FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

EVALUACIÓN DE RECUPERACIÓN ANTE DESASTRES EN LA INFRAESTRUCTURA TECNOLÓGICA DE COCESNA

SUSTENTADO POR:

LUZ MARIEL GONZALES ESPINAL

OSCAR ROLANDO VILLELA MOLINA

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

JULIO, 2014

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

LUIS ORLANDO ZELAYA MEDRANO

SECRETARIO GENERAL

JOSÉ LÉSTER LÓPEZ

VICERRECTOR ACADÉMICO

MARLON BREVÉ REYES

VICERRECTORA CAMPUS SPS

ANA LOURDES LAFFITE

DECANO DE LA FACULTAD DE POSTGRADO

DESIREE TEJADA

EVALUACIÓN DE RECUPERACIÓN ANTE DESASTRES EN LA INFRAESTRUCTURA TECNOLÓGICA DE COCESNA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE MÁSTER EN GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ASESOR METODOLÓGICO
JUAN JACOBO PAREDES HELLER

ASESOR TEMÁTICO
JUAN ALBERTO SOLANO

COMISIÓN EVALUADORA:
NANCY URBINA
CLAUDIO ARCHILA

EVALUACIÓN DE RECUPERACIÓN ANTE DESASTRES EN LA INFRAESTRUCTURA TECNOLÓGICA DE COCESNA

AUTORES:

Luz Mariel Gonzales Espinal y Oscar Rolando Villela Molina

RESUMEN

Un desastre dentro de una organización puede significar muchas cosas, desde una pérdida importante de datos hasta un desastre natural que destruye la infraestructura tecnológica de la organización. Cualquier evento que cause una interrupción en la operación normal del negocio se considera un desastre, sin un plan efectivo para la recuperación ante desastres la mayoría de las organizaciones no se recuperan. El objetivo de la investigación fue proponer una estrategia de recuperación que permitiera minimizar los tiempos fuera de los servicios críticos de la infraestructura tecnología del área administrativa de COCESNA. Con un enfoque de investigación mixto, se utilizaron herramientas cualitativas y cuantitativas para comprobar la validez de la hipótesis propuesta, el estudio involucro el desarrollo de encuestas a ocho expertos dentro de la empresa y entrevista con el jefe de infraestructura informática. En el análisis de resultados del presente estudio se concluyó que el RTO es de 24 horas y el RPO es mayor a 40 minutos en caso de desastre. Para reducir estos tiempos fue necesario contar con un sitio alterno en donde la información crítica de la empresa se estuviera replicando cada hora en una plataforma ubicada en la ciudad de San Salvador, El Salvador. Reduciendo significativamente el RTO a una hora y el RPO menor a 40 minutos.

Palabras clave: recuperación ante desastres, rto,rpo, sitio alterno,respaldo datos

EVALUATION OF DISASTER RECOVERY IN TECHNOLOGICAL INFRASTRUCTURE OF COCESNA

BY:

Luz Mariel Gonzales Espinal y Oscar Rolando Villela Molina

ABSTRACT

Any type of disaster within an organization can mean many things, from a major data loss to the destruction of technological infrastructure of the organization. Any event that causes an interruption in the normal operation of the business is considered a disaster, without an effective plan for disaster recovery, most organizations do not recover. The objective of the research was to propose a recovery strategy that would minimize time outside critical infrastructure services technology for COCESNA administrative area. With a hybrid approach to research, qualitative and quantitative tools were used to check the validity of the proposed hypothesis, the study involved the development of surveys to eight experts within the corporation and interview with the head of IT infrastructure. The study results showed that the RTO is 24 hours and the RPO is greater than 40 minutes in case of disaster. To reduce both period of times it was necessary to have an alternate site where critical business information could be re derationed anytime it was needed. Today, COCESNA counts with an alternate site located in the city of San Salvador, El Salvador. This site has significantly reduced our RTO to an hour and the RPO to less than 40 minutes.

Key words:disaster recovery, rto,rpo, alternate site, data backup

DEDICATORIA

A Dios, que es el dador de vida, quien se derrama por medio del Espíritu Santo llenando con sus dones de sabiduría, entendimiento y fortaleza.

A mis padres, quienes han sido mi apoyo incondicional Cristina Espinal y Joaquín Gonzales por impulsarme hacia nuevas metas y confiar en alcanzarlas

A mis hermanas y sobrinos que son parte de mi familia que me acompañan y comparten día a día conmigo.

A mi abuela Ana Rosa, quien ya goza de la gloria del señor, por siempre creer en mí hasta su último día.

Luz Mariel Gonzales Espinal

A Dios quien supo guiarme por el buen camino, darme fuerza para seguir adelante y no desmayar ante las adversidades presentadas.

A mi esposa Alexandra Cerna que me ha brindado su apoyo y comprensión durante este tiempo, a mis hijos Oscar y Camila que son la fuente de mi inspiración para seguir adelante.

A mis padres, hermanos y sobrinas que siempre han estado apoyándome en los buenos y malos momentos de mi vida.

Oscar Rolando Villela Molina

AGRADECIMIENTO

A Jesucristo nuestro Señor y dador de vida, por guardarnos en todo tiempo, por darnos la fortaleza y guía en todo momento para seguir adelante.

A nuestras familias por su amor incondicional, comprensión y apoyo.

A UNITEC por contribuir a la formación de nuevos profesionales y facilitar el desarrollo de nuestra profesión.

Al Dr. Juan Jacobo Paredes por su guía y asesoría durante el proceso de elaboración de la tesis e investigación.

A la Corporación Centroamericana de Servicios de Navegación Aérea por brindarnos la oportunidad de poder aplicar nuestros conocimientos en el desarrollo del presente estudio.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

En este capítulo se describe el planteamiento de la investigación el cual consta de: introducción, antecedentes, definición del problema y en base a estas se logra tener una definición de las preguntas de investigación y cuáles serán los objetivos que se pretenden comprobar. Al final se realiza una justificación sobre el problema que se plantea en el presente estudio.

1.1 INTRODUCCIÓN

Los planes de recuperación de desastres (DRP) describen los pasos a seguir para recuperar y restaurar las operaciones más importantes de los elementos que forman parte de la infraestructura de tecnologías de información. Entre estos elementos se incluyen las redes de datos, servidores, centros de datos, sistemas operativos, aplicaciones y los datos de las operaciones indicadas, contiene los procedimientos necesarios para una adecuada gestión de riesgos pudiendo con esto mitigarlos o transferirlos a algún tercero.

El proceso de gestión de la continuidad del negocio debe identificar riesgos, emergencia, y la planificación de la recuperación para determinar si una organización será capaz de gestionar una crisis o desastre y poder continuar con sus operaciones habituales comenzando con las más prioritarias. La reanudación de negocios, recuperación de desastres y los planes de continuidad están siendo apreciados por aquellas organizaciones que han sufrido un desastre, lograron ejecutar de buena forma el respectivo plan, y lograron mitigar o neutralizar la amenaza (Doughty, 2001).

Hoy en día, los DRP ya no son un lujo, sino un elemento esencial del programa de gestión de riesgos de la organización. Cada DRP tiene un límite en su acción a ejecutar, un plan no podrá manejar algunos desastres, y esto es perfectamente válido. Sin embargo, también es verdad que muchos DRP se pueden ampliar para cubrir desastres mayores, situaciones que afectan a zonas más amplias, que duran más

tiempo y que, generalmente, son más graves que los planificados para casos de contingencias; requiriendo la inversión monetaria y aplicación de los procesos correspondientes para que se lleven a la práctica. Se cree que algunas empresas gastan hasta el 25 % de su presupuesto en proyectos de recuperación de desastre, sin embargo, esto lo hacen para evitar pérdidas más grandes. De las empresas que tenían una pérdida principal de registros automatizados el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años, y sólo el 6 % sobrevivirá el largo plazo (Hoffer, 2001).

Los planes apropiados varían de una empresa a otra, en función de variables como el tipo de negocio, los procesos involucrados, y el nivel de seguridad requerido. La planificación de la recuperación de desastres debe ser desarrollada dentro de una organización pudiéndose comprar una aplicación de software o por medio de una consultoría (Op.Cit.).

A pesar de contar con algún grado de aceptación por parte de la industria con temas relacionados a la recuperación de desastres, aun la mayoría de las empresas todavía están mal preparadas para afrontar un desastre.

> A pesar del número de desastres conocidos desde el 9/11, sólo el 50% de las empresas informan que tienen un plan de recuperación de desastres. De aquellos que sí lo tienen, casi la mitad nunca han puesto a prueba su plan, lo que equivale a no tener ninguno.(Margaret Rouse, 2013.)

En cualquier entorno en el que se haga uso de la tecnología es necesario estar protegido de las diferentes amenazas, detección de vulnerabilidades, garantizando el cumplimiento de las siguientes características (ISO, 2000):

1) Integridad: Asegurar la exactitud y totalidad de los datos.
2) Confidencialidad: Información accesible solo a las personas con cierto grado de autorización.

3) Disponibilidad: Tener acceso a los recursos y datos en el momento que se requiera.

El objetivo que se pretende con la presente investigación es la de proponer una estrategia de recuperación ante desastres que permita reducir el impacto negativo de situaciones que se puedan presentar y que puedan afectar el correcto funcionamiento de los sistemas de información y comunicación de la Corporación Centroamericana de Servicios de Navegación Aérea (COCESNA).

1.2 ANTECEDENTES DEL PROBLEMA

COCESNA es un organismo internacional de integración centroamericana cuya sede se encuentra en Honduras y cuenta con oficinas regionales en: Belice, Guatemala, Nicaragua, El Salvador y Costa Rica. Fue fundada en febrero de 1960, el giro principal del negocio es la prestación de servicios de navegación aérea en toda la región centroamericana. Cuenta con más de 400 empleados distribuidos en las diferentes oficinas regionales, el personal técnico-operativo labora las 24 horas los 365 días del año mediante la modalidad de turnos.

Para el apoyo de las operaciones de tránsito aéreo en la región COCESNA cuenta con departamentos administrativos como ser: Recursos Humanos, Gerencia Administrativa, Gerencia de Tecnología, Proveeduría así como un departamento técnico encargado directamente de los equipos y sistemas que soportan el seguimiento radar de los vuelos en toda la región centroamericana. El área de responsabilidad de COCESNA para brindar el servicio de tránsito aéreo es de 2,934,357 km² (Locandro, 2014).

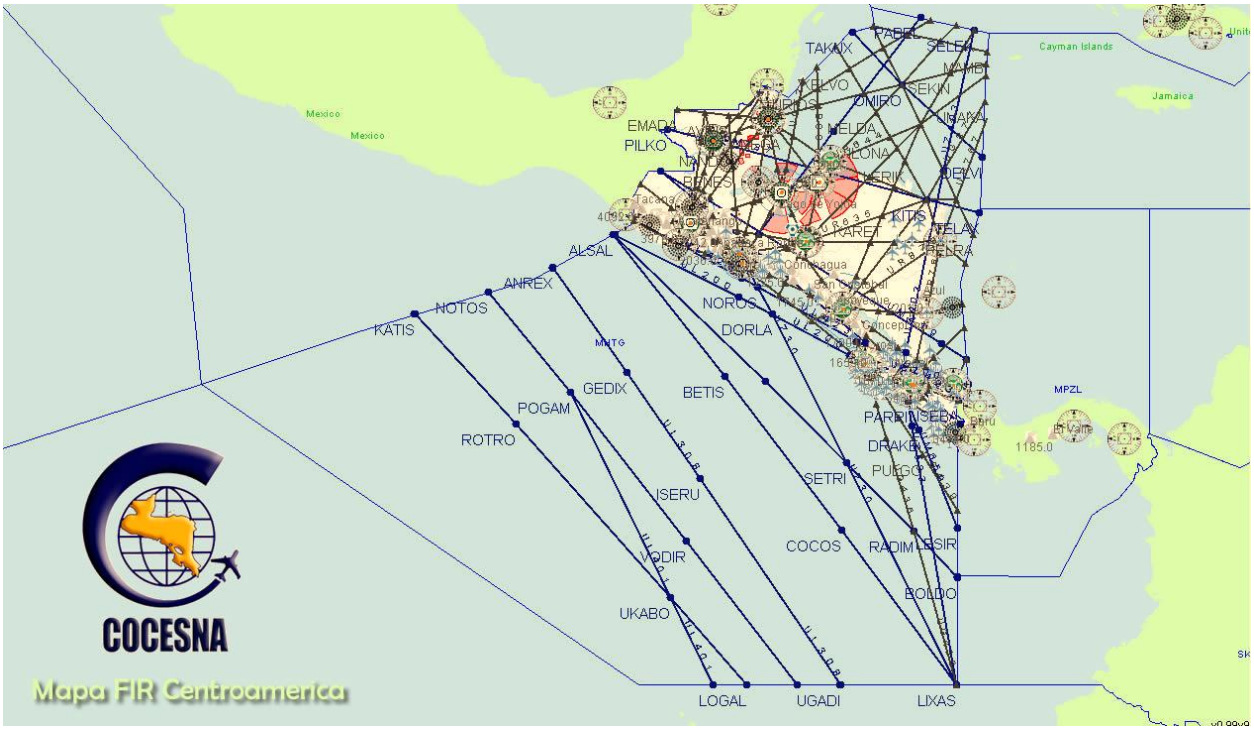

Figura 1. Área de cobertura del espacio aéreo responsabilidad de COCESNA
Fuente: COCESNA

Las operaciones diarias de vuelo a las cuales se les brinda el servicio de tránsito aéreo aproximadamente es de 400 vuelos y al mes se estiman 12,600 vuelos que cruzan por el área de cobertura. Los temas tecnológicos dentro de la empresa son manejados por la gerencia de tecnología para todo lo relacionado con las operaciones administrativas y por la gerencia de estación Honduras que se encarga de administrar el centro de datos y dar soporte técnico directamente al centro de control radar. Ambas unidades manejan información crítica para las operaciones de COCESNA.(Sánchez, 2014)

La Gerencia de Tecnología es la encargada de establecer las políticas y normativas de seguridad de la información a nivel corporativo y la responsable del funcionamiento óptimo de la plataforma tecnológica. Dentro de la Gerencia de TI se tienen identificados algunos elementos o funciones que pudieran ser críticos al momento de presentarse una eventualidad dentro de la Corporación. Se tiene declarado un plan de contingencias ante desastres el cual fue elaborado en el año 2007 y no ha tenido

ninguna actualización por lo cual la información definida en dicho plan ha quedado totalmente obsoleta ya que dentro de la empresa han existido cambios en la arquitectura hardware, actualizaciones de sistemas y rotación de personal.

En la tabla 1, se muestran las operaciones que se han tenido en la cobertura del espacio aéreo correspondiente a COCESNA durante el periodo 2010-2013. Durante este periodo la cantidad de operación ha ido en crecimiento con un promedio de 5.85% anual, llegando a tener a diciembre del 2013 un total de 167,329 operaciones en toda la región de vuelo, lo que a su vez supone un incremento de la cantidad de información que se genera dentro de la corporación.

Tabla 1. Operaciones de vuelos 2010-2013 de COCESNA

Movimientos de Operaciones en la FIR CENTROAMERICANA Datos COCESNA Fecha de Elaboración Enero 2014								
	Número de Operaciones				Incremento %			Promedio Incremento mensual 2010 - 2013
Mes	Año 2010	Año 2011	Año 2012	Año 2013	Año 10-11	Año 11-12	Año 12-13	
Enero	12,695	12,904	13,708	15,040	1.65%	6.23%	9.72%	5.86%
Febrero	11,152	11,387	12,852	13,363	2.11%	12.87%	3.98%	6.32%
Marzo	12,548	12,822	13,980	14,981	2.18%	9.03%	7.16%	6.13%
Abril	11,634	12,264	14,164	13,863	5.42%	15.49%	-2.13%	6.26%
Mayo	11,211	12,073	13,173	13,495	7.69%	9.11%	2.44%	6.41%
Junio	11,540	11,990	13,632	13,795	3.90%	13.69%	1.20%	6.26%
Julio	12,822	13,187	14,635	14,659	2.85%	10.98%	0.16%	4.66%
Agosto	12,481	12,771	13,956	14,220	2.32%	9.28%	1.89%	4.50%
Septiembre	10,476	11,031	11,087	12,116	5.30%	0.51%	9.28%	5.03%
Octubre	10,864	11,370	12,656	12,676	4.66%	11.31%	0.16%	5.38%
Noviembre	11,223	11,850	12,814	13,600	5.59%	8.14%	6.13%	6.62%
Diciembre	12,571	13,786	14,570	15,521	9.67%	5.69%	6.53%	7.29%
Anual	**141,217**	**147,435**	**161,227**	**167,329**	**4.40%**	**9.35%**	**3.78%**	**5.85%**

Fuente:(COCESNA, 2014).

El volumen de datos diario que se almacena dentro de la corporación es de alrededor de 4GB diarios, en el cual se encuentran documentos, base de datos, y archivos que son de uso de los diferentes usuarios que cuentan con la facilidad de respaldar sus

datos, el tamaño total de este respaldo es de aproximadamente 500GB. Adicionalmente a la información descrita anteriormente se realizan respaldos de información de las diferentes máquinas virtuales que se tiene configuradas para la operación de los servicios, el tamaño de este respaldo tiene un aproximado de 2TB, el cual es almacenado en la nube mediante la herramienta dropbox (Zavala, 2014).

El procedimiento que sigue el personal de soporte técnico para la realización de los respaldos es de manera incremental de forma diaria. Una copia de los datos respaldados se almacena en un servidor y otra copia se envía a la nube. Aun y cuando se tiene conocimiento de las posibles amenazas a los sistemas críticos no se tiene definido el tiempo máximo que puede quedar este fuera de servicio (Op.Cit.).

1.3 DEFINICIÓN DEL PROBLEMA

A continuación se detallan los componentes necesarios para una correcta definición del problema.

1.3.1 ENUNCIADO DEL PROBLEMA

La información y el conocimiento en el que se basa la Corporación Centroamericana de Servicios de Navegación Aérea (COCESNA), se ha vuelto uno de los activos más importantes sin el cual sería casi imposible dirigir el negocio y prestar los servicios. Los sistemas y procesos que manejan información, junto con la tecnología asociada y las instalaciones, se han vuelto factores diferenciadores. Esto implica directamente una creciente dependencia sobre la gestión de seguridad de la información.

Por lo anterior, la seguridad de la información se considera un elemento fundamental en la organización, ya que permite el resguardo de los datos logrando mantener la integridad, calidad y disponibilidad mediante el establecimiento de métricas, políticas y directrices se puede lograr aplicar mecanismos que ayuden a minimizar los impactos de una incorrecta gestión de riesgos.

En la actualidad no se cuenta con un plan de contingencia actualizado que permita estar preparados contra desastres de tipo informático o algún otro que se pudiera presentar en las operaciones del área administrativa de la corporación.

1.3.2 FORMULACIÓN DEL PROBLEMA

Las tecnologías de información y comunicaciones (TIC'S) representan una gran variedad de oportunidades así como grandes amenazas, por lo que es recomendable tener establecido procesos que ayuden a identificar estas amenazas así como su impacto en la organización . En vista que dentro de COCESNA se hace uso de las TIC'S como soporte a las operaciones no se encuentra exenta de poder sufrir algún tipo de ataque informático o ser afectado por cualquier tipo de desastre.

En base a lo descrito anteriormente, se formula la siguiente pregunta:

¿Cuál es la estrategia de recuperación de información (en términos de punto y tiempo de recuperación) ante la presencia de algún tipo de desastre que se pueda presentar en los equipos que están instalados en el centro de datos de la Corporación Centroamericana de Servicios de Navegación Aérea durante el año 2014?

1.3.3 PREGUNTAS DE INVESTIGACIÓN

A continuación se enuncian las preguntas de investigación que se estarán utilizando para evaluar el presente estudio.

1) ¿Cuál es la frecuencia de actualización de los planes de contingencia?

2) ¿Cuál es el tiempo máximo permitido para tener fuera de servicio las aplicaciones?

3) ¿Cuál será la mejor ubicación estratégica para contar con un sitio alterno de respaldo de las operaciones del negocio?

4) ¿Cómo se lleva a cabo la gestión de los riesgos?

5) ¿Cuál es el costo que tiene la empresa al no poder tener en funcionamiento sus aplicaciones críticas?

6) ¿Cuál es el tiempo máximo que se tendrán almacenados los respaldos de datos?

1.4 OBJETIVOS DEL PROYECTO

A continuación se detalla cual será el objetivo general y los específicos que se pretenden corroborar en el desarrollo del presente estudio.

1.4.1 OBJETIVO GENERAL

El objetivo general de esta investigación es el siguiente:

“Proponer una estrategia de recuperación (en términos de punto y tiempo de recuperación) ante cualquier tipo de desastre que permita minimizar los tiempos fuera de servicios críticos dentro de la Corporación Centroamericana de Servicios de Navegación Aérea”.

1.4.2 OBJETIVOS ESPECÍFICOS

A continuación se describen los objetivos específicos del tema en estudio:

1) Identificar el tiempo máximo de recuperación de la información, pérdidas monetarias, ubicación del sitio alterno y el periodo de tiempo de actualización del DRP.

2) Determinar los riesgos posibles que puedan afectar las operaciones de la infraestructura tecnológica de la empresa.

3) Analizar costo/beneficio de contar con un plan de recuperación de desastres dentro de la empresa.

1.5 HIPÓTESIS Y/O VARIABLES DE INVESTIGACIÓN

Tras determinar el problema de investigación, se procede a la formulación de la o las hipótesis. En esta sección buscaremos explicaciones tentativas de la relación entre dos o más variables que intervienen dentro de la investigación, pero al final lo determinara el tipo de investigación.

1.5.1 HIPÓTESIS

A continuación se presenta la hipótesis de investigación e hipótesis nula del presente estudio.

Hi: El tiempo máximo de recuperación de la información se ve afectada por el manejo de los riesgos, accesibilidad de los servicios, respaldo de datos, costos y ubicación.

Hø: El tiempo máximo de recuperación de la información no se ve afectada por el manejo de los riesgos, accesibilidad de los servicios, respaldos de datos, costos y ubicación.

1.5.2 VARIABLES DE INVESTIGACIÓN

“Una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse. Las variables adquieren valor para la investigación científica cuando llegan a relacionarse con otras variables, es decir forma parte de una hipótesis o teoría”. (Sampieri & Collado, 2010, p. 93)

En la figura 2, se pueden observar las variables definidas para el presente estudio.

Figura 2. Variables de estudio

"La Variable dependiente no se manipula, sino que se mide para ver el efecto que la manipulación de la variable independiente tiene en ella. (Op.Cit.)

