DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

"PROYECTO DE TRABAJO DE GRADO"

"Propuesta de Implementación del proceso Gestión de Continuidad de Servicios de TI de ITIL V3 en la Empresa YP Directories, en la Ciudad de Santo Domingo, Rep. Dom. en el periodo Septiembre – Diciembre 2014".

Proyecto de Trabajo de Grado para optar por el título de:

INGENIERO EN SISTEMAS DE COMPUTACION

SUSTENTANTES

Edward Rodríguez 2007-1627
Raúl Vanderhorst Reynoso 2010-0927
Johanna Peralta 2011-0010

ASESOR

ING. SANTO NAVARRO

Santo Domingo, Rep. Dom.
2014

“Propuesta de Implementación del proceso Gestión de Continuidad de Servicios de TI de ITIL V3 en la Empresa YP Directories, en la Ciudad de Santo Domingo, Rep. Dom. en el periodo Septiembre – Diciembre 2014”.

AGRADECIMIENTOS

Primero que nada, quiero agradecer a Dios por haberme permitido llegar hasta este punto.

También quiero agradecer al Sr. Jamie Watter, autor del libro *Disaster Recovery, Crisis Response and Business Continuity*, quien tuvo la amabilidad de siempre responder mis inquietudes en cuando al tema de Continuidad de Servicios de TI, lo cual ayudo al desarrollo de este trabajo de grado.

A mi amiga Johanna Peralta, quien siempre formó parte importante para mí en todo el proceso universitario, siendo siempre mi compañera de grupos y dándome apoyo cada vez que lo necesitaba.

Por último, quiero agradecer a mis compañeros de trabajo y nuestro asesor, el Ing. Santo Navarro, quienes siempre estuvieron en disposición de contestar todas las preguntas referentes al tema de investigación.

Edward Rodríguez Vásquez

A DIOS TODOPODEROSO:

Gracias por haberme dado la vida y el bien de la inteligencia. Por haberme sabido bendecir para dirigirme al lugar hasta donde he llegado.

A LA UNIVERSIDAD APEC:

Por haberme dado la oportunidad de haber estudiado y por haber sido en ella donde adquirí los conocimientos, para hoy ser alguien útil a la humanidad.

A NUESTRO ASESOR:

Ing. Santo Navarro gracias por habernos sabido instruir, por su esfuerzo y dedicación, quien supo orientarnos con sus conocimientos, paciencia y experiencia. Aparte de su gran motivación, para ayudarnos a lograr concluir nuestros estudios con éxito.

Existe una infinidad de personas que han sido parte de esto, que han sido parte de mi vida estudiantil, como vida profesional, a las cuales me gustaría agradecerles su amistad, los consejos en el transcurso de todo este tiempo, el apoyo incondicional y el haberme dado el ánimo y el estar acompañándome en los momentos que se presentan como "difíciles" en la vida.

Unas siguen aquí conmigo y otras solo las puedo tener en mis recuerdos almacenándolas en mi corazón, sin importar el ¿Que haya pasado?, el ¿Dónde se encuentren?, quiero aprovechar para darle las gracia por haber dejado una huella en mí, por todo lo que me han ofrecido y me brindaron pero sobre todo agradecer sus bendiciones. Gracias por formar parte de mí.

PARA TODOS ELLOS:

Muchas gracias y que el gran DIOS TODOPODEROSO los bendiga.

Raúl Vandelhorst Reynoso

En primer lugar le doy gracias a Dios, por permitirme alcanzar esta meta. A mí amigo Edward Rodríguez, quien formó parte de todo este proceso universitario, y juntos logramos vencer todas la barreras que se presentaron.

A nuestro asesor Santo Navarro, por compartir sus conocimientos y guiarnos durante el desarrollo de este trabajo.

Johanna Peralta

DEDICATORIAS

Le quiero dedicar este logro a las dos personas más importantes de mi vida: mi madre y mi padre, quienes siempre se preocuparon por mi superación y educación y siempre me apoyaron en todas las decisiones que he tomado en la vida.

Edward Rodríguez Vásquez

A DIOS TODOPODEROSO

Gracias por haberme prometido a mí y a mis padres que este día llegaría, por hacer realidad este sueño tan anhelado, por haberme guiado por los caminos de la sinceridad, honestidad y responsabilidad y sobre todo por darme fuerzas aun cuando los deseos se estaban perdiendo.

A MI MAMA:

Marcela Reynoso

Quiero darte las gracias por haber confiado en mí, por haberme puestos las pilas para seguir adelante cuando sentía que no podía seguir. Por tu palabra de aliento "Descuida mijo que por lo que hoy lloramos mañana reímos". Sin lugar a dudas eres la única que no se sorprende de este logro, gracias por creer en mí, por haberme dado la vida, por ayudarme a correr este camino, luchar estas batallas y sobre todo gracias por todo el amor que me has dado todo este tiempo.

¡Te quiero mucho y Gracias Mami!

A MI PAPA:

Raúl Vanderhorst

Gracias por ser ese padre ejemplar de cual no se puede pedir más, por haberme dado tu apoyo y ayuda que he necesitado siempre, por enseñarme los valores que te inculcaron desde pequeño para hacerme el hombre que soy hoy. Por darme los consejos para llevarme por el camino del bien. Por esforzarte día a día para que hoy llegue este momento y sobre todo por quererme tanto.

¡Te quiero mucho y Gracias Papi!

A MIS ABUELOS MATERNOS:

Rafael Reynoso y Juana Reyes (fallecidos)

Gracias por ser las personas que estuvieron conmigo en la ausencia de mis padres, por ser aquellas personas que le dieron la vida a mi madre, por enseñarla e instruirle para que sea la gran madre que es hoy en día y en especial a ti mi Ma' que fuiste aquella que siempre confió en mí, que siempre dijo "Mi niño vas a llegar bien lejos", por ser mi motor y aun sin estar hoy físicamente conmigo pienso en usted y este triunfo va bien lejos. A ustedes que donde quiera que se encuentren, sé que estarán felices porque su niño hoy cumple uno de sus mayores deseos.

¡Extrañándole siempre, los quiero Ma' y Pa'!

A MIS ABUELOS PATERNOS:

Raúl Vanderhorst y Elvira Batista (fallecidos)

Gracias por ser aquellas personas que le dieron la vida a mi padre, por darle la sabiduría y enseñarle el camino por el cual guiarme para que hoy en día sea quien soy. Gracias por creer en mí.

¡Los quiero mamá y papá!

A MIS HERMANAS:

Katherine y Leslie Vanderhorst Reynoso

Gracias a ustedes por ser aquellas personas que me han tomado de ejemplo, por sus buenos deseos y su confianza en mí. Por haberme dado el apoyo que necesite para seguir adelante. Hoy termina uno de mis sueños y espero que conmigo compartan esta alegría y que le sirva de estímulo para que puedan realizar sus sueños y verlos convertidos en realidad.

¡Las quiero mucho Kat y Les!

A MI MADRINA:

Nelly Familia

Gracias por ser usted uno de los motores de mi vida, por ser la persona que aparte de madrina es aquella que me ha adoptado como su hijo, por sus buenos consejos y por todo el cariño que ha sabido darme. Gracias por su firmeza y seguridad y por ser la hermana que mi mamá no tuvo. Este triunfo va por usted.

A MIS TIAS:

Gladys García, Denys Reyes, **Rosalía Batista**

Gracias a ustedes porque siempre conté con su ayuda y oraciones, por creer en mí y por sus buenos deseos y por ser ese soporte que siempre ocupara un lugar especial en mi corazón. *¡Muchas Gracias!*

A MI COMPAÑERA DE UNIVERSIDAD:

Stephanie Pettit

Gracias por tu compañía, por compartir conmigo todos los momentos de alegría y tristeza, por tu preocupación por ti para conmigo. Por siempre darme ánimo y por decirme "Descuida que cuando esto termine podrás decir: LO LOGRE"

A MIS AMIGO@S:

LMG, Gteatro Unapec, Los Mastadores y aquellos que son independientes

Gracias por saber comprender mis sacrificios, por sus consejos y apoyo a lo largo de todo este largo recorrido. Gracias por creer en mí y por sus buenos deseos para conmigo

A MIS COMPAÑEROS DE TESIS:

Johanna Peralta y Edward Rodriguez

Gracias por su entera dedicación en la elaboración de este trabajo y por saber superar los obstáculos presentados para la realización de la misma, para que hoy podamos ver esto llegar felizmente a su término. *¡Muchas Gracias!*

Raúl Vanderhorst Reynoso

Le dedico este trabajo a mis padres por darme la vida y a mi esposo por apoyarme en cada uno de los pasos que he dado para salir adelante. Gracias a ellos he podido seguir adelante en la vida y luchar para lograr cada uno de mis objetivos y alcanzar mis metas.

Johanna Peralta

INDICE DE CONTENIDO

4. CAPITULO IV - ALMACENAMIENTO Y SEGURIDAD DE LA INFORMACIÓN EN LOS CENTROS DE DATOS

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRAFICOS

RESUMEN EJECUTIVO

Hoy en día, las empresas dependen mucho de los servicios de tecnología para la toma de decisiones y para dar soporte a los procesos de negocios. Si estos servicios son interrumpidos, la empresa podría verse afectada de manera significativa. Es por esto que toda organización debe de contar con un Plan de Continuidad de Servicios de TI efectivo que le permita continuar con sus operaciones normales o retornar a ellas lo más rápido posible luego de una interrupción de servicio.

En este proyecto se propone la implementación del Proceso de Gestión de Continuidad de Servicios de TI de ITIL en la Empresa YP Directories. ITIL es un código de buenas prácticas diseñado para mejorar la gestión de servicios de TI de las organizaciones y alinearlos con las necesidades del negocio. El proceso comprende cuatro pasos: 1. Iniciación, 2. Requerimientos y Estrategias, 3. Implementación, 4. Gestión Operativa.

Con el fin de validar si la inversión de la implementación es aconsejable, se llevó a cabo un Análisis de Factibilidad por medio del Método del Valor Presente Neto (VPN), tomando en cuenta las alternativas propuestas para el plan de continuidad.

INTRODUCCION

Anteriormente el departamento de TI era visto como un centro de costos para las organizaciones. Esto era debido a que las inversiones que hacia el departamento de TI eran consideradas como gastos y no como inversiones. Hoy en día, este paradigma ha cambiado por completo. El departamento de TI ha dejado de ser visto como un soporte de oficina y ha pasado a formar parte de la estrategia de las organizaciones ayudando a estas a ser más eficientes en sus operaciones y mejorar los servicios que ofrecen.

Los servicios de TI se vuelven cada vez más importantes para los negocios porque de la eficiencia y disponibilidad de estos depende en gran parte el éxito de la organización. Hoy en día, las empresas buscan y necesitan soluciones tecnológicas que les permitan estar a la vanguardia en un mercado global tan competitivo y tienen como reto buscar métodos tecnológicos eficientes y que estos vayan alineados con las estragáis del negocio.

Es por todo lo anteriormente descrito que los servicios de TI deben mantenerse en constante funcionamiento. Es indispensable que su infraestructura se mantenga siempre operando y disponible y que, ante incidentes críticos que puedan provocar interrupciones que impacten de forma negativa al negocio, la organización pueda seguir ofreciendo sus

servicios críticos. Para poder lograr esto es necesario que las organizaciones cuenten con un Plan de Continuidad de Servicios de TI.

El propósito general de un Plan de Continuidad de Servicios de TI (ITSCM) es dar soporte en lo general al proceso de Gestión de Continuidad de Negocio (BCM) y asegurarse de gestionar los riesgos que puedan afectar a los servicios de TI de modo que se pueda cumplir con los Acuerdos de Niveles de Servicios. El proceso de Gestión de Continuidad de Servicios de TI está definido bajo el código de buenas prácticas de ITIL v3.

ITIL es un conjunto de buenas prácticas que tiene como objetivo gestionar de forma eficiente los servicios de TI.

La siguiente propuesta tiene como objetivo principal ofrecer una respuesta efectiva frente a las amenazas asociadas a los servicios de TI que dan soporte a los procesos de negocio de la Empresa YP Directories. La propuesta hace su enfoque en el ciclo de vida del proceso de ITIL v3, Gestión de Continuidad de Servicios de TI (ITSCM).

PLANTEAMIENTO DEL PROBLEMA

Las empresas hoy en día dependen mucho del Departamento de Tecnología de la Información, debido a que este sirve como soporte a todos los procesos de negocios ofreciendo servicios tecnológicos de calidad y la indisponibilidad de estos servicios de forma prolongada podría llegar a impactar al negocio negativamente.

En el Global Disaster Recovery Index 2012 publicado por Acronis, 6 mil funcionarios de Tecnologías de la Información (TI) reportaron que los desastres naturales causaron sólo 4% de las interrupciones de servicio, mientras incidentes en las instalaciones de los servidores (problemas eléctricos, fuegos y explosiones) representaron el 38%. Sin embargo, errores humanos, actualizaciones problemáticas y los virus encabezaron la lista con el 52% (Pérez L. , 2013).

En un estudio realizado por CA Technologies (2011), en Europa, a 1808 organizaciones en 11 países sobre los efectos de la inactividad de los servicios de TI y recuperación de datos, se identificó que las organizaciones europeas de más de 50 empleados están perdiendo en conjunto más de 37 millones de horas hombre al año por el tiempo de inactividad de TI y recuperación de datos. En promedio, cada empresa pierde 552 horas-hombre por año. En la investigación salió a relucir que la mayoría de estas

interrupciones pudieron haber sido evitadas si se hubiese implementado una mejor estrategia de continuidad de servicios.

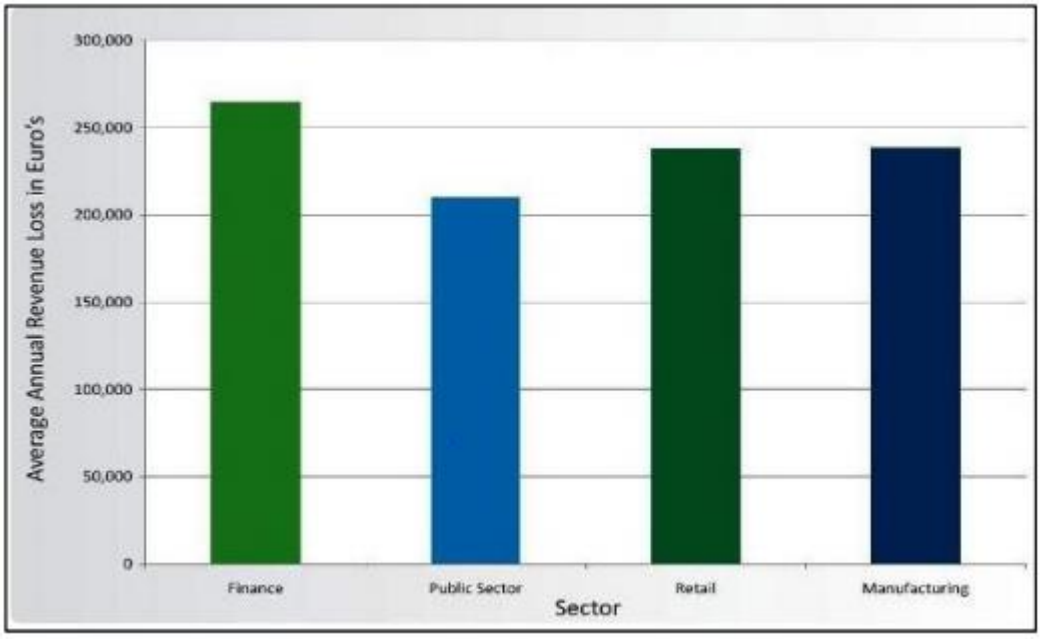

Gráfico 1. Costo evitable del tiempo de inactividad[1]

El estudio también revela cuando existe un downtime en los servicios críticos de TI los ingresos de la organización quedan reducidos a 36%. El departamento más afectado por la inactividad de servicio es el departamento de operaciones con un 60% Seguido por finanzas con un 44% y ventas con un 42%.

[1] Fuente: Tesis Modelo de Continuidad de Negocio y Recuperación de Desastres Basada en la Nube para la EMPRESAREYES & HERMANOS

La empresa YP Directories ha venido presentando algunos inconvenientes con su infraestructura tecnológica que han producido paros en las actividades críticas del negocio, provocando así impactos negativos en la organización. Dentro de los problemas identificados se pueden mencionar los siguientes:

- Switch de acceso defectuoso, el cual se apaga solo y deja sin sistema a varios departamentos.
- No existe redundancia de cableado estructurado en la conexión hacia el proveedor principal.
- No existe puerta cortafuegos en el centro de datos ni sistema de alarma inteligente contra incendios.
- Existen equipos de red críticos sin garantía y sin redundancia.

Debido a estas problemáticas, se ha podido llegar a la conclusión de que la empresa responde de forma reactiva a los problemas y que no cuenta con un plan de continuidad de servicios de TI que le ayude a minimizar el impacto del downtime de los servicios críticos y estar preparada ante eventos tales como desastres naturales (terremotos, huracanas, etc), perdida de conectividad en los sistemas y otros eventos que pueden impactar al negocio negativamente.

OBJETIVOS DE LA INVESTIGACION

Objetivo General

Dar continuidad a los Servicios de TI de la Empresa YP Directories a través de la implementación del proceso de Gestión de Continuidad de Servicios de TI de ITIL v3.

Objetivos Específicos

- Establecer la calidad de Servicios TI a través de la estrategia de continuidad de negocio.

- Definir el plan de continuidad basado en ITIL v3.

- Especificar las alternativas a utilizar para prevenir interrupciones de servicios.

- Realizar un análisis del impacto al negocio (BIA).

- Implementar un análisis de riesgo en los procesos asociados a los servicios de TI

- Identificar los riesgos asociados a los servicios críticos de TI.

- Identificar cuáles son los servicios que ofrece el departamento de TI.

- Identificar los tiempos máximos de inactividad de servicios de TI tolerables por la organización en relación a su amenaza y vulnerabilidad.

- Conocer las los costos de operación de los servicios críticos del Centro de Dato de la empresa YP.

METODOLOGIA DE LA INVESTIGACION

METODO

Los métodos utilizados en el proyecto de investigación son:

- La observación, ya que se observaron directamente los elementos de infraestructura que soportan los servicios de TI y luego se analizaron los riesgos asociados a estos.
- Análisis, ya que se identificaron las partes que forman parte del problema así como su relación causa-efecto entre los elementos relacionados con la investigación.
- Método inductivo.

TECNICAS

Las técnicas de investigación de recolección de datos que se utilizaran en el proyecto de investigación serán entrevistas, cuestionarios y la observación. De esta forma se pudieron obtener datos confiables que sirvieron como soporte para la investigación y permitieron dar las recomendaciones de lugar.

TIPO DE ESTUDIO

El tipo de estudio que se implementado durante la realización de este proyecto fue de carácter descriptivo-explicativo.

1. CAPITULO I - ASPECTOS GENERALES

1.1. Antecedentes

YP Directories USA es una empresa norteamericana dedicada a la creación de directorios telefónicos. Un Directorio Telefónico es un libro o catálogo con los teléfonos publicables de los abonados de las compañías telefónicas. Este contiene una gran gama de información relacionada con personas, lugares, servicios, productos y profesiones, las cuales son reunidas y compaginadas en forma clara y sencilla, facilitando la labor de vendedores y compradores.

La primera Guía Telefónica se publica en el 1878 en la Primera Feria Mundial en New Heaven, EEUU. Constaba de una lista de 50 teléfonos en una sola hoja de papel. La lista fue organizada en diferentes categorías para localizar un producto o un servicio como:

- Residencias
- Mercado de Carnes
- Establos

YP Directories USA fue fundada en 1920 por el pionero de las Páginas Amarillas Martin M. Marschall, y ha sido un líder en la industria por más de 100 años,

proporcionando un servicio al cliente excepcional y una inigualable gama de productos generadores de posicionamiento a nuestros socios comerciales.

1.2. Estructura Organizacional

YP Directories es filial de Directories YP USA en República Dominicana. En esta localidad de la empresa se encuentran situados la mayoría de los Departamentos de Producción y de Tecnología. Esta empresa funciona dentro del régimen de Zona Franca Especial vigente en República Dominicana. Situada en el centro de la ciudad de Santo Domingo, YP Directories cuenta con una estructura organizacional que está dividida en tres grandes grupos: Producción, Tecnología de Información y Administrativo. El grupo de Producción está compuesto por los departamentos responsables de trabajar con los directorios que publicamos y productos digitales que ofrecemos a nuestros clientes. El grupo de Tecnología de Información brinda soporte en la creación, manejo y mantenimiento de diversos sistemas utilizados por Berry a nivel global. El grupo Administrativo se encarga de gestionar la empresa dando soporte a las necesidades de los empleados.

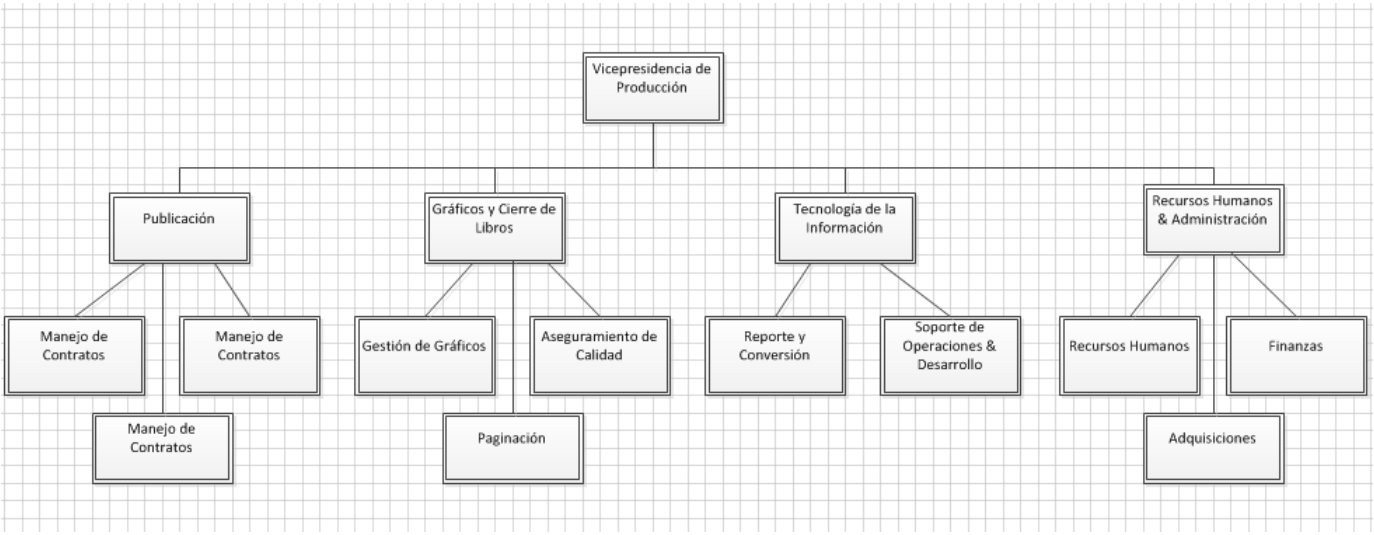

Figura 1. Organigrama organizacional de la Empresa YP Directories. Fuente: Propia

1.3. Misión

Ser un proveedor líder de direccionamiento local y soluciones de marketing, permitiendo a nuestros clientes de pequeñas y medianas empresas generar clientes potenciales y efectivamente llegar a los consumidores a través de múltiples medios de comunicación.

1.4. Valores

- Pasión por el Servicio
- Orientación a la acción
- Integridad y Respeto
- Responsabilidad Individual
- Establecer el estándar

1.5. Visión

Crear relaciones a través de experiencias esenciales e información clave.

2. CAPITULO II - CENTRO DE PROCESAMIENTO DE DATOS (CPD)

2.1. Concepto de Centro de Procesamiento de Datos

Hoy en día las empresas necesitan un Data Center, debido a que allí se maneja todo el flujo de información que permite a las instituciones manejar y mantener las operaciones que se realizan día a día.

Un Data Center (centro de cómputos, centro de proceso de datos), es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento. Generalmente incluye fuentes de alimentación redundantes o de respaldo, conexiones redundantes de comunicaciones, controles de ambiente (por ejemplo, aire acondicionado) y otros dispositivos de seguridad. (ITC Group, 2013).

En definitiva, podemos definir un Data Center como un centro donde se almacenan datos, estos son tratados y son divididos entre el personal o procesos para consultar y/o modificar.

2.2. Objetivo de los centros de Procesamiento de Datos

El principal objetivo de un Data center es el de poner en marcha las aplicaciones centrales de la empresa y así almacenar los datos operativos ya que con estos se pueden ofrecer los medios de recuperación de desastres.

Otro de los objetivos de este, es el de complacer las necesidades que pudiesen presentarse en un presente y futuro con el fin de ofertar las soluciones más completas y con mayor fiabilidad para así garantizar el éxito.

2.3. Importancia de los Centros de Datos

Como se explica al inicio del capítulo los Data center son de vital importancia para la empresa debido a que estos:

- Garantizan mayor disponibilidad de los servicios de tecnología de la información para la empresa.

- Ofrecen continuidad en el servicio de la institución esto significa que la interrupción en los procesos es muy bajo ya que este ofrece mayor potencial en redundancia y monitoreo.

- Dispone de una mayor agilidad, ya que en un centro de tecnología de la información se genera agilidad en nuevas implementaciones y estas no tienen que ser lanzadas en lugares físicos.

2.4. Tipos de Centros de Datos

2.4.1. TIER I

Es uno de los tipos de data center más susceptible a las interrupciones. Este cuenta con un sistema de A/C (aire acondicionado) y distribución de energía; este puede contener piso técnico, un UPS o un generador de electricidad si los contiene puede que no tengan redundancia y que existan varios puntos únicos de falla.

Esta infraestructura debe de estar fuera de servicio como mínimo una vez al año para darle mantenimiento y/o realizar operaciones. La tasa de disponibilidad de este tipo de Data Center es de 99.671% del tiempo.

Este es aplicado en empresas pequeñas que poseen una infraestructura de TI solo para trabajar en procesos internos, compañías que utilizan la web como una herramienta de mercadeo y empresas que basan su negocio en internet y que no requieren calidad en sus servicios.

2.4.2. TIER II

Este tipo de Data Center posee componentes redundantes que lo hacen menos susceptible a las interrupciones tanto planeadas como no planeadas. Poseen un piso falso, UPS y generadores eléctricos aunque solo están conectados a una línea de distribución eléctrica. Al estar conectado a una sola línea de distribución eléctrica el mantenimiento en esta o en otros componentes puede causar una interrupción del procesamiento. Este ofrece una tasa de disponibilidad máxima de 99.749% del tiempo.

Este tipo también se utiliza en pequeñas empresas y que el uso de TI este limitado solo a las horas de trabajo y empresas que no ofertan servicios online o real-time.

2.4.3. TIER III

Este tipo de Data Center permite trabajar con cualquier actividad planeada sobre cualquier componente sin interrumpir las operaciones. El mantenimiento planeado, reparaciones o reemplazar algún componente, quitar y/o poner cualquier elemento, realizar pruebas entre los componentes, entre otras son actividades planeadas.

Contienen suficiente capacidad y existen doble línea de división de componentes y esto es porque mientras se trabaja con una línea como por ejemplo algún tipo de mantenimiento, la otra trabaja con una totalidad de carga. En actividades no planeadas este TIER puede causar una interrupción en el Data Center. Este ofrece una tasa de disponibilidad máxima del Data Center de 99.982% del tiempo.

Es utilizado en compañías que ofrecen soporte las 24 horas los 7 días de la semana como son los centros de servicios e información. Empresas que dan soporte a los procesos automatizados en múltiples zonas horarias.

2.4.4. TIER IV

Es el tipo de Data Center más completo, ya que este ofrece la capacidad para trabajar con cualquier actividad planeada sin contar con interrupciones en las cargas críticas, este además de funcionar tolerando fallas permite continuar con las operaciones ante un evento no planeado. Este contiene dos líneas de distribución que están activas simultáneamente, esto significa que trabaja con dos sistemas de UPS independientes. La tasa de disponibilidad que este tipo de Data Center ofrece es de un 99.995% del tiempo.

Se utiliza en compañías que ofrezcan presencia en un mercado internacional, que ofrezcan servicios en mercados altamente competitivos las 24 horas del día, los 365 días del año. Un ejemplo a esta son las compañías que se basan en comercio electrónico y compañías que oferten el acceso a los procesos y a realizar transacciones en línea.

2.5. Climatización

Hablar de climatización es referirnos a establecer circunstancia de temperatura, humedad, pureza y velocidad del aire, creándolo en espacios donde sea necesario para la comodidad del usuario y mantener en buen estado de las cosas, como equipos electrónicos.

En una definición más técnica, la climatización es un proceso de tratamiento del aire que se efectúa a lo largo de todo el año, controlando en los espacios interiores la temperatura, la humedad, la pureza y velocidad del aire, para crear condiciones adecuadas para la comodidad del usuario y lograr el intercambio de aire a los espacios que no pueden ser ventilados de manera natural o que requieran condiciones especiales de temperatura controlada (Colocho, Daza, & Guzmán, 2011).

2.6. Climatizar un Centro de Procesamiento de Datos

Climatizar un Data Center (CPD) es referirnos a las normas creadas para su funcionamiento. La climatización de estos espacios obliga a avalar condiciones esenciales de temperatura y humedad y para esto es necesario utilizar unidades de

alta precisión. Antes de arrancar con la instalación es obligatorio el cuantificar y evaluar las cargas térmicas del espacio a climatizar y adecuarlo a los equipos informáticos.

La conducción de aire climatizado debe estar previamente filtrada, para luego llegar a los recintos donde se encuentran los equipos informáticos, ahí es donde se concentra la mayor proporción de calor. Las ventanillas o rejillas de aire deben ubicarse en el suelo o en su defecto en el techo, por medio de estos conductos el aire que va dirigido al compartimiento debe estar en sobrepresión para evitar las entradas de polvo del exterior (Nuno, Rivas, & Ares, 2006).

2.7. Tipos de Aires Comerciales

Actualmente en el mercado podemos encontrar una gran variedad de sistemas de aires acondicionados, a continuación se detallan los tipos de aires más comunes y utilizados.

2.7.1. Consolas de Pared

Es uno de los modelos que se adaptan a la necesidad de locales pequeños y utilizan una fácil instalación y manejo en cuanto a mantenimiento se refiere.

2.7.2. Consola de Techo

Es utilizado al igual que el de pared en locales pequeños y con una alta visita de clientes que se encuentran en ambientes abiertos, este recibe un mantenimiento más frecuente.

2.7.3. Precisión

Son aquellos que están hechos para complacer los requerimientos de cargas electrónicas densas, están creados con la finalidad de ofrecer un enfriamiento que perdure todo el ano las 24 horas del día. Diseñado para trabajar bajo los lineamientos requeridos en equipos electrónicos que necesitan un nivel preciso de humedad y su calidad en cuanto al aire que reciben.

2.7.4. Roof-Top

Esta es una unidad más compacta y permite seleccionar la ubicación de salida de los conductos.

2.8. Control de Humedad

En cuanto a la humedad, como la temperatura en los Data Centers deben ser exactas, debido a que si la humedad sube mucho puede suscitar problemas de condensación en las partes electrónicas. En tanto si el ambiente se vuelve muy seco, la electricidad estática que resulta de un simple dedo puede echar a perder los componentes y alterar la información. Asimismo sus medios de almacenamiento pueden sufrir perdida de oxidación lo que incrementa la posibilidad de pérdidas o de alteración de la información.

Para evitar los casos anteriores es necesaria una humedad relativa de un 45% con variante no mayores de ±5% para un Sistema de Aire Acondicionado de Precisión. Ya que estos tienen la exactitud y precisión necesarias para operar en el modo requerido (humidificación, enfriamiento o calefacción) para mantener el ambiente en los

parámetros seleccionados cosa que los sistemas de confort no lo tienen. (Nuno, Rivas, & Ares, 2006)

2.9. Distribución de Aire

Para el reparto del aire climatizado se utilizan varias formas dependiendo de la conformación de la máquina y a las singularidades propias que tiene el local.

Existen cuatro forma para la circulación del aire:

1. Insuflación en la región del suelo, esta se realiza mediante suelo falso.
2. Insuflación por encima de la maquina
3. Insuflación mediante rejillas frontales
4. Utilizando el sistema displacement: es un método de distribución de aire en el que el aire refrigerado es insuflado a baja velocidad al nivel del suelo. La circulación del aire se hace por convección como resultado de la carga térmica existente en el local. (Nuno, Rivas, & Ares, 2006).

2.10. Energía Eléctrica en un Centro de Procesamiento de Datos

Se puede definir la energía eléctrica como la forma de energía resultante de la existencia de la diferencia de potencial entre dos puntos, posición que permitirá establecer una corriente eléctrica entre los puntos si se los colocan en contacto por intermedio de un conductor eléctrico para obtener el trabajo mencionado

2.11. Componentes de Suministro de Energía de un Data Center

2.11.1. UPS

Sistema de alimentación ininterrumpida (SAIs), en inglés Uninterruptible Power Supply (UPS). Este es un sistema que con sus baterías u otros elementos que almacenan energía, presta energía eléctrica limitada. Su principal objetivo está en ofrecer continuidad al suministro eléctrico en caso de un fallo, pero además puede ofrecer corrección y filtra los defectos que tenemos en el suministro.

2.11.2. Tipos de UPS

En la actualidad se pueden encontrar una gran diversidad de diseños de UPS. Dependiendo el tipo de modelo existen tres renglones de clasificación para estos.

2.11.3. Tipo Fuera de Línea (OFF-LINE)

Son aquellos que solo tienen una alimentación principal, un cargador para su batería, la batería, un inversor de DC/AC, Relé de transferencia, sus respectivos filtros y salida hacia la carga.

Este tipo de UPS funciona con la energía de la calle. Esta llega a la transferencia y al cargador simultáneamente para así cargar la batería.

2.11.4. Tipo en Línea Interactiva (INTERATIV-LINE)

Este posee su alimentación principal, sus filtros, un regulador para el voltaje, convertidor, sus baterías, filtros y salida hacia la carga.

Este funciona al igual que el anterior con la energía de la calle. Esta se conduce a los filtros que posee de entrada, para luego pasar al regulador de voltaje, pasando por el convertidor y así cargar las baterías.

2.11.5. Tipo en Línea (ON-LINE)

Este posee su alimentación principal, un supresor para los bajos voltajes, un corrector de factor para la potencia, su rectificador, cargador, batería inversor de DC a AC y salida hacia la carga. Además posee un conmutador dinámico de bypass que se utiliza para ofrecer un servicio de mantenimiento en el UPS sin desconectarlo.

Funciona cuando la energía de la calle llega al supresor, luego pasa al corrector de factor de potencia, pasa por el rectificador, luego por el cargador y posteriormente a la batería; de la batería pasa al inversor de DC a AC y finalmente la carga.

2.11.6. Grupos Electrógenos

Son los encargados de ofrecer energía eléctrica mediante otra fuente alternativa a la compañía de energía eléctrica como puede ser gasoil, biodiesel, queroseno, pilas de combustibles, hidrogeno, entre otras.

2.11.7. STS (Static Transfer System)

Esto se conmuta entre dos fuentes de alimentación eléctrica para alimentar equipos que equipan una única fuente de alimentación y se deben proteger en caso de fallos eléctrico.

2.11.8. Cableados de Energía

Son elementos de distribución que aseguran una instalación ordenada y para dar el mantenimiento y sus modificaciones.

2.11.9. PDU

Son regletas de conexión eléctrica según los tipos de conectores, su potencia, distribución interna en el rack, su posibilidad de monitorización y del control remoto del encendido de la toma, con programación para alertas de consumo excesivo en las líneas.

