dicha información.

- Que tan accesible debe ser para las personas o áreas que la requieren.
- Si es información procesada en línea o por lotes.
- La confidencialidad con que debe será manejada.

En general la administración de la información ha dejado de ser un lujo para la mayoría de las empresas y ha pasado a considerarse como uno de los activos más valiosos de la misma. “Hay una creciente interdependencia entre la capacidad de una empresa para utilizar tecnología de información y su capacidad para implementar estrategias corporativas y lograr metas corporativas.” (Laudon & Laudon, 2008) Por este motivo es difícil que una organización ya sea pequeña, mediana o grande pueda ser capaz de ignorar la importancia de su gestión correcta.

Una empresa siendo en si un conjunto de actividades que tienen como fin el logro de objetivos ya sea de carácter económico o social, requiere con más frecuencia poder procesar los datos que resultan o son requeridos por las mismas. Estas actividades van desde las administrativas a las operativas, cada una con necesidades específicas de información. Entre ellas podemos enumerar como algunas de las más comunes:

- Contabilidad
- Facturación
- Ventas
- Compras
- Mercadeo
- Recursos Humanos

Para procesar los datos recolectados por los diferentes actividades que se llevan a cabo dentro de la organización es necesario una herramienta que permita agruparlos, analizarlos, relacionarlos entre sí, en fin darles un valor más allá del que puedan tener por si solos. Aquí es donde entran los sistemas de información. Estos pueden ser definidos como “un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen, información para apoyar la toma de decisiones y el control en una organización.” (Laudon & Laudon, 2008)

Cabe mencionar que es muy poco probable que una empresa logre competir al mismo nivel con las demás (sobre todo en un mundo globalizado) si su información todavía es manejada manualmente. En los últimos años la tecnología de la información se ha vuelto más accesible, sobre todo en lo que concierne a las computadoras personales, y otros dispositivos como las tabletas y los teléfonos inteligentes. Por lo tanto los sistemas de información para las empresas medianas y grandes necesariamente tienen que ser desarrolladas sobre una plataforma tecnológica.

Los sistemas de información como su definición lo dice involucran la interrelación de varios componentes, estos van desde componentes físicos (hardware) como lo son las computadoras personales, servidores, equipo de la red, hasta los no físicos (software) que pueden ser aplicaciones con las que interactúan los usuarios (ya sean clientes instalados en sus equipos o aplicaciones web), bases de datos, etc…

Según Daft, Richard L. (2007) entre los tipos de sistemas de información que podemos enumerar están:

1. Sistemas de Procesamiento de Transacciones (SPT): “Automatizan la rutina de la organización y las transacciones cotidianas de un negocio” (Daft, 2007). Estos sistemas son utilizados a nivel operativo y son la entrada de información que luego será utilizada por otros sistemas en la toma de decisiones. Aquí podríamos incluir un sistema de reservación de boletos aéreos, o el sistema en el que son ingresadas las ordenes en un restaurante.

2. Sistemas para la toma de Decisiones Organizacionales.

   Estos sistemas se subdividen en los siguientes:

   - Sistemas de información para la administración (SIA): Estos utilizan la información obtenida de los sistemas de procesamiento de transacciones para “mantener o alterar patrones en las actividades organizacionales” (Daft, 2007). Estos son utilizados por los mandos medios dentro de la organización.

- Sistemas de información Ejecutiva(SIE): Estos sistemas tienen como principal objetivo, sintetizar grandes cantidades de información que vienen los niveles inferiores para poder mostrar a los altos mandos de la organización la información de una forma más sencilla y “de una manera oportuna” (Daft, 2007).
- Sistemas de Apoyo a la Toma de Decisiones (SAD) Estos son utilizados para poder modelar alguna situación específica que pueda darse en los procesos de la organización. Por medio de manipular variables se puede evaluar el impacto un cambio propuesto. Los SAD “dependen de modelos de decisión y de bases de datos integradas” (Daft, 2007).

3. Sistemas para el Control Administrativo

“Las mediciones del desempeño fijan el rumbo y motivan a los administradores” (Horngren T., Sundem, & Stratton, 2006).

Basados en ciertos parámetros de medición o índices de lo que es aceptable o no como resultado de una actividad de la empresa, estos sistemas proporcionan una forma de determinar si se están logrando o no los objetivos que la organización se ha propuesto. Dentro de estos sistemas podemos incluir los Cuadros de Mando Integral, los Balance Score Cards y los Dashboards (Tableros de Mando). Muchas empresas dependen de sistemas de control para saber si sus servicios están operando de forma adecuada e incluso en tiempo real. Como ejemplo: Una empresa de telecomunicaciones necesita llevar un control de forma real sobre la disponibilidad de sus servicios, ya que una caída representa pérdidas en dinero y satisfacción de los clientes.

Como ejemplos de algunos de estos sistemas utilizados en las organizaciones podemos mencionar:

1. Sistemas ERP (Enterprise Resource Planning): Sistemas de información que buscan resolver el problema de las islas de información. Los ERP están compuestos por módulos que engloban varias de las áreas de la empresa como

son Ventas, Contabilidad, Activos Fijos, Recursos Humanos. Lo que se busca con ellos es agrupar las actividades principales de la empresa ya que la información procesada por cada una de ellas alimenta las demás. Los ERP siendo un tanto costosos se venden usualmente por módulos comenzado con lo básico y escalando a medida que se dé la necesidad.
Ejemplos de estos sistemas son el SAP, Great Plains.

2. Los sistemas CRM: Son aquellos orientados a llevar la gestión de clientes de una organización. Esta información es importante para las áreas de Venta, Mercadeo y atención al cliente. En ellos se lleva un registro de los servicios o productos ofrecidos y brindados a los distintos clientes, así como las oportunidades de nuevos negocios. También ayudan a darle seguimiento a los problemas que hayan tenido con estos productos o servicios. Algunos ejemplos de estos son el SugarCrm, el Tiger, Oracle.

3. Los Service Desks, Helpdesks: Permiten almacenar, categorizar y dar seguimiento a solicitudes hechas por un cliente ya sea para soporte de un servicio o producto o para consultas sobre el estado de un pedido. Los Service Desks permiten la creación de una base de datos de conocimiento (Knowledge Base) la cual puede ser utilizada para resolver problemas que se dan con frecuencia sin necesidad de volver a hacer una investigación sobre su causa.

Los sistemas de información son usualmente complementados por otros servicios, como por ejemplo, los servicios de correo electrónico y mensajería instantánea. El correo se ha vuelto la forma estándar de comunicación entre los empleados de una empresa y por cuestiones de seguridad o privacidad muchas empresas optan por tener sus propios servidores de correo o de mensajería instantánea.

Además de esto están las aplicaciones ofimáticas como lo son las hojas de cálculo, procesadores de palabras o herramientas de diseño como lo son el Visio o el AutoCAD, que son utilizadas por los diferentes departamentos en sus operaciones diarias y que

pueden ser utilizadas para manipular la información extraída de los sistemas de información.

Los sistemas de información y demás aplicaciones complementarias necesitan de una infraestructura que asegure su disponibilidad a los usuarios. A continuación se mostrará cómo se han ido desarrollando nuevas formas de brindar estos servicios.

Para que los usuarios puedan tener acceso a los sistemas de información dentro de una empresa, es necesario contar con una infraestructura de Tecnologías de Información (IT) adecuada a la necesidad de cada empresa.

Según Laudon & Laudon(2008) la estructura IT dentro de las empresas ha pasado por varios cambios a través de la historia. Estos son:

1. Maquina Electrónica de Contabilidad (1930-1950)
2. Mainframe/Minicomputadora(1959- a la fecha)
3. Computadora Personal (1981 – a la fecha)
4. Cliente-Servidor (1983- a la fecha)
5. Internet Empresarial(1992-a la fecha)

Cabe agregar a este listado el auge que han tenido en los últimos años los dispositivos móviles como son las tabletas y los teléfonos inteligentes (Smartphones) que han pasado a ser para muchas personas una extensión de sus computadoras de escritorio o laptops (en algunos casos un substituto para ellas), permitiéndoles estar conectados a los sistemas de sus empresas en cualquier parte que se encuentren. De acuerdo a la IDC las ventas de tabletas a nivel global se va a duplicar para el 2016 a medida que los consumidores prefieren dispositivos móviles más pequeños sobre las computadoras personales tradicionales (Rapaport, 2012).

El objetivo de la infraestructura IT es proveer los medios por los cuales los usuarios puedan tener acceso a los sistemas de información, a las aplicaciones o almacenes de información que necesitan ya sea para la toma de decisiones en los mandos altos y medios o las actividades del día a día en los niveles operativos. Sea cual sea la actividad a realizar el usuario necesita al menos una entrada o interfaz (ya sea un aparato móvil, una estación de trabajo, una terminal tonta, o una computadora personal) que permita la

entrada y visualización de datos, un lugar donde almacenar y procesar la información (mainframes, minicomputadoras o servidores), y una forma de comunicar a ambos.

Ya que usualmente la información en una empresa mediana a grande no es de uso de una sola persona, esta debe ser compartida de alguna forma con los demás miembros del mismo o inclusive otros departamentos de la empresa. Para esto fue necesaria la centralización de la información en un lugar donde pueda ser procesada y visualizada por todos los interesados. En un principio esto se hacía mediante la adquisición de costosos mainframes a los que claramente no todas las organizaciones podían tener acceso y después a las minicomputadoras que "ofrecían potentes maquinas a precios más bajos que los mainframes de IBM" (Laudon & Laudon, 2008).

Con el desarrollo de las computadoras personales que cada vez se volvían más potentes y menos costosas, se podía distribuir la carga de procesamiento entre un cliente y un servidor y no solo dejarlo todo a un mainframe que debía hacer el trabajo de almacenamiento y procesamiento por sí solo. Esto dio paso a la arquitectura cliente servidor donde la carga del procesamiento de la información es distribuida entre el cliente (que puede ser una estación de trabajo o dispositivo móvil) y un servidor.

Por servidor entendemos tanto el hardware compuesto de discos, memoria, procesadores, interfaces de red, controladores etc… como el software que está a la espera de requerimientos por parte de un cliente. Con la arquitectura cliente servidor fue posible para empresas que antes no tenían el presupuesto a tener una ambiente de computación a gran escala, en la que se la información podía ser presentada y manipulada por varias personas en distintas áreas geográficas.

Para la arquitectura cliente servidor funcione es necesario la transferencia rápida de datos entre el cliente y el servidor, por lo que su desarrollo ha ido de la mano con el desarrollo de las redes.

Según Effy (2008) podemos diferenciar entre los siguientes tipos de redes:

1. Redes LAN: Se utilizan para interconectar ubicaciones que están físicamente cerca. Dentro de un radio de aproximadamente 5 a 6 Kilómetros (Oz, 2008).

En las redes LAN se han utilizado varios tipos de protocolos para la comunicación de dispositivos siendo Ethernet el estándar hoy en día.

Ethernet ha evolucionado y ha pasado por las siguientes etapas según Wendell (2008):

- Ethernet 10base2 y 10base5: En este estándar se utiliza el cable coaxial para conectar las NICS (Tarjetas de interface de red). No se utilizan todavía los hubs o switches, en su lugar crea un circuito llamado bus al conectar directamente la nic de cada dispositivo en la red. Las redes estaban limitadas a un ancho de banda de 10Mbps y distancias de 500m (10base5) y 200m (10base2).

- Ethernet 10base-T (1990): Utiliza cable de cobre UTP (cable de par trenzado), utiliza un hubo en vez de un bus para conectar los dispositivos y su ancho de banda es de 10Mbps. Estos hubs después fueron reemplazados por bridges, dispositivos de capa dos, que no solamente actuaban como repetidores de capa 1. Los bridges reducían el número de colisiones en la red y le agregaron ancho de banda (Odom, 2008). Los bridges daban permitían que por cada puerto en el que estaba conectado un dispositivo este pudiera contar con el ancho de banda que antes tenía que ser compartido con el uso de los hubs. Ya que no todos los datos encapsulados en tramas tenían que ser escuchados por todos los demás equipos en la misma LAN, esto reducía el número de colisiones. Los bridges también permitieron que los dispositivos conectados a la red pudieran mandar datos al mismo tiempo que se recibían (lo que se conoce como una conexión full dúplex) a diferencia de la conexión Half dúplex en el que el dispositivo tenía que esperar hasta que otro dispositivo no estuviera transmitiendo por la LAN al mismo tiempo. Finalmente los bridges fueron reemplazados por switches. En si los switches son bridges

con mayor capacidad de puertos y con “hardware optimizado para poder transmitir millones de tramas por segundo” (Odom, 2008).

- Ethernet 100base-TX (Fast Ethernet o FE) (1995): Permite ancho de banda 100Mbps, utiliza cable UTP.

- Ethernet 1000base-T (Gigabit Ethernet o GE)(1999): Permite una ancho de banda de 1000Mbps y puede utilizar cableado de cobre(UTP) o fibra.

- Ethernet 10Gbase-T (10 Gigabit Ethernet)(2002): Permite una ancho de banda de 10,000Mbps y puede utilizar cableado de cobre(UTP) o fibra.

2. Redes MAN: (Redes de Área Metropolitana): Compuesta de varias LANS que se interconectan dentro de una misma ciudad, y “abarcan una distancia de hasta 50km” (Oz, 2008).

3. Redes WAN: Estas son las que interconectan dos o más redes LAN o MAN a distancias mayores de los 50km. Las WAN pueden ser privadas, conectando una empresa que este ubicada en varias ciudades o incluso en diferentes países, o públicas como es el caso del Internet. Para establecer una red WAN (o MAN) se necesita el servicio de una empresa de telecomunicaciones, ya que el cableado tiene que pasar por la portería de que usualmente pertenece al Estado.

4. Redes PAN: “es una red diseñada por portátiles como los PDA, teléfonos celulares, y computadoras de tablilla o laptops y que está diseñada para la utilicen solo una o dos personas” (Odom, 2008). Este tipo de redes se han popularizado en los últimos años por el uso de los Smartphone que pueden ser utilizados como Hotspots o módems y permitir que otros dispositivos; ya sean tabletas o laptops, se conecten a Internet a través de ellos.

En resumen, con los avances experimentados en las comunicaciones y aunque en los países de Latino América siguen siendo más costosos que en los países más

desarrollados, si ha habido un crecimiento importante en esta área. Ya no es necesario que los servidores donde se alojan los sistemas de información y sus datos se encuentren en el área inmediata de las personas que accedan a ellos. No solamente es posible tener los centros de datos en lugares alejados en una ciudad, incluso empresas internacionales pueden extender sus LANs hacia los demás países donde están sus sucursales. Con el aumento del ancho de banda en las redes WAN y LAN con la utilización de fibra en vez de cobre, se ha hecho posible la transmisión de una cantidad considerable de información a través de la red.

Es importante mencionar que a medida que los servidores se han vuelto más potentes y de menor costo, ha surgido una tendencia a transferir la carga de trabajo de nuevo en su totalidad a los servidores. Ejemplos de estos son la utilización de Escritorio Remoto (Terminal Services en Microsoft), que básicamente hacen que la computadora personal actué como una terminal tonta, solamente presentándole una interfaz gráfica en la que la persona ejecuta las aplicaciones en su totalidad dentro del servidor. Así mismo las aplicaciones web utilizando como interface un explorador de internet (browser), dejan la mayoría o todo el trabajo de almacenamiento y análisis al servidor que aloja la aplicación.

El desarrollo de la infraestructura IT ha traído consigo una amplia gama de componentes físicos, los cuales necesitan de ciertos requerimientos para su funcionamiento correcto.

Como se mencionó anteriormente para que un sistema de información cumpla con su función de recibir, analizar y distribuir datos hacia todas las áreas de una organización, es necesario contar con medios para almacenar y procesar los datos.

También además de los equipos donde están alojados los diversos sistemas utilizados por la empresa ya sea en transacciones diarias o en el apoyo a la toma de decisiones es necesario contar con otros dispositivos que complementan a estos sistemas como por ejemplo:

1. Servidores de Directorio: En una empresa de tamaño medio que cuenta con un número considerable de usuarios, se vuelve complejo la administración de las

estaciones de trabajo o laptops asignadas a cada usuario, así como también la otorgación de permisos y accesos a dicho usuario a otros dispositivos de la red. Debido a esto surge la necesidad de contar con un lugar donde queden registrados los equipos conectados a la red, donde se puedan crear los usuarios que puedan tener permisos a recursos de la red, y donde se puedan distribuir políticas de seguridad hacia los dispositivos de usuario final. Estas labores de autenticación y distribución de políticas se realizan en un Directorio (en una red Microsoft conocido como un directorio Activo o Controlador de Dominio). Este debe ser alojado en un servidor físico separado de las demás aplicaciones de la empresa.

2. Servidores de Correo: Muchas empresas optan por no utilizar los servicios de correo públicos (Gmail, Hotmail, Yahoo mail etc.) debido a razones de seguridad o un mejor control de su acceso, utilizando en muchos casos los usuarios o políticas definidos en el controlador de Dominio. Estos servidores por lo general son intensivos en el uso de procesador y memoria y requieren de una buena capacidad de almacenamiento. Por esto debe alojarse en hardware específico para esta función. Los servidores de correo muchas veces son utilizados directamente por otras aplicaciones de la red, como lo son impresoras, sistemas de monitoreo u otros sistemas que requieren mandar alertas al usuario vía este medio.

3. Dispositivo Antispam: La cantidad de correos basura (spam) a los que están sujetos los servidores de correo hacen necesario que estén protegidos por un sistema antispam que puede ser software instalado en el mismo servidor. Sin embargo muchas empresas eligen utilizar otro dispositivo físico colocado antes del servidor de correo ya que los servicios antispam o antivirus pueden requerir utilización intensiva del procesador y memoria.

4. Dispositivos en la SAN (Storage área network): Muchas empresas hoy en día requieren almacenar, procesar y respaldar una gran cantidad de información la cual no es factible tenerla centralizada en un solo servidor o utilizar la red LAN

para mover esa información. Por esto se puede requerir una solución de almacenamiento que sea más escalable. La SAN “es una red especializada, de alta velocidad que conecta servidores con dispositivos de almacenamiento” (Tate, Lucchese, & Moore, 2006).

Según Tate, Lucchese & Moore (2006) una SAN está compuesta por los siguientes componentes:

a. Un sistema de discos: Este puede ser simplemente un conjunto de discos que se miran como dispositivos individuales, con una funcionalidad básica de lectura y escritura, o pueden ser un arreglo redundante de discos independientes (RAID) en el cual los discos se miran como una sola unidad lógica al dispositivo al cual están conectados. En el RAID una controladora central permite que se puedan configurar los discos de tal forma que permitan tolerancia a una falla y operen de manera más óptima. El almacenamiento también puede estar compuesto por cintas o librerías de cintas.

b. Un medio de conectividad: Los medios de almacenamiento deben poder leer y escribir una gran cantidad de datos a través de un medio rápido y confiable. Para conectar las SAN se pueden utilizar una variedad de protocolos , algunos de ellos son :

    - Protocolo de Fibra Canal(FCP)
    - Internet SCSI (ISCSI)
    - Fibra canal sobre IP (FCIP)
    - Internet FCP

c. El ultimo componente son los servidores: Según Tate,Lucchese & Moore(2006) estos pueden ser:

    - Mainframes

- Servidores basados en el sistema operativo UNIX.
- Servidores basados en el sistema operativo LINUX.
- Servidores basados en los sistemas operativos de Microsoft.

5. Dispositivos de Conectividad: Los servidores deben estar accesibles a los usuarios de la empresa por lo que se requiere como mínimo un Switch para conectar los diferentes equipos a la red. Ya que la seguridad se ha vuelto un tema fundamental en la lo que se refiere a los dispositivos conectados a la red es también se puede necesitar de la utilización de un Firewall (dispositivo de capa 3 que controla las conexiones a equipos de la red basándose en una serie de reglas configuradas por el administrador). El firewall puede ser simplemente una aplicación en cada servidor, pero usualmente un dispositivo físico dentro de la red. Además de esto algunas empresas cuentan con equipo de seguridad más especializado como lo son los Sistemas de detección y prevención de intrusiones (IPS y IDS). Estos en muchos casos también son equipos físicos que necesitan ser instalados por aparte.

6. Planta Telefónica: Las plantas telefónicas han caído en el dominio de IT y por consiguiente se consideran un elemento más de la infraestructura. La planta es un equipo físico más de la red.

Aparte de todo lo anterior debemos tomar en consideración la posibilidad de que un solo servidor no sea suficiente para todas las aplicaciones de una empresa. Muchas veces estas aplicaciones requieren diferentes sistemas operativos, o son demasiado pesados en términos de procesamiento para que puedan residir en el mismo servidor físico por lo que es muy común tener varios servidores separados corriendo aplicaciones específicas para diferentes áreas de la empresa.

Como se puede apreciar la infraestructura detrás de un sistema de información en una empresa puede constar de un sin número de aparatos. Todos ellos con necesidad de un espacio adecuado para su instalación. Es aquí donde entra la necesidad del Data Center.

“Un Data Center esta generalmente organizado en filas de racks, donde cada rack contiene dispositivos modulares como lo son switches, servidores, dispositivos de almacenamiento y otras aplicaciones de funcionalidad específica” (Kant, 2009). Los racks que pueden ser abiertos o cerrados, son estructuras de dos o cuatro postes donde se montan los servidores, switches, routers, firewall, dispositivos de almacenamiento u otros equipos que necesiten estar en el ambiente protegido del centro de datos. El objetivo del Data center es asegurar la disponibilidad de los equipos que están alojados en él ya que muchos de ellos son parte de aplicaciones críticas para las funciones de la empresa, y en algunos casos deben estar arriba las 24 horas del día y todos los días del año.

Para esto un centro de datos debe garantizar lo siguiente:

1. Ambiente seguro, donde se controla el acceso físico a todos los equipos que están alojados en él. De ser posible el centro de datos debe contar con controles de acceso y monitoreo (cámaras) para que solo las personas autorizadas puedan entrar y manipular los servidores. Debe llevarse un registro de quien ha entrado, en que día y a qué hora para que sea posible darle seguimiento a cualquier problema que pueda ocurrir dentro de las instalaciones.

