UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:
ANÁLISIS Y EVALUACIÓN PARA EL DISEÑO DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) APLICADO EN UN CENTRO DE DATOS PARA EMPRESAS MUNICIPALES BASADO EN LA NORMA ISO/IEC 24762:2008.

AUTOR:
BYRON VICENTE NIETO MUÑOZ

DIRECTOR:
ING. RICHARD ROMERO IZURIETA MAE

Guayaquil, abril de 2015

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Yo, Byron Vicente Nieto Muñoz, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción del mismo sin fines de lucro.

Además de aquello declaro que las definiciones y análisis desarrollados y conclusiones empleadas en el siguiente trabajo son de exclusiva responsabilidad del autor.

Byron Vicente Nieto Muñoz

C.I.: 0928651009

DEDICATORIA

Este proyecto está dedicado a Dios, a mi madre, a mis hermanos, amigos y profesores que siempre me dieron fuerza y su apoyo incondicional para poder llegar a la meta.

Nieto Muñoz Byron Vicente

AGRADECIMIENTO

La gratitud es el más noble de los sentimientos, es por ello que deseo expresar mis más sinceros agradecimientos principalmente a:

Mi padre celestial Jehová que me dio las fuerzas necesarias, apoyo y cuidado amoroso durante toda mi vida y en especial en estos años de carrera universitaria.

A mí querida madre, fiel amiga, acompañante y consejera que si no fuera por su sacrificio no estaría escribiendo esta nueva página en mi vida.

Gracias a la vida que me brinda Dios y a mis amigos que más quiero, si no fuese por ellos mi sueño no lo habría cumplido; no tengo las palabras suficientes para seguir describiendo el gran regocijo que siente mi corazón al poder terminar mi carrera en donde profesores y compañeros compartimos en un salón de clase y parte de nuestra vida, para dar vida a las ilusiones que tuve cuando niño y que hoy en día se hacen realidad.

ÍNDICE

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE ABREVIATURAS

DRP…..Siglas en ingles de Plan de Recuperación de Desastres (Disaster Recovery Planning)

BCP…..Siglas en ingles de Plan de Continuidad del Negocio (Business Continuity Planning)

BIA…...Siglas en ingles del termino Análisis de Impacto del Negocio (Business Impact Analysis)

RPO……Siglas en ingles del termino Objetivo de Punto de Recuperación (Recovery Point Objetive).

RTO….. Siglas en ingles del término Objetivo de tiempo de Recuperación (Recovery Time Objetive).

PMR…..Siglas del termino Plan de Administración de riesgos.

ISO/IEC.….Siglas en ingles de la organización de estandarización internacional (International Standar Organization); Comisión internacional Electrotécnica (International Electro technical Commission).

B2D…..Siglas en ingles del termino Respaldo de disco a disco (Backup Disk to Disk)

VTL…..Siglas en ingles del termino Librerías de cinta virtual (Virtual Tape Library)

CDP…..Siglas en ingles del termino Protección continua de datos (Carry on Data Protección)

HA……Siglas en ingles del termino Alta Disponibilidad (High Availability)

FT…….Siglas en ingles del termino tolerancia a fallos (Fault Tolerance)

LB…….Siglas en ingles del termino Balanceo de Carga (Load Balancing)

DT…….Siglas en ingles del termino Tiempo de inactividad (Down-Time)

RAID…Siglas en ingles del termino conjunto redundante de Discos independientes (Redundant Array Independent Disks)

RESUMEN

Este documento resume el proyecto de un plan de recuperación ante desastres realizado en una empresa municipal usando como método el estándar ISO/IEC 24762:2008.

Se debe tener en consideración que un riesgo siempre va a estar presente en toda institución ya sea pública o privada, es por ello que nacen los planes de recuperación.

Este proyecto tiene como objetivo general diseñar una guía que le permita a la empresa pública identificar los riesgos potenciales y servicios de misión crítica que son de vital importancia en toda institución, además crear un procedimiento de recuperación que pueda ser ejecutado por personal designado para restablecer el servicio a pocas horas de haberse suscitado el desastre.

Como parte de los objetivos específicos es brindar una solución de recuperación, la misma que consiste en diseñar un plan de contingencias basado es un sitio alterno y que cumpla con los lineamientos de alta disponibilidad, escalabilidad y redundancia necesarios para satisfacer y asegurar la continuidad del negocio.

A lo largo del proyecto es de vital importancia contar con el apoyo y soporte de la alta gerencia, ya que esto asegura el éxito del proyecto. Es de suma importancia definir el alcance del proyecto para determinar el tiempo mínimo de inactividad que está dispuesta a enfrentar la empresa municipal.

ABSTRACT

In this document, a summary of a disasters recovery plan Project is done in a city enterprise using ISO/IEC 24762:2008.

It is necessary to consider that there is always a risk present in every institution, either public or private, so that is the main for recovery plans to exist.

This project's main purpose is to design a guide that allows a public enterprise to identify the potential risks and necessary and most important vital services in every institution; and to elaborate a recovery procedure that can be executed by the designed personnel in order to reestablish the service few hours after the disaster.

As part of the specific objectives of this project is to provide a solution for recovery, which includes the design of a contingency plan based in a similar place that fulfills certain factors of availability, improvement and redundancy necessary to satisfy and asseverate the continuity of business.

Along the project, it is extremely important to count on the support of the main management to guarantee success. It is vital to define the significance of the project to determine the inactive minimum period the city enterprise is willing to confront.

INTRODUCCIÓN

Mientras fluyen las operaciones normales del negocio, debe tener en consideración que siempre está presente el riesgo y por consiguiente la probabilidad de que existan pérdidas potenciales o interrupciones no programadas asociadas con un desastre o contingencia mayor, por lo que es de suma importancia el desarrollo de un plan viable y factible de recuperación el cual le permita asegurar la continuidad de las operaciones de la organización.

Con una planificación adecuada, la preparación, y la comunicación son los componentes claves, para un exitoso plan de recuperación ante desastres (DRP).

En el caso de suscitarse, es importante disponer de una estrategia de recuperación inmediata que le permita proveer el restablecimiento del negocio a corto plazo. Es por ello la importancia de contar con un plan de contingencias y recuperación en caso de desastres es vital.

En el presente documento se pueden mostrar los posibles tipos de contingencias, desastres, y los planes de acción para la recuperación de la información y la continuidad del negocio. Además poder proporcionar de una directiva estratégica y una estructura común para todas las actividades. De la misma manera esta debe cumplir con los estándares corporativos y se deben adecuar a la norma ISO/IEC 24762:2008.

CAPITULO I

PROBLEMÁTICA DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

Una empresa municipal muy reconocida en el país, está considerando en realizar un análisis para la planificación eficiente de un plan de recuperación ante desastres, que le permita reanudar rápidamente sus funciones de misión crítica ante una falla en la infraestructura o por causa de algún desastre natural. A medida que van pasando los años, la infraestructura de dicha empresa se mantiene en constante crecimiento y por consiguiente el volumen de sus datos y el nivel de transaccionalidad es aún mayor, por ello es vital contar con una planificación que les permita contar con una contingencia a corto plazo si se hace factible el siniestro.

En el peor de los escenarios, se plantean la pérdida por completa de la infraestructura, para lo cual la empresa no se encuentra preparada para afrontar dicha situación ya que no cuentan con una planificación estratégica para la recuperación ante sucesos imprevistos.

Los costes de los servidores son altos como para ser remplazados en el caso que estos se vean afectados; pero lo más importante de todo es evitar la pérdida de información, ya que en la actualidad no cuentan con alta disponibilidad o un sistema de protección de la información en los servicios, que provoquen fallas o interrupciones en la infraestructura.

1.2 Formulación del Problema

¿Porque es de vital importancia que las organizaciones adopten un plan de contingencia que proteja su infraestructura y asegure la disponibilidad sus datos?

¿Qué alternativa de respaldo de información se ajusta más a las necesidades de una empresa municipal?

¿Cómo se puede lograr restablecer la infraestructura actual ante la ocurrencia de un desastre?

¿Al tener un plan de recuperación obtengo asegurada la infraestructura y la información de la empresa al 100%?

¿Para qué organizaciones se adapta mejor un plan de recuperación ante desastres?

¿Cuán factible es que la implementación de un datacenter alterno reemplace la infraestructura del datacenter principal?

1.3 Objetivos

1.3.1 Objetivo General

Diseñar un plan de recuperación que le permita restablecer los servicios de una empresa municipal en caso de haberse suscitado un evento inesperado y que reduzca al mínimo la pérdida de información y mitigue los riesgos mediante la aplicación de la norma ISO/IEC 24762:2008.

1.3.2 Objetivos Específicos

1. Identificar los posibles riesgos y vulnerabilidades que pueden afectar adversamente la integridad de la organización.

2. Diseñar un plan de recuperación de la infraestructura actual del centro de datos con el fin de prevenir y mitigar los efectos de pérdidas potenciales.

3. Conocer las maneras más óptimas del restablecimiento de la infraestructura del centro de datos una vez que se ha suscitado el desastre.

4. Sugerir alternativas factibles que ayuden a la recuperación de un centro de datos.

5. Designar responsabilidades administrativas que permitan seguir manteniendo la fiabilidad e integridad del centro de datos.

1.4 Justificación

El presente desarrollo de este estudio-análisis se realiza por la necesidad que surge en una empresa municipal, para contar con un plan de contingencia que le permita mitigar los efectos de la perdida potencial de la infraestructura y reducir al mínimo la pérdida de información y disponibilidad del servicio.

El diseño del plan de recuperación le permite disponer de un mecanismo o metodologías que le ayuden a disminuir la proclividad del negocio a interrupciones

y reducir considerablemente los riesgos relacionados con la integridad, confidencialidad y disponibilidad del centro de datos.

Además este plan le permite el dar a conocer el costo-beneficio de las estrategias de recuperación, analizar funciones de nivel crítico para la supervivencia del área, seleccionar las mejores alternativas de operación y respaldo de datos.

Se estima que el diseño del plan de recuperación se proyecta para funcionar los próximos 2 años, demostrando su factibilidad en el caso de que un evento inesperado ocurra en la infraestructura y reduciendo al mínimo los riesgos.

