Diseño y Simulación de un Data Center Cloud Computing que cumpla con la norma PCI-DSS

María Aguirre Patiño(1), Rut España Peláez(2), Iván Solís Granda (3), Alfonso Aranda Segovia (4)
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil, Ecuador
marylim_a@hotmail.com (1), respana@fiec.espol.edu.ec (2), iisolis@espol.edu.ec(3)
Escuela Superior Politécnica del Litoral (ESPOL)(4), Ingeniero en Computación (4), jaranda@espol.edu.ec(4)

Resumen

El proyecto consistió en el diseño y análisis de un Centro de Datos Cloud Computing que cumpla con la Norma PCI-DSS analizando sus objetivos y el alcance del mismo. Se presentan la descripción del servicio como es su funcionalidad de un Centro de Datos con su respectivo Estándar TIA-942, y así mismo explicaremos acerca del Cloud Computing con la Norma PCI-DSS.

Posteriormente, se describe el marco teórico acerca del Centro de Datos Cloud Computing, explicando los requerimientos que conllevan para la creación de un Centro de Datos en su parte eléctrica, mecánica, el cableado, etc. También describe acerca de la tecnología y la virtualización que se usa en el Cloud Computing.

Luego, se mencionará todo lo concerniente al diseño del Centro de Datos como las recomendaciones, ubicación, el cableado, el detalle de cada cuarto que contiene dicho Centro de Datos. Así mismo en este capítulo describiremos los requisitos de hardware y software para el servicio del Cloud Computing.

Palabras Claves: Diseño de un Centro de Datos, Estándar TIA-942, Norma PCI-DSS, Cloud Computing.

Abstract

The Project consisted on the design and analysis of a Cloud Computing Data Center fulfilling PCI-DSS standards, analyzing the objectives and reach of it. The service description is shown: the Data Center functionality, according to the TIA-942 standard, as well as the Cloud Computing according to the PCI-DSS standard.

Afterwards, the theorical framework of the Cloud Computing Center is described, explaining the requirements for the creation of a Data Center, based on its electrical, mechanical parts, etc. The technology and virtualization used on Cloud computing is also described.

Later, everything concerning the Data Center design, such as the location, wiring and each room in detail is mentioned. In this very chapter the hardware and software requirements for the Cloud Computing will be described.

Keywords: Design a data center, TIA-942 Standard, PCI-DSS standard, Cloud Computing.

1. Introducción

Un data center está relacionado con todos los recursos necesarios para el procesamiento de la información de una organización, por otro lado un Cloud Computing es una nueva tecnología o mezclas de tecnologías.

Por tal motivo es la respuesta a la tecnología de información a varios problemas, tales como costos de infraestructura, problemas ambientales, costo de energía y la mayor prioridad de contar con una infraestructura que sea fácil de usar pero a la vez confiable y redundantes a fallos, manteniendo los parámetros de disponibilidad, confidencialidad, integridad de la seguridad de la información como también es la respuesta de los altos costos de infraestructura que demanda las modernas empresa en la actualidad.

Diseñar un Data Center que provea servicios de Cloud Computing involucra el desarrollo de una serie de conocimientos que va desde la capa física hasta la capa lógica.

Este diseño sirve de referencia para cualquier organización que desee implementar un Centro de dato o Data Center con Tier III de última generación cumpliendo estándares internacionales.

2. Descripción del Proyecto

2.1. Objetivo General

Diseñar y simular un Data Center que provea servicios de Cloud Computing al mercado local cumpliendo con el estándar de la norma PCI-DSS.

2.1.1. Objetivos Específicos

- Ofrecer un servicio eficiente a través del Data Center usando la tecnología del Cloud Computing aplicando las normas que se exigen.
- Brindar ayuda a las empresas que manejan grandes cantidades de información la cual necesitan tener disponibilidad, integridad y seguridad al manejar sus datos.
- Proveer un ahorro económico en las empresas al momento de contratar el servicio del Data Center y mejorar la experiencia de conexión de los usuarios.
- Realizar un análisis financiero para la adquisión de los servicios del Cloud Computing, comparando los costos actuales con los obtenidos en el análisis.