   El centro de datos también debe contar con mecanismos de prevención de incendios, como dispositivos de alarma y extintores que se puedan accionar de forma automática ante la presencia de fuego en la sala.

2. Flujo continuo de energía: Para esto el centro de datos debe contar con bancos de baterías, UPS, inversores que permitan el funcionamiento de los equipos DC, e inclusive una planta de energía que asegure la continua operación del sitio en caso de una falla de energía prolongada.

3. Control de temperatura y humedad: Los equipos de cómputo requieren operar dentro de parámetros establecidos de temperatura. Un sitio que este demasiado caliente o demasiado frio puede deteriorar los equipos de cómputo y comunicación causando pérdidas de datos o caídas en los servicios.

4. Lugar que permita el ordenamiento adecuado del cableado: Por lo general los centros de datos cuentan con piso o cielo falso por donde pasar los cables de energía y de comunicación, en su ausencia también pueden utilizarse escalerillas para ordenar estos cables.

Como se puede ver el centro de datos en si requiere de planeación y administración, en la utilización de recursos. Dependiendo del tamaño del centro de datos así variará la complejidad de manejarlo. Entre más equipos se agreguen a él mayor es la demanda de espacio, energía, y de sistemas de enfriamiento más costosos.

También debe considerarse que agrupar la mayoría de los equipos críticos de la empresa en un solo sitio presenta un peligro, ya que una catástrofe que incapacite el sitio dejaría a la empresa inoperante por un periodo de tiempo indefinido. Esto da lugar a la necesidad de redundancia de los equipos colocando equipos de respaldo en otro sitio separado geográficamente el cual en el mejor de los casos contara con todos los beneficios del sitio primario.

Es claro que todo esto impacta en los costos de operación de una empresa, lo cual puede resultar muy doloroso para una empresa cuya actividad principal no sean los sistemas de información. Por ello se han buscado formas de bajar estos costos ya sea vía la virtualización y los servicios en la nube, como veremos a continuación.

2.3 VIRTUALIZACIÓN

Como se mencionó en la sección anterior, la infraestructura de información puede llegar a estar compuesta por más de un servidor físico. Esto debido a que algunos servicios o aplicaciones que utilizan los usuarios no pueden compartir los mismos recursos. Algunas de las razones para esto son las siguientes:

1. Dos o más servicios no están diseñados para ejecutarse sobre el mismo sistema operativo. Muchas de las aplicaciones siguen estando sujetas a un ambiente de Microsoft, sin embargo para muchos otros servicios se ha vuelto viable utilizar otros sistemas operativos como lo son Linux y sus muchas variantes, ya que

pueden resultar más económicos (bajo el concepto de Open Source) e incluso más estables y (esto es sujeto a debate, dependiendo que tan hábil es la persona que administra y configura dicho sistema) pueden ser menos vulnerables a virus o ataques que los basados en Windows.

2. Aplicaciones que corran en diferentes sistemas operativos de Windows. Algunas empresas tienen aplicaciones que solo son compatibles con uno solo de los sistemas operativos de Windows ya sea Windows server 2000, Windows Server 2003, Windows Server 2008, Windows XP o incluso versiones anteriores.
   Cuando se presenta este escenario no queda más que comprar un servidor aparte para cada aplicación que necesita un sistema operativo diferente.

3. Algunos servicios son más vulnerables a ataques o producir errores que dejen degraden la funcionalidad de un servidor. Es preferible mantener los servicios más críticos aislados de otros que puedan interrumpir su funcionamiento con un error imprevisto del sistema.

4. Por razones de seguridad también se recomienda que ciertos servicios no se manejen dentro del mismo servidor físico. Por ejemplo la persona que maneja el controlador de dominio puede que no esté autorizada a manipular la aplicación o base de datos de recursos humanos. En este caso es recomendable no tener los dos servicios trabajando en una misma instancia de un servidor.

Tener muchos servidores para aplicaciones diversas trae consigo más gasto, como se explicó anteriormente y también da lugar al desperdicio de recursos. Por lo general es difícil adquirir hardware a la medida del software que estará ejecutándose en él lo que lleva al sobre dimensionamiento. Los servidores usualmente no utilizan el cien por ciento de los recursos disponibles. Algunas aplicaciones simplemente no tienen una gran necesidad de utilización de CPU, almacenamiento en disco duro o en memoria volátil. Simplemente no pueden compartir el mismo sistema operativo con otras aplicaciones por las razones antes expuestas.

Aquí es donde entra un el concepto de la virtualización de servidores. Virtualización puede ser definida como “una forma de abstraer aplicaciones y sus componentes subyacentes del hardware que las soporta presentando una vista lógica o virtual de estos recursos” (Kusnetzky, 2011).

Según Kusnetzky (2011), el modelo de virtualización está compuesto por varios niveles o capas de tecnología que permiten aislar alguna parte del ambiente de computación:

1. Virtualización de Acceso: Esto es el hardware y software que permiten que usuarios remotos puedan tener acceso a una interface del servidor donde residen las aplicaciones, permitiéndole al mismo interactuar con ellas.

2. Virtualización de Aplicación: Este tipo de virtualización puede ser de dos tipos:
    a. Virtualización de aplicación del lado del cliente: Esto consiste en que un usuario indistintamente del sistema operativo con el que cuenta pueda interactuar con una aplicación del lado del servidor, la cual es presentada en forma encapsulada por el sistema operativo del servidor. Ejemplos de esto son los protocolos de escritorio remoto (RDP) o los que permiten las sesiones VNC.

    b. Virtualización del lado del Servidor: Esta es la que permite que diferentes aplicaciones que no comparten el mismo sistema operativo puedan trabajar juntas en el mismo hardware.

    c. Virtualización de Procesamiento: “Permite encapsular el procesamiento de manera que muchos sistemas virtuales puedan ejecutarse en un sistema único…” (Kusnetzky, 2011)

    d. Virtualización de la Red: Esta capa de virtualización permite presentar una vista lógica de la red física. Permite que ciertos clientes o servidores solo miren cierta de parte de la red, aislándolos de forma lógica de los demás dispositivos.

e. Virtualización del almacenamiento: Esta es la capa que permite que varios sistemas puedan compartir la misma unidad de almacenamientos, sin importar de que tipo sea. Al igual que las capas anteriores esconde la parte física y presenta solamente una vista lógica de los medios de almacenamiento.

f. Capa de Seguridad de los ambientes virtuales: Es el software que provee el control del acceso a los diferentes niveles de virtualización y trata de prevenir ataques o usos malintencionados de los recursos.

g. Capa de administración de los sistemas virtuales: Según Kusnetzky (2011) aquí se llevan a cabo las siguientes funciones:
    - Por medio de esta capa se gestiona la creación de los ambientes virtuales.
    - Se provisionan los recursos físicos y lógicos con los que van a contar dichos ambientes.
    - Se monitorea la ejecución de los ambientes virtuales. Esto incluye monitoreo de la utilización de los recursos compartidos monitoreo del rendimiento de los sistemas virtuales en general.
    - Análisis de las bitácoras para identificar y solucionar problemas con el funcionamiento de los sistemas virtuales.
    - Optimización de los componentes de una ambiente virtual.
    - Automatización de procesos en los sistemas virtuales.

Con la virtualización se trata de racionalizar los recursos utilizados en un centro de datos, buscando minimizar la necesidad de componentes físicos, como los son los servidores. Se busca reducir el crecimiento del centro de datos y al mismo tiempo buscar la forma de agrupar aplicaciones obligándolas a compartir un “pool” de recursos dentro de los cuales están procesadores, sistemas de almacenamiento volátil y no volátil, componentes de la red, y sobre todo el espacio físico dentro de los gabinetes o racks en el centro de datos.

Mediante la práctica de consolidación de servidores se puede hacer un análisis de todas las aplicaciones críticas y no críticas que están alojadas en el centro de datos y buscar formas de agruparlas en un solo hardware. Aplicaciones que estaban obligadas a trabajar en diferentes plataformas o sistemas operativos pueden unirse en un solo servidor trabajando bajo una ambiente de virtualización. Mediante este ambiente se puede lograr de forma lógica la separación de los servicios en los diferentes sistemas operativos requeridos. De esta forma también se puede tratar con el problema del sobre dimensionamiento, ya que se pueden asignar recursos a las servidores virtualizados (máquinas virtuales) de forma dinámica.

Además de las ventajas de reducir el número de servidores físicos en la red y de esta forma economizar en el gasto de energía, espacio y control de temperatura, al independizar las aplicaciones de las capas físicas sobre las que se ejecutan, también tiene presenta otras facilidades en lo que se refiere a redundancia y respaldos.

Ya que los servidores o máquinas virtuales son simplemente software que no dependen de la plataforma física donde residen, se vuelve posible poder moverlas a otro servidor físico cuando el anterior ya esté llegando al final de su vida útil sin tener que volver a instalar y configurar dicha aplicación desde cero en un servidor nuevo como se hacía antes. Las máquinas virtuales también permiten mediante otras aplicaciones que puedan ser respaldadas en su totalidad incluso mientras están funcionando. En lo que se refiere a la redundancia se pueden tener dos o más servidores físicos que sirvan de respaldo entre ellos de forma que se puedan mover los servidores virtuales en su totalidad entre ellos en caso de alguna falla física de alguno de ellos. Utilizados con los mecanismos de almacenamiento que vimos anteriormente estos servidores pudieran incluso separar el procesamiento del almacenamiento de las máquinas virtuales. De esta forma la falla total de uno de los servidores puede ser solucionada en cuestión de segundos, asumiendo el otro servidor sus funciones, y utilizando los servidores virtuales que se encuentran en el almacenamiento compartido.

Vale la pena mencionar que aparte de la virtualización de servidores también existe la virtualización de estaciones de trabajo o Desktops. Este concepto aprovecha todos los beneficios de la virtualización y los enfoca en el usuario final. Con esto se busca

solucionar el problema de disponibilidad. Un usuario siempre puede tener a su disposición todos los recursos de su estación de trabajo, todas sus aplicaciones, con estar conectado a la red. Con la virtualización del desktop el usuario se puede dejar de preocuparse por el mantenimiento de una maquina física, ya que su desktop con toda su información y su software se vuelven independiente de ella. Al igual que con la virtualización de servidores, las desktop virtualizadas se convierten en software que igual puede ser trasladado a otras plataformas fiscas, y puede ser respaldado en su totalidad.

Bajo este esquema la PC que el usuario utiliza para conectarse a su desktop puede contar con menos recursos ya que no necesitara ejecutar todas las aplicaciones que necesita en sus funciones diarias. También se simplifica la labor del departamento de IT en lo que se refiere a provisionar computadoras, al tiempo que se gasta en tener que mandar una PC a su estado inicial por medio de una reinstalación de sistema operativo o formateo de disco, y volver a cargar todos los programas que el usuario necesita.

Algunos ejemplos de los ambientes de virtualización hoy en día está el hypervisor Vsphere de Vmware, el Virtual PC de Microsoft, Xen server de Citrix entre otros.

Hay que recordar que todo sistema de información ya sea virtualizado o no debe de ser protegido por los datos invaluables que contiene y es por ello que en la siguiente sección hablaremos específicamente de seguridad de la información y su importancia.

2.4 SEGURIDAD DE LA INFORMACIÓN

Según Escrivá (2013) la seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información, estos tres últimos es lo que normalmente se conoce como los principios de la seguridad de la información.

Existen también diferentes definiciones del término Seguridad Informática, de ellas se toma la definición ofrecida por el estándar para la seguridad de la información ISO/IEC 27001, que fue aprobado y publicado en octubre de 2005 por la International Organization

for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

Sobre este tema Eugene Spafford, profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que “el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él”.

Según Escriva (2013) los principios de la seguridad de la información se conceptualizan de la siguiente forma:

1. Integridad: Certificado que tanto la información como sus métodos de proceso son exactos y completos.
2. Confidencialidad: asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados
3. Disponibilidad: permitiendo que la información esté disponible cuando los usuarios la necesiten.

La figura 2 nos muestra de forma gráfica como estas bases están interrelacionadas entre si y se desarrollaran a detalle más delante en este documento.

Figura 2: Bases de la Seguridad de la Información

La seguridad informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura de TI y de telecomunicaciones para ser almacenada o transmitida. (Escrivá Gascó, 2013) distingue los siguientes tipos de seguridad:

En función a lo que se quiere proteger:

1. Seguridad física: Se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc
2. Seguridad lógica: Mecanismos que protegen la parte lógica de un sistema informático. Uno de los medios más utilizados es la criptografía.

En función del momento en que tiene lugar la protección:

1. Seguridad activa: se encarga de prevenir, detectar, y evitar cualquier incidente en los sistemas informáticos antes de que se reduzca, por ejemplo el uso de contraseñas.
2. Seguridad pasiva: Comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad, por ejemplo copias de seguridad.

2.4.1 PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Aunque la mayoría de expertos coinciden en que no existe ningún sistema totalmente seguro e infalible al 100%, se debe tratar de proteger la información y el sistema que la utiliza para ofrecer un nivel de seguridad razonable a los usuarios.

Para que un sistema se pueda considerar razonablemente seguro se debe garantizar que se cumplen los principios básicos de la seguridad informática: integridad, confidencialidad y disponibilidad.

2.5 COMPUTACIÓN EN LA NUBE

Se observa que la tendencia en la tecnología está en simplificar la manera en que se presenta la información y las aplicaciones al usuario final. Como vimos anteriormente los servicios y aplicaciones necesarios para la construcción de un sistema de información que ayude a la organización a alcanzar sus objetivos están implementados sobre una multitud de componentes lógicos y físicos. Se requiere la interacción de uno o más servidores, dispositivos de comunicación, cableado, instalaciones adecuadas que cuenten con los requerimientos básicos de energía y control de temperatura que en mejor de casos será un centro de datos.

Se puede ver que todos estos requerimientos tienen un costo asociado que se reflejan en:

1. La compra de equipo de cómputo y de comunicación. Desde computadoras personales hasta servidores, equipos de comunicación como lo son Routers y Switches, UPS, etc... todos los cuales están sujetos a quedar obsoletos en un periodo de no más de 3 a 5 años.

2. Costo del mantenimiento de dicho equipo.

3. Costos de energía para mantener los equipos en producción y para enfriamiento de salas de cómputo.

4. Costo de personal que sea capaz de administrar y dar mantenimiento a todos estos componentes de la infraestructura IT. Algunas empresas eligen subcontratar estos servicios pero muchas necesitan personal de planta dependiendo de la inmediatez con que se requiera el soporte del personal de Informática.

5. Costo de mantener soluciones de redundancia para los servicios críticos y soluciones de seguridad para evitar el acceso indebido a la información almacenada en diferentes dispositivos y lugares de la red.

La virtualización ayuda en cierta medida a consolidar algunos de los servicios y poder contar con menos hardware pero de igual forma no elimina en su totalidad los costos mencionados anteriormente ni la complejidad de administrar los sistemas.

Esto ha llevado a tratar de separar a un más la infraestructura de las tecnologías de la información de los usuarios u organizaciones que los necesitan. Ya que para los que necesitan interactuar con los sistemas de información y demás aplicaciones en la red, la estructura que está en los niveles inferiores es indistinta, en si es una “nube” sobre la cual no necesita tener conocimiento de sus detalles de funcionamiento ni de todos los módulos que la conforman.

“La Computación en la nube permite una mayor agilidad y eficiencia de costos en la gestión de la información digital de cualquier organización o empresa, a través de una implantación sencilla y flexible”. (Observatorio Regional de Sociedad de la Información, 2010)

2.5.1 ¿QUE ES LA NUBE?

Hay muchas definiciones para lo que es el concepto de nube e incluso se ha dicho que esta tecnología ya existe desde hace mucho y en la actualidad solo se ha tratado de poner de moda bajo esta terminología.

El CEO de Oracle dijo lo siguiente acerca de la computación en la nube: “Lo interesante del concepto de Computación en la nube es que lo hemos redefinido para incluir todo lo que ya hacemos…no veo que tendríamos que hacer diferente a la luz de la Computación en la Nube además de tener que cambia la terminología de algunos de nuestros anuncios”. (Armbrust, y otros, Volume 53 Issue 4, April 2010)

A continuación se mencionan algunas de estas definiciones:

“Es un conjunto de servicios habilitados en la red los cuales pueden ser utilizados en forma simple y frecuente” (Chang, Wills, & De Roure, 2010)

“Esencialmente, la computación en nube consiste en la gestión y suministro de aplicaciones, información y datos como un servicio. Estos servicios se proporcionan a través de la “nube” (una red de telecomunicaciones pública, generalmente Internet), a menudo en un modelo basado en el consumo”. (Observatorio Regional de Sociedad de la Información, 2010)

“La computación en la nube está compuesta tanto por las aplicaciones que son entregadas como un servicio así como el hardware y sistemas de software que en los centros de datos que proveen estos servicios” (Armbrust, y otros, Volume 53 Issue 4, April 2010)

Se puede decir entonces que en sí, la nube es un conjunto de servicios, aplicaciones, hardware y software que son accesibles a través de la red por los usuarios finales y cuyo objetivo es permitir a los usuarios contar con aplicaciones y recursos de procesamiento y almacenamiento sin tener que contar con una compleja infraestructura IT para su funcionamiento.

De acuerdo con (Armbrust, y otros, Volume 53 Issue 4, April 2010) en términos de hardware la computación en la nube cambia su concepto en los siguientes aspectos:

1. Da la ilusión de contarse con recursos infinitos de computación dependiendo de la demanda. Esto evita las complicaciones de tener que provisionar un sistema sin estar seguros que tantos recursos vaya a utilizar en el futuro.

2. Elimina la necesidad de la empresa de comprometerse adquiriendo software y hardware que posiblemente quede obsoleto de forma muy rápida o que no vaya a usar en su totalidad.

3. Los recursos se pueden asignar de forma dinámica conforme surge la necesidad o en base a un periodo de tiempo, siendo liberados cuando ya no se utilicen.

Según Jamsa (2012), existen cuatro modelos principales de nubes que se explicaran a continuación y especifican como los recursos de la nube son compartidos.

1. Nube Privada:

   Esta es propiedad de una sola organización, que requiere tener sus aplicaciones y servidores en el sitio por motivos de seguridad. Este tipo de arquitectura consiste en sí de un centro de datos mantenido por la empresa.

   Los principales inconvenientes de este modelo son los analizados para el paradigma tradicional, por ejemplo los relativos a la ampliación de los sistemas informáticos. Esto obliga a adquirir nuevos sistemas antes de hacer uso de ellos, contrariamente a lo ofrecido por las nubes públicas, donde ampliar los recursos se reduce a contratarlos con el proveedor de servicios.

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

2. Nube Pública:

   Esta es disponible al público en general, y es propiedad de una empresa que se dedique a brindar servicios en la nube. Ya que es compartida por varios clientes resulta una solución más económica a la nube privada.

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

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

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

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

    - Protección de datos, control de la propiedad de la información e imposición de restricciones sobre su ubicación geográfica.

    - Condiciones para que el usuario pueda auditar o inspeccionar su información en cualquier momento.

    - Estándares de seguridad cumplidos por la información.

    - Garantías sobre posibles pérdidas de información o falta de disponibilidad de la misma.

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

3. Nube Comunitaria:

   Es mantenida por un grupo de organizaciones usualmente con propósitos académicos.

4. Nube Híbrida:

   Está compuesta por una combinación de nubes privadas, públicas o comunitarias. Las principales cuestiones a vigilar en este modelo son la privacidad y la protección de datos, al igual que en la nube pública.

Las nubes híbridas consisten en combinar las aplicaciones propias de la empresa con las consumidas a través de la nube pública, entendiéndose también como la incorporación de servicios de Computación en la nube a las aplicaciones privadas de la organización. Esto permite a una empresa mantener el control sobre las aplicaciones críticas para su negocio y aprovechar al mismo tiempo las posibilidades ofrecidas por los servicios ofertados por la nube en aquellas áreas donde resulte más adecuado.

A continuación se muestra una figura que ejemplifica gráficamente los tipos de nubes.

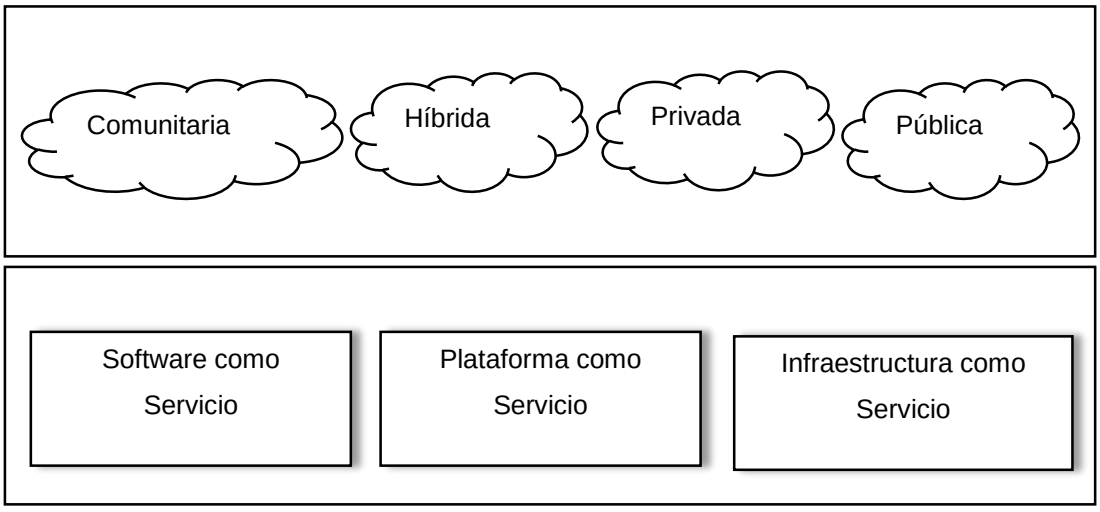

Figura 3: Modelo de Implementación de la nube

Fuente: (Jamsa, 2012)

La computación en la nube puede tomar varias formas, incluyendo: SaaS, PaaS y IaaS.

1. Software como servicio (SaaS): Ofrece el consumo de una gran variedad de aplicaciones proporcionadas por los proveedores del servicio y que se ejecutan en la infraestructura de la nube. Las aplicaciones en la “nube” son accesibles por varios dispositivos del cliente a través de una interfaz sencilla, como puede ser un navegador web. El consumidor del servicio no gestiona o controla la infraestructura subyacente del servicio, que incluye la red de comunicaciones, los servidores, los sistemas operativos y el almacenamiento.