1.5 Alcance del Proyecto

El alcance es diseñar un plan de recuperación ante desastres (DRP) en el centro de datos en una empresa municipal, el mismo que le permita proveer de mecanismos y establecer prioridades claras sobre los tipos de procesos que son los más esenciales y por consiguiente reducir el riesgo de interrupción operacional en caso de algún suceso imprevisto, el cual se vea involucrado y que perjudique la continuidad del negocio. Además de poder permitir la recuperación a corto plazo de sistemas tecnológicos, funciones y procesos de nivel crítico y la mitigación de riesgos ocasionados por siniestros naturales, daños por terceros, daños intencionados o no por los empleados, errores humanos, etc. , que atenten con la funcionalidad normal de las operaciones del negocio.

CAPITULO II
MARCO TEORICO

2.1 Marco Referencial

2.1.1 Introducción

La planificación de la continuidad del negocio BCP y la planificación de la contingencia para los sistemas de información son elementos de un sistema de control interno, que se establece para gestionar la disponibilidad de los procesos críticos en el caso de una interrupción. La parte más importante de ese plan trata con el soporte rentable del sistema de información. La disponibilidad de los datos del negocio es vital para el desarrollo sostenible y/o incluso para la supervivencia de cualquier organización. (BSCCONSULTORES, BSCCONSULTORES, 2010)

La BCP (Bussiness Continuity Planning) es un proceso continuo más que un proyecto. Los planes que el planificador desarrolla como parte de este proceso dirigirán la respuesta a incidentes desde simples emergencias hasta desastres totales.

La meta última del proceso es poder responder a los incidentes que puedan impactar en la gente, las operaciones y la capacidad de entregar bienes y servicios al mercado.

Esta área le presenta una visión general de los principios de continuidad del negocio y recuperación de desastres y específicamente las siguientes áreas:

- Los procesos de BCP y planeación de recuperación ante desastres DRP.

- Análisis de impacto al negocio BIA.

- Estrategias y Alternativas de Recuperación.

- Pruebas de Plan.

- Respaldo y Restauración.

- Consideraciones de Auditoría.

Una pérdida de energía, una inundación, un incendio o un robo han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitarse, en caso de que éstas sucedan, que las pérdidas sean tan graves que le afecten a la viabilidad del negocio.

Son múltiples las organizaciones que, independientemente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestas y les garanticen una alta disponibilidad en las operaciones de su negocio.

De este modo, es necesario que las organizaciones establezcan una serie de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio en caso de tener que afrontar una contingencia grave. (INTECO, 2007)

2.1.2 Norma ISO/IEC 24762:2008

Esta norma tiene por objeto ayudarle a la operación de un Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando orientación sobre la provisión de la recuperación de información y tecnología de comunicaciones de desastres como parte de los servicios de gestión de la continuidad del negocio.

Gestión de la continuidad del negocio es una parte integral de un proceso de gestión de riesgos integral que salvaguarde los intereses de las principales partes interesadas de una organización, la reputación, la marca y la creación de valor a través de las actividades:

1. Identificar las amenazas potenciales que pueden causar impactos adversos en las operaciones de negocio de una organización, y los riesgos asociados.

2. Proporcionar un marco para aumentar la resiliencia de las operaciones comerciales;

3. Proporcionar capacidades, instalaciones, procesos, listas de tareas de acción, etc., para una respuesta eficaz a los desastres y fracasos. (ISO)

La norma será aplicada como base para el desarrollo de las actividades y tareas al diseñar el plan de recuperación.

2.1.3 Disaster Recovery Plan (DRP)

Disaster Recovery Plan (DRP). Como sugiere su nombre, el DRP se aplica a los grandes desastres, por lo general hechos catastróficos que niegan el acceso a la instalación normal por un período prolongado. Con frecuencia, se refiere a un DRP de TI centrada en el plan destinado a restablecer la operatividad del sistema de destino, aplicación o instalación de equipo en un sitio alternativo después de una emergencia. El ámbito de aplicación de DRP puede superponerse a la del plan de contingencia de TI, sin embargo, el DRP es más limitado en su alcance y no responde a las interrupciones de menor importancia que no requieren de reubicación. Dependiendo de las necesidades de la organización, el DRP también puede incluirse el BCP. (Vigo Jaccottet, 2010)

Aparte de prevenir o minimizar las pérdidas para el negocio que un desastre puede causar, el objetivo principal de cualquier programa orientado a gestionar la continuidad de negocio de una organización es garantizar que ésta dispone de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia.

El DRP es aplicado en el proyecto mediante la identificación de amenazas, determinación el hardware y procesos de misión crítica, designación de responsabilidades, selección de mecanismos de copias de seguridad y acciones de mitigación del impacto ante sucesos imprevistos.

Ilustración 1- Beneficios de contar con un DRP.

Fuente: (INTECO, 2007)

2.1.4 Tipos de Contingencias

Existen diferentes tipos de contingencia de acuerdo a los daños sufridos:

Contingencia Menor: Es aquella que tiene repercusiones sólo en la operación diaria y se puede recuperar en menos de 8 horas.

Contingencia Grave: Es aquella que causa daños a las instalaciones, pero se pueden reiniciar las operaciones en menos de 24 horas.

Contingencia Crítica: Afecta la operación y a las instalaciones, este no es recuperable a corto plazo y puede suceder por que no existen normas preventivas o bien porque estas no son suficientes. Además puede suceder por ocurrir algún tipo de desastre natural como incendios, inundaciones, terremotos, etc. (Granada, 2012)

Los tipos de contingencias se pueden ver aplicados en el proyecto dependiendo de la criticidad y manifestación del evento. A medida que el nivel de riesgo aumenta también el nivel de contingencia.

2.1.5 Métodos de recuperación ante desastres

Online Recovery : La recuperación se realiza a través de la web , es accesible desde cualquier sitio en Internet y está disponible las 24 horas del día y la cual puede ser la solución más adecuada e inmediata a los problemas , ahorrando tiempo y dinero.

Offline Recovery: Se la debe llevar a cabo si la interfaz de administración no es accesible (por ejemplo, debido a problemas en la red, el Administrador de la interfaz de los equipos han experimentado un fallo, en este caso la recuperación en línea no es posible). Sólo autónomos y dispositivos biblioteca SCSI se pueden utilizar para la recuperación offline.

Remote Recovery: La recuperación se realiza mediante un software o un cliente remoto que le permita acceder a la infraestructura y si alguno de ellos falla, el proceso de recuperación de desastres se conmuta a modo local. Esto significa que el sistema de destino busca dispositivos conectados localmente. (HP, 2011)

2.1.6 Fases de un Desastre

Los desastres al estudiarlos se pueden apreciar que tienen tres fases bien definidas:

Etapa Pre-patente: Es antes de empezar o manifestarse el fenómeno. Los desastres en su fase Pre-patente aún no se han desarrollado como tal. Los factores de riesgo están interactuando entre sí en diferentes grados de intensidad, existen los factores de riesgo interactuando o no.

Estos factores en muchos casos pueden ser predecibles y hasta controlables.

Etapa patente: Es cuando se la propicia con causalidad de los factores de riesgo y se desarrolla el fenómeno, impactando a la comunidad. Esta fase se enfrenta con la atención del fenómeno y su impacto.

Etapa consecuencial: Es donde ya culmina o cede el fenómeno y se pueden apreciar con certeza las consecuencias del impacto. Se detiene el efecto y queda el estigma del impacto o las pérdidas. Esta fase se enfrenta con la Recuperación o Rehabilitación y se comienza nuevamente en la fase pre patente. (Serrano, 2005)

Las fases de un desastre se aplican en el proyecto mediante informes que den a conocer las situaciones por las que atraviesa la organización las mismas que permitan detallar el impacto y los efectos que se han propiciados ante y durante un evento.

2.1.7 Clasificación de los Desastres

a) Por su aparición:

I. **Súbitos:** Aquellos fenómenos que ocurren sorpresivamente y de manera inmediata Por ejemplo: Avalanchas , Terremotos, Tsunamis

II. **Mediatos:** Son aquellos que se desarrollan de forma más lenta y es factible predecirlos como por ejemplo: Huracanes, erupciones volcánicas, sequías, etc.

b) Por su duración:

I. **Corta a mediana duración:** Tales como terremotos, huracanes, erupciones volcánicas, tsunamis, avalanchas.

II. **Extendida duración:** Sequias, epidemias, inundaciones.

c) Por su origen - Natural:

I. **Naturales:** Originados por la acción espontanea de la vida misma de la naturaleza o de la evolución del planeta

II. **Inundaciones:** En temporada de invierno aumenta el caudal de los ríos o causes de aguas en la ciudad las mismas que pueden desbordarse y arrasar con las propiedades, animales, cultivos y hasta pérdidas humanas.

III. **Terremotos:** Originado principalmente por el movimiento de las placas técnicas causa cúmulos de energía en forma de tensión las mismas que al liberarse hacen que se deslicen capas de la tierra con propagación de la onda. Dicha vibración puede ocasionar daños en edificaciones, inclusive tomar vidas humanas.

IV. **Tsunami (Maremotos):** Originado principalmente desde las placas tectónicas inducidas en el fondo del mar que al salir a la superficie y debido a su desplazamiento se generan olas de gran magnitud las mismas que llegan a las costas de los principales puertos o playas y

donde desatan todo su poder destructivo y toma tiempo en poder recuperarse ante una situación de estas dimensiones.

V. **Erupciones Volcánicas:** Como su nombre lo indica producidos por el lava que emerge desde los yacimientos de los volcanes y el mismo que afectan a las localidades, vegetación y fauna que se encuentre a sus alrededores. Es considerado como un desastre del que si es viable una recuperación a corto plazo (semanas).

d) Por su origen – Inducidos :

I. **Incendios:** Son provocados por el uso inadecuado de combustibles, fallas de instalación eléctricas en mal estado y el inadecuado almacenamiento y traslado de sustancias inflamables. El fuego es una de las principales amenazas contra la seguridad.

II. **Robo Informático:** Es uno de los peligros actuales que consiste en utilizar técnicas o estrategias sutiles para hacer que los usuarios caigan de manera ingenua y así proceder sustraer en la mayoría de veces dinero o información , de un individuo o una organización. Es considerado un riesgo pero existen medidas para tratar de minimizarlo.