2.2. Requerimientos de un Centro Datos TIER 3

El Centro de Datos es un ambiente especialmente diseñado para albergar todos los equipos y elementos necesarios para el procesamiento de información de una organización. Es por esto que deben ser extremadamente confiables y seguros al tiempo que deben ser capaces de adaptarse al crecimiento y la re-configuración permitiendo que cualquiera alteración al diseño y mantenimiento ocurra sin paralizar los servicios y proveer por lo menos una redundancia N+1.

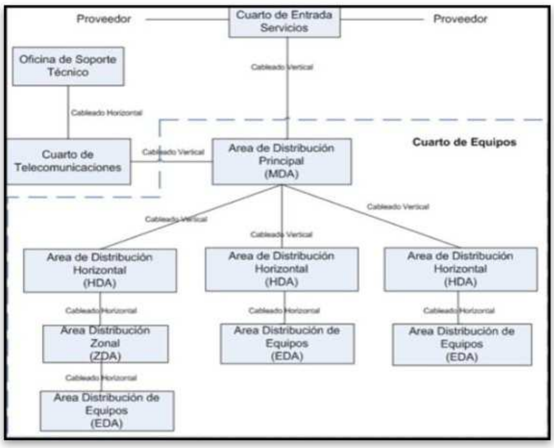

Figura 1. Diseño de la Topología del Centro de Datos TIER III

2.3. Tecnología que Soporta el Cloud Computing

2.3.1. Arquitectura del Cloud Computing

Es el conjunto de capas que se encuentran acopladas entre sí para brindar la funcionalidad del sistema, en este caso la arquitectura de Cloud Computing es similar a la arquitectura de red, desde un nivel físico hasta un nivel de aplicación. A continuación se menciona una arquitectura genérica para Cloud Computing, que tienen las siguientes capas mencionadas de abajo hacia arriba:

- Aplicación: incluye servicios basados en web y software como servicio.
- Plataforma: incluye componentes de aplicación como servicio.
- Infraestructura: incluye software de plataforma como servicio.
- Virtualización: incluye infraestructura virtual como un servicio.

- Recursos físicos: incluyen elementos como servidores, almacenamiento y red.

Figura 2. Niveles de Servicio Cloud Computing

2.3.2. Virtualización del Cloud Computing.

La virtualización es una tecnología de software orientado a ahorrar tiempo, dinero y energía; y usar una mejor manera el hardware disponible de la empresa. “Básicamente, la virtualización permite transformar hardware en software”, para crear una máquina virtual completamente funcional que puede ejecutar su propio sistema operativo y aplicaciones de la misma forma que lo hace un ordenador “real”.

Varias máquinas virtuales comparten recursos de hardware sin interferir entre sí de modo que se puede ejecutar simultáneamente y de forma segura varios sistemas operativos y aplicaciones en un único ordenador.

Entre las ventajas de la virtualización tenemos:

- Índice de utilización más altos.
- Consolidación de Recursos.
- Uso/costo menor energía.
- Ahorro de espacio.
- Recuperación de desastre/ continuidad de negocio.
- Costo de operación reducida.
- Virtualización del Sistema Operativo.

2.4. Mercado Objetivo.

Es fundamental estudiar el mercado objetivo de este proyecto; para referirse a quien va dirigido nuestro servicio así como también satisfacer sus necesidades.

- PYMES: son Pequeñas y Medianas Empresas, con un número no muy grande de trabajadores, es decir, tienen que tener como número menos de 250 empleados contratados refiriéndose a los de planta, como también a los empleados externos que se puedan llegar a subcontratar.
- Corporaciones: es una entidad constituida en forma legal y separada de sus accionistas. Una corporación puede ser una universidad, una empresa, un gremio, un sindicato u otro tipo de persona colectiva.
- Entidades Financieras: Son aquellas encargadas de facilitar la financiación a los que necesitan recursos, sean sociedades o particulares. Van desde los bancos y cajas de ahorros hasta las sociedades que nos prestan dinero para la compra de un bien concreto como pueda ser un vehículo.
- Services Provider: es una entidad que proporciona servicios a otras entidades. Por lo general, esto se refiere a un negocio que ofrece la suscripción o servicio web a otras empresas o individuos. Ejemplos de estos servicios incluyen acceso a Internet , operador de telefonía móvil, y aplicaciones web hosting . El término se aplica con mayor frecuencia a los servicios de comunicación que a otros tipos de industria de servicios.