2.11.10. Tierra Física

Es una instalación eléctrica que permite absorber descargas eléctricas, conformada por 1 varilla de cobre de 3mts. Enterrada bajo el nivel del suelo y de preferencia en un lugar con humedad, y es complementado con sales y carbón para mejorar su asimilación de descargas.

3. CAPITULO III - CONECTIVIDAD Y NETWORKING

3.1. Modelo OSI y Modelo TCP/IP

Antes de la década de los 80, las redes estaban limitadas a tener todos los dispositivos de una misma marca, ya que no era posible hacerlo con equipos de fabricantes diferentes. Para el año 1984 la Organización Internacional de Normalización, (ISO), creó el conocido modelo de sistemas de interconexiones abiertas (OSI), el cual permite la interoperabilidad entre equipos de diferentes fabricantes, lo que a su vez causaba un gran impacto porque las limitaciones que existían hasta ese momento se reducirían de manera muy significativa.

El modelo de interconexión de sistemas abiertos (OSI), es el ejemplo típico o patrón de los protocolos de capas, pero no es en sí mismo un protocolo (o conjunto de protocolos), sino más bien la definición cuidadosa de las capas funcionales para la conformación de todos los protocolos modernos. El objetivo es establecer estándares mundiales de diseño para todos los protocolos de datos de telecomunicaciones con la idea de que todos equipos que se fabriquen sean compatibles (Perez, 2003, p. 42).

Este modelo consta de 7 capas y divide las funciones de comunicación de datos entre cada una de ellas, entregando a cada capa su propia función específica. Esto permitió lograr una serie de ventajas entre las que se destacan:

- El desarrollo de varios protocolos que permiten la comunicación entre diferentes tipos de ordenadores para poderse comunicar en diferentes tipos de redes.

- Fácil escalabilidad en la red, ya que permite que se integren nuevos dispositivos de manera muy fácil.

- Se incentivó la competencia entre los fabricantes.

Figura 2. Capas del modelo OSI

3.2. Capas del Modelo OSI

El modelo OSI es un modelo de referencia que consta de siete capas, las cuales sirven como guía para el diseño de los protocolos que permiten en el buen funcionamiento de la red.

El proceso de las redes está dividido en diferentes capas lógicas por OSI. Estas capas tienen funciones diferentes dentro de la red, cada una trabaja con protocolos específicos y únicos de cada capa.

Estas capas se describen según el proceso por el que pasa la información dentro de la red.

3.2.1. Capa de Aplicación

Esta es la capa 7, pero es la que sirve de intermediario entre la red humana y la red de datos, ya que en ella se encuentran los protocolos que proporcionan servicios a los usuarios, tales como el protocolo de transferencia de archivos triviales (TFTP), protocolo

de oficina de correo (POP), protocolo de transferencia de hipertextos (HTTP), entre otros protocolos.

3.2.2. Capa de Presentación

La capa de presentación es la número 6, está relacionada con el significado (semántica) y formato de los datos intercambiados en una sesión entre procesos de aplicación. (Pérez E. H., 2003, p. 42)

Es la capa responsable del entendimiento de la información. Esta trabaja con la presentación de los datos para su mejor entendimiento sin importar el tipo que sea, ella se encargará de que sea entendible por el destino. No importante el tipo de caracteres sonidos o imagen entre ordenadores. La información llega de manera reconocible.

3.2.3. Capa de Sesión

La capa de sesión es la número 6 y es responsable de la comunicación entre los dispositivos de la red. Esta garantiza que se establezca una sesión entre dos máquinas y que de esta manera se pueda realizar el intercambio de información de principio a fin. También mantiene un enlace por el cual se transmitirán los archivos.

3.2.4. Capa de Transporte

Esta es la capa 4, la cual controla la integridad del mensaje de origen a destino, al recibir la información de la capa de red, esta verifica que todo esté en el orden adecuado y revisa si existe información duplicada o extraviada. Si la información recibida está desorganizada, lo cual es posible en redes grandes cuando se enrutan las tramas, la capa de transporte corrige el problema y transfiere la información a la capa de sesión en donde se le dará un proceso adicional (Perez, 2003, p. 45)

Esta capa acepta los datos de capas superiores y los divide convirtiéndolos en pequeños segmentos, le agrega número de Puerto origen para identificar de donde vino el paquete y número de Puerto destino para identificar la aplicación a la que está dirigida el segmento.

3.2.5. Capa de Red

Esta es la capa responsable del enrutamiento en la red. En ella operan tanto los protocolos enrutados como los protocolos de enrutamiento. Cada uno ofrece funciones diferentes.

Algunos de los protocolos que trabajan en esta capa son: Protocolo de información de enrutamiento (RIP), Protocolo de control de mensaje de Internet (ICMP), Protocolo Internet (IP), Primero la ruta más corta (OSPF), Protocolo de Gateway mejorado (EIGRP), etc. Cada uno por sus siglas en ingles.

3.2.6. Capa de Enlace de Datos

Esta es la capa 2 cuya función es recibir los paquetes que provienen de la capa de red y convertirlos en tramas, controlando el acceso a los medios físicos para que sean transportados desde un host origen hacia un host destino. Estas tramas deben recorrer diferentes redes físicas. Las redes físicas pueden componerse de diferentes tipos de medios físicos, tales como alambres de cobre, microondas, fibras ópticas y enlaces satelitales. Los paquetes de capas de red no tienen una manera de acceder directamente a estos diferentes medios.

Según Cisco (2013), Los protocolos de capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

3.2.7. Capa Física

Esta capa es la número 1, toma las tramas que provienen de la capa de enlace de datos y las convierte en bits para que puedan ser transmitidos por el medio.

En esta capa trabajan los dispositivos que brutos (no toman decisiones de envío), tales como el HUB, el cual es un equipo que no tiene la capacidad de analizar tráfico, razón por la cual no puede tomar una decisión sobre el destino al cual va dirigida esa información.

La curricula de Cisco (2013) comenta que los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.

3.3. Modelo TCP/IP

El modelo TCP/IP a diferencia de OSI es un modelo de implementación. TCP (Protocolo de Control de Transmisión), es un protocolo que opera en la capa 4 del modelo OSI (capa de transporte). Este protocolo se encarga de la transmisión de los datos, verifica que se entreguen en el mismo orden en el cual fueron enviados. Si los datos llegan desordenados el los ordena antes de entregarlos, usa número de secuencia para identificar cada segmento ya que la información viaja en pequeñas partes y debido a que los segmentos viajan por diferentes vías, no llegan en el mismo orden en el cual fueron enviados, pero este protocolo se encarga de corregir esto. En caso de que se pierda un segmento de dato, el protocolo vuelve a retransmitirlo.

TCP se considera un protocolo confiable, pero con mayor sobrecarga que otros protocolos como el Protocolo de Datagrama de Usuario (UDP).

IP: Este es un protocolo que opera en la capa 3 del modelo OSI (Capa de Red), se considera que es un protocolo no confiable y de mayor esfuerzo. Este protocolo se basa en protocolos de capa superior para la confiabilidad de los datos.

Los protocolos tanto TCP como IP tienen funciones diferentes como tal, pero ya el modelo TCP/IP es un conjunto de protocolos que permiten el buen funcionamiento de la red.

Una de las consideraciones más importantes a tener en cuenta al hablar de TCP/IP, es que no es una entidad única, es decir, es una familia de protocolos interdependientes. Es el acrónimo de Transmission Control Protocol / Internet Protocol. Estos son los dos protocolos más importantes, pero no los únicos de esta familia. Hay una serie de protocolos adicionales que trabajan en este conjunto de protocolos.

Un conjunto de protocolos es una combinación de protocolos que funciona juntos (Laporta & Aguiñiga, 2005, pág. 229)

Según Cisco (2007), el modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red. Un flujo de datos que se envía desde un origen hasta un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros hosts hacia otros destinos. Miles de millones de estas partes de información viajan por una red en cualquier momento. Es muy importante que cada parte de los datos contenga suficiente información de identificación para llegar al destino correcto.

Existen varios tipos de direcciones que deben incluirse para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un host hasta la aplicación de destino correcta que se ejecuta en otro. Al utilizar el modelo OSI como guía, se pueden observar las distintas direcciones e identificadores necesarios en cada capa.

El modelo TCP/IP contiene menos capas que el modelo OSI, pero no menos funciones, ya que este agrupa las funciones de hasta 3 capas en una sola. En este modelo varían algunos nombres pero no sus funciones. Entre ambos modelo existen similitudes y diferencias como se muestra en la figura 3.

Figura 3. Comparación del modelo OSI con el modelo TCP/IP

Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en que se relacionan con las capas que están por encima y por debajo de cada capa.

3.3.1. Dispositivos de Redes

Los dispositivos de redes se clasifican en dos grandes grupos: dispositivos finales y dispositivos intermediarios.

a. Los dispositivos finales, son aquellos que sirven para que el humano interactúe con la red de datos, entre estos se encuentran, las computadoras, los celulares, etc.

b. Los dispositivos intermediarios: son aquellos que permiten que los dispositivos finales se conecten a la red de datos. En otras palabras, son los que interconectan los dispositivos finales.

Algunos de los dispositivos de redes son:

a. **HUB**: es un dispositivo intermediario que opera en la capa física del modelo OSI, cuya función es interconectar dispositivos finales. Este equipo recibe una señal por un Puerto y la reenvía por todos los puertos, excepto por el que la recibió. Tiene como característica y a la vez desventaja, que divide el ancho de banda entre la cantidad de Puerto que tiene conectado. Ej: si tiene un ancho de banda a 100 y tiene 10 dispositivos conectados, cada uno se comunica a 10, ya que el divide 100 entre 10. Otra característica es que la información la envía tipo broadcast (a todo el mundo), logrando de esta manera el desperdicio del ancho de banda de la red, tampoco trabaja en base a ninguna dirección, por estas razones se considera un dispositivo bruto.

b. **Puente (Bridge)**: Es un dispositivo que opera en la capa de enlace de datos del modelo OSI. Este se creó para corregir las limitantes que tenía el HUB en cuanto a las decisiones de envío, y al problema relacionado con la división del ancho de banda; pero a su vez carecía de alta disponibilidad de puertos, ya que solo tenía 2 conexiones. Esto dio paso a la creación de otro dispositivo que trabaje en base a la dirección MAC (Media Control Access), trabaje en la misma capa, pero que tenga mayor cantidad de puertos y tenga una comunicación full dúplex (comunicación de doble vía).

c. **Switch**: Es un dispositivo que al igual que el Puente, trabaja en la capa de enlace de datos, no divide el ancho de banda.

d. **Router**: Es un dispositivo que opera en la capa de red del modelo OSI. Su función principal es seleccionar la mejor ruta para llegar a un destino y luego enviar los paquetes. Este host trabaja en base a la dirección IP de destino para tomar sus decisiones de envío.

3.3.2. Tipos de Redes

Aunque puedan establecerse multitud de criterios, las redes se clasifican tradicionalmente según tres parámetros: Velocidad de acceso, distancia cubierta y tipo de propiedad, así se tienen las redes WAN, LAN y MAN.

3.3.3. Redes de Área Amplia (WAN)

Las redes WAN alcanzan enormes distancias geográficas que abarcan desde varios kilómetros hasta continentes completos. Las WAN constan de una combinación de líneas conmutadas y dedicadas, microondas y comunicaciones de satélite. Las líneas conmutadas son líneas telefónicas a las que una persona puede tener acceso desde su terminal para transmitir datos a otra computadora; la llamada se enruta o conmuta a través de rutas preestablecidas al destino designado.

Las empresas comerciales individuales podrían establecer sus propias redes WAN. La empresa es responsable del contenido y la administración de las telecomunicaciones. Sin embargo, el mantenimiento de las redes privadas de área amplia es caro y talvez las empresas no tengan los recursos para administrar sus propias redes de este tipo (Kenneth C. Laudon, 2004, p. 260).

Debido al alto costo y responsabilidad que les otorga a las empresas el implementar su propia red amplia, casi el 100% opta por arrendar el servicio a un proveedor, ya que consideran que es mejor en cuanto a costo beneficio.

La figura 4 muestra un ejemplo de cómo se representa físicamente una red WAN interconectando solo dos redes LAN.

Figura 4. Representación gráfica de una red WAN

3.3.4. Redes de Área Local (LAN)

Una red de área local (LAN, por sus siglas en inglés) abarca una distancia limitada, usualmente un edificio o varios edificios cercanos.

La mayoría de las LAN interconectan dispositivos ubicados en un radio de 650 metros y se han utilizado ampliamente para enlazar PCs. Las LANs requieren sus propios canales de comunicaciones y en ocasiones las controlan y operan grupos de usuarios o departamentos de la empresa (Laporta & Aguiñiga, 2005).

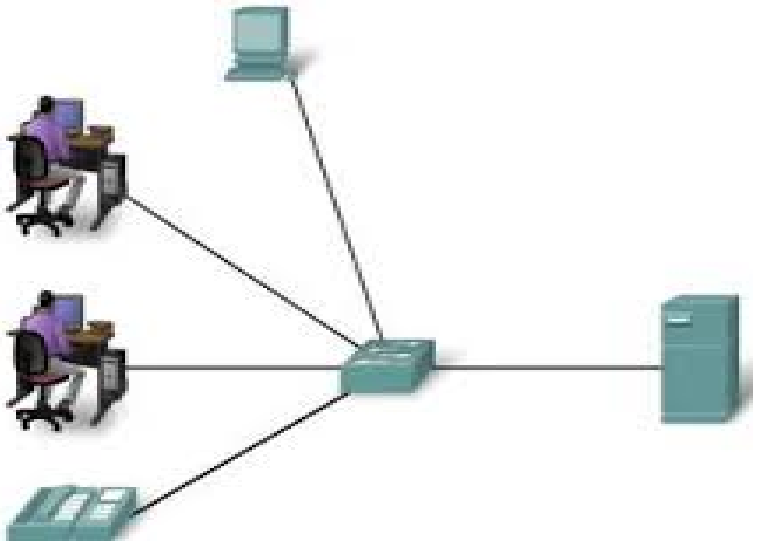

Figura 5. Representación gráfica de una red LAN

3.3.5. Red de Área Metropolitana (MAN)

Una red de área metropolitana (MAN) abarca una ciudad. El ejemplo más conocido de una MAN es la red de televisión por cable en muchas ciudades. Este sistema creció a partir de los primeros sistemas de antena comunitaria en áreas donde la recepción de la televisión al aire era pobre. En dichos sistemas se colocaba una antena grande en la cima de una colina cercana y la señal se canalizaba a las casas de los suscriptores.

Al principio eran sistemas diseñados de manera local con fines específicos. Después las compañías empezaron a pasar a los negocios, y obtuvieron contratos de los gobiernos de las ciudades para cablear toda una ciudad. El siguiente paso fue la programación de televisión e incluso canales designados únicamente para cable (Tanenbaum, 2003, pág. 18)

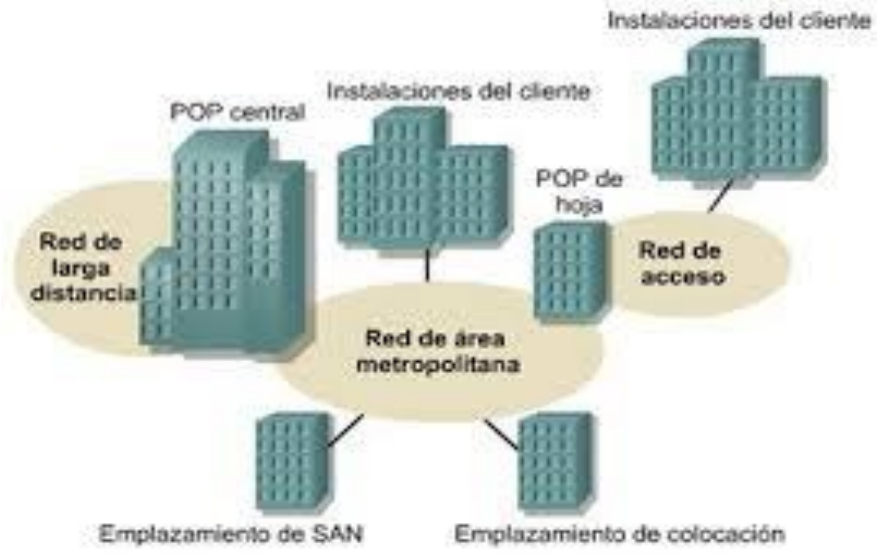

Figura 6. Representación gráfica de una red MAN

3.4. Topología de Red

En una red los dispositivos se encuentran interconectados entre sí de forma física. La manera en cómo están es lo que da paso a la definición de topología.

La topología de la red, es la disposición lógica de los elementos (enlaces, nodos) de una red. Así pueden definirse diversos modelos de topologías básicas:

La forma de interconectar las estaciones de una red local, mediante un recurso de comunicación, es decir la estructura topológica de la red, es un parámetro primario que condiciona fuertemente las prestaciones que de la red pueden definirse diversos modelos de topologías básicas (Serra & Bosch, 2002, p. 27)

En una red local se pueden mostrar diferentes estructuras de topologías, tales como: la topología de bus, la de estrella y la de anillo, aunque en algunos casos se pueden presentar topologías combinadas, así como la de árbol, cada una de estas cumple con características diferentes.

Según Pérez (2003) define el término topología el cual se refiere a la configuración del a red, es decir, a su forma de conectividad física.

3.4.1. Topología de Estrella

La topología en estrella consiste en concentrar todas las conexiones a un ordenador central. Para estos dispositivos comunicarse en la red, es necesario pasar por el ordenador central, ya que toda la comunicación se hace a través de este.

El ordenador central es normalmente el servidor de la red, si bien puede ser un dispositivo especial de conexión o un concentrador (HUB), Esta configuración presenta

buena flexibilidad para incrementar o disminuir el número de estaciones; además, una falla en alguno de los ordenadores periféricos no tiene efecto sobre el comportamiento general de la red.

En la figura 7 se hace referencia a la representación de una topología en estrella física.

Figura 7. Topología en Estrella

3.4.2. Topología de Anillo

En este tipo de topología las estaciones de trabajo se ordenan individualmente en forma de anillo y la información va pasando de estación en estación hasta llegar al nodo receptor (destinatario) que va dirigida. Cada dispositivo se conecta a dos más, y así sucesivamente lo hacen los demás. Este tipo de topología tiene como desventaja, que si el anillo queda interrumpido por alguna falla en una de las estaciones de trabajo, toda la red se ve afectada, debido a que todas las estaciones deben estar en funcionamiento para que el anillo pueda trabajar.

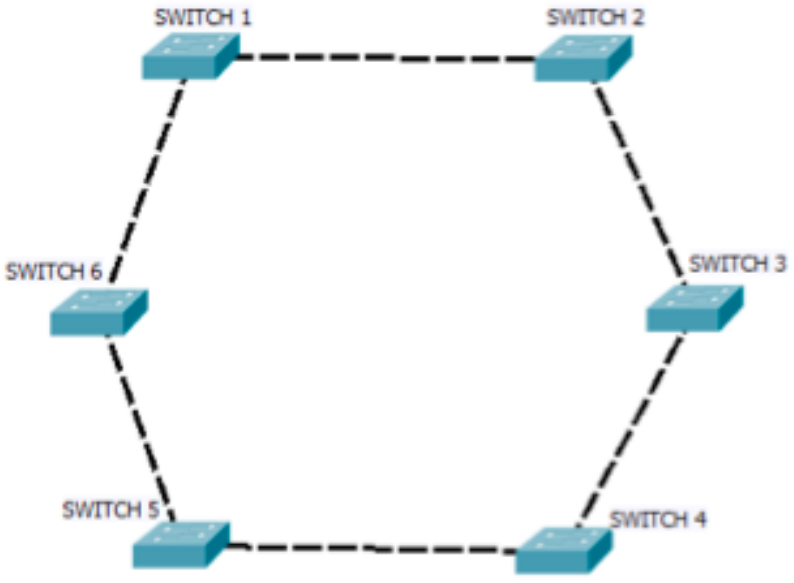

Figura 8. Topología en Anillo

3.4.3. Topología de Bus

Esta estructura es la más utilizada en redes pequeñas, y también se utiliza, por ejemplo, la red Ethernet. Consiste en que todas las estaciones de trabajo, con su servidor incluido, se conectan a un segmento de red a través de un cable único (propio) que lleva una resistencia terminal en cada extremo.

Son redes que utilizan la topología lineal (o en línea) en esta tecnología, todas las estaciones de trabajo se conectan a un canal de comunicaciones único (bus), Toda la información fluye por el canal y cada estación recibe solo la información que va dirigida a ella. Este tipo de redes son sencillas de instalar y brindar gran flexibilidad para aumentar o disminuir el número de estaciones.

Esta topología fue una de las primeras utilizadas en la LAN, consiste en un cable terminado con una impedancia en los extremos, al cual están conectadas todas las estaciones. Cada estación conectada al bus escucha el tráfico que transmiten todas las demás y cuando detecta su dirección recoge la información enviada por otra estación al bus.

Esta configuración es muy sencilla, se puede expandir con facilidad y reconfigurar fácilmente además tiene bajo coste y se puede utilizar para varios métodos de accesos.

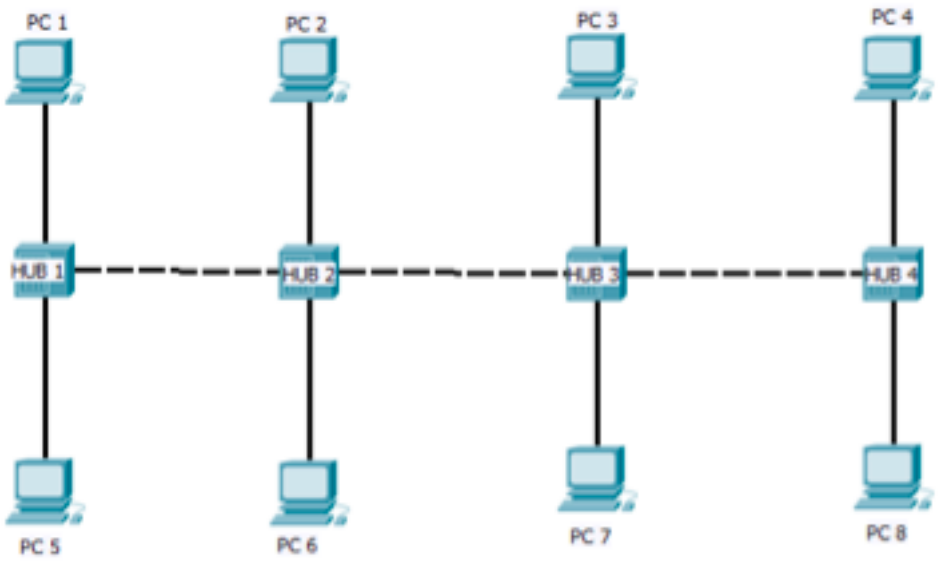

Figura 9. Topología Bus

3.4.4. Topología de Árbol

Es una estructura sin limitaciones. Las redes no se encuentran limitadas a seguir una topología, en esta mientras más grande sea la red, mayor es el uso de varias topologías a la vez, obteniendo así como resultante una topología combinada. Esta topología tiene lugar en un escalamiento de la red mediante concentradores de cables (hub) y (switches).

3.4.5. Paso de Token

Este protocolo es utilizado en la topología de anillo Token-Ring, es utilizado para el control de datos que va pasando, dentro del anillo de una estación de trabajo a la siguiente.

La estación que quiere enviar los datos, selecciona el Token como ocupado y añade los datos que desea enviar y la dirección de la estación de destino. Las estaciones van observando la dirección para saber si los datos enviados pertenecen a ellas y en caso de que sea negativo, el Token va pasando de una a otra hasta llegar a la estación destino. La estación destino acepta el mensaje, lo borra y marca de nuevo el Token como libre.

3.5. Cableado Estructurado

El sistema de cableado estructurado es la plataforma universal sobre la que construir la estrategia general de sistemas de información. Un cableado estructurado propiamente diseñado e instalado proporciona una infraestructura de cableado que suministra un desempeño predefinido y la flexibilidad de acomodar futuro crecimiento por un período extendido de tiempo (Corrales, 2005, pág. 406).

Hay tres reglas que ayudan a garantizar la efectividad y eficiencia en los proyectos de diseño del cableado estructurado.

a. La primera regla es buscar una solución completa de conectividad.
b. La segunda regla es planificar teniendo en cuenta el crecimiento futuro.
c. La regla final es conservar la libertad de elección de proveedores.

Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar ser mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones.

3.5.1. Subsistemas de Cableado Estructurado

Hay siete subsistemas relacionados con el sistema de cableado estructurado. Cada subsistema realiza funciones determinadas para proveer servicios de datos y voz en toda la planta de cables:

1) Punto de demarcación (demarc) dentro de las instalaciones de entrada (EF) en la sala de equipamiento.

2) Sala de equipamiento (ER)
3) Sala de telecomunicaciones (TR)
4) Cableado backbone, también conocido como cableado vertical
5) Cableado de distribución, también conocido como cableado horizontal.
6) Área de trabajo (WA)
7) Administración

El demarc es donde los cables del proveedor externo de servicios se conectan a los cables del cliente en su edificio. El cableado backbone está compuesto por cables de alimentación que van desde el demarc hasta la salas de equipamiento y luego a la salas de telecomunicaciones en todo el edificio. El cableado horizontal distribuye los cables desde las salas de telecomunicaciones hasta las áreas de trabajo. Las salas de telecomunicaciones es donde se producen las conexiones que proporcionan una transición entre el cableado backbone y el horizontal.

Estos subsistemas convierten al cableado estructurado en una arquitectura distribuida con capacidades de administración que están limitadas al equipo activo, como por ejemplo los PC, switches, hubs, etc.

El diseño de una infraestructura de cableado estructurado que enrute, proteja, identifique y termine los medios de cobre o fibra de manera apropiada, es esencial para el funcionamiento de la red y sus futuras actualizaciones (Panduit, 2003).

3.5.2. Normas de Cableado Estructurado

La Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias de Electrónica (EIA) son asociaciones industriales que desarrollan y ofrecen una serie de estándares sobre el cableado estructurado para voz y datos. Tanto la TIA como la EIA son acreditadas por el Instituto Nacional Americano de Normalización (ANSI) para desarrollar los estándares voluntarios para la industria de las telecomunicaciones. Los distintos comités y subcomités de TIA/EIA desarrollan los estándares para fibra óptica, equipo terminal del usuario, equipos de redes, comunicaciones inalámbricas y satelitales.

3.5.3. Estándares de Cableado Estructurado

La Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias de Electrónica (EIA) son asociaciones industriales que desarrollan y ofrecen una serie de estándares sobre el cableado estructurado para voz y datos. Tanto la TIA como la EIA son acreditadas por el Instituto Nacional Americano de Normalización

(ANSI) para desarrollar los estándares voluntarios para la industria de las telecomunicaciones. Los distintos comités y subcomités de TIA/EIA desarrollan los estándares para fibra óptica, equipo terminal del usuario, equipos de redes, comunicaciones inalámbricas y satelitales.

3.5.4. TIA/EIA-568-A

Este es un estándar antiguo utilizado para cableados de telecomunicaciones en los Edificios Comerciales, en este e especificaban los requisitos mínimos de cableado para las telecomunicaciones, las topologías recomendadas y los límites establecidos de distancia, las especificaciones sobre el rendimiento de los equipos de conexión y medios, los conectores y las asignaciones de pin.

3.5.5. TIA/EIA-568-B

Es el actual Estándar de Cableado, en este se especifican los requisitos sobre componentes y transmisión para los medio de telecomunicaciones. Este estándar se divide en tres secciones diferentes: 568-B.1, 568-B.2 y 568-B.3.

3.5.6. TIA/EIA-568-B.1

Este especifica un sistema genérico de cableado para telecomunicaciones en edificios comerciales que admite un entorno de múltiples proveedores y productos.

3.5.7. TIA/EIA-568-B.1.1

Es una enmienda aplicada al radio de curvatura del cable de conexión UTP de 4 pares y par trenzado apantallado (ScTP) de 4 pares.

3.5.8. TIA/EIA-568-B.2

Este especifica los componentes de cableado, transmisión, modelos de sistemas y los procedimientos de medición imprescindibles para la validación del cableado de par trenzado.

3.5.9. TIA/EIA-568-B.2.1

Es la enmienda utilizada para especificar los requisitos en el cableado de Categoría 6.

3.5.10. TIA/EIA-568-B.3

En esta se especifican los componentes y requisitos de transmisión para un sistema de cableado de fibra óptica.

3.5.11. TIA/EIA-569-A

El estándar utilizado para Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales, este especifica las prácticas de diseño y construcción dentro de los edificios y entre los mismos, que admiten equipos y medios de telecomunicaciones.

3.5.12. TIA/EIA-606-A

Este Estándar es utilizado para la Administración de Infraestructura de Telecomunicaciones de Edificios Comerciales incluye estándares de rotulación del cableado. Los estándares especifican que cada unidad de finalización de hardware debe usar una identificación exclusiva. También detalla los requisitos de registros y mantenimiento de la documentación para la administración de la red.

3.5.13. TIA/EIA-607-A

Este estándar corresponde a los Requisito de Conexión a Tierra y Conexión de Telecomunicaciones para Edificios Comerciales admiten un entorno de varios proveedores y productos diferentes, así como las prácticas de conexión a tierra para los sistemas que pueden instalarse en las instalaciones del cliente. Este estándar especifica los puntos exactos de interfaz entre los sistemas de conexión a tierra y su configuración de conexión a tierra para los equipos de telecomunicaciones. Este estándar especifica las configuraciones de la conexión a tierra y de las conexiones necesarias para el funcionamiento de estos equipos.

3.6. Tipos De Cables

El medio de transmisión empleado en una red de computadores constituye el canal por el cual fluye la información desde el origen hasta el destino de la comunicación. En cualquier red de computadores, el medio de comunicación empleado adquiere un papel fundamental ya que de las características del mismo van a depender directamente aspectos de la red tales como la velocidad de transmisión máxima que se pueda alcanzar, el número de equipos conectados o los errores que puedan generarse a la hora de comunicar los datos. En la tabla se muestran distintas tecnologías de la red.

Teconología	Velocidad de transisión	Tipo de cable	Distancia máxima	Tecnología
10 Base 2	10 Mbps	Coaxial fino (50Ω)	200 m	Bus (Conector BNC-T)
10 Base 5	10 Mbps	Coaxial grueso (50Ω)	500 m	Bus (Conector AUI)
10Base T	10 Mbps	2 pares trenzado (categoría UTP3)	100 m	Estrella (Hub o Switch)
10 Base F	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100 Base T4	100 Mbps	4 pares trenzados (categorí UTP3)	100 m	Estrella Half Duplex(hub) y Full Duplex(switch)
100 Base TX	100 Mbps	2 pares trenzado (UTP5)	100 m	Estrella Half Duplex(hub) y Full Duplex(switch)

100 Base FX	100 Mbps	Fibra óptica (multimodo)	2000 m	No permite el uso de hubs
100 Base CX	100 Mbps	2 pares trenzado (STP)	25 m	Estrella (Hub o Switch)
1000 Base T	1000 Mbps	4 pares trenzado (ctaegoría 5e ó UTP6)	100 m	Estrella Full Duplex (switch)
1000 Base SX	1000 Mbps	Fibra óptica (multimodo)	550 m	Estrella Full Duplex (switch)
1000 Base LX	1000 Mbps	Fibra óptica (monomodo)	5000 m	Estrella Full Duplex (switch)
10 GBase SR	10 Gbps	Fibra óptica (multimodo)	500 m	Estrella Full Duplex (switch)
10 GBase LX4	10 Gbps	Fibra óptica (multimodo)	500 m	Estrella Full Duplex (switch)
10 GBase T	10 Gbps	Par Trenzado (UTP6)	55 m	Estrella Full Duplex (switch)

Tabla 1. Diferentes categorías de cableado estructurado. Fuente: Propia.

3.6.1. Medios Guiados

Los medios guiados son aquellos en los que el canal por el que se transmiten las señales son medios físicos, es decir, por medio de un cable. Estos medios son los siguientes: par trenzado, cable coaxial y fibra óptica.

3.6.2. Par trenzado

Este se trata de uno de los medios de transmisión más empleados en las redes de área local actuales. En su configuración básica está constituido por 2 cables de cobre entrecruzados en forma de espiral recubiertos por un aislante.

Normalmente un cable de par trenzado está formado por un grupo de pares trenzados, habitualmente cuatro, recubiertos de una envoltura protectora. Cada uno de estos cables se identifica mediante un color, siendo los colores asignados y las agrupaciones de los pares de la siguiente forma:

- Par 1: Blanco-Azul/Azul
- Par 2: Blanco-Naranja/Naranja
- Par 3: Blanco-Verde/Verde
- Par 4: Blanco Marrón/Marrón

En la figura 10 se muestra la estructura interna de los cables de par trenzado y su combinación de colores.

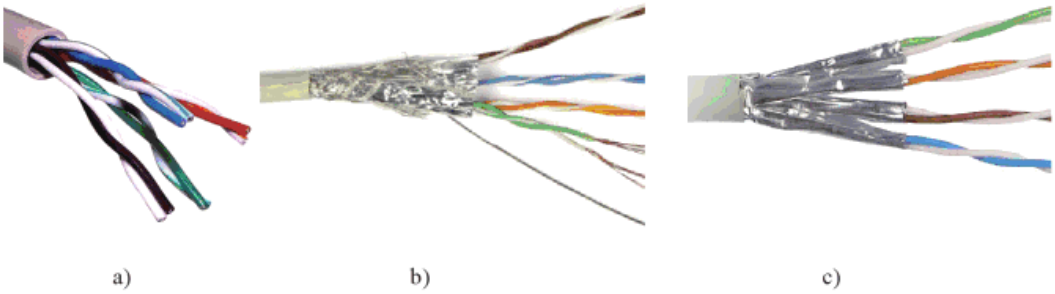

Figura 10. Estructura internet de cables de par trenzado

3.6.3. Aplicaciones

El par trenzado es empleado indistintamente para la transmisión de señales analógicas y digitales. Su éxito se ha debido a que es mucho menos costoso que cualquiera de los otros tipos de medios de transmisión.

3.6.4. Tipos de par trenzado

Existen básicamente dos tipos de pares trenzados: pantallados y sin apantallar.

- UTP Unshielded Twisted Pair (Par trenzado no apantallado). Este es el más empleado en telefonía y LANs debido a su bajo precio y su fácil manipulación. A pesar del aumento de robustez que proporciona el trenzado del cable, los pares trenzados no apantallados se pueden ver

afectados por interferencias electromagnéticas externas como pueden ser interferencias causadas por pares cercanos. El estándar para conectores del cable UTP es el RJ-45.

- STP Shielded Twist Pair (Par trenzado apantallado). En este caso el par trenzado se encuentra recubierto por una malla metálica, lo que garantiza un aislamiento a interferencias electromagnéticas externas. Existe una variante, denominada S/STP en el que se encuentra apantallado cada par de cables, aunque más costoso que el UTP.

3.6.5. Fibra Óptica

En las fibras ópticas las señales se transmiten en forma de luz. Están constituidas por un núcleo de cristal de silicio por el que se envía un haz de naturaleza óptica que codifica la información. El núcleo está rodeado por un recubrimiento que puede ser otro cristal o plástico con propiedades ópticas distintas al núcleo. La separación entre el núcleo y el revestimiento actúa como reflector, confinando así el haz de luz dentro del núcleo.