III. **Error humano:** Puede darse el caso que una persona muchas veces por inexperiencia llegue al punto de eliminar información valiosa y provocar irregularidades en la lógica del negocio.

IV. **Terrorismo:** Generado principalmente por la inconformidad de grupos rebeldes que como no pueden defenderse con palabras inducen la fuerza y generan daños mayores. Es necesario tomar las debidas precauciones y las respectivas contingencias ante este tipo de daños. (Westen, 2010)

2.2. Evaluación del Riesgo

El propósito de ofrecer una valoración del riesgo es el de conocer los riesgos implicados para las instalaciones de la organización y el potencial tiempo de caída de las funciones del negocio y operaciones computacionales derivadas. El análisis de estos peligros es muy importante en el desarrollo de un plan de Continuidad del Negocio, el cual es necesario para la recuperación después de una situación de desastre. Los recursos, personal y tiempos necesarios pueden ser identificados después de que el impacto ha sido analizado. Lo importante es:

1. Deduzca la vulnerabilidad antes de que ocurra un desastre y establezca medidas preventivas para eliminar o minimizar la ocurrencia del desastre.
2. Cuente con un sitio alterno o una localidad segura, no sujeta a los mismos peligros que las instalaciones de computación principales, para respaldar el activo-información en el caso de alguna contingencia. (J. & K., 2000)

Para evaluar los riesgos en el proyecto debe realizar una inspección en el sitio y listar las vulnerabilidades existenciales en la empresa municipal y por consiguiente dar a conocer a la gerencia o al departamento de tecnología las causas y efectos que desencadenaran si no son tratadas a tiempo.

2.3 Análisis de Criticidad

El objetivo de coordinar un análisis de criticidad le permite determinar o darle un valor porcentual a las posibles tareas u operaciones que se llevan a cabo en dicha empresa, denominando críticas a las tareas que ponen en riesgo total al negocio, vitales la cual se haya generado por errar humano, sensitivas tienen que ver con impactos externos ya sean estos naturales o personas ajenas a la organización y no críticas a las cuales no se aplica mucho el riesgo de perderlas. (J. & K., 2000)

El análisis de criticidad se aplica en el proyecto mediante la realización de un listado que le permita identificar los servicios que la empresa considera críticos y ponen en riesgo la continuidad del negocio. Deberá programar una reunión con el personal que está al cargo de la administración de los servicios críticos, para detallar y obtener información de los procesos que se llevan a cabo.

Tabla 1 - Clasificación de Procesos

OPERACIONES	POSIBLES CAUSAS
Criticas	Falla de la red en una localidad. Falla de los enlaces de telecomunicaciones. Falla del Servidor de aplicaciones. Falla del Suministro eléctrico.
Vitales	Fallas humanas en la operación de los equipos de cómputo. Fallas humanas en el mantenimiento de redes y equipos.
Sensitivas	Cambio Climático. Clientes.
No criticas	Cambios de departamentalización indirecta. Errores no críticos del Usuario.

Fuente: (Ibarra, 2008)

2.4 Política de continuidad del negocio

Una política de continuidad del negocio debe ser proactiva y abarcar controles preventivos, de detección y correctivos. El BCP es el control correctivo más crítico. Depende de que otros controles sean efectivos, en particular la gestión de incidentes y respaldo de medios. (BSCCONSULTORES, BSCCONSULTORES, 2010)

2.5 Estrategias para la protección y recuperación de datos

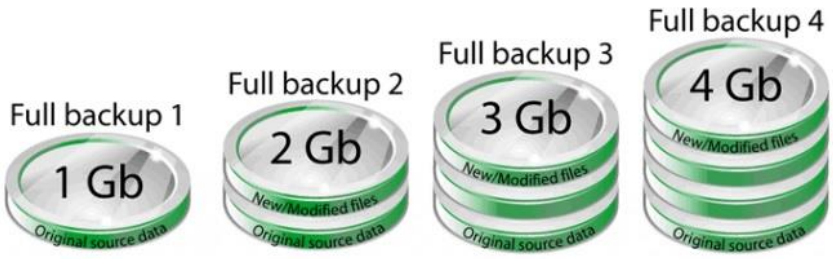
El mercado de la protección y recuperación de datos es el mercado del almacenamiento de mayor madurez. Todas las empresas tienen implantado algún tipo de proceso de protección de datos. A pesar de su madurez, se han producido numerosas innovaciones en el mercado, como la redundancia, el backup de disco a disco (B2D), las librerías de cinta virtual (VTL), y la protección continua de datos (CDP). Las organizaciones se enfrentan ahora al desafío de aprovechar las nuevas tecnologías para mejorar las estrategias de backup y recuperación existentes sin aumentar la complejidad ni perturbar los procesos ya establecidos. Además, dado que estas nuevas tecnologías suponen un gasto añadido, los administradores de almacenamiento deben decidir qué nuevas tecnologías son las más apropiadas para cada tipo de datos, relacionando así el coste de almacenamiento con el valor para el negocio de los datos almacenados. (Arend, 2008)

Para aplicar la estrategia de protección y recuperación en el proyecto se procederá a revisar la infraestructura tecnológica existencial con el fin no alterar el modelo de negocio tomando en consideración parámetros como el RTO , presupuesto y configuraciones actuales, con el fin de seleccionar la mejor estrategia que se adapte a la entidad municipal.

2.6 Granularidad en el respaldo y recuperación de datos

Full Backup: Las copias de seguridad completas y contiene todos los datos de las carpetas y archivos que se seleccionan para ser respaldados, se realizan solo una vez a la semana y forman parte de un plan global de copias de seguridad.

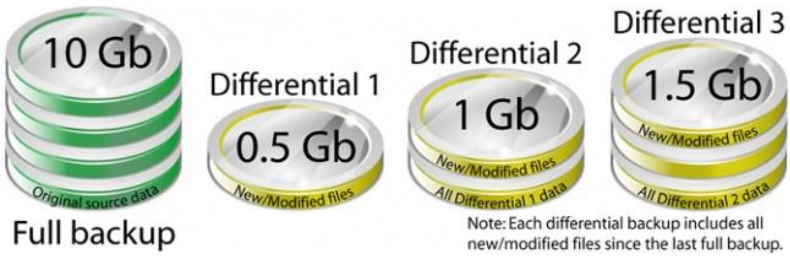
Ilustración 2 - Respaldo Completo



Fuente: (Softland, 2012)

Diferencial Backup: Copia de seguridad diferencial contiene todos los archivos que han cambiado desde la última copia de seguridad completa. La ventaja de una copia de seguridad diferencial es que acorta el tiempo de restauración en comparación con una copia de seguridad completa.

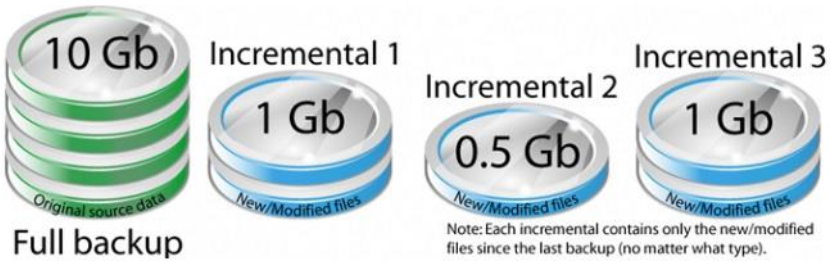
Ilustración 3 - Respaldo Diferencial



Fuente: (Softland, 2012)

Incremental Backup: Las copias de seguridad incrementales solo realizan copias de seguridad de los datos cambiados, pero únicamente de los que han cambiado desde la última copia de seguridad, sea completa o incremental. Mientras que las copias de seguridad incrementales le dan mucha más flexibilidad y granularidad (tiempo entre copias de seguridad), tienen la reputación de tardar más tiempo en restaurarse porque la copia de seguridad debe reconstruirse desde la última copia de seguridad completa y con todas las copias de seguridad incrementales realizadas desde entonces. (Acronis, 2014)

Ilustración 4 - Respaldo Incremental



Fuente: (Softland, 2012)

Las copias de seguridad o respaldos son aplicados en el proyecto mediante la ejecución de tareas de respaldos programadas por medio de herramientas como HP Data Protector y la replicación por el vCenter Site Recovery Manager, las mismas que van hacer determinados por las administradores de base de datos e infraestructura en conjunto con el gerente de TI.

2.7 Marco Conceptual

Disaster Recovery Planning (DRP): Es el proceso planificado que una organización utiliza para recuperar el acceso a su infraestructura (software, datos y / o hardware) que son necesarios para reanudar el ejercicio de las funciones normales de trabajo, críticos después del evento ya sea de un desastre natural o una catástrofe causada por los seres humanos. (EMC2)

Bussiness Continuity Planning (BCP): Un plan de continuidad del negocio (BCP) es un plan para ayudar a asegurar que los procesos de negocio fluyan normalmente durante un tiempo de emergencia o desastre. Este tipo de emergencias o desastres

pueden incluir un incendio o cualquier otro caso en el que el negocio no es capaz de producir en condiciones normales. Las empresas tienen que mirar a todas esas amenazas potenciales y diseñar los pasos fronterizos para garantizar la continuidad de las operaciones. (Tittel, 2013)

Un plan de continuidad del negocio le ayudará a:

1. Identificar y prevenir los riesgos cuando sea posible
2. Prepararse para los riesgos que usted no puede controlar
3. Responder y recuperarse si se produce un riesgo (por ejemplo, un incidente o crisis).

Desastre: Suceso o evento que produce mucho daño o destrucción y se hace inoperable la mayor parte de los recursos en las instalaciones.

Plan de Contingencia: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas y que a su vez intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales.
Un plan de contingencia incluye cuatro etapas básicas: la evaluación, la planificación, las pruebas de viabilidad y la ejecución. (Jiménez, 2014)

Evaluación del riesgo: Metodología orientada a determinar la vulnerabilidad de la organización. Con el objetivo de determinar las posibles eventos que pueden alterar considerablemente el proceso de las operaciones de la organización.