3. Diseño Físico del Centro de Datos.

La ubicación del Centro de Datos debe ser en un lugar de terreno alto, de rápido acceso para el personal y libre de interferencia electromagnética.

Para esto se eligió la zona norte de la ciudad de Guayaquil en un terreno de 1500m2 en el cual se establecerá las oficinas de personal administrativo, el centro de datos y el área de los generadores y sistema de climatización.

3.1. Topología Física.

El cableado horizontal y el cableado vertical tendrán una topología física en estrella.

El cableado horizontal se conectara con la conexión cruzada del rack de telecomunicaciones.

Para el cableado vertical todas las conexiones cruzadas horizontales se deben conectar a la conexión cruzada principal.

Todos los equipos que se conecten a la conexión cruzada principal se conectaran a un switch de núcleo.

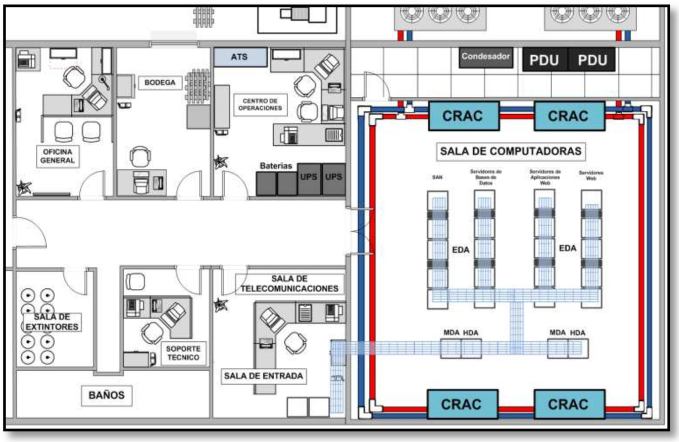

Figura 3. Cableado Horizontal del Centro de Datos

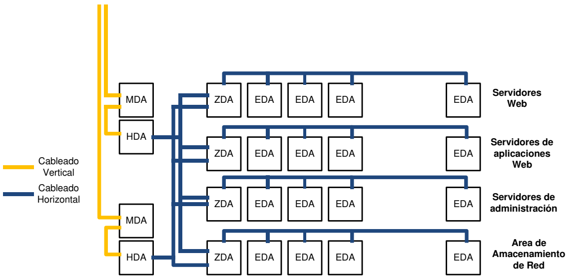

Figura 4. Distribución de los gabinetes en la sala de cómputo

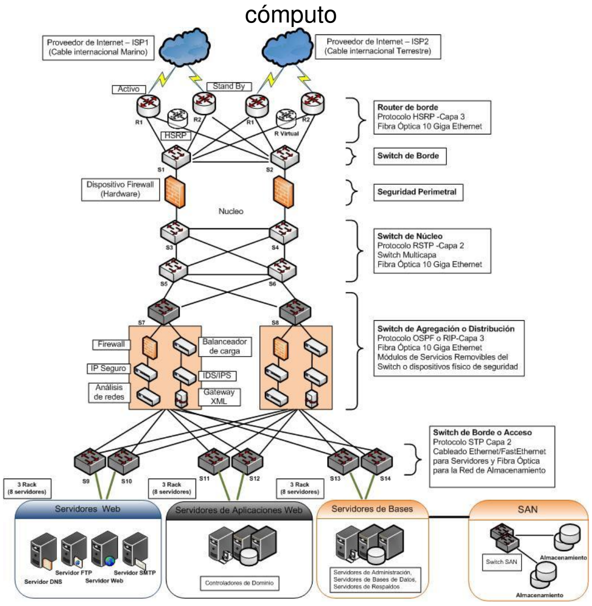

Figura 5. Diseño Físico del Centro de Datos.