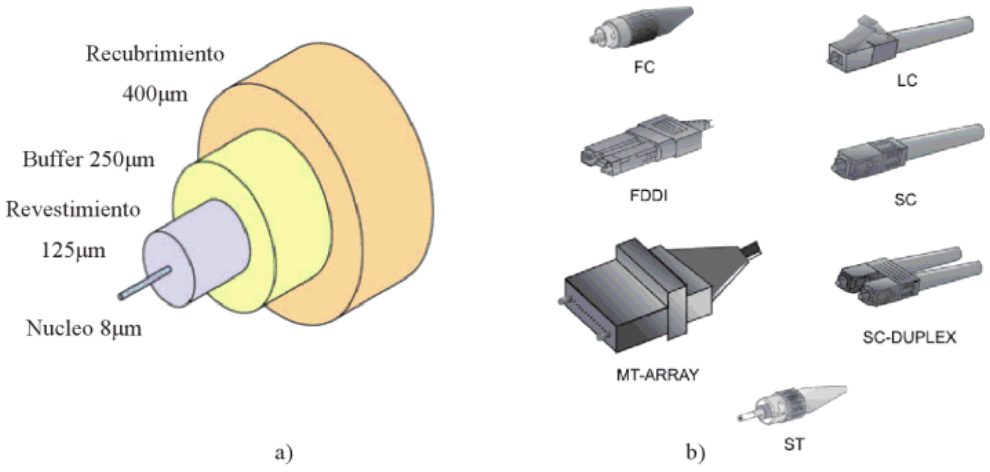

Figura 11. Composición de un cable de fibra óptica[2]

3.6.6. Aplicaciones

Las fibras ópticas constituyen actualmente el medio físico más ampliamente utilizado para la transmisión de datos a largas distancias, siendo cada vez más utilizado en las redes de telefonía. También es un medio muy extendido como red de área metropolitana enlazando centrales telefónicas o cabeceras de cable-módem dentro del área metropolitana y sin la necesidad de emplear repetidores (Vázquez, Baeza, & A., 2010, pág. 81).

[2] Fuente: Libro Redes y Transmisión de Datos

4. CAPITULO IV - ALMACENAMIENTO Y SEGURIDAD DE LA INFORMACIÓN EN LOS CENTROS DE DATOS

4.1. Almacenamiento y Seguridad de la Información

Este capítulo aborda dos temas sumamente importantes dentro de los centros de datos. Estos son el almacenamiento y la seguridad de la información.

La información es considerada uno de los activos más importante de las organizaciones y de esta depende mucho el éxito de la empresa. Todas las decisiones que definen el éxito o no de una organización son tomadas en base a datos de diferentes tipos y es por esto que deben de ser almacenados y contar con una arquitectura de red que complemente su seguridad.

Existen diversas arquitecturas de almacenamiento y protección de la información pero la elección de un sistema de almacenamiento y seguridad en específico va a depender de las necesidades de la empresa.

El capítulo tratará los diferentes tipos de arquitectura de almacenamiento y los diferentes tipos de servidores y métodos de almacenamiento. También se aborda el tema de la seguridad informática, los diferentes tipos de seguridad que existen y sus características más relevantes y los sistemas de seguridad informática y su importancia dentro de la organización.

4.2. Servidores

Un servidor es un elemento informático crítico dentro de una infraestructura de red empresarial. Este se encarga de ofrecer los servicios en la red a otros nodos conocidos como clientes. Existen diversos tipos de servidores y generalmente son muy potentes ya que soportan mayor cantidad de procesadores, mayor cantidad de memoria RAM[3] y su almacenamiento no está limitado a un solo disco duro.

Según Marchionni (2011), los servidores pueden llegar a soportar cantidades de memoria entre 16GB[4] a 1TB[5], o más y puede soportar varios discos duros. También, indica que pueden ofrecer más de un servicio.

Hay que aclarar que un servidor no necesariamente tiene que ser una máquina potente, con grandes cantidades de espacio de almacenamiento y gran cantidad de memoria RAM. Un servidor puede también llegar a ser una computadora pequeña que ofrezca cualquier tipo de servicio, por ejemplo servicio

[3] Random Access Memory o Memoria de Acceso Aleatorio utilizada por el computador para guardar los datos que utiliza en el momento.
[4] Acrónimo de Gigabyte, unidad de medida de almacenamiento de información equivalente a 1000 kilobytes.
[5] Acrónimo de Terabyte, unidad de medida de almacenamiento de información equivalente a 1000 GB.

de almacenamiento. Sin embargo, cuando se trata de una organización que maneja una cantidad de datos considerable, es necesario contar con servidores robustos para manejar de forma eficiente la información.

4.2.1. Modelo Cliente-Servidor

El modelo cliente-servidor es un modelo de sistema en donde clientes solicitan servicios y servidores ofrecen el servicio solicitado. Quien remite la solicitud es el cliente, este generalmente espera y recibe respuesta del servidor, tiene interacción directa con el usuario final y se puede conectar a varios servidores.

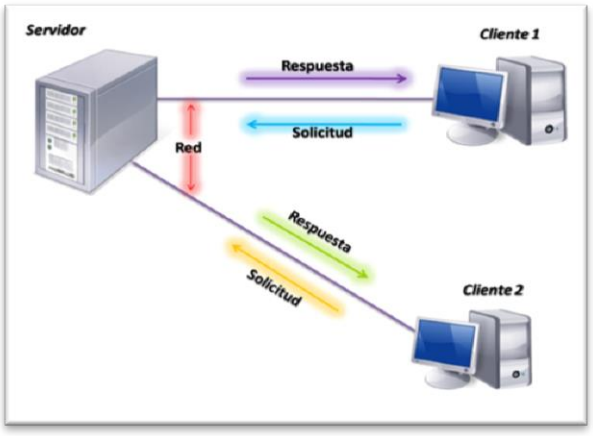

Figura 12. Modelo Cliente-Servidor[6]

[6] Fuente: http://redes5cp22013g6.blogspot.com/

Por otro lado, el servidor es el encargado recibir las solicitudes de parte del cliente, procesarlas y enviar respuesta. Los servidores no interactúan con el usuario final.

La siguiente tabla muestra las principales ventajas y desventajas de dicho modelo según Ordinas (2008):

VENTAJAS	DESVENTAJAS
• Datos en los servidores, lo que facilita el control de la seguridad, el control de acceso, la consistencia de la información, etc. • Hay muchas tecnologías maduras para los sistemas cliente-servidor. Ello implica que se den soluciones muy probadas y que garanticen la seguridad, la facilidad de uso y la amigabilidad de la interfaz. • Relativa facilidad para actualizar los elementos de un sistema cliente-servidor. • El desarrollo de aplicaciones centralizadas es más sencillo que las descentralizadas. • Existen unos responsables de garantizar el servicio, que son los proveedores del servicio (o de cada una de las partes de este).	• La centralización del modelo: punto único de fallo, dependencia de la autoridad administrativa que provee el servicio, vulnerabilidad a ataques. • Escalabilidad condicionada a la capacidad de hacer crecer el servidor o el conjunto de servidores que proporcionan el servicio. Relacionado con ello: es muy costoso construir un sistema que soporte cargas altas de contenidos pesados. • Cuando se encuentran muchos clientes que hacen peticiones el servidor se puede congestionar.

Tabla 2. Ventajas y desventajas del modelo cliente-servidor

4.2.2. Tipos de Servidores

Los servidores pueden ser clasificados básicamente en dos categorías: servidores físicos y servidores virtuales.

4.2.3. Servidores Físicos

Dentro de los servidores físicos se pueden encontrar los siguientes, aunque no se limitan a estos:

4.2.4. Servidores de Impresión

Tienen conectadas varias impresoras de red y administran las colas de impresión según la petición de sus clientes (Marchionni, 2011).

En la figura 13 se puede ver cómo funciona básicamente un servidor de impresión, donde todas las solicitudes son manejadas por el servidor.

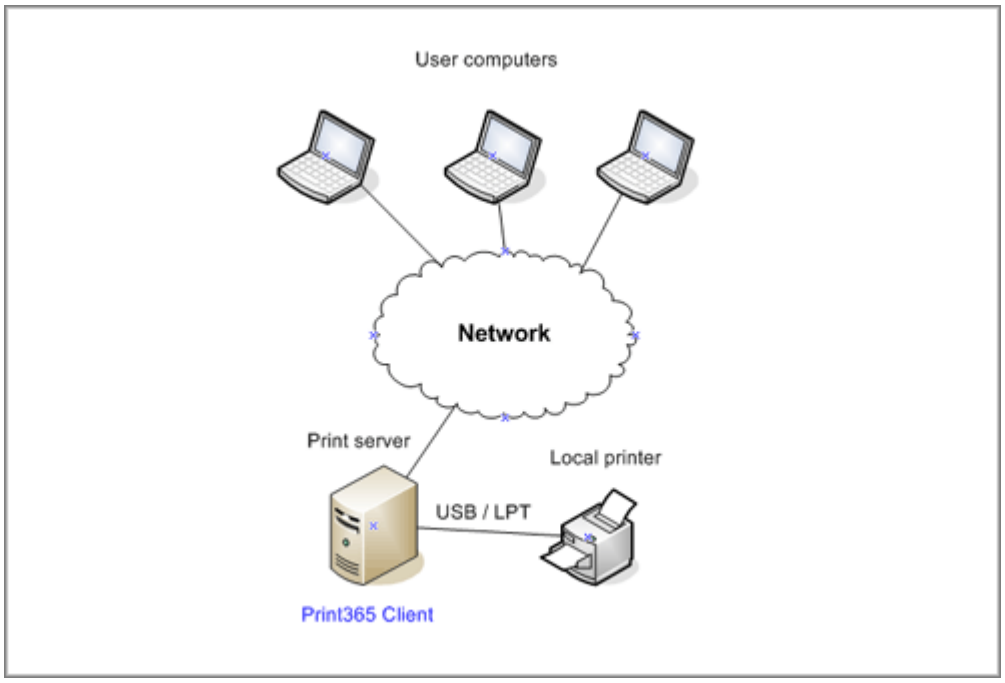

Figura 13. Diagrama de un Servidor de impresión

Estos servidores manejan todas las solicitudes de impresión recibidas por los clientes conectados a la red y hacen que la impresora se comporte como si estuviera conectada directamente al cliente, cuando en realidad está conectada al servidor de impresión.

4.2.5. Servidores Web

Este tipo de servidores se encargan de almacenar sitios en la red internet (intranet). Pueden publicar cualquier aplicación web, brindarle la seguridad correspondiente y administrarla por completo (Marchionni, 2011).

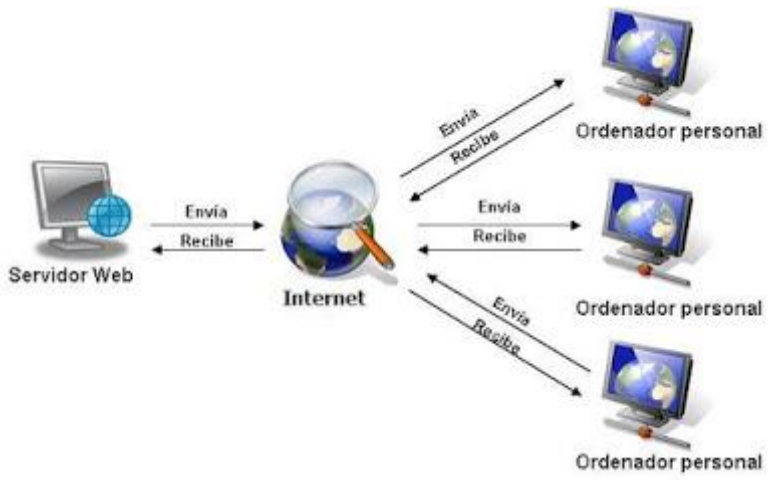

Figura 14. Diagrama de un Servidor Web

El servidor web también es conocido como Servidor HTTP[7]. Las respuestas recibidas por el cliente son compiladas y procesadas por un navegador web.

[7] Es el protocolo de transferencia de hipertexto o Hypertext Transfer Protocol utilizado para acceder a páginas web.

4.2.6. Servidores de Base de Datos

Son servidores que manejan una gran cantidad de información para ser consultada con posterioridad.

Una base de datos es un conjunto de datos que se relacionan entre si y se almacenan para uso futuro. Esto se logra mediante un sistema de gestión de base de datos o SGBD (o en sus siglas en ingles DBSM).

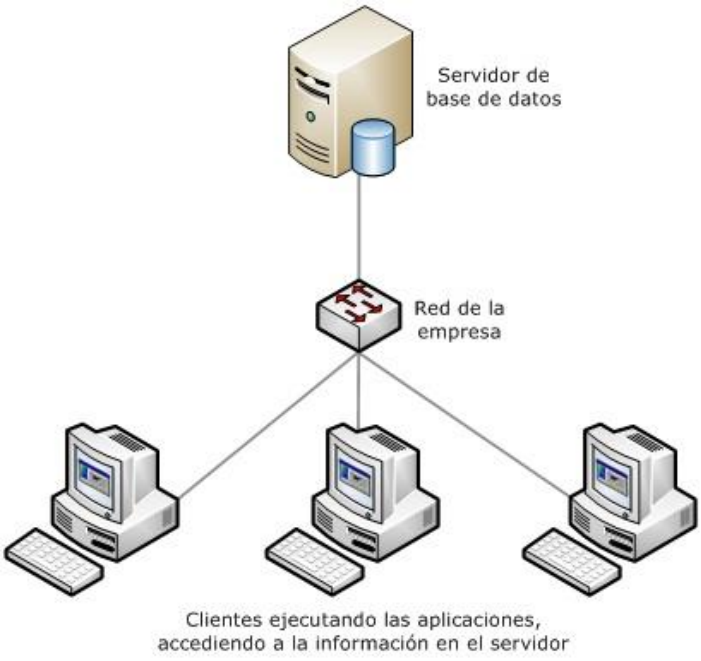

Figura 15. Diagrama de un Servidor de Base de Datos

Existen diversos tipos de base de datos según su uso, por ejemplo, las bases de datos estáticas, que son base de datos de solo lectura y almacena datos históricos para posterior análisis. También existen las bases de datos dinámicas, donde su información si puede ser modificada con el tiempo. Un ejemplo de claro de una base de datos es una biblioteca, las bibliotecas contienen diferente tipos de información y documentos que luego serán consultados.

Los servidores de base de datos tienen diversos usos, por ejemplo, pueden ser utilizados para la gestión de archivos, alojar páginas web y servidores de correo electrónico.

4.2.7. Servidores de Correo Electrónico

Administran todos los correos de la organización y manejan gran cantidad de datos. Almacenan todos los correos y según Marchionni (2011) se los redirecciona a clientes y servidores de seguridad, analizadores y replicadores. Algunos también brindan opciones de seguridad, como antispam[i8], lista blanca, lista negra y antivirus.

[8] Método utilizado para prevenir los correos basura.

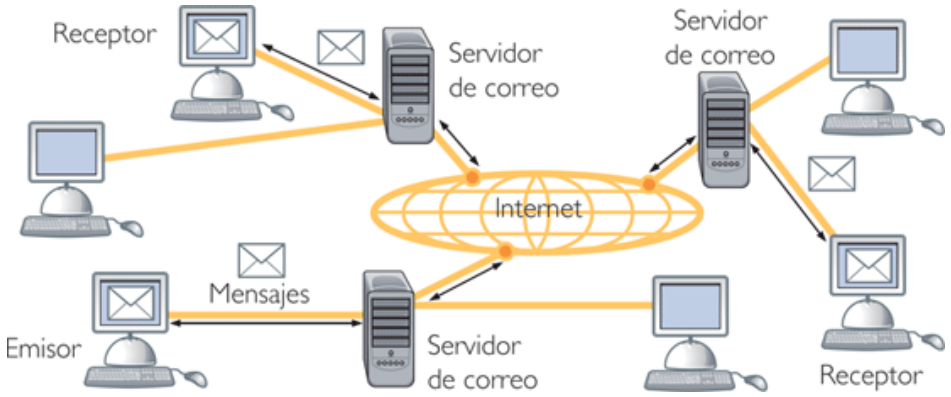

Figura 16. Representación gráfica de un Servidor de Correo Electrónico

Los servidores de correo electrónico son muy utilizados dentro de las empresas para la comunicación entre las personas.

4.2.8. Servidores de Directorio

Se ocupan de almacenar los datos de todos los usuarios de la red, propiedades y características que los identifican (Marchionni, 2011).

Esto permite que los administradores tengan un control de los usuarios que acceden a dicha red.

4.2.9. Servidores de Comunicaciones

Brindan servicios de chat, telefonía IP, teleconferencia, video, etc. (Marchionni, 2011).

Los servidores de comunicación permiten el acceso remoto a información, herramientas o aplicaciones que están localizadas en una red remota. También se les conoce como servidores de acceso remoto, RAS en inglés.

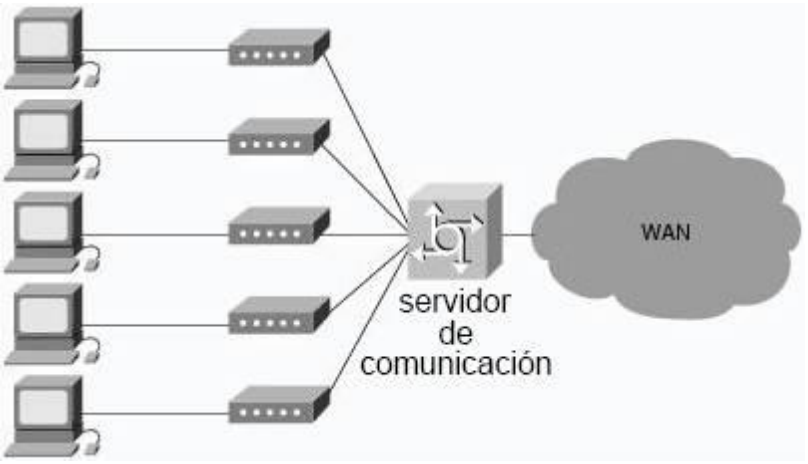

Figura 17. Representación gráfica de un Servidor de Comunicaciones

4.2.10. Servidores de Archivos

Permiten compartir el material y guardarlo de manera segura y ofrecen una mayor capacidad de almacenamiento que los equipos de escritorio. Pueden tener conectados a varias unidades de almacenamiento de distintas capacidades. (Marchionni, 2011).

En la figura 18 se puede ver como los diferentes usuarios de la red acceden a carpetas ubicadas en el servidor de archivo.

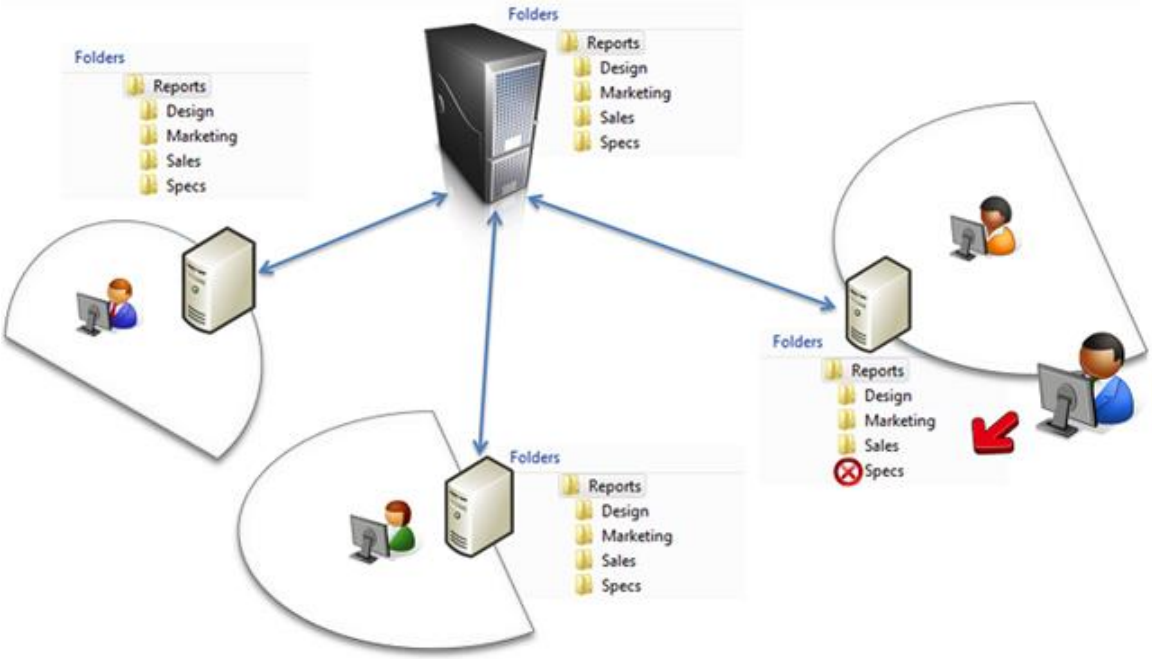

Figura 18. Representación gráfica de un Servidor de Archivos

Los servidores de archivos tienen como función principal la gestión de los archivos dentro de las organizaciones. Los usuarios pueden modificar, eliminar y crear datos dentro de ellos dependiendo de los permisos otorgados por el administrador de sistema. Generalmente, los servidores de archivos tienen asignado una cantidad considerable de espacio en disco duro para el almacenamiento de la información.

4.2.11. Servidores de Seguridad

Se dedican a escanear la red en busca de virus, máquinas desactualizadas por falta de parches del sistema operativo, equipos con determinado software instalado, y muchas otras acciones más. (Marchionni, 2011).

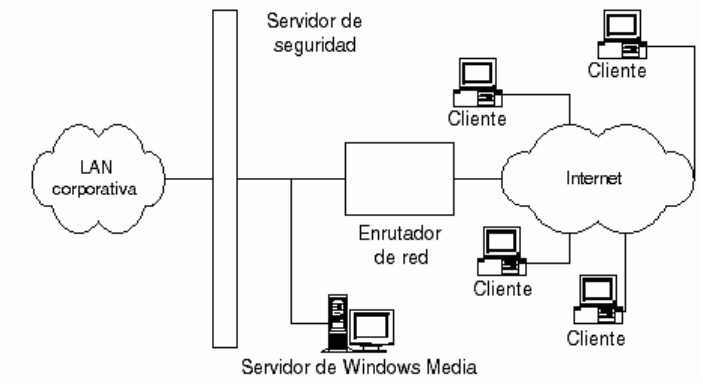

Figura 19. Representación gráfica de un Servidor de Seguridad

El servidor de seguridad impide los ataques maliciosos de internet hacia la red LAN corporativa que intentan infiltrarse en los equipos.

4.2.12. Servidores Proxy

Brindan acceso a Internet. En ellos generalmente residen firewalls a los que se les configuran reglas para permitir la navegación por ciertas páginas y bloquear otras (Marchionni, 2011).

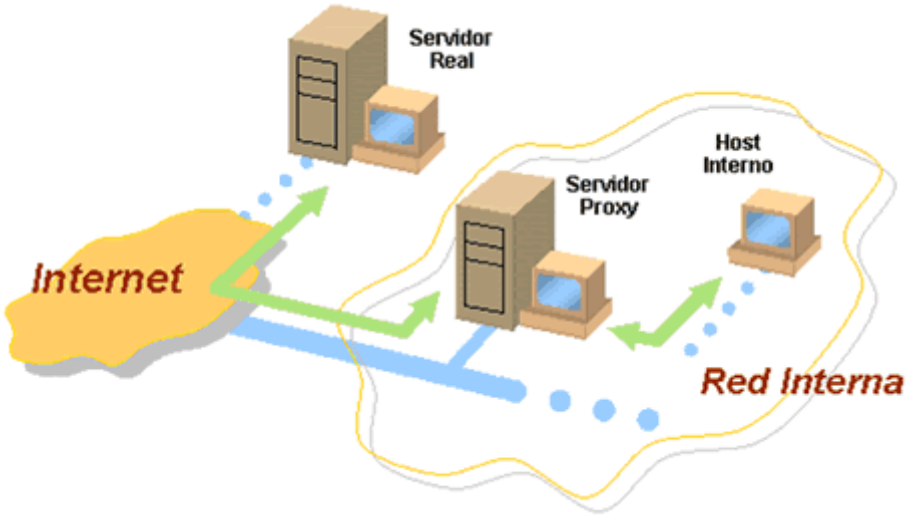

Figura 20. Representación gráfica de un Servidor Proxy

Los cortafuegos, o firewalls en inglés, son dispositivos o aplicaciones que controlan el tráfico de la red, denegando tráfico no autorizado y permitiendo a la vez las comunicaciones que si son autorizadas.

Los servidores Proxy pueden ser locales y externos. Son locales cuando se encuentran instalados en la máquina del cliente y este puede controlar el tráfico y son externos cuando lo implementa una entidad externa, por ejemplo, una institución y generalmente se utilizan para bloquear contenido y controlar el tráfico en general.

Dentro de sus ventajas se pueden mencionar que controla el tráfico de la red, filtra peticiones que están prohibidas, sirve como intermediario en la red por lo tanto todos derechos y permiso se pueden hacer a través de el sin necesidad de hacerlo a través del usuario.

Dentro de sus desventajas se pueden mencionar que al recibir muchas peticiones de muchos usuarios, está muy cargado, puede responder equívocamente a una petición cuando guarda en caché, al representar a más de un usuario puede dar problemas en la comunicación TCP/IP.

Existen diferentes tipos de servidores proxy pero el más famoso y utilizado es el proxy web, que monitorea la navegación web de los usuarios.

4.2.13. Servidor de Aplicaciones

Se instalan para cada aplicación que se utiliza en la red. Por ejemplo, servidores de RR.HH, de *contabilidad*, de finanzas, etc. Estos servidores contienen todas las aplicaciones del negocio.

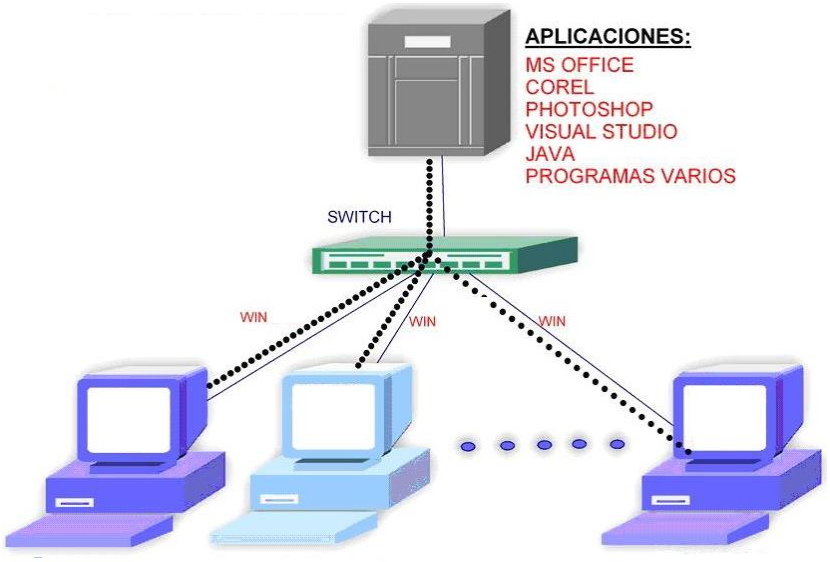

Figura 21. Representación gráfica de un Servidor de Aplicaciones

4.2.14. Servidores Virtuales

La virtualización permite usar toda la capacidad de los servidores durante el mayor tiempo posible. Así, se *pueden exprimir los* recursos de hardware sin gastar de más. *La virtualización hace posible* tener varios servidores en uno solo y, de este modo, compartir todos los recursos. Por ejemplo, se puede virtualizar un sistema de base de datos y compartir el hardware con algún otro servidor, como uno de archivos o de impresión. La virtualización pone una capa de tecnología entre el hardware y el sistema operativo; hace creer a este último que está instalado en un equipo físico cuando, en realidad, está virtualizado. (Marchionni, 2011).

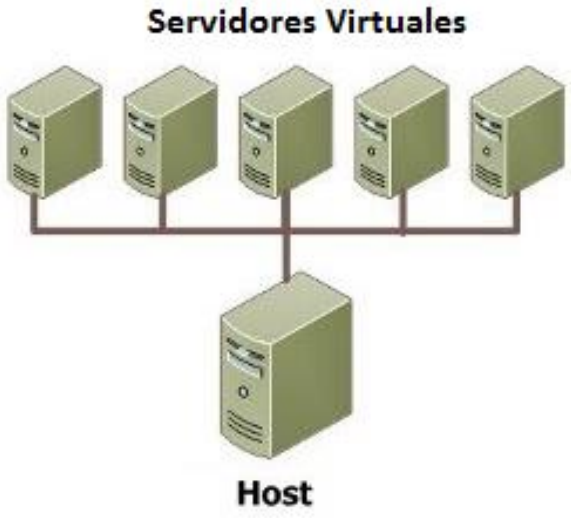

Figura 22. Virtualización

Un servidor virtual es un servidor que contiene particiones virtuales y cada una de estas particiones tiene su propio sistema operativo, lo que hace que funcione al igual que una computadora física.

Unas de las principales ventajas de la virtualización son la reducción de costos y ahorro de espacio.

4.3. Arquitecturas de Almacenamiento

El almacenamiento de datos es una actividad que se realiza sin complicaciones en los data centers. Esta actividad es transparente para los usuarios pero es de vital importancia.

Existen diversos tipos de modelos de almacenamientos que pueden ser implementados con el objetivo de gestionar de manera más efectiva los recursos y acceder a los datos de forma más rápida y sencilla.

4.3.1. Arquitectura de Almacenamiento Externo Directo (DAS)

La arquitectura de almacenamiento DAS (Direct Attached Storage) es la forma más simple y tradicional de almacenamiento. En este modelo, el dispositivo de almacenamiento está conectado directamente al equipo o es parte de él. El equipo puede ser un servidor o una PC.

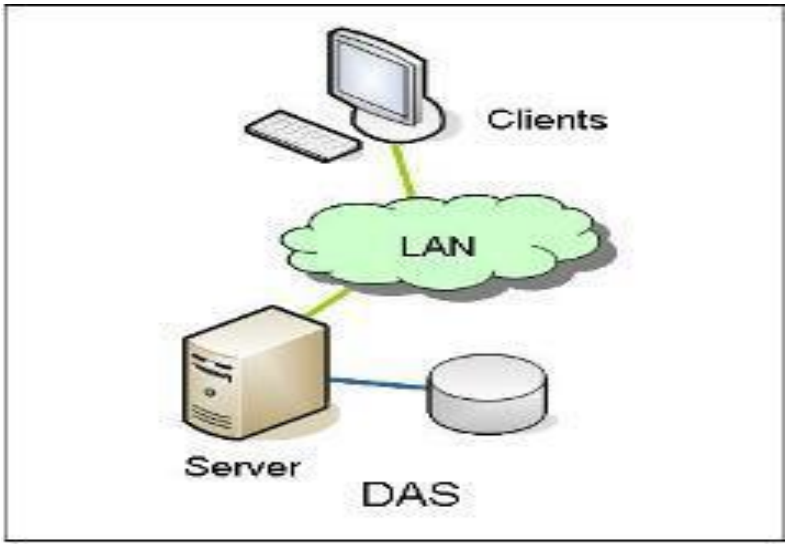

Figura 23. Esquema de almacenamiento DAS

Según Holtsnider & Jaffe (2007) esta es la diferencia entre DAS y otras arquitecturas de almacenamiento como son SAN y NAS.

Actualmente esta arquitectura no es muy utilizada en organizaciones y es más utilizada en computadoras de escritorio. Según Holtsnider & Jaffe (2007) para manejo de

gran cantidad de datos, DAS es considerada como un uso ineficiente de hardware ya que se debe hacer una considerada inversión de este en servidores, lo cual puede terminar siendo subutilizado.

De acuerdo con el sitio web GuilleSQL (2009), la arquitectura de almacenamiento DAS, presenta muchos inconvenientes, como es la dispersión del almacenamiento que implica una dificultad en la gestión de las copias de respaldo (backups), una relativamente baja tolerancia a fallos (sólo posible a través de soluciones RAID), y un alto TCO[9] debido a las dificultades de mantenimiento.

4.3.2. Arquitectura de Almacenamiento Conectado en Red (Network-Attached Storage o NAS)

NAS (Network Attached Storage) se refiere a un dispositivo de almacenamiento que es conectado directamente la red Ethernet a través de un conector RJ45. Muchas veces es considerado como un servidor porque trae incluido procesador y un sistema operativo pero su principal función es ser utilizado para el almacenamiento de información.

[9] Costo total de propiedad, que es el costo del producto a lo largo de su ciclo de vida completo.

Los archivos de un sistema NAS son accesibles a través de la red utilizando protocolos de compartimiento de archivos tales como NFS[10] o CIFS[11] de Microsoft. Los usuarios en una red NAS son capaces de acceder a los archivos sin la necesidad de tener que conectarse a un servidor tradicional. (Holtsnider & Jaffe, 2007).

Las soluciones de tipo NAS son escalables, tienen bajo coste y su instalación es sencilla. Según el portal web D-Link (2012) el principal inconveniente de este tipo de arquitectura es la propia LAN que al transportar todo el tráfico de datos de la empresa (aplicaciones, web, almacenamiento,…) puede constituir un cuello de botella.

[10]Network File System o Sistema de archivos de Red. NFS se utiliza para el compartimiento de archivos en una red LAN.

[11] Common Internet File System o Sistema de archivos común de internet. Es un protocolo que permite a los programas hacer solicitudes de archivos y servicios en computadoras remotas en internet.

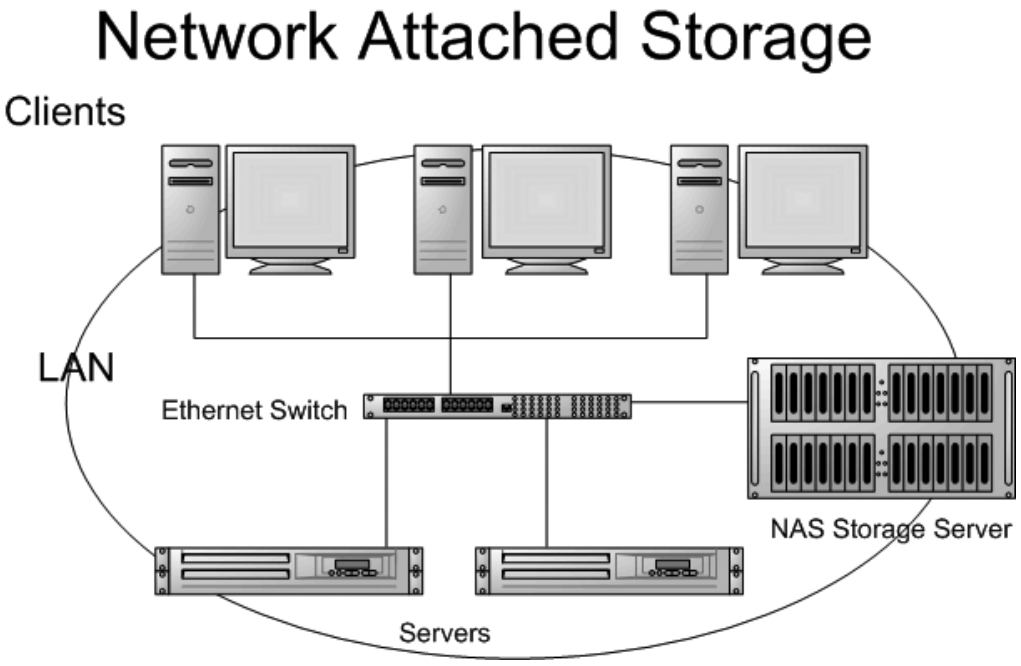

Figura 24. Esquema de almacenamiento NAS

Para aumentar su capacidad total, los sistemas NAS pueden contar con varios dispositivos de almacenamiento dispuestos en RAID (Redundant Arrays of Independent Disks) con discos SCSI (Small Computer System Interface), SAS (Serial SCSI), ATA (Advanced Technology Attachment) y SATA (Serial ATA). Además de discos los sistemas NAS pueden incorporar unidades de cinta magnética y soportes ópticos. (D-Link, 2012).

4.3.3. Arquitectura de Almacenamiento SAN

SAN (Storage Area Network), o red de área de almacenamiento, es una arquitectura de almacenamiento de alto rendimiento y está diseñada de modo que diferentes sistemas puedan tener comunicación con distintos sistemas de almacenamiento.