Riesgo: Se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas, evento que puede ocasionar un daño en un activo. El riesgo es la materialización de una amenaza aprovechando la vulnerabilidad de un activo. (CIIFEN)

Amenaza: Es un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a

la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales. (CIIFEN)

Vulnerabilidad: Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo. (CIIFEN)

Impacto: Consecuencias para el negocio dado el daño al activo .Conjunto de consecuencias provocadas por un hecho o actuación que afecta a un entorno o ambiente.

Recuperación: Evento que describe planes que brindan ayuda a largo plazo a quienes han sufrido daños o pérdidas debido a un desastre de gran magnitud.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución.

Back-up: Copia de seguridad de uno o más archivos informáticos que se hace, generalmente, para prevenir posibles pérdidas de información.

Hot-Back-up: Una copia de seguridad en caliente, también llamado una copia de seguridad dinámica, Copias de seguridad calientes pueden proporcionar una solución conveniente en sistemas multiusuario, porque no requieren tiempo de inactividad

Cold-Back-up: Una copia de seguridad en frío, también llamado una copia de seguridad fuera de línea, Esta es la forma más segura de realizar copias de seguridad, ya que evita el riesgo de que la copia de datos que pueden estar en el proceso de actualización.

Cold Site: Centro de Procesamiento de Datos con infraestructura básica , que tarda en operar varios días (RED HAT)

Hot Site: Centro de Procesamiento de datos parcialmente configurado, tarda menos en un día en operar (RED HAT)

Warm Site: Centro de Datos listo para operar en pocas horas (RED HAT)

Recovery Point Objetive (RPO): Punto Objetivo de Recuperación, Periodo máximo de tiempo en el cual se han podido ver afectados los datos debido a la ocurrencia de un determinado evento.

Recovery Time Objetive (RTO): Tiempo Objetivo de Recuperación, Periodo máximo de tiempo entre el punto de interrupción y el asumible en tener los sistemas de información funcionando nuevamente después de un incidente y con los datos actualizados.

High Availability (HA): La alta disponibilidad consiste en la capacidad del sistema para ofrecer un servicio activo durante un tanto por ciento de un tiempo determinado o a la capacidad de recuperación del mismo en caso de producirse un fallo en la red.

Fault Tolerance (FT): La tolerancia a fallos puede definirse como una máquina, equipo o sistema que tiene la capacidad de recuperarse ante una falla sin interrumpir las operaciones. Un sistema informático con tolerancia a fallos se basa en tecnologías como la duplicación de discos (*disk mirroring*) y controladores redundantes.

Load Balancing (LB): El balanceo de carga tiene como propósito distribuir la carga de trabajo de una aplicación en varios equipos, por lo que la aplicación puede

procesar una carga de trabajo superior. El balanceo de carga es una manera de escalar una aplicación que demande mayor número de recursos.

Como objetivo secundario de equilibrio de carga es a menudo para proporcionar redundancia en su aplicación y de esta manera aumentar la eficiencia en los servidores.

Down-time (Tiempo de Inactividad): Es el periodo de tiempo cuando un host, sistema, etc., no se encuentra disponible o no esta en funcionamiento por diversos factores ya sean estos desde un mantenimiento, desconexión de la red, daño físico del equipo

2.8 HIPÓTESIS

2.8.1 Hipótesis General

El contar con un plan de recuperación eficaz le permite a la organización minimizar considerablemente pérdida potenciales de información y mejorar la capacidad de recuperar las operaciones normales del negocio, minimizar los tiempos de inactividad (Down time), mantener estabilidad y confiabilidad en la infraestructura que garanticen tolerancia a fallos (Fault Tolerance) y proveer de alta disponibilidad (High Availability) en los servicios que dispone la organización.

2.8.2 Hipótesis Particulares

El Plan de Recuperación de desastres, le permite minimizar la cantidad de pérdida de datos y acelerar la recuperación de procesos de las operaciones críticas.

Le simplificará el proceso de tener que levantar la infraestructura en producción, que de lo contrario hubiese sido más complejo el hecho de no tener ningún respaldo que garantice la integridad de sus datos y volver a empezar nuevamente desde cero.

Además se obtendrán una manera más planificada, organizada y ágil en caso de que ocurra un incidente.

Mediante este análisis se intenta demostrar la suma importancia y el impacto que tendría el contar con DRP en caso de una catástrofe o un incidente y que es totalmente viable y conveniente para la institución.

VARIABLES E INDICADORES

Tabla 2 - Matriz de Operaciones de Variables e indicadores

MATRIZ DE OPERACIÓN DE VARIABLES			
Variable	**Definición Conceptual**	**Dimensiones**	**Indicadores**
Plan de recuperación	Consiste básicamente en las planificación de pasos y acciones para evitar riesgos, mitigarlos y transferirlos a alguien más por medios confiables	Periodo de planificación	Tiempo considerado para la elaboración de planes estratégicos (en semanas)
		Costo/beneficio	1. Presupuesto que va a ser destinado para cubrir la planificación estratégica de recuperación (en USD). 2. Cantidad de dinero destinado para ofrecer las mejores medidas de recuperación (en USD).

		Información del plan de recuperación	1. Percepción de la problemática relacionada con el plan de recuperación. 2. Comprensión acerca de las estrategias de recuperación.
Continuidad del negocio	Consiste en la utilización del plan de recuperación para permitirle al negocio funcionar durante e inmediatamente después de declarada la emergencia	Identificación de amenazas	Determinar las posibles amenazas y riesgos según el tipo de siniestro
		Análisis del Impacto	1. Porcentaje de conocimientos acerca de las técnicas que se emplearan para la recuperación. 2.Utilizar las contingencias
		Información de la continuidad del negocio	1. Percepción de la problemática relacionada con el tipo de siniestro. 2.Poner a prueba los planes de recuperación

Elaborado por: Autor

CAPITULO III
MARCO METODOLÓGICO

3.1 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

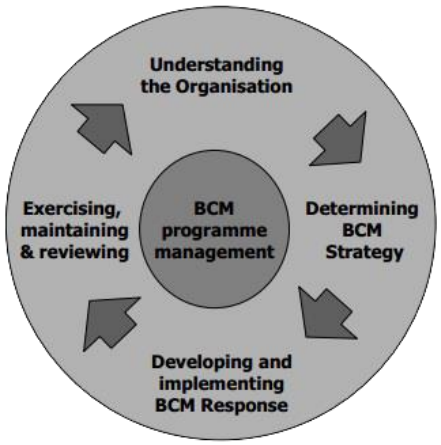
En este capítulo se aplicara la metodología de la norma ISO/IEC 24762:2008 y la norma BS 25777:2008 que es un código de buenas prácticas sobre la continuidad del negocio ; ambas se complementan y propician de ayuda en el desarrollo una guía práctica sobre el diseño de un plan de recuperación de desastres; se busca asegurar que los procesos de la organización están protegidos contra las perturbaciones y que la organización es capaz de responder de manera positiva y eficaz cuando se produce la interrupción, además le permite identificar los riesgos y decidir las medidas necesarias para ayudar a mitigarlos.

3.1.1 Metodología Propuesta

La metodología utilizada le proporciona hacer frente a los objetivos prioritarios, que le permitan asegurar la continuidad del negocio como parte de la estrategia que utilizara la organización para reanudar sus actividades y procesos críticos.

Establecer estrategias y procedimientos que le proporcionen una secuencia definida de pasos para la elaboración sistemática de una metodología propuesta, cuya planificación va a ser gestionados por un equipo designado para restablecer la infraestructura de la organización basándose en el diseño del plan de recuperación.

Ilustración 5 - BCM Ciclo de Vida – Norma BS 25777:2008



Fuente: (ISO)

Por consiguiente, se describe manera general la metodología propuesta:

Fase 1: Planificar y Conocer el Ambiente Organizacional

Fase 2: Analizar, evaluar y diagnosticar los riesgos y determinar su impacto

Fase 3: Diseñar y determinar estrategias de recuperación ante desastres (DRP).

Fase 4: Comprobación y Verificación del Diseño de recuperación.

3.1.2 Análisis del entorno actual

En la actualidad la empresa municipal cuenta con sus servicios y procesos de misión crítica virtualizados, de esta manera reducen espacio físico y aumenta la rapidez en sus operaciones, pero la discontinuidad de sus equipos no permiten sacarle provecho a esta tecnología, además muy pocas veces se brinda un mantenimiento adecuado de los mismos esto aumenta el riesgo de pérdida de sus datos, además de los constantes apagones sufridos y con contingencias muy mecánicas es de vital importancia optar por un plan de recuperación de desastres que se adapte a las necesidades de su infraestructura actual.

3.1.3 Fase de planificación

En esta primera etapa se tiene como objetivo la planificación y determinación de los procesos que planteará en el desarrollo del diseño de un plan ante desastres el mismo que involucra a directivos y personal de la empresa a designar un equipo líder o coordinador encargado de gestionar y supervisar todos los procesos involucrados en las diferentes etapas del diseño del DRP.

Como primera fase es una de las importantes y en donde se expondrá y planificara los puntos y estrategias que van a ser claves al momento de que se suscite un imprevisto y se pueda manejar con eficiencia la situación.

3.1.4 Conocer el medio ambiente general

El conocer el modelo de negocio de la empresa municipal le permita involucrarse con las actividades que se realizan a diario. Además es necesario conocer su visión, misión, planes, políticas y estrategias actuales, para poder tener una idea de cómo proceder al proponer una estrategia de recuperación que sea la más viable y que se ajuste al sistema de negocio sin alteraciones del que la empresa ya tiene definido. Una vez que se ha conocido el medio ambiente general que lo rige se procederá a identificar la estructura organizacional.

3.1.5 Identificación de la estructura Organizacional

Una parte esencial en lo que respecta a conocer el ambiente y estructura organizacional es la identificación de las áreas en particular de la empresa. El conocer de las mismas ayudará a ubicar los departamentos a los que el datacenter proveerá de los servicios que se desean respaldar y de la misma manera conocer dónde y a quien se deberá entrevistar y pedir información para poder desarrollar el plan de recuperación.