4. Diseño Lógico y Servicios del Centro de Datos.

4.1. Protocolos del Centro de Datos

Los protocolos son un conjunto de reglas usadas por la computadora para comunicarse unas con otras a través de la red.

Para la elección de protocolos de conmutación y enrutamiento se debe tener en cuenta los siguientes criterios:

- Trafico de la red
- Ancho de banda, memoria y CPU
- Capacidad para adaptare ante los cambios
- Numero de nodos soportados
- Soporte de autenticidad

Al conocer estos criterios se eligió los siguientes protocolos de enrutamiento y conmutación:

- Protocolo HSRP (Hot Standby Router Protocol)
- Protocolos de Árbol Extendido (STP)
- Protocolo Rápido de Árbol Extendido (RSTP)
- Protocolo del Camino más Corto Primero (OSPF)
- Switch Multicapa
- Protocolo de Ordenes Seguras (SSH)

4.2. Servicios del Centro de Datos

El Centro de Datos ofrecerá diferentes tipos de servicios que varía dependiendo del mercado local como son PYMES, Corporaciones, Entidades Financieras y Servicios Privados.

Los servicios del Centro de Datos son:

1. Servicios Compartidos
2. Servidores Dedicados
3. Hosting Dedicados
4. Servidores Virtuales
5. Servicio de Colocación

Los cuales están divididos en tres subservicio Oro, Bronce y Plata.

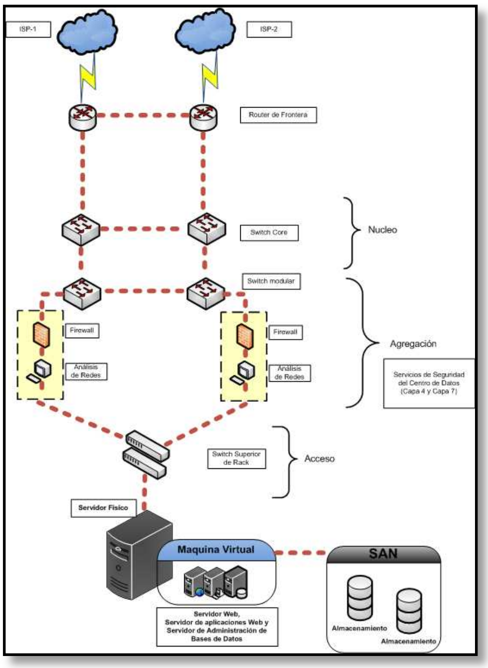

Figura 6. Diseño Topológico del Servicio Bronce.

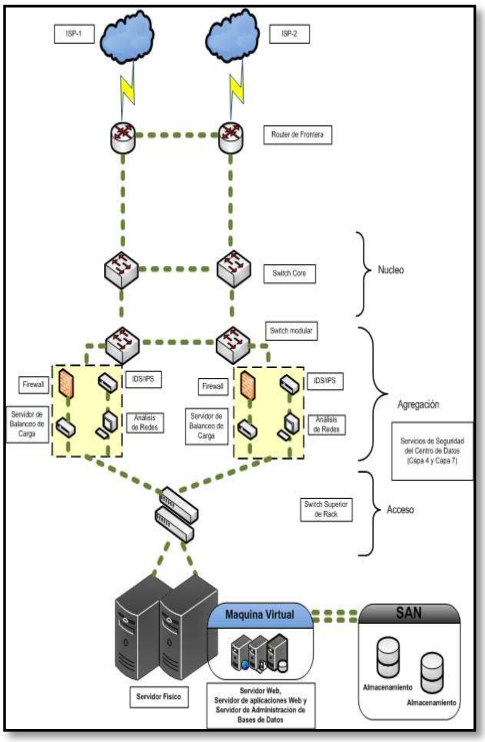

Figura 7. Diseño Topológico del Servicio Plata.