Tabla 2 Variables de investigación

Variable	Descripción	Unidad de Análisis y Medición	Indicador
Actualización	Indica las veces en que sucede un hecho en un determinado periodo de tiempo.	Período de tiempo en el cual se realizarán actualizaciones la estrategia de recuperación de la información	Meses
Respaldos	Período en que se mantendrán los datos en los respectivos respaldos	Tiempo máximo que se tendrá almacenada información de respaldo de las aplicaciones.	Meses
Accesibilidad	Período determinado en el cual sucede algo que imposibilita brindar un servicio	Tiempo de inoperatividad de los servicios	Horas
Ubicación	Localización física en donde se podría ubicar un data center de respaldo	Identificar lugar adecuado para respaldar el data center	Espacio Físico
Manejo de Riesgos	Identificación de posibles riegos que podrían afectar las operaciones del negocio para realizar planes de mitigación.	Estudio de los riesgos que afectan el negocio y los potenciales que podrían causar algún tipo de daño	% de Riesgos mitigados
Costos	Costos que deberá asumir la empresa como perdida al no poder operar con normalidad	Costo de no operación	Valor en dólares americanos

1.6 JUSTIFICACIÓN

El tema de investigación se basa en la importancia de contar con una estrategia de recuperación de la información en caso que se presente algún tipo de desastre, sea este de tipo informático o cualquier otro que pueda afectar la operatividad del negocio. La dependencia tecnológica que existe en COCESNA pone de manifiesto la necesidad de respaldar toda la información catalogada como importante y poder anticiparse a los ataques o posibles desastres que se puedan presentar en el centro de datos ocasionando la no operatividad de sus sistemas.

Es importante poder determinar cuáles son las vulnerabilidades que se pueden presentar y en base a ello poder tener una efectiva gestión de riesgos que conlleve a la generación de planes de acción para poder mitigar los mismos, pudiendo con esto minimizar las pérdidas que puede incurrir la empresa al detener su funcionamiento operacional y técnico. Considerando que una interrupción prolongada en las TIC'S puede suspender las continuidad del negocio o incluso llegar a cerrar operaciones es de suma importancia contar con una estrategia bien diseñada que permita a la empresa su continuidad en la prestación de servicios. Cabe recordar cuanto mayor es el tiempo que se toma para recuperar la operatividad de la empresa, las perdidas monetarias son elevadas.

En vista de lo expuesto anteriormente es necesario proponer una estrategia de recuperación ante desastres que permita minimizar los tiempos fuera de servicios críticos dentro de COCESNA.

CAPÍTULO II MARCO TEÓRICO

En el presente capítulo se realiza una sustentación teórica del estudio más conocido como marco teórico. En este estudio se presenta un enfoque del macro entorno, micro entorno y un análisis interno de la empresa, todo esto permite tener una mejor comprensión del tema en estudio. Así mismo se exponen las teorías, las conceptualizaciones que se consideran idóneas para la correcta delimitación del estudio.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

A continuación se hace un análisis sobre el entorno en el cual está planteado el problema de estudio en esta investigación analizando el entorno en tres niveles: a nivel mundial, a nivel de país y dentro de la organización objeto de estudio.

2.1.1 ANÁLISIS MACROENTORNO

El concepto de plan de continuidad del negocio se empieza a utilizar alrededor de los años 70's. Durante todo este tiempo no había sido un tema tan importante en las empresas, es hasta los eventos ocurridos en septiembre 11 del año 2001 en las torres gemelas de New York, debido a que la magnitud del evento dejo sin operación a muchas de las empresas del sector financiero que se encontraban instaladas en el lugar y cuya estrategia de recuperación se encontraba en ocasiones en la otra torre.(Aristizábal, 2011)

En las empresas los planes de contingencia deben ser considerados parte integral de una estrategia del negocio, "1 de cada 2 empresas en el mundo ha tenido la experiencia de algún tipo de eventualidad o desastre; 40% de estas desaparece inmediatamente o pocos años después del desastre." (Cabrera & Martínez, 2008)

Los planes de contingencia pueden aplicar a cualquier tipo de empresa independiente del rubro al que esta se dedique, pero los sectores en donde se encuentran definidos dichos planes son el sector del comercio al detalle, financiero, telecomunicaciones, manufactura, industrial, de servicios y automotriz. La mayoría de las empresas a nivel mundial e independiente del sector en el que se ubiquen pueden ser afectadas por cualquier tipo de interrupción que provoque inconvenientes negativos (Op.Cit.).

En la figura 3, se puede observar que las interrupciones que afectan en gran medida a las empresas son los fallos en la electricidad como el factor más determinante con un 59.07% seguido por las fallas en el hardware con un 51.04%.

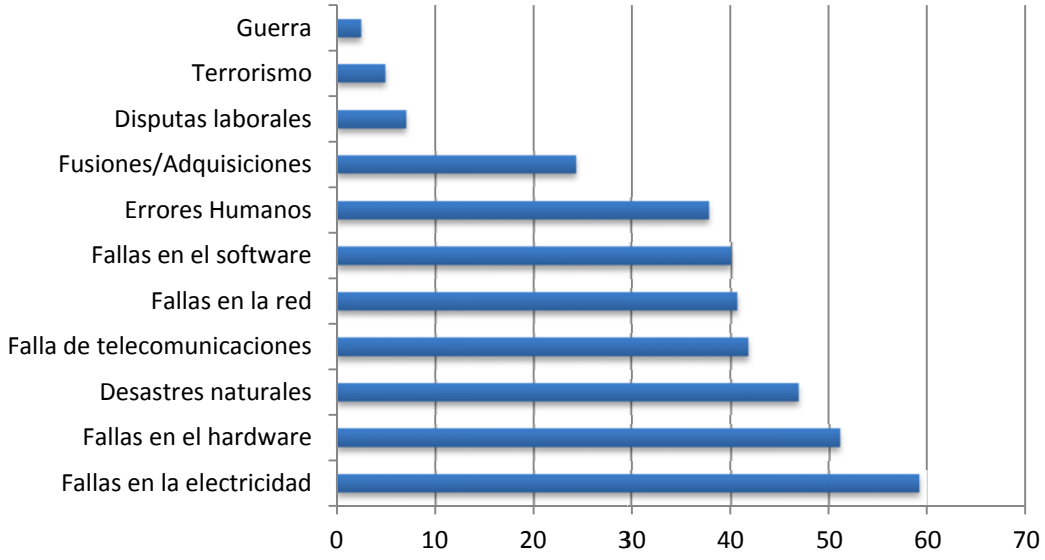

Figura 3. Interrupciones que afectan a los negocios

Fuente:(Cabrera & Martínez, 2008).

Teniendo en consideración el elevado uso de las tecnologías como un medio de soporte a las operaciones de las empresas las mismas se ven afectadas en gran medida cuando se presenta cualquier tipo de interrupción y se vuelve más crítica si no se cuenta con los respectivos planes de contingencia.

> Ante las crecientes amenazas a la seguridad de la información, las organizaciones en todo el mundo están fallando en su protección. Aunque los más altos responsables de las compañías están cada vez más concientizados de los riesgos a los que está expuesta su información, no actúan consecuentemente (Ernest & Young, 2004).

Algunas estadísticas que se tiene acerca del impacto que han causado algunos desastres independientemente de su naturaleza (Robertson, 1997):

1) El gasto en recuperación por desastres en 1995 fue de aproximadamente $3.1 billones y se estimó que crecería anualmente un 20%.
2) Cada desastre tardo en promedio 4 horas para recuperarse y produjo pérdidas en promedio de $329,000.00.
3) El sector financiero es el que tiene la mayor cantidad de empresas con planes de recuperación, cerca del 70% contra un 50% de las compañías de bienes y consumos y un 43% de las compañías de seguros.
4) En promedio cada hora fuera de servicio les costó a las empresas aproximadamente $78,000.00.
5) El 60% de las compañías afectadas salieron del mercado en los siguientes años.

Tomando en cuenta las consecuencias que podría tener la ocurrencia de cualquier desastre en las empresas nace el concepto de los planes de recuperación ante desastres, los cuales consisten básicamente en acciones para recuperarse en caso de presentarse un desastre. Dentro de dicho plan se incluye una adecuada gestión de riesgos. Dichos planes son aplicables para cualquier tipo de negocio (Sandhu, 2002).

Como se explicó anteriormente el sector financiero cuenta con mayores regulaciones concernientes a los planes de recuperación ante desastres, el comité de Basilea responsable de dictar pautas al sector financiero a nivel mundial estableció la creación

de algunos principios algunos de los cuales se describen a continuación (J. Martínez, 2004):

1) Principio 7: «Los Bancos deben disponer de planes de contingencia y de continuidad de negocio para asegurar su capacidad de operar de forma continuada y limitar las pérdidas en el supuesto de una interrupción grave».
2) Principio 9: «Las autoridades de supervisión deben realizar de forma regular, directa o indirectamente, evaluaciones independientes de las políticas, procedimientos y prácticas de los Bancos con relación a los riesgos operacionales.» Como ejemplos incluye: «La calidad y amplitud de los planes de recuperación ante desastres y de continuidad de negocio de los Bancos».

Otras legislaciones vigentes en el sector financiero mundial son los siguientes (Op.Cit.):

1) Argentina: El banco central en un comunicado A-3198 con fecha del 12 de Diciembre del 2000, indica que todas las entidades bancarias deberán contar un plan de contingencias de los centros informáticos.
2) México: La circular 1506/2001 habla sobre los planes de contingencia cuyo funcionamiento deberá ser sometido regularmente a pruebas.
3) Chile: La superintendencia de bancos publico la circular 3043/2000 que exige un plan de contingencias de los centros informáticos de las entidades bancarias.

Como se puede observar en la figura 4, uno de los mayores retos para la realización de copias de seguridad de los datos es la falta de recursos de TI, En segundo lugar está la opinión que tienen algunas empresas las cuales suponen que si previamente no se han tenido pérdidas de datos no lo ven como posible amenaza. En un tercer lugar se ubica la falta de presupuesto en las empresas.

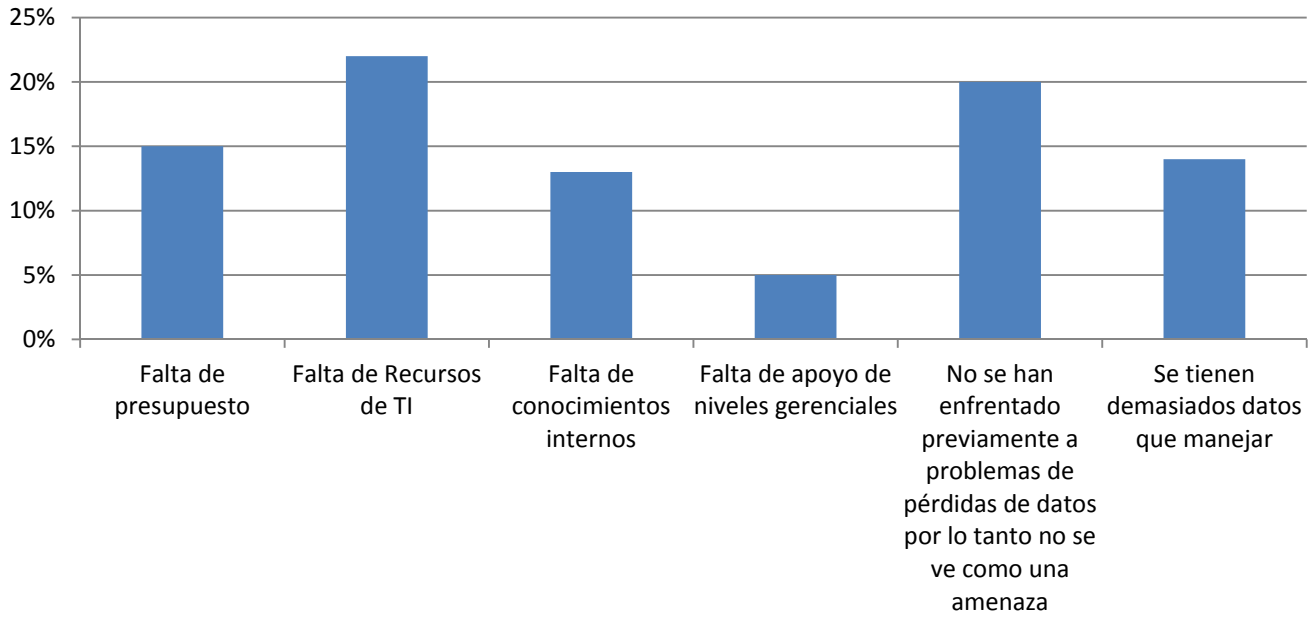

Figura 4. Retos respecto a copias de seguridad y la recuperación ante desastres

Fuente: Acronis Global Disaster, 2012.

Según un estudio realizado por la Cámara de Comercio de Londres, el 90% de las empresas que sufren una pérdida de datos importantes desparece del mercado en el plazo de dos años.

> La consultora Aberden Group realizo un estudio en el cual indica que el costo medio por cada hora de interrupción de servicios en una empresa europea andaba alrededor de los 110,000.00 euros. La empresa de seguridad Symantec estimaba en 2012 que las compañías sufren una media de 16 fallas o interrupciones en sus centros de datos lo que eleva el costo total a 3,700.00 millones de euros anuales. (Digitech, 2013)

A nivel mundial empresas relacionadas con la aviación han tenido importantes eventos en los cuales las fallas de sus sistemas les han creado pérdidas económicas y de imagen considerables, todo esto por no contar con un efectivo plan de recuperación

ante desastres. Dentro de los incidentes encontrados durante la investigación se encuentran:

1) La empresa de aviación Southwest tuvo que suspender alrededor de 57 vuelos luego de un fallo en sus sistemas de reservaciones principales y cuyo respaldo de datos tardo demasiado tiempo en estar operativo.(Associated Press, 2013)
2) Una falla ocurrida en el centro de control aéreo de Swanwick del condado de Hampshire al sur de Inglaterra provocó la cancelación y retrasos de vuelos en gran parte de los aeropuertos británicos, los retrasos de los vuelos eran de 25 minutos en las llegadas y 45 minutos en las salidas.(EFE, 2013)
3) Un fallo en los sistemas informáticos provocó que todas las gestiones de vuelos se realizaran de forma manual en todos los aeropuertos de Estados Unidos. El aeropuerto John F. Kennedy ubicado en New York y considerado uno de los que más tráfico de vuelos gestiona, vio reducida su capacidad en un 40%.(AEREOO, 2009)
4) Un fallo en los sistemas informáticos de migración en el aeropuerto de Los Ángeles, Estados Unidos provocó que alrededor de 6,000 pasajeros permanecieran en las terminales o dentro de los aviones. Esto debido a que los agentes de migración no podían tener acceso a la información de los pasajeros que estarían intentando ingresar al país. (Associated Press, 2007)
5) Por una falla en la red tecnológica, la empresa Copa Airlines se vio obligada en cancelar aproximadamente 110 vuelos ocasionando con esto una gran concentración de pasajeros en la terminal aérea del aeropuerto ubicado en Tocumen, Ciudad de Panamá. Debido a dicha falla se tuvo que buscar alojamiento para 2,000 personas cuyos costos fueron asumidos por la empresa.(Radio Panamá, 2013)

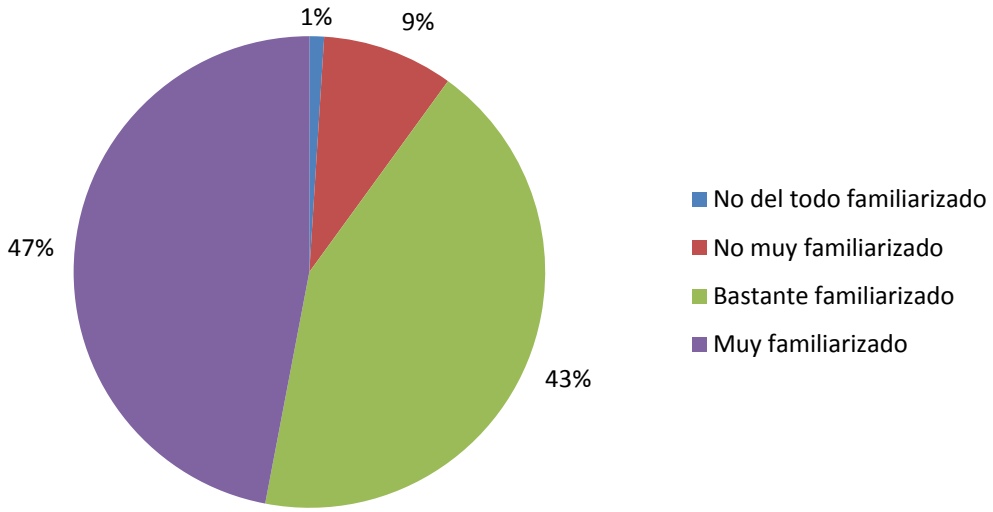

Figura 5. Administradores familiarizados con planes de continuidad del negocio
Fuente: (Musgrave & Woodman, 2013, p. 21).

En la figura 5, se observa los resultados de una encuesta realizada en el Reino Unido a diferentes gerentes de empresas de TI en la cual se consultó que tan familiarizados están con la continuidad del negocio, se puede observar que el 90% de los gerentes están familiarizados con dichos temas y solo un 10% no conoce sobre la continuidad del negocio. Mostrando la importancia que dichos gerentes tiene sobre los planes de continuidad del negocio.

2.1.2 ANÁLISIS MICROENTORNO

Al empezar a entender y comprender los planes de continuidad del negocio planificados, aplicados y ejecutados en Honduras, por lo general son muy pocas las empresas que los poseen, no existe un registro exacto de la fecha, y cuando comenzaron a darles un seguimiento en las organizaciones que poseen un departamento de tecnologías de información.

Se obtuvo información referente de los planes de continuidad del negocio de las instituciones bancarias, empresas de telefonía y la Secretaria de Finanzas del país por medio de una solicitud de información donde se les requiere puedan brindar datos de los planes, referentes a conocer el tiempo desde el cual se inició su utilización, frecuencia de actualización y el periodo de tiempo definido para las pruebas correspondientes, dicha petición de información fue enviada por medios electrónicos(e-correo), donde se relata la forma que se ha implementado dichos planes para cumplir con los lineamientos solicitados.

A nivel nacional se encontró que la Comisión Nacional de Bancos y Seguros mediante la circular CNBS No. 119/2005 con fecha del 22 de noviembre del 2005 obliga a las instituciones financieras del país a proceder según se establece en la circular y dentro de la que se encuentra la formulación de planes de continuidad del negocio para asegurar la recuperación y poder operar la tecnología de información en los casos de mal funcionamiento y/o desastres que se puedan presentar en dicho sector financiero.

La institución deberá examinar y revisar su plan de contingencias atendiendo los cambios que han ocurrido desde la revisión anterior. Dicha revisión deberá realizarse como mínimo cada dos (2) años, así como cada vez que ocurran cambios significativos. Asimismo, al menos anualmente y cuando ocurran cambios significativos, la institución deberá realizar y documentar pruebas de sus procesos de respaldo y recuperación. Se determina que los equipos de almacenamiento de respaldos de datos deberán estar localizados en un lugar diferente en donde se originó la información, adicionalmente se deberá asegurar la restauración de los datos desde los respaldos (CNBS, 2005).

La planificación de continuidad de negocio se enfoca en la forma en que la compañía puede restaurar las operaciones de negocios después de ocurrido un desastre. El plan de continuidad de negocios identifica los procesos de negocios críticos y determina los

planes de acción para manejar las funciones de misión crítica en casos de que los sistemas fallen. (Laudon & Laudon, 2012).

La empresa de telefonía de TIGO en Honduras aprobó el plan de continuidad en el año 2009, cada tres meses realizan una actualización del mismo y las pruebas se llevan a cabo cada seis meses para contar con la seguridad de que la información ahí contenida se encuentre vigente ante las situaciones de riesgo que pueden afectar a la institución. Por otra parte la compañía CLARO en Honduras no posee un plan de continuidad de negocio específico para el país, pero si lo manejan a nivel corporativo de toda latinoamérica dada la estructura que se mantiene en la organización (Torres, 2014).

En la Empresa Hondureña de Telecomunicaciones se realizan planes para responder ante situaciones de riesgo y desastres pero es a nivel de los equipo de trabajo, respaldos de información y conexiones alternas. La parte relacionada a la recuperación de la información no se poseen datos de que se haya efectuado (Inestroza, 2014).

La Secretaria de Finanzas de la República de Honduras (SEFIN) inicia el uso de los planes a partir del mes de julio del año 2012, el cual tiene un alcance orientado a los procesos críticos identificados en la institución y se actualiza de forma manual, actualmente se tiene planificado la adquisición de una herramienta para gestión automatizada del BCP, Se tienen planificadas realizar dos pruebas anuales, además de las ocasiones en las que por problemas en la parte de infraestructura se pone en marcha el BCP garantizando la disponibilidad de los sistemas que requiere la institución (Pérez, 2014).

2.1.3 ANÁLISIS INTERNO

Hace ya casi 54 años que la empresa COCESNA organismo de integración centroamericana que se encuentra en operaciones dedicadas al servicio del tránsito aéreo en su zona de responsabilidad de vuelo. Durante estos años el uso de la

tecnología ha venido teniendo una evolución muy significativa hasta llegar al punto de depender la mayoría de sus actividades de la tecnología. El crecimiento tanto en la capacidad de equipos, instalaciones estructura organizacional y recurso humano ha sido considerable lo cual ha creado la necesidad de automatizar la mayoría de los procesos que se realizan día con día. Dentro de los procesos se encuentran: Facturación y Cobros, Contabilidad, Presupuesto, Recursos Humanos, Propiedad, Planta y Equipo, Tesorería.

En vista de lo anterior los datos que se generan por dichos procesos se han convertido en parte de los activos más valiosos de la corporación, lo que a su vez genera la necesidad de contar con una efectiva política de respaldos de datos y recuperación de la información en caso de presentarse alguna falla a nivel de sistemas o de los equipos. Aunado a la generación de datos por medio de sistemas se tiene información importante y crítica que es generada por el personal referente a informes, manuales, procedimientos, evaluaciones de personal, políticas etc. Que también necesitan ser respaldados en medios de almacenamiento seguro.(Zavala, 2014)

Actualmente la generación diaria de información dentro de la empresa es de 4GB diarios en el cual se encuentran datos estructurados y los no estructurados que se han considerado prioritarios para su respectivo respaldo. La Gerencia de Tecnología Informática (GTI) es la unidad responsable de emitir las políticas de uso de las tecnologías dentro de la empresa así como la de asegurar la protección de datos que son considerados como críticos dentro de la empresa y almacenar los mismos en medios seguros para su respectiva protección y custodia.(Sánchez, 2014)

Dentro de los procedimientos que están definidos en la GTI se encuentra el concerniente a los respaldos de datos los cuales se realizan con una estrategia de respaldo combinada. El primer día de la semana se realiza un respaldo total de los datos y los subsiguientes días se hace de manera incremental. Se cuentan con herramientas automatizadas para realizar dicho trabajo. La verificación de los respaldos

es realizada por la herramienta. Una vez respaldada la información se realiza una copia en una ubicación en la nube.(Op.Cit.)