Tabla 3 - Identificación de Áreas en la Organización

Área	Actividades de Negocio
Recursos Humanos	-Administración de personal -Gestión de Nominas -Control de Desarrollo Profesional
Dirección Financiera	-Control y autorización de salarios -Control de ingresos y egresos -Custodiar los bienes, fondos e ingresos -Control de presupuestos anuales

Dirección de Ingeniería Civil	-Coordinar obras de instalaciones hidráulicas -Gestionar obras de abastecimiento de agua -Controlar obras de riego, desagüe y drenaje -Coordinar obras de saneamiento urbano y rural
Dirección de Ingeniería Industrial	-Planeamiento de la producción e inventarios -Decisiones logísticas y manejo de materiales
Asesoría Jurídica	-Asesoramiento en asuntos jurídicos -Elaborar proyectos de ordenanzas y acuerdos -Gestión Societaria -Gestión de trámites legales, judiciales y extrajudiciales
Auditoria Interna	-Garantizar y regular los procesos internos -Control , fiabilidad e integridad de informes -Control eficiente de recursos -Verificación constante de activos
Tecnología y Sistemas	-Soporte y mejora continua de la infraestructura informática -Asesoría informática -Establecer políticas y toma de decisiones TI

Elaborado por: Autor

3.1.6 Definición de una estructura de procesos

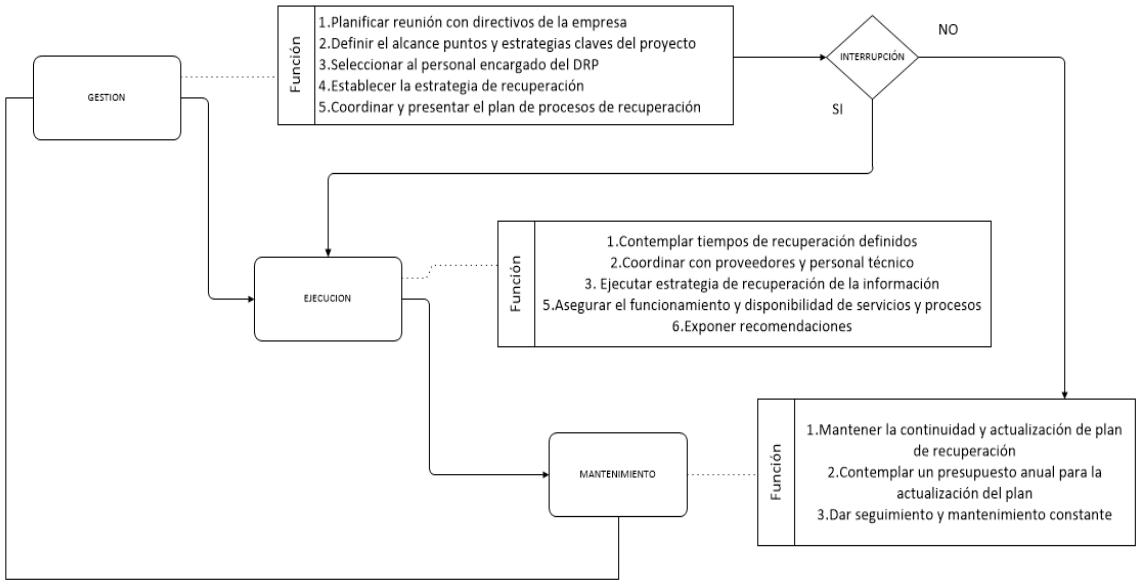
Una vez que se estableció el plan y determinó las áreas principales, debe definir una estructura de procesos con el fin de dar el seguimiento de actividades relacionadas con el procedimiento de recuperación. (Jenny Caicedo, 2012)

GESTIÓN: Conjunto de tareas o subprocesos generales en donde se va a contemplar la planificación y estrategias a utilizar en el proceso de un plan de recuperación.

EJECUCIÓN: Es el proceso donde va a poner en marcha las acciones y estrategias de recuperación que se determinaron en el planificación del proyecto.

MANTENIMIENTO: Es el proceso donde coordina la actualización continua del plan.

Ilustración 6 - Diagrama de flujo de procesos y actividades de planificación



Elaborado por: Autor

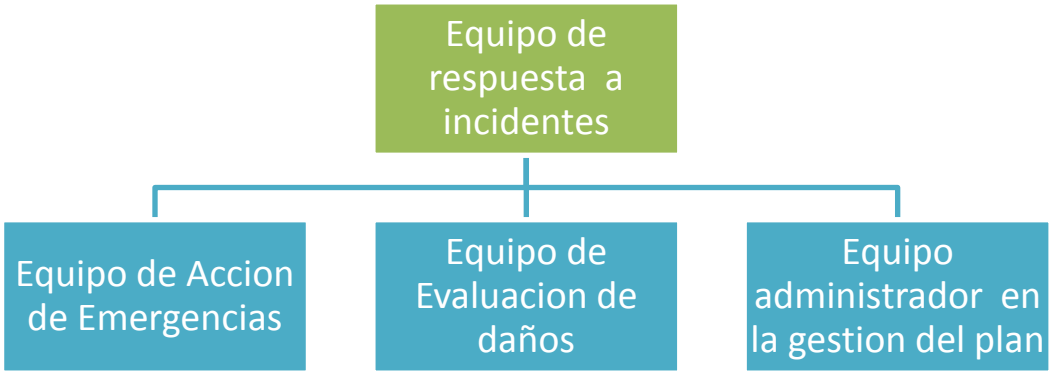
3.1.7 Designar un equipo coordinador DRP

Una vez identificado la estructura organizacional, se debe designar un equipo para liderar la tarea de recuperación, el coordinador o el equipo deben trabajar en conjunto con la dirección gerencial y administrativa para identificar el alcance, objetivos y actividades de negocio que son críticas en la empresa municipal.

Adicionalmente, se debe escoger al personal con el perfil de la figura de gestión de la continuidad del negocio, no es necesario que este localizado en áreas de tecnología o sistemas.

Dependiendo si la empresa tiene un presupuesto promedio, es recomendable asignar personal adicional y establecer un equipo dedicado a la continuidad del negocio.

Ilustración 7 - Grupo de trabajo para la respuesta de incidentes



Elaborado por: Autor

3.1.8 Definición de objetivos y alcances del DRP.

Al definir los objetivos y contemplar el alcance de un plan ante desastres, se observa que los equipos físicos son sin duda alguna los que determinaran en parte la gestión de los objetivos puestos que estos deben estar contemplados en el presupuesto de la organización.

3.1.9 Aprobación de la alta gerencia.

Una vez determinado toda la gestión para realizar la planificación del plan es necesario exponer y presentar un informe a la alta gerencia junto con el personal de TI, ya que serán los encargados de examinar los puntos expuestos y decidir si se da o no la aprobación para que el proyecto continúe. Entre algunas responsabilidades que el encargado de la gestión de esta fase debe cumplir:

- ✓ Coordinar y ser capaz de organizar al personal por cada etapa del proyecto
- ✓ Dirigir el procedimiento de los objetivos, políticas y actividades críticas del negocio.
- ✓ Mantener controlado los tiempos establecidos para el proceso de recuperación.
- ✓ Contemplar las delimitaciones del presupuesto asignado.
- ✓ De la misma manera se exponen las siguientes acciones a tomar:

- ✓ Asignar el equipo del proyecto y determinar sus responsabilidades.
- ✓ Comunicar la necesidad de obtener un plan de recuperación y continuidad del negocio.
- ✓ Comprometer a la alta gerencia en las decisiones a tomar.
- ✓ Coordinar y desarrollar las actividades del proyecto.
- ✓ Dar seguimiento en el avance del plan de recuperación.

3.2 TIPO DE INVESTIGACIÓN

Con el desarrollo del proyecto se hará uso de la metodología investigativa que pretende reducir riesgos y brindar mayor seguridad e integridad de la información en la empresa además de ofrecer una mayor efectividad mediante un plan de contingencia contra desastres.

El tipo de investigación que se utilizará para este fin será descriptivo, de campo y explicativo.

Investigación descriptiva: Le permite detallar y describir las actividades y características que presenta el centro de datos de dicha organización.

Investigación de campo: Se basara en la observación de los sucesos reales. Se realizara un estudio de la situación actual para diagnosticar las posibles vulnerabilidades, amenazas, riesgos y necesidades que acontecen en la organización.

Investigación explicativa: Es explicativa porque se encargará de determinar cuáles son los motivos por el cual se suscitan irregularidades ante alguna situación inesperada en el centro de datos.

3.3 POBLACIÓN Y MUESTRA

El universo estuvo constituido por un segmento de 150 empleados [N] que laboran permanentemente en la empresa municipal de la ciudad de Guayaquil, para obtener la muestra se calculó mediante la formula $n = \frac{K^2 * p * q * N}{(e^2 * (N-1)) + K^2 * p * q}$ tomando en consideración un nivel de confianza [K] del 90% y con un error de muestra [e] del

5%, el cual generó una muestra de 84 individuos que indagarán sobre la utilidad y el beneficio de contar con un plan de recuperación ante desastres. (FeedBack-Networks, 2013)

3.4 PLAN DE RECOLECCIÓN DE INFORMACIÓN

Se basara en 2 métodos a fin de recopilar información sobre la situación existente.

La Observación: Se realizará un avistamiento de la infraestructura en producción del centro de datos con el fin de determinar las posibles vulnerabilidades y riesgos existentes en la misma y se documentará las situaciones de mayor importancia para posteriormente dar las respectivas recomendaciones.

La Entrevista: Se basara en la formulación de preguntas que se plantearan al personal de TI responsable del centro de datos, para tratar temas logísticos de infraestructura y de seguridad necesarios para realizar el plan de recuperación.

3.5 PLAN DE PROCESAMIENTO DE INFORMACIÓN

Mediante el estudio de la situación actual de la infraestructura tecnológica de la empresa municipal se aplicara una estrategia para el análisis de un plan de recuperación ante desastres mediante la utilización de la norma ISO/IEC 24762:2008. Esta norma servirá como guía para el desarrollo del diseño del plan de recuperación. Una vez hecho el análisis de criticidad y detectado los riesgos y vulnerabilidades que envuelve el ambiente organizacional se podrá determinar y ofrecer alternativas de recuperación factibles.