Así, SaaS está orientado principalmente a reducir el costo de implantación y uso de los sistemas informáticos asociados a la gestión de los recursos empresariales (como pueden ser los ERP y CRM) de una organización. El costo se reduce debido a que la inversión inicial es prácticamente inexistente, y las tarifas por el uso posterior de los servicios SaaS son bastante reducidas debido a la economía de escala y a alta especialización de las empresas proveedoras de esos servicios. En cuanto a los agentes destinatarios de SaaS, pueden ser cualquier empresa que esté interesada en alguno de los servicios ofrecidos por proveedores SaaS, los cuales pueden ser de muy distinto tipo: desde servicios genéricos relacionados con actividades transversales a toda la empresa (gestión del correo electrónico, repositorio de documentos compartidos, etc.) hasta servicios que cubran procesos de negocio estratégicos para la organización, en los que se puede llegar a cierto acuerdo de parametrización o personalización con el proveedor de servicios SaaS. (Observatorio Regional de Sociedad de la Información, 2010)

2. Plataforma como un servicio (PaaS): Agrupa un conjunto de funcionalidades que permiten a los usuarios crear nuevas aplicaciones informáticas. Los servicios PaaS proveen desde la nube todos los componentes necesarios para la creación de una nueva aplicación informática, ofreciendo un servicio que normalmente integra un entorno de desarrollo y una interfaz de programación de aplicaciones.

   Algunos ejemplos comerciales PaaS son Google Apps, Engine, Velneo, Abiquo, SimpleDB SQS, que ofrecen aquellas funcionalidades necesarias para que los diseñadores de software puedan desarrollar aplicaciones web y otras funcionalidades que se ejecuten en su infraestructura.

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

en unas mismas máquinas. Así, se reduce el costopor el mantenimiento de varios equipos, se evitan problemas de incompatibilidad entre equipos y se disminuye el esfuerzo de creación de las aplicaciones, ya que se dispone de un sistema que unifica y centraliza de manera simple un desarrollo distribuido. (Observatorio Regional de Sociedad de la Información, 2010)

3. Infraestructura como servicio (IaaS): Es un modelo de Computación en la nube que permite utilizar recursos informáticos hardware de un proveedor en forma de servicio. Con ello, IaaS permite que los clientes puedan comprar recursos hardware (servidores, sistemas de almacenamiento, conmutadores, routers, etc.) como si se tratara de servicios totalmente externalizados. Con este modelo se logra poder ampliar o reducir los recursos informáticos físicos en un periodo de tiempo muy breve. (Observatorio Regional de Sociedad de la Información, 2010)

   Uno de los sistemas IaaS más conocido es Amazon Web Services que ofrece, entre otros, recursos de computación distribuida, sistemas de almacenamiento de información y sistemas de bases de datos. Otro ejemplo es la empresa Akamai, que incluye soluciones escalables de infraestructura para el despliegue de aplicaciones Web en ellas. Pero sin duda, los ejemplos más cercanos los encontramos en los proveedores de hosting como Arsys, Mosso, rackspacecloud, etc. ya que todos los servicios de hosting2 de aplicaciones, de amplia penetración en el mercado desde hace varios años, también entrarían dentro de esta categoría. (Observatorio Regional de Sociedad de la Información, 2010).

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

En la tabla 1, que se presenta a continuación, se ejemplifica en resumen las diversas formas que puede tomar la nube según el servicio que se ofrece, el nivel y una breve descripción de los servicios

Tabla 1: Formas de Nube según el Servicio

Nivel	Nombre	Descripción
Nivel de Usuario	Saas (Software as a Service) Software como Servicio	Consiste en alojar en la nube aplicaciones que muchos usuarios pueden utilizar a través de sus conexiones a internet. Lo que se vende es la aplicación.
Nivel de Desarrollador	Paas (Platform as a Service) Plataforma como un servicio	Los desarrolladores pueden crear sus propias aplicaciones sobre la infraestructura que da el proveedor en la nube. Después se entregan estas aplicaciones a los usuarios a través de esta infraestructura.
Nivel de IT	IaaS (Infrastructure as a Service) Infraestructura como un servicio	Los administradores reciben servicios de procesamiento, almacenamiento, administración de bases de datos a través de la red y solo se paga por los recursos utilizados.

Fuente: (Rayport & Heyward, 2009)

2.5.2 BENEFICIOS DE LA NUBE

Según Rayport & Heyward (2009) existen seis grandes beneficios de la computación en la nube que se han vuelto claros:

1. Acceso a cualquier hora y en cualquier lugar: La nube promete acceso universal para sobrecarga y almacenamiento de datos de cualquier persona que cuente con un aparato que pueda acceder a la red.

2. Especialización y personalización de las aplicaciones: La nube es una plataforma con mucho potencial para la creación de software para hacer frente una diversidad de tareas y retos.

3. Colaboración entre usuarios: La nube representa un entorno en el cual los usuarios pueden desarrollar programas basados en servicios y a través de ellos pueden hacer las entregas.
4. Procesamiento de potencia sobre demanda: La nube es un recurso siempre “on” que permite al usuario ajustar el consumo a sus necesidades específicas.

5. Almacenamiento como un servicio universal: La nube representa un almacén remoto pero escalable para los usuarios que se encuentran en cualquier lugar y momento.

6. Costos: La nube promete entregar potencia y servicios a un menor costo.

2.5.3 PUNTOS EN CONTRA DE LA NUBE

Entre las desventajas más comunes acerca de la computación en la nube podemos mencionar:

1. Se requiere de una conexión a internet permanentemente que permita acceder a los recursos de la nube. Además para aquellas aplicaciones que necesitan la transferencia de grandes volúmenes de datos se requeriría un ancho de banda adecuado. Considerado el costo y la disponibilidad de estos servicios en los países menos desarrollados esto puede significar una gran debilidad.

2. Problemas de Continuidad de Negocio: La nube puede convertirse en un punto único de falla. Si los servicios de la nube son interrumpidos, el usuario no tendrá acceso a su información. Se debe considerar que pasaría si la compañía que ofrezca los servicios en la nube deja de existir o por alguna catástrofe en su área geográfica no pueda continuar dando este servicio a los usuarios remotos. Para que esto no se dé se debe estar seguro de que la empresa que brinda servicios en la nube se encuentra preparada para una eventualidad así, que

ofrezca alguna forma al usuario de conservar su información en un repositorio local, o simplemente tener a otra empresa que pueda comprometerse a actuar como un respaldo.

3. Preocupaciones de seguridad: Siempre que la información se encuentre en un sitio alejado se corre el riesgo de que esta pueda ser utilizada de forma indebida. Existen también organizaciones como los bancos que son exigidas por normas internacionales a poder auditar sus sistemas, lo que sería muy difícil si tuviera sus aplicaciones en una nube administrada por terceros.

4. Funcionabilidad limitada: La versión en la nube de ciertas aplicaciones pueden no tener la misma funcionalidad que las versiones instaladas en la PC del usuario, esto puede ser un problema para los usuarios más avanzados.

5. Problemas de rendimiento: En una nube compartida que no esté bien dimensionada, la sobreutilización de recursos como el tiempo de procesador por alguna aplicación podría impactar en el rendimiento de los servicios de otros clientes.

En resumen, balanceando los pros y los contras, los servicios en la nube sobre todo en la nube pública pueden considerarse como una solución viable a los altos costos de mantener una infraestructura IT para los sistemas de información de una empresa. Los servicios en la nube ya se están comenzando a implementar en países más desarrollados como en Estados Unidos algunos sistemas de información de agencias gubernamentales se encuentran en la nube. Se estima que las agencias federales de Estados Unidos ya están ahorrando 5.5 mil millones de dólares anualmente con sus implementaciones en la nube (Forbes, 2012). También ya implementaciones de servicios en la nube para empresas y el público en general como lo son Google Apps que contiene un conjunto de aplicaciones que compiten con el suite Office de Microsoft (un procesador de palabras, hoja de cálculo, calendario, creador de presentaciones). Existen otros algunos servicios

de almacenamiento en la nube como lo son Dropbox, y Google Drive que ofrecen espacio en la nube para subir y compartir información.

2.6 SEGURIDAD EN LA NUBE

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), ha publicado un documento (ENISA, 2009) que lista los riesgos en tres categorías, Riesgos Políticos y Organizativos, Riesgos Técnicos y Riesgos Legales para la seguridad en la nube, estos se priorizan y se analiza el impacto al que una empresa se expone si se llevan a cabo.

Así como también se enumeran riesgos no específicos de la nube y vulnerabilidades, para todos estos se realizan recomendaciones que ayudan a mitigarlos.

En nuestro documento, nos centraremos en los riesgos técnicos de seguridad en la nube.

2.6.1 VENTAJAS DE LA COMPUTACIÓN EN LA NUBE EN TÉRMINOS DE SEGURIDAD

Apenas resulta necesario reproducir las incontables páginas de material escrito sobre las ventajas económicas, técnicas, arquitectónicas y ecológicas de la computación en nube. Sin embargo, a la luz de la experiencia directa de los integrantes de nuestro grupo de expertos y según las noticias recientes del «mundo real», el examen de los riesgos de la computación en nube en materia de seguridad debe tener su contrapunto en una revisión de las ventajas concretas que ofrece en materia de seguridad. La computación en nube posee un potencial considerable para mejorar la seguridad y la resistencia a los fallos. Lo que sigue a continuación es una descripción de las contribuciones clave que puede realizar.

- LA SEGURIDAD Y LAS VENTAJAS DE LA ESCALA

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

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

- **Ubicaciones múltiples:** la mayoría de proveedores en nube cuentan con los recursos económicos necesarios para replicar el contenido en ubicaciones múltiples por defecto. De este modo se aumenta la redundancia y la independencia de los errores y se proporciona un grado de recuperación de desastres listo para su uso.

- **Redes de proximidad:** el almacenamiento, procesamiento y entrega más cerca de la red de proximidad supone una confianza en el servicio y un incremento de la calidad en general; del mismo modo, es menos probable que los problemas de redes locales tengan efectos secundarios globales.
- **Mejora del tiempo de respuesta a los incidentes:** los sistemas a mayor escala gestionados satisfactoriamente, por ejemplo, a raíz de la detección temprana de nuevos despliegues de programas maliciosos, pueden desarrollar capacidades más eficaces de respuesta ante incidentes.
- **Gestión de amenazas:** los proveedores en nube también pueden permitirse contratar a especialistas para que se ocupen de las amenazas concretas a la seguridad, mientras que las compañías más pequeñas sólo se pueden permitir los servicios de un número reducido de profesionales generalistas.

- LA SEGURIDAD COMO ELEMENTO DIFERENCIADOR DE MERCADO

La seguridad constituye una prioridad para muchos clientes en nube, los clientes toman las decisiones relativas a la adquisición basándose en el renombre del

proveedor en cuanto a confidencialidad, integridad y resistencia a los fallos, así como en los servicios de seguridad ofrecidos por el proveedor, todavía más que en los entornos tradicionales. Éste es un motivo de peso para que los proveedores en nube mejoren sus prácticas de seguridad y generen competencia en este aspecto.

- INTERFACES NORMALIZADAS PARA SERVICIOS DE SEGURIDAD GESTIONADOS

Los grandes proveedores en nube pueden ofrecer una interfaz abierta y estandarizada a los proveedores de servicios de seguridad gestionadas que ofrecen servicios a todos sus clientes. Potencialmente, ello genera un mercado más abierto y disponible de servicios de seguridad, donde los clientes pueden cambiar de proveedor con mayor facilidad e incurriendo en menores gastos de configuración.

- ESCALADA RÁPIDA E INTELIGENTE DE RECURSOS

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

Un proveedor en nube tiene potencial para reasignar recursos de manera dinámica para el filtrado, la catalogación de tráfico, la codificación, etc., con vistas a incrementar el apoyo a las medidas defensivas (por ejemplo, frente a los ataques distribuidos de denegación de servicio (DDoS)) cuando un ataque está produciéndose o puede producirse. Cuando esta capacidad de reasignación dinámica de recursos se combina con métodos adecuados de optimización de recursos, el proveedor en nube puede limitar las posibles consecuencias de determinados ataques sobre la disponibilidad de los recursos que utilizan los servicios alojados legítimamente, así como reducir el impacto del incremento de uso de los recursos por la defensa de seguridad para hacer frente a dichos ataques. Sin embargo, para lograr este efecto, el proveedor debe aplicar una coordinación adecuada de la autonomía para la defensa de seguridad y para la gestión y optimización de los recursos.

La capacidad de escalar dinámicamente los recursos defensivos bajo demanda posee ventajas evidentes con respecto a la resistencia a los fallos. Además, cuanto mayor sea la escalada de los distintos tipos de recursos individuales de manera granular —sin escalar la totalidad de los recursos del sistema—, más barato será responder a los picos repentinos (no maliciosos) de demanda.

- AUDITORÍA Y RECOGIDA DE PRUEBAS

La OFERTA de la IaaS apoya la clonación de máquinas virtuales bajo demanda. En caso de supuesto incumplimiento de la seguridad, el cliente puede tomar una imagen de una máquina virtual activa —o de los componentes virtuales de la misma— para llevar a cabo un análisis forense fuera de línea, lo cual reduce el tiempo de espera para la realización el análisis. Con el almacenamiento a libre disposición, es posible crear clones múltiples y poner en paralelo actividades de análisis y así reducir el tiempo dedicado a la investigación. De este modo se mejora el análisis *ex post* de los incidentes de seguridad y se incrementa la probabilidad de localizar a los atacantes y de solucionar las deficiencias. Sin embargo, se presupone que el cliente tiene acceso a expertos forenses bien formados (lo que no constituye un servicio en nube estándar en el momento de redactar este documento).

También puede aportar un almacenamiento de registros más rentable a la vez que permite una actividad de registro más amplia sin afectar al rendimiento. El almacenamiento en nube de pago por uso aporta transparencia a sus gastos de almacenamiento de auditoría y facilita el proceso de ajuste a los requisitos futuros de los registros de auditoría. De este modo se incrementa la eficacia del proceso de identificación de incidentes de seguridad a medida que se producen (7).

- ACTUALIZACIONES Y OPCIONES POR DEFECTO MÁS PUNTUALES, EFECTIVAS Y EFICACES

Las imágenes por defecto de las máquinas virtuales y los módulos de software utilizados por los clientes pueden ser reforzados y actualizados previamente con los últimos parches y configuraciones de seguridad, conforme a procesos ajustados; las API del servicio en nube de la IaaS también permiten tomar imágenes de la

infraestructura virtual de manera frecuente y comparada con un punto inicial (por ejemplo, para garantizar que las normas del cortafuegos de software no se han modificado) (8). Las actualizaciones pueden aplicarse con mucha más rapidez en una plataforma homogénea que en los sistemas tradiciones de los clientes, que se apoyan en el modelo de parches. Por último, en los modelos de PaaS y SaaS, es más probable que las aplicaciones se hayan reforzado para ejecutarse fuera del entorno empresarial, lo cual hace más probable que sean más portátiles y robustas que el software empresarial equivalente (si lo hay). También es más probable que se sean actualizadas periódicamente y que sean parcheadas de manera centralizada, minimizando la ventana de vulnerabilidad.

- LA AUDITORÍA Y LOS ACUERDOS DE NIVEL DE SERVICIO OBLIGAN A GESTIONAR MEJOR EL RIESGO

La necesidad de cuantificar las sanciones de los distintos escenarios de riesgo en los Acuerdos de nivel de servicio y la posible repercusión de los incumplimientos de la seguridad sobre el renombre (véase Seguridad como diferenciador de mercado) motivan una auditoría interna y unos procedimientos de evaluación del riesgo más minuciosos que los que se llevarían a cabo en condiciones normales. La frecuencia de las auditorías impuestas a los proveedores en nube tiende a exponer los riesgos que, de otro modo, no habrían sido identificados, con lo que tiene el mismo efecto positivo.

- BENEFICIOS DE LA CONCENTRACIÓN DE RECURSOS

Aunque sin duda la concentración de recursos tiene desventajas para la seguridad (véase Riesgos), posee el beneficio evidente de abaratar la perimetrización y el control de acceso físicos (por recurso unitario) y permite una aplicación más sencilla y económica de una política de seguridad exhaustiva y un control sobre la gestión de datos, la administración de parches, la gestión de incidentes y los procesos de mantenimiento. Obviamente, la medida en que este ahorro se transmite a los clientes varía.

2.6.2 PRINCIPALES RIESGOS EN TÉRMINOS DE SEGURIDAD

Los tipos más importantes de riesgos específicos de la nube que identificamos en el presente documento son los siguientes:

- **PÉRDIDA DE GOBERNANZA:** al utilizar las infraestructuras en nube, el cliente necesariamente cede el control de una serie de cuestiones que pueden influir en la seguridad al proveedor en nube. Al mismo tiempo, puede ocurrir que los Acuerdos de nivel de servicio no incluyan la prestación de dichos servicios por parte del proveedor en nube, dejando así una laguna en las defensas de seguridad.
- **VINCULACIÓN:** la oferta actual en cuanto a herramientas, procedimientos o formatos de datos estandarizados o interfaces de servicio que puedan garantizar la portabilidad del servicio, de las aplicaciones y de los datos resulta escasa. Por este motivo, la migración del cliente de un proveedor a otro o la migración de datos y servicios de vuelta a un entorno de tecnologías de la información interno puede ser compleja. Ello introduce la dependencia de un proveedor en nube concreto para la prestación del servicio, especialmente si no está activada la portabilidad de los datos como aspecto más fundamental.
- **FALLO DE AISLAMIENTO:** la multiprestación y los recursos compartidos son características que definen la computación en nube. Esta categoría de riesgo abarca el fallo de los mecanismos que separan el almacenamiento, la memoria, el enrutamiento e incluso el renombre entre los distintos proveedores (por ejemplo, los denominados ataques «*guest hopping*». No obstante, debe considerarse que los ataques a los mecanismos de aislamiento de recursos (por ejemplo, contra hipervisores) todavía son menos numerosos, y su puesta en práctica para el atacante presenta una mayor dificultad en comparación con los ataques a los sistemas operativos tradicionales.
- **RIESGOS DE CUMPLIMIENTO:** la inversión en la obtención de la certificación (por ejemplo, requisitos reglamentarios o normativos del sector) puede verse amenazada por la migración a la nube:

- Si el proveedor en nube no puede demostrar su propio cumplimiento de los requisitos pertinentes
- Si el proveedor en nube no permite que el cliente en nube realice la auditoría.

En determinados casos, también significa que el uso de una infraestructura pública en nube implica que no pueden alcanzarse determinados niveles de cumplimiento

- **COMPROMISO DE INTERFAZ DE GESTIÓN:** las interfaces de gestión de cliente de un proveedor en nube público son accesibles a través de Internet, y canalizan el acceso a conjuntos de recursos más grandes (que los proveedores tradicionales de alojamiento), por lo que plantean un riesgo mayor, especialmente cuando son combinados con el acceso remoto y las vulnerabilidades del navegador de web.
- **PROTECCIÓN DE DATOS:** la computación en nube plantea varios riesgos relativos a la protección de datos tanto para clientes en nube como para proveedores en nube. En algunos casos, puede resultar difícil para el cliente en nube (en su función de controlador de datos) comprobar de manera eficaz las prácticas de gestión de datos del proveedor en nube, y en consecuencia, tener la certeza de que los datos son gestionados de conformidad con la ley. Este problema se ve exacerbado en los casos de transferencias múltiples de datos, por ejemplo, entre nubes federadas. Por otra parte, algunos proveedores en nube sí proporcionan información sobre sus prácticas de gestión de datos. Otros también ofrecen resúmenes de certificación sobre sus actividades de procesamiento y seguridad de datos y los controles de datos a que se someten, por ejemplo, la certificación SAS 70.
- **SUPRESIÓN DE DATOS INSEGURA O INCOMPLETA:** cuando se realiza una solicitud para suprimir un recurso en nube, al igual que sucede con la mayoría de sistemas operativos, en ocasiones el proceso no elimina definitivamente los datos. En ocasiones, la supresión adecuada o puntual de los datos también resulta imposible (o no deseable, desde la perspectiva del cliente), bien porque existen copias adicionales de datos almacenadas pero no disponibles o porque el disco que va a ser destruido también incluye datos de otros clientes. La

multiprestación y la reutilización de recursos de hardware representan un riesgo mayor para el cliente que la opción del hardware dedicado.

- **MIEMBRO MALICIOSO:** aunque no suelen producirse habitualmente, los daños causados por miembros maliciosos son, con frecuencia, mucho más perjudiciales. Las arquitecturas en nube necesitan ciertas funciones cuyo perfil de riesgo es muy elevado. Algunos ejemplos son los administradores de sistemas de proveedores en nube y los proveedores de servicios de seguridad gestionada.
- **NB:** los riesgos enumerados anteriormente no siguen un orden de criticidad concreto, sino que simplemente constituyen diez de los riesgos más importantes de la computación en nube identificados durante la evaluación. Los riesgos del uso de la computación en nube deben ser comparados con los riesgos derivados de mantener las soluciones tradicionales, como los modelos de sobremesa. Para facilitar este proceso, hemos incluido en el documento principal estimaciones de los riesgos relativos comparados con un entorno tradicional típico.

Adviértase que a menudo es posible, y en algunos casos recomendable, que el cliente en nube transfiera el riesgo al proveedor en nube; *sin embargo, no todos los riesgos pueden ser transferidos*: Si un riesgo provoca el fracaso de un negocio, perjuicios graves al renombre del mismo o consecuencias legales, es muy difícil, y en ocasiones, imposible, que un tercero compense estos daños. En última instancia, puede subcontratar la responsabilidad, pero no puede subcontratar la obligación de rendir cuentas.

2.6.3 REQUERIMIENTOS NECESARIOS PARA UN BUEN SERVICIO DE SEGURIDAD EN LA NUBE.

En esta sección se hablará de los lo que las empresas deben tomar en cuenta para poder adquirir servicios de seguridad en la nube sin importar la empresa que le brinde el servicio.