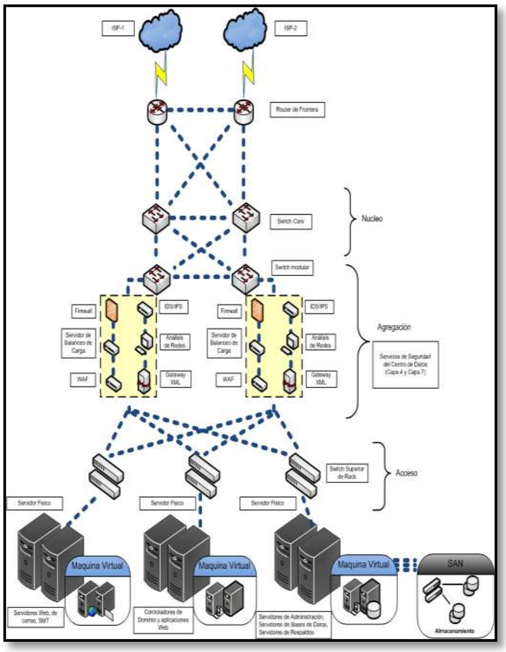

Figura 8. Diseño Topológico del Servicio Oro.

4.3 Seguridad en la topología lógica

La red utiliza una topología lógica en estrella, debido a que los dos switch principales son los encargados de dirigir el tráfico y se tiene una conectividad con routers, switch, rack de comunicaciones y paneles de conexión.

Analizando la topología el throughput requerido en nuestro diseño es 400mpps según los dispositivos presentes. Así mismo en tiempo de conmutación para los dispositivos es de 1 a 3 segundos

4.3.1 Protocolos del Centro de Datos

Los protocolos son un conjunto de reglas usadas por la computadora para comunicarse unas con otras a través de la red.

Para la elección de protocolos de conmutación y enrutamiento se debe tener en cuenta los siguientes criterios:

- ✓ Trafico de la red
- ✓ Ancho de banda, memoria y CPU
- ✓ Capacidad para adaptare ante los cambios
- ✓ Numero de nodos soportados
- ✓ Soporte de autenticidad

Al conocer estos criterios se eligió los siguientes protocolos de enrutamiento y conmutación:

- Protocolo HSRP:

El Hot Standby Router Protocol es un protocolo de nivel 3 de la capa OSI, permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

El protocolo HSRP es utilizado en los routers de frontera del Centro de Datos mediante la siguiente configuración:

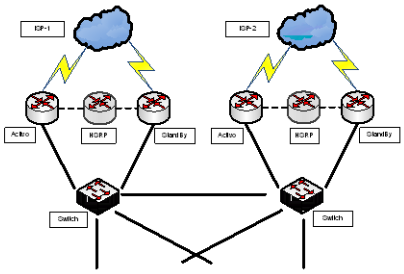

Figura 9. Diseño del Protocolo HSRP

Si el router primario no envía los paquetes en el momento de la trasmisión por un cierto tiempo el router standby asume que el router primario esta fuera de servicio y este se pone en activo.

- Protocolo OSFP

Open Shortest Path First(El camino más corto primero) es un protocolo de enrutamiento jerárquico de gateway interior o IGP que calcula la ruta más corta posible construyendo una base de datos con los enlaces y estado.

- Protocolo STP

Spanning Tree Protocol(Protocolo de árbol extendido) es un protocolo de nivel 2 de la capa OSI, automatiza la administración de la topología de la red con enlaces redundantes.

La función del protocolo es permitir rutas conmutadas duplicadas sin considerar los efectos de latencia de los loops en la red. Su algoritmo calcula la ruta libre de loops.

- Protocolo RSTP

Rapid Spanning Tree Protocol(Protocolo rápido de árbol extendido) puede ser visto como la evolución del estándar 802.1D. El RSTP siendo más rápido que el STP conserva todos los conceptos básicos de la STP e interactúa con él también. Los usuarios familiarizados con la funcionamiento de STP puede aprender rápidamente el nuevo algoritmo ya que tanto la terminología y de base parámetros se han quedado sin cambios.es un protocolo de red de la segunda capa OSI, que gestiona enlaces redundantes. El RSTP es utilizado en la capa de agregación y de acceso del Centro de Datos.

- Switch Multicapa

Son switch que operan en capa 2 según el modelo OSI y puede ser incorporado como un enrutador funcionando en capa 3. Es decir, que tiene las funcionalidades de un enrutador para diferentes VLANs.

Para la seguridad de nuestra red ante posibles ataques maliciosos se va a establecer un protocolo de seguridad.