Dentro de la corporación esta creado un plan de continuidad de negocio para el área administrativa el cual fue elaborado en el año 2007, el cual tiene ya 7 años de no ser actualizado. Dicho plan se encuentra obsoleto ya que durante ese tiempo ha habido cambios a nivel de la infraestructura de equipos, movimientos de personal, cambio de prioridades, aparición de nuevos riesgos, etc.(Zavala, 2014)

Para poder asegurar las operaciones del negocio se cuenta con algunas medidas de control y seguridad para lograr reducir ataques o fallas que se puedan presentar, dentro de estas medidas se encuentran (Op.Cit.):

1) Autenticación: Mediante la asignación de usuarios y claves a los diferentes usuarios para poder tener acceso a la red corporativa, sistemas de información.
2) Permisos: Establecimiento de niveles de acceso a la información y equipos a los diferentes usuarios.
3) Anti-Virus: Para protección de las máquinas de los usuarios contra ataques de virus y evitar la propagación de los mismos por la red corporativa.
4) Firewalls: Para aplicar políticas de control de acceso a internet.
5) Respaldo de Datos: Mantener copia de los datos que son considerados críticos dentro de la empresa.
6) Infraestructura Virtualizada de todos los servidores en producción.

Actualmente no se cuenta con un sitio alterno para poder reanudar las operaciones del negocio en caso de presentarse algún tipo de desastre que provoque la no operación del centro de datos principal. En cuanto a los costos que tendrían en caso de no tener operativos los sistemas no están estimados, por lo cual no se puede conocer cuáles serían las pérdidas económicas al no poder operar un sistema o equipo crítico.

Se tiene identificada una matriz de riesgos posibles con sus respectivas acciones correctivas, pero el mismo no se encuentra actualizado.(Sánchez, 2014)

2.2 TEORÍAS

A continuación se describen las principales teorías que se encuentran relacionadas con las variables del estudio.

2.2.1 COSTOS

Según (Van Horne & Wachowicz, 2010) define el costo como “Un sacrificio de recursos que se asigna para lograr un objetivo específico”. Por lo general los costos se miden en cantidad monetaria que se debe pagar para poder adquirir un servicio. La estimación de los costos que proporciona la planificación de la continuidad del negocio requiere de una profunda evaluación de los beneficios que se desprenden de la adopción de los planes al negocio.

> Cuando se toma una decisión para empeñarse en determinada alternativa, se abandonan los beneficios de otras opciones. Los beneficios perdidos al descartar la siguiente mejor alternativa son los costos de oportunidad de la acción escogida. Puesto que realmente no se incurre en costos de oportunidad, no se incluyen en los registros contables. Sin embargo, constituyen costos relevantes para propósitos de toma de decisiones y deben tenerse en cuenta al evaluar una alternativa.” (Polimeni, Fabozi, & Adelberg, 1994)

El costo por lo general es la mayor preocupación de las organizaciones que evalúan las soluciones de recuperación de desastres, especialmente durante los difíciles tiempos económicos que viven las empresas. Se espera que dentro de las empresas no ocurran desastres por lo cual se hace difícil poder conseguir el presupuesto necesario por algo que pueda tener poco uso, pero se debe tomar en cuenta que los servidores en producción en el centro de datos tienen un grado de valor para el negocio por lo tanto es un activo que merece la pena proteger. Con lo anterior como base las

organizaciones deben procurar asignar suficiente presupuesto equilibrando los costos de protección contra la importancia de los componentes del centro de datos (NetIQ, 2012).

El costo de oportunidad se encuentra presente en las organizaciones de hoy en día cuando se enfrentan ante la situación de tomar decisiones a la ligera, sino analizar las consecuencias que traerán las alternativas presentadas y decidirse por la mejor opción en busca del beneficio de la empresa. Los planes de continuidad se consideran costos preventivos debido a que estos se preparan ante una posible interrupción de servicios o de desastres naturales a futuro y así tener todo controlado si llegase a suceder algún acontecimiento anormal (Polimeni et al., 1994).

“Una evaluación del riesgo determina el nivel de riesgo para la firma si no se controla una actividad o proceso específico de manera apropiada. No todos los riesgos se pueden anticipar o medir, pero la mayoría de las empresas podrán adquirir cierta comprensión de los riesgos a los que se enfrentan”. (Laudon & Laudon, Sistemas de Información Gerencial, 2012, p. 309).

En el caso de estudio de COCESNA se debe realizar una evaluación entre dedicar tiempo y recursos económicos para la correcta planificación de la continuidad de negocio con respecto a los riesgos que se pueden predecir. Posee dos opciones:

1) La aprobación, administración y planificación de los planes de continuidad,
2) No realizar los planes para la empresa.

El costo-beneficio de implementar los planes de continuidad de negocios se enfoca en cuanto a las pérdidas monetarias que obtiene la empresa al momento de la falta de disponibilidad de los sistemas e información crítica para las organizaciones.

2.2.2 GESTIÓN DE RIESGOS

En toda actividad por realizar se tiene la posibilidad de que ocurra un riesgo el cual pueda o no provocar un daño.

> En los últimos años, desde la perspectiva de los desastres naturales, el riesgo se ha intentado dimensionar para efectos de la gestión, como las posibles consecuencias económicas, sociales y ambientales que pueden ocurrir en un lugar y en un tiempo determinado.(Cardona, 2003)

“Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización.” (ISACA, 2009)

Con la gestión del riesgo se pretende hacer una alineación con la estrategia de la empresa y de todos los procesos que se encuentren definidos. El término de riesgo se define como: “Es un suceso incierto que puede llegar a presentarse en un futuro dependiendo de variables externas o internas. Es entonces la cuantificación de una amenaza.”(IMARPE, 2012)

Dentro de los objetivos que se pretenden alcanzar con el análisis de riesgos se encuentran los siguientes (J. Martínez, 2004):

1) Análisis y reducción de los riesgos a los que está expuesta la empresa.
2) Identificación de amenazas y vulnerabilidades.
3) Identificación de riesgos potenciales, probabilidad y consecuencias.
4) Determinación de niveles aceptables de riesgo, alternativas y el compromiso de la dirección.

Una vez que se tienen identificados los riesgos se deberá cuantificar y cualificar cual es la probabilidad de ocurrencia y el tipo de impacto que tendrá dentro de la organización

si se llegara a presentar dicho riesgo, para lo cual se deberán establecer acciones correctivas y preventivas para poder mitigarlos. En un riesgo se deben considerar los siguientes elementos (Op.Cit.):

1) Valor de los activos: Valor económico de los activos de la empresa.
2) Frecuencia de la amenaza: Las veces en que se puede presentar el riesgo.
3) Impacto de la amenaza: Costo o daño que pueda causar el riesgo si llegara a ocurrir.
4) Eficacia de las medidas adoptadas: Si las medidas adoptadas lograron mitigar los riesgos identificados en la empresa.
5) Costo de las medidas adoptadas: Costos de la implementación y mantenimiento de las medidas tomadas para mitigar el riesgo.
6) Incertidumbre: Grado de confianza que se le aplica a los ítems descritos anteriormente.

> Riesgo de un proyecto es un evento o condición incierto que, si se produce, tiene un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, costo, alcance o calidad. Un riesgo puede tener una o más causas y, si se produce, uno o más impactos.(F. Martínez & Hernández, 2010)

En la figura 6, se pude observar la clasificación de los riesgos que pueden existir en una organización

Figura 6 Jerarquía de riesgos

Fuente: Risk IT Framework, 2009.

> Los métodos cuantitativos que se han intentado aplicar, en la práctica, tienen finalmente una carga subjetiva que hace de dichos valores cuantitativos una expresión más cualitativa que otra cosa, por lo que se ha terminado por imponer la metodología cualitativa en la que los elementos del riesgo se miden como «Alto, Medio, Bajo» o por niveles numéricos, de 1 a 3 o de 1 a 5, o se clasifican como «Vital, Crítico, Importante, Conveniente, Para Información», aunque esta clasificación solo es aplicable a los activos.(J. Martínez, 2004)

Los pasos para planificar una adecuada respuesta a los riegos son (F. Martínez & Hernández, 2010):

1) Identificación.
2) Cualificación y Cuantificación.
3) Definición de acciones preventivas.
4) Acciones correctivas.

Los riesgos que pueden afectar a la organización deben ser "*Identificados*", para ello se pueden hacer grupos de trabajos cuyo fin sea el de poder identificar los riesgos

probables que podrían presentarse dentro de la empresa o se puede hacer uso de datos estadísticos que se tengan sobre ataques informáticos o de alguna otra índole. También se puede hacer uso de organismos que tengan identificados algunos riesgos que se puedan presentar en cualquier sector por rubro.

"La cualificación de los riesgos se realiza considerando su probabilidad de ocurrencia y el grado del impacto potencial del evento."(Op.Cit.). Al listado de riesgos que se hayan identificado en el grupo de trabajo se le deberá hacer una cualificación a cada uno de ellos para luego indicar cuál será la probabilidad de ocurrencia y el impacto que este podría tener de llegar a presentarse. En la siguiente tabla se muestra una matriz de riesgos que se puede utilizar para realizar la identificación y cualificación del riesgo.

Tabla 3. Matriz de riesgos

CATEGORIA	RIESGO	PROBABILIDAD OCURRENCIA	IMPACTO POTENCIAL

En vista que la evaluación del riesgo es cualitativa se deberá usar valores como ser: (Alto, Medio, Bajo), (Probable, Poco Probable, Improbable) o cualquier otro que se considere pertinente para la cualificación del riesgo. La cuantificación se realiza de una manera similar la única diferencia que existe es que el análisis se deberá expresar en valor monetario o numérico.(J. Martínez, 2004)

Para realizar el cálculo de un análisis cuantitativo del riesgo se deben tomar en cuenta los siguientes factores (Jiménez, 2013b):

1) Probabilidad de Amenaza (PA): Valor en un rango de 0 a 100.
2) Esfuerzo (E): 1 valor más bajo y 10 valor más alto.
3) Factor de Gravedad (FG): 1 valor más bajo y 10 valor más alto.
4) Factor de Riesgo (FR): FG/FE.
5) Nivel de Frecuencia de la Amenaza (NF): PA*FR.
6) Factor de Vulnerabilidad (FV): El más bajo es 1 y el más alto 10.
7) Factor de Repercusión (Fre): FV*PA.

8) Valor del Activo (VA): Valor expresado en monetario del costo del activo.
9) Factor de Exposición (FE): (NF*Fre)/1000.
10) Expectativas de perdidas únicas (SLE): VA*FE.
11) Probabilidad de amenaza tratada (AROt): Constante entre 0.1 a 0.5
12) Tasa anualidad de ocurrencia (ARO).
13) Perdida financiera anual original (ALE original): SLE*ARO.
14) Perdida financiera anual tratada (ALE tratado):SLE*AROt
15) Valor en Riesgo (VAR): (ALE original – ALE tratado).

Para el factor Esfuerzo se toma en cuenta las capacidades necesarias para que un atacante saque provecho de la explotación del activo vulnerado. El factor ALE se define como la perdida financiera anual que se espera que una amenaza específica cause un activo, ALE tratado es la perdida financiera anual una vez que se ha tratado de disminuir la amenaza. El valor en riesgo (VAR) define como la peor perdida que se puede tener ante la presencia de un riesgo. Esta variable permite establecer un balance entre el riesgo y el costo asociado. El nivel de riesgo aceptable debe ser definido por la organización. Si el valor de VAR excede el monto definido se debe invertir en eliminar el riesgo.(Op.Cit.)

Una vez que se tengan identificados, clasificados, cualificados y cuantificados los riesgos se deberá proceder a realizar un plan de acción que permita identificar las acciones correctivas o preventivas a realizar para cada uno de los riesgos identificados.

El plan de riesgos a generar deberá contener los siguientes elementos (F. Martínez & Hernández, 2010):

1) Riesgos.
2) Probabilidad de ocurrencia.
3) Monto potencial del impacto.
4) Eventos disparadores del evento.

5) Acciones preventivas.
6) Acciones correctivas.
7) Responsables.

Terminada la fase de análisis y valoración de los riesgos que se pueden presentar en la organización, corresponde a la alta dirección tomar las decisiones referentes a que alternativa se tomara ante cada uno de los riesgos identificados, las posibles opciones que se pueden tener los riesgos son (J. Martínez, 2004):

1) Transferir el riesgo: Pasar el riesgo que lo maneje un tercero o contratar pólizas de seguros.
2) Eliminar el riesgo: De ser posible mediante la ejecución de las acciones correctivas.
3) Reducir el riesgo: En caso que la eliminación del mismo no sea posible.
4) Aceptar el riesgo: Cuando la probabilidad que ocurra sea baja o el costo de mitigarlo sea muy alto.
5) Una combinación de las anteriores.

En la figura 7, se puede observar el proceso que se debe realizar en el tratamiento de los riesgos, en el cual se indica los pasos a realizar en la identificación y clasificación del riesgo para poder desarrollar planes de acción permitiendo tratar el riesgo logrando reducir la probabilidad y consecuencia o evaluar si resulta factible hacer una transferencia a terceros para que administre el riesgo. En todo este proceso debe estar presente la actividad de comunicar a todos los interesados sobre cómo se administraran los riesgos y en base a ello realizar un monitoreo constante para ver si se está logrando lo establecido en los planes de acción.

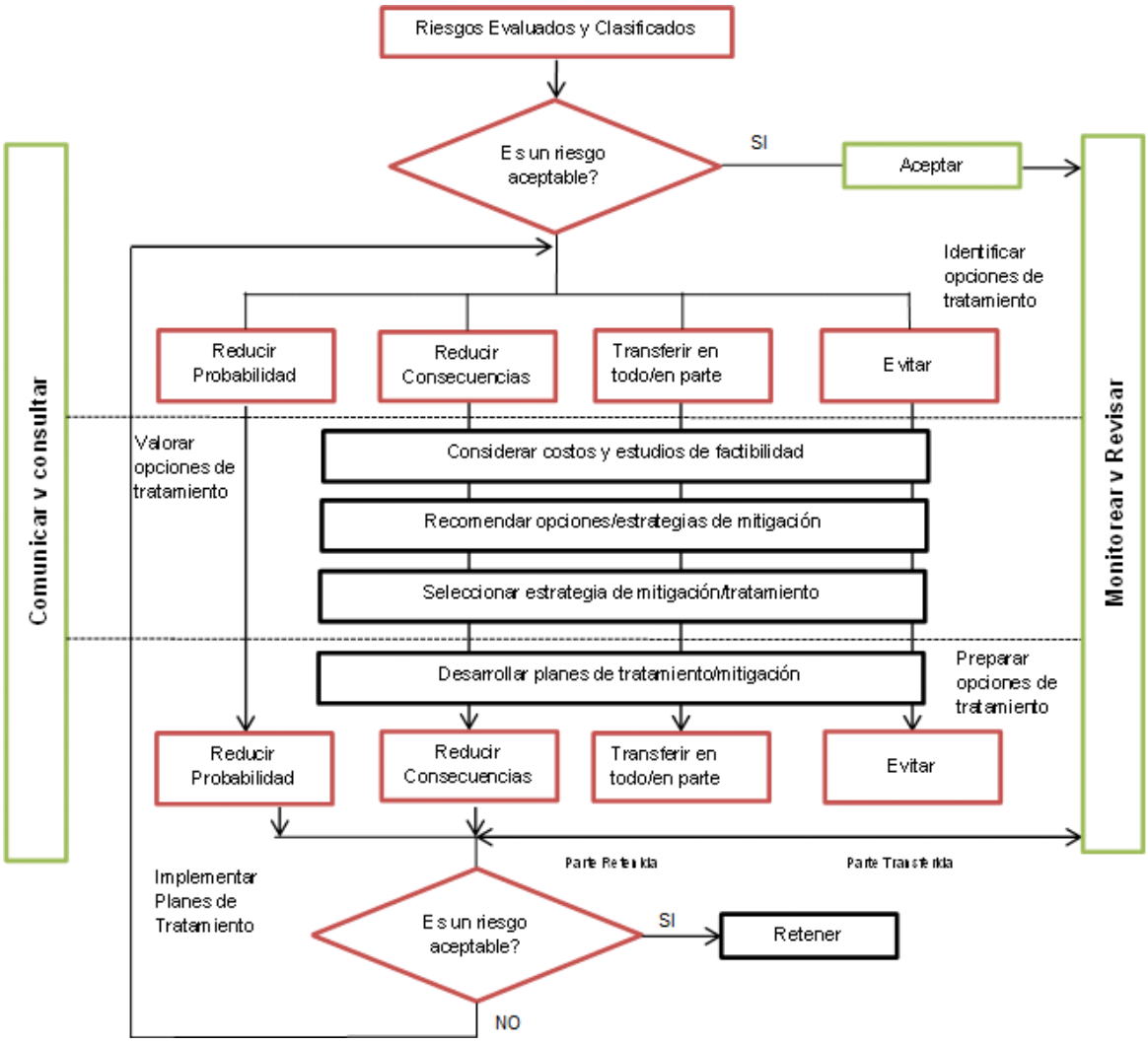

Figura 7. Tratamiento del riesgo.

Fuente: (Jiménez, 2013)

Adicionalmente al análisis de riesgos se deberá efectuar un análisis de impacto cuyo objetivo sería la de brindar datos válidos para la toma de decisiones al momento de estar creando estrategias de recuperación identificando el grado de criticidad y el tiempo máximo permitido de la interrupción. Lo tipos de impactos puede ser diversos y están determinados siempre a un periodo de tiempo, dentro de los tipos de impacto se pueden encontrar (J. Martínez, 2004):

1) Pérdida de ingresos y beneficios.

2) Incremento de costos/gastos.
3) Peligro para las personas.
4) Impacto operacional.
5) Impacto comercial.
6) Pérdida de calidad.
7) Impacto en la imagen de la organización.
8) Incumplimiento de obligaciones jurídicas
9) Impacto ambiental.
10) Desmoralización del personal.

Una vez definido el plan de riesgos de la empresa el mismo debe tener un proceso de mejora continua en el cual el plan original se esté revisando ya que los riesgos cambian con el tiempo o las medidas correctivas ya no sean efectivas para controlar el riesgo. En la figura 8 se presenta un diagrama indicando como se debe llevar a cabo la gestión continua de los riesgos.

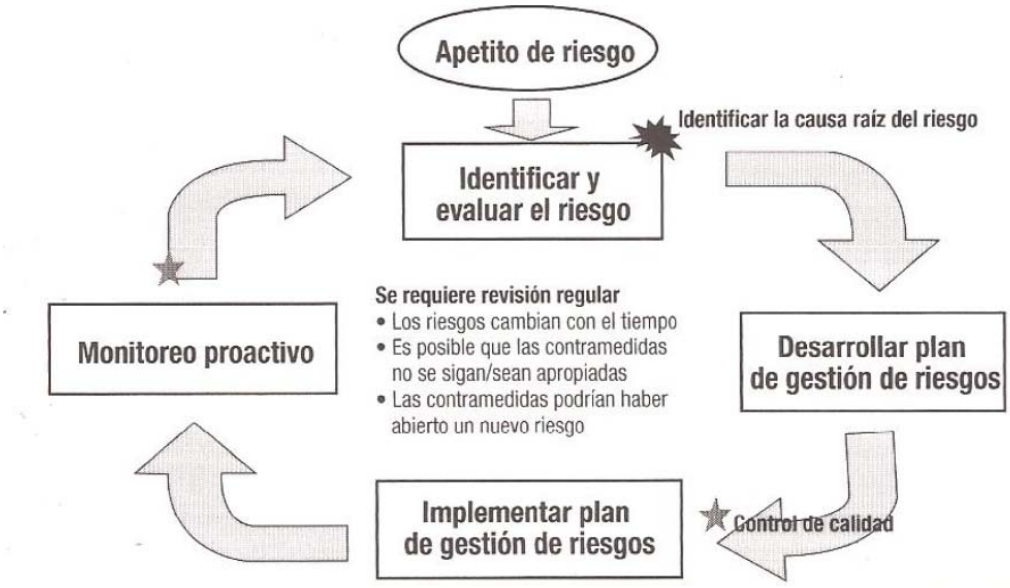

Figura 8. Gestión continúa de riesgos

Fuente: (Jiménez, 2013)

Los beneficios de un análisis de riesgos son los siguientes (Sandhu, 2002):

1) Facilidad de comprensión de los datos.
2) Identificación y priorización de actividades y funciones críticas.
3) Identificación de las áreas en que las políticas y procedimientos necesitan estar optimizados y aplicados.
4) Justificación del costo que se incurre en ejecutar las medidas de prevención.

2.2.3 RECUPERACIÓN ANTE DESASTRES

La planificación de la recuperación ante desastres está asociado a la preparación y respuesta cuando ocurre un desastre, el objetivo principal es la supervivencia de una organización, algunos de los desastres que se pudieran presentar en una organización son (Gregory, 2008):

1) Incendios.
2) Inundaciones.
3) Huracanes.
4) Terremotos.
5) Erupción volcánica.
6) Incidentes de seguridad.
7) Falla en los equipos.
8) Fallas de energía.
9) Sabotajes.
10) Huelgas.
11) Guerra.
12) Ataque terrorista.
13) Incendios forestales.
14) Deslizamiento de tierra.
15) Incendio provocado.

> Plan de recuperación de desastres es un conjunto aprobado de actividades y procedimientos los cuales hacen posible a una organización responder a un desastre y reiniciar sus funciones críticas en una condición aceptable, en un marco de tiempo determinado.(Guzmán, 2013)

Las consecuencias de los desastres están teniendo mayores efectos adversos sobre las poblaciones y sus entornos. En la medida de lo posible, algunos gobiernos aprueban leyes y toman medidas para estar preparados y mitigar los efectos de estos peligros que pueden ser de origen natural, tecnológicos o intencionales (Coppola, 2007).

> Un Plan es conveniente para todas las entidades, si bien en algunas, porque den servicio a un gran número de empresas o usuarios, por el sector de actividad o por otras razones, es absolutamente imprescindible, para evitar que en el caso de un problema grave la entidad haya terminado su actividad para siempre o sufrido un daño importante.(J. Martínez, 2004)

El objetivo principal de contar en las empresas con un plan de recuperación de desastres es la de poder tener una respuesta efectiva y poder recuperar las operaciones ante la presencia de un desastre, para poder minimizar el impacto que puedan causar los desastres en las empresas se puede lograr mediante las siguientes estrategias (Sandhu, 2002):

1) Estrategia de Prevención: Los esfuerzos están orientados a prevenir los desastres intentando reducir la probabilidad de ocurrencia.
2) Estrategia de Predicción: Se identifican los procedimientos para responder y recuperarse de los desastres, para lograr esto se hace uso de escenarios de predicción de los posibles impactos que pueda causar un desastre.
3) Estrategia de Mitigación: Implementar medidas para minimizar el impacto de un desastre.

Los desastres potenciales que se puedan presentar tienden a causar daños a los edificios, equipos, sistemas de información, personas, algunos de los efectos que tienen en las organizaciones son los siguientes (Gregory, 2008):

1) Daños directos.
2) Inaccesibilidad.
3) Cortes de energía.
4) Interrupción de transporte.
5) Interrupción en las comunicaciones.
6) Evacuaciones.
7) Ausentismo Laboral.

En la figura 9, se puede observar como desde los años 1900 hasta el 2002 los desastres naturales han tenido un aumento significativo llegando a tener 700 desastres naturales en el 2002.