2.6.3.1 SLA (Service Level Agreement)

Un SLA o Acuerdo de Nivel de Servicio por sus siglas en inglés (Service Level Agreement), es simplemente un documento que describe el nivel de servicio esperado por un cliente de un proveedor, esclareciendo las métricas por las cuales el servicio es medido, y la remediación o sanciones, si es que existen, si los niveles de servicio acordados no son alcanzados. Usualmente, los SLA existen entre compañías y proveedores externos, pero también tienden a existir entre dos departamentos dentro de una compañía en específico. (Greiner & Gibbons Paul, 2009)

¿Por qué son necesarios los SLAs?

Un SLA reúne información sobre todos los servicios contratados y su fiabilidad acordada en un único documento. Se establecen claramente métricas, responsabilidades y expectativas por lo que en caso de problemas con el servicio, ninguna de las partes puede alegar ignorancia. Esto asegura que ambos lados tienen la misma comprensión de los requisitos del servicio contratado.

Cualquier contrato significativo sin un SLA asociado (revisado por un abogado) está abierto a una interpretación errónea deliberada o inadvertida. El SLA protege a ambas partes en el acuerdo.

El SLA no sólo debe incluir una descripción de los servicios que se prestarán y sus niveles de servicio esperados, sino también las métricas por las que se miden los servicios, las funciones y responsabilidades de cada parte, y los recursos y / o sanciones por incumplimiento.

La mayoría de los proveedores de servicios mantienen estadísticas disponibles a sus clientes, a menudo en un portal Web. Allí, los clientes pueden comprobar si se están cumpliendo los SLA, y si están autorizados para dar servicio a los créditos u otras sanciones como se establecen en el SLA. (Greiner & Gibbons Paul, 2009)

Según (Greiner & Gibbons Paul) dependiendo del servicio, los tipos de métricas para monitorear un SLA pueden incluir:

La disponibilidad del servicio: La cantidad de tiempo que el servicio está disponible para su uso. Esto se puede medir por franja horaria, con, por ejemplo, el 99,5% de disponibilidad requerido entre las horas de 8 am y las 6 pm. Las operaciones de comercio electrónico suelen tener SLAs extremadamente agresivos en todo momento; 99,999% el tiempo de actividad es un requisito, no es raro para un sitio que genera millones de dólares por hora.

Las tasas de defectos: Conteos o porcentajes de errores en los entregables principales. Fallas de producción, tales como copias de seguridad y restauraciones incompletas, errores de codificación, y el incumplimiento de plazos se pueden incluir en esta categoría.

Calidad técnica: En el desarrollo de aplicaciones externalizadas, la medición de la calidad técnica de las herramientas de análisis comerciales que analizan factores como el tamaño del programa y los defectos de codificación.

Seguridad: En estos híper-regulados tiempos, las brechas de seguridad de aplicaciones y de red pueden ser costosas. La medición de las medidas de seguridad controlables tales como actualizaciones de antivirus y parches es clave para demostrar se tomaron todas las medidas preventivas razonables, en caso de un incidente.

2.6.3.2 Sistema de Soporte de varios niveles o Escalabilidad de Soporte.

Un sistema soporte de varios niveles, las habilidades de los técnicos se clasifica. Los técnicos altamente calificados se asignan para abordar los problemas más difíciles, mientras que los técnicos de la media especializada manejan los más fáciles.

El soporte técnico a menudo se subdivide en niveles o capas. Una estructura de soporte común tiene tres niveles, pero se puede aumentar o disminuir dependiendo de la gama de dificultades en que la empresa quiera dividir las preocupaciones. Según (Global, 2013) un sistema de soporte de tres niveles se manejaría de la siguiente manera:

Nivel 1

Nivel 1 es como su primer nivel de defensa frente a una oleada de personas que llaman. En el Nivel 1 los agentes de apoyo son aquellas que solicitan información de la persona que llama, documentan el tema en cuestión y suelen asignar códigos de seguimiento para garantizar la calidad. Los agentes tienen conocimiento para solucionar problemas básicos y repetitivos, navegación en línea y software de reparación simple. Si un agente de nivel 1 no puede resolver el problema, la llamada se retransmite a un nivel superior para que los agentes con las habilidades y los conocimientos adecuados pueden resolver el problema.

Nivel 2

Cuando una llamada se ha escalado hasta el Nivel 2, el agente examina las medidas adoptadas por el agente anterior para eliminar otros arreglos simples. Los agentes de Nivel 2 suelen ser analistas de soporte con más experiencia que han tenido al menos 3-8 años de servicio de soporte de TI.

Nivel 3

Nivel 3 se compone de ingenieros de alto nivel. Analistas de Nivel 3 suelen ser expertos en la materia de la industria de TI o un campo en particular. Los problemas que se escalan al Nivel 3 son raros, sin embargo, implican el dominio del producto o software con el fin de resolver el problema. La mayoría de las empresas requieren que los agentes de Nivel 3 se certificarán con acreditaciones como CCNA, MCSE o CCNP.

2.6.3.3 Contratos de Confidencialidad y No Divulgación.

Un NDA (Non-Disclosure Agreement) o Contrato de confidencialidad y no divulgación en su forma más básica, es un contrato de cumplimiento legal que crea una relación de confianza entre una persona que tiene algún tipo de secreto comercial y una persona a la que se dará a conocer el secreto. (Rocket Lawyer, 2014)

Los acuerdos de confidencialidad por lo general tienen tres funciones principales:

Proteger la información sensible: Al firmar un acuerdo de confidencialidad, los participantes se comprometen a no divulgar o entregar información compartida con ellos por las otras personas involucradas. Si la información se filtró, el perjudicado puede reclamar incumplimiento de contrato.

En el caso de nuevos productos o desarrollo del concepto, un acuerdo de confidencialidad puede ayudar al inventor a mantener los derechos de patente: En muchos casos, la divulgación pública de un nuevo invento puede anular los derechos de patente. Un NDA redactado correctamente puede ayudar al creador original a mantener los derechos sobre un producto o idea.

Los acuerdos de confidencialidad y NDA delinean expresamente qué información es privada y lo que es juego limpio: En muchos casos, el acuerdo sirve como un documento que clasifica la información exclusiva y confidencial.

El tipo de información cubierta por un acuerdo de confidencialidad es prácticamente ilimitada. De hecho, cualquier conocimiento intercambiado entre los involucrados puede considerarse confidencial. Piense en los resultados de pruebas, listas de clientes, software, contraseñas, las especificaciones del sistema y otros datos. Si bien esta lista no es exhaustiva, puede ayudarle a pensar de otras instancias de información protegida.

Según (Rocket Lawyer, 2014) independientemente de su función o la información que protege, un NDA deben contener algunas piezas específicas: Definiciones y exclusiones de la información confidencial, obligaciones de todas las personas involucradas o partidos, y períodos de tiempo.

Definiciones de información confidencial explican las categorías o tipos de información incluidos en el acuerdo. Este elemento específico sirve para establecer las reglas del contrato sin llegar a la liberación de la información precisa. Por ejemplo, un acuerdo de confidencialidad para boutique de ropa de un diseñador exclusivo podría incluir una declaración como esta: "La información confidencial incluye listas de clientes y el historial de compras, información crediticia y financiera, procesos innovadores, el inventario y las cifras de ventas."

Además, NDA mencionan expresamente que la persona que recibe la información debe mantenerlo en secreto y limitar su uso. Esto significa que no se puede violar el acuerdo, animar a otros a violar, o permitir que otras personas accedan a la información confidencial a través de métodos inadecuados o no convencionales. Por ejemplo, si un diseñador de una empresa de informática deja un prototipo de aparato en un bar donde se descubrió por un reportero de tecnología, el diseñador probablemente estaría en violación del contrato NDA que firmó cuando aceptó el trabajo.

Los períodos de tiempo también son comúnmente tratados en acuerdos de confidencialidad y por lo general requieren que la parte que recibe la información resguarde silencio respecto a esta por un número determinado de años. Esta información específica suele ser objeto de negociación.

2.6.3.4 Mantenimiento preventivo y correctivo

Mantenimiento preventivo

Acción eficaz para mejorar aspectos operativos relevantes de un establecimiento tales como funcionalidad, seguridad, productividad, confort, imagen corporativa, salubridad e higiene. El mantenimiento debe ser tanto periódico como permanente, preventivo y correctivo. El mantenimiento es la segunda rama de la conservación y se refiere a los trabajos que son necesarios hacer con objeto de proporcionar un servicio de calidad estipulada (Unidad Técnica, 2009).

Mantenimiento correctivo

Acción de carácter puntual a raíz del uso, agotamiento de la vida útil u otros factores externos, de componentes, partes, piezas, materiales y en general, de elementos que constituyen la infraestructura o planta física, permitiendo su recuperación, restauración o renovación, sin agregarle valor al establecimiento. Es la actividad humana desarrollada en los recursos físicos de una empresa, cuando a consecuencia de una falla han dejado

de proporcionar la calidad de servicio esperada (Unidad Técnica, 2009). Este tipo de mantenimiento de divide en dos ramas:

- Correctivo urgente

El mantenimiento correctivo urgente se refiere a las actividades que se realizan en forma inmediata, debido a que algún equipo proporciona servicio vital ha dejado de hacerlo, por cualquier causa, y tenemos que actuar en forma urgente y, en el mejor de los casos, bajo un plan contingente.

Las labores que en este caso deben realizarse, tienen por objeto la recuperación inmediata de la calidad de servicio; es decir, que esta se coloque dentro de los limites esperados por medio de arreglos provisionales, así, el personal de conservación debe efectuar solamente trabajos indispensables, evitando arreglar otros elementos de la maquina o hacer otro trabajo adicional, que quite tiempo para volverla a poner en funcionamiento con una adecuada fiabilidad –que permite la atención complementaria cuando el mencionado servicio ya no se requiera o la importancia de este sea menor y, por lo tanto, al ejecutar estos trabajos se reduzcan las perdidas.

- Correctivo programable

El mantenimiento correctivo programable se refiere a las actividades que se desarrollan en los equipos o maquinas que están proporcionando un servicio y este, aunque necesario, no es indispensable para dar una buena calidad de servicio, por lo que es mejor programar su atención, por cuestiones económicas; de esta forma, se puede compaginar estos trabajos con los programas de mantenimiento preventivo.

Los reportes de mantenimiento preventivo y correctivo se definen como el conjunto de acciones y tareas periódicas que se realizan a objeto específico con el fin de ayudar a optimizar su funcionamiento y prevenir fallos serios, prolongando así su vida útil. También consiste en la reparación de alguno de sus componente.

2.6.3.5 Plan de Continuidad del Negocio

Un Plan de Continuidad del Negocio o BCP por sus siglas en inglés (Business Continuity Plan), ofrece una restauración rápida y suave de las operaciones después de un evento perjudicial. La planificación de la continuidad del negocio es un componente importante de la Gestión de Riesgos. La planificación de la continuidad de negocios incluye el análisis de impacto de negocio, el desarrollo del plan de continuidad del negocio (BCP), las pruebas, la sensibilización, la formación, y mantenimiento. Un plan de continuidad de negocio se dirige a las acciones que deben tomarse antes, durante y después de un desastre. Un BCP explica en detalle qué, quién, cómo y cuándo. Se requiere una continua inversión de tiempo y recursos. Las interrupciones de las funciones de negocio pueden resultar de grandes desastres naturales como tornados, inundaciones, e incendios, o desastres causados por el hombre, como los ataques terroristas. Los trastornos más frecuentes son los menos sensacionalistas como fallas en los equipos, el robo y el sabotaje interno. La definición de un desastre, entonces, es cualquier incidente que causa una interrupción prolongada de las funciones de negocio.

Tradicionalmente, la planificación de recuperación de desastres se ha centrado en los sistemas informáticos. Debido a que funciones de misión crítica dependen inevitablemente de la tecnología y las telecomunicaciones redes, la rápida recuperación de estos es de poco valor si no se recuperan también las unidades de negocio operativas. Hoy, sin embargo, muchas aplicaciones críticas se han emigrado a ambientes más distribuidos y descentralizados con controles menos rígidos.

Al igual que con una póliza de seguro, se espera que un plan de continuidad de negocio nunca sea necesario para un desastre real. Tenga en cuenta que un BCP sin mantenimiento o actualización puede ser peor que no tener ningún plan. La capacidad de un organismo para recuperar los procesos de misión crítica, reanudar las operaciones, y finalmente, regresar a un ambiente de negocios normal puede ser considerada un activo importante. La planificación minuciosa de un BCP puede reducir la responsabilidad, la interrupción de las operaciones normales, la toma de decisiones durante un desastre y la pérdida financiera.

¿Qué es un BCP?

Un plan de recuperación es un manual con los procedimientos, las responsabilidades y la información crítica necesaria para ejecutar una recuperación. La recuperación de la pérdida de instalaciones, recursos de información, y personal clave cualificados es generalmente el método aceptado para la construcción de un plan de recuperación. Una premisa fundamental de un plan de continuidad de negocio de éxito es que el plan es desarrollado por quienes vayan a llevar a cabo la recuperación en caso de un real desastre. (Departamento de Recursos de IT del Estado de Texas, 2004)

BCP en la nube

Después de años en expectativa, la industria de TI, finalmente tuvo un duro despertar de esta primavera, que nos recuerda que las infraestructuras de cloud computing (en la nube) son vulnerables al mismo defecto genético que afecta a TI tradicionales operaciones de centros de datos: todo falla, tarde o temprano.

En marzo de 2011, un terremoto de 8.9 y posteriormente un tsunami causaron interrupciones generalizadas a fuentes de alimentación eléctrica y conectividad de red para centros de datos a través de Japón, causando que las empresas japonesas volviesen a diseñar sus estrategias tradicionales de recuperación de desastres. Varias semanas más tarde, el sistema EBS en uno de los centros de datos de Amazon EC2 en los EE.UU. tuvo un fallo debido a una actualización defectuosa de uno de sus Core Routers que causó una cascada de eventos como resultado, envió a cientos de clientes- incluyendo muchas compañías Web 2.0 tales como Foursquare y Reddit- a un arduo esfuerzo para reanudar los servicios. (Crandell, 2011)

Irónicamente, estos eventos también ponen de relieve cómo las infraestructuras en la nube, cuando se gestionan correctamente, realmente ofrecen capacidades sin precedentes para ofrecer alta disponibilidad, capacidad de recuperación y la continuidad del negocio en las operaciones de TI.

La protección de su organización desde el tiempo de inactividad no planificado depende ampliamente en la construcción de redundancia y diversidad directamente en sus sistemas de recuperación de desastres y continuidad del negocio. Sistemas de negocios

deben ser capaces de funcionar con un número de diferentes infraestructuras - ya se trate de nubes públicas como Amazon o Rackspace, o nubes privadas utilizando hardware tradicional en las instalaciones - y ser capaz de conmutar por error entre ellos de forma rápida y eficientemente como sea necesario. (Crandell, 2011)

A pesar de la interrupción de Amazon, las nubes públicas ahora proporcionan a las organizaciones una serie impresionante variedad de opciones para implementar la continuidad del negocio a un nivel de asequibilidad que simplemente no existía hace unos años. Considere esto: Ahora, desde mi portátil, puedo lanzar servidores en una docena de lugares diferentes de todo el mundo - incluyendo los EE.UU., Europa y Asia - por unos centavos por hora. Como resultado, puedo diseñar un sistema para mi negocio que puede soportar razonablemente cortes localizadas a un costo menor que antes era posible.

La clave está en el diseño de sus infraestructuras para la posibilidad de un fracaso. Werner Vogels, el CTO de Amazon, ha estado predicando esta religión durante muchos años, lo que sugiere la única manera de probar la verdadera solidez de un sistema es "tirar del enchufe" o desconectar el sistema de golpe. Netflix - en sí un importante usuario infraestructura cloud - ha creado un proceso que denomina "The Monkey Chaos" o el Mono del Caos, que mata al azar instancias y servicios que se ejecutan en servidores sólo para asegurarse de que el sistema en su conjunto sigue funcionando bien sin ellos. No es sorprendente que el funcionamiento general de Netflix vio poco impacto de la interrupción de AWS en el Este de Estados Unidos cuando ocurrió.

La implementación de sistemas resistentes a fallos no es fácil. ¿Cómo se puede mover rápidamente sus operaciones de una infraestructura a la siguiente cuando la presión está encendida y las campanas de alarma están sonando? ¿Cómo se diseña un sistema que no sólo permite que los nuevos recursos informáticos para comenzar a operar como parte de su servicio, sino que también se pliega en una copia actualizada de los datos en la que sus usuarios y clientes dependen?

DRP

Un plan de recuperación de desastres (DRP) es un proceso documentado o conjunto de procedimientos para recuperar y proteger el negocio de infraestructura de TI en el caso

de un desastre. Dicho plan, normalmente documentado en forma escrita, especifica los procedimientos de una organización debe seguir en el caso de un desastre. Se trata de "una declaración exhaustiva de acciones coherentes que deben tomarse antes, durante y después de un desastre".

La planificación de continuidad del negocio y recuperación ante desastres se pasan por alto con frecuencia, es evitado o demorado en el olvido. Cada año, muchos usuarios informan que ellos no tienen confianza en la capacidad de su organización para recuperarse tras el desastre. Ellos citan con frecuencia la falta de apoyo de la dirección, porque la planificación de BC / DR puede ser caro y no tiene un retorno de la inversión inmediato. A menudo se hace la comparación con la compra de seguros - invertir en algo que espero que nunca va a necesitar. Pero, no tiene que ser de esa manera.

La continuidad del negocio y la planificación de recuperación de desastres pueden y no deberían ser integradas con las operaciones del día a día. En los últimos años, la planificación de DR se ha vuelto más fácil y más asequible gracias a los avances en las tecnologías. Planificadores creativos están encontrando maneras de integrar la recuperación de desastres con otras operaciones esenciales para agilizar los procesos. (TechTarget, techtarget.com, 2012)

BIA

Análisis de impacto de negocio (BIA) es un componente esencial del plan de continuidad del negocio de una organización; que incluye un componente exploratorio para revelar cualquier vulnerabilidad, y un componente de planificación para desarrollar estrategias para minimizar el riesgo. El resultado del análisis es un informe de análisis de impacto en el negocio, que describe los riesgos potenciales específicos para la organización estudiada. Uno de los supuestos básicos detrás BIA es que todos los componentes de la organización depende de la continuidad del funcionamiento de todos los demás componentes, sino que algunos son más importantes que otros y requieren una mayor asignación de fondos a raíz de un desastre. (Rouse, 2005)

2.6.3.6 Redundancia y Automatización en la Nube

No existe una varita mágica, pero hay un planteamiento general que hace el trabajo: la combinación de redundancia en el diseño con la automatización en la nube de gestión de capa. El primer paso requiere la arquitectura de una solución que utiliza componentes que pueden soportar errores de nodos individuales, ya sean servidores, volúmenes de almacenamiento o centros de datos enteros. Cada componente (por ejemplo, en la capa de red, capa de aplicación, capa de datos) debe ser considerado de forma independiente, y diseñado con las realidades de la infraestructura del centro de datos y el ancho de banda de Internet, el costo y el rendimiento en mente. Las soluciones para un diseño sólido y resistente son casi tan numerosos y variados como son los componentes de software que utilizan. Por ejemplo, las bases de datos solo comprenden una amplia gama de enfoques y características de resistencia, incluidas las tecnologías de SQL, NoSQL, replicación, almacenamiento en caché, etc.

Pero el ingrediente secreto realmente viene en cómo se maneja su arquitectura ¿Qué partes del sistema puede responder automáticamente a un fallo, partes que pueden responder de forma semiautomática, y partes que no lo pueden hacer en lo absoluto? Para ser más específicos, si un recurso dado en la nube cae - ya sea un disco duro, un servidor, un dispositivo de red, una red SAN, o una región geográfica entera - cómo perfectamente se puede poner en marcha y mantener las operaciones en funcionamiento? Lo ideal sería, por supuesto, mientras más automatizado (o casi), mejor será su excelencia operativa.

Según Crandell (2011), alcanzar ese nivel de automatización requiere que su diseño y configuración del sistema sea fácilmente replicable. Los servidores, por ejemplo, tienen que tener la capacidad de volverse a desplegar de una manera rápida y predecible a través de diferentes infraestructuras de nube. Es esta automatización que ofrece a las organizaciones la flexibilidad “salva vidas” cuando ocurre una crisis.

Administración en la nube

Gestión de la nube significa todo el software y tecnologías diseñadas para el funcionamiento y el seguimiento de las aplicaciones, los datos y servicios que residen en la nube. Herramientas de gestión de la nube ayudan a asegurar que los recursos basados en cloud computing de la compañía están trabajando de manera óptima e interactúan correctamente con los usuarios y otros servicios.

Estrategias de gestión de las nubes

Estrategias de gestión de la nube suelen incluir numerosas tareas, como la supervisión del rendimiento (tiempos de respuesta, la latencia, el tiempo de actividad, etc.), la seguridad y el cumplimiento de la auditoría y la gestión, que inician y supervisan los planes de recuperación de desastres y de contingencia.

Las herramientas de gestión de la nube de una empresa tienen que ser tan flexible y escalable como su estrategia de cloud computing.

2.6.3.7 Métodos de Autenticación

Durante años, la autenticación de la empresa ha reducido a una sola palabra: contraseñas. Sin embargo, la aparición de cada vez más grandes tablas de arco iris para el descifrado de contraseñas y el robo de contraseñas terriblemente creativo a través de la ingeniería social significa que las organizaciones ya no pueden confiar en la autenticación basada en contraseñas solo. (Gamby, 2012)

En la era de la banca en línea y robo de identidad, lo que demuestra que usted es usted - y evitar que otras personas utilicen su identidad - es cada vez más importante. Algunos métodos de autenticación, como la contraseña, son fáciles de implementar. Otros, como la comprobación de las huellas dactilares de una persona, son mucho más precisos. Elegir el método de autenticación correcta depende de cómo se va a utilizar. (Ryan, 2012)

¿Qué es la autenticación?

Autenticación implica determinar si un usuario es, de hecho, quien él o ella dice ser. La autenticación puede llevarse a cabo mediante el uso de contraseñas de inicio de sesión, los sistemas de Single Sign-On (SSO), biometría, certificados digitales y una infraestructura de clave pública (PKI). (TechTarget, 2008)

La autenticación de usuarios es fundamental para asegurar la debida autorización y acceso a los sistemas y servicios, sobre todo porque las amenazas de robo de datos e información de seguridad son cada vez más avanzada. Aunque la autenticación no puede detener por completo el robo de información e identidad, podemos asegurarnos de que nuestros recursos están protegidos con varios métodos de autenticación.