Las redes SAN son redes secundarias dedicadas exclusivamente al almacenamiento de datos que incluyen componentes estándar como servidores, multiplexores (MUX), puentes y dispositivos de almacenamiento (por ejemplo, cintas o arrays de disco). Cada servidor de la red principal se conecta a la red SAN mediante una conexión SCSI o de canal de fibra, de forma que todos ellos gozan de acceso de alta velocidad a los dispositivos de almacenamiento. Los servidores de la red tratan al espacio que se les ha asignado en la red SAN como si fuera un disco conectado directamente al servidor, y la red SAN utiliza el mismo protocolo de comunicación que emplea la mayoría de los servidores para comunicarse con sus discos respectivos. El modelo SAN agrupa a varios dispositivos de almacenamiento formando una red a la que todos los servidores de la red LAN se encuentran conectados. La información se almacena en la red SAN, por lo que, a diferencia del modelo NAS, los clientes tienen que solicitar los archivos a los servidores para que éstos se los suministren. (BitHoy, 2008).

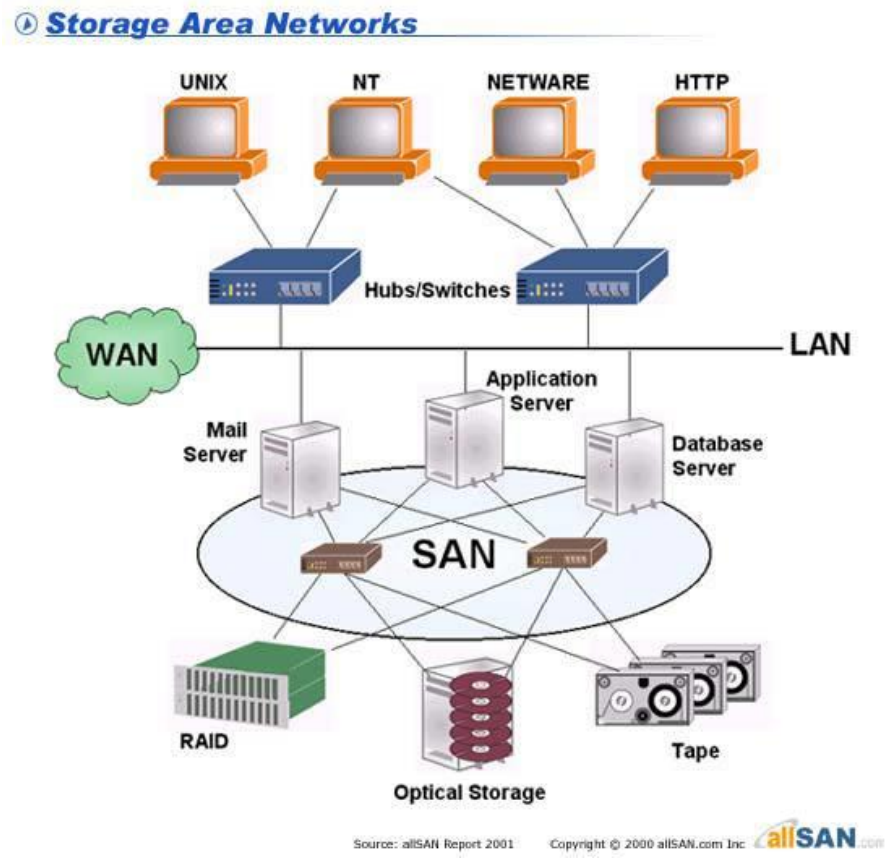

Figura 25. Esquema de almacenamiento SAN

La forma en la que se encuentra estructurada una red con sistema SAN evita un impacto significativo en la red de usuario, esto es porque dicha red está separada de la red de almacenamiento.

4.3.4. Almacenamiento en la Nube (Cloud Storage)

Esta arquitectura de almacenamiento permite almacenar información en la nube. El término en "nube" es una metáfora y se refiere básicamente a servicios utilizados por medio del internet. El servicio de almacenamiento en la nube permite almacenar y respalda los datos de forma remota sin la necesidad de utilizar servidores físicos. En cambio la información se almacena en servidores de que son administrados por algún proveedor de servicios. Generalmente para acceder a los datos el usuario debe autenticarse proveyendo un nombre de usuario y una contraseña.

Miranda (2014) dice que la gran ventaja de este sistema es la posibilidad de acceder a los archivos desde cualquier dispositivo que se conecte a internet entrando a través de la cuenta. Sin embargo, este sistema puede vulnerar la privacidad de los usuarios o limitar su capacidad de acción. También resalta que el dejar todos los datos privados en manos de servidores de terceros es una idea que a mucha gente no le agrada.

4.4. Seguridad Informática

La seguridad es un elemento crítico dentro de los sistemas informáticos. Poder preservar la información es algo muy importante para las organizaciones. Cualquier factor que ponga en riesgo la información de una organización es considerado como una amenaza y esto podría traer serias consecuencias, en cuanto a tiempo y dinero se refiere, esto sin tomar en cuenta el acceso de un usuario no autorizado.

Según García-Cervigón & Ramos (2011) la seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar el mismo.

Esta sección trata temas de importancia en cuanto a la seguridad informática dentro de las organizaciones.

4.4.1. Conceptos Generales

Los siguientes conceptos se consideran importantes al momento de hablar de seguridad de la información[12]:

- **Integridad:** asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido recibido es el correcto.

- **Confidencialidad:** proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

- **Disponibilidad:** permitirá que la información esté disponible cuando lo requieran las entidades autorizadas.

- **Autenticación (o identificación):** el sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o genera una determinada información es quien dice ser.

[12] Los conceptos fueron extraídos de (López, 2010, pp. 12-16)

- **No repudio (o irrenunciabilidad):** el no repudio consiste en no poder negar haber emitido una información que si se emitió y en no poder negar su recepción cuando si ha sido recibida.

- **Control de acceso:** podrán acceder a los recursos del sistema del sistema solamente el personal y usuarios con autorización.

- **Activos:** son los recursos que pertenecen al propio sistema de información o que están relacionados con este. Este pueden ser: datos, software, hardware, redes, soportes, instalaciones, personal y servicios.

- **Amenaza:** es la presencia de uno o más factores de diversa índole 9personas, maquinas o sucesos) que – de tener la oportunidad – atacarían al sistema produciéndoles daños aprovechándose de su nivel de vulnerabilidad.

- **Riesgos:** es la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad.

- **Vulnerabilidades:** probabilidades que existen de que una amenaza se materialice contra un activo.

- **Ataques:** se dice que se ha producido un ataque accidental o deliberado contra el sistema cuando se ha materializado una amenaza.

- **Impactos:** son las consecuencias de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

4.5. Herramientas de Análisis y Gestión de Riesgo

4.5.1. Política de Seguridad

Una política de seguridad es una serie de lineamientos que indican al usuario como debe de actuar con relación a los servicios y recursos de la empresa.

Según López (2010), una política de seguridad recoge las directrices u objetivos de una organización con respecto a la seguridad de la información y su objetivo es

concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer que principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados.

4.5.2. Auditoría

Una auditoria es el proceso de evaluación por el cual pasa el sistema de información que permite identificar y corregir problemas o posibles vulnerabilidades en los procesos y componentes que forman el sistema. Su principal objetivo el cumplimiento de los objetivos establecidos en la política de seguridad.

4.5.3. Plan de Contingencias

El plan de contingencia es un instrumento de gestión que contiene las medidas (tecnologías, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperarlo tras un impacto. (López, 2010).

La continuidad de negocio no es más que la continuidad de las operaciones en caso de que ocurra una interrupción no deseada o algún desastre en las actividades criticas del negocio. Para esto es necesario crear un plan el cual es conocido como plan de continuidad de negocios.

Se puede decir que un plan de contingencia es una variante de un plan de continuidad de negocios. El plan de contingencia sigue el ciclo de vida PDCA (Plan-do-check-act, es decir, planear-hacer-verificar-actuar).

Figura 26. Ciclo Deming

- **Planificar**: definir los objetivos y los medios para conseguirlos.

- **Hacer**: implementar la visión preestablecida.
- **Verificar**: comprobar que se alcanzan los objetivos previstos con los recursos asignados.
- **Actuar**: analizar y corregir las desviaciones detectadas así como proponer mejoras a los procesos utilizados.

Las fases del ciclo de vida del servicio son un reflejo de esta estructura básica[13]:

El plan de contingencia se realiza después de hacer un análisis de riesgo e identificar las amenazas que afectan la continuidad del negocio.

4.5.4. Modelos de Seguridad

Un modelo de seguridad es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información. (López, 2010).

[13] Ver sección 5.11 para saber acerca el Ciclo de Vida Del Servicio y sus fases.

4.6. Normas de Seguridad

Una norma es un documento cuyo uso es voluntario y que es fruto del consenso de las partes interesadas y que deben aprobarse por un Organismo de Normalización reconocido (García-Cervigón & Ramos, 2011).

El organismo encargado de desarrollar las diferentes reglas de normalización es la ISO (International Organization for Standardization, Organización Internacional para la Estandarización). Dentro del conjunto de normas utilizadas para lograr una estandarización, en cuanto a la seguridad se refiere, dentro de las organizaciones existe la serie de normas ISO/IEC 27000. Estas normas abarcan materias como los controles, valoración de riesgo y sistema de gestión de la seguridad de la información.

García-Cervigón & Ramos (2011) menciona las siguientes normas con relación a la seguridad informática:

4.6.1. ISO/IEC 27000-Series

ISO/IEC 27000-Series es un conjunto de normas de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que contiene un conjunto de mejores prácticas recomendadas para la implementación y mantenimiento de especificaciones de un Sistema de Gestión de Seguridad de la Información (SGSI). La norma ISO/IEC 27000, específicamente, define el vocabulario estándar para el SGSI.

4.6.2. ISO/IEC 27001

Que sustituye a las ISO 17799-1, abarca un conjunto de normas relaciones con la seguridad informática. Se basa en la norma BS 7799-2 de British Standard, otro organismo de normalización. Según esta norma, que es la principal de la serie, la seguridad de la información es la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento.

4.6.3. ISO/IEC 27002

Que se corresponde con la ISO 17799, y que describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendables relacionados con la seguridad.

4.6.4. ISO/IEC 27003

Que contiene una guía para la implementación de la norma. Esta norma se enfoca en los aspectos necesarios para implementar un sistema de gestión de la seguridad de la información exitoso. La norma contiene diferentes planes de implementación y su diseño.

4.6.5. ISO/IEC 27004

Que contiene los estándares en materia de seguridad para poder evaluar el sistema de gestión de la seguridad de la información.

La norma incluye la política, gestión de información de riesgo de seguridad, objetivos de control, controles, procesos y procedimientos, y apoyar el proceso de su

revisión, ayudar a determinar si alguno de los procesos de SGSI o controles necesitan ser cambiados o mejorados. Hay que tener en cuenta que ninguna de las mediciones de los controles puede garantizar la seguridad total.

4.6.6. ISO/IEC 27005

Que recoge el estándar para la gestión del riesgo de la seguridad. Esta norma aplica a cualquier tipo de empresa que tenga la necesidad de gestionar el riesgo de la seguridad de la información.

La norma resalta la necesidad de identificar los activos en riesgo, las amenazas y vulnerabilidades potenciales, e impacto en caso de llegar a materializarse el riesgo.

La norma no recomienda o menciona un método específico con cual deba ser gestionado el riesgo pero si ofrece un estructurado, riguroso y sistemático método de análisis de riesgo a través de un plan de tratamiento del riesgo.

4.6.7. ISO/IEC 27006

Requisitos a cumplir por las organizaciones encargadas de emitir certificaciones ISO 27001.

El principal objetivo de esta norma es proporcionar una guía y los requerimientos necesarios para que las entidades que proveen auditorias y certificaciones de un sistema de gestión de seguridad de la información puedan realmente hacerlo. Cualquier organización que se encargue de proveer certificaciones de la ISO/IEC 27001 debe de cumplir con los requerimientos establecidos en la norma ISO/IEC 27006. Adicional a esto, también deben de cumplir con los requisitos especificados en las normas ISO/IEC 1702-1 y la ISO 19011.

4.6.8. ISO/IEC 27015

Que contiene una guía para organizaciones del sector financiero y de seguros. Esto incluye organizaciones tales como bancos, compañías de seguros y cualquier otro tipo de entidad financiera. La norma amplia algunas recomendaciones ofrecidas en la norma ISO/IEC 27002 sobre las entidades financieras y dice que la seguridad debe de

cubrir no solo los empleados sino también los clientes. Este estándar fue publicado en noviembre del 2012.

4.6.9. ISO/IEC 27032

Es una guía sobre la seguridad de internet o ciberseguridad. La norma tiene como objetivo la preservación de la confidencialidad, integridad y disponibilidad de la información en internet.

4.6.10. ISO/IEC 27033

Es una norma aplicada a la seguridad de redes, dividida en varias partes, entre ellas, diseño e implementación de seguridad en redes, asegurar las comunicaciones entre redes mediante gateways, asegurar las comunicaciones mediante VPN, redes inalámbricas, etc.

La norma no solo intenta implementar la seguridad en los dispositivos, esta también aplica a los usuarios de la red y a los servicios y aplicaciones de red.

La norma va dirigida básicamente a los arquitectos de seguridad, gerentes, oficiales y diseñadores de esta.

4.6.11. ISO/IEC 27034

La norma ISO/ICE 27034 ofrece una guía sobre la seguridad de la información para esos que implementan, procuran o programan sistemas de aplicaciones. Su finalidad es asegurar que las aplicaciones desarrolladas cumplan con el nivel de seguridad deseado en soporte al sistema de gestión de seguridad de la información de la organización. Esta norma provee una guía sobre cómo especificar, implementar, seleccionar y diseñar controles de seguridad de la información a través de una serie de procesos integrados al ciclo de vida de desarrollo de sistema de la organización.

4.7. Clasificación de la Seguridad Informática

Tomando en cuenta el activo que se va a proteger, la seguridad informática se puede clasificar en: seguridad pasiva, seguridad activa, seguridad lógica y seguridad física.

4.7.1. Seguridad Pasiva

La seguridad pasiva está constituida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema (López, 2010, p. 30).

La seguridad pasiva se encarga de corregir daños ocasionados incidentes de seguridad y puede ser aplicada tanto a los elementos físicos como a los lógicos. Es decir, se puede aplicar la seguridad pasiva en las instalaciones y también en los sistemas operativos.

El objetivo de la seguridad pasiva es hacer que el impacto de los daños ocasionados sea menor. Se pueden considerar como ejemplo de seguridad pasiva, pero no limitándose a estos, el respaldo de información (backup), los arreglos de discos o RAIDs o los sistemas de alimentación interrumpida (UPSs).

4.7.2. Seguridad Activa

Según López (2010), los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información constituyen la seguridad activa del mismo.

La seguridad activa, a diferencia de la seguridad pasiva, es de prevención. Esta previene los riesgos y los identifica antes de que se lleguen a producir daños en el sistema de información. Se aplica a la parte física y la parte lógica.

4.8. Seguridad Física

El entorno entiende por entorno físico, como su nombre lo indica, está compuesto por los elementos físicos, es decir, el edificio o el salón en el que se encuentran los equipos informáticos, el sistema de red y los periféricos.

La seguridad física tiene como objetivo proteger los equipos informáticos (computadoras, cableado de red, servidores, etc.) principalmente de posibles desastres naturales (inundaciones, incendios, terremotos, etc.). Las amenazas físicas pueden ser provocadas por el hombre de forma accidental o involuntaria.

Dentro de la seguridad física se pueden encontrar: UPSs, guardias de seguridad, control de acceso, alarmas, extintores, cámaras de seguridad, alarmas antiincendios, climatizadores, entre otros.

4.8.1. Ubicación de los Equipos

Para determinar cuál ubicación deben de tener los elementos de un sistema informático se deben de tomar más en cuenta aquellos elementos que son críticos para el funcionamiento del sistema o aquellos que contienen información de suma importancia.

Según García-Cervigón & Ramos (2011), los servidores son el elemento dentro de un sistema informático más importante, luego su situación y las condiciones de la habitación donde se ubiquen deben estar especialmente protegidas, y encontrarse en condiciones buenas de humedad, temperatura, limpieza…. Para ello es necesario que cuenten con un especial sistema de acondicionamiento de la temperatura y la humedad. Es por esto que existen los centros de procesamientos de datos (CPD).

4.8.2. Sistemas de Protección

Dentro de los sistemas de protección necesarios para la asegurar los equipos del sistema informático se pueden mencionar los siguientes:

4.8.3. Sistema Contra Incendios

Un sistema contra incendios es un sistema de protección crítico dentro de los centros de procesamientos de datos ya que en caso de incendio ayudara a evitar la propagación del mismo y a su extinción, evitando así daños mayores.

López (2010) dice que un sistema contra incendio también comprender la existencia de vías de evacuación de personas con la señalización correspondiente y los sistemas de extinción. Dentro de los elementos que debe de tener un sistema contra incendios se pueden mencionar:

- **Muros cortafuegos:** separan edificios o zonas distintas de un mismo edificio. Su objetivo es impedir durante un periodo más o menos largo de tiempo que el incendio se propague a sus áreas colindantes, reduciendo los daños y el riesgo para las personas.

- **Puertas cortafuegos:** Impiden la propagación no solo del fuego a zonas colindantes, sino también de humo y gases tóxicos y deben proteger las vías de evacuación.

- **Compuertas cortafuegos:** se colocan en las salidas de los conductos de ventilación y aire acondicionado para cerrarse de forma manual o automática en caso de incendio e impedir que el fuego, el humo y los gases se propaguen a otras secciones.

- **Detectores de incendio:** son dispositivos que se instalan normalmente en el techo o en la parte más alta de los muros de las habitaciones, que son los puntos hacia donde se desplaza el humo, evitando las esquinas, a las que el humo llega más tarde que al resto de la superficie.

- **Extintores**: son elementos destinados a combatir el fuego. Se clasifican en:

1) **Tipo A (Sólidos):** Se denominan fuego de clase A los que se producen en combustibles sólidos que producen brasas, por ejemplo: papel, cartón, madera, plásticos, etc.

2) **Tipo B (Líquidos inflamables):** Se denominan fuegos de clase B los que se producen en combustibles líquidos, por ejemplo: aceites vegetales, derivados del petróleo, etc.

3) **Tipo C (Gases):** Se denomina fuegos de clase C los que se producen en gases, por ejemplo: butano, acetileno, metano, propano, etc.

4) **Tipo D (Metales combustibles):** Se denomina fuegos de clase D los que se producen en metales y aleaciones, por ejemplo: magnesio, potasio, sodio.

4.8.4. Sistema de Protección Eléctrica

El sistema de protección eléctrica debe de ser tomado en consideración cuando se habla de seguridad ya que todos los equipos funcionan gracias a él.

Según López (2010), se puede ver la red eléctrica desde dos puntos de vista: la externa, que pertenece a la compañía proveedora de electricidad, y la interna que es propiedad de la empresa. Sobre la externa poco se puede hacer en cuestión de seguridad, excepto ocultar el cableado visible o fácil de alcanzar en la fachada del edificio y que se convertiría en un punto vulnerable si alguna mano malintencionada quisiese cortar el suministro. Para cubrir y proteger esa parte externa se necesitan los permisos de la compañía eléctrica.

En cuanto a la parte externa, se recomienda instalar dispositivos que sirvan para suplir las necesidades de energía eléctrica en caso de que haya alguna interrupción. Estos sistemas pueden ser:

a. **Grupos electrógenos:** es un generador de corriente eléctrica que funciona con combustible. También son conocidos como plantas eléctricas.

b. **Sistema de alimentación ininterrumpida (SAI o UPS en inglés):** este también es un generador de corriente eléctrica que carga sus baterías y provee energía eléctrica a los equipos en caso de interrupción del servicio.

4.8.5. Sistema de Control de Acceso

Estos sistemas son utilizados para impedir la entrada de personal no autorizado a las instalaciones. Dentro de estos sistemas se pueden mencionar:

- **Personal de seguridad:** para comprobar la identidad de la persona al momento de entrar a las instalaciones.

- **Sistemas biométricos:** utilizan una característica del cuerpo humano para dar el acceso. Puede utilizar huellas digitales, verificación de voz, patrones oculares o firmas.

- **Tarjetas de acceso:** son tarjetas que tienen un circuito integrado codificado para dar acceso. También son conocidas como tarjetas inteligentes (Smart Cards).

- **Videovigilancia:** es la utilización de cámaras para monitorear las instalaciones y visualizar quien accede a ella. Dependiendo de la necesidad de la empresa se pueden utilizar cámaras IP o Circuito cerrado de televisión (CCTV).

a. **Cámaras IP:** transmiten imágenes, audio y video directamente a través de una red de internet o intranet que desde un explorador web o de un concentrador en una red.

b. **CCTV:** El circuito cerrado de televisión o CCTV es un sistema diseñado para un número limitado de espectadores. Puede componerse de una o

más cámaras conectadas a monitores de video o televisiones que reproducen la imagen capturada por las cámaras.

- **Alarmas:** se encargan de alertar al personal pertinente sobre cualquier evento que pudiese ocurrir. De acuerdo con López (2010) algunos data centers cuentan con un panel de control que monitoriza las distintas alarmas: incendios, temperatura, gases, líquidos, intrusos…, y que indica qué tipo de alarma se ha producido y en qué punto del edificio, además de activar los mecanismos de seguridad asociados a cada tipo de alarma.

4.8.6. Sistema de Climatización

El sistema de climatización vela porque los equipos se encuentren con una temperatura adecuada. Los equipos informáticos general una gran cantidad de calor debido a la cantidad de datos que procesan y la capacidad a la que trabajan. Sin un sistema de climatización óptimo estos podrían sobrecalentarse y afectar su funcionamiento.

Según Gallego (2014), los sistemas de climatización pueden ser simples (como un aparato de aire acondicionado convencional) o complejos, llegando incluso a afectar la estructura del edificio.

4.9. Seguridad Lógica

La seguridad lógica se encarga de la protección de la parte lógica de la organización, es decir, se encarga de todo lo que es software y de los datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa, usando una VPN (protocolos PPP, PPTP,…) la web (protocolos http, https), transmisión de ficheros (ftp), conexión remota (SSH, telnet)… (García-Cervigón & Ramos, 2011).

La seguridad lógica tiene como fin lograr los siguientes objetivos:

- Restringir el acceso a los programas y archivos.
- Asegurar que los usuarios puedan trabajar sin supervisión y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Verificar que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

4.9.1. Medidas de Seguridad Lógica

La seguridad lógica es controlada mayormente por software. Cada vez los sistemas operativos controlan más la seguridad del equipo informático ya sea por parte de un error, por un uno incorrecto del sistema operativo o del usuario, o bien por un acceso no controlado físicamente a través de la red, o por un programa malicioso, como los virus, espías, troyanos, gusanos, entre otros. (García-Cervigón & Ramos, 2011).

4.9.2. Mecanismos de Seguridad Lógica

Al igual que la seguridad física cuenta con mecanismos de seguridad que previenen, detectan o corrigen ataques al sistema, la seguridad lógica cuenta con los mismo. Dentro de los mecanismos de seguridad que utiliza se pueden mencionar los siguientes:

- Control de accesos
- Cifrado o encriptación de datos
- Antivirus
- Cortafuegos (firewall)
- Firma digital
- Certificados digitales
- Utilización de SSID (Service Set Identifier)
- Protección de la red mediante claves encriptadas WEP (Wired Equivalent Privacy)
- Filtrado de direcciones MAC (Media Access Control).

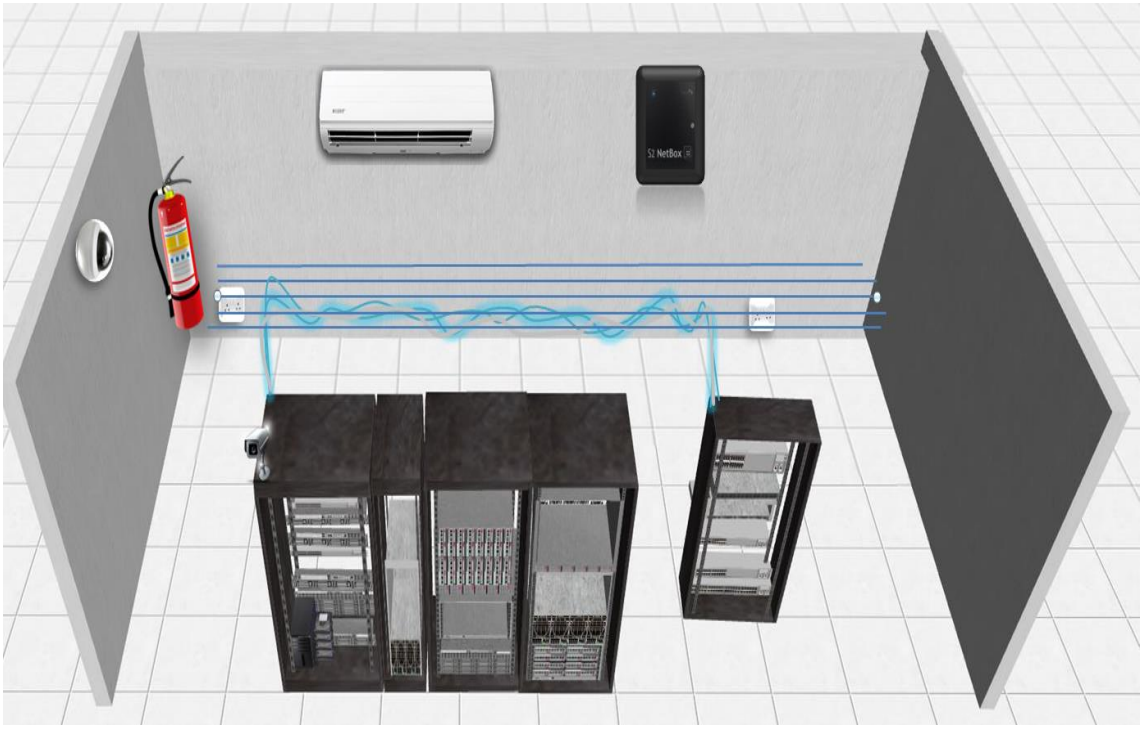

Figura 27. Modelo Data Center YP Directories

La figura 27 es un modelo del Data Center de la Empresa YP Directories. Este contiene los elementos descritos durante el capítulo y sirve de soporte para poder brindar los diferentes servicios de TI.

5. CAPITULO V – LIBRERÍA DE INFRAESTRUCTURA DE LA TECNOLOGIA DE LA INFORMACION VERSION 3 (ITILV3)

5.1. ITILv3 – Antecedentes

En los años 80, la calidad de los servicios TI que prestaba el gobierno británico era tal que se instruyó a la par entonces CCTA (Agencia Central de Telecomunicaciones y Computación, hoy Ministerio de Comercio, OGC) para que desarrollara una propuesta con el fin de que los ministerios y demás oficinas del sector público de Gran Bretaña utilizaran de manera eficaz y con eficiencia de costes los recursos de TI. El objetivo era desarrollar una propuesta sin independiente de todo proveedor. Esto dio como resultado la Biblioteca de Infraestructura de Tecnologías de Información (Information Technology Infrastructure Library o ITIL) (itSMF International, 2008, pág. 1).

ITIL es un conjunto de buenas prácticas de TI que busca mejorar y entregar soportes de servicios de TI de calidad a través de una serie de procesos, funciones, roles, tareas y procedimientos.

ITIL toma el enfoque del ciclo de vida para implementar La Gestión de Servicios y está basado en cinco libros fundamentales: Estrategia del Servicio, Diseño del Servicios, Transición del Servicio, Operación del Servicios y Mejoramiento Continuo del Servicio.

Basándose en ITIL se han desarrollado varios sistemas para la Gestión de Servicios de TI, generalmente organizaciones de negocio. Los ejemplos incluyen Hewlett & Packard (HP ITSM modelo de referencia), IBM (TI Modelo de Proceso), Microsoft (MOF) y muchos otros. Esta es una de las razones por las que ITIL se ha convertido en el estándar de facto para describir varios procesos fundamentales de la Gestión de Servicios de TI. Esta adopción y adaptaciones de ITIL reflejan la propia filosofía de ITIL, y son desarrollos para que ITIL se transforme en el tan necesario orden metodológico, imprescindibles para los actuales entornos heterogéneos y distribuidos de TI (itSMF International, 2008, pág. 1).

Existen tres versiones de ITIL. La versión 3 fue lanzada por la OGC en el 2007 y hasta la fecha no ha habido actualización. Esta última versión esta estructuralmente basada en el concepto de Ciclo de vida de los Servicios.

5.2. Conceptos Generales

5.2.1. ¿Qué es un Servicio?

Según Pink Elephant (2013), los servicios son el medio para entregar valor a los clientes, facilitando los resultados que quieren logara sin la propiedad de los costos y riesgos específicos.

Los servicios son el conjunto de tareas que buscan obtener como resultado final la satisfacción de los clientes sin necesidad de que estos tengan que ver con los costos y los riesgos asociados a dicho servicio.

5.2.2. Clasificación de los Servicios los servicios se clasifican en:

- **Servicios base:** que son los servicios propuestos originalmente al cliente y que fundamentan la propuesta de valor.

- **Servicios habilitantes:** que son los servicios necesarios para poder ofrecer el servicio base.

- **Servicios complementarios**: que son servicios de valor agregado, es decir, servicios extras que se añaden al servicio base con la intención de hacer que el cliente utilice más el servicio. Estos servicios no son esenciales para brindar el servicio base.

Los servicios también pueden ser internos, que son los entregados desde TI a otros departamentos o unidades de la misma organización, o externos cuando se entregan a clientes externos directamente.

5.2.3. Servicios de TI

Es el servicio ofrecido por un proveedor de servicios de TI, en este caso el departamento de tecnología de la organización. Los servicios de TI pueden ser de dos tipos, de cara al cliente, cuando TI provee los servicios a los clientes (pueden ser internos o externos) y de soporte, cuando que es el servicio que se da dentro de la misma estructura de TI.

Estos servicios pueden ser los siguientes:

- Servicio de infraestructura
- Servicio de soporte y desarrollo a aplicaciones
- Servicio de Helpdesk
- Servicio de soporte

5.2.4. Valor

Pink Elephant (2013) define el valor como la combinación de utilidad y garantía del servicio. Utilidad es la funcionalidad que ofrece un producto o servicio para satisfacer una necesidad particular. La garantía es el hecho de que el servicio cumple con los requerimientos acordados.

Para que el servicio entregado tenga valor, ambas, la utilidad y la garantía, son necesarias. El valor es el medio a través el cual se entrega el servicio al cliente.

5.2.5. ¿Qué es un Proceso?

Un proceso es una serie bien definida y estructurada de actividades que tiene como objetivo cumplir con un objetivo en específico. Un proceso toma entradas definidas, las procesa y produce salidas definidas.

Los procesos bien definidos pueden traer consigo valor para las partes interesadas de diferentes maneras, tales como incrementar la productividad dentro y a lo largo de las organizaciones y las funciones, así como mejorar la efectividad y la eficiencia de los servicios soportados por los procesos (Pink Elephant, 2013).

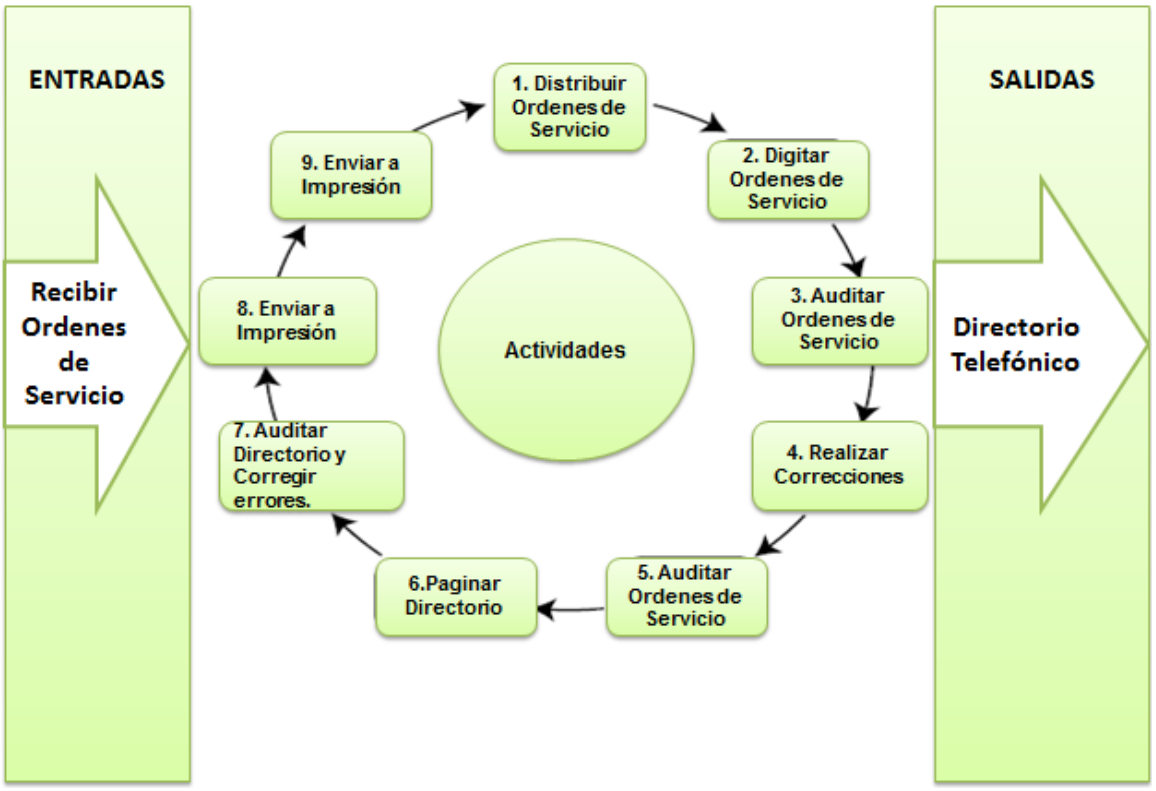

Figura 28. Proceso de Negocio de YP Directories. Fuente: Propia

La figura 28 es un ejemplo de proceso basado en el proceso de negocio de la compañía YP Directories. El proceso tiene entradas definidas, que son las ordenes de servicios recibidas por las telefónicas, actividades que abarcan las tareas y procesos necesarios para obtener el resultado y las salidas que son directorios ya impresos.

Todos los procesos tienen las siguientes cuatro características en común:

- Son medibles

- Entregan resultados específicos
- Tiene clientes, es decir, el resultado final es recibido por un cliente
- Responde a eventos específicos

Los procesos siempre tienen un disparador, es decir, no existen solo porque sí, tienen una razón de ser y tienen resultados específicos orientados a los clientes.

5.2.6. Gestión de Servicios de TI (ITSM)

Pink Elephant (2013) define la Gestión de Servicios como el conjunto de capacidades especializadas de la organización para proveer valor a los clientes en forma de servicios.

La gestión de servicios comprende una serie de procesos necesarios para obtener la calidad de los servicios prestados. Transforma las capacidades y los recursos en servicios valiosos.

Tradicionalmente TI siempre ha tenido un enfoque basado únicamente en la tecnología y tomando en cuenta únicamente la calidad del hardware que soporta su infraestructura. Sin embargo, hoy en día ese paradigma ha cambiado y el uso de TI hoy

en día se ha convertido en algo similar a los servicios públicos para el negocio y es por esto que para poder satisfacer las necesidades de negocio, TI debe de tener un enfoque diferente tomando en cuenta no solo la tecnología de la información, sino las personas y procesos adecuados.

La gestión de servicios de TI busca satisfacer las necesidades de negocio por medio de la calidad de sus servicios basándose en procesos y funciones gestionados a lo largo de un ciclo de vida. Tiene su enfoque en la estrategia, diseño, operación y mejora continua.