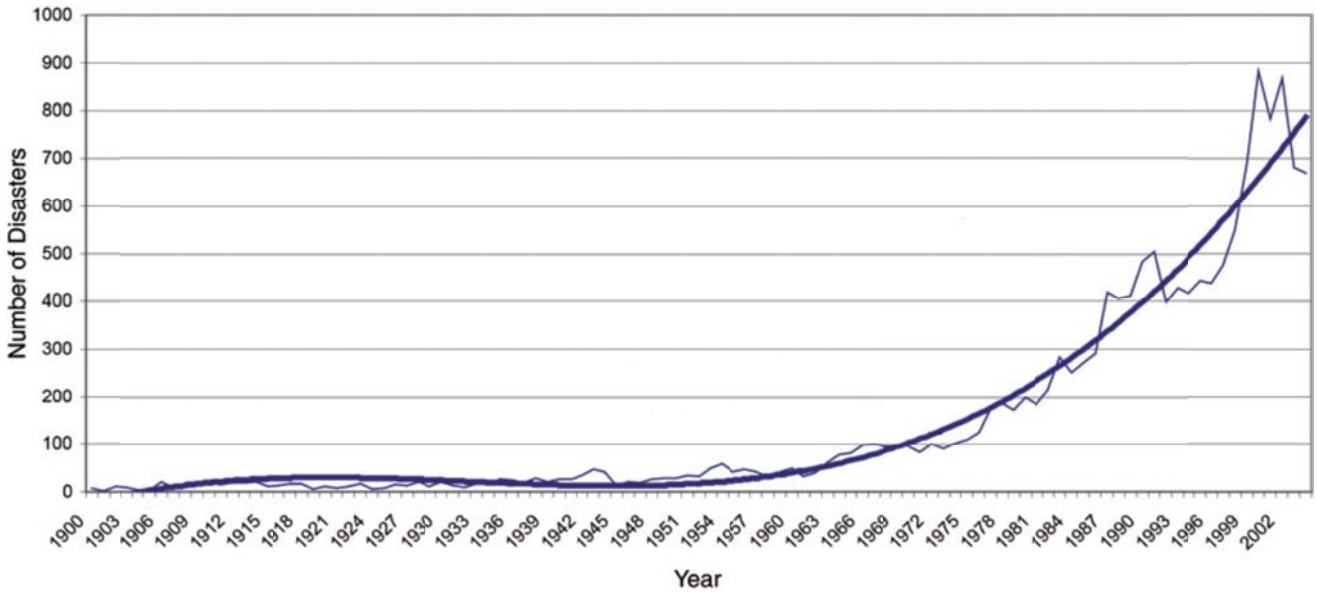

Figura 9. Número de desastres naturales reportados en el mundo

Fuente: (Coppola, 2007, p. 23)

En el procesamiento de datos o la planificación de recuperación de negocios el término desastre es lo que más se utiliza. Algunas definiciones utilizadas para referirse a los planes de continuidad del negocio son (Wallace & Webber, 2004):

1) Planificación de recuperación de desastres (DRP): Contiene las acciones que se pueden tomar para recuperarse ante un desastre, incluye los pasos para la administración de riesgos. El DRP se puede aplicar a todos los aspectos del negocio, pero generalmente se utiliza en el contexto de las operaciones del procesamiento de datos.
2) Planificación de recuperación de negocios (BRP): Se basa en la planificación de la recuperación ante desastres, adicionalmente se incluye los esfuerzos del resto de las operaciones del negocio tomando en cuenta las relaciones con los clientes y proveedores para poder recuperarse de un problema.
3) Plan de continuidad del negocio (BCP): Este plan permite al negocio poder operar a un nivel reducido posiblemente durante o inmediatamente después de presentarse una emergencia.

Un plan de recuperación ante desastres debe estar compuesto por lo siguiente (Op. Cit):

1) Procedimientos de declaración de desastres.
2) Listado de contactos de emergencia.
3) Listado de miembros del equipo de emergencias.
4) Procedimiento de evaluación de daños.
5) Procedimientos de recuperación y reinicio.
6) Transición a las operaciones normales.
7) Listado de miembros del equipo de recuperación.

Una vez que se haya generado el plan de recuperación el mismo deberá ser distribuido al personal involucrado en la estrategia de recuperación, se deben utilizar múltiples

fuentes de almacenamiento a las cuales el personal tenga acceso en todo momento y desde cualquier lugar, no se debe dejar la información del plan solamente en las oficinas de la empresa.(J. Martínez, 2004)

En la elaboración del plan de recuperación ante desastres se deben definir objetivos de recuperación para la toma de decisiones relacionadas con la recuperación de recursos, actividades o funciones. Los objetivos de recuperación recomendados son los siguientes (Sandhu, 2002):

1) Objetivo de punto de recuperación (RPO): Tiempo de recuperación de las actividades críticas del negocio.
2) Objetivo de tiempo de recuperación (RTO): Tiempo en el cual debe estar recuperado un equipo o sistema para iniciar los trabajos después de haberse presentado un desastre.
3) Máximo de interrupción aceptable (MAO): Tiempo máximo permitido de una interrupción durante el cual se debe poner en ejecución el plan de recuperación para no poner en peligro las operaciones del negocio.

En la figura 10, se muestra la interrupción de un servidor Web y la interrupción del servicio de comercio electrónico de un negocio, La escala está representada en períodos de tiempo. El valor del RPO para la interrupción del servidor Web puede variar en el rango de los segundos hasta semanas en contraste con el RTO del servicio de comercio electrónico que solo deberá durar unos segundos, si la interrupción de dicho servicio se prolonga más tiempo del estipulado la organización podrá tener pérdidas financieras, de imagen, consecuencias legales, etc.

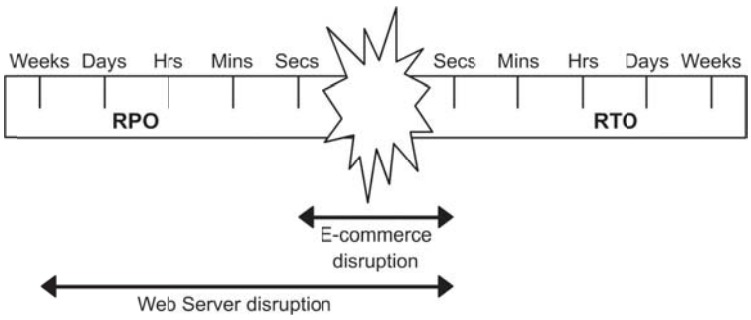

Figura 10. Ejemplo de RPO y RTO

Fuente: (Jeet Sandhu, 2002, p. 42)

Dentro del plan de recuperación se debe realizar un inventario de todo el equipo informático así como del software y demás aplicaciones que se utilicen dentro de la empresa, algunos elementos que se pueden utilizar para la elaboración del inventario se muestra a continuación (Gregory, 2008):

1) Inventario de Hardware: Debe incluir servidores, routers, firewalls, componentes de red, cableado, partes o piezas.
2) Inventario de Software: Que aplicaciones se están utilizando dentro de la empresa y en que oficinas específicas, que software está alojado dentro de los servidores. Se debe indicar las versiones, parches, configuraciones y cualquier otro dato relevante.

Una vez que el plan de recuperación ante desastres este elaborado se deberán poner en marcha procedimientos de revisión al plan y de ejecución de pruebas que permitan validar los procedimientos creados y no tener sorpresas desagradables al momento de ocurrencia de un desastre en la organización.

Un Plan de Continuidad debe ser actualizado a lo largo del tiempo. En una buena medida, está reflejando la situación de la organización y es consecuencia de ella. Por tanto, cualquier evaluación debe realizarse con el objetivo de

subsanar las deficiencias que se encuentren, y en consecuencia, las evaluaciones deben repetirse periódicamente. (J. Martínez, 2004)

Uno de los puntos que se deben tomar en cuenta en el plan de recuperación ante desastres es la de contar con un sitio alterno donde se puedan reestablecer las operaciones del negocio. Dentro de las alternativas para ubicar un centro de datos de respaldo están las siguientes (Gregory, 2008):

1) Sitio Frío (cold site): Es un área acondicionada para poder funcionar como centro de respaldo pero no tiene instalado ningún equipo.
2) Sitio Cálido (warm site): Área acondicionada con el equipo pero que no se encuentra configurado.
3) Sitio Caliente (hot site): Sala que cuenta con los equipos necesarios para entrar en operación de forma inmediata.
4) Otros lugares del negocio: Algún otro sitio que posea la empresa y que reúna las condiciones para funcionar como centro de datos.
5) Centro Móvil: Consiste en una sala equipada con todas las condiciones dentro de un contenedor.
6) Acuerdos de ayuda mutua: Se establecen entre dos o más centros de datos con equipo compatible.

En la tabla 4, se muestra un cuadro comparativo entre los sitios denominados como "Frío, Cálido y Caliente".

Tabla 4 Comparación de categorías de centro de respaldo

Categoría	Caliente	Cálido	Frío
Disponibilidad	Minutos a horas	Horas a días	Días a semanas
Sistemas de aplicación	Cargados y listos para operar	Presentes pero no están listos para operar	Ausente; deben ser comprados e instalados
Comunicaciones	Listos para operar	Eficientes	Poco o nada
Datos de la aplicación	Actualizados y al día	No se encuentran al día; deben ser restaurados	No están presentes; deben ser cargados
Costos	Muy altos	Moderado	Bajo

Fuente:(Gregory, 2008)

Con base en lo mostrado en la tabla No. 4, se puede tener un mejor panorama sobre el tipo de sitio con el cual deben de contar las organizaciones para respaldar las operaciones. La elección final del tipo de sitio debe tomar en consideración los costos de tiempo de inactividad y los costos de largo plazo así como el nivel de capacidad de recuperación requerida. Las empresas deben realizar el análisis costo/beneficio ante la probabilidad de que ocurra un desastre.

Otras alternativas para respaldar el centro de datos son (J. Martínez, 2004):

1) Acuerdos con los proveedores del equipo.
2) Empresas de servicio.

En vista de la alta dependencia de la información y de las infraestructuras informáticas; la alta motivación que tienen hoy en día los atacantes; los eventos inesperados del 11 de septiembre del 2001 en New York, muestran que hoy en día los planes de contingencia ya no son un lujo sino una necesidad. En 1988 fue fundado el Instituto de recuperación de desastres (DRI) por sus siglas en inglés, por la universidad de Washington. Dicho instituto propone los lineamientos para los profesionales en la planeación de recuperación de negocios mediante la definición de áreas de conocimiento, adicionalmente se ofrecen capacitaciones, certificaciones y asesorías. Se estima que alrededor de 1500 empresas a nivel mundial aplican los conceptos y metodologías del DRI (Guzmán, 2013).

En la figura 11, se muestra la metodología de trabajo que propone el instituto de recuperación ante desastres a las empresas para la creación del plan de recuperación ante desastres.

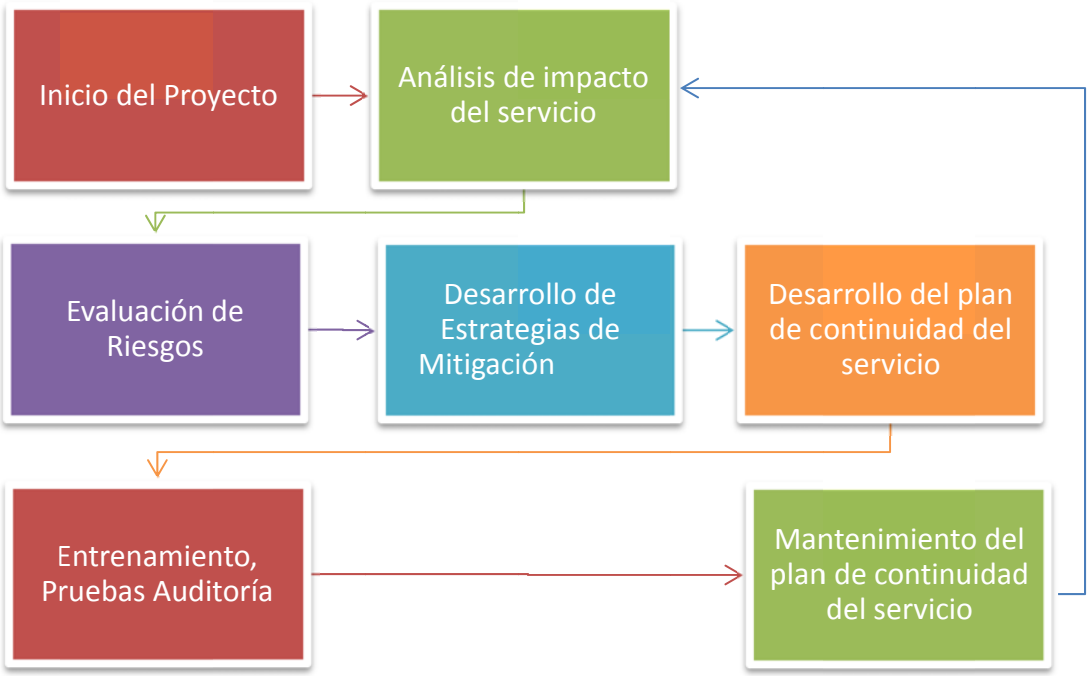

Figura 11. Metodología de trabajo del DRI

Fuente:(Ferrer, 2009).

2.2.4 RESPALDO Y RECUPERACIÓN DE DATOS

El almacenamiento de datos dentro de las organizaciones es un pilar clave de las tecnologías de información, la gran cantidad de información digital que se está generando a cada momento por las personas o empresas, crea la necesidad de su almacenamiento, protección y optimización (Somasundaram & Shrivastava, 2009).

> Hoy en día, lo importante es el valor de los datos. El costo de una computadora es cada vez menor. Por el contrario, el costo de los datos es cada vez mayor. Inclusive, en la mayoría de las aplicaciones, resulta difícil calcular el costo de cada dato. Existen costos computables (por ejemplo, el tiempo de ingreso) y otros que no lo son, tales como los costos indirectos (por ejemplo, los efectos del dato en todo el sistema).(Tener, 2000)

En la figura 12, se observa los distintos tipos de datos que se convierten en datos digitales.

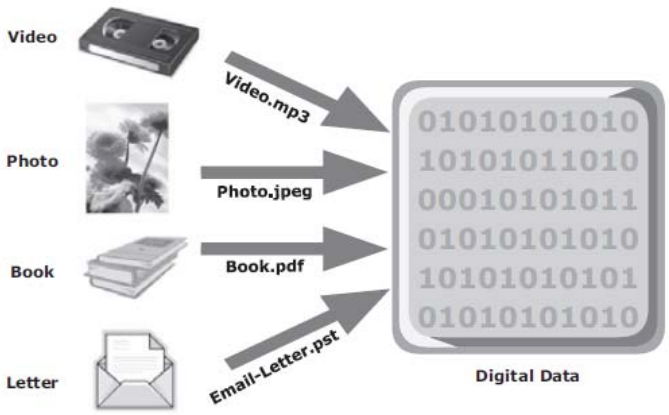

Figura 12. Datos Digitales

Fuente(Somasundaram & Shrivastava, 2009, p. 5)

Fue en la década de los años 80's que las copias de seguridad de los datos se convirtió en una necesidad y en una exigencia mayor. Con la dependencia que se tienen en las empresas con la tecnología ha obligado a la creación de los controles necesarios para restringir el acceso a los datos (Doughty, 2001). Para poder tener un plan de respaldo de datos efectivo se debe de realizar una clasificación de la información así como determinar la ubicación de la misma en toda la organización, identificados los datos críticos se deberán respaldar dándole una prioridad alta (Sandhu, 2002).

Se debe hacer una diferenciación entre los términos recuperación y respaldo, recuperación es la actividad que se ejecuta para volver a un punto determinado logrando con esto obtener los datos que se hayan perdido, respaldo se refiere a la realización de una copia de la información en algún medio, los respaldos deberían ser una actividad prioritaria dentro de las organizaciones (Tener, 2000).

Los datos están clasificados en estructurados y no estructurados, los datos estructurados corresponde a la información que se almacena en los gestores de base

de datos. Los datos no estructurados son los más difíciles de recuperar desde las aplicaciones ya que la información puede ser almacenada en diferentes tipos de formato: email, .pdf,.doc.xls,.ppt,.txt, etc. Por su naturaleza no estructurada es que se dificulta su recuperación mediante una determinada aplicación ya que no tienen suficientes elementos que permita identificarlos de manera única. El 80% de los datos en la empresa son datos no estructurados lo que hace necesario una gran capacidad de almacenamiento (Somasundaram & Shrivastava, 2009).

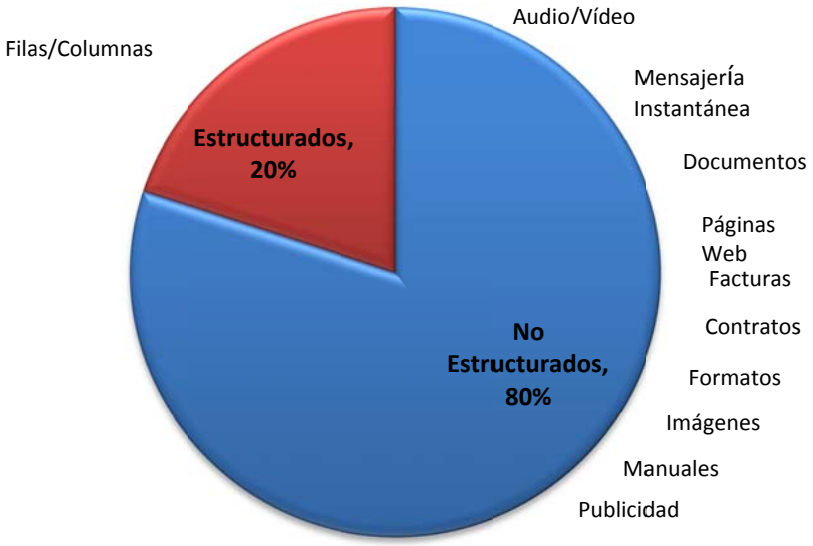

Figura 13. Tipos de Datos

Fuente(Somasundaram & Shrivastava, 2009, p. 8)

Para el correcto almacenamiento de los diferentes tipos de información la tecnología de almacenamiento ha ido evolucionando con el tiempo de acuerdo a las necesidades que se están presentando en las empresas, algunos medios actuales que se pueden utilizar para almacenar la información son los siguientes (Op.Cit.):

1) Conjunto redundante de discos independientes (RAID): Se desarrolló para cumplir con los requisitos de costos, rendimiento y disponibilidad de los datos. Es utilizado en todas las arquitecturas de almacenamiento.
2) Almacenamiento de conexión directa (DAS): Se conecta directamente a un servidor o grupo de servidores, el almacenamiento puede ser interno o externo al servidor. Con el DAS externo se incrementa la capacidad de almacenamiento.
3) Red de área de almacenamiento (SAN): se hace uso de un canal de fibra que facilita la comunicación a nivel de bloques entre el servidor y la unidad de almacenamiento. Con este tipo de almacenamiento se tiene escalabilidad, disponibilidad y rendimiento.
4) Almacenamiento conectado a red (NAS): Dispositivos de almacenamiento a los que se accede desde las computadoras o servidores mediante una interconexión de red de área local (LAN).
5) Protocolo de internet SAN (IP-SAN): Es una convergencia de las tecnologías utilizadas en SAN y NAS, proporciona comunicación por bloque a través de una red de área local.

Adicionalmente a los medios de almacenamiento descritos anteriormente aún se siguen utilizando los discos duros internos o externos, unidades de cinta magnética, CD-ROM.

La mayoría de las estrategias de respaldos de datos hace uso de los siguientes métodos (Cannon, Bergmann, & Pamplin, 2006):

1) Respaldo Total: Crea una copia completa de cada archivo en el sistema, método eficaz de respaldo pero se requiere gran cantidad de tiempo. En la figura 14 se presenta un ejemplo de cómo es la creación de los respaldos totales en el cual todos los días se debe hacer un respaldo general de toda la información. Este tipo de respaldo a parte de requerir una gran cantidad de tiempo se necesita una gran cantidad de almacenamiento.

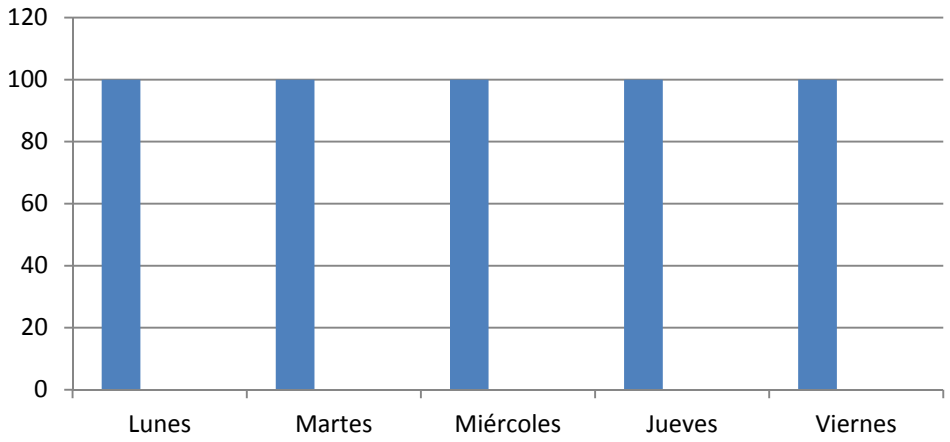

Figura 14. Ejemplo respaldo total de datos

2) Respaldo Incremental: Se realiza una copia de aquellos archivos que han cambiado desde la última vez que se realizó la copia de seguridad, este método solo se realiza durante los días de la semana. Requiere menos tiempo de respaldo pero en la restauración de archivos se demora mucho tiempo. En la figura 15, se muestra un ejemplo de cómo se deberá realizar un respaldo incremental, se hace un respaldo total los días lunes y los demás días solo se respalda la información que ha sufrido cambios desde la última vez que se hizo el respaldo.

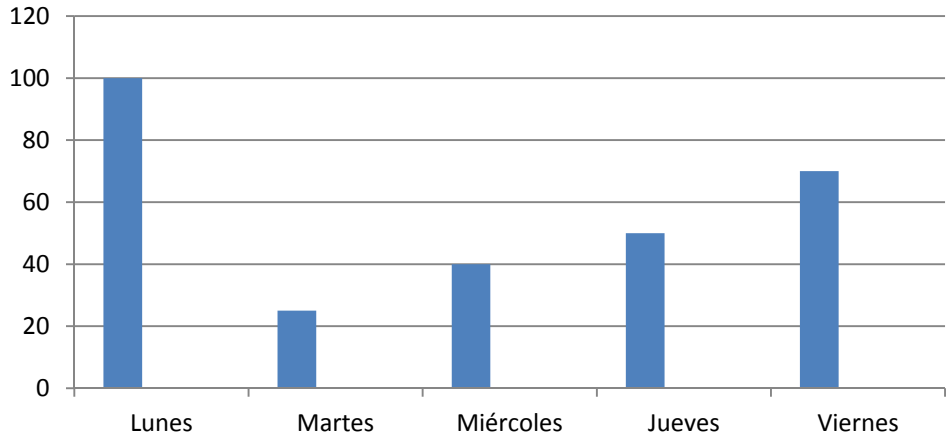

Figura 15. Ejemplo de respaldo incremental.