Hay tres factores de autenticación para considerar: algo que usted sabe, por ejemplo, un ID de usuario y contraseña; algo que usted tiene, por ejemplo, una tarjeta inteligente; y algo que es, lo que se refiere a una característica física, como una huella digital que se verifica por medio de la tecnología biométrica. Estos factores se pueden usar solos, o se pueden combinar para construir una estrategia de autenticación más fuerte en lo que se conoce como de dos factores de autenticación o multifactorial.

A continuación se describen los métodos de autenticación más comunes según TechTarget (2008):

Contraseñas

Las contraseñas son el tipo más común de autenticación, pero también son inseguros. Este método funciona simplemente preguntando al usuario una contraseña secreta y la concesión de acceso si se proporciona la contraseña correcta. Las contraseñas son vulnerables porque las personas suelen elegir contraseñas débiles que son demasiado cortos y contienen palabras en el diccionario, lo que los hace susceptibles a ataques de fuerza bruta que van a través de posibles contraseñas débiles hasta que se encuentra una coincidencia. El uso de caracteres especiales y "frases de paso" - que son especialmente contraseñas largas - es un método más seguro. Listas de contraseñas, en el que cada contraseña sólo se utiliza una sola vez, aumentar la seguridad, pero la

molestia de generar nuevas contraseñas o el envío de forma segura de las contraseñas nuevas tanto para el usuario como para el servidor que hace que este método no sea práctico en muchas situaciones.

Respuesta de desafío

El método de desafío-respuesta utiliza contraseñas, pero la contraseña no se envía nunca. En lugar de ello, un centro de autenticación envía un número aleatorio para el usuario. El usuario responde entonces mediante la combinación de la contraseña con el número aleatorio y luego usando una función hash para crear el equivalente de una huella dactilar digital. El centro de autentificación, que conoce la contraseña, el número aleatorio y la función hash, es capaz de producir la misma huella y compararlas. Si coinciden, entonces el usuario está autenticado. Este sistema es seguro porque incluso si un atacante conoce el número y la función hash aleatoria usada, no es suficiente para calcular la contraseña.

Clave Pública

Cifrado de clave pública se basa en operaciones matemáticas que son fáciles de realizar, pero muy difícil de deshacer. Multiplicar números primos muy grandes es el ejemplo más común. Mientras multiplicándolos es fácil, si una segunda persona se les dio el producto, sería casi imposible entonces determinar qué dos números primos habían sido multiplicados entre sí. Estas funciones unidireccionales crear una clave pública y una clave privada. Cualquiera puede usar la clave pública para cifrar la información, que sólo puede ser descifrado con la clave privada. En el protocolo de autentificación de clave pública, el usuario A encripta un número aleatorio con la clave pública del usuario B. Usuario B descifra el número, lo cifra con la clave pública del usuario A y luego lo envía de vuelta. Es la capacidad del usuario B para descifrar el mensaje original que demuestra su identidad.

Biometría

Biometría, la medición directa de una característica física o de comportamiento, también se puede utilizar para la autenticación. Toma de huellas dactilares, pruebas de ADN y escáner de retina son algunos de los métodos biométricos más familiares, mientras que

las firmas manuscritas - uno de los más antiguos métodos de autenticación - pueden considerarse un método biométrico, también.

Mientras que la autenticación de factores múltiples puede ser difícil de implementar a nivel de infraestructura, (Schilling, 2014) dijo que es un proceso sencillo para los clientes de los principales proveedores de cloud hosting. Como control de seguridad, dijo que ofrece una barrera que desalienta hasta a los atacantes más sofisticados, por lo que la falta de información proporcionada al respecto por los proveedores es lo más frustrante para ellos.

Las contraseñas hay que cambiarlas con una cierta regularidad. Un 53% de los usuarios no cambian nunca la contraseña salvo que el sistema le obligue a ello cada cierto tiempo. Y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. P. ej.: pasar de “01Juitnx” a “02Juitnx”. (INTECO, 2013)

Criptografía

¿Qué es la criptografía?

Según la RAE:

Criptografía: Arte de escribir con clave secreta o de un modo enigmático.
Conocemos entonces a la Criptografía (derivado del griego Crypto, que significa "Oculto" y Graphos, "Escribir") como el estudio de las técnicas que se aplican, tanto a la ciencia como al arte, para poder alterar los caracteres del lenguaje en la transmisión de un mensaje.

Esta alteración lleva a cabo distintas técnicas que giran en torno a un Codificado o Cifrado (o bien su combinación de ambas), y tiene la única finalidad de que el mensaje que está siendo enviado no sea leído por otra persona que no sea el destinatario, haciéndose nada legible para quienes no han sido autorizados y no tienen la forma de poder descifrarlo.

La criptografía es la creación de técnicas para el cifrado de datos. Teniendo como objetivo conseguir la confidencialidad de los mensajes.

Existen tres tipos de criptografía, la simétrica, asimétrica e hibrida, a continuación se explica cada una:

Criptografía simétrica

La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad (diciéndola en alto, mandándola por correo electrónico u ordinario o haciendo una llamada telefónica). (Gutierrez, 2013)

Dentro de los algoritmos más conocidos se encuentran:

RC5: Realiza operaciones, suma modular y desplazamiento de bits; es un algoritmo que cifra en bloques de tamaño variable, cifra bloques de texto de 32, 64 y 128 bits. Para el tamaño dela clave se sugiere 128 bits, el número de vueltas van de la 0 a la 255 y tiene la estructura de red fiable.

AES: Es el estándar de encriptación avanzada, es un algoritmo de cifrado de 128, 192 y 256 de longitud de clave (Matriz 4*4).

BlowFish: Algoritmo de tipo Feistel, es una calve variable, cifra bloques de texto de 64 bits, el tamaño de la clave va de los 32 hasta los 448 bits; se generan 18 sub-claves de 32 bits y cuatro cajas-S de 8*32 bits, en total 4,168 bytes.

Criptografía asimétrica

La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca). (Gutierrez, 2013)

Cifrado de claves públicas

Diffie-Hellman: Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión. Siendo no autenticado, sin embargo provee las bases para varios protocolos autenticados. Su seguridad radica en la extrema dificultad demostrada, de calcular logaritmos discretos en un campo finito. (Perez, 2011)

RSA: Es un algoritmo asimétrico que cifra bloques, que utiliza una clave pública, la cual redistribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario. Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario y como una cadena de bits o bytes. Cuando se quiere enviar un mensaje, el emisor busca la clave pública de cifrado del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. (Perez, 2011)

Cifrado de claves privadas

DSA: Digital Signatura Algoritmo, en español algoritmo de firma digital. Es un estándar del gobierno federal de los Estados Unidos o FIPS para firmas digitales. Fue un algoritmo propuesto por el Instituto Nacional de Normas y Tecnologías de Estados Unidos para su uso en su Estándar de Firma Digital (DSS), Especificado en el FIPS 186. DSA se hizo público el 30 de agosto de 1991, este algoritmo como su nombre lo indica, sirve para firmar y no para cifrar información. Una desventaja de este algoritmo es que quiere mucho más tiempo de cómputo de RSA. (Perez, 2011)

IDEA: Trabaja con bloques de Texto de 64 bits, operando siempre con números de 64 bits usando operaciones como XOR y suma y multiplicación de enteros. El algoritmo de des encriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar. Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como Unix y en programas de cifrado de correo como PGP. (Perez, 2011)

Criptografía híbrida

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento. (Gutierrez, 2013)

- El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

2.6.3.8 Seguridad Perimetral

La Seguridad Perimetral o seguridad de la red es la estrategia y las disposiciones para garantizar la seguridad de sus activos y de todo el tráfico de red de una organización. La seguridad perimetral se manifiesta en una implementación de la política de seguridad, hardware y software (Palo Alto Networks, s.f.). A los efectos de esta discusión, el siguiente enfoque se adoptó en un esfuerzo para ver la seguridad de la red en su totalidad:

- Política
- Cumplimiento
- Auditoría

Política

La Política de Seguridad de TI es el principal documento de seguridad de la red. Su objetivo es describir las normas para garantizar la seguridad de los activos de la organización. Los empleados actuales utilizan varias herramientas y aplicaciones para realizar negocios de manera productiva. La política que es impulsada desde la cultura de la organización apoya a estas rutinas y se centra en la habilitación de seguridad de estas herramientas a sus empleados. Los procedimientos de ejecución y auditoría para

cualquier cumplimiento de la normativa se requiere una organización para cumplir deben ser trazadas en la política también. (Palo Alto Networks, s.f.)

Cumplimiento

La mayoría de las definiciones de seguridad de red se reducen al mecanismo de aplicación. Los intereses de las autoridades que analizan todos los flujos de tráfico de la red deben estar dirigidos a preservar la confidencialidad, integridad y disponibilidad de los sistemas y la información en la red. Según Palo Alto Networks estos tres principios componen la tríada CIA:

- Confidencialidad - consiste en la protección de los activos de las entidades no autorizadas
- Integridad - garantizar la modificación de los activos se maneja de una manera específica y autorizada
- Availability o Disponibilidad - un estado del sistema en el que los usuarios autorizados tengan acceso continuo a dichos activos.

La aplicación estricta de la CIA se esfuerza por ofrecer a los flujos de tráfico de la red. Esto comienza con una clasificación de los flujos de tráfico por aplicación, usuario y contenido. Todas las aplicaciones deben primero ser identificados por el servidor de seguridad independientemente del puerto, protocolo, táctica evasiva, o SSL. La identificación adecuada de la aplicación permite una total visibilidad del contenido que lleva. La administración de políticas puede ser simplificada mediante la identificación de aplicaciones y un seguimiento de su uso a una identidad de usuario al inspeccionar el contenido en todo momento por la preservación de la CIA.

El concepto de defensa en profundidad se observa como las mejores prácticas en seguridad de la red, la prescripción de la red para asegurarse en capas. Estas capas se aplican una variedad de controles de seguridad para tamizar a cabo amenazas tratando de entrar en la red:

- El control de acceso
- Identificación
- Autenticación
- Detección de malware
- Cifrado
- Filtrado de tipo de archivo
- Filtrado de URL
- El filtrado de contenidos

Estas capas se construyen a través de la implementación de firewalls, sistemas de prevención de intrusiones (IPS), antivirus y componentes de red como Routers de capa 3. Entre los componentes de la aplicación se encuentra el firewall o cortafuegos (un mecanismo de control de acceso) es el fundamento de la seguridad de la red. (Palo Alto Networks, s.f.)

Proporcionar CIA de los flujos de tráfico de la red era difícil de lograr con las tecnologías anteriores. Los firewalls tradicionales estaban plagados de controles que se basaban en el puerto / protocolo para identificar las aplicaciones y el supuesto de que la dirección IP equivale a una identidad usuarios.

El firewall de próxima generación conserva una misión de control de acceso, pero rediseña la tecnología; se observa todo el tráfico en todos los puertos, puede clasificar las aplicaciones y su contenido, y se identifican los empleados como los usuarios. Esto permite que los controles de acceso matizados suficiente para hacer cumplir la política de seguridad de TI a medida que se aplica a cada empleado de la organización, sin comprometer la seguridad.

Servicios adicionales para capas de seguridad de red para implementar una estrategia de defensa en profundidad han sido incorporados al modelo tradicional como componentes adicionales. Sistemas de prevención de intrusiones (IPS) y antivirus, por ejemplo, son herramientas eficaces para el contenido de la exploración y la prevención de ataques de malware. Sin embargo, las organizaciones deben tener cuidado con la

complejidad y el costo que los componentes adicionales pueden agregar a su seguridad de red, y lo más importante, no depender de estos componentes adicionales para hacer el trabajo básico del firewall.

Auditoría

El proceso de auditoría de seguridad de la red requiere que se revise de nuevo en las medidas de ejecución para determinar lo bien que se han alineado con la política de seguridad. La auditoría fomenta la mejora continua, al exigir a las organizaciones a reflexionar sobre la aplicación de su política sobre una base consistente. Esto le da a las organizaciones la oportunidad de ajustar su política y estrategia de aplicación en áreas de necesidad de desarrollo. (Palo Alto Networks, s.f.)

2.6.3.9 Certificaciones de Seguridad Informática conocidas

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. (ISO27001 Academy, 2014)

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:

Otras normas relacionadas con seguridad de la información

ISO/IEC 27002 proporciona directrices para la implementación de los controles indicados en ISO 27001. ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799-1. (ISO27001 Academy, 2014)

ISO/IEC 27004 proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO 27001 ya que explica cómo determinar si el SGSI ha alcanzado los objetivos.

ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO 27001 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación. ISO 27005 ha surgido de la norma británica BS 7799-3. (ISO27001 Academy, 2014)

ISO 22301 define los requerimientos para los sistemas de gestión de continuidad del negocio, se adapta muy bien con ISO 27001 porque el punto A.17 de esta última requiere la implementación de la continuidad del negocio aunque no proporciona demasiada información.

ISO 9001 define los requerimientos para los sistemas de gestión de calidad. Aunque a primera vista la gestión de calidad y la gestión de seguridad de la información no tienen mucho en común, lo cierto es que aproximadamente el 25% de los requisitos de ISO 27001 y de ISO 9001 son los mismos: control de documentos, auditoría interna, revisión por parte de la dirección, medidas correctivas, definición de objetivos y gestión de competencias. Esto quiere decir que si una empresa ha implementado ISO 9001 le resultará mucho más sencillo implementar ISO 27001. (ISO27001 Academy, 2014)

SAS 70

Declaración sobre Normas de Auditoría o Statement on Auditing Standards (SAS) No. 70, Organizaciones de Servicios, era una norma de auditoría ampliamente reconocida

desarrollado por el Instituto Americano de Contadores Públicos Certificados (AICPA). El examen de un auditor del servicio realizado de acuerdo con el SAS No. 70 (también comúnmente se conoce como un "Auditoría SAS 70") representa que una organización de servicio ha sido examinada a fondo a través de sus objetivos de control y actividades de control, que a menudo incluyen controles sobre tecnología de la información y los procesos relacionados. (SAS70, 2014)

CAPITULO III. METODOLOGÍA

En este capítulo se presentará la estrategia que se llevó a cabo en dicha investigación, el enfoque y método, las técnicas y las herramientas que se utilizaron para obtener la información necesaria y contestar los objetivos del estudio.

En este apartado se enunciará el enfoque que se le dio a la investigación así como los métodos a utilizar para fundamentar las variables que se desean verificar.

La investigación tiene un alcance descriptivo. Su valor consiste en mostrar diferentes ángulos y dimensiones de la seguridad de servicios en la nube, así como también realizar una recolección de información de parte de usuarios de servicios en la nube como de una empresa proveedora del servicio.

3.1 CONGRUENCIA METODOLOGICA

Esta sección ayuda corroborar la relación que existe entre las partes del planteamiento del problema y la metodología a usar.

3.1.1 MATRIZ METODOLOGÍCA

En este apartado se muestra la interdependencia de las variables de esta propuesta y cómo las mismas se relacionan con cada pregunta de investigación que se desea responder en el estudio.

Esta matriz permite que se demuestre que todas las variables implicadas en dicha propuesta son necesarias para la resolución exitosa de la misma.

Tabla 2: Matriz Metodológica

Título	Problema	Pregunta de Investigación	Objetivo		Variables
			General	Especifico	
Propuesta Técnica para empresas que están adquiriendo servicios en la nube	Condiciones necesarias para poder contar con un apropiado servicio de seguridad en la nube	¿Qué factores son considerados importantes a la hora de establecer términos y condiciones de servicio al contratar seguridad en la nube?	Determinar una estrategia integrada de seguridad para una arquitectura de servicios en la nube pública según los estándares actuales de los fabricantes líderes en seguridad.	Describir estándares de estrategias de seguridad de empresas líderes para servicios en la nube pública.	V1. Términos y condiciones de servicio
		¿Qué factores son considerados importantes para la seguridad de accesos y protección de datos al contratar seguridad en la nube?		Identificar estrategias de seguridad para nubes públicas utilizadas actualmente por empresas ubicadas en la ciudad de Tegucigalpa	V2. Seguridad de accesos y la protección de los datos
		¿Qué factores son considerados importantes para el establecimiento de la administración y propiedad de los datos al contratar seguridad en la nube?		Evaluar las estrategias de seguridad para nubes públicas en uso actualmente por las empresas nacionales según la determinación de los estándares de empresas líderes.	V3.La administración de los servicios y la propiedad de los datos

		¿Qué factores son considerados importantes al evaluar la seguridad perimetral y las certificaciones de empresas que ofrecen seguridad en la nube?		Construir estrategias integradas de seguridad para nubes públicas basadas en la evaluación aplicada a las estrategias de seguridad.	V4. Seguridad perimetral y certificaciones

3.1.2 DEFINICIÓN OPERACIONAL DE VARIABLES

En esta sección se muestra un análisis general en forma de diagrama de la interrelación de las variables de esta propuesta. También se puede encontrar la descripción específica de las variables involucradas.

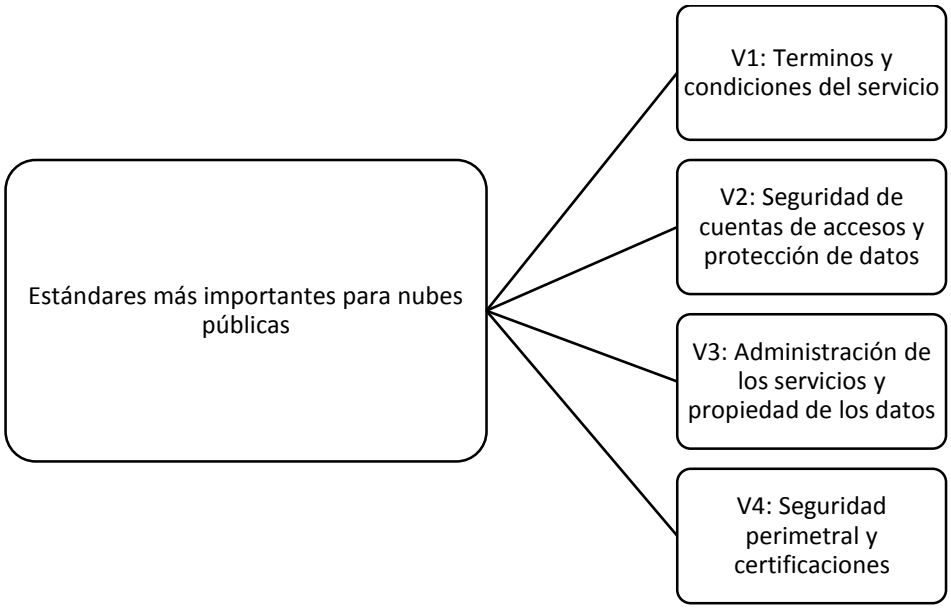

Figura 4: Diagrama de variables

Después de presentar el detalle de las variables que se muestran en la figura 4 se define cada tipo de variable.

Tabla 3: Variable 1

V1. Términos y condiciones de servicio	
Variable	Numérica
Enfoque	Cuantitativa
Escala	Nominal
Atributos	Ninguno
Características	Posee categorías a las que se asigna un nombre sin que exista ningún orden implícito entre ellas.
Tipo	Discreta (Porque provendría de un conteo)

Tabla 4: Variable 2

V3. Seguridad de accesos y la protección de los datos	
Variable	Numérica
Enfoque	Cuantitativa
Escala	Nominal
Atributos	Ninguno
Características	Posee categorías a las que se asigna un nombre sin que exista ningún orden implícito entre ellas.
Tipo	Discreta (Porque provendría de un conteo)

Tabla 5: Variable 3

V4. Administración de los servicios y la propiedad de los datos	
Variable	Numérica
Enfoque	Cuantitativa
Escala	Nominal
Atributos	Ninguno
Características	Posee categorías a las que se asigna un nombre sin que exista ningún orden implícito entre ellas.
Tipo	Discreta (Porque provendría de un conteo)

Tabla 6: Variable 4

V5. Seguridad perimetral y certificaciones	
Variable	Numérica
Enfoque	Cuantitativa
Escala	Nominal
Atributos	Ninguno
Características	Posee categorías a las que se asigna un nombre sin que exista ningún orden implícito entre ellas.
Tipo	Discreta (Porque provendría de un conteo)

Tabla 7: Operacionalización de variables

Variable	Definición		Dimensiones	Indicador	Items	Unidades (Categóricas)	Escala
	Conceptual	**Operacional**					
Términos y condiciones del Servicio, Continuidad del Servicio y Políticas de privacidad.	Un acuerdo de nivel de servicio o ANS es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. Un plan de continuidad del negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.	Revisión de existencia de documentos de servicio, contratos, planes de continuidad y políticas.	Seguridad Informática. Legal.	Existe o no la documentación necesaria.	• SLA • Escalabilidad de Niveles de Soporte (telefónico) • Uso secundario de información. • Cómo terminar el contrato y asegurar la eliminación total de los datos. • Cómo son almacenados y protegidos los datos por el Proveedor de Servicio. • El Proveedor de Servicio envía reportes de mantenimiento y resolución de incidentes. • Evaluar el impacto potencial en una interrupción del servicio. • BCP. (Business Continuity Plan). • Divulgación por parte del Proveedor de Servicio de garantías de seguridad en su Infraestructura (Firewalls, IPS,	Dicotómicas (si o no)	Nominal

					NAC, Sistemas de Acceso, etc). • Proveedor de Servicio de Internet de respaldo (por diferente ruta/hilo). • Reputación y Estabilidad Económica del Proveedor de Servicio.		
Seguridad de Cuentas de Acceso y Protección de datos	En el contexto de la informática, un usuario es una persona que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc, dichos usuarios deberán identificarse. Para que uno pueda identificarse, el usuario necesita una cuenta (una cuenta de usuario) y un usuario, en la mayoría de los casos asociados a una contraseña. Los usuarios utilizan una interfaz de usuario para acceder a los sistemas, el proceso de identificación es conocido como identificación de usuario o acceso del usuario al sistema.	Observación y preguntas al encargado de Seguridad de IT sobre existencia de documentación que compruebe la aplicación de prácticas de protección adecuadas.	Seguridad Informática. Seguridad de acceso físico. Derecho Informático	Niveles de autenticación. Existencia de políticas de seguridad para accesos. Existe o no la documentación necesaria, métodos de cifrado, niveles de criticidad de datos almacenados.	• Fuerte método de autenticación, preferiblemente de dos factores. (Ej. certificado digital y password). • Contraseñas con alto nivel de seguridad. • Cambios de contraseñas periódicos. • Cambio y deshabilitación de usuarios inmediatos con cambios de staff. • Políticas de Seguridad para Usuarios (compartición de credenciales, etc.). • Monitoreo Proactivo. • Implementación de un fuerte control de acceso en API. • Mantener una bitácora de qué tipo de Datos son los que	Categóricas (Autenticación de un factor, dos factores o más) Dicotómicas (Si o no)	Nominal

	Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.				se almacenan en el servicio en la nube. • Conocer la ubicación (junto con su jurisdicción) de todas las copias de datos existentes, y conocer si esto conlleva a impactos de procesos de seguridad, cumplimientos regulatorios o diferencias legales. • Conocer el nivel de criticidad de los datos que se almacenan en la nube. • Mantener un respaldo de los datos en caso de desastre. • Confidencialidad del Proveedor para proteger los datos. • Métodos de cifrado en comunicaciones. • Cifrado en Datos Almacenados (Data at Rest).		
Administración de Servicios en la nube y Propiedad de los Datos.		Observación y preguntas al encargado de IT de la empresa y	Seguridad Informática. Propiedad Intelectual. Legal		• Política de seguridad para acceso a los servicios en la nube. • Selección de personal de confianza para	Categóricas (Autenticación de un factor, dos factores o más)	Nominal

		proveedor del servicio.			administrar la solución en la nube. • Revisiones periódicas sobre derechos de acceso a los datos en la nube. • Entrenamiento de concientización acerca de la seguridad del servicio en la nube. • Procesos de registro y validación inicial estrictos para el uso de los servicios. • Derechos de uso de los datos, divulgación y uso público. • Propiedad Intelectual. • Posibilidad de mover o transferir los datos a otro Proveedor de Servicio de ser necesario. • Borrado permanente de Datos, incluyendo respaldos cuando se termina el contrato.	Dicotómicas (Si o no)	
Seguridad Perimetral e Infraestructura de Red y Certificaciones		Observación y preguntas a encargados de IT		Documentación de respaldo Equipos de seguridad	• Firewall • IPS • Método de cifrado de comunicaciones (SSL, IPSec, SSH, etc).	Categóricas (Autenticación de un factor,	Nominal

de Cumplimiento.		Comprobantes de certificado			• Si el Proveedor de Servicio cuenta y puede demostrar la existencia de un certificado independiente de seguridad de la información. (ISO/IEC 27001, SAS70)	dos factores o más) Dicotómicas (Si o no)	

En esta sección se estableció la definición conceptual y operacional de las variables, así como sus dimensiones, indicadores, ítems, unidades categóricas y escala.