3.5.1 El método

Se aplicara el método inductivo, puesto que se realizará la observación, análisis y determinación de los riesgos y vulnerabilidades que justifiquen la necesidad de adoptar un plan de recuperación .Una vez hecho el análisis se recomendará a la empresa municipal la mejor estrategia que deben considerar para recuperarse ante un desastre.

CAPITULO IV

4.1 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

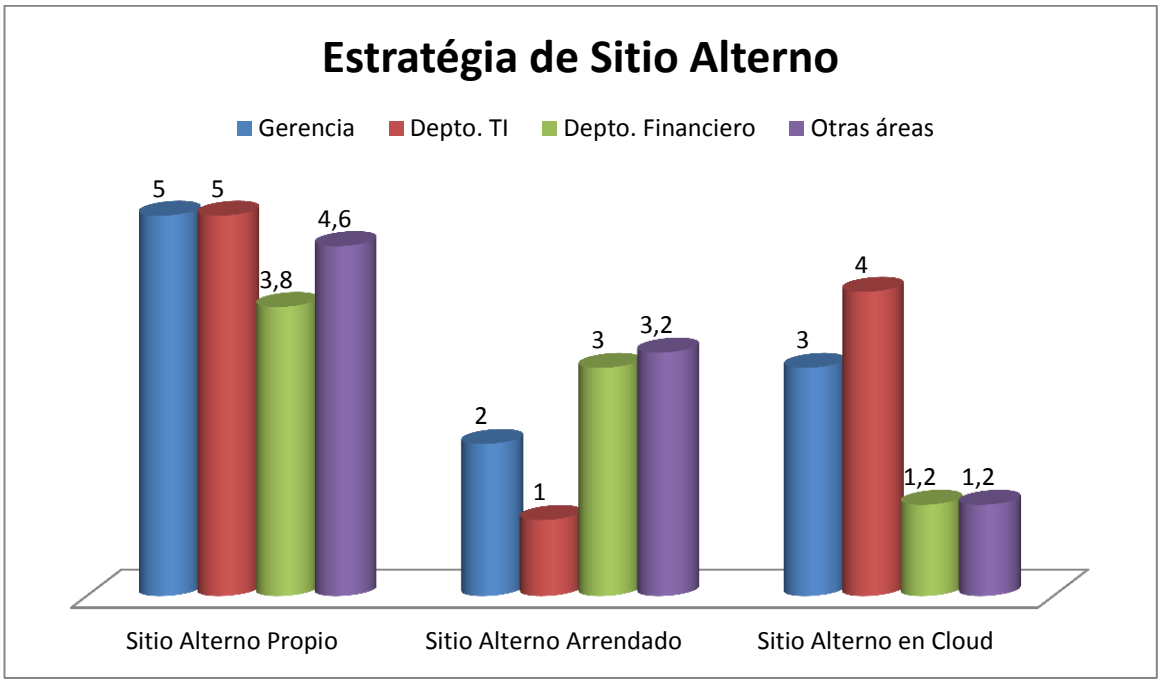
4.1.1 Análisis de los resultados

Tomando en consideración la muestra establecida anteriormente de 84 personas encuestadas de los diversos departamentos de la empresa municipal acerca de los beneficios de contar con un plan de recuperación y las consecuencias que este podrá desencadenar, se procede a plasmarlo estadísticamente los resultados obtenidos por cada una de las áreas que posiblemente se podrían ver afectadas a causa del siniestro. El gerente general es el principal interesado y encargado de tomar decisiones en cuanto el desarrollo del plan y es de suma importancia mantener protegido los datos (16%) ; el personal de TI reconoce la importancia del proyecto y los efectos que se ocasionaría el no contar con un plan estratégico (16%) ; el resto de áreas tales como RRHH(15%), Financiero(13%), Comercial(15%), Obra civil(10%), Jurídico(10%) también están conscientes de los efectos drásticos que se obtendrían en caso de no contar con un plan de contingencias.

Ilustración 8 - Gráfico estadístico de la encuesta de un plan de recuperación

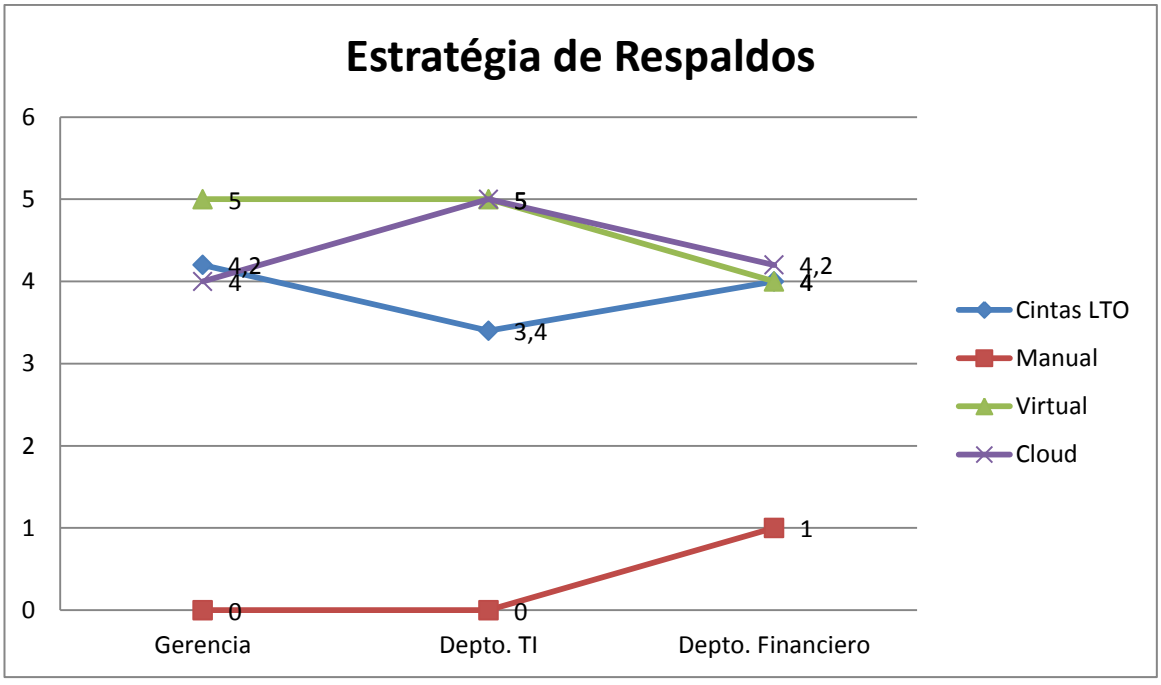
Elaborado por: Autor

Ilustración 9 - Gráfico de barras sobre la encuesta de sitio alterno



Elaborado por: Byron Nieto

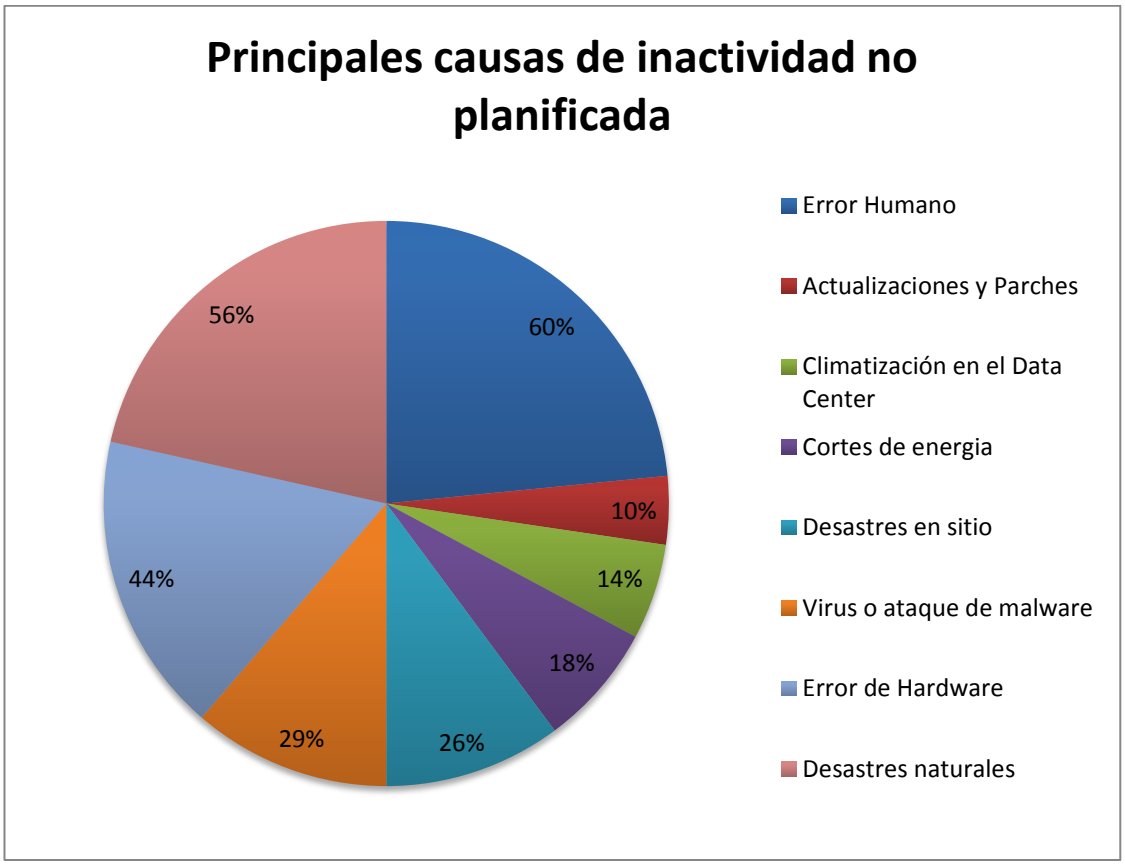
Ilustración 10 - Gráfico estadístico sobre encuesta de estrategia de respaldos



Elaborado por: Byron Nieto

Mientras que la naturaleza podría ser la causa de los desastres más dramáticos a ocurrir a una empresa, el error humano es todavía el más común ya que causa (60%) del tiempo de inactividad del sistema. La incapacidad de poder recuperarse inmediatamente a causa de un fallo del sistema, especialmente como resultado de error humano, es un negocio costoso y a su vez rentable para las empresas que se encarga de ofrecer este tipo de servicios. (Ponemon Institute, 2012)