3) Respaldo Diferencial: Copia de los archivos que han cambiado durante la ejecución de los respaldos totales, este método es el recomendado para la continuidad del negocio. En la figura 16 se muestra un ejemplo de cómo funciona el respaldo diferencial en el cual el primer día de la semana se realiza un respaldo total y los demás días solo de los archivos que han sufrido cambio., este tipo de respaldo toma menos tiempo en ejecutarse y se reduce el tamaño de almacenamiento.

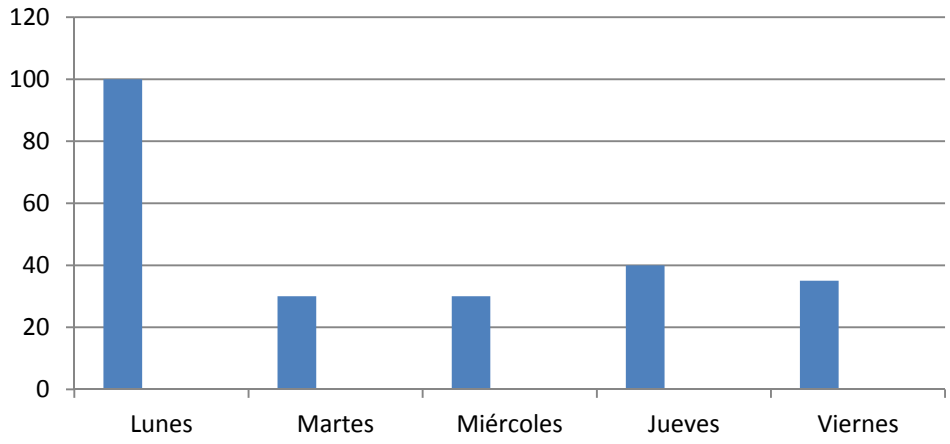

Figura 16. Ejemplo de respaldo diferencial

La estrategia de respaldos será decisión de la empresa dependiendo de cuáles son sus necesidades de copia de datos y del volumen que se requiera almacenar.

> Los diferentes tipos de respaldo son utilizados en forma complementaria. para definir el tipo o tipos de respaldo a utilizar, se debe tener en cuenta la criticidad de los datos, capacidad de almacenamiento, tiempo disponible para realizarlos y tiempo necesario para recuperarlos.(Tener, 2000)

El diseño de soluciones apropiadas para recuperar los datos en caso de una falla se logra utilizando alguna de las siguientes estrategias para hacer una o varias copias de los datos originales (Somasundaram & Shrivastava, 2009):

1) Respaldo y Recuperación: La copia de los datos se puede realizar en unidades de cinta magnética o con discos de gran capacidad todo esto para asegurar la disponibilidad de los datos. la frecuencia de las copias están determinadas por las variables RTO y RPO.
2) Replicación basada en arreglo de almacenamiento (local): Los datos se pueden replicar a una ubicación independiente dentro del mismo arreglo de almacenamiento.
3) Replicación basada en arreglo de almacenamiento (remota): Los datos del arreglo local puede ser replicado a otra matriz de almacenamiento ubicado en un sitio remoto.

La frecuencia en la cual se deberá realizar el respaldo de datos está determinada por la cantidad de operaciones que se realicen en una empresa generalmente en las organizaciones se realiza respaldos diarios combinando las estrategias de respaldo mencionadas anteriormente (Tener, 2000). Al tener definido el tipo de estrategia de respaldos a utilizar dentro de la empresa y el medio de almacenamiento se deberá considerar dentro del plan de recuperación un lugar alterno de respaldo. Dentro de los factores que se deben tomar en consideración para la selección del sitio remoto están los costos de reserva, costos durante el desastre y la disponibilidad requerida así como el tamaño de las instalaciones, aspectos de seguridad, etc. (J. Martínez, 2004)

Algunos de los tipos de instalaciones para la ubicación del centro alterno de almacenamiento de datos son los siguientes (Gregory, 2008):

1) Centro de almacenamiento comercial: Organizaciones que se dedican a brindar el servicio de almacenamiento de datos en instalaciones de alta seguridad.
2) Sitio Alterno: La recuperación con éxito de una falla provocada por un desastre en ocasiones es dependiente de los datos críticos y los recursos de recuperación almacenados en un sitio alterno generalmente lejos de las instalaciones principales.

3) Servicio proporcionado por terceros: Los servicios de respaldo son brindados por un tercero proporcionando sus propias instalaciones para el almacenamiento de datos.

2.3 METODOLOGÍA E INSTRUMENTOS

De los instrumentos a utilizar para encontrar las respuestas a las interrogantes de la investigación se seleccionan los cuestionarios y la entrevista dirigida de donde se procederá a la obtención de información para el estudio.

2.3.1 ENTREVISTA

La entrevista está orientada a poder recabar información de una conversación dirigida con la intención de obtener la información necesaria sobre algún tema, en dicha actividad se hace uso de un formato con preguntas y respuestas. El fin de la entrevista es obtener la opinión de los entrevistados sobre algún tema en particular.(Kendall & Kendall, 2005).

La finalidad de una entrevista es la de poder conversar e intercambiar opiniones entre la persona que tendrá el rol de entrevistador y la persona que tendrá el rol de entrevistado o también se puede entrevistar a grupos pequeños (Sampieri & Collado, 2010).

> La técnica de encuesta para obtener información se basa en el interrogatorio de los individuos, a quienes se les plantea una variedad de preguntas con respecto a su comportamiento, intenciones, actitudes, conocimiento, motivaciones, así como características demográficas y de su estilo de vida. Estas preguntas se pueden hacer verbalmente, por escrito, mediante una computadora, y las respuestas se pueden obtener en cualquiera de estas formas (Malhotra, 2008).

Las entrevistas se dividen en(Hernández, Fernández, & Baptista, 2010):

1) Estructuradas: El entrevistador realiza su labor con base en una guía de preguntas específicas.
2) Semiestructuradas: Se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener mayor información sobre los temas deseados.
3) Abiertas: Se fundamentan en una guía general del contenido y el entrevistador posee toda la flexibilidad para manejarla.

Para el presente estudio se eligió la entrevista abierta para poder obtener opiniones relativas a los planes de recuperación ante desastres.

2.3.2 CUESTIONARIOS

El uso de cuestionarios permite la recopilación de información para poder estudiar las actitudes, creencias, comportamiento y características de las personas que laboran en una organización. Los cuestionarios pueden ser utilizados para aplicar una encuesta a una muestra considerable de la población, con el fin de poder detectar problemas (Kendall & Kendall, 2005).

“Un cuestionario, es un conjunto formalizado de preguntas para obtener información de los encuestados.” (Malhotra, 2008). Se puede decir que uno de los instrumentos que tiene una mayor aplicabilidad para facilitar la recolección de los datos es el cuestionario, que está formado por una serie de preguntas basadas en variables de las cuales se desea obtener algún tipo de medición, en los cuestionarios se tiene dos tipos de preguntas (Hernández et al., 2010):

1) Abiertas: Este tipo de preguntas no delimitan las alternativas de respuesta lo cual puede ocasionar un número elevado de las mismas, en teoría es infinito y

puede variar de población en población. Son útiles cuando no hay suficiente información sobre las posibles respuestas.

2) Cerradas: Contienen categorías u opciones de respuesta que han sido previamente delimitadas, se presentan las posibilidades de respuesta a los entrevistados quienes se deben limitar a contestar en base a las respuestas presentadas. Este tipo de pregunta es la más sencilla de analizar y codificar.

Los objetivos que se persiguen con el uso de los cuestionarios son (Malhotra, 2008):

1) Debe traducir la información necesaria en un conjunto de preguntas específicas que los encuestados puedan responder. Este objetivo es un reto ya que es difícil desarrollar preguntas que los encuestados puedan y quieran responder y que brinden la información deseada.
2) Debe animar, motivar y alentar al encuestado para que participe activamente en la entrevista, colabore y concluya el proceso. El investigador debe esforzarse por minimizar la fatiga, el aburrimiento, la falta de interés o la ausencia de respuestas por parte del encuestado.
3) Se debe minimizar el error de respuesta, este surge cuando los encuestados dan respuestas incorrectas, o cuando sus respuestas se registran o analizan mal. El cuestionario puede ser una fuente importante de error de respuesta.

La elección del tipo de preguntas que contenga el cuestionario depende del grado en que se puedan anticipar las posibles respuestas, los tiempos de que se disponga para codificar y si se quiere una respuesta más precisa o profundizar en alguna cuestión. Una recomendación para construir un cuestionario es que se analice, variable por variable, que tipo de pregunta o preguntas suelen ser más confiables y válidas para medir esa variable , de acuerdo con la situación del estudio (Hernández et al., 2010).

En la presente investigación se desarrolló un cuestionario con preguntas cerradas para delimitar las posibles respuestas de los entrevistados que permita un mejor análisis y codificación del cuestionario.

CAPÍTULO III METODOLOGÍA

Después de describir el marco teórico, es preciso estipular la metodología de la investigación a utilizar. Esta involucra el tipo de enfoque, método, diseño, instrumentos y fuentes de información que serán necesarios para llevar a cabo el estudio. La metodología de la investigación sirve de guía, ya que establece que se utilizará para poder recabar información valiosa.

3.1 ENFOQUES Y MÉTODOS

Se presenta el enfoque mixto de la investigación, que implica un proceso de recolección, análisis y vinculación de datos cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento del problema. El enfoque cuantitativo usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías. Lo que pretende el enfoque cualitativo es obtener datos proporcionando descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones. (Hernández et al., 2010, p. 9)

El siguiente diagrama muestra el enfoque y los métodos a utilizar en la presente investigación.

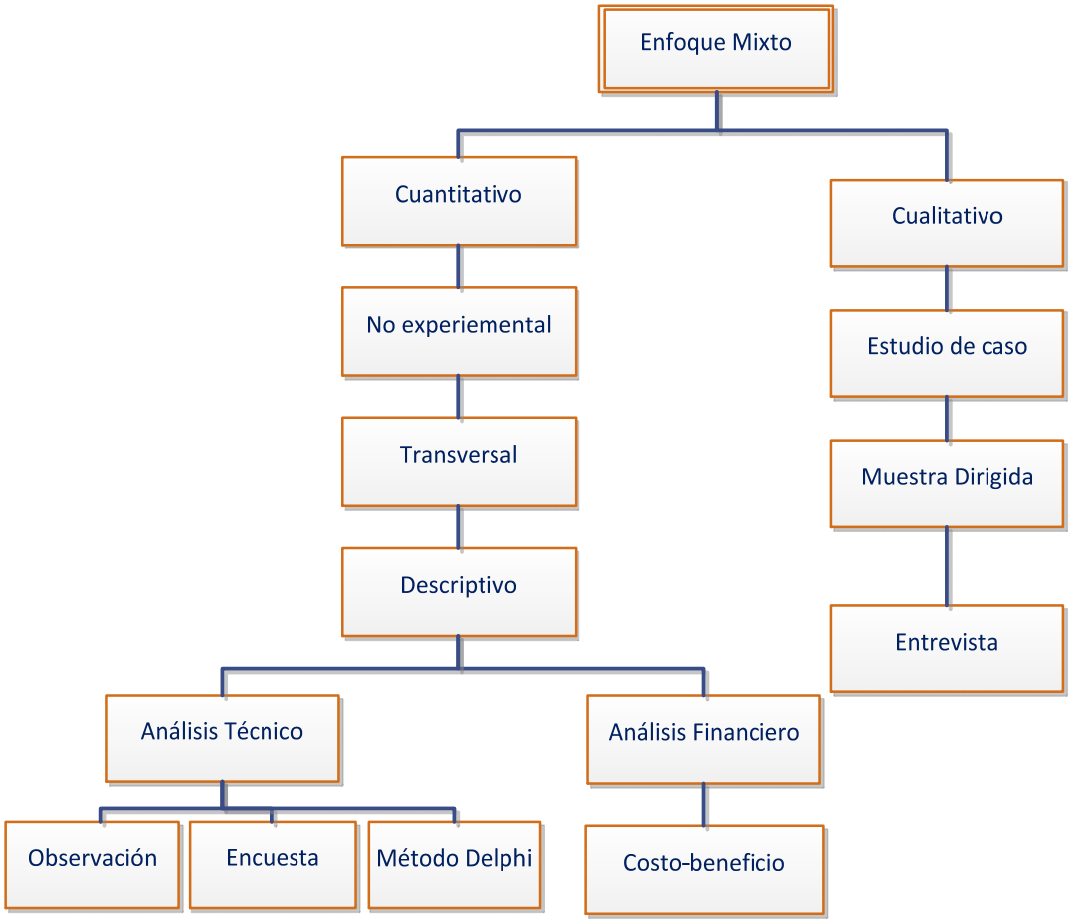

Figura 17. Enfoque del estudio

La figura 17, representa el enfoque de la investigación que se determinó que es mixto ya que involucra la combinación de enfoques cualitativos y cuantitativos. Para el correspondiente estudio, el enfoque cuantitativo es de tipo no experimental debido a que las variables de investigación no se manipulan permanecen tal cual se encuentran, solo se limita a observar el comportamiento dentro del proceso de exploración. Cabe mencionar, que el estudio es transversal, ya que la recolección de información se realiza una única vez. El alcance de la investigación es de carácter descriptivo, pues describe las variables, se efectúan dos análisis: técnico y financiero, en los que se aplican los instrumentos idóneos para los estudios que darán respuesta a las interrogantes y objetivos planteados en el capítulo uno.

El análisis técnico se encuentra basado en la recolección de información por medio de la observación y encuesta que dará respuesta a las siguientes preguntas y objetivos.

1) Preguntas

   1.1) ¿Cuál es el tiempo máximo permitido para tener fuera de servicio las aplicaciones?

   1.2) ¿Cuál será la mejor ubicación estratégica para contar con un sitio alterno de respaldo de las operaciones del negocio?

   1.3) ¿Cómo se lleva a cabo la gestión de los riesgos en cuanto a seguridad?

2) Objetivos

   2.1) Identificar el tiempo máximo, pérdidas monetarias, ubicación y el periodo de tiempo de actualización.

   2.2) Diseñar una metodología de gestión de riesgo en base a la seguridad.

Para el Análisis financiero se incluyen:

1) Pregunta

   1.1) ¿Cuál es el costo que tiene la empresa al no poder tener en funcionamiento sus aplicaciones críticas?

2) Objetivos

   2.1) Identificar el tiempo máximo, pérdidas monetarias, ubicación y el periodo de tiempo de actualización.

2.2) Determinar la ubicación del sitio alterno.

3.2 DISEÑO DE LA INVESTIGACIÓN

De la naturaleza del problema depende el diseño de la investigación que se debe emplear (Malhotra, 2008).Este se refiere a la estrategia concebida para obtener la información que se desea (Hernández et al., 2010). A continuación se describe la población, muestra y la unidad de análisis.

3.2.1 POBLACIÓN

La población es el conjunto de elementos u objetos que poseen la información buscada por el investigador y acerca del cual se harán deducciones. Todos los elementos comparten un conjunto común de características que constituyen el universo para el propósito del problema a estudiar. La población debe definirse en términos de los elementos, las unidades de muestreo, la extensión y el tiempo (Op. Cit.). Para la presente investigación se cuenta con una población finita la cual está conformada por el personal que labora en la unidad de infraestructura informática de COCESNA cuya función es administrar los equipos y sistemas de cada uno de los departamentos que se encuentran dentro de la empresa, Dicho personal posee el conocimiento y experiencia con respecto al área en función, lo que permite conocer los diversos puntos de vista sobre los planes de recuperación ante desastres conforme a la experiencia en el medio de trabajo que desempeñan.

3.2.2 MUESTRA

“La muestra es un subconjunto de la población que brindara información específica del universo a estudiar.” (Hernández et al., 2010), Muestra no probabilística o dirigida es un subgrupo de la población en la que la elección de los elementos no depende de la probabilidad sino de las características de la investigación (Op.Cit). La muestra intencional se basa en juicios. El muestreo ayuda a acelerar el proceso mediante la

recopilación de datos seleccionados, la efectividad en el proceso de recolectar los datos es un aspecto importante (Kendall & Kendall, 2005).

La porción seleccionada es el personal en su totalidad, descrito anteriormente en la sección de la población, que labora en la unidad de Infraestructura Informática. El tamaño de la muestra es tomar su totalidad de su población a causa de su proporción reducida, la cual tiene un total de ocho personas.

3.2.3 UNIDAD DE ANÁLISIS

“Unidades de análisis se le denomina casos o elementos.” (Hernández et al., 2010). La unidad de análisis en el estudio está conformada por las personas que forman parte de las muestras seleccionadas en la población, los individuos que llamaremos personal técnico.

3.2.4 UNIDAD DE RESPUESTAS

Al tener definido la población, la muestra y la unidad de análisis se procede a la elaboración de las encuestas y entrevistas para encontrar respuestas a las preguntas de investigación. Dicha información se utilizó para poder desarrollar las conclusiones y recomendaciones de la presente tesis. El enfoque de la investigación es mixto por lo cual las respuestas son de tipo cualitativa y cuantitativa, En el presente trabajo de investigación la unidad de respuesta a determinar es el tiempo de recuperación de información en caso de un desastre.

3.3 INSTRUMENTOS Y TÉCNICAS

Establecido el enfoque, métodos del estudio y el diseño de la investigación, se debe seleccionar las técnicas e instrumentos de medición aplicables al estudio para recabar información sobre las variables que se estudian. Al recurrir a los instrumentos y técnicas se debe tener en consideración los aspectos que ofrezcan certeza en la

información, de manera que sea auténtico. “Toda medición o instrumento de recolección de datos debe reunir tres requisitos esenciales: confiabilidad, validez y objetividad.” (Hernández et al., 2010)

3.3.1 INSTRUMENTOS

Una vez que se ha identificado y clasificado el tipo de información que se necesita para resolver un problema, se procede agrupar dicha información, para ello es necesario seleccionar los instrumentos que servirán para recabar los datos y proseguir con el análisis (Benassini, 2009). A continuación se detallan los instrumentos a utilizar en el estudio.

3.3.1.1 CUESTIONARIOS

“Un cuestionario es un conjunto formalizado de preguntas para obtener información de los encuestados.” (Malhotra, 2008). El uso de cuestionarios es una práctica de recopilación de información que permite estudiar las actitudes, creencias, comportamientos y características de muchas personas en la organización que podrían resultar afectadas por los sistemas actuales y los propuestos, los cuestionarios se pueden usar para para encuestar a la muestra seleccionada para detectar los problemas o poner de manifiesto aspectos importantes antes de que se realicen las entrevistas (Kendall & Kendall, 2005). El cuestionario consta de un total de 12 preguntas las cuales son del tipo escala de Likert.

El cuestionario utilizado para recabar la información para poder contestar las preguntas de investigación se puede encontrar en el anexo 1.

Tabla 5. Relación de variables

Preguntas del Cuestionario	Variables	Hipótesis	Preguntas del Estudio
Aplicaciones administrativas que son consideradas críticas	Respaldos	Hi: El tiempo máximo de recuperación de la información se ve afectada por el manejo de los riesgos, accesibilidad de los servicios, respaldo de datos, costos y ubicación.	2) ¿Cuál es el tiempo máximo permitido para tener fuera de servicio las aplicaciones? 6) ¿Cuál es el tiempo máximo que se tendrán almacenados los respaldos de datos?
De los siguientes posibles riesgos, cual considera que pueden afectar las operaciones del negocio	Manejo de Riesgos	Hi	4) ¿Cómo se lleva a cabo la gestión de los riesgos?
Nivel de conocimiento del procedimiento a seguir en caso de presentarse una situación de desastre en la infraestructura tecnológica dentro de la empresa	Accesibilidad Manejo de Riesgos		
Existe un plan de contingencia ante desastres que este operativo dentro de la empresa	Accesibilidad		4) ¿Cómo se lleva a cabo la gestión de los riesgos?
De existir un plan de contingencia ante desastre definido dentro de la empresa ¿cuál es su frecuencia de actualización?	Actualización		1) ¿Cuál es la frecuencia de actualización de los planes de contingencia?
Ha existido algún incidente mayor en la infraestructura tecnológica bajo la cual operan los servicios administrativos de la empresa en los últimos 24 meses, cual fue la magnitud de los daños.	Manejo de Riesgos		4) ¿Cómo se lleva a cabo la gestión de los riesgos?
En caso de un incidente en la infraestructura tecnología quien es el responsable de activar nuevamente los servicios.	Accesibilidad		
¿Qué tiempo máximo permitido se tiene definido para estar sin servicio de la infraestructura tecnológica?	Accesibilidad	Hi	2) ¿Cuál es el tiempo máximo permitido para tener fuera de servicio las aplicaciones?
¿Qué estrategia de respaldo de datos se lleva a cabo dentro de la empresa?	Respaldos		4) ¿Cómo se lleva a cabo la gestión de los riesgos?

Continuación de Tabla 5. Relación de variables

Preguntas del Cuestionario	Variables	Hipótesis	Preguntas del Estudio
Seleccione según su criterio el sitio alterno para recuperar las operaciones del negocio en caso de presentarse un desastre.	Ubicación	Hi	3) ¿Cuál será la mejor ubicación estratégica para contar con un sitio alterno de respaldo de las operaciones del negocio?
Tiempo máximo que una aplicación ha estado fuera de servicio. ¿Cuál ha sido su consecuencia?	Accesibilidad Costos		5) ¿Cuál es el costo que tiene la empresa al no poder tener en funcionamiento sus aplicaciones críticas?

3.3.1.2 GUIA DE LA ENTREVISTA

Se utilizó un método de entrevista abierta con el fin de obtener la mayor cantidad de información de parte del entrevistado. Se buscó obtener la opinión relacionada a la experiencia del Jefe de Infraestructura Informática en el campo de los planes de recuperación ante desastres y como estos se llevan dentro de la empresa. En dicha guía se tomó en cuenta las variables de investigación para la formulación de las preguntas, algunas de las cuales fueron:

1) Se tienen identificados y tratados los posibles riesgos que puedan suceder en la plataforma tecnológica de la empresa.
2) Está definido el RPO y RTO que se puede ofrecer en caso de algún desastre.
3) En general cual ha sido su experiencia con el tema de los planes de recuperación ante desastres dentro de la empresa.

3.3.2 TÉCNICAS

Las técnicas sirven para la recolección de datos pueden ser variadas y de acuerdo al estudio de investigación se emplean las que se acoplen mejor al tipo de datos que se obtendrán. La selección de las técnicas se toma en consideración el enfoque mixto del

estudio que incluye técnicas cuantitativas y cualitativas. Para el desarrollo de la investigación se aplicaron las técnicas que se detallan a continuación (Sampieri & Collado, 2010).