Después de analizar la congruencia de esta propuesta es necesario establecer la hipótesis que regirá el norte de este documento.

3.2 ENFOQUES Y METODOS DE INVESTIGACIÓN

Para alcanzar los objetivos propuestos de investigación se utilizaron como métodos la investigación de tipo bibliográfico e investigación empírica.

Para efectuar la revisión de la literatura se utilizaron diferentes fuentes y se efectuó una revisión bibliográfica de informes especializados, libros, folletos, revistas científicas, boletines, tesis, páginas de internet y otros tipos de información escrita disponible para tal fin.

En cuanto a la investigación empírica se aplicaron dos encuestas, una a empresas que cuenten con servicios en la nube actualmente, y otra a una empresa proveedora de servicios en la nube, también se aplicó una ficha de evaluación a la empresa proveedora del servicio, todos estos instrumentos será aplicado a empresas que tengan oficinas ubicadas en la ciudad de Tegucigalpa con el fin de visualizar y describir los riesgos de seguridad en la nube con su respectivo nivel de impacto en los negocios en caso de que estos ocurran.

3.3 DISEÑO DE LA INVESTIGACIÓN

Este apartado describe la forma en que se aplicó la investigación y los instrumentos que se utilizaran para resolver las interrogantes planteadas.

Se desarrolló un diseño de investigación no experimental porque no se manipula ninguna variable para observar el comportamiento de otra variable, transeccional de tipo descriptivo porque se planea evaluar los riesgos de seguridad para servicios en la nube en un momento dado (ocurre una recolección de datos única).

3.4 POBLACIÓN Y MUESTRA

La población universal de este estudio son todas las empresas con oficinas en la ciudad de Tegucigalpa que cuentan actualmente con servicios en la nube y que existan dentro de las bases de datos de un reconocido proveedor de servicios en la nube del país.

Dentro de esta base de datos se eligió una cantidad considerable de empresas al azar para aplicar el instrumento destinado a usuarios finales de servicios en la nube.

Se utilizó una muestra no probabilística o dirigida, debido a la naturaleza y las especificaciones del universo o población:

- Empresas que utilicen servicios informáticos en la nube dentro de la base de datos de clientes de un proveedor de servicios en la nube del país.
- Que tengan oficinas ubicadas en la ciudad de Tegucigalpa.

La propuesta tiene las siguientes limitaciones:

- La encuesta se realizó sólo a empresas con oficinas ubicadas en la ciudad de Tegucigalpa, ya sean clientes de las empresas donde trabajamos o donde logremos contactar a un encargado del departamento de informática

3.5 TÉCNICAS E INSTRUMENTOS UTILIZADOS

Para la presente investigación se utilizó la técnica de encuesta, usando como instrumento un cuestionario prediseñado.

El contenido de los instrumentos se basó en responder las variables elegidas y planteadas en la investigación, sintetizando el contenido del Marco Teórico de nuestra tesis y luego se utilizaron las siguientes herramientas para poder analizar los datos y dar conclusiones.

- Microsoft Office Excel 2013.
- SPSS (Statistical Product and Service Solutions).
- Encuestas vía web.

CAPITULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se plantean los resultados correspondientes al análisis de los datos obtenidos producto de la información recabada a través de la encuesta que se realizó a los usuarios y proveedores de servicios en la nube. La información descrita en este análisis está alineada a los objetivos y preguntas planteadas en la investigación.

La información analizada en esta investigación fue de tipo exploratoria descriptiva, ya que permitió establecer el nivel de conocimiento sobre servicios en la nube que poseen los usuarios y sobre todo el conocimiento que poseen en cuanto a los parámetros necesarios para poder tomar decisiones con respecto a la seguridad en la nube. El nivel de conocimiento se reflejó en las respuestas brindadas en la encuesta y a continuación se plantea el análisis de tales resultados.

4.1 ANÁLISIS DE RESULTADOS

En este apartado se describe a detalle los datos obtenidos para cada variable de estudio descritas en la sección 1.6 de este informe.

Se aplicaron 25 encuestas a los usuarios de servicios en la nube y 2 encuestas a dos de tres empresas de servicios en la nube actualmente en funcionamiento en el país, esto con el fin de poder contestar las respuestas de esta investigación.

Se diseñó un cuestionario con preguntas cerradas, en su mayoría, para usuarios y otro para los proveedores y se distribuyó su aplicación por medio de la herramienta Google Docs.

A continuación se presentan los resultados de cada una de las variables que se definieron con anterioridad y se espera permitan tomar decisiones sobre el total de la población de los clientes.

4.1.1 VARIABLE 1: ESTÁNDARES MÁS IMPORTANTES PARA UNA NUBE PÚBLICA.

Para evaluar esta variable se consultó a los usuarios en la nube que tipo de arquitectura utilizaban y los datos recopilados se presentan en la figura siguiente.

Figura 6: Estándares

En esta figura se demuestra que los proveedores de servicios en la nube le están dando mayor importancia a estándares como lo son los SLA, la seguridad de cuentas de acceso y la seguridad perimetral e infraestructura de red, ya que de los 3 proveedores encuestados estos fueron los ITEMS en los que ellos concuerdan en que están cubriendo a la hora de brindar los servicios en la nube

4.1.2 VARIABLE 2: TÉRMINOS Y CONDICIONES DE SERVICIO

Para evaluar esta variable se consultó a los usuarios sobre requerimientos de SLA y los datos recopilados se presentan en las tablas y figuras siguientes.

a) El proveedor del servicio ofrece el directorio telefónico para el nivel de soporte técnico requerido.

Figura 6: Directorio Telefónico para Usuarios

b) Cuenta de este directorio telefónico ofrece números alternos de solución, si no se resuelve en el tiempo establecido.

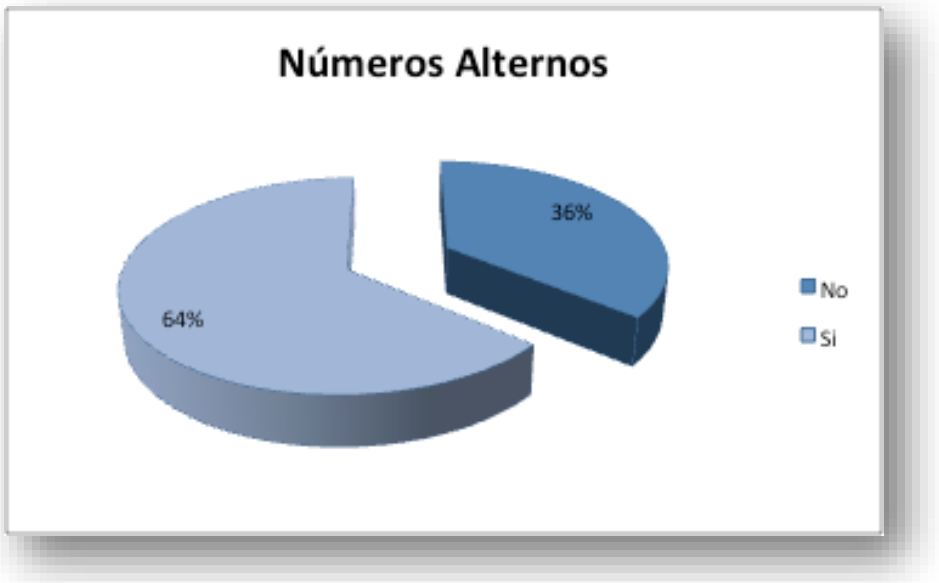

Figura 7: Números Alternos

En los dos gráficos anteriores se puede observar que el 88% de los clientes que poseen servicios en la nube pueden llamar un número específico para solicitar soporte en el momento que sus servicios en la nube presenten problemas pero también se observa que solamente un 64% de los proveedores ofrecen números alternos en el caso de que la línea principal no se encuentre disponible. Con estos datos y según nuestra experiencia es más probable que los usuarios se inclinen por proveedores que ofrezcan mayores alternativas de comunicación a la hora que se presente la falla.

c) ¿Qué tipo de informes recibe de parte del proveedor de servicio?

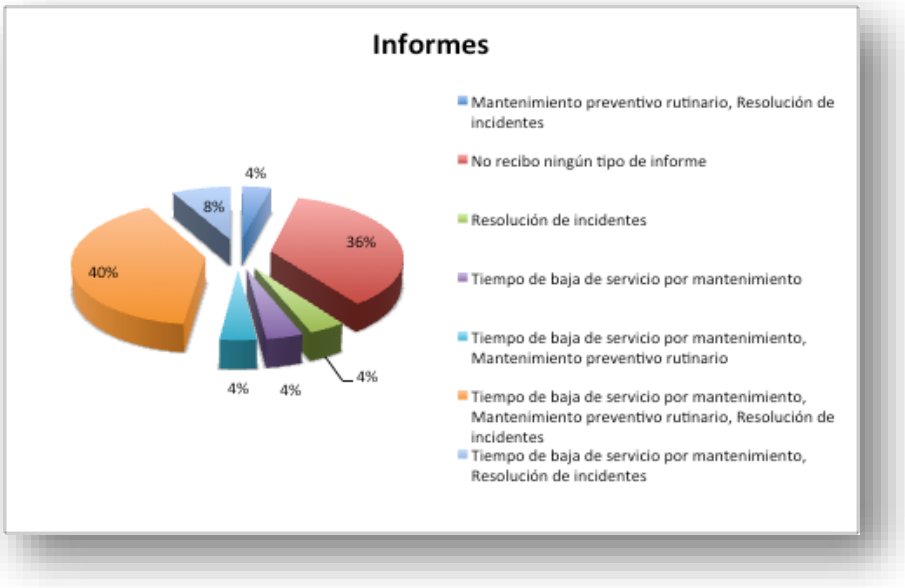

Figura 8: Tipos de Informes recibidos por el Proveedor

En este gráfico se muestra que solamente el 40% de los clientes recibe reportes de tiempo de baja de servicio por mantenimiento y resolución de incidentes, pero lo alarmante es que también se nota que el 36% de los usuarios afirma que no recibe informes por parte del proveedor lo cual a nuestro punto de vista es una debilidad para el usuario ya que no cuenta con un respaldo que le permita hacer valer sus derechos establecidos en el SLA.

También al no recibir reportes el cliente se encuentra a ciegas en cuanto a los mantenimientos de su servicio lo que le puede ocasionar perdidas de información y sobre todo tiempo valioso de trabajo para sus empleados.

d) Nivel de impacto potencial en su empresa, cuando el proveedor del servicio o causas externas provocan la interrupción del servicio.

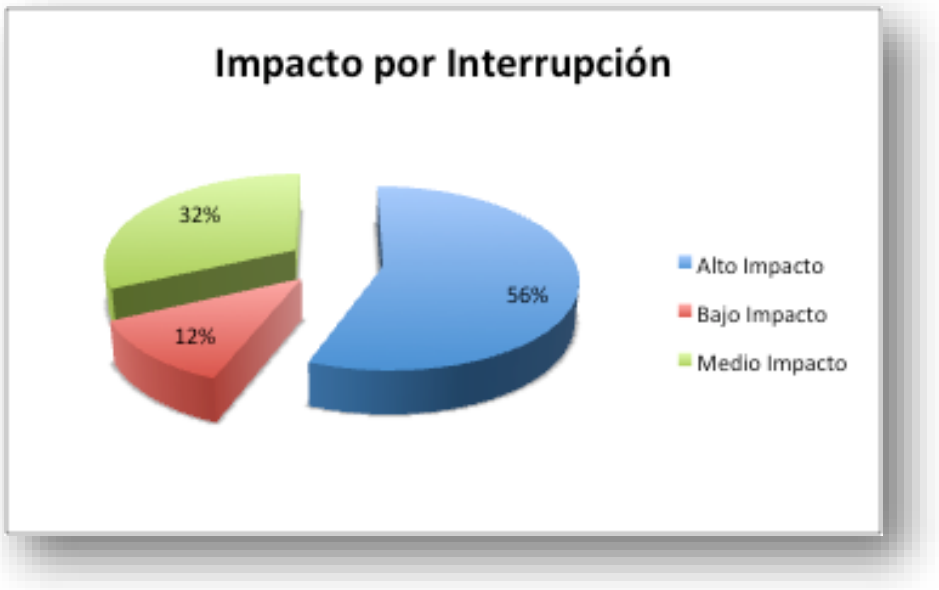

Figura 9: Impacto producido por interrupción del Proveedor

En este momento se puede concluir que el 56% de los usuarios de servicios en la nube considera que la información que aloja en la nube es de vital importancia y una interrupción por parte del proveedor tendrá un gran impacto en su operativa mientras que el 32% de los usuarios considera que la interrupción tendrá un impacto medio en su operativa y solamente el 12% de los usuarios piensa que las interrupciones tienen un bajo impacto en sus operaciones.

e) ¿Cuentan actualmente con un Plan de Continuidad de Negocio (BCP)?

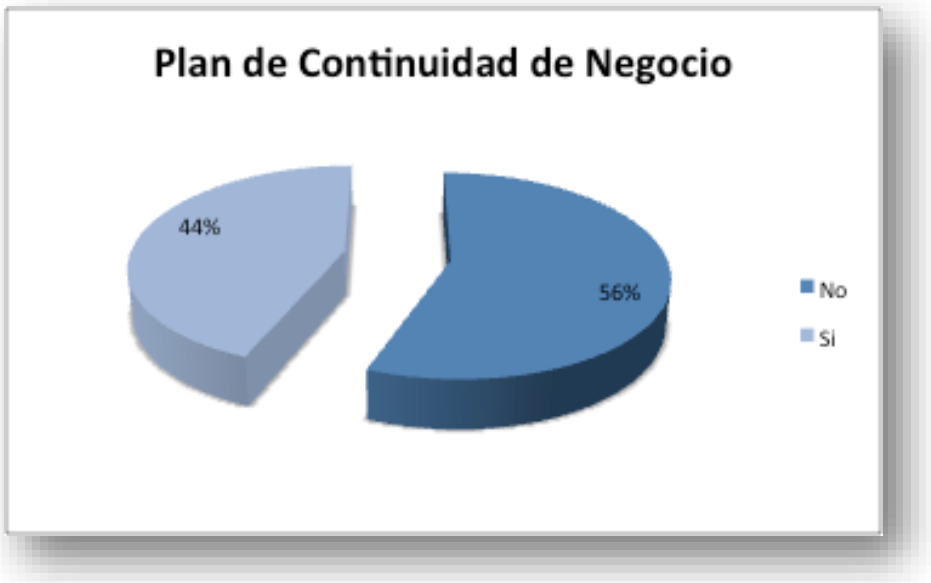

Figura 10: Plan de Continuidad de Negocio

f) ¿Cuándo fue la última vez que se actualizó la información del Plan de Continuidad de Negocio de su empresa?

Figura 11: Última actualización del Plan de Continuidad de Negocio

En las imágenes 10 y 11 se muestra que el 56% de los usuarios de servicios en la nube no cuenta con un plan de continuidad de negocio pero también se concluye que el 44% del 44% de los usuarios que cuentan con plan de contingencia no lo han actualizado hace más de un año lo que realmente los expone en gran manera a cualquier imprevisto que pueda suceder ya sea provocado o por algún desastre natural.

g) ¿Actualmente su empresa cuenta con un Proveedor de Servicio de Internet de respaldo con conectividad física independiente del Proveedor de Servicio de Internet principal?

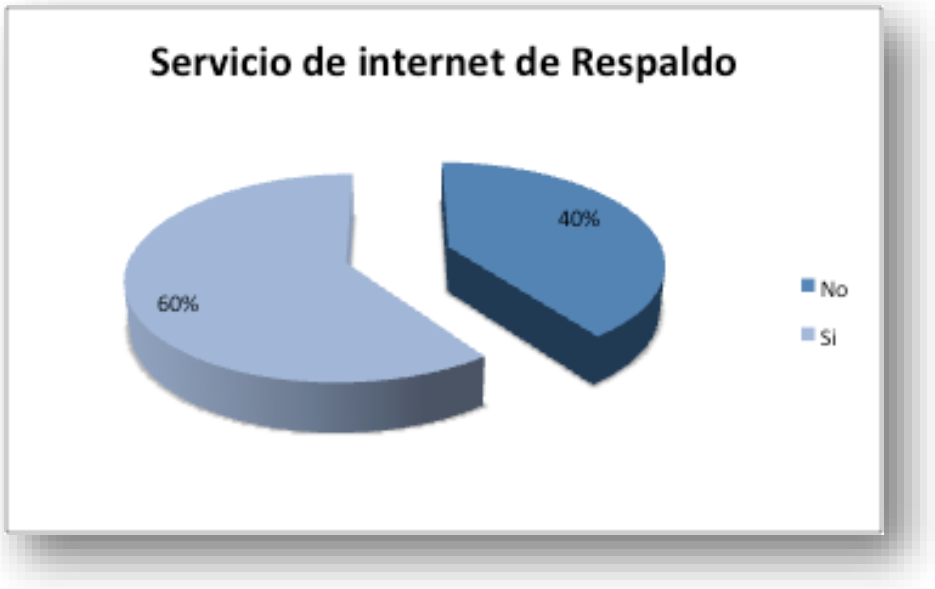

Figura 12: Servicio de Internet de Respaldo

En este gráfico se muestra que el 60% de los clientes cuenta con un enlace de Internet de respaldo por parte de su proveedor por lo cual podemos deducir según nuestro conocimiento que esta puede ser una de las variables que han influido en la no aplicación de un plan de contingencia o en la no actualización del mismo.

4.1.3 VARIABLE 3: SEGURIDAD DE ACCESOS Y LA PROTECCIÓN DE LOS DATOS

Para evaluar esta variable se consultó a los usuarios sobre seguridad de accesos y protección de datos y las respuestas se presentan en las tablas y figuras siguientes.

a) ¿Qué método de autenticación utiliza para acceder a la administración de sus servicios en la nube.

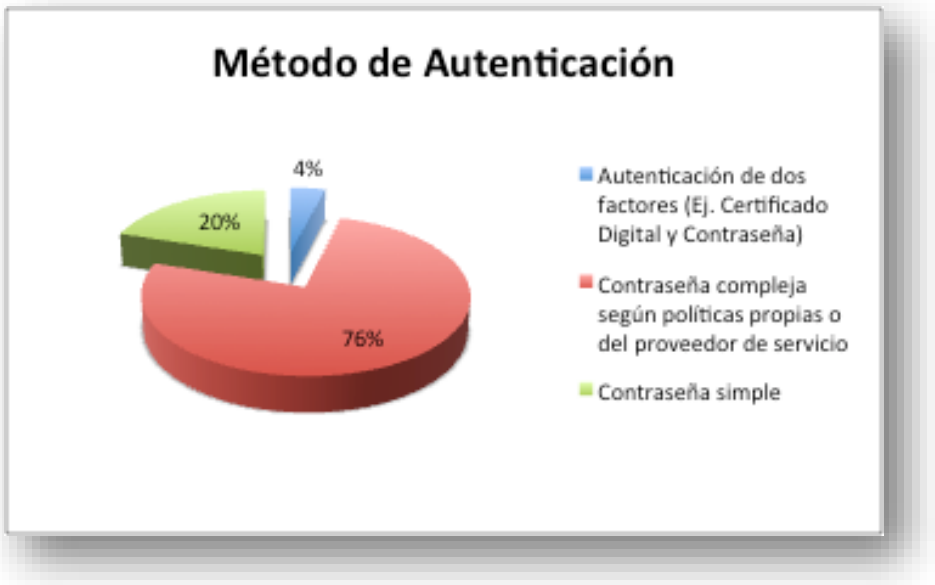

Figura 13: Métodos de Autenticación

b) ¿Su empresa cuenta con políticas específicas para el cambio periódico de contraseñas de acceso a su infraestructura en la nube?