5.3. ITIL Versión 2 vs ITIL Versión 3

ITIL Versión 2 fue lanzada en el 2001 con los libros de *"Service Support" y "Service Delivery"* (Soporte del Servicio y Entrega del Servicio). En el 2007 se lanzó la versión 3 pero está aún tenía como enfoque los principios fundamentales de la versión 2. La versión fue organizada bajo el concepto de Ciclo de Vida del Servicio e incluyo algunos nuevos beneficios. En el 2011 se realizó una actualización a la versión 3 de ITIL (B.S, 2014).

De acuerdo con B.S (2014), el contenido y la estructura de la versión 3 de ITIL está basada en extensas consultorías públicas y contribuciones de líderes de la industria, clientes, usuarios, vendedores, proveedores de servicio y otras organizaciones de mejores prácticas, para así determinar cuáles mejores se ajustan más a las organizaciones de hoy en día.

Según OSIATIS S.A, "La principal diferencia entre las versiones v2 y v3 de ITIL es que esta última versión basa su estructura sobre el concepto de Ciclo de Vida de los Servicios".

De acuerdo con B.S (2014), la diferencia entre las dos versiones está en el enfoque, la versión 2 de ITIL está basada en procesos y orientada a operaciones y la versión 3 se basa en el valor y al servicio y enfoca en alinear a TI con las necesidades del negocio.

Según Herold (2008), ITIL v3 es mas facil para los Gerentes de TI implementar y seguir porque se acerca mas al ciclo de vida de las operaciones del negocio y de como este es gestionado.

La siguiente figura muestra los procesos que fueron incorporados a la versión 3 y pone los procesos de la versión 2 bajo el concepto del Ciclo de Vida del Servicio.

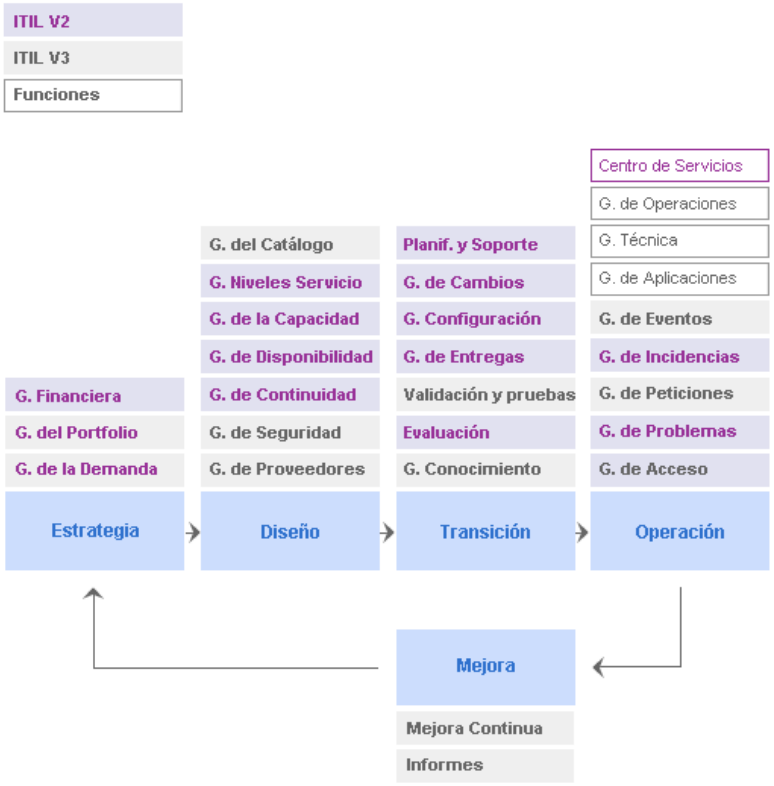

Figura 29. Fases del Ciclo de Vida con sus procesos y funciones más destacados. Fuente: econocom osiatis.

5.4. Frameworks de la Industria

Un framework sirve como referencia para poder resolver y enfrentar problemas con igual similitudes. Es un conjunto de criterios utilizados para enfocarse en una problemática en particular.

Según Herold (2008), un framework, o Marco de Trabajo, es un conjunto de controles organizados para destacar lo que hay que hacer en los distintos niveles de la organización.

A parte de ITIL existen otros modelos de mejores prácticas alrededor del mundo. Dentro de estos modelos se destacan los siguientes[14]:

5.4.1. COBIT

COBIT quiere decir Objetivos de Control para Información y Tecnologías Relacionadas (o Control Objectives for Information and related Technology, por sus siglas en inglés). Es una guía de mejores prácticas al igual que ITIL y está dirigida al control y supervisión de TI. Fue creado en el 1995 y se enfocaba en auditoria de TI. Recientemente se ha involucrado en la gestión de TI. Es manejado por el IT Governace Institute.

[14] Fuente: Libro The Shortcut Guide to IT Service Management and Automation - 2da edicion.

5.4.2. Integración de modelos de madurez de capacidades (CMMI)

El CMMI (Capability maturity model Integration) fue creado por el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon en 1991, CMMI fue desarrollado inicialmente para realizar un seguimiento de la madurez de los procesos de desarrollo de software, pero se convirtió en el que se utiliza para medir la madurez de cualquier tipo de proceso. Este se puede utilizar muy bien para determinar la madurez de los procesos de TI.

5.4.3. Comité de Organizaciones Patrocinadoras (COSO)

El Capability Maturity Model Integration o COSO es una organización voluntaria del sector privado creada en 1985 que proporciona la dirección ejecutiva con marcos y orientación para establecer operaciones de negocio más eficaces, eficientes y éticas en base global. Los conceptos de COSO pueden ser utilizados por las áreas de TI para ayudar a identificar de riesgos y las actividades de mitigación de los mismos.

5.4.4. ISO/IEC 2000

Se utiliza para proporcionar el suministro de servicios gestionados más eficaz a través de un enfoque de procesos integrados para mejores cumplen con los requisitos de negocio y de los clientes. Los conceptos pueden ser adoptados dentro de TI para mejorar servicios gestionados de TI.

5.4.5. Microsoft Operations Framework (MOF):

Según Rouse (2008), Microsoft Operations Framework (MOF) es una serie de 23 documentos que orientan los profesionales de TI a través de los procesos de creación, implementación y gestión de servicios eficientes y rentables. MOF es un marco alternativo para la Tecnología de la Información Biblioteca de Infraestructura de TI (ITIL). Como ITIL, MOF incluye directrices para todo el ciclo de vida de un servicio de TI, desde el concepto hasta el retiro o reemplazo. MOF versión 4.0 fue lanzado en abril de 2008. MOF 4.0 incluye todos los procesos de MOF 3.0 y está alineado con ITIL versión 3. La alineación con ITIL v3 permite a los administradores de TI evitar reentrenar a los miembros del personal sobre los elementos esenciales de MOS si ya estos están familiarizados con ITIL.

5.5. ¿Por qué ITIL v3?

Se escoge ITIL v3 debido a que cada vez este es cada vez más importante para los servicios de TI y se alinea y se integra con el negocio, ITIL V3 ayuda a los líderes de TI a establecer un enfoque de la gestión empresarial y la disciplina de la gestión de servicios de TI. ITIL v3 hace un buen trabajo de mapeo de las actividades y servicios de TI, relacionándolas con aspectos similares a cómo se maneja un negocio.

Por otro lado, algunos de los frameworks mencionados se basan en ITIL, como el Microsoft Operations Framework. También, ITIL es el framework más utilizado a nivel mundial.

5.6. Ciclo de Vida de un Servicio

El ciclo de vida de un servicio son las fases por las cuales el servicio debe de pasar para ser un servicio de calidad. Según ITILv3, el ciclo de vida de un servicio está basado en cinco fases: estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio.

Figura 30. Fase del clico de vida del servicio[15]

Es importante aclarar que esta propuesta se basará exclusivamente en el proceso de Continuidad de Servicios de TI que pertenece a la fase del Diseño del Servicio del Ciclo de Vida de un servicio. Los demás proceso y fases se mencionan solo para el conocimiento del lector.

[15] Fuente: http://www.tcpsi.com/servicios/gestion_ti.htm

Cada una de las etapas está compuesta por una serie de procesos que ayudaran a la buena gestión de los servicios. Estas fases se mencionan a continuación:

5.6.1. Estrategia del Servicio

Es la primera fase del ciclo de vida del servicio. La estrategia de servicio tiene como objetivo definir de forma clara, los servicios que serán entregados y financiados, a quien y por qué. En la estrategia de servicio se define la perspectiva, posición, planes y patrones que el proveedor de servicio tiene que ejecutar para cumplir con los resultados preestablecidos por la organización.

Los procesos que componen la fase de Estrategia del Servicio son:

- **Gestión Estratégica para los Servicios de TI:** Gestiona la estrategia de los servicios a lo largo de su ciclo de vida.
- **Gestión de Relaciones del Negocio:** encargado de establecer las relaciones de negocio entre los proveedores de servicios de TI y clientes.
- **Gestión Financiera para Servicios de TI:** encargado de la garantizar la correcta gestión de los servicios en cuanto a costo.
- **Gestión de la Demanda:** responsable de planificar y predecir la demanda de los servicios con el fin de adaptar a "*producción los picos de mayor*

exigencia para asegurar que el servicio se sigue prestando de acuerdo a los tiempos y niveles de calidad acordados con el cliente".

- **Gestión de Portafolio de Servicios:** responsable de definir cuales servicios serán ingresados en el *portafolio de servicio*[16] y justificar en costo su inversión con el menor riesgo posible.

5.6.2. Estrategia del Servicio

Es la segunda fase del ciclo de vida del servicio. Es prácticamente la materialización de la estrategia del servicio y tiene como objetivo diseñar nuevos servicios o modificar los ya existentes que cumplan con los objetivos del negocio.

Según Pink Elephant (2013), "es importante tener un enfoque holístico para garantizar un diseño integral y exitoso", esto quiere decir que se debe tener una visión general del servicio, tener en cuenta todo, no se puede trabajar de forma aislada porque el servicio forma parte de un sistema y hay que tener en cuenta el impacto que un servicio puede tener sobre otros.

[16] Portafolio de Servicio es el conjunto de servicios que es gestionado por un Proveedor de Servicios de TI.

Un buen diseño del servicio aporta valor al negocio: calidad, servicios efectivos en costo, procesos más efectivos, implementación más sencilla, entre otros. Según ITIL, Para que un diseño de un servicio sea exitoso, debe de contemplar los siguientes factores: personas, procesos, productos/tecnología y proveedores o socios.

Cuando se diseña un servicio nuevo, todos los aspectos y requerimientos relacionados con el servicio deben de ser almacenados en el Paquete de Diseño del Servicio (SDP) que es la representación de los documentos donde se definen los aspectos del servicio, estos aspectos pueden ser el plan de entrenamiento del servicio, sus objetivos de calidad, la evaluación de disponibilidad, procesos, procedimientos, plan de comunicación, entre otros. El SDP es la salida de la fase del diseño del servicio y se pasa a las siguientes fases y luego a producción.

Los procesos de la fase del Diseño del Servicio son:

- **Coordinación del Diseño:** responsable de que los objetivos de la fase del Diseño del Servicio se cumplan.
- **Gestión de Niveles de Servicio:** responsable de que los servicios de TI se entreguen de acuerdo a los niveles acordados con los clientes.

- **Gestión del Catálogo de Servicios:** responsable del mantenimiento de un catálogo de servicios de TI que incluya toda la información importante sobre el servicio: estado, responsables, proveedores, etc.
- **Gestión de Proveedores:** responsable de las relaciones entre el proveedor de servicios de TI y los proveedores de servicios externos.
- **Gestión de la Seguridad:** responsable de mantener la confidencialidad, disponibilidad e integridad de la información y los servicios de TI y que estos estén alineados con las necesidades del negocio.
- **Gestión de la Disponibilidad:** responsable de que los servicios siempre estén disponible y del cumplimiento de los SLAs.
- **Gestión de la Capacidad:** responsable de garantizar que la infraestructura y los servicios de TI cumplan con los niveles de capacidad acordados.
- ***Gestión de Continuidad de Servicios de TI:*** *responsable de garantizar la continuidad de los servicios de TI en caso de que ocurra algún desastre.*

5.6.3. Transición del Servicio

Es la tercera etapa del ciclo de vida del servicio. Se encarga asegurar que los servicios definidos en las etapas de diseño y transición cumplan con su finalidad y que cumplan con las expectativas del negocio y de su integración a producción y procura que sean accesibles por las personas autorizadas.

Según Pink Elephant (2013), los objetivos de la transición del servicio son: planificar y gestionar cambios en el servicio de manera efectiva y eficiente, gestionar los riesgos derivados de los servicios nuevos, modificados o retirados, implementar con éxito liberaciones de servicios en los entornos operativos, establecer expectativas correctas sobre el desempeño y utilización de servicios nuevos o modificados, asegurar que los cambios de servicios puedan crear el valor de negocio esperado y proveer una buena calidad de conocimiento e información sobre los servicios y activos del servicio.

Los procesos de la Transición del Servicio son:

- **Planificación de la Transición y Soporte:** responsable de garantizar que todos los servicios de TI (nuevos, modificados o retirados) cumplen con las expectativas de negocio tal como está documentado en las fases Estrategia y Diseño del Servicio.

- **Gestión de Activos de Servicios y Configuración:** Responsable de asegurar que todos los activos necesarios para ofrecer el servicio estén controlados, estructurados y configurados y asegurar que la información este siempre disponible cuando sea necesario.

- **Gestión de Cambios:** responsable de la gestión del ciclo de vida de todos los cambios desde su principio hasta su final, permitiendo realizar cambios interrumpiendo en forma mínima los servicios de TI.
- **Gestión de Liberación e Implementación:** responsable de implementar, desarrollar y probar las nuevas funcionalidades de los servicios requeridas por el negocio según lo descrito en la fase del Diseño del Servicio.

- **Validación y Pruebas:** responsable de validar y probar los servicios antes de que pasen a producción.

- **Evaluación de Cambios:** responsable de analizar el posible impacto de los cambios, los efectos previstos e imprevistos.

- **Gestión del Conocimiento:** responsable de gestionar toda la información relevante concerniente a los servicios y asegurar que esté disponible para las personas pertinentes.

5.6.4. Operación del Servicio

Es la cuarta fase del ciclo de vida del servicio. Se encarga de coordinar y ejecutar las actividades y procesos necesarios para entregar y Gestionar servicio en los niveles acordados con los usuarios y clientes de negocio (Pink Elephant, 2013).

Según Bon, et al. (2008), la Operación del Servicio es una fase esencial del ciclo de vida del servicio. También dice que disponer de procesos bien diseñados e implementados sirve de muy poco si no se organiza correctamente la ejecución diaria de dichos procesos. Indica que tampoco es posible introducir mejoras si durante la Operación del Servicio no se realizan sistemáticamente actividades diarias de recopilación de datos, valoración de métricas y monitorización del rendimiento.

La Operación del Servicio también está encargada de la Gestionar eficientemente y de manera efectiva la tecnología utilizada para entregar y soportar los servicios de TI.

La Operación del Servicio incluye los siguientes conceptos:[17]

[17] Los conceptos fueron extraídos del Manual de Trabajo de Fundamentos de ITIL en Español por PinkElephant.

- **Evento:** cualquier cambio de estado relevante para la gestión de servicios de TI o Elemento de Configuración (CI)[18]
- **Alerta**: una alerta es una notificación que indica que algo ha cambiado o alguna falla ha ocurrido o que se ha alcanzado algún umbral. Las alertas son parte del evento.

- **Incidente:** es la interrupción no planificada de un servicio de TI o la reducción en la calidad de un servicio de TI. Es también la falla de un elemento de configuración que aún no ha impactado el servicio.

- **Impacto**: es una medida del efecto de un incidente, problema o cambio en el proceso del negocio.

- **Urgencia**: es una medida de cuánto tiempo pasara hasta que un incidente,

La Operación del Servicio comprende los siguientes procesos:

- **Gestión de Eventos:** responsable de gestionar todos los eventos y su ciclo de vida.

[18]Cualquier componente del servicio que debe ser gestionado para entregar el servicio de TI. Este puede ser hardware, software, documentación o un servicio.

- **Gestión de Incidentes:** responsable de la gestión de todas las incidencias que disminuyan la calidad del servicio y restaurar la operación normal del servicio lo más pronto posible minimizando el impacto y garantizando los Acuerdos de Niveles de Servicios acorados.

- **Cumplimiento de Solicitudes:** gestionar el ciclo de vida de todas las solicitudes generadas por los clientes.

- **Gestión de Problemas:** responsable de diagnosticar la causa raíz de los incidentes y ofrecer las soluciones de lugar, prevenir los problemas e incidentes, eliminarlos y minimizar el impacto de los que no se pueden prevenir.

- **Gestión de Accesos:** responsable de otorgar acceso a los servicios de TI a los usuarios autorizados y restringir el acceso a los no autorizados.

5.6.5. Mejoramiento Continuo del Servicio

La mejora continua es la quinta y última fase del ciclo de vida del servicio. Esta tiene como identificado identificar las mejoras que se deben de realizar en el servicio con el fin de alinear estos con las siempre cambiantes necesidades de negocio.

De acuerdo con Pink Elephant (2013), los objetivos más importantes esta fase son:

- ✓ Recomendar mejoras en cada etapa del ciclo de vida.
- ✓ Revisión y análisis de los logros de nivel de servicio.
- ✓ Mejora la calidad del servicio de TI, la eficiencia y efectividad de los procesos.
- ✓ Mejora la efectividad de costos sin sacrificar la satisfacción del cliente.
- ✓ Garantizar la utilización de métodos de gestión de calidad aplicables.
- ✓ Garantizar los objetivos y las mediciones claras del proceso.
- ✓ Comprender las métricas como deben ser los resultados positivos.

Todas las actividades y procesos involucrados dentro de los servicios de TI deben de ser monitoreados y medidos para poder identificar mejoras en ellos.

La Mejora Continua del Servicio sugiere establecer una línea base para los servicios. Estos es evaluar el estado actual del servicio o proceso para determinar si debe de ser mejorado.

También sugiere crear un Registro CSI (Continual Service Improvement) que es una lista bien definida que proporciona una visión clara y coherente de cuáles son las oportunidades de mejora. El registro debe de ser categorizado e incluir información sobre el tamaño de la iniciativa, cantidad de tiempo que tomara, nivel de prioridad y beneficios potenciales.

Las tomas de decisiones de la Mejora Continua del Servicio siempre deben de ir de acuerdo a las metas de negocio y este último siempre debe de participar en el proceso.

Según Pink Elephant (2013) el enfoque de Mejoramiento Continuo del Servicio incluye preguntas clave para garantizar que tanto el negocio como TI sean considerados. Estas preguntas son:

- ¿Cuál es la visión?
- ¿Dónde estamos ahora?
- ¿Dónde queremos llegar?

- ¿Cómo llegamos ahí?
- ¿Llegamos ahí?
- ¿Cómo hacemos que el ímpetu continúe?

5.6.6. Mejora Continua en Siete Pasos

El proceso de mejora en siete pasos es uno de los procesos más importantes del Proceso de Mejoramiento Continuo. El proceso debe de ser aplicado a todo el ciclo de vida del servicio y los elementos involucrados en el, es decir, procesos, actividades, tareas, etc. El proceso de mejora continua se hace aplicando el Ciclo Deming[19]. Los pasos son los siguientes:

1. **Identificar la estrategia para la mejora:** Aquí se tiene que identificar cual es la estrategia y visión global de TI basada en las necesidades del negocio para así identificar que se debe de mejorar.

2. **Definir que se medirá:** En este paso se identifica aquello que se va a medir tomando en cuenta la situación actual del servicio y las métricas.

3. **Obtener los datos:** Una vez que se haya definido que es lo que se va a medir y la estrategia de mejora, entonces se hace la recopilación de datos. Estos pueden provenir de diferentes fuentes como informes, reportes, etc.

[19] Ver sección 4.9.3

4. **Procesar los datos:** En este paso se procesan los datos recopilados y se convierten en información útil para su posterior análisis.

5. **Analizar la información y datos:** Consiste en el análisis de los datos recopilados para convertirla en "conocimiento" y poder dar respuestas a preguntas sobre el impacto del negocio. En este paso se comprueba que se están cumpliendo los Acuerdos de Niveles de Servicio y que se están cumpliendo los objetivos del servicio de acuerdo a las necesidades del negocio.

6. **Presentación y uso de la información:** Luego de que los datos han sido analizados estos son presentados a negocio para así dar a conocer la iniciativa de mejora. Estos son presentados mediante informes.

7. **Implementar las mejoras:** Aquí es donde se hace la implementación de la mejora basada en la información recopilada de los pasos anteriores.

6. CAPITULO VI – GESTION DE LA CONTINUIDAD DE SERVICIOS DE TI (ITSCM)

6.1. Antecedentes

Dentro de las investigaciones que se realizaron en la empresa YP Directories se pudo determinar que la empresa funciona de una forma reactiva a los problemas relacionados con TI. Si bien cuentan con políticas de seguridad y gestión de riesgo, no cuentan con un plan de continuidad de servicios de TI que permita la continuidad de las operaciones en caso de interrupciones severas.

Y es que según A.Abreu, Jose (2014), de acuerdo a las informaciones disponibles y encuestas realizadas el 80% de las empresas nacionales no cuenta con un sistema implementado y funcional de Continuidad de Negocios. También establece que aproximadamente el 5% de las empresas afectadas por un evento critico se recuperan satisfactoriamente luego de su ocurrencia por lo que la adopción del BCMS (Sistema de Gestión de Continuidad de Negocio) debe ser seriamente considerado como parte de la planificación de los objetivos empresariales a largo plazo.

6.2. Gestión de la Continuidad de Negocio (BCM)

Según Watters (2014), la Gestión de la Continuidad de Negocio (o Business Continuity Management – BCM por sus siglas en ingles), existe para evitar interrupciones que puedan conllevar pérdidas significativas o un fracaso en el proceso de alcanzar los objetivos organizacionales.

El BCM está definido bajo el estándar ISO/PAS 22399 y sirve para desarrollar planes que permitan la recuperación o continuidad de las operaciones o servicios críticos de la organización de forma parcial o completa ante una interrupción de servicio en un tiempo determinado.

Según Watters (2014) el Ciclo de vida de un BCM es el Siguiente:

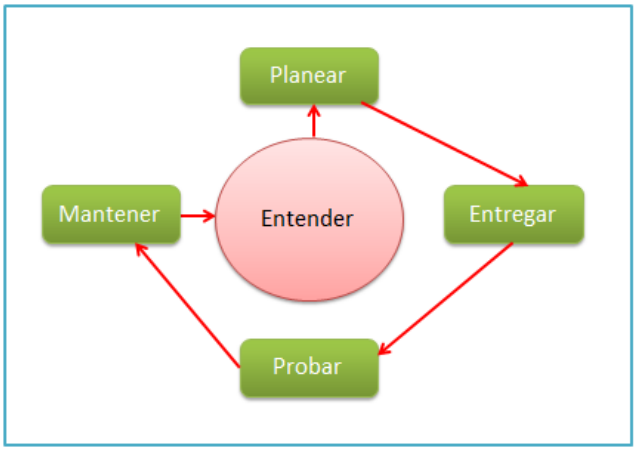

Figura 31. Ciclo de Vida del Proceso de Continuidad de Negocio

En la figura 31 se presenta el ciclo de vida del Proceso de Continuidad de Negocio. Lo primero que hay que hacer es entender cuáles son los procesos críticos del negocio, luego planear como se van a introducir, luego entregar las soluciones de lugar, hacer las pruebas de esas soluciones y darle mantenimiento.

Un BCM abarca otros planes tales como el Plan de Continuidad de Negocio (BCP), que es donde se prepara todo para enfrentar un desastre, Continuidad de Servicio de TI, que se enfoca en las continuidad de las soluciones tecnológicas que soportan al negocio y la Gestión de Crisis que trata aquellos eventos de mayor magnitud que pueden causar daños severos a la organización en general incluyendo infraestructura física, personas, etc.

Al implementar un Plan de Continuidad se debe tener lo siguiente:

- Políticas claras con los objetivos de plan de continuidad alineados al negocio.
- Procesos definidos que expliquen como la organización lograra la continuidad del negocio.
- Temples utilizados por las personas interesadas para monitorear las actividades.
- Un programa donde se maneje todo lo relacionado con los procesos, la concientización al personal, los checklists de las actividades, se identifiquen problemas y se escalen de ser necesario.
- Roles y funciones bien definidas hacia el personal.
- Se debe de entender que es crítico y que no lo es, que tiene prioridad alta o baja.

Un BCM debe de responder ante diferentes escenarios. Son muchas las posibles causas o riesgos para un negocio pero según Watters (2014), estos escenarios se pueden clasificar en los siguientes cinco:

- **Perdida de tecnología:** cuando la tecnología utilizada no funciona.
- **Perdida del edificio:** cuando se destruye el edificio.
- **Denegación de acceso al personal:** cuando el personal no puede acceder a su lugar de trabajo.

- **Perdida de personal:** cuando personas claves no pueden ir al trabajo.
- **Perdida de proveedores:** cuando un proveedor no puede ofrecer servicios críticos o productos importantes al negocio.

6.2.1. Roles del BCM

Un BCM cuenta con personas que tienen distintas responsabilidades y llevan a cabo diferentes actividades con el fin de que el plan funcione. La siguiente tabla describe los principales roles de un BCM según Watters (2014)[20].

En la tabla se describen los objetivos de cada rol, sus tareas principales y sus entregables.

ROL	OBJETIVOS	TAREAS	ENTREGABLES
Gerente de Continuidad de Negocio	Asegurar que el plan de continuidad esté en su lugar y asegurar que la empresa tenga la habilidad válida para recuperarse	• Establecer políticas. • Crear e implementar el proceso del BCM. • Concientizar al personal en sus tareas. • Asegurar las pruebas de los planes y el BCM. • Reportar riesgos y problemas. • Evaluar la madurez y calidad del BCM.	• Políticas • Proceso BCM. • Entrenamientos. • Ejercicios. • Pruebas. • Reportes de gestión.
Tecnología de la Información (TI)	Entregar un plan de Recuperación de Desastres para los sistemas.	• Diseñar las soluciones del plan de Recuperación de Desastre (DR). • Construir e implementar soluciones. • Probar el plan de Recuperación de Desastres.	• Capacidad de Recuperación de Desastres de los sistemas. • Documentación de la Recuperación de Desastres. • Pruebas de la Recuperación de Desastres.

[20] La tabla es un resumen de lo descrito en el libro.

Negocio	Identificar las necesidades del negocio, preparar los planes y mantenerlos, tomar entrenamientos y participar en las pruebas.	• Llevar a cabo el Análisis de Impacto al Negocio (BIA). • Llevar a cabo el Plan de Continuidad de Negocio (BCP). • Llevar a cabo los programas de concientización de las actividades y educar al personal. • Crear la "llamada en Cascada" • Gestionar y mantener los planes en general. • Realizar las pruebas de lugar.	• BIA. • BCP. • Información sobre "llamada en casada" • Reseñas de los planes. • Pruebas (WAR y DR).
Gerente Senior	Aprobar la política del BCM, evaluar los posibles riesgos o problemas y asegurar buena respuesta del plan	• Aprobar las políticas y proceso del plan de continuidad. • Revisar la capacidad. • Monitorear problemas, riesgos y acciones.	• Aprobación de política. • Aprobación del proceso
Auditor	Asegurar que el plan de Continuidad de Negocio cumpla con las necesidades de negocio y las partes externas interesadas.	• Auditar la política, procesos, programa de BCM en proceso para asegurar que cumplan con las necesidades del negocio. • Auditar el BCM para asegurar que cumpla con lo establecido en la política y asegurar que está siendo eficiente. • Evaluar la madurez del programa contra las mejores prácticas y los estándares.	• Reporte de Auditoria.

Tabla 3. Roles del BCM

6.2.2. Partes Esenciales de la Gestión de Continuidad de Negocio

Todo plan de un BCM debe de contar con las siguientes partes fundamentales:

- **Equipo de Gestión de Crisis:** es el grupo de personas claves que lidera la organización en momentos de crisis. Los grupos o personas que componen este equipo son generalmente:
    - **TI:** para manejar cualquier problema relación con TI.

- **Recursos Humanos:** para manejar cualquier problema relacionado con el personal.
- **Instalaciones:** que es la persona relacionada con los problemas del edificio y sus servicios.
- **Comunicaciones:** para manejar la comunicación a los clientes, usuarios, suplidores, etc.
- **Director Ejecutivo:** generalmente quien maneja la organización en momentos de crisis.

- **"Llamada en Cascada" o Call Cascade:** es una lista con los nombres, teléfonos y responsabilidades de las partes interesadas claves utilizada para facilitar la comunicación en caso de que ocurra alguna interrupción significativa.

- **Plan de Continuidad de Negocio (BCP):** Es el plan general a poner en marcha, este puede incluir otros planes como son planes de comunicación, planes de educación, concientización al personal, entrenamientos, entre otro.

- **Plan de Recuperación de Desastre (DRP):** es el plan desarrollado por TI para la recuperación de las soluciones tecnológicas. Este puede estar incluido en el BCP.

Watters (2014), también habla de otros planes y factores a ser considerados dentro del BCM como son:

- **Plan de Recursos Humanos**: que comprende la parte financiera y el cómo la empresa seguirá manejándose después de los desastres, ejemplo, como seguirá pagando a los empleados.

- **Plan de TI:** en este plan, TI se encargara de formar el equipo de recuperación y definir cómo se va a actuar ante la situación.

6.3. Plan de Continuidad de Negocio (BCP)

El BCP está definido bajo el estándar ISO 22301. Un BCP detalla todo lo que se necesita hacer para recuperarse de un desastre y de esta manera dar continuidad a los servicios y operaciones del negocio.

Una vez hecha la evaluación de riesgo y de haber identificado lo que es crítico para el negocio, aquellos sistemas y servicios que deben estar siempre arriba y haber definido que tan rápido se deben de hacer las cosas, entonces es necesario poner todo eso en un plan, este plan es el Plan de Continuidad de Negocio (Business Continuity Plan o BCP por sus siglas en inglés).

6.3.1. Partes esenciales de un Plan de Continuidad de Negocio

Según Watters (2014), un BCP debe de contener los siguientes elementos:

- **Contactos Clave:** todo contacto que sea critico dentro de un BCP, incluyendo su información de contacto.
- **Proceso de escalamiento:** son los diferentes escenarios de un evento que muestran como este será detectado y escalado.
- **Lista de Verificación (Checklist) del BCP:** es una lista que muestra lo que hay que hacer inmediatamente ocurra el incidente.
- **Punto de reunión:** indica hacia donde ir si el área de trabajo es evacuada o no está disponible.
- **Plan de acción de prioridad:** define las actividades críticas a hacerse, y quien o quienes realizará estas actividades, luego del desastre haber sido declarado.
- **Detalles del Call Cascade:** es una lista de contactos que abarca todo el personal involucrado en el plan y que describe quien contacta a quien.
- **Detalles sobre lugares de contingencia:** maneja detalles tales como el modo de transporte hacia el lugar de contingencia, informaciones como de hoteles y restaurantes.

6.4. Gestión de Continuidad de Servicios de TI: Alcance, Objetivos y Propósito

El propósito general de la ITSCM es dar soporte en lo general al proceso de Gestión de Continuidad de Negocio (BCM) y asegurarse de gestionar los riesgos que puedan afectar a los servicios de TI de modo que se pueda cumplir con los SLAs o Acuerdos de Niveles de Servicios.

Según OSIATIS S.A, *es importante diferenciar entre desastres "de toda la vida", tales como incendios, inundaciones, etcétera, y desastres "puramente informáticos", tales como los producidos por ataques distribuidos de denegación de servicio (DDOS), virus informáticos, etcétera. Aunque es responsabilidad de la ITSCM prever los riesgos asociados en ambos casos y restaurar el servicio TI con prontitud, es evidente que recae sobre la ITSCM una responsabilidad especial en el último caso pues:*

- *Sólo afectan directamente a los servicios TI pero paralizan a toda la organización.*
- *Son más previsibles y más habituales.*
- *La percepción del cliente es diferente: los desastres naturales son más asumibles y no se asocian a actitudes negligentes, aunque esto no sea siempre cierto.*

Lo primero que se debe hacer para la implementación de la ITSCM es definir una política que comprenda cuáles serán sus objetivos, su alcance y el grado de compromiso de TI. Según Pink Elephant (2013), *los objetivos, alcance y requerimientos de Gestión de la Continuidad de Servicios de TI son establecidos a través de la Gestión de la Continuidad del Negocio (BCM),* que es el proceso encargado de gestionar los riesgos que afecta seriamente al negocio.

Los objetivos de la ITSCM son:

- *Generar y mantener un conjunto de planes de continuidad del servicio de TI que soporten los planes generales de continuidad del negocio de la organización.*
- *Completar con regularidad ejercicios de BIA (Business Impact Analysis) para garantizar que todos los planes de continuidad sean mantenidos en línea con los impactos y requerimientos cambiantes del negocio.*
- *Llevar a cabo con regularidad ejercicios de evaluación y gestión de riesgo para gestionar los servicios de TI dentro de un nivel acordado de riesgos de negocio en conjunto con los procesos de negocio, de la gestión de la disponibilidad y de gestión de seguridad de la información.*
- *Dar asesoría y orientación a otras áreas del negocio y a TI sobre todos los asuntos relaciones con continuidad.*

- *Garantizar que los mecanismos apropiados de continuidad sean establecidos para cumplir o exceder los objetivos de continuidad del negocio acordados.*
- *Evaluar el impacto de todos los cambios en los planes de continuidad del servicio de TI así como en los métodos de soporte y procedimientos.*
- *Garantizar que se implementen medidas proactivas para mejorar la disponibilidad de los servicios cuando sea justificable en costo hacerlo.*
- *Negociar y acordar contratos con los proveedores para la provisión de la capacidad de recuperación necesaria para soportar todos los planes de continuidad en forma conjunta con el proceso de gestión de proveedores.*

El alcance de la ITSCM estará definido por la organización y solo contemplará aquello que sea considerado como "desastre" y que pueda tener un impacto significativo para el negocio. Todo lo demás será considerado como incidente. El alcance debe de contemplar los siguientes puntos:

- Los recursos disponibles.
- Los planes de continuidad de negocio.
- Los servicios críticos y estratégicos de TI.
- El historial de las interrupciones críticas de los servicios de TI.
- Las expectativas del negocio.

6.5. Ciclo de Vida de la Gestión de Continuidad de Servicios de TI

El ciclo de vida de la ITSCM consta de cuatro etapas: Iniciación, Requerimientos y Estrategia, Implementación y Gestión Operativa.