3.3.2.1 ENTREVISTA

En esta técnica se pretende recabar información mediante una conversación dirigida con un propósito específico que utiliza un formato de preguntas y respuestas. En la entrevista se necesita obtener opiniones de los entrevistados y su parecer acerca del estado actual, metas organizacionales y personales y procedimientos informales (Kendall & Kendall, 2005). En la investigación se realizó una entrevista cara a cara con el Jefe de Infraestructura Informática, de forma abierta

3.3.2.2 MÉTODO DELPHI

Se procedió a la aplicación del método Delphi para identificar los riesgos potenciales que afectan las operaciones del negocio. Para ello, se reunión a un grupo de expertos tomando una lista inicial de riesgos que se consideran pueden ocasionar la no operación del negocio y en base a ello realizar una efectiva identificación de los riesgos más importantes a los que se le debe dar tratamiento.

3.3.2.3 ENCUESTA

La técnica de la encuesta es un cuestionario estructurado que se aplica a la muestra de una población y está desarrollado para obtener información específica de los participantes. El uso de preguntas de alternativa fija reduce la variabilidad de los resultados que habría por las diferencias entre los encuestadores, al finalizar la codificación, el análisis y la interpretación de los datos resulta relativamente sencillos (Malhotra, 2008). Esta técnica se aplicó al personal técnico que labora en la unidad de infraestructura tecnológica de COCESNA. Las interrogantes que se utilizaron en esta técnica se pueden apreciar en el anexo 1.

3.3.2.4 CONFIABILIDAD

La confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo individuo u objeto produce resultados iguales (Hernández et al., 2010). En el estudio se utilizó la ecuación del método del coeficiente de Kendall, para validar el número total de expertos que se deben tener en la presente investigación. Mediante el programa SPSS 22.0 se procedió a realizar el análisis para pruebas no paramétricas (W) de Kendall para probar el acuerdo de los expertos que contestaron la encuesta.

Tabla 6 Coeficiente de concordancia de kendall

N	8
W de Kendall[a]	,682
Chi-cuadrado	92,760
Gl	17
Sig. asintótica	,000

Fuente: SPSS 22.0

En la tabla 6, se muestra el resultado de la prueba no paramétrica (W) de Kendall, en la cual se obtuvo un valor de 0.682, lo que indica que las ocho personas encuestadas son expertos en la temática consultada.

3.3.3 PROCEDIMIENTOS

Para la aplicación de las técnicas descritas anteriormente es imprescindible planificar el proceso a desarrollar para la compilación de la información. En primer lugar se elaboró un cuestionario para la encuesta y la entrevista, estos incluyen preguntas relevantes para obtener los datos donde se aplicara al personal que labora en la unidad de infraestructura tecnológica, recabando información desde las diferentes perspectivas de entorno a investigar. Antes de aplicar los instrumentos y técnicas se realizó una validación de las interrogantes.

3.3.1 ENCUESTAS

Para la elaboración de la encuesta se tomaron en cuenta tanto las variables del presente estudio y en base a ello se formularon las preguntas que fueron consultadas a los miembros que forman parte de la muestra. Las preguntas formuladas en su totalidad utilizan la escala de Likert que permite medir las respuestas cerradas por rangos. Con el cuestionario formulado se procedió a diseñar el mismo haciendo uso de la herramienta para encuestas de google drive, finalizada la encuesta se procedió a enviar a los correos electrónicos del personal técnico que labora en la unidad de infraestructura informática de COCESNA. Una vez completas las encuestas se procedió con la tabulación y análisis de los datos auxiliándose de la herramienta estadística SPSS 22.0

3.3.2 ENTREVISTA

La entrevista se hace con el propósito de conocer la opinión de las personas en relación a una serie de preguntas planteadas de forma abierta, mediante la realización de una plática cordial con el entrevistado. Para la realización de la entrevista se hizo uso de la grabadora de voz de un teléfono celular para dejar constancia de los diferentes temas tratados. La entrevista fue dirigida al Lic. Denis Alberto Sánchez Jefe de Infraestructura Informática para conocer y profundizar sobre los planes de contingencia de la empresa específicamente en el área administrativa. Dicha entrevista se llevó a cabo en las oficinas del Lic. Sánchez en COCESNA, en horas de la tarde del día veintinueve de abril.

3.4 FUENTES DE INFORMACIÓN

Proporcionan datos de primera mano, pues se trata de documentos que contienen los resultados de los estudios correspondientes (Hernández, Fernández, & Baptista, 2010). Las fuentes de información lo constituyen los documentos de donde se obtienen la

información para el análisis e interpretación, en otras palabras esparcen los conocimientos de una determinada área de interés.

3.4.1 FUENTES PRIMARIAS

Las fuentes primarias que se utilizaron son:

1) Documentación del proceso.
2) Artículos.
3) Documentos oficiales.
4) Tesis.
5) Libros.
6) Páginas de internet.
7) Entrevistas.
8) Grupos de discusión.
9) Encuestas.

3.4.2 FUENTES SECUNDARIAS

Entre las fuentes secundarias utilizadas están:

1) Fuentes electrónicas.
2) Manual para la redacción de tesis.

CAPÍTULO IV RESULTADOS Y ANÁLISIS

En los capítulos anteriores se definió el contexto específico del objeto de la presente investigación detallando cada etapa, iniciando con el planteamiento del problema, seguidamente la redacción del marco teórico y la selección de la metodología delimitando el universo y la muestra. En base a la información anterior se elaboró los instrumentos para proceder a la obtención de los resultados y analizar dicha información con respecto a las preguntas de investigación e hipótesis planteadas.

4.1 TIEMPO DE RECUPERACIÓN DE INFORMACIÓN

El tiempo de recuperación de la información tiene como objetivo determinar el tiempo máximo en el cual se debe tener recuperado un equipo o sistema para reiniciar los trabajos después de haberse suscitado un desastre

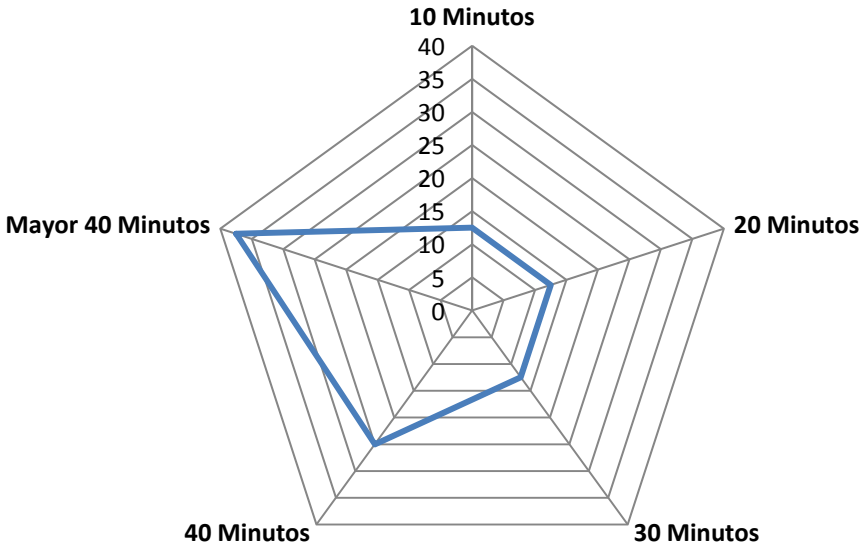

Figura 18. Tiempo de recuperación de la infraestructura tecnológica.

En la figura 18, se puede observar que en general el tiempo máximo en la cual se puede estar sin acceso a la plataforma tecnológica es mayor a los 40 minutos. Esto

indica que pudieran existir que algunas de las variables independientes detectadas en el presente estudio pudieran estar influenciando para que el tiempo de recuperación fuera mayor o menor. En la entrevista realizada al Jefe de Infraestructura Informática se corroboro que el período de recuperación de los equipos en su mayoría se encuentra arriba de los 40 minutos y que en cuanto a la recuperación de los datos es de 24 horas y se cuenta con respaldo máximo de hasta 15 días. El respaldo de la información se realiza de forma diaria en horas de la noche, razón por la cual el respaldo de datos es de 24 horas. Adicionalmente indico que no se tiene establecida ninguna clasificación de criticidad de los datos por lo cual en el respaldo de datos se agregan los datos estructurados y no estructurados.

Dentro de la herramienta de la encuesta se presentó una matriz de algunos de los sistemas administrativos importantes dentro de la empresa para que el personal encuestado pudiera identificar los que se consideran críticos para la organización. En la figura 19 se puede observar que el sistema de Facturación y Cuentas por cobrar es considerado el más crítico, por lo cual el tiempo máximo que puede estar fuera de operación deberá ser bajo.

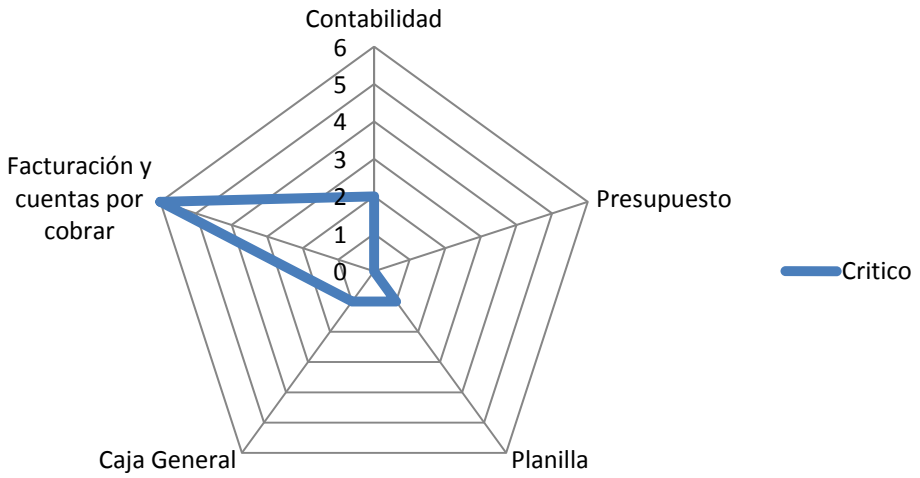

Figura 19. Nivel de criticidad de los sistemas dentro de la empresa.

Para mejorar el tiempo de recuperación de los datos de las aplicaciones críticas se debe disminuir la frecuencia del respaldo de datos, activando la replicación de base de datos hacia el equipo que se tenga en funcionamiento en el sitio alterno. Dicha replica de datos se puede generar cada hora, así el RPO será de 60 minutos mejorando el tiempo actual de 24 horas.

Para la validación de la hipótesis y tomando en cuenta que los datos no son paramétricos y la muestra es menor a 30 encuestados, se hizo uso de la prueba de Kruskal-Wallis que sirve para identificar si las muestras proceden de la misma población o de poblaciones idénticas con la misma mediana. La prueba de Kruskal-Wallis funciona como contraparte no paramétrica del diseño completamente utilizado en las pruebas de ANOVA (Webster, 2000). Las pruebas estadísticas permiten comprobar si existe relación entre la variable dependiente y las variables independientes, que generan un número para representar la fuerza de relación.

La distribución de la prueba de Kruskal-Wallis es aproximada por una distribución de Chi-cuadrado, que permite determinar si el comportamiento de las variables presenta diferencias estadísticamente significativas. El cálculo del Chi-cuadrado muestra el resultado un valor numérico denominado alfa (α), este valor debe ser comparado con el valor teórico de 0.05. Cuando el valor calculado es menor al 0.05 se rechaza la hipótesis nula, con lo que se concluye que existe una relación entre las variables, en el caso contrario si el valor calculado es mayor de 0.05 no se rechaza la hipótesis nula aceptando que no existe ninguna relación entre las variables.

Para determinar la prueba se hizo uso de la herramienta del SPSS 22.0.

Tabla 7. Prueba de Kruskal-Wallis

	Riesgos	Admon	Tipo	5. Existe un plan de contingencia ante desastres que este operativo dentro de la empresa	6. De existir un plan de contingencia ante desastre definido dentro de la empresa ¿cuál es su frecuencia de actualización?	10. Qué estrategia de respaldo de datos se lleva a cabo dentro de la empresa.
Chi-cuadrado	5,833	5,250	5,833	7,000	7,000	4,986
Gl	4	4	4	4	4	4
Sig. Asintótica	,212	,263	,212	,136	,136	,289

	11. Seleccione según su criterio el sitio alterno para recuperar las operaciones del negocio en caso de presentarse un desastre	12. Tiempo máximo que una aplicación ha estado fuera de servicio. ¿Cuál ha sido su consecuencia
Chi-cuadrado	4,733	3,400
Gl	4	4
Sig. Asintótica	,316	,493

Fuente: (SPSS,2014)

En la tabla 7, se muestran los resultados de la prueba de Kruskal-Wallis para las variables independientes y dependientes del estudio realizado. En dicha tabla se puede observar que los valores relativos a la significancia asintótica son mayores a un nivel de significancia (valor alfa α) de 0.05 en cada una de las preguntas aplicadas y que se encuentran relacionadas con las variables de investigación del presente trabajo. Por lo tanto se acepta la hipótesis nula. En base a lo anterior se demuestra que el tiempo máximo de recuperación de la información no se ve afectada por el manejo de los riesgos, accesibilidad de los servicios, respaldo de datos, costos y ubicación.

4.2 ACTUALIZACIÓN

Uno de los aspectos importantes que se deben tomar en cuenta en los planes de recuperación ante desastres es determinar el período en el cual dichos planes deberán ser actualizados. En dichas actualizaciones se debe determinar si la información publicada sigue vigente o es necesario realizar ajustes de acuerdo a cambios que se

hayan tenido ya sea en la infraestructura tecnológica, recurso humano, identificación de riesgos.

Para determinar la frecuencia de actualización del plan dentro de COCESNA se le consultó al personal que labora en el área de infraestructura informática si conocían cual era el período en el cual se realizaba la actualización del plan.

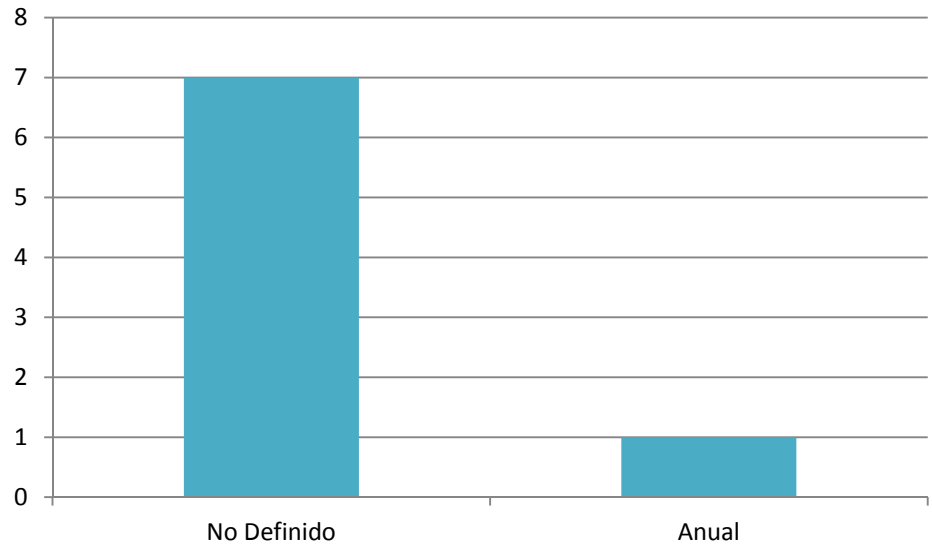

Figura 20. Frecuencia actualización plan recuperación

En la figura 20, se puede observar que siete personas entrevistas indicaron que la frecuencia de actualización del plan de recuperación antes desastres de la empresa no se encuentra definido, solo una persona contesto que el período de actualización era de forma anual. En la tabla 8, se muestra un cruce entre la pregunta relacionada a la frecuencia de actualización del plan y el tiempo que tiene de laborar el personal dentro de la empresa. Esto con el fin de determinar qué tan familiarizado puede estar el personal con el plan de recuperación ante desastres que existe en la empresa.

Tabla 8. Cruce variable actualización con antigüedad laboral

		1. Cuanto tiempo tiene de laborar en la empresa			
		0-4	10-14	15-19	Total
6. De existir un plan de contingencia ante desastre definido dentro de la empresa ¿cuál es su frecuencia de actualización?	No Definido	1	4	2	7
	Anual	1	0	0	1
Total		2	4	2	8

En la tabla anterior se puede observar que la mayoría de los casos que identificaron que no está definido la frecuencia de actualización del plan de recuperación en su mayoría son personas que tienen mayor antigüedad laboral, no así una sola persona que tiene de 0-4 años de laborar en la empresa y que respondió que el plan de recuperación se hace de forma anual. En la entrevista realizada al Jefe de Infraestructura Informática indico que la frecuencia de actualización del plan no se encuentra definido, lo cual viene a representar un problema en el caso que se tenga que activar el plan de recuperación ante desastres ya que el mismo estaría desfasado en cuanto al equipo, personal y acciones que se deberán tomar para la correcta ejecución del plan.

En la empresa se cuenta con un plan cuya fecha de elaboración fue en el año 2007 y desde entonces no se ha realizado ninguna modificación aunque si se han cambiado equipos, personas, aplicaciones. Para la elaboración del nuevo plan de recuperación ante desastres se deberá tomar como base la metodología propuesta por el DRI (Disaster Recovery Institute), la cual tiene como temas principales los siguientes:

1) Análisis del Impacto del Servicio.
    1.1) Relación de Procesos.
    1.2) Relación de Aplicaciones.
    1.3) Relación de Departamentos y Usuarios.
    1.4) Determinar Procesos Críticos.

1.5) Periodo Máximo de Interrupción.

2) Evaluación de Riesgos.
   2.1) Identificar los Activos.
   2.2) Identificar Amenazas.
   2.3) Evaluar Vulnerabilidades.
   2.4) Evaluar Impacto.
   2.5) Evaluar el Riesgo.
   2.6) Evaluar Contramedidas.
3) Desarrollo de Estrategias de Mitigación.
   3.1) Selección de Estrategia.
4) Desarrollo del plan de continuidad del servicio.
   4.1) Organización de Equipos.
   4.2) Desarrollo de Procedimientos.
5) Entrenamiento, Pruebas y Auditoría.
6) Mantenimiento del plan de continuidad del servicio.

Dentro del plan de recuperación es importante quede definida la frecuencia de actualización de la información así como el periodo en el cual se estarán realizando pruebas al mismo y que personas serán las encargadas de realizar dichas tareas. Así mismo se deberá crear una conciencia dentro del personal de infraestructura informática para que dichos planes no queden en el abandono por el contrario tengan una actualización periódica. Para la ejecución del plan se debe de tomar en cuenta la participación de todo el equipo que sea designado para tal fin.

4.3 RESPALDOS

Los respaldos representan la manera idónea de proteger los activos de la empresa, para comprender la importancia de estos, la encuesta arrojó los siguientes datos significativos relacionando la variable independiente de respaldo y la variable dependiente de tiempo de recuperación de la información.

En la figura 21, se muestra el conocimiento del procedimiento a seguir en el aspecto de los respaldos de la información a realizar. Existen diferentes puntos de vistas en relación a los tipos de estrategias de respaldar la información en COCESNA, donde el 50% contestó que el tipo de estrategia de respaldo de datos utilizada en la organización es mixta, que incluye las estrategias de tipo total e incremental. Por otra parte un 25% manifestó que la estrategia de respaldo es incremental, que involucra el procedimiento poco a poco a medida se efectúen los cambios en los datos.

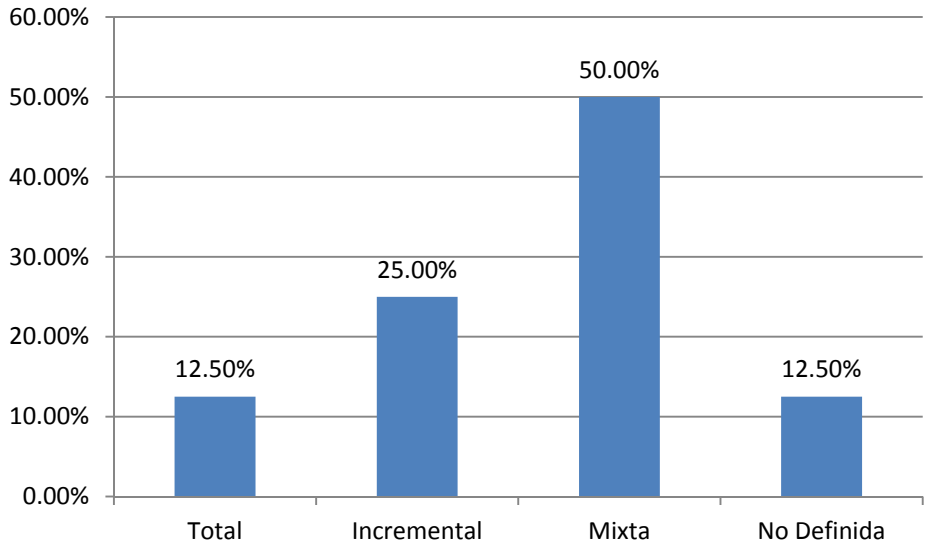

Figura 21. Respaldo de Datos

Un 12.5% definió que la estrategia utilizada es la de tipo total donde se respaldan todos los datos que se poseen en la empresa y por último el 12.5% no conoce una estrategia definida en la empresa para el respaldo de los datos. Por lo cual se debe comunicar el proceso de respaldo de datos de una manera que sea del conocimiento del personal.

Actualmente en la empresa está definida una estrategia de respaldo de la información mixta, haciendo un respaldo total de los datos al inicio de la semana (lunes) y el resto de días se ejecuta la estrategia incremental. Esta actividad se hace de forma automática cada 24 horas respaldando los datos no estructurados y estructurados así

como una imagen de los servidores. Para mejorar el tiempo de recuperación de los datos es necesario realizar una clasificación de la información para en base a esto poder determinar la frecuencia del respaldo y el tiempo máximo de retención de la misma. Para los datos estructurados (Base de datos) se deberá acortar el tiempo actual de 24 horas, para ello se requiere que se habilite la replicación de base de datos con el sitio alterno el cual se debe ejecutar cada 60 minutos.

4.4 ACCESIBILIDAD

La variable de accesibilidad se analiza por el período determinado en el cual sucede algo que imposibilita brindar un servicio en el curso de las operaciones de la empresa. En la figura 22 se observa el tiempo de accesibilidad.