Figura 14: Cambio de contraseñas

c) ¿Cuánto tiempo transcurre desde que un empleado deja de trabajar en la empresa y sus credenciales son eliminadas de su infraestructura en la nube?

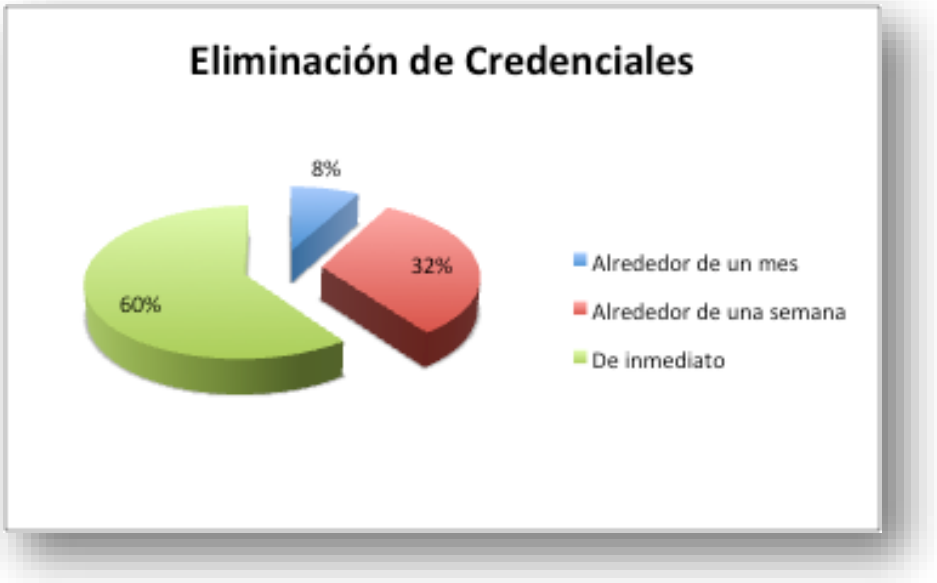

Figura 15: Eliminación de Credenciales

d) ¿Existen políticas de seguridad referentes a la compartición de credenciales entre usuarios?

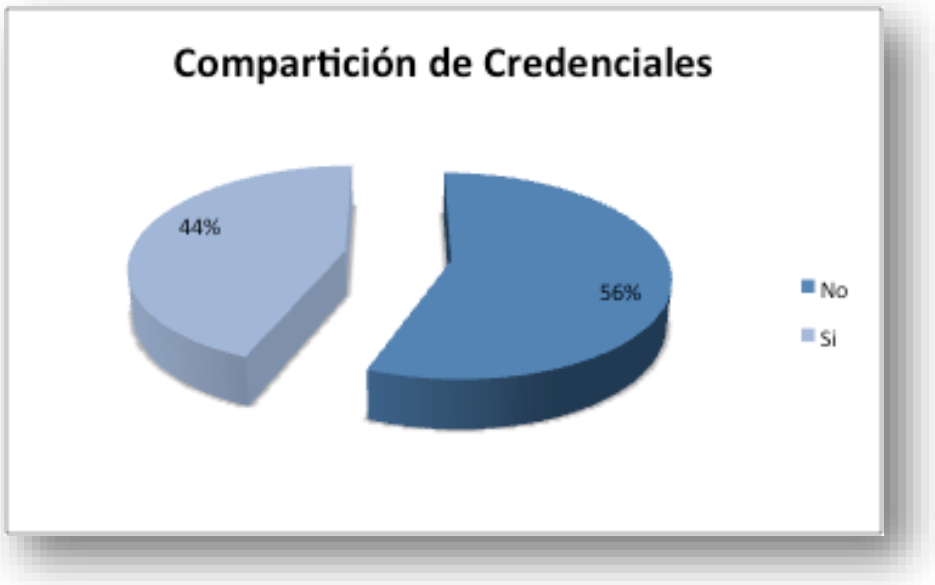

Figura 16: Compartición de Credenciales

En esta sección de las figuras 13 hasta la 16 se demuestra que el 76% de los clientes autentica a todos sus usuarios a través de la contraseña compleja según políticas propias o del proveedor del servicio, el 60% de los usuarios elimina las credenciales de manera inmediata cuando se prescinde del servicio de un empleado, el 32% elimina las credenciales dentro la primera semana después del despido mientras que el 8% lo realiza dentro del primer mes después del despido de los empleados.

En la tabla 18 se muestra que el 56% de los usuarios no permite la compartición de contraseñas entre empleados pero hay un 44% preocupante sí permite la compartición de contraseñas, esto abre una brecha para el posible sabotaje de las organizaciones porque al prestarse las contraseñas se hace más difícil la detección de los intrusos.

e) ¿Se documenta el tipo de datos que se almacenan en su servicio en la nube?

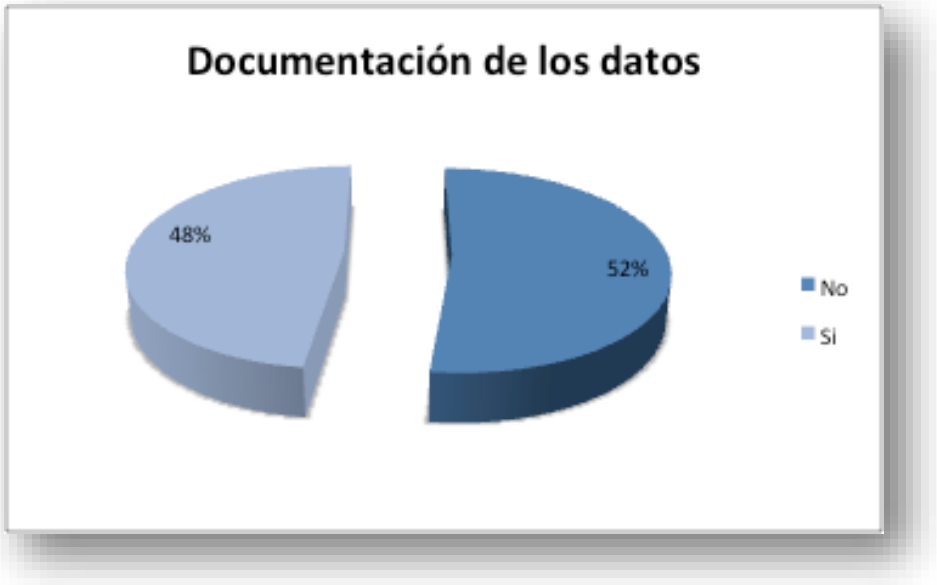

Figura 17: Documentación de los datos almacenados en la nube

Según la figura anterior se puede concluir que el 52% de loa usuarios de los servicios en la nube no documentan que tipo de datos son los que se almacenan en la nube lo que puede afectar a los usuarios a la hora que se realice un cambio en el personal que maneja estos servicios porque cuando entre un nuevo elemento en esta área de la empresa no tendrá manejo ni conocimiento de los procedimientos de los datos que se almacenan. Solamente el 48% de los usuarios hace documentación del tipo de datos que almacenan en la nube de los proveedores.

f) ¿Qué nivel de criticidad tiene la información que almacena su empresa en su servicio en la nube?

Figura 18: Nivel de criticidad de la Información almacenada

En esta figura podemos notar que el 60% de los usuarios considera que su información almacenada en la nube es de suma importancia para la operativa de sus empresas, dividiéndose un 20% de los clientes que menciona que su información es altamente confidencial y el 40% de ese 60% considera que su información es muy crítica para su operatividad.

g) ¿Conoce la ubicación de todas las copias de seguridad que existen de sus datos?

Figura 19: Ubicación de las Copias de Seguridad

En esta figura se demuestra que el 60% de los usuarios de servicios en la nube desconoce la ubicación física de las copias de seguridad de sus datos lo que realmente deja mucho que pensar en cuanto a si los datos están en un sitio adecuado de manera física por parte del proveedor. El 40% restante presenta una ventaja sobre el otro sector ya que conoce con seguridad la protección de sus datos y la ubicación adecuada de los mismos.

4.1.4 VARIABLE 4: ADMINISTRACIÓN DE LOS SERVICIOS Y LA PROPIEDAD DE LOS DATOS

Para evaluar esta variable se consultó a los proveedores sobre seguridad perimetral y certificaciones y los datos recopilados se presentan en la tabla y figuras siguientes.

a) ¿Su empresa cuenta con políticas específicas de seguridad para los accesos a servicios en la nube por parte de los clientes?

En este caso el 100% de los provceedores encuestados cuenta con políticas de seguridad específicas para cuando los clientes desean ingresar a los servicios que tienen alojados en la nube, lo que brinda confianza a los usuarios de que su información no puede ser accesada con tanta facilidad por cualquier intruso que desee conseguir la información.

b) ¿Su empresa realiza campañas de concientización y entrenamiento acerca de seguridad en la nube a los clientes?

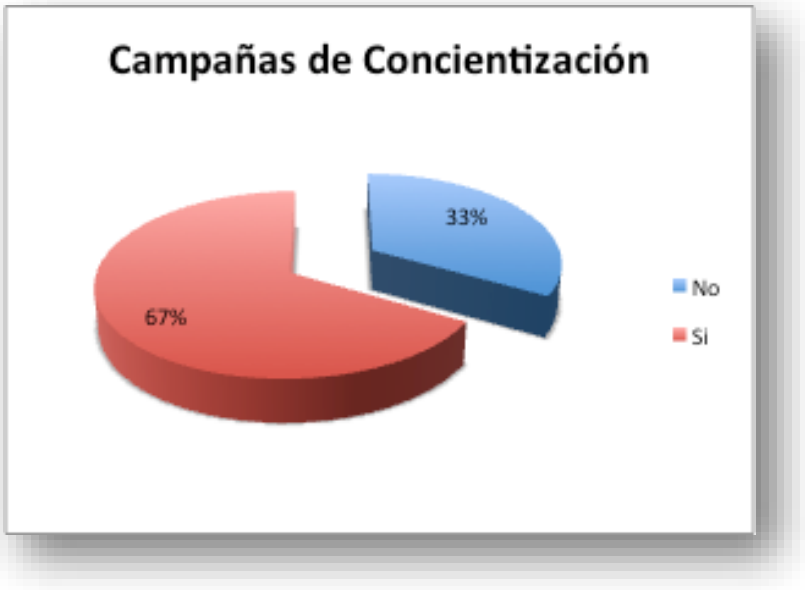

Figura 20: Campañas de concientización sobre seguridad

En este gráfico se demuestra que el 67% de los proveedores encuestados realiza campañas de concientización y entrenamiento sobre seguridad en la nube lo que a nuestra forma de analizar esta situación se concluye este puedes ser un punto a favor para dichos proveedores porque para algunos clientes es muy importante la capacitación de sus colaboradores involucrados en los procesos de los servicios en la nube.

c) ¿Su empresa establece procesos de validación inicial estrictos para los servicios en la nube que accesen los clientes?

d) ¿Su empresa cuenta con políticas que le permitan a los clientes el solicitar la transferencia de los datos hacia otro proveedor de servicios de ser necesarios?

En cuanto a los dos incisos anteriores, la encuesta reveló que el 100% de los proveedores de servicios en la nube ofrecen procesos de validación inicial estrictos y también ofrecen la oportunidad de que le cliente solicite la transferencia de sus datos de los equipos de un proveedor a los de otro, por lo que los usuarios pueden estar tranquilos con respecto a la manejabilidad de sus datos y la gobernabilidad de los mismos por parte estos.

e) ¿Su empresa cuenta con politicas establecidas de borrado permanente de datos incluyendo respaldos cuando se ha terminado el contrato?

El 100% de los proveedores encuestados afirma realizar un borrado permanente de los datos de los clientes después de que se dé la terminación definitiva del contrato de prestación de servicios con lo que los usuarios pueden asegurar que su información no será utilizada con otros fines después de prescindir de los servicios del proveedor.

4.1.5 VARIABLE 5: SEGURIDAD PERIMETRAL Y CERTIFICACIONES

Para evaluar esta variable se consultó a los usuarios y proveedores sobre seguridad perimetral y certificaciones y los datos más representativos recopilados se presentan en la siguiente figura.

a) La empresa Proveedora de Servicio en la Nube puede demostrar la existencia de algún certificado de Seguridad de la Información (Ej. ISO/IEC 27001, SAS70, etc).

Figura 26: Certificados de Seguridad de la Información

En este gráfico queda demostrado que solamente el 33% de los proveedores encuestados cuenta con certificados propios de seguridad y el 67% de los proveedores no cuenta con este tipo de certificados sino que su casa matriz es la que posee dichos certificados y administradores de estos servicios. En este caso el proveedor que posee su administrador y sus certificados propios en el país cuenta con una gran ventaja competitiva sobre los otros.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Cada cliente o potencial cliente de Servicios en la Nube decide tomar este tipo de servicio, en su mayoría, basado solamente en la información brindada por los proveedores pero no cuentan con ningún tipo de informe que les oriente sobre cuáles son los requerimientos mínimos a solicitar a los proveedores de servicios de seguridad en la nube.

- No se está dando la debida atención a los planes de continuidad de negocios ya que hay varios usuarios que no los poseen y hay otros que no los han actualizado desde el momento que adquirieron los servicios en la nube con un tercero.

- Actualmente existe bastante desconocimiento sobre las prácticas de seguridad que ponen en práctica los proveedores de servicios en la nube respecto a la valiosa información de los clientes, un 60% de los usuarios finales de servicios en la nube que encuestamos con nuestro instrumento desconoce la ubicación física de posibles copias de seguridad de su información.

- Un 60% de los clientes o usuarios finales de servicios en la nube concuerda que la información que utilizan en sus servicios es de un alto nivel de criticidad, y un 52% de estos clientes considera que la pérdida o interrupción del servicio tendría un alto impacto en sus operaciones del negocio, lo que indica que estas empresas han invertido su confianza en los proveedores de servicios en la nube del país, a pesar de que solamente uno de los tres en operación cuente con certificaciones de cumplimiento de seguridad de la información.

5.2 RECOMENDACIONES

- Se recomienda a todo usuario que desee adquirir un servicio en la nube, sobre todo de seguridad, que base su elección de acuerdo a la información del proveedor pero también buscando la información necesaria por parte de ellos mismos en sitios y lugares de prestigio que brinden información correcta y útil. Este consejo es muy importante, sobretodo, para negocios pequeños en los cuales adquirir este tipo de servicio representa una gran inversión.

- Es necesario que los Proveedores de servicios en la nube a nivel nacional procuren adquirir los certificados y conocimientos pertinentes sobre la nube para que de estar forma todos los usuarios y posibles clientes sientan mayor confianza a la hora de tomar la decisión de adquirir este tipo de servicios y no traten de buscar un proveedor de fuera del país.

- Siempre es necesario tomarse el tiempo de involucrarse en la elaboración de un plan de recuperación de desastres propio, así como también revisar si el proveedor también cuenta con un plan actualizado, este tipo de planes son de vital importancia ya que se manejan datos altamente críticos o confidenciales y la interrupción del servicio causa un alto impacto en las funciones cotidianas del negocio.

- Este documento pretende señalar los factores importantes dentro de varios dominios claves para asegurar la información en el uso de servicios en la nube, los proveedores de servicios en la nube de nuestro país deberían formular informes donde detallen sus fortalezas referentes a la seguridad, como ser ubicación física de copias de seguridad de la información de sus clientes, certificados de estándares de seguridad de la información vigentes y así como también sugerencias de seguridad sobre el uso de sus servicios fundamentados con su experiencia en el tema, esto daría mayor confianza y un valor agregado en el aspecto profesional de los proveedores hacia los usuarios finales.

- Un 52% de los usuarios finales de servicios en la nube desconoce qué tipo de información está siendo almacenada por su proveedor, por lo general esta información es difícil de monitorear en su totalidad debido a la infraestructura necesaria para hacerlo, aunque el nivel de confidencialidad que arrojaron los resultados de nuestro instrumento, un 40% con información de alto nivel de criticidad y un 20% con información de nivel altamente confidencial, las empresas deberían preocuparse más por establecer políticas sólidas de seguridad al momento de subir información a sus herramientas en la nube.

- Al analizar y evaluar los resultados de los usuarios finales, los datos de nivel de criticidad de la información y el alto impacto que tendría la interrupción de estos servicios en sus negocios, estos deberían mostrar más interés en redundar los recursos que mantienen funcionando estos servicios, como ser la conexión de internet necesaria para el propósito de sus servicios en la nube, solamente un 60% de los usuarios finales cuentan con una conexión alterna de internet en caso de que la conexión principal falle.

CAPITULO VI. APLICABILIDAD

PROPUESTA DE ESTRATEGIA DE SEGURIDAD PARA SERVICIOS EN LA NUBE.

RECOMENDACIONES PRINCIPALES

- GARANTÍAS PARA LOS CLIENTES EN NUBE

Los clientes en nube necesitan que se les garantice que los proveedores aplican prácticas adecuadas de seguridad para mitigar los riesgos a los que se enfrentan el cliente y el proveedor (por ejemplo, los ataques distribuidos de denegación de servicio, o DDoS). Necesitan esta garantía para poder tomar decisiones de negocio correctas y para mantener u obtener certificados de seguridad. Un síntoma inicial de esta necesidad de aseguración es que numerosos proveedores en nube (PN) se ven bombardeados con solicitudes de auditorías.

Por este motivo, hemos expresado muchas de las recomendaciones del informe en forma de listado de cuestiones que puede ser utilizado para ofrecer o recibir aseguraciones.

Los documentos basados en la lista de comprobación deben aportar a los clientes medios para:

1. evaluar el riesgo de utilizar servicios en nube;

2. comparar las ofertas de los distintos proveedores en nube;

3. obtener aseguraciones de los proveedores en nube seleccionados:

4. reducir la carga de la aseguración con respecto a los proveedores en nube.

La lista de comprobación de seguridad abarca todos los aspectos de los requisitos en materia de seguridad, incluidas la seguridad física y las implicaciones legales, políticas y técnicas.

A continuación se presenta una lista de chequeo de características que el proveedor de servicios en la nube debería cumplir para un aseguramiento de disponibilidad, integridad y confidencialidad de la información. Se presenta solamente del proveedor de servicios en la nube y no del cliente porque se asume que el cliente confiará en el perímetro del proveedor y no al revés.

Parámetro sujeto a revisión	
Seguridad Física: Rigurosidad de acceso físico del proveedor de servicios	
Todas las áreas seguras (Centros de Datos) utilizan tarjetas para el control de acceso	
Registro de visitas de terceros (Visitas, proveedores de servicio, etc.)	
Todas las visitas a sitios seguros deben ser acompañadas en todo momento por personal interno del proveedor de servicios en la nube.	
Todos los empleados, contratistas, visitas, etc. Deben portar un gafete de seguridad que los identifique en todo momento.	
Todas las áreas seguras utilizan escáneres biométricos o alguna otra tecnología de control de acceso	
Todas las áreas seguras y colindantes son monitoreadas por cámaras de seguridad 24x7x365	
Comprobación de antecedentes de empleados: Rigurosidad de confirmación de antecedentes y competencias del personal que maneja información de clientes.	
El proveedor de servicios en la nube revisa antecedentes de sus empleados	
El proveedor de servicios en la nube realiza confirmaciones de credenciales de educación y competencias técnicas.	
Auditorias de Control de cambios y Accesos: Auditorias y certificados especiales	
Recibe auditorias periódicamente para control de cambios y accesos.	
Nombre la empresa que realiza auditorias de accesos y control de cambios:_____	

Evaluación de Vulnerabilidades: Evaluación regular de vulnerabilidades para determinar la existencia de brechas de seguridad	
Escriba la fecha de su última evaluación de vulnerabilidades: _____	
Provea una lista considerable de riesgos o brechas de seguridad que ha identificado: _____ _____ _____	
¿Se han mitigado los riesgos/brechas identificadas en la última evaluación de vulnerabilidades?	
Almacenamiento de Datos: Procesos adecuados, sistemas y servicios activos para asegurar la integridad y persistencia de los datos.	
¿Dónde se encuentra localizada la data? Por favor listar localidades, estados o países: _____	
¿Existe alguna ley de privacidad o restricción de retransmisión y almacenamiento de los datos?	
¿Existen respaldos de datos almacenados dentro o fuera del sitio principal?	
¿Si los datos se almacenan fuera del sitio, la almacena algún otro contratista? De ser así, por favor liste los contratistas más relevantes: _____ _____	
¿Los datos almacenados se encuentran cifrados?	
¿Existe un acceso controlado a los datos almacenados?	
Continuidad de Negocio: Existencia de un Plan de Continuidad de Negocio o un DRP	
Describa el plan para fallas de fuentes de poder o fallas críticas de servicio: _____ _____	
Describa el plan para desastres físicos como incendios, daños por agua o inundaciones ya sean provocados o desastres naturales:	

_____ _____	
Describa un plan para operaciones de grabado por desobediencia civil o inestabilidad del gobierno: _____ _____	
Describa el plan para brechas de seguridad resultantes de fallos de sistemas, tales como un ataque de denegación de servicios (DDOS):_____ _____	
Trafico de Red y Accesos de Usuarios: Documentación de registros de eventos de red, acceso a servidores y archivos.	
Registro de eventos de Sistemas de Seguridad	
Registro de eventos de switches de red, routers y otros dispositivos de red.	
Registro de eventos de Bases de Datos y Servidores	
Registro de eventos de Directorio Activo	
Registro de eventos de Servidores Web y de Correo Electrónico	
Registro de eventos de Sistemas VPN	
Registro de eventos de Máquinas Virtuales	
Conexiones y Autenticación: Registros de seguridad adecuada para accesos de red y cifrado de datos.	
¿Cómo son cifradas las conexiones? (SSL, SSH, etc) _____	
¿Existen políticas de elaboración de contraseñas seguras? De ser así, describa los requerimientos mínimos y períodos de expiración de credenciales: _____ _____	
¿Utilizan autenticación de doble factor? De ser así, por favor describa cuáles: _____ _____	

Infraestructura: Medidas de seguridad de infraestructura, incluyendo sub contratistas.	
¿Es su infraestructura compartida con otro servicio? Por favor describir: _____	
¿El servicio se encuentra en una localidad dedicada única y exclusivamente para el servicio? Por favor describa: _____ _____	
¿El servicio se encuentra en equipos segmentados con virtualización? Por favor describa: _____ _____	
Estándares de SLA: El proveedor cuenta con un Contrato de Nivel de Servicio activo identificando límites de desempeño mínimo y alguna penalidad por el incumplimiento del contrato.	
Describa el Contrato de Nivel de Servicio (SLA): _____ _____ _____ _____	
Describa las penalidades asociadas con el incumplimiento del Contrato de Nivel de Servicio (SLA): _____ _____	

- RECOMENDACIONES LEGALES

La mayoría de cuestiones legales asociadas a la computación en nube se suele resolver durante la evaluación (es decir, al comparar los distintos proveedores) o la negociación del contrato. El caso más común de computación en nube es la selección de los distintos contratos que ofrece el mercado (evaluación de contratos), en

contraste con la negociación del contrato. No obstante, podría haber oportunidades para que clientes potenciales de servicios en nube seleccionaran proveedores con contratos negociables.