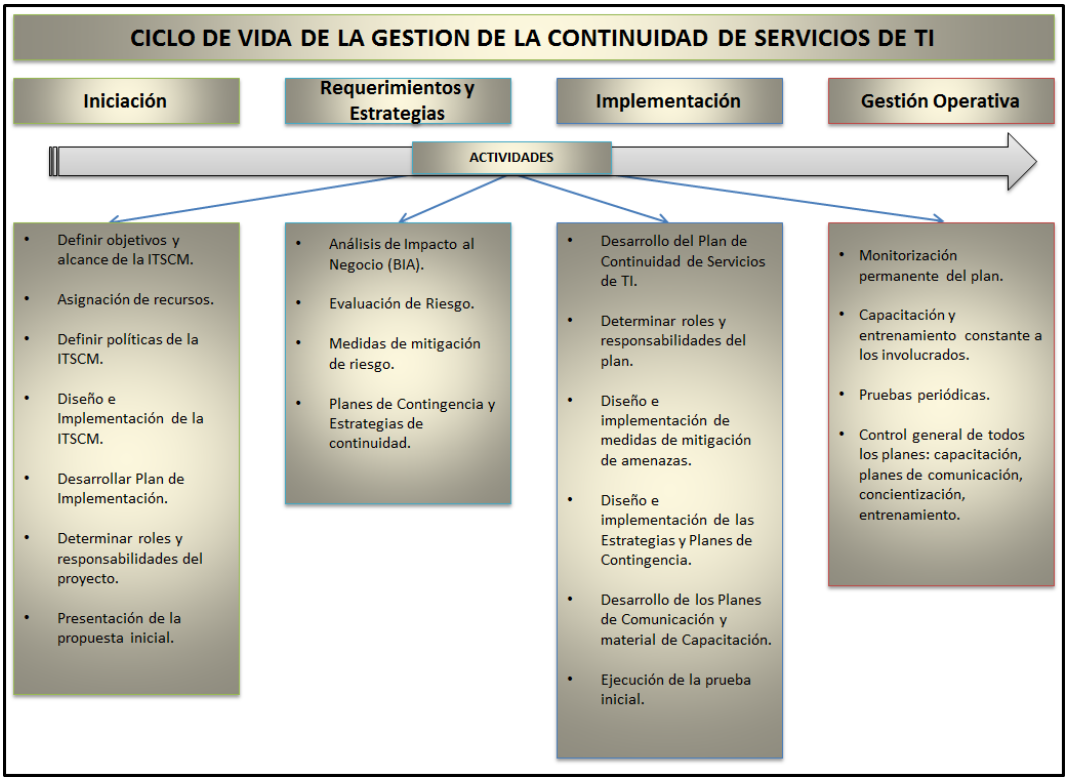

Figura 32. Etapas y actividades del Ciclo de Vida de la ITSCM. Fuente: Propia

- **Iniciación:** fase inicial del ciclo de vida donde se define la iniciativa del plan, las políticas, se asignan recursos y se definen los objetivos y el alcance.
- **Requerimientos y Estrategias:** en esta etapa se establecen los requerimientos del plan de continuidad y se establecen las medidas necesarias para satisfacer dichos requerimientos.

- **Implementación:** en esta etapa se implementan los planes y estrategias definidos en las etapas anteriores.
- **Gestión Operativa:** en esta etapa se le da seguimiento constante al Plan de Continuidad de los Servicios de TI.

6.6. Requisitos de la Gestión de Continuidad de Servicios de TI (ITSCM)

La ITSCM tiene dos requisitos fundamentales para su implementación dentro de las organizaciones, estos son: el Análisis de Impacto del Negocio (Business Impact Analysis o BIA) y la Evaluación de Riesgo.

6.6.1. Análisis de Impacto del Negocio (BIA)

El BIA es un tipo de análisis que tiene como propósito cuantificar el impacto que causaría la pérdida de un servicio a la empresa. El BIA identifica cuales son los servicios críticos del negocio necesarios para que las operaciones de negocio continúen.

El BIA toma en consideración factores tales como:

- ✓ Las pérdidas de ingreso que se podrían tener al perder un servicio.
- ✓ Reputación de la organización.
- ✓ Pérdida de rentabilidad del negocio.
- ✓ Tiempo de recuperación con niveles mínimos de personal, instalaciones y servicios.
- ✓ Tiempo para recuperación completa de recuperación de las operaciones, incluyendo sus servicios, personal de soporte y las instalaciones.
- ✓ Priorización de los servicios de TI.
- ✓ Compromisos adquiridos en los Acuerdos de Niveles de Servicios.

Dependiendo de los factores anteriormente mencionados se establecen acciones de preventivas y de recuperación tomando en cuenta sus costos.

6.6.2. Completando el BIA

Watters (2014) recomienda hacer un cuestionario acerca de los servicios con el fin de determinar qué es crítico y a partir de ahí establecer los requerimientos para el Plan de Continuidad. El cuestionario puede incluir preguntas sobre asuntos legales, sobre el cliente, financieras y sobre la reputación del negocio.

Watters (2014) propone el siguiente ciclo para realizar el BIA:

Figura 33. Ciclo de Vida del BIA

La imagen muestra el ciclo de vida del Análisis de Impacto al Negocio recomendado por Watter (2014). A continuación se explica en que consiste cada fase:

1. **Estructura del BIA:** significa elaborar diferentes cuestionarios en referencia a los distintos tipos de servicios que revelen información relevante tales como, impacto financiero que puede tener si el servicio está abajo.

2. **Identificar los Stakeholders:** esto quiere decir identificar quien o quienes llenaran los cuestionarios del BIA. Generalmente esto lo hace el gerente del área y lo aprueba el Gerente Senior. Sin embargo, los gerentes y usuarios de otros departamentos pueden jugar un papel importante en el desarrollo del cuestionario.

En YP Directories, los stakehodlers son: usuarios, gerentes de departamentos y personal de TI.

3. **Arreglar las reuniones:** en esta fase de organizan las reuniones de lugar con las partes interesadas, aquellas que van a completar los cuestionarios del BIA.

4. **Entrevista del BIA:** es la parte donde se realizan las preguntas de lugar a las partes interesadas.

5. **Analizar Respuestas:** se analizan las respuestas obtenidas.

6. **Revisar Reunión:** en esta parte se muestran los resultados al gerente del área para mostrarle los resultados del BIA y saber si existe alguna pregunta en referencia a la información recaudada para así aclarar dudas y hacer modificaciones si es necesario.

7. **Aprobar BIA:** Una vez revisados los resultados, estos son presentados al gerente encardo de dar aprobación y que este revise si los requerimientos de continuidad están correctos.

8. **Análisis Final:** se realiza un análisis final para consolidar todos los cuestionarios y verificar si hay requerimientos que se repiten y corregirlos.

9. **BIA final:** se analiza el documento con la información final, que tiene como resultado los requerimientos necesarios para afrontar un desastre.

6.6.3. Evaluación de Riesgo

La Evaluación de Riesgo se refiere a evaluar y enumerar los distintos factores de riesgo para reducir los incidentes potenciales y garantizar una disponibilidad mínima ante cualquier desastre o interrupción no desea que pueda ocurrir.

Según OSIATIS S.A, para lograr lo anteriormente dicho la ITSCM debe de:

- Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración (CIs) involucrados en la prestación de cada servicio, especialmente los servicios TI críticos y estratégicos.
- Analizar las posibles amenazas y estimar su probabilidad.

- Detectar los puntos más vulnerables de la infraestructura TI.

6.6.4. Estrategias de Evaluación de Riesgo

Las estrategias de gestión de riesgo pueden ser de dos tipos: preventivas y de recuperación.

- **Estrategias Preventivas:** son acciones estratégicas que se toman antes de que ocurra el desastre o interrupción del servicio. Requieren un análisis de evaluación de riesgo, amenazas y vulnerabilidades y pueden cubrir tanto aspectos generales tales como incendios, inundaciones, terremotos y otros tipos de desastres naturales; como también aspectos específicos tales como la falla del sistema de backup o la caída de un enlace de red.
- **Estrategias de Recuperación:** son acciones estratégicas que se ejecutan luego de que ocurre el desastre y su objetivo es lograr la recuperación de los servicios luego de la interrupción. Dentro de las opciones de recuperación se encuentran: Cold Standby, Warm Standby y Hot Standy[21].

[21] Ver sección 6.8: Recuperación de Desastres para más detalles sobre estas y otras opciones de recuperación.

6.7. El Tiempo

El tiempo es uno de los factores más importantes cuando se habla de continuidad de servicios. Antes cualquier interrupción de los servicios, es necesario saber cuánto tiempo se está dispuesto a durar sin el servicio, o que tanto tiempo las operaciones se pueden sostener trabajando a una capacidad reducida, o que tiempo se puede estar sin hacer nada frente a la interrupción.

6.7.1. Objetivo de Punto de Recuperación (RPO)

El RPO indica que cantidad de perdida de información se puede tolerar ante un desastre.

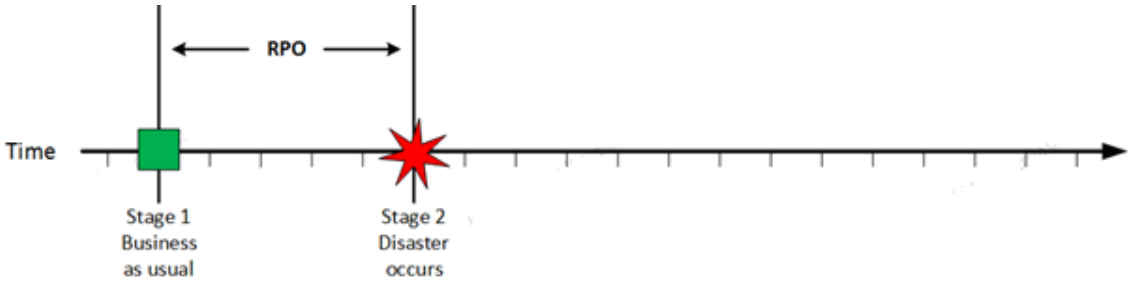

Figura 34. Imagen representativa de un RPO[22]

[22] Fuente: http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

En la figura 34, el “Escenario 1” representa al negocio con sus operaciones normales y el “Escenario 2” representa la ocurrencia de un desastre. En el tramo de tiempo transcurrido desde el Escenario 1 al Escenario 2 se define qué cantidad de tiempo se está dispuesto a tolerar en cuanto a perdida de datos se refiere, este puede ir desde 0 hasta la cantidad de horas tolerables.

6.7.2. Objetivo de Tiempo de Recuperación (RTO)

El RTO es la etapa de la recuperación de los datos. Define el tiempo límite dentro del cual se recuperan los datos luego de la presencia de un desastre.

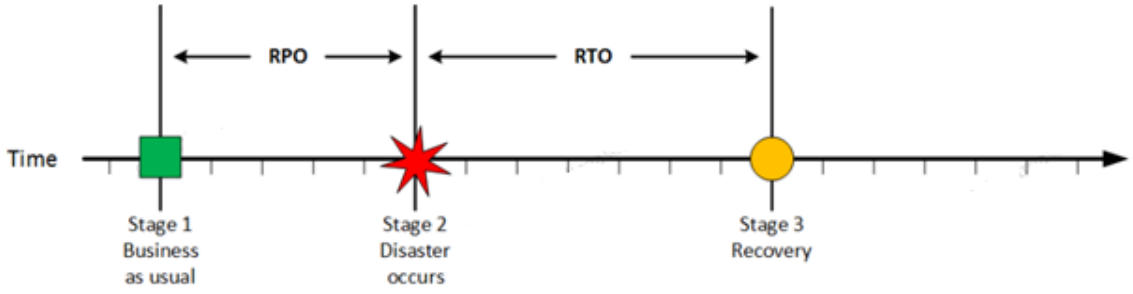

Figura 35. Imagen representativa de un RTO[23]

[23] Fuente: http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

La figura 35 muestra que luego de que ocurre el desastre los datos o servicios se deben de recuperar. El RTO establece este tiempo de recuperación necesario para poner en funcionamiento los servicios críticos.

6.7.3. Tiempo de Trabajo de Recuperación (WRT)

El WRT es el tiempo máximo tolerable y necesario para verificar la integridad y funcionalidad de los servicios críticos una vez que haya sido otra vez.

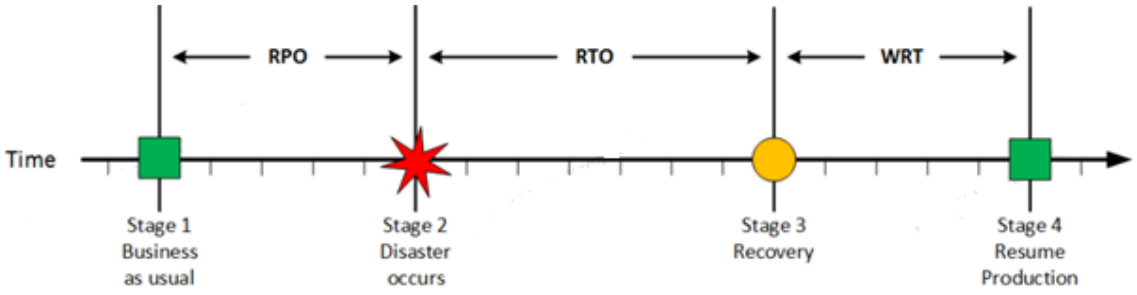

Figura 36. Imagen representativa de un WRT[24]

[24] Fuente: http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

6.7.4. Tiempo Máximo de Inactividad Tolerable (MTD)

Es el tiempo máximo tolerable que un servicio crítico o algún proceso puede estar inactivo sin causar consecuencias inaceptables. El MTD es la suma del RTO y el WRT.

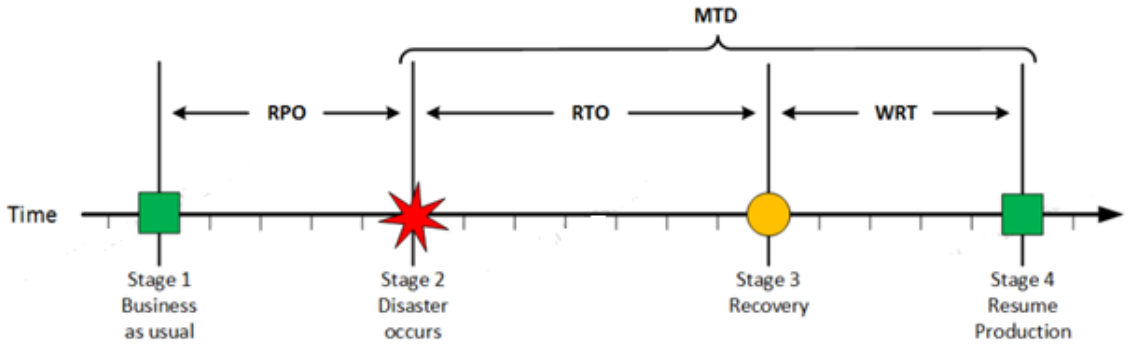

Figura 37. Imagen representativa de un MTD[25]

6.8. Plan Recuperación de Desastres de TI (ITDRP)

Según Watters (2014), la "Recuperación de Desastres de TI, o DR, es la parte del plan de continuidad que tiene que ver con proteger y rescatar los servicios críticos de TI)" (p. 57).

[25] Fuente: http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Es necesario aclarar que la Gestión de Continuidad de Negocio o BCM no es lo mismo que un Plan de Recuperación de Desastres. Este último solo trata la recuperación de los servicios de TI, mientras que el primero es algo más complejo, pues contiene dentro de él otros planes tales como el BCP, Gestión de Crisis e incluso el mismo ITDRP.

6.9. Soluciones de Recuperación de Desastres

Las soluciones de recuperación de desastres pueden ser diversas y depende mucho de los requerimientos del negocio en cuanto a los tiempos de recuperación y están restringidas ya sea por presupuesto, localidad o el que tanto esta la compañía dispuesta a lograr. Dentro de las soluciones de recuperación se pueden mencionar las siguientes:

6.9.1. Hot Standby

Esta solución es básicamente el ambiente de producción replicado en un lugar alternativo. Siempre está listo para el reemplazo inmediato de producción en caso de una interrupción severa. Esta solución replica el hardware, software y la data, es tolerante a fallo y el tiempo de recuperación es extremadamente rápido.

Dentro de sus ventajas se pueden mencionar que es sumamente confiable, la pérdida de datos es mínima, siempre está activa, reducción de riesgo debido a que no se

requieren intercesiones manuales y que es una arquitectura ya conocida y no se necesitan muchos pasos para la recuperación.

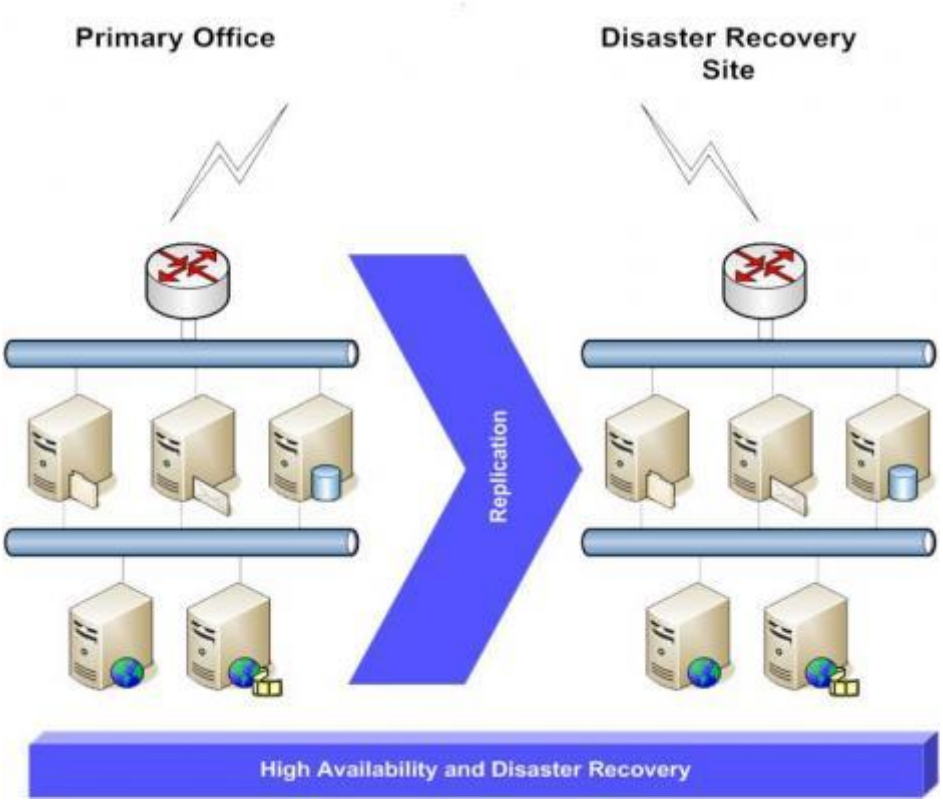

Figura 38. Arquitectura Hot Recovery

Por otro lado, su desventaja más significativa es el costo debido a su arquitectura que incluye desde la infraestructura hasta el hardware con las mismas capacidades que los del entorno de producción. Esta opción es recomendable solo si el Down time de las operaciones afecta de forma inmediata las finanzas del negocio y aspectos comerciales.

6.9.2. Warm Standby

Esta solución funciona casi de igual manera que la Hot Standby con la diferencia de que el hardware no está activo ni los datos de las aplicaciones están actualizados. Es necesario que los servicios se inicien desde principio una vez ocurra la interrupción.

Figura 39. Arquitectura Warm Recovery

Requiere intervención manual por lo tanto el riesgo en general aumenta. La información se puede almacenar en cintas físicas o virtuales y es una solución que la provee un tercero, lo que hace más difícil su control y la implementación de pruebas.

6.9.3. Cold Recovery

Esta estrategia consiste en contar con un espacio reservado para poder migrar los equipos en caso de algún desastre. Este espacio debe de contar con la red de

comunicación, energía eléctrica y climatización para los equipos del data center. Para esta solución generalmente se contratan los servicios de otro proveedor el cual proveerá el espacio de trabajo. Es la opción más económica en comparación con el Warm Recovery y el Hot Recovery.

Figura 40. Arquitectura Cold Recovery

Esta solución requiere mucha intervención manual de parte de la organización debido a que se deben coordinar las acciones de recuperación a través de un número de departamentos y personas. Existe también riesgo de pérdida de datos en el proceso y más si la información a mover está en cintas de backup, pues estas pueden dañarse en el proceso.

6.9.4. Recuperación Móvil

Esta estrategia puede cubrir un gran número de soluciones. En vez de utilizar las operaciones de un data center, que es la forma tradicional, se pueden

utilizar opciones como por ejemplo el alquiler de trailers. Estos se llevan a la localidad y se habilitan para continuar las operaciones normales.

7. CAPITULO VII – MARCO APLICATIVO

7.1. Fundamentos de la Propuesta

Debido a la gran importancia que representan los servicios de la Tecnología de Información para las organizaciones y sus procesos de negocio, es de suma importancia que estos servicios permanezcan siempre en funcionamiento y que, en caso de que ocurriese alguna interrupción en estos que pudiese tener un impacto negativo en la empresa, dichos servicios sean recuperados lo más pronto posible.

YP Directories es una empresa americana que tiene como misión ser líder en soluciones de marketing para sus clientes. Esta empresa maneja alrededor de 700 directorios telefónicos en diferentes estados de los Estados Unidos e imprimiré unos 58 directorios mensualmente. Cuenta con aproximadamente 250 empleados y obtiene ganancias anuales de $150, 000,000.00 de dólares. YP Directories es una organización que depende mucho de su infraestructura tecnológica para poder entregar los resultados esperados a sus clientes. La indisponibilidad prolongada de los servicios de TI sería fatal para esta compañía y es por eso que se necesita contar con planes de contingencia y alternativas de recuperación de desastres para estos servicios que forman parte esencial del negocio.

La propuesta busca identificar oportunidades de mejoras en la infraestructura utilizada para dar los servicios de TI que apoyan los procesos de negocio y la creación de

un plan de continuidad estos servicios, esto incluye dar alternativas para recuperación de desastres y continuidad de servicios.

7.2. Presentación de la Propuesta

La siguiente propuesta tiene como objetivo principal ofrecer una respuesta efectiva frente a las amenazas asociadas a los servicios de TI que dan soporte a los procesos de negocio de la empresa YP Directories. La propuesta hace su enfoque en el ciclo de vida del proceso de ITIL v3, Gestión de Continuidad de Servicios de TI (ITSCM).

Esta primera etapa de la propuesta solo busca identificar aquellos servicios críticos de TI que soportan al negocio y evaluar sus riesgos para definir estrategias de recuperación efectivas que permitan la continuidad de estos servicios.

Para identificar los servicios de TI críticos que dan soporte a los proceso de negocios, se realizará un Análisis de Impacto al Negocio (BIA) y luego se procederá a realizar una Evaluación de Riesgo para identificar los riesgos asociados a los servicios y proveer alternativas y/o estrategias de recuperación.

En una segunda etapa se realizará la implementación de dichas estrategias por medio de la creación de planes de continuidad y los procedimientos que conllevan, así como las pruebas necesarias para probar las estrategias propuestas. Luego, es responsabilidad de la empresa capacitar al personal necesario en sus roles para poner en marcha el proceso, realizar las auditorias de lugar y las pruebas de lugar necearías.

La implementación de esta propuesta permitirá a la empresa continuar con sus operaciones críticas en caso de que llegase a ocurrir un evento que impacte negativamente a la organización.

7.3. Análisis de la Información

Con el objetivo de identificar cuáles son los servicios críticos de TI que dan soporte a los procesos de negocios y sus riesgos asociados, para poder ofrecer establecer estrategias de recuperación y/o alternativas de mejoras para estos, se realizó un Análisis de Impacto al Negocio (BIA) y una Evaluación de Riesgo (Risk Assessment).

7.4. Análisis de Impacto al Negocio (BIA) para YP Directories

La función principal de un BIA poder identificar los servicios críticos de la una organización, es decir, esos servicios de los cuales la organización depende para continuar con sus operaciones. En este caso, se deben identificar los servicios de TI críticos para los procesos de negocio de la organización.

Para realizar el análisis, primero se identificaron cuáles servicios ofrece el departamento de TI de YP Directories. El catálogo de servicios es el siguiente:

CATALOGO DE SERVICIOS DE TI YP DIRECTORIES	
Servicio	**Modalidad**
Servicio de Telecomunicaciones	Acceso a Internet
	Acceso a Intranet
	Telefonía
	Correo Electrénico
Servicio de Infraestructura Tecnológica	Backup & Restore
	Gestión de servidores (acceso, carpetas compartidas, almacenamiento)
	Red LAN
	Adecuación del CPD
Desarrollo y Soporte de Aplicaciones	Desarrollo de Aplicaciones
	Soporte a Aplicaciones
Servicio Soporte Técnico a Escritorio	Diagnostico y/o Reparación de PCs y perifericos (scanners, printers, faxes, etc)
	Instalación de Aplicaciones
	Asesoria Informática

Tabla 4. Catálogo de Servicios de TI de YP Directories

Luego se procedió a determinar cuáles eran los procesos de negocio para así poder identificar los sistemas que dan soporte a esos procesos y así poder definir su grado importancia.

Para esto se entrevistó a los gerentes encargados de las diferentes áreas (producción y auditoria) y mediante un cuestionario se obtuvieron los RTOs y RPOs de cada proceso de negocio crítico, así como el monto que tendría que pagar la empresa si un directorio no imprime en la fecha estipulada por la telefónica. Esta información está representada en la tabla 5.

ID Proceso	Proceso de Negocio	RTO Negocio	RPO Negocio	Costos Adicionales	Cantidad de Dependientes	Proceso ID dependiente	Sistema de TI
1	Digitación de tasas del Mercado	3 días	14 días	$ 100,000.00	9	1 al 9	CORE System
2	Preparación de Mercado	3 días	14 días	$ 100,000.00	1	11	Sistema de Nómina
3	Digitación de Ordenes de Servicio	4 días	1 día	$ 100,000.00	3	7,8,9	Sistema Gestor de Reportes
4	Manejo y Digitación de Contratos	4 días	1 día	$ 100,000.00	1	11	Sistema Gestión de Empleados
5	Auditoría de anuncios	7 días	7 días	$ 100,000.00	3	3,4,6	Sistema de Consultas a la TELCO
6	Auditoría General	5 dias	2 dias	$ 100,000.00	8	3,4,5,6,7,8,9,10	Sistema de Programa Maestro
7	Diseño y envío de pruebas	7 dias	7 días	$ 100,000.00	2	9,10	Sistema de Suministro de Correcciones
8	Servicios Creativos de Directorio	7 días	7 días	$ 100,000.00	7	7	Sistema de Prueba Electrónica
9	Cierre de Libro	4 dias	5 horas	$ 100,000.00	10	10	Sistema de Paginación de directorios
10	Paginación	4 Horas	4 Horas	$ 100,000.00	1	1	Sistema Generador Y Actualizador de precios del mercado
11	RR.HH	30 días	7 días	$ -	2	7,8	Sistema de Gráficos
					1	11	Sistema de Reembolsos
					1	11	Sistema de pago a Suplidores
					2	9,10	Sistema de envio de Directorios a Printer (TAPS)
					11	1 al 11	Servicio de Telefonía
					11	1 al 11	Servicio de Correo Electrónico
					11	1 al 11	Almacenamiento compartido

Tabla 5. Procesos de negocio y sus sistemas de soporte. Fuente: Propia.

Leyenda

- **ID Proceso** - Número utilizado para identifica al proceso de negocio.
- **Proceso de Negocio** - Proceso clave de negocio.
- **RTO Negocio** - Tiempo de Recuperación Objetivo de proceso del negocio.
- **RPO Negocio** - Objetivo de punto de recuperación del proceso de negocio.
- **Costos Adicionales:** Perdida monetaria para la empresa si los servicios de TI no son recuperados en el RTO establecido por negocio.
- **Proceso ID dependiente:** IDs de los procesos que dependen del sistema de TI.
- **Sistema de TI:** son los sistemas y/o servicios de TI que dan soporte a los procesos del negocio.

7.4.1. Cálculos de los Tiempos

En base a la información recopilada en la tabla 5, se pudo identificar cuáles eran los tiempos RTO, RPO, WRT Y MDT de los servicios y sistemas de TI.

Para identificar el RTO y RPO de cada servicio y sistema de TI, se tomaron como referencia los RTOs Y RPOs de los procesos de negocio.

El proceso de selección fue en base a las siguientes reglas:

- Si de un sistema o servicio de TI depende un único proceso de negocio, el RTO y RPO de ese sistema o servicio es menor al RTO y RPO de su proceso dependiente.

- Si un sistema o servicio de TI depende de más de un proceso de negocio, se elige el RTO y RPO menor entre todos los procesos y el RTO y RPO del sistema o servicio de TI debe ser menor que el menor de los tiempos de todos los procesos.

- El RTO y RPO de los servicios de los cuales dependen los sistemas y servicios de TI debe ser menor al de su sistema dependiente.

Unidad de Negocio	Servicio de TI	Sub- Servicio	MTD (horas)	WRT	RTO	RPO
TI	Infraestructura y Telecomunicaciones	Gestión de servidores (acceso, carpetas compartidas, almacenamiento)	7	4 horas	3 horas	3 horas
		Correo Electrónico	7	4 horas	3 horas	3 horas
		Acceso a Intranet	6	4 horas	2 horas	2 horas
		Acceso a Internet	6	4 horas	2 horas	2 horas
		Respaldo y Recuperación de información	6	4 horas	2 horas	2 horas
		Telefonía	7	4 horas	3 horas	3 horas
	Aplicaciones (desarrollo y soporte)	CORE System	52	4 horas	2 días	3 horas
		Aplicación Nómina	700	4 horas	29 días	6 días
		Sistema Gestor de Reportes	76	4 horas	3 días	4 Horas
		Sistema Gestión de Empleados	76	4 horas	3 días	23 horas
		Sistema Indexador de Contratos	76	4 horas	3 días	23 horas
		Sistema de Consultas a la TELCO	76	4 horas	3 días	23 horas
		Sistema de Programa Maestro	76	4 horas	3 días	23 horas
		Sistema de Suministro de Correcciones	7	4 horas	3 horas	3 horas
		Sistema de Prueba Electrónica	148	4 horas	6 días	6 días
		Sistema de Paginación de directorios	7	4 horas	3 horas	3 horas
		Sistema Generador Y Actualizador de precios del mercado	52	4 horas	2 días	13 días
		Sistema de Gráficos	148	4 horas	6 días	6 días
		Sistema de Reembolsos	700	4 horas	29 días	6 días
		Sistema de pago a Suplidores	700	4 horas	29 días	6 días
		Sistema de Registro de Auditoria	100	4 horas	4 días	1 día
		Sistema de envio de Directorios a Printer	7	4 horas	3 horas	3 horas
	Servicio de Soporte	Adquisición de productos y servicios de TI	28	4 horas	1 días	10 días
		Selección de Proveedores, productos y servicios de TI	N/A	N/A	N/A	N/A
	Servicio Soporte Técnico a Escritorio	Diagnostico y/o Reparación de PCs y perifericos (scanners, printers, faxes, etc)	N/A	N/A	N/A	N/A
		Instalación de Aplicaciones	N/A	N/A	N/A	N/A
		Asesoria Informática	N/A	N/A	1 mes	N/A

Tabla 6. Tiempos Máximos Toreable de Inactividad y pérdida de datos de los Servicios de TI de YP Directories. Fuente: Propia

Leyenda:

- **Unidad de negocio:** Unidad de negocio.
- **Servicio de TI:** Servicio de TI principal.
- **Sub-servicio de TI:** Sub-servicios o sistemas que componen el servicio de TI.
- **MTD:** Tiempo Máximo de Inactividad
- **RTO:** Tiempo Objetivo de Recuperación
- **RPO:** Punto Objetivo de Recuperación.
- **WRT:** Tiempo de Trabajo de Recuperación.
- **N/A:** No aplica, estos servicios

7.4.2. Criterio de selección para los servicios críticos de TI

Luego de haber identificado los tiempos objetivos asociados a los servicios y sistemas de TI. Se seleccionaron los servicios críticos basado en su MTD. El criterio de selección se presenta en la siguiente tabla.

Criterio de Selección de Servicios Críticos basados en el MTD	
Rango de Horas	**Prioridad**
1 a 99	Alta
100 a 200	Media
201 en adelante	Baja

Tabla 7. Criterio de selección de los Servicios Críticos. Fuente: Propia.

Como se puede ver en la tabla 7, los servicios más críticos serán los que tengan un Tiempo Máximo Tolerable de Inactividad (MTD) de 1 a 99 horas. Estos servicios están resaltados en color amarillo en la tabla 6.

En base a los criterios de evaluación se puede concluir en que la empresa cuenta con 17 servicios de TI críticos, para 63%. Los servicios con prioridad media son seis, para un 22% y los cuatro servicios restantes con un 15% que representan prioridad baja.

7.5. Identificación de Riesgos para YP Directories

La siguiente tabla muestra los riesgos asociados a los servicios de TI más críticos de la organización, sus causas y sus efectos. En esta tabla se incluyeron riesgos que están y no en control por la organización:

Registro de Riesgo			
ID	**Causa**	**Riesgo**	**Efecto**
1	Terremoto.	Pérdida de las instalaciones y personal de la empresa.	Indisponibilidad de las operaciones del negocio.
2	Desconexión física hacia proveedoor principal.	Desconexión de la red MPLS.	Los usuarios no podrán utilizar las aplicaciones remotas ubicadas en servidores remotos. Caída del servicio de internet y los servicios que dependen de él.
3	Pérdida de energia eléctrica.	Falla en aire acondicionado y falla elétrica en general.	Pueden apagarse los equipos del data center.
4	Huracanes.	Falla eléctrica.	Pueden apagarse los equipos del data center.
5	Falla en UPS del data center.	Indisponibilidad de los servidores y otros equipos de infraestructura del data center momentaneamente.	Los usuarios no podrán acceder a la información ni aplicaciones ubicadas en los servidores, produciendo retrasos en las operaciones. Indisponibilidad de la red.
6	Falla de Aire Acondicionado.	Sobrecalentamiento de los equipos del data center.	Mal funcionamiento del hardware del centro de datos, pudiendo provocar que estos se apaguen.
7	Inundación.	Daño en los equipos de infraestrucutra del centro de datos.	Pérdida de información. Indisponibilidad de los servicios de TI.
8	Incendio.	Pérdida de hardware, daño en las instalaciones y pérdida de personal.	Pérdida de los servicios en general.
9	Robo de equipo.	Pérdida de activo de TI.	Pérdida monetaria para la organización.
10	Robo de información.	Mal uso de la información.	Vulnerabilidad de la empresa.

11	Falla en servidores externos.	Los usuarios no podrán acceder a información ni aplicaciones ubicadas en dichos servidores.	Lo cual producirá atrasos en las actividades de producción del negocio.
12	Falla en servidores internos.	Los usuarios no podrán acceder a información ni aplicaciones ubicadas en dichos servidores.	No se podrá hacer uso de la información contenida en dichos servidores.
13	Interrupción de servicio Callmanager.	Servicio de telefonía no disponible.	No existirá comunicación telefónica con casa matriz.
14	Falla en CORE Switch.	Desconexión de la red MPLS.	Los usuarios no podrán utilizar las aplicaciones remotas ubicadas en servidores remotos. Caída del servicio de internet y los servicios que dependen de él.
15	Saturación en el núcleo de comunicaciones.	Problema en el procesamiento de la información.	Pérdida de desempeño hasta posible desconexión de la red MPLS.
16	Falta de redundancia de enlace entre Switches 3750G	Perdida de comunicación entre los dos swtiches.	Pérdida de comunicación para los hosts conectados al switch.
17	Interrupción servicio de Internet.	Falla en el acceso a los servicios que dependen de internet.	Operaciones que necesiten internet para efectuarse se ven afectadas. Posible desconexión de la red MPLS, debido a que el mismo equipo físico provee ambos servicios.
18	Interrupción del servicio de Firewall.	Falla en la seguridad de la red.	Desconexión hacia servidores y hacia Internet. Los usuarios podrían tener acceso a páginas previamente restringidas.
19	Acceso al Núcleo de comunicaciones por personal no autorizado.	Modificación de la configuración del CORE Switch.	Desconexión de la red MPLS.
20	Falla de Planta Eléctrica	Si hay corte de energia prolongado de parte del proveedor de electricidad, los equipos del data center se apagarán.	Indisponibilidad de las operaciones del negocio.
21	Terrorismo	Perdida de las instalaciones y personal de la institución.	Indisponibilidad de las operaciones del negocio.
22	Virus Informático	Corrupción y robo de información relevante.	Poner en riesgo imagen de la empresa.
23	Daños en las cintas de backup	Perdida de información vital de respaldo.	La empresa no puede recuperar información vital para las operaciones del negocio produciendo atrasos severos en producción.