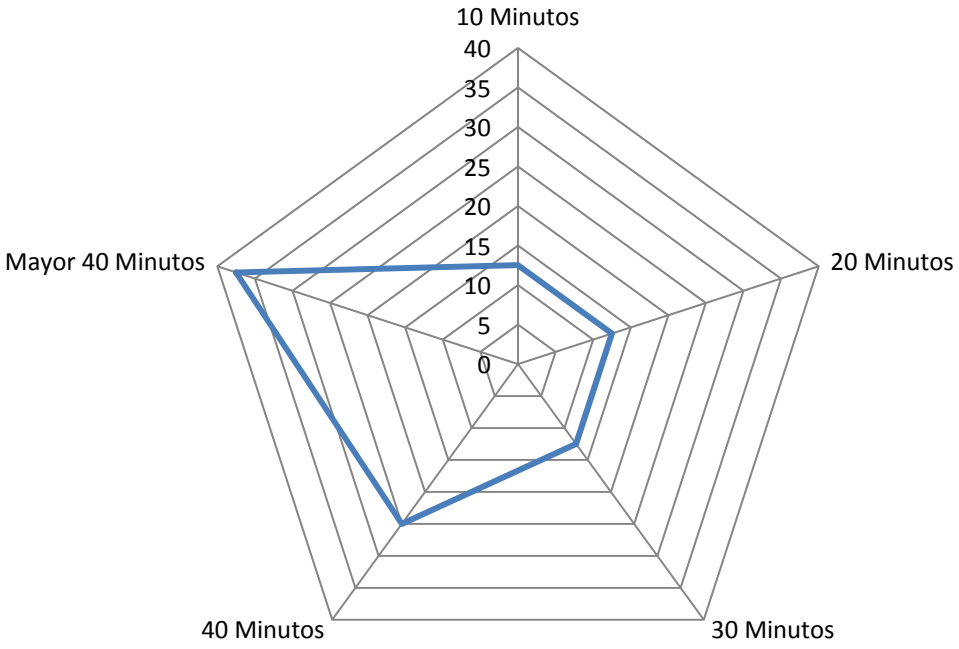

Figura 22. Tiempo de accesibilidad.

La figura anterior demuestra que al presentarse una interrupción de las aplicaciones administrativas se accede a estas, con una espera de más de 40 minutos de tardanza

que representa el 38%, continuando con los resultados del tiempo de accesibilidad se obtiene un 25% en la accesibilidad a los 40 minutos de pérdida de las conexiones, dependiendo de las aplicaciones, fecha del mes y criticidad se establecen dichos enlaces para toda la empresa.

Al proponer un tiempo de accesibilidad a las aplicaciones administrativas se requiere de preparación metódica e inversión de recursos financieros y técnicos para poseer de inmediato el acceso a todas las instancias de la empresa.

En la actualidad dentro de la empresa se ha realizado una inversión para mejorar la plataforma tecnológica la cual está completamente virtualizada contando con el licenciamiento VMware para tal efecto. Dicha plataforma ha permitido un mejor tiempo de respuesta en caso de falla de alguno de los servicios virtualizados contando con un tiempo en algunos casos mayor a los 40 minutos. El tiempo de recuperación del equipo podría ser mayor (días, semanas) en caso de presentarse algún tipo de desastre en el centro de datos principal que afecte directamente las operaciones de la infraestructura tecnológica del área administrativa ya que en la actualidad no se cuenta con equipo de repuesto donde se pueda poner a funcionar las aplicaciones si falla el equipo principal, en dichos casos se tendría que coordinar con los diferentes proveedores la disponibilidad de equipo que pueda soportar las operaciones del negocio, la puesta en marcha nuevamente de la plataforma dependerá en el tiempo que el proveedor pueda suministrar el equipo mínimo para iniciar operaciones el cual puede ser un tiempo considerable.

Para mejorar la respuesta en caso de presentarse alguna falla causada por cualquier tipo de desastre se propone la creación de un sitio alterno que tenga el equipo y las configuraciones necesarias para poder activar en dicho sitio las operaciones críticas del negocio en caso de falla del equipo principal.

4.5 UBICACIÓN

La variable ubicación del sitio alterno se analizó en base a los resultados recopilados en la encuesta en la que se destacan a detalle cada elemento de esta variable. En la figura 23, se interpreta la ubicación del sitio alterno para mantener de forma permanente los datos de la empresa en caso de riesgo o desastre.

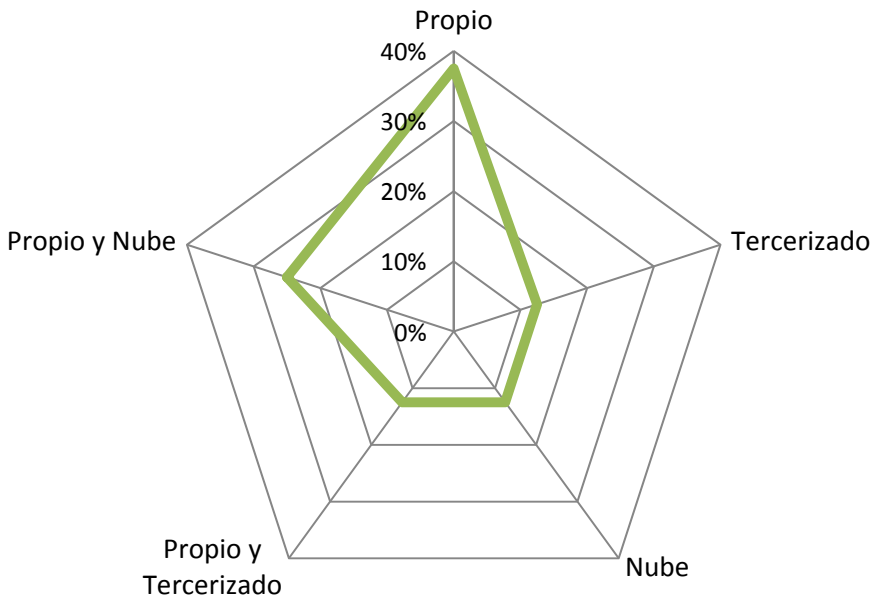

Figura 23. Ubicación sitio alterno.

Se puede observar que del total de la muestra encuestada, el 37.5% confirman que el lugar para ubicar el sitio alterno debe de pertenecer a la empresa de esta forma no se arriesga la manipulación de información sensible a personal extraño a la empresa. El 25% comparte la opinión de poseer el sitio propio y de forma simultánea tercerizar este servicio con esta estrategia de ubicación del sitio alterno, para mantener las opciones rentables e inmediatas en caso de emergencia. El otro 37.5% se dividen entre las opciones de sitio alterno tercerizado (12.5%), o contar con los datos en la Nube(12.5%), en igual porcentaje se encuentra la ubicación de propio y en la Nube.

La ubicación del sitio alterno se maneja de forma estricta ya que por políticas de la empresa se debe mantener los recursos propios por lo que este aspecto del plan de recuperación ante desastres y en particular dicha ubicación debe ser propio y en la nube son los perfiles que se enlazan bien en este punto.

En la actualidad COCESNA cuenta con un sitio alterno en la ciudad de San Salvador, El Salvador destinado para funcionar como contingencia en caso de presentarse algún desastre en el centro de control de tránsito aéreo ubicado en la ciudad de Tegucigalpa, Honduras. Dichas instalaciones cuenta con las características necesarias de un centro de datos, por lo cual se puede hacer uso de estas instalaciones para que funcione también como sitio alterno de la plataforma tecnológica administrativa logrando una reducción en los costos, solamente se deberá comprar el equipamiento necesario para respaldar las operaciones del negocio.

Tabla 9. Especificaciones equipo sitio alterno

Cantidad	Especificación
1	Servidor con procesador con capacidad de soportar como mínimo 30 máquinas virtuales, 128 GB de memoria RAM, capacidad en disco duro de 300 GB, cuatro tarjetas de red
1	Unidad de almacenamiento en red (SAN) con capacidad de 9TB con opción de expansión de capacidad futura.
1	Switch cisco de 12 puertos 10/100/1000 Gigabit

En la tabla 9, se detallan las especificaciones mínimas que deberá tener el equipo a ser instalado en el sitio alterno cuya función será alojar los servidores de las aplicaciones críticas de la empresa en caso de presentarse algún desastre en el centro de datos principal. Las características del equipo permitirán el suficiente espacio y procesamiento para alojar los sistemas críticos que actualmente se encuentran en funcionamiento que son alrededor de diez máquinas virtuales y se deja provisto para crecimiento futuro.

4.6 MANEJO DE RIESGOS

Los riesgos son una vulnerabilidad a la cual se enfrenta el negocio y donde se deben establecer las alternativas para contrarrestar los riesgos. En la tabla 10 se muestra la escala de riesgos de manejo aplicada a esta investigación.

Tabla 10.Escala de manejo de riesgos

1	2	3	4	5
Critica	Severo	Moderado	Normal	No Critica

De la tabla anterior se interpreta el valor uno es un riesgo crítico para el negocio y lo coloca en estado de alerta para identificar cada situación, el número dos es un riesgo severo el cual merece la atención del personal asignado a este aspecto, el número tres se le atribuye a un tipo de riesgo moderado pudiendo afectar a la empresa pero se puede tratar, el número cuatro es un riesgo de tipo normal al que se enfrenta el negocio y se puede aceptar y por último el valor cinco no representa criticidad para la empresa.

Los riesgos seleccionados para calcular su impacto son: Incendios, Incidentes de seguridad, fallas en los equipos, fallas de energía y el sabotaje. En la figura 24 se describe un promedio de los riesgos mencionados a evaluar en este estudio

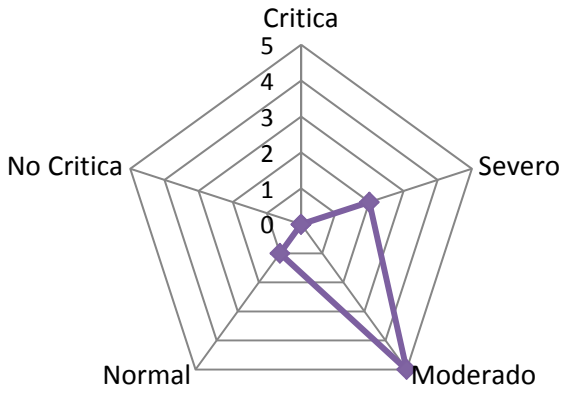

Figura 24. Categorización de riesgos.

La figura 24, muestra el resultado de calcular un promedio de los riesgos tratados, el 63% de los datos se encuentran en un riesgo moderado el cual indica que se debe de prestar atención a estos puntos para no llegar en un futuro cause daños al negocio, no obstante se debe tener presente que el 25% de los riesgos de tipo severo que al presentarse se pasaría a un estado muy complejo de resolver en la empresa, en última instancia con el 13% se ubica el tipo normal según la escala de riesgo detallada con anterioridad. Los puntos extremos de la escala no se encuentran en la empresa.

Tabla 11 Análisis de riesgos

	Riesgo	Consecuencia	Probabilidad	Severidad
1	Incendio	Mayor	Probable	Extremo
2	Falla en los Equipos	Mayor	Posible	Extremo
3	Incidentes de Seguridad	Mayor	Posible	Extremo
4	Sabotaje	Catastrófico	Improbable	Extremo
5	Guerra	Catastrófico	Raro	Alto
6	Falla de Energía	Mayor	Raro	Alto
7	Robo	Mayor	Raro	Alto
8	Artefactos Explosivos	Mayor	Raro	Alto
9	Incendio Provocado	Mayor	Raro	Alto
10	Ataque Terrorista	Mayor	Raro	Alto
11	Tormenta Eléctrica	Moderado	Raro	Moderado
12	Terremoto	Moderado	Raro	Moderado
13	Inundaciones	Moderado	Raro	Moderado
14	Huracán	Menor	Raro	Bajo
15	Huelgas	Menor	Raro	Bajo
16	Deslizamiento de Tierra	Insignificante	Improbable	Bajo
17	Incendio Forestal	Insignificante	Raro	Bajo
18	Erupción Volcánica	Insignificante	Raro	Bajo

En la tabla 11, se presenta un análisis de posibles riesgos que pudieran afectar las operaciones del negocio así como su nivel de criticidad y la probabilidad de ocurrencia del riesgo y en base a estos dos últimos factores se calcula el nivel de severidad en caso de presentarse el riesgo. Dicho análisis preliminar de riesgos puede servir como base para la creación del manejo de riesgos dentro de la empresa. Para atenuar la probabilidad y la consecuencia de los riesgos se debe realizar un tratamiento mediante la inserción de actividades y recursos en la operación diaria de la empresa encaminada a tomar acción oportuna para poder tener cualquiera de las siguientes opciones:

1) Eliminar el riesgo.
2) Reducir o mitigar el riesgo.
3) Trasladar a un tercero el riesgo.
4) Aceptar el riesgo.

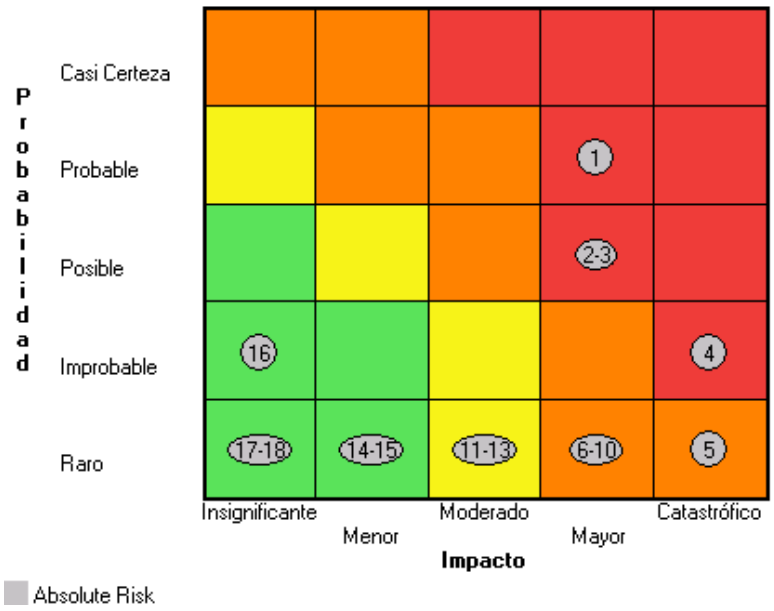

Figura 25. Mapa de Calor Riesgos.

En la figura 25, se observa el mapa de calor para los riesgos descritos en la tabla 9. Se puede observar que los riesgos que representan un gran impacto a la empresa en caso de que se presenten son: Incendio, Falla en los equipos, Incidentes de seguridad y Sabotaje. Se debe realizar un adecuado plan de acción para lograr mitigar en la medida de lo posible dichos riesgos.

En el anexo 2, se muestra un formato de matriz de gestión de riesgos en la cual se deben de analizar los efectos de cada riesgo y cuál será la estrategia de defensa para minimizarlo.

4.7 COSTOS

En la recolección de las fuentes primarias como ser la entrevista con el Jefe de Infraestructura Informática, se obtuvo información relacionado a que actualmente en la empresa no se tiene una identificación de los costos de no operación en los que podría incurrir la empresa en caso de no tener operativos sus sistemas administrativos. Dicha situación no permite conocer de forma exacta las pérdidas económicas a las que se puede enfrentar la empresa en caso de permanecer determinado tiempo sin operar.

Para poder dar una solución se propone la implementación de costo por servicio que permita conocer las pérdidas reales de la empresa por cada hora que se esté sin operación y cual deberá ser el umbral máximo permitido de pérdidas económicas que puede tener la empresa.

Analizando a detalle esta sección, se utiliza el Costo-Beneficio de la puesta en marcha del sitio alterno para la empresa. El análisis Costo-Beneficio, permite definir la factibilidad de las alternativas planteadas o de un proyecto a ser desarrollado.

Tabla 12. Análisis Costo/Beneficio

Características	Costo $	Beneficio $	Costo/Beneficio	Deseable	
				S	N
Adquisición del equipo necesario	$17,050.00	$50,000.00	2.93	X	
Operación del equipo	$4,000.00	$5,000.00	1.25	X	
Ubicación física	$1,500.00	$10,000.00	6.67	X	
Traslado del personal	$5,630.00	$5,630.00	1.00		X
Capacitación	$5,400.00	$10,000.00	1.85	X	
Accesibilidad inmediata a los sistemas	$ 33,580.00	$ 75,000.00	2.23	X	

Nota. Los valores representados en la tabla análisis costo/beneficio son datos estimados debido a la falta de elementos cuantitativos que permitan establecer dichos valores de una forma exacta.

En la tabla 12, se proyecta el análisis de costo/beneficio de la implementación del sitio alterno para respaldo de los sistemas administrativos de COCESNA, donde se obtuvo información para evaluar ambas alternativas, poseen costos altos pero al final se reflejan beneficios de la accesibilidad a las aplicaciones en el caso de presentarse una situación de desastres que interrumpa las operaciones en la sede central.

Al momento de tomar la decisión de la realización del plan de recuperación, mantenimiento y su actualización corresponde enumerar las ventajas que ofrecerá esta alternativa.

Pros para la implementación del DRP:

1) Minimizar las demoras al acceder a los recursos de la organización.
2) Proteger a la organización.
3) Seguridad en cuanto a la información.
4) Evitar la improvisación en cuanto a las decisiones al presentarse una situación de desastre.
5) Fiabilidad al mantener un plan actualizado y probado.
6) Conocimiento por parte del personal involucrado.
7) Trabajar con eficiencia de forma generalizada en la organización y la identificación de los bienes financieros y humano.
8) Reducción de pérdidas tras un incidente de desastre.

Contra de la implementación del DRP

1) Invertir recursos económicos para la adquisición del equipo, sitio alterno, capacitación del personal, pruebas y mantenimiento, entre otros.
2) Dedicar tiempo para una eficiente planificación, prueba y mantenimiento de la alternativa.

3) Participación directa de los involucrados donde se requiere mayor responsabilidad.
4) Actualización constante de las medidas del plan.

Colocando una balanza de los pros y contra del DRP en la organización se inclina en los ayudas que nos ofrecen ante una situación inesperada.

Es una alternativa ambiciosa que brinda beneficios a largo plazo y así procurar la continuidad del negocio, ya que es costoso mantener los sistemas respaldados y accesibles en cualquier momento.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se dan a conocer las conclusiones, que aunado al análisis de los resultados obtenidos de las fuentes primarias y fuentes secundarias, proporcionan una visión más amplia de la solución al problema de investigación planteado. De la misma manera se describen las recomendaciones que a juicio de los investigadores, son las acciones que COCESNA debe seguir para tener éxito en la elaboración de un plan de recuperación ante desastres.

5.1 CONCLUSIONES

En base a la información recopilada se presentan las siguientes conclusiones:

1) En base a los resultados obtenidos al aplicar la prueba de Kruskal-Wallis para datos no paramétricos, se acepta la hipótesis nula ya que según los datos estadísticos no existe una relación que afecta el tiempo de recuperación de la información de las variables de manejo de riesgos, costos, ubicación, accesibilidad, respaldos y actualización.
2) Dentro de COCESNA específicamente en el área que maneja la infraestructura informática administrativa no se tiene definido la frecuencia de actualización que deberá tener el plan de recuperación ante desastre lo que podría suponer algún inconveniente en el momento que se ejecute un plan desactualizado.
3) Con respecto a la estrategia de respaldo de los datos no se maneja un estándar por parte del personal encargado debido a ese punto se puede enfrentar en una situación de incertidumbre por no conocer de forma precisa el tipo de estrategia de respaldo de datos en la empresa.
4) La accesibilidad concierne y se encuentra relacionado con la ubicación del sitio alterno y así determinar el tiempo ideal para la accesibilidad de las aplicaciones administrativas de COCESNA.

5) La ubicación del sitio alterno es un aspecto que es punto crucial y depende del manejo interno que se define en COCESNA, los resultados nos revelan que se mantienen en la posición de que este sitio sea propio.
6) Los riesgos y su manejo nos conducen por la vía correcta en la administración de las organizaciones, en el caso particular de la empresa que se estudia se observa una alza hacia el punto crítico del riesgo, actualmente se encuentra en un estado medio pero si se descuida puede colocar en un estado que no será de tranquilidad.
7) Actualmente no existe una identificación de los costos de no operación ante la interrupción de los servicios y/o sistemas de la empresa, lo que no permite establecer con claridad las pérdidas económicas que se tendrían al no poder operar.
8) Al realizar la evaluación de la inversión para la ubicación de sitio alterno sobresalen con mayor peso los beneficios que se obtendrán al momento de presentarse una situación de desastre.

5.2 RECOMENDACIONES

Con la finalidad que en COCESNA se cuente con un adecuado plan de recuperación ante desastres, se hace el planteamiento de las siguientes recomendaciones:

1) Es necesario enfocar esfuerzos para identificar mejoras en las áreas de respaldo de datos, accesibilidad del equipo, manejo de riesgos que permita a la empresa poder ofrecer una pronta respuesta a los diferentes usuarios ante la presencia y declaración de ejecución del plan de recuperación de desastres y así minimizar lo más posible los costos de no operación de la empresa.
2) Tomando en consideración que los planes de recuperación ante desastres deben ser actualizados a lo largo del tiempo, se recomienda que dentro de la Jefatura de Infraestructura Informática se defina la frecuencia de actualización que deberá tener el plan, para asegurar que ante la necesidad de su ejecución no se encuentre ningún tipo de inconveniente.

3) Establecer políticas de respaldo de datos donde se difunde al personal asignado de realizarlo y manejar bitácoras de cada procedimiento ejecutado para que exista un registro preciso de los datos que se encuentran respaldados. Así mismo se debe realizar una clasificación de los datos para determinar los más críticos y poder disminuir el rango de tiempo en el cual se respalda dicha información y poder ofrecer mejores tiempos de recuperación de datos.
4) Revisar los procesos y la infraestructura tecnológica para ver en qué puntos se puede disminuir el tiempo de recuperación o si es necesaria la adquisición de nuevo equipo que permita reducir dichos tiempos de inactividad.
5) La ubicación del sitio alterno deberá ser en la ciudad de San Salvador, El Salvador considerando que en dicho país ya se encuentra en funcionamiento el centro de respaldo del centro de control de tránsito aéreo debidamente equipado y con personal técnico encargado de la operaciones del sitio alterno.
6) La elaboración del plan de riesgos integrando a todos los involucrados para no dejar por fuera algún aspecto concerniente a la gestión eficiente y eficaz de este tratado. Para la planificación se recomienda orientarse en base a un estándar de los que se encuentran estipulados ya que proporcionan una guía del actuar para que se maneje con éxito
7) Desde la perspectiva del análisis financiero es necesario poder determinar cuáles son los costos de no operación que tiene la empresa durante el tiempo que se encuentran fuera de servicio sus sistemas. Se recomienda realizar un estudio que permita determinar dichos costos y en base a ello poder tomar decisiones encaminadas a reducir el tiempo de recuperación de la información.
8) Aprobar el presupuesto para la compra del equipo necesario para el sitio alterno así como la capacitación y traslado del personal para realizar las actividades de instalación y configuración del equipo que se adquiera.

CAPÍTULO VI. APLICABILIDAD

En los capítulos anteriores se indagó y analizó la situación con respecto a la situación de COCESNA en cuanto a los planes de recuperación ante desastres. Al realizar el estudio de la situación que se encuentra la organización por medio de los resultados y análisis obtenidos en la investigación, conclusiones y recomendaciones sugeridas. La eventualidad de presentarse una emergencia ante desastre de cualquier índole conlleva al desarrollo de la aplicabilidad de un plan de acción a seguir para el tratamiento y recuperación en cualquier instancia.