A diferencia de los servicios tradicionales de Internet, se recomienda revisar detenidamente las cláusulas estándar del contrato, debido a la naturaleza de la computación en nube. Las partes del contrato deben prestar especial atención a sus derechos y obligaciones en lo que respecta a las notificaciones de incumplimiento de los requisitos de seguridad, transferencias de datos, creación de obras derivadas, cambio de control y acceso a los datos por parte de las fuerzas policiales. Debido a que la nube puede utilizarse para subcontratar infraestructura interna crítica, y a que la interrupción de dicha infraestructura puede tener consecuencias de gran alcance, las partes deben considerar detenidamente si las limitaciones estándar de la responsabilidad se ajustan a las asignaciones de responsabilidad, habida cuenta del uso de la nube por las distintas partes, o a las responsabilidades en cuanto a la infraestructura.

Hasta que los reglamentos y precedentes legales aborden las preocupaciones concretas en materia de seguridad relativas a la computación en nube, los clientes y los proveedores en nube deben asegurarse de que las condiciones de su contrato abordan de manera efectiva los riesgos de seguridad.

- RECOMENDACIONES EN MATERIA DE INVESTIGACIÓN

Recomendamos ámbitos prioritarios de investigación a fin de mejorar la seguridad de las tecnologías de computación en nube. Hemos considerado las siguientes categorías, con algunos ejemplos de ámbitos específicos extraídos la lista completa:

1. CREACIÓN DE UN CLIMA DE CONFIANZA EN LA NUBE
    a. Efectos de las distintas formas de notificación de los incumplimientos relativos a la seguridad
    b. Confidencialidad integral de los datos en la nube y más allá
    c. Nubes con mayor aseguración, nubes privadas virtuales (VPC), etc.

2. PROTECCIÓN DE DATOS EN LOS GRANDES SISTEMAS INTERORGANIZACIONES
    a. Informática forense y mecanismos de recogida de pruebas.
    b. Gestión de incidentes – seguimiento y localización
    c. Diferencias internacionales en la normativa aplicable, incluida la privacidad y la protección de datos
3. INGENIERÍA DE SISTEMAS DE COMPUTACIÓN A GRAN ESCALA
    a. Mecanismos de aislamiento de recursos: datos, procesamiento, memoria, registros, etc.
    b. Interoperabilidad entre proveedores en nube.
    c. Resistencia a los fallos de la computación en nube. ¿Cómo puede la nube mejorar esa resistencia?

Para poder contar con un servicio de seguridad en la nube acorde a los estándares y necesidades del cliente se deben tomar en cuenta los puntos que se presentan a continuación.

BIBLIOGRAFÍA

Antwerp, A. L. (2011). *Assessing the Security Risks of Cloud Computing .* Cloud Security Alliance.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., KonwinsKi, A., . . . ZahAria, M. (Volume 53 Issue 4, April 2010). A View of Cloud Computing. *Communications of the ACM*, Pages 50-58 .

Boss, G., Malladi, P., Quan, D., & Linda, L. (2007, Octubre 8). *http://files.spogel.com/projectsqa/qa-00135--how%20a%20business%20can%20use%20cloud%20computing%20to%20reduce%20cost.docx.* Retrieved from www.ibm.com/developerworks/websphere/zones/hipods/.

Chang, V., Wills, G., & De Roure, D. (2010). A Review of Cloud Business Models and Sustainability. *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, (pp. 43- 50). Miami,FL.

Crandell, M. (2011, Mayo 29). Retrieved from https://gigaom.com/2011/05/29/how-to-design-your-service-for-failures-in-the-cloud/

Daft, R. L. (2007). *Teoria y Diseño Organizacional.* Mexico: International Thomson Editores.

Departamento de Recursos de IT del Estado de Texas. (2004, Diciembre). Retrieved from EEPC: http://www.epcc.edu/IT/InformationSecurity/Documents/Business_Continuity/Business_Continuity_Planning_Guidelines.pdf

ENISA. (2009, Noviembre). *Beneficios, riesgos y recomendaciones para la seguridad de la información.* Retrieved from http://www.enisa.europa.eu/:

http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/view

Escrivá Gascó, G. R. (2013). *Seguridad Informatica.* España, España: Macmillan Iberia, S.A. .

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. *Grid Computing Environments Workshop, 2008. GCE '08* (pp. 1- 10). Austin,TX: Conference Publications.

Gamby, R. (2012). *TechTarget.com.* Retrieved from http://searchsecurity.techtarget.com/video/Alternative-authentication-New-authentication-methods-for-enterprises

Gartner. (2008, Junio 3). *Gartner.com.* Retrieved from www.gartner.com: http://www.globalcloudbusiness.com/SharedFiles/Download.aspx?pageid=138&mid=220&fileid=12

Global, S. (2013, Mayo 20). *http://www.spi-global.com.* Retrieved from http://www.spi-global.com/blog/think-tank/multi-tiered-technical-support/

Gossweiler, G. (2012, Octubre 2). *ámbito.com*. Retrieved from ámbito.com: http://www.ambito.com/noticia.asp?id=656914

Goth, G. (2008). Software-as-a-Service: The Spark That Will Change Software Engineering? *Distributed Systems Online, IEEE*, 3.

Greiner, L., & Gibbons Paul, L. (2009, Junio 18). *www.cio.com.* Retrieved from CIO: http://www.cio.com/article/2438284/outsourcingla-definitions-and-solutions/outsourcing/sla-definitions-and-solutions.html

Gutierrez, P. (2013, Enero 3). *Genbetadev.com*. Retrieved from http://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Hofmann, P. (2010). Cloud Computing: The Limits of Public Clouds for Business Applications. *Internet Computing, IEEE*, 90- 93 .

Horngren T., C., Sundem, G. L., & Stratton, W. O. (2006). *Contabilidad Administrativa.* Mexico: Pearson Eduacion.

INTECO. (2013). *Política de contraseñas y seguridad de la información.* La Rioja: Instituto Nacional de Tecnologías de Comunicación.

ISO27001 Academy. (2014). Retrieved from http://www.iso27001standard.com/es/que-es-iso-27001/

Jamsa, K. A. (2012). *Cloud Computing.* Burlintong, MA: Jones & Barlett Lerning LLC.

Jericho Forum. (2009, Abril). *https://collaboration.opengroup.org.* Retrieved from https://collaboration.opengroup.org: https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Kant, K. (2009). *Data center evolution A tutorial on state of the art, issues, and challenges.* Oregon, USA: Elsevier B.V.

Klems, M., Nimis, J., & Stößer, J. (2009). Do Clouds Compute? A Framework for Estimating the Value of Cloud Computing. In M. Klems, J. Nimis, & J. Stößer, *Designing E-Business Systems. Markets, Services, and Networks* (pp. 110-123). Springer Berlin Heidelberg.

Kusnetzky, D. (2011). *Virtualization: A Manager's Guide.* O'Reilly Media, Inc.

Laudon, K., & Laudon, J. (2008). *Sistemas de información gerencial.* Mexico: Pearson Educación.

Microsoft. (2009, Mayo). *Securing Microsoft's Cloud Infrastructure.* Retrieved from https://cloudsecurityalliance.org: https://cloudsecurityalliance.org/securing-the-MS-Cloud.pdf

Miller, M. (2009). *Cloud Computing: Web-Based Applications That.* United States of America: Que Publishing.

Negocios, C. (2012, Marzo 18). *Crece Negocios*. Retrieved from Crece Negocios: http://www.crecenegocios.com/el-analisis-costo-beneficio/

Observatorio Regional de Sociedad de la Información, (. (2010). *Cloud Computing La Tecnología como Servicio.* Castilla y León.

Odom, W. (2008). *CCENT/CCNA ICND1 Official Exam Certification Guide, Second Edition.* Indianapolis: Cisco Press.

Oz, E. (2008). *Administracion de los Sistemas de Informacion, 5a edicion.* Mexico: Cengage Learning.

Palo Alto Networks. (n.d.). *Palo Alto* . Retrieved from https://www.paloaltonetworks.com/resources/learning-center/what-is-network-security.html

Perez, A. (2011, Mayo). *es.scribd.com*. Retrieved from http://es.scribd.com/doc/55231771/Encriptacion-o-Cifrado-de-Datos

Rapaport, L. (2012, Diciembre 5). *Bloomberg.com*.

Rayport, J. F., & Heyward, A. (2009). *Envisioning the Cloud: The Next Computing Paradigm.* Marketspace LLC.

Rocket Lawyer. (2014). *Rocket Lawyer Incorporated.* Retrieved from https://www.rocketlawyer.com/article/nda-101:-what-is-a-non-disclosure-agreement.rl

Rouse, M. (2005, Septiembre). *TechTarget*. Retrieved from http://searchstorage.techtarget.com/definition/business-impact-analysis

Rus, G. d. (Septiembre 2008). *Análisis Coste - Beneficio.* Barcelona: Book Print Digital.

Ryan, M. (2012). *eHow.com.* Retrieved from www.ehow.co.uk: http://www.ehow.co.uk/list_7301132_alternative-authentication-methods.html

Saffirio, M. (2006, Abril 08). *Wordpress.com*. Retrieved from Wordpress.com: http://msaffirio.wordpress.com/2006/04/08/costo-total-de-propiedad-tco-y-administracion-del-ciclo-de-vida-lcm/

SAS70. (2014). *sas70.com*. Retrieved from http://sas70.com/sas70_overview.html

Schilling, J. (2014, Julio 8). Multifactor authentication key to cloud security success. (B. Blevins, Interviewer)

Stair, R. M., & Reynolds, G. W. (2000). *Principios de Sistemas de Informacion: enfoque administrativo.* Mexico: International Thomson Editores, S. A. de C. V.

Tate, J., Lucchese, F., & Moore, R. (2006). *Introduction to Storage Area Networks.* IBM Redbooks.

TechTarget. (2008, Noviembre). Retrieved from http://searchsecurity.techtarget.com/tutorial/Exploring-authentication-methods-How-to-develop-secure-systems

TechTarget. (2012). *techtarget.com*. Retrieved from http://searchdisasterrecovery.techtarget.com/essentialguide/Essential-guide-to-business-continuity-and-disaster-recovery-plans#guideSection1

Unidad Técnica. (2009, Enero 23). *Universidad de Córdoba.* Retrieved from Universidad de Córdoba: http://www.uco.es/gestion/unidadtecnica/pages/docs/calidad/mantcorrec.pdf

Waters, B. (2005). Software as a service: A look at the customer benefits. *Journal of Digital Asset Management* , 32-39.

Wyld, D. C. (2009). THE UTILITY OF CLOUD COMPUTING AS A NEW PRICING – AND CONSUMPTION - MODEL FOR INFORMATION TECHNOLOGY. *International Journal of Database Management Systems (IJDMS),Vol.1, No.1*.

ANEXOS

FICHA DE EVALUACIÓN

ESTRATEGIAS DE SEGURIDAD PARA SERVICIOS EN LA NUBE

Términos y condiciones del Servicio, Continuidad del Servicio y Políticas de privacidad.

b) Nombre de la Empresa Proveedora de Servicios en la Nube

c) Clasificación de reputación y estabilidad económica del Proveedor de Servicios en la Nube.
Marque con una X una sola opción

- ☐ Excelente reputación
- ☐ Buena reputación
- ☐ Reputación regular
- ☐ Mala reputación

Administración de Servicios en la nube y Propiedad de los Datos.

d) Antigüedad en la empresa del administrador del servicio en la nube.

Marque con una X una sola opción

- ☐ Menos de 6 meses
- ☐ 1 año – 2 años
- ☐ 2 años – 4 años
- ☐ Más de 4 años

Seguridad Perimetral e Infraestructura de Red y Certificaciones de Cumplimiento.

e) Método de cifrado de comunicaciones entre los servidores públicos del Proveedor de Servicios en la Nube y los equipos de los usuarios finales.

Marque con una X una sola opción

- ☐ TSL (SSL)
- ☐ GnuPG
- ☐ PGP
- ☐ IPSec
- ☐ Otro ¿Cuál? _____

f) La empresa Proveedora de Servicio en la Nube puede demostrar la existencia de algún certificado de Seguridad de la Información (Ej. ISO/IEC 27001, SAS70, etc).

Marque con una X una sola opción

- ☐ Si
- ☐ No

CUESTIONARIO PARA USUARIOS DE SERVICIOS EN LA NUBE

Estimado usuario: Somos estudiantes de la Meatría de Gestión de las Tecnologías de la Información y estamos realizando nuestro trabajo de tesis sobre Seguridad en la nube, especificamente en los parametros que se consideran fundamentales para contar con una excelente Seguridad en la nube por lo que le solicitamos contestar la siguiente encuenta para conocer sus intereses respecto a este tema.

Generalidades de la Empresa

1. Nombre de la Empresa
   Escriba de forma precisa o concisa lo que se le pide

2. Rubro al cual se dedica su empresa

   Marque con una X una sola opción

   ☐ Bienes

   ☐ Servicios

   ☐ Otro ¿Cuál? _____

3. Empleados que usan servicios en la nube
   Marque con una X una sola opción

   ☐ Todos

   ☐ Puestos ejecutivos

   ☐ Puestos operativos

   ☐ Los que así deseen

4. Información trabajada en la Nube
   a) _____
   b) _____
   c) _____

Términos y condiciones del Servicio, Continuidad del Servicio y Políticas de privacidad.

5. El proveedor del servicio ofrece el directorio telefónico para el nivel de soporte técnico requerido.
   Marque con una X una sola opción

   ☐ Si
   ☐ No

6. Este directorio telefónico ofrece números alternos de solución, si no se resuelve en el tiempo establecido.
   Marque con una X una sola opción

   ☐ Si
   ☐ No

7. Recibe de parte del proveedor de servicio, informes de:

   Marque con una X una sola opción en cada caso

Tiempo de baja de servicio por mantenimiento	
Mantenimiento preventivo rutinario	
Resolución de incidentes	

8. Nivel de impacto potencial en su empresa, cuando el proveedor del servicio o causas externas provocan la interrupción del servicio.
Marque con una X una sola opción

- [ ] Alto impacto
- [ ] Medio impacto
- [ ] Bajo impacto
- [ ] Ningún impacto

9. ¿Cuentan actualmente con un Plan de Continuidad de Negocio (BCP)?
Marque con una X una sola opción

- [ ] Si
- [ ] No

10. ¿Cuándo fue la última vez que se actualizó la información del Plan de Continuidad de Negocio de su empresa?
Marque con una X una sola opción

- [ ] En los últimos tres meses
- [ ] En el último año
- [ ] Hace más de un año

11. ¿Actualmente su empresa cuenta con un Proveedor de Servicio de Internet de respaldo con conectividad física independiente del Proveedor de Servicio de Internet principal?
Marque con una X una sola opción

- [ ] Si
- [ ] No

Seguridad de Cuentas de Acceso y Protección de Datos

12. Qué método de autenticación utiliza para acceder a la administración de sus servicios en la nube.

    Marque con una X una sola opción

    - ☐ Contraseña simple
    - ☐ Contraseña compleja según políticas propias o del proveedor de servicio
    - ☐ Autenticación de dos factores (Ej. Certificado Digital y Contraseña)
    - ☐ Otro ¿Cuál? _____

13. ¿Su empresa cuenta con políticas específicas para el cambio periódico de contraseñas de acceso a su infraestructura en la nube?

    Marque con una X una sola opción

    - ☐ Si
    - ☐ No

14. ¿Cuánto tiempo transcurre desde que un empleado deja de trabajar en la empresa y sus credenciales son eliminadas de su infraestructura en la nube?

    Marque con una X una sola opción

    - ☐ De inmediato
    - ☐ Alrededor de una semana
    - ☐ Alrededor de un mes

15. ¿Existen políticas de seguridad referentes a la compartición de credenciales entre usuarios?

    Marque con una X una sola opción

    - ☐ Si

☐ No

16. ¿Se documenta el tipo de datos que se almacenan en su servicio en la nube?
Marque con una X una sola opción

☐ Si
☐ No

17. ¿Qué nivel de criticidad tiene la información que almacena su empresa en su servicio en la nube?
Marque con una X una sola opción

☐ Nada crítica
☐ Poco crítica
☐ Muy crítica
☐ Altamente confidencial

18. ¿Conoce la ubicación de todas las copias de seguridad que existen de sus datos?

Marque con una X una sola opción

☐ Si
☐ No

Seguridad Perimetral e Infraestructura de Red y Certificaciones de Cumplimiento.

19. Dentro de su infraestructura de red cuenta con los siguientes elementos:

Marque con una X cada caso que aplique

Firewall	

IPS (Sistema de Prevención contra Intrusos)	
Router(s) de capa 3	

CUESTIONARIO PARA PROVEEDORES DE SERVICIOS EN LA NUBE

Somos estudiantes de la Maestría de Gestión de las Tecnologías de la Información y estamos realizando nuestro Trabajo de Tesis sobre Seguridad de Servicios en la Nube, específicamente en los parámetros que se consideran fundamentales para contar con una estrategia sólida de Seguridad en la Nube por lo que le solicitamos por favor contestar la siguiente encuesta para ayudarnos a alcanzar nuestro propósito.

NOTA: El uso de esta información será estrictamente para fines académicos.

Generalidades de la Empresa

1. Nombre de la Empresa
   Escriba de forma precisa o concisa lo que se le pide

2. Servicios en la nube que ofrece

   Marque con una X las opciones necesarias

   - ☐ Continuidad de negocio
   - ☐ Seguridad en la nube
   - ☐ Infraestructura en la nube
   - ☐ Escritorios remotos
   - ☐ Colocation
   - ☐ Otro ¿Cuál? _____

3. Empleados que usan servicios en la nube
Marque con una X una sola opción

- ☐ Todos
- ☐ Puestos ejecutivos
- ☐ Puestos operativos
- ☐ Los que así deseen

Términos y condiciones del Servicio, Continuidad del Servicio y Políticas de privacidad.

4. ¿Que puntos esenciales cubre el SLA que se firma con los posibles clientes?
Marque con una X una sola opción

Tipos de Servicios	
Soporte a Clientes y asistencias	
Proviciones para serguridad y datos	
Garantias del sistema y tiempos de respusta	
Disponibilidad del sistema	
Conectividad	
Multas por caida del sistema	

5. ¿Existe un uso secundario de la información del cliente por parte del proveedor?
Marque con una X una sola opción

- ☐ Si
- ☐ No

6. ¿Que requisitos son necesarios para poder dar por terminado un contrato cliente proveedor y de qué forma los datos son entregados al cliente y eliminados de los equipos del proveedor?

   _____

   _____

   _____

   _____

7. Que garantias de seguridad ofrece el proveedor al cliente?
   Marque con una X una sola opción

   - ☐ Firewall
   - ☐ IPS
   - ☐ NACS
   - ☐ Sistemas de acceso
   - ☐ Otro. Cuál? _____

Seguridad de Cuentas de Acceso y Protección de datos

8. ¿ Se realizara Monitoreo Proactivo para todos los clientes?
   Marque con una X una sola opción

   - ☐ Si
   - ☐ No

9. ¿Actualmente cuentan con un un respaldo de los datos de los clientes en casos de desastre?

   Marque con una X una sola opción

   - ☐ Si
   - ☐ No

10. Cuenta el proveedor con una politica de confidencialidad para proteger los datos del cliente?

Marque con una X una sola opción

- ☐ Si
- ☐ No

11. ¿Su empresa cuenta con políticas específicas para el cifrado de las comunicaciones y los datos?

Marque con una X una sola opción

- ☐ Si
- ☐ No

Administración de servicios y Propiedad de los datos

12. ¿Su empresa cuenta con políticas específicas de seguridad para los accesos a servicios en la nube por parte de los clientes?

Marque con una X una sola opción

- ☐ Si
- ☐ No

13. ¿Su empresa realiza campañas de concientización y entrenamiento acerca de seguridad en la nube a los clientes?

Marque con una X una sola opción

- ☐ Si
- ☐ No

14. ¿Su empresa establece procesos de validación inicial estrictos para los servicios en la nube que accesen los clientes?

Marque con una X una sola opción

- ☐ Si
- ☐ No

15. ¿Su empresa cuenta con politicas que le permitan a los clientes el solicitar la transferencia de los datos hacia otro proveedor de servicios de ser necesarios?

Marque con una X una sola opción

- ☐ Si
- ☐ No

16. ¿Su empresa cuenta con politicas establecidad de borrado permanente de datos incluyendo respaldos cuando se ha terminado el contrato?

Marque con una X una sola opción

- ☐ Si
- ☐ No

Estándares más importantes para nubes públicas

17. ¿Con qué estándares de seguridad para nubes públicas cuenta su empresa?

Marque con una X cada caso que aplique

SLA	
Seguridad de cuentas de acceso	

Administración de servicios en la nube	
Seguridad Perimetral e Infraestructura de red	
Certificaciones de cumplimiento	
Propiedad de los datos	
Protección de datos	
Otro. Cual? _____	