Tabla 8. Registro de Riesgo

7.5.1. Análisis de Riesgo

Analizar el riesgo conlleva evaluar los siguientes puntos:

- Probabilidad, que es la frecuencia con la cual puede ocurrir el riesgo.
- Impacto, que es el impacto que causará en caso de que suceda el riesgo.
- Evaluación de los controles existentes con el fin de mejorarlos y establecer nuevos controles de ser necesario.
- Magnitud del riesgo, que es determinada por la probidad y el impacto. (Magnitud = Probabilidad x Impacto)

Para determinar la probabilidad, el impacto y su magnitud se utilizara la siguiente matriz denominada Matriz de Riesgo.[26]

MATRIZ DE RIESGO				
PROBABILIDAD	ALTA	B	A	A
	MEDIA	B	B	A
	BAJA	C	B	B
		BAJO	MEDIA	ALTO
		IMPACTO		

Tabla 9. Matriz de Riesgo

[26] Fuente: http://www.utp.edu.co/php/controlInterno/docsFTP/ADMINISTRACION_DE_RIESGOS172.ppt

En donde:

Magnitud A = Nivel alto riesgo.

Magnitud B = Nivel medio riesgo.

Magnitud C = Nivel bajo riesgo.

El significado para los elementos de la matriz es el siguiente:

ESCALA DE PROBABILIDAD

ALTO – es muy probable que el riesgo se presente.

MEDIO – es probable que el riesgo se presente.

BAJO – es muy poco probable que el riesgo se prestente.

ESCALA DE IMPACTO

ALTO – afecta en alto grado la disponibilidad del servicio.

MEDIO – afecta en medio grado la disponibilidad del servicio.

BAJO - afecta en alto bajo la disponibilidad del servicio.

En la siguiente tabla se exponen los riesgos con su magnitud basada en la matriz de riesgo. También presenta la respuesta que se le dará al riesgo. Esto permitirá posteriormente priorizarlos y definir cuáles deben de ser tratados con mayor urgencia y cuáles deben ser dejados en un watchlist.

Registro de Riesgo							
ID	**Causa**	**Riesgo**	**Efecto**	**Probabilidad**	**Impacto**	**Magnitud de Riesgo**	**Respuesta de Riesgo**
1	Terremoto.	Pérdida de las instalaciones y personal de la empresa.	Indisponibilidad de las operaciones del negocio.	**Media**	**Alto**	**A**	**Aceptar**
2	Desconexión física hacia proveedoor principal.	Desconexión de la red MPLS.	Los usuarios no podrán utilizar las aplicaciones remotas ubicadas en servidores remotos. Caída del servicio de internet y los servicios que dependen de él.	**Media**	**Alto**	**A**	**Mitigar**
3	Pérdida de energia eléctrica.	Falla en aire acondicionado y falla elétrica en general.	Pueden apagarse los equipos del data center.	**Baja**	**Medio**	**B**	**Mitigar**
4	Huracanes.	Falla eléctrica.	Pueden apagarse los equipos del data center.	**Media**	**Medio**	**B**	**Mitigar**
5	Falla en UPS del data center.	Indisponibilidad de los servidores y otros equipos de infraestructura del data center momentaneamente.	Los usuarios no podrán acceder a la información ni aplicaciones ubicadas en los servidores, produciendo retrasos en las operaciones. Indisponibilidad de la red.	**Baja**	**Alto**	**B**	**Mitigar**

6	Falla de Aire Acondicionado.	Sobrecalentamiento de los equipos del data center.	Mal funcionamiento del hardware del centro de datos,	**Baja**	**Bajo**	**C**	**Mitigar**
7	Inundación.	Daño en los equipos de infraestrucutra del centro de datos.	Pérdida de información. Indisponibilidad de los servicios de TI.	**Baja**	**Alto**	**B**	**Aceptar**
8	Incendio.	Pérdida de hardware, daño en las instalaciones y pérdida de personal.	Pérdida de los servicios en general.	**Baja**	**Alto**	**B**	**Mitigar**
9	Robo de equipo.	Pérdida de activo de TI.	Pérdida monetaria para la organización.	**Baja**	**Bajo**	**C**	**Mitigar**
10	Robo de información.	Mal uso de la información.	Vulnerabilidad de la empresa.	**Baja**	**Bajo**	**C**	**Mitigar**
11	Falla en servidores externos.	Los usuarios no podrán acceder a información ni aplicaciones ubicadas en dichos servidores.	Lo cual producirá atrasos en las actividades de producción del negocio.	**Media**	**Alto**	**A**	**Transferir**
12	Falla en servidores internos.	Los usuarios no podrán acceder a información ni aplicaciones ubicadas en dichos servidores.	No se podrá hacer uso de la información contenida en dichos servidores.	**Media**	**Medio**	**B**	**Transferir**
13	Interrupción de servicio Callmanager.	Servicio de telefonía no disponible.	No existirá comunicación telefónica con casa matriz.	**Media**	**Bajo**	**B**	**Transferir**
14	Falla en CORE Switch.	Desconexión de la red MPLS.	Los usuarios no podrán utilizar las aplicaciones remotas ubicadas en servidores remotos. Caída del servicio de internet y los servicios que dependen de él.	**Media**	**Alto**	**A**	**Mitigar**
15	Saturación en el núcleo de comunicaciones.	Problema en el procesamiento de la información.	Pérdida de desempeño hasta posible desconexión de la red MPLS.	**Media**	**Alto**	**A**	**Mitigar**
16	Falta de redundancia de enlace entre Switches 3750G	Perdida de comunicación entre los dos swtiches.	Pérdida de comunicación para los hosts conectados al switch.	**Media**	**Alto**	**A**	**Mitigar**
17	Interrupción servicio de Internet.	Falla en el acceso a los servicios que dependen de internet.	Operaciones que necesiten internet para efectuarse se ven afectadas. Posible desconexión de la red MPLS, debido a que el mismo equipo físico provee ambos servicios.	**Media**	**Alto**	**A**	**Mitigar**

18	Interrupción del servicio de Firewall.	Falla en la seguridad de la red.	Desconexión hacia servidores y hacia Internet. Los usuarios podrían tener acceso a páginas previamente restringidas.	**Baja**	**Alto**	**B**	**Transferir**
19	Acceso al Núcleo de comunicaciones por personal no autorizado.	Modificación de la configuración del CORE Switch.	Desconexión de la red MPLS.	**Baja**	**Alto**	**B**	**Mitigar**
20	Falla de Planta Eléctrica	Si hay corte de energia prolongado de parte del proveedor de electricidad, los equipos del data center se apagarán.	Indisponibilidad de las operaciones del negocio.	**Media**	**Alto**	**A**	**Mitigar**
21	Terrorismo	Perdida de las instalaciones y personal de la institución.	Indisponibilidad de las operaciones del negocio.	**Baja**	**Alto**	**B**	**Aceptar**
22	Virus Informático	Corrupción y robo de información relevante.	Poner en riesgo imagen de la empresa.	**Media**	**Medio**	**B**	**Mitigar**
23	Daños en las cintas de backup	Perdida de información vital de respaldo.	La empresa no puede recuperar información vital para las operaciones del negocio produciendo atrasos severos en producción.	**Baja**	**Alto**	**B**	**Mitigar**

Tabla 10. Magnitud y Respuesta al Riesgo. Fuente: Propia

En la tabla 10 fueron evaluados 23 riesgos en totales. El 30% son riesgos de magnitud A, el 57% son riesgos de magnitud B y el 13% son de magnitud C.

7.5.2. Evaluación de Riesgo

Para evaluar los riesgos se tomará el siguiente criterio de evaluación.[27]

:

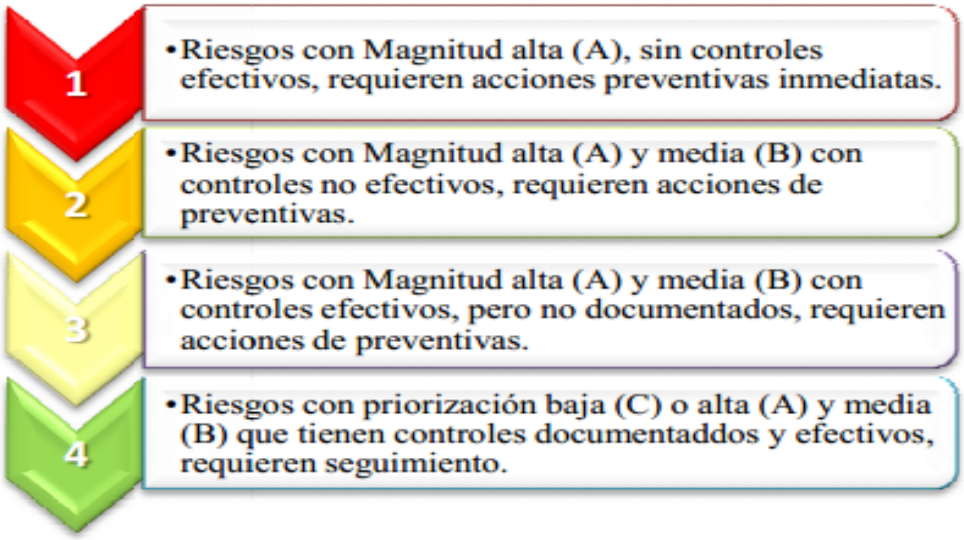

Tabla 11. Criterios de Evaluación de Riesgo.
Fuente: Propia.

[27] Fuente: http://www.utp.edu.co/php/controlInterno/docsFTP/ADMINISTRACION_DE_RIESGOS172.ppt

La siguiente tabla muestra, en base a los criterios de evaluación, cuáles son los riesgos que deben realmente ser evaluados:

ID	RIESGO	CONTROLES EXISTENTES	MAGNITUD DE RIESGO	CRITERIO	¿TRATAR RIESGO?
1	Terremoto.	-	A	1	SI
2	Desconexión física hacia proveedoor principal.	-	A	1	SI
3	Pérdida de energia eléctrica.	Sistema de UPS y Grupo electrógeno respaldo.	B	3	NO
4	Huracanes.	-	B	2	SI
5	Falla en UPS del data center.	-	B	2	SI
6	Falla de Aire Acondicionado.	Aire Split de respaldo.	C	4	NO
7	Inundación.	-	B	2	SI
8	Incendio.	Estinguidores y Sistema de Alarma contra incendio.	B	3	SI
9	Robo de equipo.	Seguridad en el edificio.	C	4	NO
10	Robo de información.	Bloqueo de puertos USB.	C	4	NO
11	Falla en servidores externos.	Contactar al proveedor externo.	A	2	SI
12	Falla en servidores internos.	Contactar al proveedor externo.	B	3	SI
13	Interrupción de servicio Callmanager.	Contactar al proveedor externo.	B	4	NO
14	Falla en CORE Switch.	-	A	1	SI
15	Saturación en el núcleo de comunicaciones.	-	A	1	SI
16	Falta de redundancia de enlace entre Switches 3750G.	-	A	1	SI
17	Interrupción servicio de Internet.	Contactar al proveedor externo.	A	2	SI
18	Interrupción del servicio de Firewall.	Contactar al proveedor externo.	B	3	SI
19	Acceso al Núcleo de comunicaciones por personal no autorizado.	Contraseñas seguras.	B	2	SI
20	Falla de Planta Eléctrica	-	B	2	SI
21	Terrorismo	Personal y camaras de seguridad en toda la organización.	B	2	NO
22	Virus Informático	Programa antivirus y servicio de firewall	B	4	NO
23	Daños en las cintas de backup	-	B	2	SI

Tabla 12. Evaluación de Riesgo. Fuente: Propia

7.6. Alternativas Propuestas de Recuperación

La siguiente tabla presenta las alternativas propuestas para la continuidad de los servicios de TI, la respuesta al riesgo para cada riesgo, muestra el control existente y el departamento responsable de realizar la implementación.

ALTERNATIVAS DE RECUPERACION					
ID	RIESGO	RESPUESTA AL RIESGO	CONTROL EXISTENTE	ALTERNATIVA DE RECUPERACION	RESPONSABLE
1	**Terremoto.**	Aceptar	-	Implementar solución Warm Recovery Implementar solución Hot Recovery Implementar solución Cold Recovery	TI
2	**Desconexión física hacia proveedor principal.**	Mitigar	-	Implementar conexión redundante.	TI
4	**Huracanes.**	Mitigar	-	Proteger ventanas.	Facilities
5	**Falla en UPS del data center.**	Mitigar	-	Instalación de un UPS de Respaldo.	TI
7	**Inundación.**	Mitigar	-	Instalación de puerta hermética.	Facilities
8	**Incendio.**	Mitigar	Extinguidores y Sistema de Alarma contra incendio.	Adquisición de un seguro contra incendios. Instalación de Sistema de Alarma Inteligente en el data center. Implementación de una sala cofre para data center. Instalación de puerta corta fuego en el data center.	Facilities
11	**Falla en servidores externos.**	Transferir	Contactar al proveedor externo.	Conexión redundante a servidores externos.	TI
12	**Falla en servidores internos.**	Transferir	Contactar al proveedor externo.	-	TI
14	**Falla en CORE Switch.**	Mitigar	-	Conectar los switches de acceso a ambos CORE Switches	TI
15	**Saturación en el núcleo de comunicaciones.**	Mitigar	-	Implementación de balanceo de carga.	TI
16	**Falta de redundancia de enlace entre Switches 3750G.**	Mitigar	-	Implementación de línea redundante.	TI
17	**Interrupción servicio de Internet.**	Mitigar	Contactar al proveedor externo.	Conexión de enlace redundante de Internet. Proveedor de servicios de respaldo.	TI
18	**Interrupción del servicio de Firewall.**	Transferir	Contactar al proveedor externo.	-	TI
19	**Acceso al Núcleo de comunicaciones por personal no autorizado.**	Mitigar	Contraseñas seguras.	-	TI
20	**Falla de Planta Eléctrica.**	Mitigar	-	Conexión a planta eléctrica alterna.	Facilities
23	**Daños en las cintas de backup.**	Mitigar	-	Contratar servicio de proveedor externo para reguardo de cintas de backup en bóvedas seguras. Implementar solución de backup virtual.	TI

Tabla 13. Alternativas de Recuperación. Fuente: Propia.

Cabe destacar, que el responsable estará definido en el alcance y esta propuesta abarca solo el departamento de TI. Las alternativas seleccionadas están sombreadas en color amarillo.

7.7. Tratamiento de las Alternativas Seleccionadas

Las alternativas para los siguientes riesgos serán tratadas en manera conjunta y se representaran en el diagrama de red propuesto:

- Desconexión física hacia proveedor principal.
- Falla en servidores externos.
- Falla en CORE Switch.
- Saturación en el núcleo de comunicaciones.
- Interrupción servicio de Internet.
- Interrupción del servicio de Firewall.

Las alternativas para el riesgo del terremoto se tratarán de manera independiente y para los demás riesgos, las alternativas que se aplicarán están definidas en la tabla 13 y no requieren diseño, sino la creación de un plan para poner en marcha su implementación.

7.8. Estrategias de recuperación frente problemas de infraestructura y telecomunicaciones de YP Directories.

A continuación se presentan las alternativas seleccionadas para problemas relacionados con la red empresarial

7.8.1. Diseño de red actual

El siguiente diagrama es una representación de cómo está estructurada la red de la empresa YP Directories:

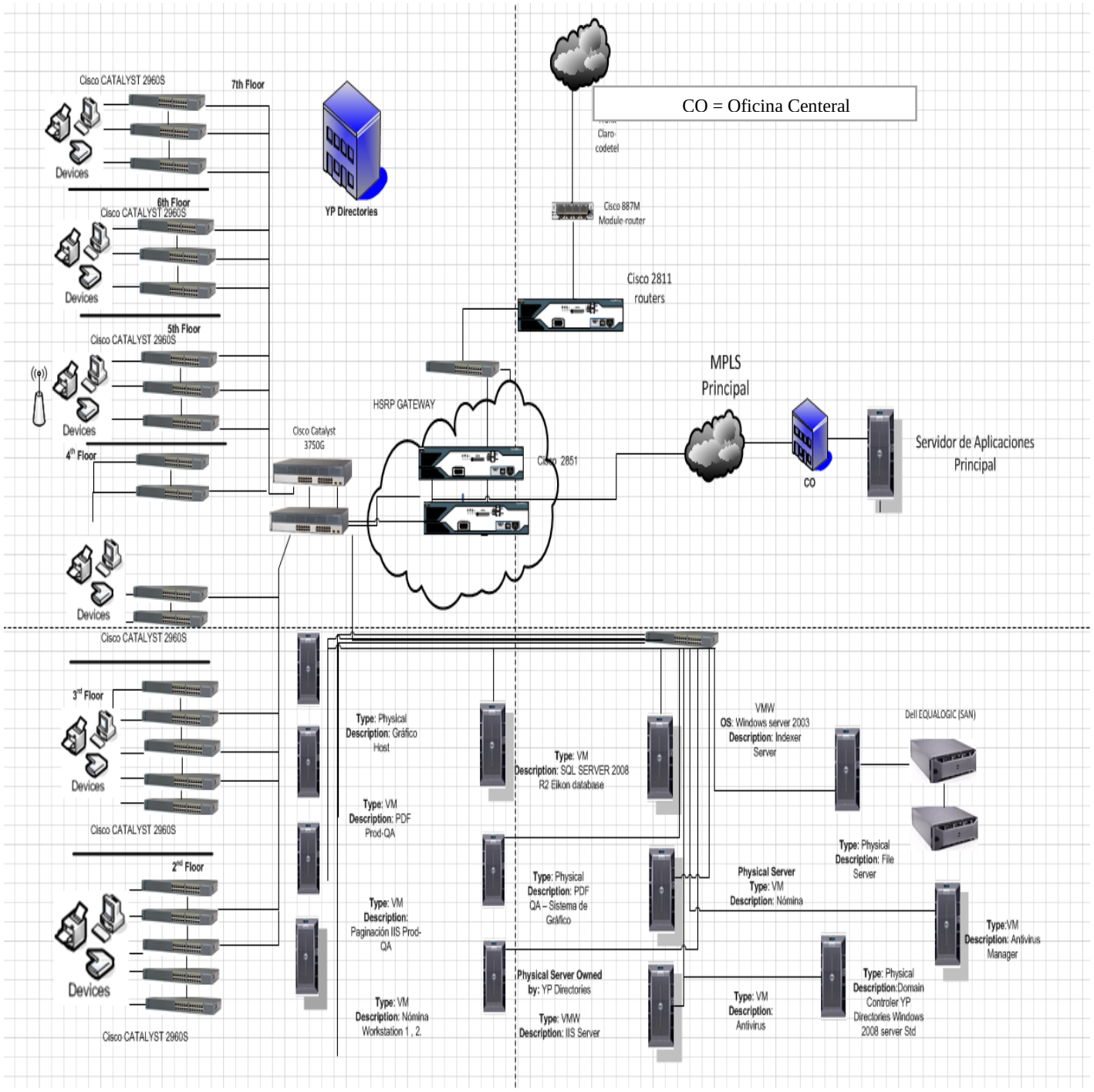

Figura 41. Diseño de red actual de YP Directories. Fuente: Propia.

Como se puede ver en la figura 41, YP Directories cuenta con una infraestructura de red que, aunque tiene algunos componentes redundantes, la redundancia de estos no es suficiente para dar continuidad a los servicios.

Se puede ver que esta compañía es muy dependiente del enlace que provee su proveedor de servicios principal y que a través de esta conexión se puede comunicar con el servidor de aplicaciones, con sede en los Estados Unidos, que contiene las aplicaciones más críticas del negocio. Si este enlace falla, la empresa queda sin comunicación y sus operaciones se paralizan. Para esta conexión la empresa utiliza el protocolo de red MPLS (Multiprotocol Label Switching).

Otra debilidad que se puede observar en el diagrama, es que no existe redundancia de enlace entre los CORE switches que conectan con los switches de acceso de la organización. Si el único enlace que los conecta falla, entonces habrá problemas de conectividad en los hosts que dependen ellos. Por otro lado, todos los switches de acceso están conectados a un único CORE switch, lo que indica que si ese switch falla, los hosts conectados a él perderán comunicación.

Por otro lado, existe un solo servidor de aplicaciones que contiene todas las aplicaciones críticas del negocio. Si este servidor deja de funcionar entonces las

operaciones del negocio se paralizarán. Es por todo lo anteriormente descrito que se requiere implementar un diseño de red más redundante que haga frente a fallas que pudiesen afectar la continuidad de los servicios de TI.

7.8.2. Diseño de red propuesto

En base a las alternativas seleccionadas definidas en la tabla 13, el siguiente diagrama representa el diseño de red propuesto para la empresa YP Directories:

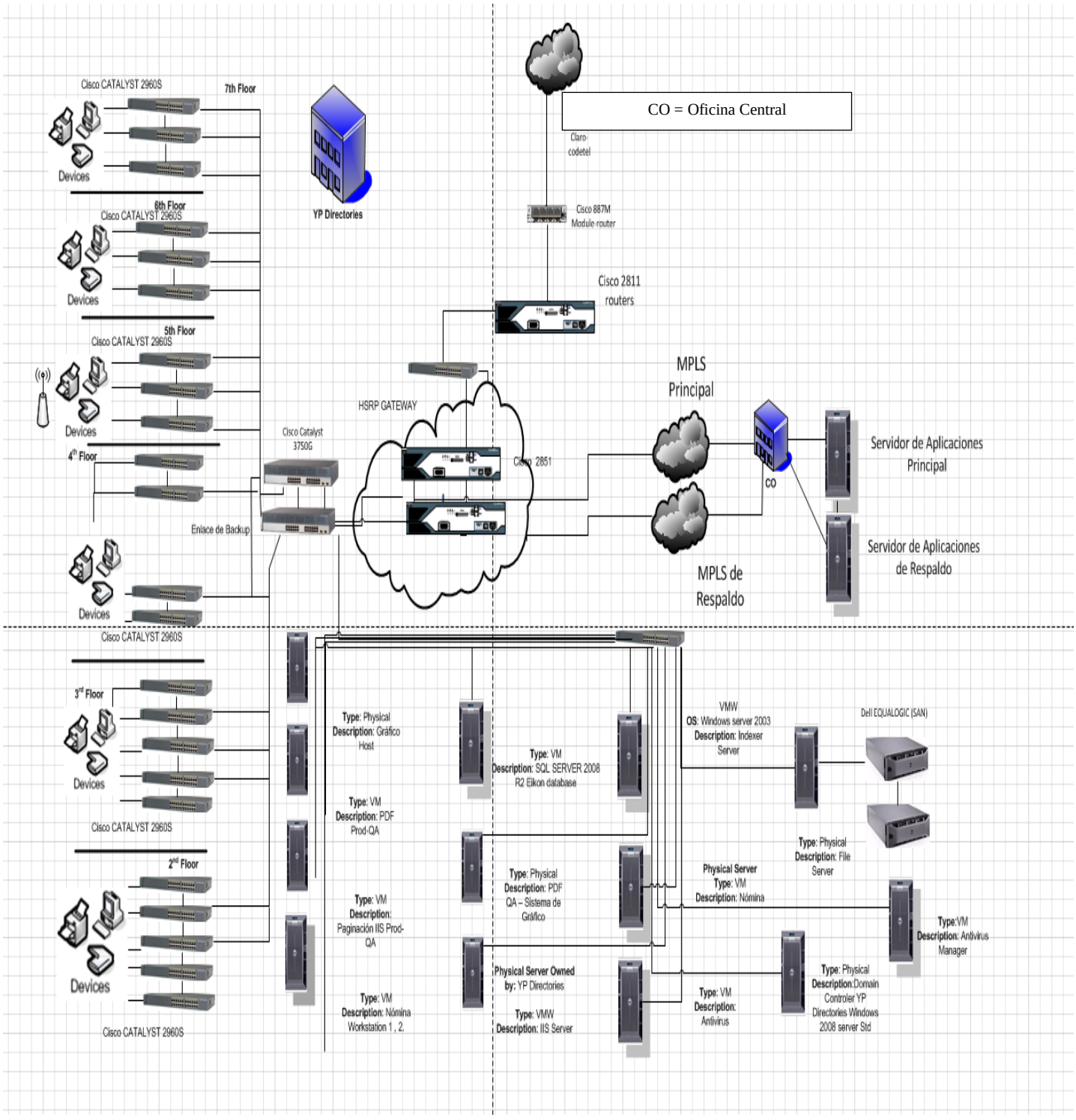

Figura 42. Diseño de red de YP Directories con alternativas de mejoras aplicadas. Fuente: Propia.

Como se puede ver en la figura 42 se ha modificado el diseño original de la red de YP Directories para agregar componentes y enlaces redundantes y evitar que las operaciones del negocio se paralicen.

En este diseño se han agregado enlaces redundantes entre los core switches y se han conectado los swtiches de acceso a ambos CORE switches para evitar que si se cae uno, los demás hosts conectados a él dejen de funcionar. También se ha agregado otro proveedor de servicios el cual servirá de respaldo en caso de que el proveedor principal falle. Por otro lado, se ha agregado un servidor de aplicaciones de respaldo el cual se pondrá en funcionamiento una vez falle el servidor principal.

7.9. Estrategia de recuperación frente a terremotos.

Frente a un terremoto y asumiendo que se pierda el centro de datos de la compañía, la organización puede optar por la estrategia de recuperación *Cold Recovery.*

Esta estrategia consiste en contar con un espacio reservado, puede ser móvil o fijo, que tenga que este habilitado con energía eléctrica, control ambiental y telecomunicación y que pueda ser utilizado para casos de emergencia. No necesariamente debe contar con los equipos de TI o las aplicaciones.

Generalmente este tipo de soluciones las provee una compañía tercera lo cual evita tener mantener los costos asociados a tener otro data center y la organización solo tendría que pagar por el servicio. El servicio incluiría tanto la configuración del hardware y el uso de los equipos en caso de que la organización no los tenga.

7.10. Análisis Financiero

Para verificar si la implementación de la propuesta será factible para la organización, se ha realizado un análisis financiero donde se detallan los costos operacionales asociados a la implementación de las alternativas seleccionadas, así como también los beneficios percibidos por dicha implementación. El método utilizado para el cálculo de factibilidad de inversión fue el Método del Valor Presente Neto (VPN).

7.10.1. Costos Operacionales

Los costos operacionales representan los gastos que realizará la Empresa en la implementación. Estos gastos incluyen: costo por mantenimiento, adquisición de equipos, pago de servicios y pago por concepto de entrenamiento en el proceso de Gestión de Continuidad de Servicios de TI. La siguiente tabla es un presupuesto que se realizó para estimar los costes. Los precios especificados en la tabla 14 están estimados en dólares.

PRESUPUESTO				
Elemento	Descripción	Cantidad	Precio Unitario	Total
Servidor Dell	PowerEdge R720, Intel® Xeon serie E5-2600, 32TB, 1.5TB RAM	1	$ 1,500.00	$ 1,500.00
Cableado	CAJA RJ45 UTP Cat.6 10/100/1000	2	$ 200.00	$ 400.00
Cableado	Proyecto Reestructuración Cableado Interno	1	$ 600.00	$ 600.00
UPS Respaldo	Smart-UPS® VT, 40kVA + Instalación	1	$ 20,000.00	$ 20,000.00
Servicio de Proveedor Respaldo	Servicio Internet Proveedor Secundario	1	$ 12,000.00	$ 12,000.00
Solución Cold Recovery	Servicio Cold-Site, Equipos DataCenter, Configuración Equipo	1	$ 8,400.00	$ 8,400.00
Contrato de Mantenimiento CORE Switch	Cisco SmartNet CORE Switches 3750	2	$ 6,675.84	$ 13,351.68
Servicio de solución en la nube para backup	Storage Backup CLOUD 1TB, Soporte 24/7/365	1	$ 3,696.00	$ 3,696.00
Puerta Contra Incendios / Inundaciones	Puerta Hermética Contra Incendios/Inundaciones	1	$ 3,000.00	$ 3,000.00
Curso Entrenamiento	ITIL V3 Foundation	8	$ 1,500.00	$ 12,000.00

Tabla 14. Presupuesto estimado de costos implementando la propuesta. Fuente: Propia.

La tabla 14 detalla los elementos a utilizar para la implementación. Se sugiere tomar en cuenta el entrenamiento para los usuarios de TI que estarán involucrados en la implementación del proceso. Es recomendable que el personal tenga conocimiento de lo que se va a realizar y por lo tanto se sugiere que la Empresa pague el entrenamiento adecuado al personal de TI.

7.10.2. Análisis de Gastos sin la Implementación

Para realizar este análisis, se han identificado cuáles son las desventajas asociadas a las interrupciones de los servicios críticos de TI. Estas variables son las siguientes:

- Imagen de la empresa puede verse afectada.
- Clientes insatisfechos por no recibir el directorio telefónico en la fecha estipulada.
- Pago de multas de hasta $100mil dólares por atraso en producto final.
- Pago de horas extras al personal pertinente.
- Pago por distribución de directorios atrasados.
- Reducción de las ventas debido a insatisfacción de los clientes.

De las desventajas anteriormente mencionadas las que acarrean costos directos en la organización son:

1. **Pago de horas extras al personal pertinente.**
2. **Pago de multas de hasta $100mil dólares por atraso en producto final.**
3. **Pago por distribución de directorios atrasados.**

A continuación, se explica cuáles son los costos asociados a las tres desventajas mencionadas anteriormente.

1. Pago de horas extras al personal por horas de interrupción de servicios.

La siguiente tabla presenta el cálculo de horas extras que la empresa deberá pagar si ocurre una interrupción de los servicios críticos de TI:

CALCULO DE HORAS EXTRAS							
Unidad	**Departamento**	**Cantidad de empleados**	**Sueldo**	**Sueldo por hora**	**Hora Extra**	**Tiempo de Recuperación Objetivo (RTO) de Negocio**	**Total a pagar por día de horas extras**
Producción	Digitación	80	20,000.00	104.91	141.63	79	11,188.63
Producción	Paginación	10	25,000.00	131.14	177.04	79	13,985.78
Calidad	Auditoria	25	30,000.00	157.36	212.44	127	26,980.17
Producción	Gráficos	25	27,000.00	141.63	191.20	175	33,459.66
Producción	Preparación de Mercado	9	27,000.00	141.63	191.20	79	15,104.65
Calidad	Cierre de Libro	12	27,000.00	141.63	191.20	103	19,693.40
						Total RD$	**120,412.30**
Tasa Dólar	$ 44.00					**Total US$**	**2,736.64**

Tabla 15. Cantidad de Dinero a pagar por horas extras en caso de interrupción de servicios críticos de TI en YP Directories. Fuente: Propia.

Como se puede ver en la tabla 15, la empresa tendrá que pagar $2736.64 dólares en horas extras si llegase a ocurrir un evento que impacte a los servicios críticos de TI.

Para el cálculo de las horas, se ha tomado como referencia los Tiempos Objetivos de Recuperación (RTO) de cada proceso de negocio en horas.

2. Pago de multas de hasta $100mil dólares por atraso en producto final.

Para calcular las multas que recibiría la Empresa por atrasados en directorios se toma en cuenta cuántos directorios la empresa maneja, cuántos pagan multas, cuánto no pagan multas y cuántos directorios se imprimen mensualmente.

	Cantidad impresa anual	Porcentaje %	Cantidad Impresa por mes
Total Directorios	700	100%	58
Pagan Multa	36	5%	3
No Pagan Multa	664	95%	55

Tabla 16. Total de directorios que pagan y no pagan multas por atrasos. Fuente: Propia.

Los resultados de la tabla 16 muestran que la empresa imprime mensualmente tres directorios que pagan multa y anualmente imprime 36. Esto quiere decir, que si en un mes llegase a ocurrir una interrupción de servicios de TI para cualquier departamento, la empresa estaría pagando $300,000.00 dólares mensuales por multa, para un equivalente de $3,600,000.00 por multa anual.

3. Pagos por distribución de directorios atrasados

La distribución de los directorios es un gasto que corre por cuenta de la compañía telefónica, sin embargo, según las investigaciones realizadas, está estipulado en el contrato con las telefónicas, que YP Directories correrá con los gastos de este servicio si por alguna razón no llegase a cumplir con las fechas estipuladas de entrega del producto final. Esto quiere decir que si la Empresa imprime 58 directorios mensuales y el costo estimado, por directorio, para pagos por distribución es de $750.00 dólares entonces la Empresa estaría pagando *$43,500.00 dólares mensuales por la distribución de cada directorio. Esto anualmente equivale a $522,000.00 dólares anuales.*

7.10.3. Análisis de Factibilidad de Inversión por Método del VPN

El Método del Valor Presente Neto (VPN) es un método de evaluación de proyectos que tiene como objetivo determinar si la inversión de dicho proyecto es aconsejable. Consiste en determinar la sumatoria algebraica de todos los ingresos y egresos de un proyecto de negocio de inversión con la finalidad de determinar la rentabilidad del mismo para su correspondiente toma de decisión. Este método se caracteriza por observar las siguientes posibilidades: VPN $\geq$ 0 – La inversión es rentable y VPN < 0 – La inversión no es aconsejable.

La siguiente tabla detalla los ingresos y egresos asociados al proyecto. Se han tomado como ingresos la reducción de pago de horas extras, la reducción de pagos de multas por atrasados, el ahorro en costos de distribución y el aumento de las ventas. En cuanto a egresos, se han tomado los montos de los gastos operacionales. También, debido a la compra de equipos, se ha estimado un monto por valor de salvamento para el cálculo del VPN. Todos los montos de la tabla se han calculado en años.

CALCULO DE VALOR PRESENTE NETO						
	2014	2015	2016	2017	2018	TOTAL
Beneficios						
Reducción de pago de horas Extras	$ -	$ 32,839.72	$ 37,839.72	$ 42,839.72	$ 47,839.72	$ 161,358.87
Reducción de pago de multas por atraso en directorios	$ -	$ 3,600,000.00	$ 3,600,000.00	$ 3,600,000.00	$ 3,600,000.00	$ 14,400,000.00
Ahorro de costos de distribución de directorios	$ -	$ 522,000.00	$ 522,000.00	$ 522,000.00	$ 522,000.00	$ 2,088,000.00
Aumento en las ventas	$ -	$ 3,000,000.00	$ 3,500,000.00	$ 4,000,000.00	$ 4,500,000.00	$ 15,000,000.00
Total Beneficios US$	**$ -**	**$ 7,154,839.72**	**$ 7,659,839.72**	**$ 8,164,839.72**	**$ 8,669,839.72**	**$ 31,649,358.87**
Gestos de Desarrollo						
Pago entrenamiento Curso ITIL v3 - Foundation	**$ 12,000.00**	$ -	$ -	$ -	$ -	**$ 12,000.00**
Gastos Operacionales						
Adquisición de Equipos	$ 1,500.00	$ -	$ -	$ -	$ -	$ 1,500.00
Servicio de Proveedor Respaldo	$ 12,000.00	$ 12,000.00	$ 12,000.00	$ 12,000.00	$ 12,000.00	$ 60,000.00
Solución Cold Recovery	$ 8,400.00	$ 8,400.00	$ 8,400.00	$ 8,400.00	$ 8,400.00	$ 42,000.00
Contrato de Mantenimiento CORE Switch	$ 13,351.68	$ 13,351.68	$ 13,351.68	$ 13,351.68	$ 13,351.68	$ 66,758.40
Cableado Estructurado	$ 1,000.00	$ -	$ -	$ -	$ -	$ 1,000.00
Servicio de solución en la nube para backup	$ 3,696.00	$ 3,696.00	$ 3,696.00	$ 3,696.00	$ 3,696.00	$ 18,480.00
Instalación UPS de Respaldo	$ 20,000.00	$ -	$ -	$ -	$ -	$ 20,000.00
Mantenimiento de UPS	$ -	$ 600.00	$ 600.00	$ 600.00	$ 600.00	$ 2,400.00
Instalación Puerta Contra Incendios	$ 3,000.00	$ -	$ -	$ -	$ -	$ 3,000.00
Total Costo de Operaciones US$	**$ 74,947.68**	**$ 38,047.68**	**$ 38,047.68**	**$ 38,047.68**	**$ 38,047.68**	**$ 227,138.40**
Valor de Salvamento	**$ 50,000.00**					
Valor presente neto (VPN)	**$ 32,620,623.94**					
% Tasa de interés, i	**0.16**					

Tabla 17. Detalle de ingresos y egresos anuales por la implementación del proyecto. Fuente: Propia.