- Protocolo SSH

Secure Shell(Ordenes Securas) es un protocolo que facilita las comunicaciones seguras entre nos permite manejar por completo la computadora mediante un intérprete de comandos, utilizando la arquitectura de cliente/servidor activando el puerto 22 por default al servidor esperando que algún cliente con SSH se conecte para ofrecerle una sesión segura encriptándola de extremo a extremo.

4.3.2 Servicios del Centro de Datos

En la actualidad el escenario de negocios de las empresas ha sufrido cambios muy rápidos por lo que muy pocas empresas han podido controlar todos los aspectos de la infraestructura de la tecnología informática.

La solución más conveniente es la adquisición de servicios de infraestructura de tecnología informática de un Centro de Datos y pagarlo de acuerdo con lo que se utilice por una simple tasa mensual siguiendo el acuerdo SLA.

Los requisitos que el Centro de Datos va a tener para un buen funcionamiento:

- ✓ Disponibilidad de conexión y servicio las 24/7.
- ✓ Protección contra incendio y otras catástrofes naturales. Igualmente no debe existir en este espacio ningún material que no haga parte de los equipos, es decir material inflamable como el papel o cartón (incluyendo la completa limpieza de los pisos)
- ✓ Control constante del ambiente del espacio, es decir que la temperatura y la humedad estén en constante control y entre un rango recomendado para los Centro de Datos.
- ✓ Sistema inteligente para el acceso a los equipos. Toda persona que ingrese a este espacio debe ser un usuario autorizado y con la seguridad necesaria.

- ✓ El cableado debe estar perfectamente identificado para no tener confusiones, incluyendo identificación de los canales por donde pasa.
- ✓ Tener un sistema ininterrumpido como UPS, para garantizar que no se caigan los servidores, y por supuesto que soporten los equipos

4.3.3 Servicio ofrecidos por el Centro de Datos

El Centro de Datos ofrecerá diferentes tipos de servicios que varía dependiendo del mercado local como son PYMES, Corporaciones, Entidades Financieras y Servicios Privados.

Los servicios del Centro de Datos son:

- Servicios Compartidos
- Servidores Dedicados
- Hosting Dedicados
- Servidores Virtuales
- Servicio de Colocación

Servicios Compartidos

Una plataforma compartida le permite tener disponibilidad de servicios básicos para asegurar su presencia en internet de forma económica y segura, no importa si requiere una base de datos, correo electrónico u hospedaje de un sitio web o de una aplicación.

Cuenta con:

- Sistema Operativo Linux
- Hospedaje de Aplicaciones (Java, PHP, Perl, CGI)
- Hospedaje de Sitios Web (HTML,PHP,JSP,Servlets)
- Servicios de Correo Electrónico (SMTP, POP3,IMAP)
- Servicios de FTP – SSL Compartido
- WebServer: Apache, Tomcat
- Servicios de Bases de Datos (MySql, Postgresql y SQL Server)
- Respaldos Diarios
- SSL
- Seguridad en Puertos
- Tasas de Transferencia Fijas.

Servidores Dedicados (Hosting)

El hospedaje de servidores dedicado que ofrecemos, le permite hacer uso de un servidor con las mejores características de seguridad y accesibilidad desde cualquier parte del país o del mundo, asegurando la disponibilidad de sus sistemas. También ofrecemos servidores alquilados de cualquier marca de última generación o el cliente puede traer su propio servidor siguiendo las especificaciones del Centro de Datos.

El servicio de servidores dedicados cuenta con un sistema operativo con aplicaciones alojado dentro del Centro de Datos. El precio de este servicio varia por las características del servidor, el sistema operativo, las aplicaciones adicionales y el ancho de banda.

Los servidores alquilados cuenta con:

- Linux Server
- Servidores Intel y AMD
- Hospedaje de Aplicaciones
- Hospedaje de Sitios Web
- Servicios de Correo Electrónico
- Servicios de FTP
- Servicios de Bases de Datos (SQL Server, Oracle, MySql)
- Respaldos Diarios
- Expansión de Discos SATA
- Expansión de Memoria
- Tasas de Transferencia Fijas e ilimitadas

5. CONCLUSIONES

- Las diferentes normas necesarias para el diseño de infraestructura de red, se puede concluir que no siempre se cumplirán en su totalidad ya que las características de las instalaciones de un edificio y las exigencias del cliente serán las que definan el diseño real. Lo que se debe procurar es buscar solución que más se acerque a las recomendaciones de las diferentes normas.