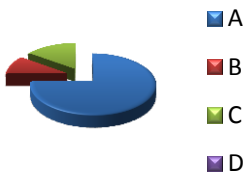
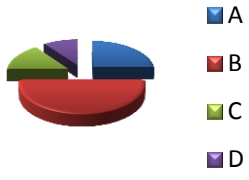
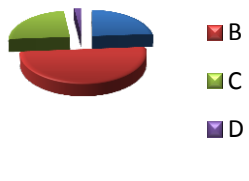
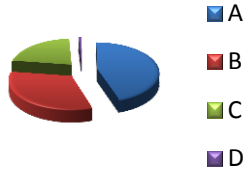
Ilustración 11 - Causas principales de inactividad no planificada

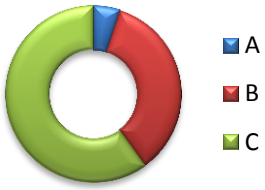


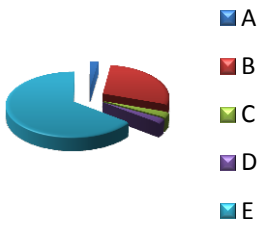
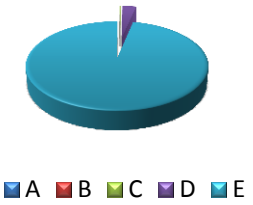
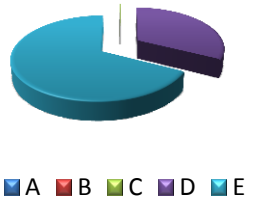
Fuente: **(Acronis, 2012)**

La gran mayoría de las organizaciones encuestadas (86%) había experimentado una o más instancias de inactividad del sistema durante los últimos 12 meses que tenían, en promedio, duró 2,2 días. Las empresas calculan que la pérdida de productividad debido directamente a esta el tiempo de inactividad les cuesta cada una de aproximadamente USD $ 366.363 al año.

4.1.2 Resultados de la encuesta realizada al personal de la empresa municipal

Ítem	Indicadores del cumplimiento de los objetivos	Escala	Porcentaje obtenido	Gráfico representativo de los porcentaje obtenidos
1	¿Qué método de respaldos es utilizado actualmente en la empresa municipal?	A. Backup por cintas	75%	
		B. Backup por mirroring	10%	
		C. Backup medios extraíbles	15%	
		D. Backup en la nube	0%	
2	¿Con cuanta frecuencia se realizan los respaldos en la empresa?	A. Diario	25%	
		B. Semanal	50%	
		C. Quincenal	15%	
		D. Mensual	10%	
3	¿De qué manera se administran los respaldos y restauración de los datos?	A. Full Backup	23,8%	
		B. Incremental	50%	
		C. Diferencial	24,2%	
		D. Desconozco	2%	
4	¿Conoce usted los riesgos a los que se enfrenta actualmente la empresa?	A. Apagones eléctricos	45%	
		B. Infraestructura antigua	32,3%	
		C. Virus	21,8%	
		D. Insuficiente métodos de respaldos	0,9%	

Ítem	Indicadores del cumplimiento de los objetivos	Escala	Porcentaje obtenido	Gráfico representativo de los porcentaje obtenidos
5	¿Conoce si la empresa posee un presupuesto destinado para restauración de la infraestructura en el caso de suscitarse el siniestro?	A. Si	5%	
		B. No	35%	
		C. Desconozco	60%	
6	¿Cuál de las siguientes opciones, piensa usted que es una forma estratégica de mantener almacenada de la información?	A. Sitio alterno	78%	
		B. Sitio arrendado	5,5%	
		C. Servicios en la nube	16,5	
		D. Otros	0%	
7	¿Cuál es el tiempo prudencial que considera la empresa para restablecer sus operaciones?	A. Menor a 12 horas	93,8%	
		B. Mayor a 12 horas	4,2%	
		C. Mayor a 1 día	2%	
		D. Mayor a 1 semana	0%	
8	¿Qué grado de importancia tiene la obtención de un plan de recuperación?	A. Muy Significativo	99,8%	
		B. Significativo	0,2%	
		C. Considerable	0%	
		D. Sin importancia	0%	

Ítem	Indicadores del cumplimiento de los objetivos	Escala	Porcentaje obtenido	Gráfico representativo de los porcentaje obtenidos
9	¿A escuchado de este tipo de herramientas de backup de información que sirven como técnicas útiles a nivel empresarial?	A. Symantec Netbackup	2,2%	
		B.HP data protector	27%	
		C.IBM Flash copy	2,5	
		D.EMC Networker	2,3%	
		E. VMWare Site Recovery Manager	62%	
10	¿La empresa está preparada para afrontar las diversos situaciones de desastres tales como?	A. Inundaciones	4%	
		B. Incendios	78,2%	
		C. Terremotos	7,3%	
		D. Rayos	2%	
		E. Ninguno de los anteriores	8,5%	
11	¿Qué tan beneficioso considera el adoptar un plan de recuperación ante desastres?	1	0%	
		2	0%	
		3	0,2%	
		4	3,1%	
		5	96,7%	
12	¿Según los antecedentes en la empresa, con cuanta urgencia considera el desarrollo del plan ante desastres?	1	0%	
		2	0%	
		3	0,2%	
		4	32,3%	
		5	67,5	

4.2 INTERPRETACIÓN DE DATOS

4.2.1 Interpretación del plan de recuperación ante desastres

Analizando estadisticamente los resultados obtenidos de la encuesta realizada a los principales implicados en la empresa municipal, se ha demostrado el interés por obtener un plan de recuperación ya que conocen los riesgos y los efectos que estos implican. El mayor porcentaje de interés es la gerencia, el personal de TI y el departamento financiero.

4.2.2 Interpretación en la selección estratégica de sitio alterno

Tomando en consideración las áreas de mayor interés quedo demostrado que prefieren obtener un sitio alterno propio, tomando en consideración el costo y beneficio que las alternativas de cloud y de sitio arrendado demandaban.

4.2.3 Interpretación de la estrategia de respaldos

A la empresa municipal se le planteo las diversas formas de respaldos que frecuentemente son utilizadas por algunas organizaciones, la empresa se inclina por el método de recuperación por replicación virtual, tomando en consideración el costo, seguridad y fiabilidad que esta le puede brindar. La alternativa de servicio de cloud es también una muy buena estrategia, pero siempre y cuando la empresa este disponible a asumir el costo que esta demanda y también la confianza que genera en poner a disposición toda la información de su core de negocio a la empresa que brinda este servicio. Actualmente se utiliza la estrategia de respaldos por medio de cintas LTO pero se desea que los respaldos se hagan de manera automática. Casi ninguno opto por la recuperación manual por el riesgo significante que este implica.

4.2.4 Análisis e interpretación de los resultados de las encuestas

1. ¿ Que método de respaldos es utilizado actualmente en la empresa municipal?

El personal que labora en la empresa municipal de las diversas areas respondieron de la siguiente manera, el 75% meciono que se realizan respados por cintas , el 10% menciono que se realizan los respaldos por disk mirroring, el 15% que se realizan los respaldos por medios extraibles y con un 0% no se realiza de ninguna manera respaldos en cloud.

2. ¿Con cuanta frecuencia se realizan los respaldos en la empresa?

El personal que labora en la empresa municipal de las diversas areas respondieron de la siguiente manera, el 25% mencionó que se realizan los respaldos a cinta de los servicios mas criticos a diario,el 50% expuso que se realizan semanlmente, el 15% mencionó que se realiza quincenalmente, el 10% mecionó que se realizan mensualmente.

3. ¿De qué manera se administran los respaldos y restauración de los datos?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 23,8% que se realizan los respaldos como full backup, el 50% mencionó que se realizan incremental debido a que eran mas rápido la resatauración, el 24,2% mencionó que realizan el respaldo de manera diferencial, un 2% desconocen la forma en como se generan los respaldos.

4. ¿Conoce usted los riesgos a los que se enfrenta actualmente la empresa?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 45% mencionó que sufrían constantemente apagones eléctricos, el 32,3% contestaron que los riesgos se deben a la infraestructura muy antigua, el 21,8% aludieron que estaban expuestos a virus, el 0,9% citaron que los riesgos se debían por insuficientes métodos de respaldos.

5. ¿Conoce si la empresa posee un presupuesto destinado para restauración de la infraestructura en el caso de suscitarse el siniestro?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 5% indicaron que sí disponen de un presupuesto ,el 35%

contestaron que no tenían un presupuesto destinado a solventar el incidente, el 60% desconocían de estos valores.

6. ¿Cuál de las siguientes opciones, piensa usted que es una forma estratégica de mantener almacenada de la información?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 78% indico que seria una buena estrategia mantener almacenada y replicada la información en un sitio alterno, el 5,5% se acojió a citar un sitio alterno arrendado, el 16,5 citaron a la estrategia de servicios en cloud.

7. ¿Cuál es el tiempo prudencial que considera la empresa para restablecer las operaciones normales del negocio?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 93,8% la maroria del personal consideró que la empresa deba restablecerse en menos de 12 horas, el 4,2% mencionó que la empresa podria ser restablecida en un lapso mayor a 12 horas, el 2% aludio que la recuperación se prolongaría más de 1 día.

8. ¿Qué grado de importancia tiene la obtención de un plan de recuperación?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 99,8% mencionaron que es muy significativo el obtener un plan de recuperación ante desastres y el 0.2%

9. ¿A escuchado de este tipo de herramientas de backup de información que sirven como técnicas útiles a nivel empresarial?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 2,2% mencionó que conocen sobre la herramienta Symantec Netbackup, el 27% citó conocer la herramienta HP Data protector, el 2,5% aludieron conocer la herramienta IBM Flash copy, el 2,3% mencionó que conocen la herramienta EMC Networker y la mayoria con un 62% adujo conocer la herramienta Vmware Site recovery manager.