Tabla 13. Verificación de la concordancia del documento con el plan de acción

Título	Objetivo		Conclusiones	Recomendaciones	Plan de Acción
	General	Específico			
Evaluación de recuperación ante desastres en la infraestructura tecnológica de COCESNA	Proponer una estrategia de recuperación ante cualquier tipo de desastre que permita minimizar los tiempos fuera de servicios críticos	Identificar el tiempo máximo, perdidas monetarias, ubicación y el periodo de tiempo de actualización	1) No se tiene definido la frecuencia de actualización que deberá tener el plan de recuperación ante desastres. 2) La ubicación del sitio alterno tiende a ser propio debido a manejos internos de la empresa. 3) No existe una identificación de los costos de no operación ante la interrupción de los servicios de la empresa.	1) Definir la frecuencia de actualización de deberá tener el plan, para asegurar que ante la necesidad de su ejecución no se encuentre ningún inconveniente. 2) La ubicación deberá ser en la ciudad de San Salvador considerando que en dicho país ya se encuentra funcionando el centro de respaldo del centro de control ATC debidamente equipado. 3) Realizar un estudio que permita determinar los costos de no operación.	1) Elaboración plan de recuperación ante desastres. 2) Equipamiento Sitio Alterno.

Continuación de Tabla 13.Verificación de concordancia.

Título	Objetivo		Conclusiones	Recomendaciones	Plan de Acción
	General	Específico			
Evaluación de recuperación ante desastres en la infraestructura tecnológica de COCESNA	Proponer una estrategia de recuperación ante cualquier tipo de desastre que permita minimizar los tiempos fuera de servicios críticos	Determinar los riesgos posibles que puedan afectar las operaciones de la infraestructura tecnológica de la empresa.	1) Se observa un alza hacia el punto crítico del riesgo.	1) Orientarse en base a un estándar sobre gestión de riesgos para contar con una guía para el correcto tratamiento de los riesgos.	Elaboración plan de recuperación ante desastres
		Analizar costo/beneficio de contar con un plan de recuperación de desastres dentro de la empresa.	1) Al realizar la evaluación de la inversión para la ubicación de sitio alterno sobresalen con mayor peso los beneficios que se obtendrán al momento de presentarse una situación de desastre.	1) Aprobar el presupuesto para la compra del equipo necesario para el sitio alterno así como la capacitación y traslado del personal.	Equipamiento Sitio Alterno

En la tabla 13, se muestra la concordancia que hay con los objetivos general y específicos y cuáles son las conclusiones, recomendaciones y plan de acción según el juicio de los investigadores.

6.1 TÍTULO DE LA PROPUESTA

Dado la necesidad de las empresas de poder contar con un plan que permita restablecer las operaciones críticas del negocio en caso de presentarse un desastre

para evitar ya se pérdidas económicas o de imagen. Por lo tanto se recomienda la creación de los procedimientos necesarios que permitan a la empresa poder estar preparada en caso de presentarse un desastre en el centro de datos principal. La propuesta tiene como título “Plan de recuperación ante desastres en la infraestructura tecnológica de COCESNA”.

6.2 INTRODUCCIÓN

Con el objetivo de dirigir el proyecto de elaboración del plan de recuperación ante desastres y específicamente de la continuidad del negocio, se muestra los pasos a seguir para realizarlo de acuerdo a los parámetros correspondientes. La propuesta se acompaña de un cronograma de las actividades, el tiempo necesario y los responsables de coordinar las actividades así como del presupuesto necesario para la puesta en marcha.

6.3 PLAN DE ACCIÓN

El plan de acción está compuesto por dos elementos claves; en primera instancia se deberá definir el costo aproximado del equipamiento que será instalado en el sitio alterno para que sea aprobado por los directivos de la empresa y en segunda instancia el desarrollo del plan de recuperación ante desastres.

6.3.1 EQUIPAMIENTO SITIO ALTERNO

El proceso que se deberá llevar a cabo para la adquisición del equipo necesario para la puesta en marcha del sitio alterno que estará ubicado en la ciudad de San Salvador, El Salvador debe considerar el desarrollo de los siguientes pasos detallado en el orden

1) Definición requisitos del equipo y costo aproximado, en dicho paso se debe de analizar las características necesarias del equipo en el cual estarán

ejecutándose las aplicaciones críticas del negocio en caso de presentarse un desastre en el centro de datos principal.

2) Aprobación por parte de los directivos del presupuesto requerido para el correcto equipamiento del sitio alterno.
3) Cotización de equipos, enviar invitaciones a los proveedores para realizar la valoración del costo que tendrá el equipo que se requiere.
4) Análisis de ofertas, Una vez recibidas las respectivas ofertas de los proveedores se debe realizar un análisis técnico y económico para determinar la propuesta que mejor convenga a la empresa.
5) Adjudicación de Compra, seleccionado el proveedor que ofrezca las mejores condiciones técnicas y económicas para la empresa se le deberá remitir la correspondiente orden de compra de los equipos.
6) Recepción y verificación de equipo, llegado el tiempo de entrega del equipo por parte del proveedor se requiere llevar a cabo una revisión de las características del equipo recibido para determinar si cumple con los requisitos solicitados.
7) Instalación y configuración, en esta fase se deberá realizar la instalación del software de virtualización en los equipos y posteriormente realizar las configuraciones necesarias para la puesta en funcionamiento del equipo.
8) Carga de máquinas virtuales, una vez instalado y configurado el equipo se deberán de crear una copia de los servidores virtuales que son críticos para la empresa.
9) Pruebas, realizar las pruebas necesarias para validar el correcto funcionamiento del equipo.
10) Capacitación, para una mejor optimización de los recursos la capacitación a los técnicos encargados del sitio alterno deberá ser impartido en la modalidad “On-the-job-training” (OJT), este método contribuye al proceso de aprendizaje del empleado en su propio puesto de trabajo. Se aprende mientras se realiza el trabajo.
11) Mantenimiento, definir las respectivas rutinas de mantenimiento necesarias para la correcta operación del equipo.

6.3.2 ELABORACIÓN PLAN RECUPERACIÓN ANTE DESASTRES

Para la elaboración del plan de recuperación ante desastres se recomienda seguir la metodología propuesta por el instituto de recuperación de desastres (DRII), el cual esta consta de la siguiente información:

1) Análisis del Impacto del Servicio.
    1.1) Relación de Procesos.
    1.2) Relación de Aplicaciones.
    1.3) Relación de Departamentos y Usuarios.
    1.4) Determinar Procesos Críticos.
    1.5) Periodo Máximo de Interrupción.
2) Evaluación de Riesgos.
    2.1) Identificar los Activos.
    2.2) Identificar Amenazas.
    2.3) Evaluar Vulnerabilidades.
    2.4) Evaluar Impacto.
    2.5) Evaluar el Riesgo.
    2.6) Evaluar Contramedidas.
3) Desarrollo de Estrategias de Mitigación.
    3.1) Selección de Estrategia.
4) Desarrollo del plan de continuidad del servicio.
    4.1) Organización de Equipos.
    4.2) Desarrollo de Procedimientos.
5) Entrenamiento, Pruebas y Auditoria.
6) Mantenimiento del plan de continuidad del servicio.

La gerencia de tecnología informática de COCESNA deberá nombrar las personas idóneas que formaran parte del grupo que estará elaborando el plan de recuperación ante desastres.

6.4 CRONOGRAMA

El cronograma de ejecución detalla todas las actividades a realizar desglosadas por actividad, tiempo y responsables de ejecutar las mismas. Con el propósito de seguir la organización adecuada que permita contar con un efectivo plan de recuperación ante desastres.

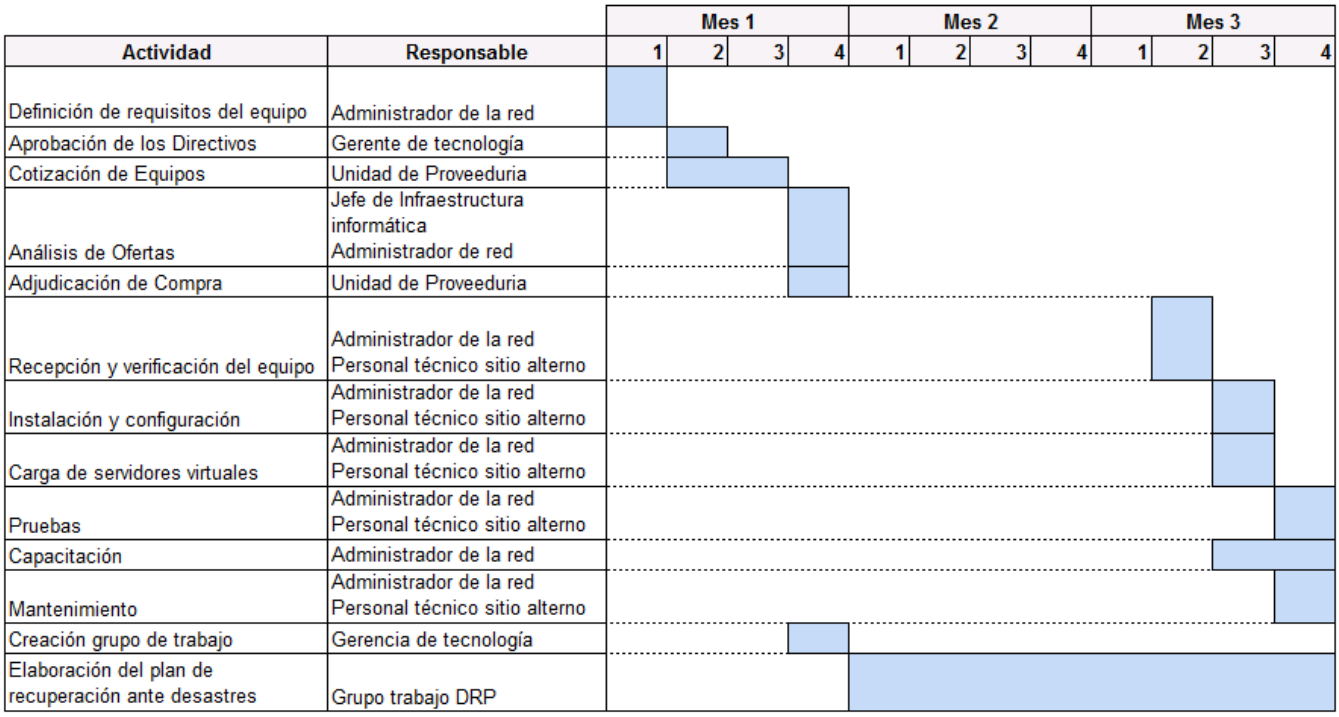

Figura 26 Cronograma de actividades.

En la figura anterior muestra los tiempos estimados de duración de cada actividad, una de las actividades importantes en la aprobación de los directivos del presupuesto requerido para poder ejecutar el equipamiento del sitio alterno que permita contar con un efectivo plan de recuperación ante desastres. La actividad que toma más tiempo es la llegada de los equipos al sitio por parte del proveedor, mientras esto sucede se puede ir trabajando en la elaboración del respectivo plan de recuperación ante desastres de COCESNA. El color azul celeste indica el mes o semana donde se llevara a cabo la actividad.

6.5 PRESUPUESTO

El presupuesto es uno de los elementos de mayor importancia al momento de presentar el proyecto para la aprobación de los directivos de la empresa, para la presente investigación se tomara en cuenta el costo aproximado de los equipos y licenciamiento necesario para poner a funcionar en el sitio alterno el respaldo de la plataforma de información administrativa de acuerdo a los niveles de respuesta deseados en los aplicativos críticos así como los gastos de traslado de personal para la instalación y configuración de los equipos como la respectiva capacitación y adaptación del personal técnico de la unidad de infraestructura informática. La tabla a continuación muestra un resumen del presupuesto requerido para asegurar el equipamiento del sitio alterno.

Tabla 14. Presupuesto equipamiento sitio alterno

Descripción	Cantidad	Costo aproximado
EQUIPO		
Servidor para alojamiento de servidores virtuales	1	$5,500.00
Unidad de almacenamiento en red (SAN)	1	$ 9,000.00
Gabinete para servidor	1	$800.00
Patch Panel	1	$50.00
Consola LCD 17” con KVM integrado	1	$1,300.00
Switch 12 puertos	1	$400
LICENCIAS		
Licenciamiento vCenter Site Recovery Manager	1	$ 5,900.00
MISCELÁNEOS		
Cable UTP Cat5e	30 metros	$15.00
Cable eléctrico forrado TSJ 3x12	20 metros	$80.00
Toma corriente polarizado	1	$10
Breaker 20 amperios	1	$20
Fajillas para cables	1 paquete 100 unidades	$10
VIÁTICOS		
Gastos de viáticos	9 días x 2 personas	$4,250.00
Compra pasajes aéreos	2	$1,380.00
CAPACITACIÓN		
Vcenter Site Recovery Manager	3	$5,400.00
TOTAL		$ 34,115.00

En la tabla 13, se desglosa el valor aproximado de compra de los equipos, el costo total aproximado asciende a un monto de $34,115.00, dicho costo aproximado del proyecto deberá ser presentado ante los directivos para la aprobación del mismo y poder realizar la compra requerida del equipo en el sitio alterno del centro de datos principal.

BIBLIOGRAFÍA

AEREOO. (2009). Colapsaron los aeropuertos en Estados Unidos por una falla en el sistema informático. Recuperado 28 de febrero de 2014, a partir de http://www.aereoo.com/2009/11/19/colapsaron-los-aeropuertos-en-estados-unidos-por-una-falla-en-el-sistema-informatico/

Aristizabal, A. (2011). ▸ ¿Sabe cómo realizar un plan de Continuidad del Negocio en su compañía? - YouTube. Recuperado 24 de febrero de 2014, a partir de http://www.youtube.com/watch?v=1IaDCGNyaUU

Associated Press. (2007). Falla de computadora ocasiona retrasos en aeropuerto de LA. Recuperado 28 de febrero de 2014, a partir de http://noticias.terra.com/noticias/falla_de_computadora_ocasiona_retrasos_en_aeropuerto_de_la/act931256

Associated Press. (2013). Southwest suspende 57 vuelos por falla. Recuperado 28 de febrero de 2014, a partir de http://www.cnnexpansion.com/negocios/2013/06/22/southwest-suspende-57-vuelos-por-falla

Benassini, M. (2009). *Introducción a la Investigación de mercados* (2.ª ed.).

Cabrera, R., & Martínez, I. (2008). BUSINESS CONTINUITY PLAN: ES MOMENTO DE ASEGURAR LA CONTINUIDAD DEL NEGOCIO.

Cannon, D., Bergmann, T., & Pamplin, B. (2006). *CISA Certified Information Systems Auditor*.

Cardona, O. (2003). La nocion del riesgo,desde las perspectiva de los desastres.

CNBS. (2005). CNBS - Circular CNBS No.119/2005. Recuperado 28 de febrero de 2014, a partir de http://www.cnbs.gov.hn/circulares/2005/C1192005.htm

COCESNA. (2014). Aspectos Relevantes en la Gestión y Resultados en el Área de Navegación Aérea (COCESNA).

Coppola, D. (2007). *Introduction to International Disaster Management*.

Digitech. (2013). Cómo sobrevivir a un desastre informático. Recuperado 28 de febrero de 2014, a partir de http://www.expansion.com/2013/11/29/empresas/digitech/1385753450.html

Doughty, K. (2001). *Business Continuity Planning*.

EFE. (2013, diciembre). Falla informática afecta cientos de vuelos en Reino Unido. Recuperado 28 de febrero de 2014, a partir de http://noticieros.televisa.com/mundo/1312/falla-informatica-afecta-cientos-vuelos-reino-unido/

Ernest & Young. (2004). *Seguridad de la informacion a nivel global*.

Ferrer, R. (2009). *Plan de Continuidad para el negocio*. Recuperado a partir de http://www.sisteseg.com/files/Microsoft_PowerPoint_-_PLANES_DE_CONTINUIDAD_NEGOCIO_V_3.0.pdf

Gregory, P. (2008). *IT Disaster Recovery Planning*.

Guzman, G. (2013). *Planes de Contingencia*.

Hernández, R., Fernández, C., & Baptista, M. (2010). *Metodología de la Investigación*. México D.F.: McGraw-Hill.

Hoffer, J. (2001). *Backing Up Business Industry Trend or Event*.

IMARPE. (2012). Plan de Contingencia 2012-2015.

Inestroza, J. (2014). Informacion sobre la implementacion de DRP en HONDUTEL.

ISACA. (2009). RISK IT.

ISO. (2000). ISO/IEC Standard 17799: Information Technology – Code of Practice for Information Security Management.

Jiménez, J. (2013a). *Valoracion del Riesgo*.

Jiménez, J. (2013b). *Vision Global del Riesgo*.

Kendall, K. ., & Kendall, J. . (2005). *Análisis y diseño de sistemas* (6.ª ed.).

Krueger, R. (1988). *Focus Groups*.

Laudon, K., & Laudon, J. (2012). *SISTEMAS DE INFORMACIÓN GERENCIAL* (12.ª ed.). PEARSON.

Locandro, A. (2014). *Sistema de Información Geográfica*. ArcGis.

Malhotra, N. (2008). *Investigación de Mercados* (5.ª ed.). PEARSON.

Margaret Rouse. (2013). ¿Qué es Plan de Recuperación de Desastres (DRP)?? Recuperado 31 de enero de 2014, a partir de http://searchdatacenter.techtarget.com/es/definicion/Que-es-Plan-de-Recuperacion-de-Desastres-DRP

Martinez, F., & Hernandez, G. (2010). *Administracion de proyectos*. PEARSON.

Martinez, J. (2004). *Planes de contingencia, la continudiad del negocio en las organizaciones*.

Musgrave, B., & Woodman, P. (2013). *The 2013 Business Continuity Management Survey*.

NetIQ. (2012). A Practical Guide to Cost-Effective Disaster Recovery Planning.

Perez, C. (2014). Informacion sobre los DRP en la Secretaria de Finanzas.

Polimeni, R. S., Fabozi, F. J., & Adelberg, A. . (1994). *CONTABILIDAD DE COSTOS CONCEPTOS Y APLICACIONES PARA LA TOMA DE DECISIONES GERENCIALES* (3.ª ed.).

Radio Panama. (2013). Copa Airlines acepta total responsabilidad en caída de red tecnológica. Recuperado 28 de febrero de 2014, a partir de http://www.radiopanama.com.pa/noticias/actualidad/copa-airlines-acepta-total-responsabilidad-en-caida-de-red-tecnologica/20131021/nota/1998333.aspx

Robertson, G. (1997). *People, Paper, Data: Disaster planning for libraries*.

Sampieri, R., & Collado, C. (2010). *METODOLOGÍA DE LA INVESTIGACION* (5.ª ed.).

Sanchez, D. (2014).

Sandhu, R. J. (2002). *Disaster Recovery Plan*. Premier Press.

Somasundaram, G., & Shrivastava, A. (2009). *Information Storage and Management Storing, Managing, and Prote*. Wiley Publishing, Inc.

Tener, S. (2000). Respaldo y Configuracion de Datos. Recuperado a partir de http://www.tenzer.com.uy/archivos/Respaldoyrecuperacion.pdf

Torres, M. (2014). Informacion de la empresa sobre planes de continudiad del negocio.

Van Horne, J., & Wachowicz, J. (2010). *Fundamentos de Administracion Financiera*. PEARSON.

Wallace, M., & Webber, L. (2004). *THE DISASTER RECOVERY HANDBOOK*.

Webster, A., (2000). *Estadística aplicada a los negocios y la economía* (3.ª ed.).

Zavala, R. (2014). Que informacion se respalda en la empresa y cual es el tamano de la data respaldada.

ANEXOS

ANEXO 1. CUESTIONARIO PRELIMINAR

ENCUESTA

Nombre: _____

Sexo: F ☐ M ☐ Edad: _____

Como parte de investigación del trabajo de tesis se desea recopilar datos acerca de los planes de recuperación ante desastres.

A continuación se presentan con una serie de preguntas cuyas respuestas deben ser claras

- ❖ Riesgos

1) ¿Cuánto tiempo tiene de trabajar en la empresa?

   ☐ 0-4
   ☐ 5-9
   ☐ 10-14
   ☐ 15-19
   ☐ Mayor a 20

2) Aplicaciones administrativas que son consideradas críticas enumérelas por su orden de prioridad donde 1 es mayor y 5 menor prioridad

	1	2	3	4	5
Contabilidad					
Presupuesto					
Planilla					
Caja General					
Facturación y cuentas por cobrar					

3) Son los tipos de riesgos identificados que pueden afectar las operaciones del negocio

	1	2	3	4	5
Incendios					

Incidentes de seguridad					
Falla en equipos					
Fallas de energía					
Sabotajes					

4) Nivel de conocimiento del procedimiento a seguir en caso de presentarse una situación de desastre

   ☐ Bajo
   ☐ Regular
   ☐ Moderado
   ☐ Muy bueno
   ☐ Excelente

5) Existe un plan de contingencia ante desastres que este operativo dentro de la empresa:

   ☐ No definido
   ☐ Existe pero no está operativo
   ☐ Existe y está operativo
   ☐ Desconoce la existencia del plan

6) De existir un plan de contingencia ante desastre definido dentro de la empresa ¿cuál es su frecuencia de actualización?

   ☐ Mensual
   ☐ Trimestral
   ☐ Semestral
   ☐ Anual
   ☐ No definido

7) Ha existido algún incidente mayor en la infraestructura tecnológica bajo la cual operan los servicios administrativos de la empresa en los últimos algunos de los siguientes daños.

   ☐ Bajo
   ☐ Regular
   ☐ Moderado
   ☐ Muy bueno
   ☐ Excelente

8) En caso de un incidente en la infraestructura tecnología quien es el responsable de activar nuevamente los servicios.

- ☐ Técnico de soporte
- ☐ Director informática
- ☐ Oficial de seguridad
- ☐ Jefe de informática
- ☐ Administrador de redes

9) ¿Qué tiempo máximo permitido se tiene definido para estar sin servicio de la infraestructura tecnológica?

- ☐ 10 minutos
- ☐ 20 minutos
- ☐ 30 minutos
- ☐ 40 minutos
- ☐ Mayor a 40 minutos

❖ Tiempo

10) Qué estrategia de respaldo de datos se lleva a cabo dentro de la empresa.

- ☐ Total
- ☐ Incremental
- ☐ Diferencial

11) Seleccione según su criterio el sitio alterno para recuperar las operaciones del negocio en caso de presentarse un desastre.

- ☐ Propio
- ☐ Tercerizado
- ☐ Nube
- ☐ Propio y tercerizado
- ☐ Propio y en la nube

12) Tiempo máximo que una aplicación ha estado fuera de servicio. ¿Cuál ha sido su consecuencia

- ☐ Bajo
- ☐ Regular
- ☐ Moderado
- ☐ Muy bueno
- ☐ Excelente

ANEXO 2. FORMATO MATRIZ GESTION DE RIESGOS

AMENAZA	CAUSA	EFECTO	PROBABILIDAD	SEVERIDAD	RIESGO	DEFENSA