La tabla 17 muestra que en el 2014 la Empresa no obtendrá ningún beneficio ya que es el periodo donde solo se invierte y este no se espera. Sin embargo, a partir del 2015 la empresa tendrá un beneficio de $ 7,154,839.717 de donde $3,000,000.00 van destinados al incremento de un 2% en las ventas debido a la satisfacción de los clientes y buena imagen de Empresa por brindar servicios de calidad apoyándose en una

infraestructura de TI confiable. Se estima que este beneficio crecerá en un valor de $505,000.00 dólares anuales.

En cuanto a los egresos, la empresa tendrá un egreso de $74,947.68 dólares en el primer año correspondientes a la inversión. A partir del 2015, tendrá gastos por mantenimiento fijos de $38,047.68 dólares anuales. El siguiente diagrama ayuda a visualizar mejor estas cifras.

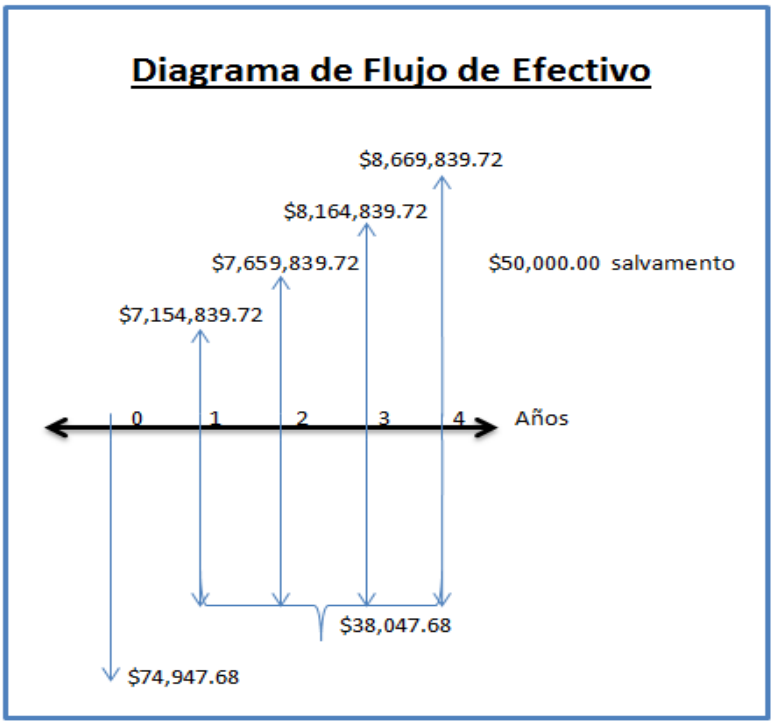

Figura 43. Diagrama de Flujo de Efectivo. Fuente: Propia.

El valor VPN es de $32, 620,623.94 dólares. Como el VPN resulto ser mayor que cero, por tanto la inversión es aconsejable. El patrimonio de la empresa aumentaría en un valor equivalente hoy de $32, 620,623.94 y aumentaría a un valor equivalente hoy de $32,695,571.62.

CONCLUSION

Luego de haber expuesto esta propuesta, las conclusiones que se obtienen son las siguientes:

- La Gestión de Continuidad de Servicios de TI es un proceso muy importante de ITIL con el cual todas las organizaciones deberían de contar ya que estas dependen mucho de estos servicios y dichos servicios son la base del negocio.

- La Gestión de Continuidad de Servicios de TI (ITSCM) va más allá de un Plan de Recuperación de Desastres, si no que va alineada al Ciclo de Vida del Negocio y forma parte esencial de la Gestión de Continuidad de Negocio (BCM).

- El proceso de Gestión de Continuidad de Servicios de TI no solo está para recuperarse de las interrupciones que ocurran con los servicios, sino que tiene como una de sus funciones principales evitar que estas interrupciones sucedan aplicando estrategias tecnológicas efectivas que impidan las interrupciones.

- La ITSCM esta supuesta a manejar todo tipos de incidentes desde desastres naturales hasta pequeños eventos como la falla de un servidor. Siempre y cuando ocurra un evento que pueda poner en riesgo los Acuerdos de Niveles de Servicios (SLAs) y que

involucren servicios de TI, entonces estos riesgos deben de ser contemplados en el proceso de la ITSCM.

- ITIL es el código de buenas prácticas más aceptado en todo el mundo y la implementación de sus procesos traen beneficios significativos para las organizaciones.

- La implementación del proceso de la ITSCM puede ser aplicado en cualquier organización. Sin embargo, su implementación puede ser costosa. Hay que tener en cuenta que implementar planes de continuidad es como tener un seguro, no se sabe que tan importante será hasta que se debe de utilizar.

RECOMENDACIONES

1. Se recomienda comprar equipos que permitan la alta disponibilidad de los servicios.

2. Incrementar sistema inteligente de alarma contra incendios.

3. Crear un equipo de Manejo de Crisis para crear planes de emergencia frente a siniestros.

4. Adquirir nuevos servicios de tecnología WAN para incrementar disponibilidad de los servicios.

5. Realizar simulacros que pongan a prueba los planes de emergencia creados.

6. Concientizar al personal sobre el nuevo proceso a implementar.

7. Documentar todos los planes de contingencia.

8. Mantener actualizado el plan de continuidad y realizar chequeos periódicos para implementar las mejoras necesarias.

9. Tener servicios de backup alternos para fines de recuperación de desastres.

10. Mantener la renovación de la garantía de los equipo al día.

11. Seguir implementando procesos de ITIL que ayuden al negocio a obtener más beneficios.

BIBLIOGRAFIA

A.Abreu, Jose. (14 de Febrero de 2014). *CONTINUIDAD DE NEGOCIOS EN REPUBLICA DOMINICANA NOVEDAD O NECESIDAD?* Recuperado el 11 de Octubre de 2014, de Outsourcing Security Services: http://www.osssecurity.net/app/articulos-noticias/67-continuidad-de-negocios-en-republica-dominicana-novedad-o-necesidad.html

B.S, T. (2014). *Practical IT Service Management: A concise guide for busy executives* (2da ed.). Ely: IT Governance Publishing.

BitHoy. (8 de 8 de 2008). *Tipos de almacenamiento - SAN*. Recuperado el 3 de 9 de 2014, de BitHoy: http://www.bithoy.com/index.php/menuitem-medios-de-almacenamiento/48-tipos-de-almacenamiento?start=2

Bon, J. v., Jong, A. d., Kolthof, A., Pieper, M., Tjassing, R., Veen, A. v., & Verheijen, T. (2008). *Gestión de Servicios TI basado en ITIL V3 - Guia de Bolsillo.* Zaltbommel: Van Haren Publishing.

Budris, P. (2011). ADMINISTRADOR DE REDES WINDOWS. En P. Budris, *ADMINISTRADOR DE REDES WINDOWS* (pág. 320). Buenos Aires: Fox Andina.

CA Technologies. (Enero de 2011). *The Avoidable Cost of Downtime: The Impact of IT downtime on employee Productivity.* Obtenido de CA Technologies - Business Rewitten by Software: http://www.ca.com/~/media/files/articles/avoidable_cost_of_downtime_part_2_ita.aspx

Colocho, N., Daza, P., & Guzman, M. (08 de Agosto de 2011). *Webquery.* Obtenido de Universidad Dr. Jose Matias Delgado: http://webquery.ujmd.edu.sv/siab/bvirtual/BIBLIOTECA%20VIRTUAL/TESIS/06/ARQ/ADTESCM0001340.pdf

Corrales, J. D. (2005). *Ayudante técnico de informática de la Junta de Andalucía: Test.* España: MAD, S.L.

D-Link. (2012). *¿Qué es RAID, iSCSI, SAN, NAS, Cloud, ...?* Recuperado el 3 de 9 de 2014, de D-Link Building Networks for People:

http://static1.aureo.es/d_link_almacenamiento/52424220/21295/IMAGE/dlink-la-alternativa-nas.pdf

Gallego, J. C. (2014). *Operaciones auxiliares para la configuración y la explotación.* Madrid: Editex, S.A.

García-Cervigón, A., & Ramos, M. d. (2011). *Seguridad Informática* (1ra ed.). Madrid, ESPAÑA: Ediciones Paraninfo, SA.

GuilleSQ. (11 de 6 de 2009). *DAS, NAS y SAN. Arquitecturas de Almacenamiento y Evolución histórica*. Recuperado el 3 de 9 de 2014, de GuilleSQL Un portal sobre Microsoft SQL Server en castellano: http://www.guillesql.es/Articulos/Almacenamiento_SAN_NAS_DAS.aspx

Herold, R. (2008). *The Shortcut Guide to IT Service Management and Automation.* Real Time Publisher, Inc.

Holtsnider, B., & Jaffe, B. D. (2007). *IT Manager's Handbook: Getting your new job done.* San Francisco: Elsevier.

itSMF International. (2008). *Fundamentos de Gestión de Servicios TI, baso en ITIL.* (J. v. Bon, M. Pieper, & A. Kolthof, Edits.) Amersfort: Van Haren Publishing.

Jacob, B., Ng, S. W., & Wang, D. T. (2008). *Memory Systems - Cache, DRAM, Disk.* Elsevier.

Kenneth C. Laudon, J. P. (2004). *Sistemas de información gerencial.* Mexico: Pearson Education.

Laporta, J. L., & Aguiñiga, M. M. (2005). *Fundamentos de telemática.* Valencia: Universidad Politecnica de Valencia.

López, P. A. (2010). *Seguridad Informática.* Madrid: Editex.

Marchionni, E. A. (2011). *Administrador de servidores* (1ra ed.). Buenos Aires: Fox Andina.

Nuno, P., Rivas, J. L., & Ares, J. E. (08 de Mayo de 2006). *Rediris.* Obtenido de Climatizacion en los Centros de Datos: http://www.rediris.es/difusion/publicaciones/boletin/76/enfoque2.pdf

Ordinas, J. M. (2008). *Protocolos y aplicaciones Internet.* Barcelona: Editorial UOC.

Panduit. (2003). *Suplemento sobre cableado estructurado.* Recuperado el 2 de 11 de 2014, de Slideshare: http://www.slideshare.net/edwinalb/cableado-estructurado-ccna-cisco-panduit

Perez, E. H. (2003). *Tecnologías y redes de transmisión de datos.* Mexico: LIMUSA S.A.

Pérez, L. (2013, Noviembre). *Pasos para un Plan de Recuperación de Desastres (DRP).* Retrieved from SearchDataCenter en Español: http://searchdatacenter.techtarget.com/es/cronica/Pasos-para-un-Plan-de-Recuperacion-de-Desastres-DRP

Pink Elephant. (2013). *Fundamentos ITIL en Español.* Burlington: Pink Elephant.

Rouse, M. (2008, Noviembre). *Definition: Microsoft Operations Framework (MOF).* Retrieved Noviembre 24, 2014, from Whatis.com: http://whatis.techtarget.com/definition/Microsoft-Operations-Framework-MOF

Serra, X. H., & Bosch, J. A. (2002). *Análisis de redes y sistemas de comunicaciones.* Barcelona: CPET.

Tanenbaum, A. S. (2003). *Redes de computadoras.* Mexico: Pearson Education.

Vázquez, P. G., Baeza, J. P., & A., F. (2010). *Redes y Transmisión de Datos.* San Vicente: Universidad de Alicante.

Watters, J. (2014). *Disaster Recovery, Crisis Response & Business Continuity: A Management Desk Reference.* New York, NY: Paul Manning.

ANEXO 1- ANTEPROYECTO

UNIVERSIDAD ACCION PRO EDUCACION Y CULTURA

(UNAPEC)

DECANATO DE INGENIERIA E INFORMATICA

ANTEPROYECTO DE TRABAJO DE GRADO

“Implementación de las mejores prácticas de ITIL v3 para la Gestión de Servicios de TI aplicadas a las operaciones del Centro de Datos de la Empresa YP Directories, en la Ciudad de Santo Domingo, Rep. Dom en el periodo Septiembre - Diciembre 2014.”

SUSTENTANTES:

JOHANNA PERALTA	2011-0010
RAUL VANDERHORST	2010-0927
EDWARD RODRIGUEZ	2007-1627

ASESOR:

SANTO NAVARRO

Santo Domingo, D.N.
Julio 2014

1. PLANTEAMIENTO DEL PROBLEMA

Las empresas hoy en día dependen mucho de su Data Center, debido a que en esta parte, se maneja todo el flujo de información que permite a las compañías mantener sus operaciones del día a día.

Un Data Center (centro de cómputos, centro de proceso de datos), es una instalación empleada para albergar los sistemas de información y sus componentes asociados, como las telecomunicaciones y los sistemas de almacenamiento. Generalmente incluye fuentes de alimentación redundantes o de respaldo, conexiones redundantes de comunicaciones, controles de ambiente (por ejemplo, aire acondicionado) y otros dispositivos de seguridad. (ITC Group, 2013).

Aunque en República Dominicana no existen cifras oficiales respecto a la tasa de falla de los data centers, a nivel mundial se han determinado algunas tendencias. El Grupo Editorial EMB (2006), cita el siguiente artículo:

Nelson Wilson, Socio Responsable de Qualitas, división de DMR Consulting, indica que de acuerdo a un estudio de Gartner Group respecto a causas de fallas en Data Centers, el 40% corresponde a aplicación, otro 40% a errores de operación y el 20% restante a problemas en el hardware, software y telecomunicaciones. Otra fuente, BIS Applied Systems, señala que respecto a estudios de falla una de las más importantes es la producida por la acción de

eventos como la exposición al fuego, que alcanza el 36%, seguida por problemas de de software en un 24% y de suministro de energía en un 21%.

Una de las características esenciales de los data centers es, como señala Cristián Álvarez, Gerente de Ventas de Elevair, su uptime o tiempo de funcionamiento, que se mide en términos de disponibilidad como porcentaje. "Generalmente se habla entre un 99% -mínimo aceptable- de disponibilidad hasta un 99,999%. En el primer caso se asume que el data center podría estar abajo 87,6 horas al año, y en el segundo que tendría un down-time de sólo 5,25 minutos por año", asegura.

Lo anterior es un tema clave para cualquier empresa hoy en día, según José Eduardo Muñoz, Gerente Comercial de Rittal, porque cualquier actividad que realiza una compañía depende de la información de los servidores que están en el data center. "Desde la documentación adjunta a un envío de material hasta la emisión de una factura para un cliente, necesita de información alojada en servidores.Esto hace que cualquier parada en el sistema informático de una empresa se convierta directamente en dinero que no se factura", afirma.

Teniendo en cuenta que los Centros de Datos son una parte crítica de las organizaciones, estos deben ser manejados de la manera más eficiente posible. Su disponibilidad es sumamente vital, y el no contar con un plan de contingencia que les permita continuar sus operaciones si llegaran a suceder imprevistos, sería algo que impactaría de forma negativa a la organización.

Existen condiciones que se deben dar para que un data center funcione de una manera óptima, entre las cuales se pueden resaltar las siguientes: climatización, alimentación eléctrica, cableado estructurado eficiente, sistema contra incendios, controles de acceso y sistemas de vigilancia.

1.1 DEFINICION CONCEPTUAL DEL PROBLEMA

YP Directories es una empresa dedicada a la creación de directorios telefónicos para los Estados Unidos. Cuenta con más de diez años de experiencia y cuatro años estabilidad la República Dominicana. YP Directories cuenta con 300 empleados y labora de lunes a sábados, tanto en horario diurno como nocturno. Esta institución tiene sus instalaciones en Av. República de Colombia #41B de la Ciudad de Santo Domingo. Sus departamentos están distribuidos entre una edificación de siete niveles.

En el centro de datos de la compañía se han detectado inconvenientes que han causado problemas en sus diferentes departamentos. Los problemas identificados han sido los siguientes:

- No existe redundancia de UPS. Si llegara a producirse una falla en este UPS dejaría los departamentos de operaciones sin energía eléctrica y provocaría posibles daños a los equipos y hasta pérdida de información relevante.

- Existen equipos sin garantías, por lo tanto, si uno de estos equipos deja de funcionar, no se tendrá el soporte del proveedor y esto incurrirá en más gastos para la empresa.
- No existe un enlace redundante en la conexión principal a internet, lo que indica que si este enlace falla, se pierde toda la conexión hacia el exterior.
- No existe un sistema de alarma inteligente contra incendio. Si llegase a ocurrir un incendio, esto podría ocasionar pérdidas tanto de activos fijos como de recursos humanos.
- No existen herramientas de monitoreo del estado de los equipos, lo que evita detectar a tiempo un mal funcionamiento que se pueda dar en alguno de ellos.
- No se tienen procesos ni procedimientos documentados sobre la funcionalidad y cambios del data center. Esto podría dar paso a repetir los mismos errores y no tomar medidas correctivas necesarias.
- No se implementa control de calidad en las operaciones del data center. Esto indica que no se tiene un control de los procesos y que TI no sabe qué debe de mejorar en el área.

Se ha detectado que la empresa responde a las problemáticas del data center de forma reactiva, lo cual indica que no se tiene claro cuáles son las normas a seguir, ni cuáles son las buenas prácticas a utilizar para eficientizar y mejorar las operaciones del data center.

1.2 DELIMITACION EN TIEMPO Y ESPACIO

El levantamiento de información se realizará a partir del mes de junio hasta noviembre del 2014. La investigación se realizara en la Ciudad de Santo Domingo en la Empresa YP Directories para determinar las dificultades que presenta el Centro de Datos.

1.3 PREGUNTAS DE INVESTIGACION

1.3.1 GRAN PREGUNTA

- ¿Cuáles son los procesos que se deben implementar de ITIL v3 en el Centro de Datos de la Empresa YP Directories?

1.3.2 SUB-PREGUNTAS

- ¿Qué relación existe entre los procesos del ITIL y los procesos del Data Center?
- ¿Cómo influye ITIL en la calidad de los servicios del Data Center?
- ¿Que tan importante es el suministro de energía en el Data Center?
- ¿Cómo influye el proceso gestión de riesgo en los servicios del Data Center?
- ¿Cuáles son las normas por las cuales debe regirse un Data Center?
- ¿Cuáles serían las ventajas de contar con un plan de contingencia para el Data Center?

2. JUSTIFICACION

La implementación de las mejores prácticas en ITIL v3 juega un papel fundamental en el logro de la calidad y la excelencia en las operaciones de empresas de TI (tecnología informática). Es del desempeño profesional que depende el fracaso o éxito de esta implementación. Siendo uno de los objetivos de la calidad, es prioritario destacar los procesos y metodologías propias para tal fin, sin olvidar que la aplicación de mejores prácticas debe ser considerada como una de las principales políticas del sistema de la empresa. En países como la República Dominicana, la implementación de data center es muy reciente, y es por tanto que en la mayoría de empresas no siguen un esquema de procesos para su uso.

La sociedad está en la actualidad en un momento donde la disponibilidad de los servicios es cada vez más exigente, las peticiones de los clientes o usuarios son más cuantiosas y urgentes y el ritmo de los negocios cambia constantemente. Es indudable la importancia de que las Tecnologías de Información (TI) estén adecuadamente organizadas y alineadas con la estrategia del negocio. ITIL es un camino al logro de este objetivo vital.

A finales de los 80 nació ITIL (Information Technology Infrastructure Library), que se ha convertido en un estándar de facto mundial para la Gestión del Servicio de las

Tecnologías de la Información, proveyendo un conjunto cohesionado de mejores prácticas que abarcan tanto el sector público como el privado. (Brújula, 2008).

Las metas que se deben lograr son: Asegurar que los servicios ofrecido por las TI estén alineados con las necesidades del negocio, aportando valor al mismo, facilitar la toma de decisiones de acuerdo a indicadores de las TI y referentes al negocio. Uno de los beneficios, que brindaría la presente investigación sería el de contar con la mejora en los sistemas, tales como seguridad, fiabilidad, velocidad y disponibilidad como se requiere en el nivel de servicio a ofrecer y así aplicar medidas correctivas con conocimiento de causa para mejorar la utilización de mejores prácticas elevando la calidad del data center en la empresa YP Directories.

3. OBJETIVO GENERAL

- Identificar cuáles son los procesos de las buenas prácticas de ITIL v3 que pueden ser aplicados para la mejora de la calidad de los servicios del Data Center de la Empresa YP Directories en la República Dominicana.

4. OBJETIVOS ESPECIFICOS

- Determinar cuáles son los servicios que ofrece el Centro de Datos.
- Identificar cuáles son los procesos de ITIL v3 que pueden ser aplicados al Centro de Datos para la mejora de la calidad de sus servicios.

- Identificar cómo mejorar el sistema de software de gestión del Centro de Datos.
- Identificar las mejoras que se pueden realizar a los sistemas de seguridad físico y lógico del Centro de Datos.
- Identificar los sistemas de almacenamiento y sus componentes.
- Identificar la oportunidad de mejora existente en la redundancia y el cableado de la red.
- Crear un plan de contingencia efectivo para el Centro de Datos.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

Gestión de Servicios de Tecnologías de la Información (ITSM).

Hoy en día, las organizaciones se encuentran en un clima de negocio bastante competitivo y hacer las cosas bien simplemente no es suficiente y es necesario dar la milla extra. Las empresas dependen mucho de su información y es que de la disponibilidad y precisión de esta dependen decisiones que llevaran al complimiento o no de las metas planteadas. Esto generalmente es logrado con el soporte del departamento de Tecnología de la Información (TI).

Las Tecnologías de Información (TI) son el medio por el cual la información se recoge, administra, almacena, comunica, transforma, visualiza e interpreta,

convirtiéndose así en un elemento que puede dar una ventaja competitiva a las organizaciones.

Es por esto que las empresas generalmente invierten mucho en nuevas tecnologías que soporten y manejen de forma efectiva su flujo de información. Sin embargo, invertir en tecnología de punta no es suficiente si TI no tiene un manejo adecuado ni un control de sus procesos operacionales.

La ISO/IEC 20000, primer estándar internacional para la gestión de servicios de TI, define la gestión de servicios de TI o ITMS (del inglés IT Service Management), de la siguiente manera: *"La gestión de servicios de TI es un enfoque integrado de proceso que permite a una organización de TI ofrecer servicios que satisfagan los requerimientos del negocio y de los clientes."*

A diferencia del enfoque orientado a tecnología tradicional de TI, la gestión de servicios de TI es una disciplina para el manejo de las operaciones de TI como servicio, que es orientado a procesos, y cuenta con el 60% a 90% de los costos de propiedad de TI. Actualmente, los proveedores de servicios de TI ya no pueden enfocarse solo en tecnología y su organización interna, sino que ahora deben de considerar la calidad de los servicios que ofrecen y su relación con los clientes. (GALUP, 2009, p. 124-125).

*V*an Bon et al. (2007) dice que una ventaja importante de una organización orientada a procesos es que estos pueden ser diseñados para apoyar el enfoque

orientado a cliente. Esto hace que se incremente de manera significativa la relación entre relación entre TI, responsable de suministrar la información, y el cliente, responsable de utilizar los sistemas de información.

De acuerdo con Knapp (2010), el enfoque de ITSM es gestionar el ciclo de vida de los servicios de TI. Su alcance no necesariamente incluye manejo de programas o proyectos ni aplicaciones y desarrollo de softwares. Sin embargo, los procesos del ITSM deben de ser diseñados de manera que se integren y alineen con la gestión de proyectos, programas y los procesos de aplicación y desarrollo de software. El uso consistente de procesos bien diseñados e implementados permite a los proveedores de TI:

- Alinear sus esfuerzos con las metas de negocio.
- Asegurar la conformidad con los controles de regulación aplicables.
- Alcanzar la satisfacción del empleado y del cliente.

Biblioteca de Infraestructura de Tecnologías de Información (ITIL).

A menudo, la gestión de servicios de TI, es asociada con La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), del gobierno británico. ITIL se centra en la entrega y soporte del servicio de las operaciones de TI. Aproximadamente el 80% de los costos de una infraestructura se encuentran en estas dos áreas. Por otro lado, al menos el 90% de las compañías en EE.UU tienen una o más implementaciones de un ITSM. (GALUP, 2009).

En los años 80, la calidad de los servicios de TI que prestaba el gobierno británico era tal que se instruyó a la, en ese entonces, CCTA (Agencia Central de Telecomunicaciones y Computación, hoy Ministerio de Comercio, OGC) para que desarrollara una propuesta con el fin de que los ministerios y demás oficinas del sector público de Gran Bretaña utilizaran de manera eficaz y con eficiencia de costes los recursos TI. El objetivo era desarrollar una propuesta sin independiente de todo proveedor. Esto dio como resultado la Information Technology Infrastructure Library (ITIL). ITIL nació de una colección de las mejores prácticas observadas en el sector de servicios de TI. (Van Haren Publishing, 2007).

ITIL proporciona un marco detallado de buenas prácticas de TI con el objetivo de entregar calidad de servicio de TI a un costo justificable. Esto lo hace a través de una series de procesos, roles, tareas, responsabilidades y procedimientos que pueden ser adaptados a cualquier institución.

En mayo del 2007 se lanzó la versión 3 de ITIL la cual consiste en cinco publicaciones y sus procesos relacionados. Las publicaciones incluyen: Estrategia del Servicio, Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio.

Estándares para la Gestión de Servicios de TI

Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido, y que ofrece reglas, guías o características para que se use repetidamente.

El Organismo Nacional de Normalización del Reino Unido es el Instituto de Normalización Británico, que opera bajo un estatuto real desde 1901 para actuar como la organización estándar para el gobierno británico. BS (British Standard) 15000, ratificado en el año 2000, fue el primer estándar del mundo para la gestión de servicios de TI o ITSM. El estándar especifica un conjunto de procesos de gestión relacionados entre sí, los cuales forman parte de la estructura donde los procesos y los sistemas son establecidos y evaluados. BS-15000 está principalmente orientado a las operaciones de TI y basado en ITIL.

ISO/IEC 20000 proporciona un estándar formal y universal para las organizaciones que buscan tener sus capacidades de Gestión de Servicios auditadas y certificadas. Mientras que ISO/IEC 20000 es un estándar para ser alcanzado y

mantenido, ITIL ofrece un cuerpo de conocimientos útil para alcanzar el Elephant, 2013, p.16).

El estándar ISO/IEC 20000 cuenta varias versiones y es el primer estándar internacional para la gestión de servicios de TI. La primera versión es el ISO/IEC 20000-1 (parte 1) y es la versión formal del estándar que define los requerimientos "obligatorios" para la entrega de la calidad de los servicios. Y por otro lado, la parte 2, ISO/IEC 20000-2, que describe las buenas prácticas de la gestión de servicios de TI. (GALUP, 2009).

Otras versiones son: ISO/IEC 20000-3, ISO/IEC 20000-4 Y ISO/IEC 20000-5 y otros más están siendo implementados. (Kunas, 2012, p.18).

Impacto Global de la Gestión de Servicios de TI.

La evolución desde la norma BS-15000 hasta el estándar internacional ISO/IEC-20000 deja claro el avance del ITSM. Según GALUP, (2009) Microsoft dio su opinión acerca del ITSM en una conferencia de TI realizada en el año 2004: *"Estudios recientes demuestran que una organización de TI puede alcanzar hasta un 48% en reducción de costos implementando los principios del ITSM."*

De acuerdo a Forrester Research, *la adopción de ITIL por compañías grandes con ingresos que excede el billón de dólares han crecido de un 13% a un 20% en el año 2006.*

Centros de Procesamiento de Datos y la Seguridad de la Información

La seguridad es un elemento crítico dentro de los sistemas informáticos actuales. García-Cervigón & Del Pilar, (2011) indican lo siguiente: "Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidarnos del peligro que podría acarrear el acceso al sistema de un usuario no autorizado."(p.2)

La seguridad puede ser tanto física (utilizadas para proteger los sistemas informáticos utilizando barreras físicas y mecanismos de control) como lógica (encargada de asegurar la parte software de un sistema informático), dependiendo de la naturaleza de la amenaza. Dentro de los mecanismos de seguridad física se pueden mencionar: UPS, guardias de seguridad del edificio, alarmas, cámaras de seguridad, sistemas anti incendios, extintores, climatizadores, entre otros. Dentro de la seguridad lógica, se tienen programas, o software, como el sistema operativo que se encarga de controlar el acceso de los procesos o usuarios a los recursos del sistema. (García-Cervigón & Del Pilar, 2011).

Los Centros de Datos, requieren tanto la seguridad física como de la lógica, debido a que cada una se encarga de proteger partes diferentes dentro del Centro de Datos.

5.2 MARCO CONCEPTUAL

Estándar: Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido, y que ofrece reglas, guías o características para que se use repetidamente.

Gestión de Servicios: es satisfacer una necesidad sin asumir directamente las capacidades y recursos necesarios para ello.

Flujo de Información: es como la información circula y pasa de un sector a otro.

Servicio: es un medio para entregar valor a los clientes facilitándoles un resultado deseado sin la necesidad de que estos asuman los costes y riesgos específicos asociados.

Procesos: son las fases sucesivas de un fenómeno que ocurren en el transcurso del tiempo, con un objetivo. Es un camino hacia el fin.

Control de Calidad: permite verificar que los productos o servicios ofrecidos por las empresas reúnan las condiciones necesarias para su provechosa, sana y confiable utilización, de acuerdo a lo ofrecido.

Contingencia: El término suele referirse a algo que es probable que ocurra, aunque no se tiene una certeza al respecto. La contingencia, por lo tanto, es lo posible o aquello que puede, o no, concretarse.

Climatización: consiste en crear condiciones de temperatura, humedad y limpieza adecuadas para la comodidad dentro de un espacio en específico y la satisfacción de una determinada necesidad en el proceso.

Sistema: es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo.

Redundancia: describe lo que abunda o es excesivo frente a una cosa o contexto.

Conexión: es un enlace o una atadura que une una cosa con otra.

Servidores: es una computadora que forma parte de una red y que provee servicios a otros ordenadores, que reciben el nombre de clientes.

ITIL: es un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI.

ITSM: La gestión de servicios de tecnologías de la información es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final.

Centro de Procesamiento de Datos: es aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

6. HIPOTESIS

El Centro de Datos de la empresa YP Directories ofrecerá mejor calidad de servicio si se implementan las mejores prácticas de ITIL v3.

7. DISEÑO METOLOGICO

7.1 METODO

Los métodos a utilizar en el proyecto de investigación serán:

- La observación, ya que se va a observar directamente el funcionamiento actual del Centro de Datos de la empresa YP Directories.

- Análisis, ya que se identificaran las partes que forman parte del problema así como su relación causa-efecto entre los elementos relacionados con la investigación.

- Método inductivo, ya que el problema de investigación estará basado en problemas específicos que presenta el Centro de Datos.

7.2 TECNICAS

Las técnicas de investigación de recolección de datos que se utilizaran en el proyecto de investigación serán entrevistas, cuestionarios y la observación. De esta forma se podrá obtener datos confiables que servirán como soporte para la investigación y permitirán dar las recomendaciones de lugar para la mejora de la calidad de servicio del Centro de Datos de la empresa YP Directories en la República Dominicana.

7.3 TIPO DE ESTUDIO

El tipo de estudio que se implementará durante la realización de este proyecto es de carácter descriptivo-explicativo porque ayudarán a analizar y ver cuáles son factores que afectan la calidad de servicio del Centro de Datos de la empresa YP Directories en la República Dominicana.

8. ESQUEMA PRELIMINAR DE TRABAJO DE GRADO

Dedicatorias

Introducción

Capitulo I. Conceptos Generales

1.1 Breve historia de la Empresa YP Directories
1.2 Misión
1.3 Visión
1.4 Valores

Capitulo II. Conceptos Generales de Centro de Datos

2.1 Conceptos de Centro de Datos

2.1.1 Definición de Centro de Datos

2.1.2 Objetivos

2.1.4 Elementos

2.1.5 Espacio

2.1.6 Diseño

2.1.7 Importancia

2.2 Tipos de Centro de Datos

2.2.1 De nivel: 1Bàsico (Tier 1)

2.2.2 Nivel 2: Componentes Redundantes (Tier 2)

7.4 Ventajas

7.5 Desventajas

Presentación y análisis de los resultados

Conclusión

Recomendación

Bibliografía

9. FUENTES DE DOCUMENTACION

Pink Elephant (2013). *Gestión de Servicios de TI*. Canada: Pink Elephant.

GALUP, S.(2009). An Overview of IT Service Management. Communications Of The ACM, 52(5), 124-127.

Van Bon et al. (2007). *Service Operation based on ITIL V3-A Management Guide.* Amersfoort: Van Bon Publishing.

Knapp, D. (2010). *ITSM Process Design Guide: Developing, Reengineering, and Improving IT Service Management.* Florida: J. Ross Publishing, Inc.

Kunas, M.(2012). *Implementing Service Quality based on ISO/IEC 2000: A Management Guide*.UK: IT Governance Publishing.

García-Cervigón & Del Pilar. (2011). *Seguridad Informática*. Madrid, España: Ediciones Paraninfo, SA.

ITC Group. (2013). *Data Center Llave en Mano*. Recuperado de: http://www.itcgroup.us/index.php/soluciones/datacenters/llave-en-mano/datacenter-llave-en-mano

ANEXO II – ENCUESTAS

FORMULARIO CUESTIONARIO DE ANALISIS DE IMPACTO AL NEGOCIO

Empresa: YP DIRECTORIES **Encuestador:** Edward Rodríguez **Fecha:**

Encuestado: **Departamento:**

Parte I: Encuesta a realizar a los Gerentes Departamentales de YP DIRECTORIES

1. ¿Cuál es el cargo que ocupa en la empresa?

2. ¿Cuál es el proceso de negocio principal que desempeña su departamento?

3. ¿De cuáles de las aplicaciones o servicios de TI depende su proceso de negocio?

• Servidores	Sistema CORE	Sistema de Programa Maestro
• Correo Electrónico	Sistema de Nómina	Sistema de Correcciones
• Internet	Gestor de Reportes	Sistema de Prueba Electrónica

- Intranet
- Sistema de Gestión de Empleados
- Sistema Paginación
- Telefonía
- Sistema Indexador de Contratos

- Generador Precios del Mercado
- Backup
- Sistema de Consultas a la TELCO
- Sistema de Gráficos
- Sistema de Reembolso
- Sistema de Registro Auditoría+
- Sistema de pago a Suplidores
- Sistema de Envío de Directorios a Printer
- Soporte técnico a escritorio

4. ¿Cuál es el Tiempo Máximo que su proceso de negocio puede estar inactivo antes de que esto cause un daño significativo al negocio (RTO)?

5. ¿Cuál es el Tiempo Máximo de Información que está dispuesto a perder si ocurriese un siniestro (RTO)? (ejemplo, terremotos, incendios, inundaciones, caída de la red)

6. ¿Cuál departamento es su cliente interno?

7. En términos monetarios, ¿Qué cantidad de dinero podría perder la empresa si su proceso de negocio estuviera interrumpido por causa de siniestros u otros eventos negativos?

8. ¿Con cuántas personas cuenta su departamento?

Parte II: ENCUESTA A REALIZAR AL GERENTE DE TECNOLOGIA YP DIRECTORIES

1. ¿Cuenta el departamento de TI con un Plan de Continuidad de Servicios de TI?

2. ¿Cuál es el tiempo estipulado para resolver las emergencias?

3. ¿Cuáles son los servicios que ofrece el departamento de TI?

4. ¿Cuáles son los tiempos de recuperación para las aplicaciones y servicios de TI?