- El diseño de una red en la actualidad debe ser analizado profundamente, es importante citar algunos factores que influyen para lograr un buen diseño, entre estos tenemos: la flexibilidad con respecto a los servicios soportados, la vida útil requerida, el tamaño de las instalaciones, la cantidad de usuarios que requerirán los servicios de una red y lo esencial los costos que implican. Al tomar en cuenta estos factores no se debe dudar en utilizar el mecanismo que provea las facilidades de estandarización, orden, rendimiento, durabilidad, integridad y la facilidad de expansión como lo provee el cableado estructurado.

- Para mejorar el consumo eléctrico del Centro de Datos se instalara en los servidores máquinas virtuales mejorando la eficiencia y disminuyendo tanto la carga que consume los equipos como el espacio en los rack.

- Usando la tecnología de los IPS/IDS en puntos estratégicos de la red, nos permite ofrecer mayor confiabilidad y robustez en el desempeño de nuestros servicios, garantizando la seguridad de la red en el Data Center.

- El Cloud Computing en la actualidad está en auge, debido a su gran utilidad en el mercado, y apoyo a las entidades de cualquier área de negocio.

- Tiene muchas ventajas la virtualización porque ayuda a reducir costos, reduce el tiempo de espera en recuperación a fallo, puede garantizar la seguridad en los activos de la empresa a una menor inversión.

- Además el Data Center cumple con todos los requisitos para el cumplimiento de la norma PCI-DSS, lo cual es un requerimiento en la actualidad para todas las empresas que manejas tarjetas de crédito, esto produce menos costos para la empresa en caso de multa por incumplimiento.

6. RECOMENDACIONES

- Se recomienda que al implementarse esta solución, se haga una certificación de la red ya que los estándares lo recomiendan. Esto será de suma importancia para ubicar posibles fallas en la instalación.

- Seleccionar una buena plataforma de virtualización que cumpla con las necesidades que se desea alcanzar.

- Definir de una manera adecuada los equipos a utilizarse, tomando en consideración la plataforma de virtualización escogida, y así evitar que se produzca errores en la ejecución de las aplicaciones de los clientes.

- Se debe profundizar aún más los conocimientos relativos a la seguridad en redes, para poder estar preparados con un plan de recuperación ante cualquier posible amenaza que pueda surgir, una vez que se encuentre en producción los servicios del Data Center.

- Se debe cumplir con las políticas de seguridad de la organización, antes de realizar cualquier modificación en los parámetros de configuración de los dispositivos de red, ya que es importante extraer copias de seguridad de la información que es relevante para la organización.

- Para realizar una administración adecuada de la red se recomienda considerar aspectos como el monitoreo, atención a fallas y seguridad, por lo que se deberá contar con un administrador de red que la mantenga activa, resuelva problemas eventuales que se puedan presentar en cuanto a permisos y autorizaciones de acceso y además realice un mantenimiento periódico tanto de hardware como de software.

- El sistema IDS/IPS también simplifica la tarea de verificar y categorizar las amenazas en los informes que se presentan a la administración ejecutiva. Esta información sólida ayuda a la dirección a aceptar la administración de la seguridad adicional.

7. REFERENCIAS

[1] CISCO: Seguridad y Virtualización en el Data Center:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.html.

[2] GEORGE GILDER: Las fábricas de la información:
http://www.wired.com/wired/archive/14.10/cloudware.html?pg=1&topic=cloudware&topic_set=

[3] MOVISTAR: Cloud Computing:

http://www.mcloud.cl/

[4] DOSMO KUUSISTO: La Arquitectura de un Data Center Eficiente:
http://www.isertec.com/datacenter_summit/_pres_pdf/003-10a_m_-Osmo_Kuusisto_La Arquitectura en un Data Center Eficiente.pdf