10. ¿La empresa está preparada para afrontar las diversos situaciones de desastres tales como?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 4% menciono que la empresa está preparada contra inundaciones,el 78,2% declaro que está preparada en situaciones de incendios, el 7,3% considero que la empresa esta preparada contra terremotos, el 2% considero que esta preparada ante tormentas y rayos, el 8,5% adució que la empresa no esta preparada para ninguno de estos eventos.

11. ¿Qué tan beneficioso considera el adoptar un plan de recuperación ante desastres?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 96,7% siendo el 5 como máximo puntaje en la escala mencionó que es de sumo beneficio obtar por un plan de recupeación, el 3,1% seleccionó en escala 4 y el 0,2%

12. ¿Según los antecedentes en la empresa, con cuanta urgencia considera el desarrollo del plan ante desastres?

El personal que labora en la empresa municipal de las diversas áreas respondieron de la siguiente manera, el 67,5% siendo 5 como máximo puntaje en la escala mencionó que es de urgencia el desarrollo del plan, el 32,3% seleccionó en escala 4 mencionó que es considerable el desarrollo del plan y el 0,2% seleccionó la escala 3 mencionó que es no es tan urgente el desarrollo del plan.

4.3 VERIFICACIÓN DE HIPÓTESIS

En la hipótesis se asume que el plan de recuperación ante desastres debería contar con aspectos muy importantes tales como alta disponibilidad (High Availability), tolerancia a fallos (Fault Tolerance) y minimización de tiempos de inactividad (Down Time).

La estrategia de respaldo que escogió la empresa reúne todos estos aspectos, mediante la utilización de VMWare Site Recovery Manager, ofrece la flexibilidad de especificar situaciones de failover lo que permite que las máquinas virtuales se encuentren replicadas y sincronizadas mejorando el RPO de 24 horas a 90 minutos y reduce el RTO un 75% desde 48 horas a menos de 1hora. (vmware) . Además se ofrece la facilidad de tener una configuración centralizada y planes de recuperación en cuestión de minutos a través de políticas predefinidas.

Se realizaron las respectivas pruebas con el software antes mencionado y se corroboro la eficacia de replicación y sincronización que se estimaban, tomando como referencia los tiempos mínimos y máximos de recuperación y de inactividad ya definidos en el capítulo 4.

CAPITULO V

5.1 CONCLUSIONES Y RECOMENDACIONES

5.1.1 Contra riesgos y vulnerabilidades

En función a los antecedentes previos se pudo comprobar la existencia de riesgos y amenazas entre estos el desconocimiento y manipulación de la tecnología moderna , la exposición imprudente de credenciales y claves de los servidores. Además hay que tener en cuenta que el riego siempre está presente en cualquier sitio, aún más si se trata de los seres humanos que por el hecho de ser imperfectos tomamos decisiones equivocadas y en algunas ocasiones somos participes de generar violencia.

5.1.2 Diseño del plan de recuperación

Se pudo constatar la existencia de una gran exposición de riesgo en sus datos ya que la mayoría de su infraestructura tecnológica es antigua y no cuentan con un mantenimiento periódico en los equipos. Con el diseño del plan de recuperación se tendrá una guia práctica acerca de los procedimientos o procesos que se deben seguir si se presenta un siniestro.

5.1.3 Restablecimiento de la información

Mediante la evaluación de los métodos actuales de backups se pudo comprobar que los respaldos se realizan de manera muy mecánica , no cuentan con una solución que permita automatizar y calendarizar las tareas de respaldos.

5.1.4 Designación de responsabilidades

Analizando el organigrama de la empresa actualmente no tienen conformado a un grupo de personas que se encarguen de la labor de recuperación del plan en mención , es de suma importancia designar a una persona o grupo de personas que se encague de cumplir logisticamente el plan de recuperación una vez desatada la catástrofe.

5.2 RECOMENDACIONES

Una vez alcanzado con éxito los objetivos y determinado las conclusiones se procede a sugerir las respectivas recomendaciones con el fin de mejorar el plan de recuperación.

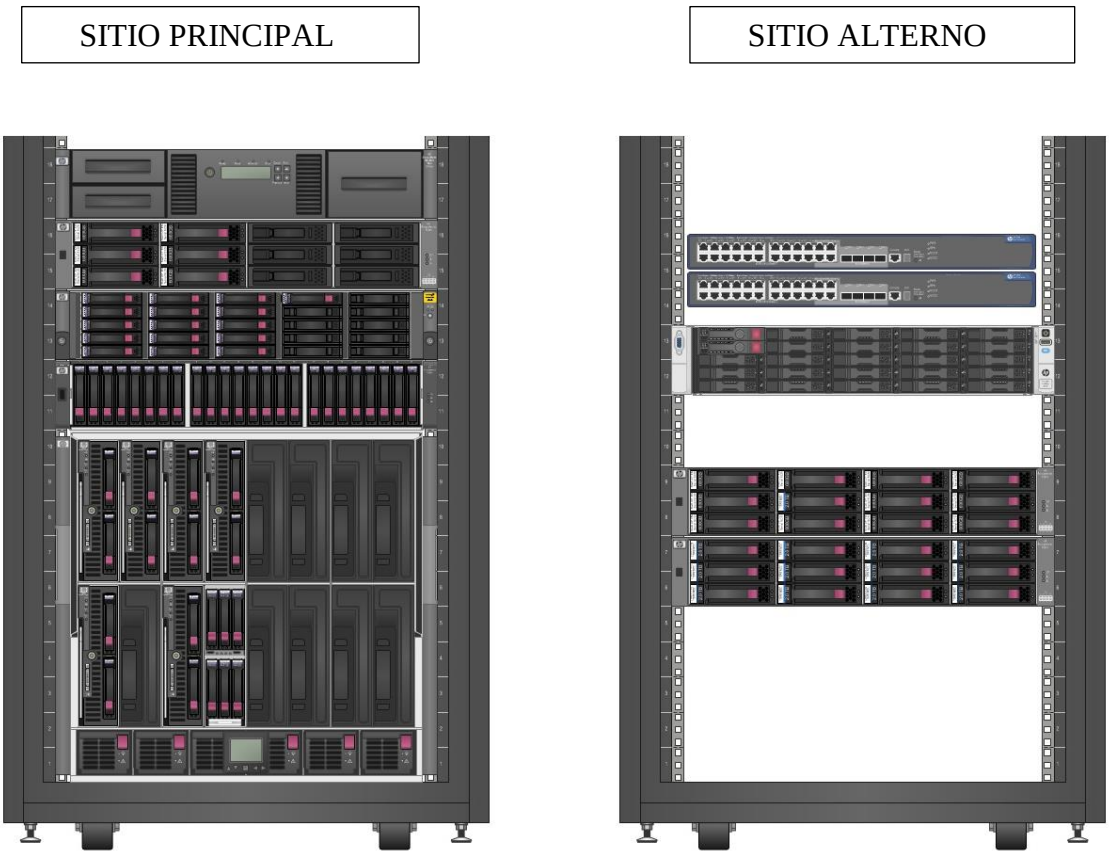
1. Para mejoras del Plan de recuperación se recomienda el diseño de un plan de continuidad del negocio (BCP) , con el objetivo de mantener la estabilidad de las operaciones del negocio
2. Se recomienda la utilización de servicios de cloud computing tales como las que ofrece Microsoft con su producto “Windows Azure”, también las que ofrece VMWare con su producto “Centro de datos definido por Software (SDDC)”.
3. Es recomendable acoplar estrategias de respaldos actuales con el objetivo de mejorar y optimizar la restauración de la información.
4. Es de suma importancia contar con auditorías especializadas para minimizar los riesgos y brindar de recomendaciones eficaces que ayuden a la mejora continua del plan de recuperación.
5. Si el presupuesto general de la organización no puede cubrir los gastos que ofrecen los servicios en cloud, se recomendaría la opción de nube hibrida.

CAPITULO VI

6.1 PROPUESTA

La propuesta que se ofrece a la empresa municipal para mantener sus operaciones, procesos activos y datos protegidos, es la adquisición de un sitio alterno que permita la recuperación inmediata y estratégica de las operaciones del negocio, se propuso virtualizarlo con (VMWare – ESXI 5.5 y vCenter Site Recovery Manager) con el propósito de disminuir costos asociados con la infraestructura y reanudar rápidamente las operaciones. Además se sugiere tener un enlace dedicado que permita realizar copias de seguridad de la información para evitar afectar el rendimiento y ancho de banda administrativo.

Ilustración 12 - Propuesta para el plan de recuperación de Desastres



Elaborado por: Autor

6.2 ANTECEDENTES DE LA PROPUESTA

La determinación de optar por un plan de recuperación en una empresa municipal se vio antecedida por la cantidad de riesgos existentes y que en ella residen.

1. El asunto de no tener sistemas redundantes en sus equipos de comunicación y sistemas de energía que impidan alterar el buen funcionamiento de los equipos o al menos el permitir el proceso de la baja adecuada de servicios y apagado de los mismos hasta que se reanuden los suministros, es un tema a considerase como muy significativo.

2. Otro punto importante que hay que destacar es el hecho de tener equipos obsoletos tecnológicamente hablando; aun cumpliendo funciones y procesos esenciales de sumo valor crítico, que quizás no generaba mayor importancia en su determinado momento, cuando aún no había crecido su nivel de negocio, pero hoy en día es vital.

3. El no contar con buenas estrategias de respaldos es otro punto muy importante que se debe tomar en consideración; el solo optar con respaldos en cintas y mantenerlas alojadas en el mismo sitio es un gran riesgo que han enfrentado durante algunos años

4. La designación de un equipo de emergencia que cumpla con la responsabilidad de poner en marcha el plan si algún acontecimiento de magnitudes significativas ocurre.

5. El no optar por una consola de antivirus que permita proteger los servidores y endpoints y además verificar el análisis de infección residente en la organización, es otro de los temas a considerar para generar una posible propuesta de solución para erradicar estos inconvenientes.

6.3 JUSTIFICACIÓN

Según los resultados anteriormente mostrados, hicieron poner en tela de juicio el porqué de la necesidad de optar por un plan de recuperación; en esta instancia se pone como justificación la necesidad de implantación del mismo, el cual le permite a la empresa a mantener estabilidad en su sistema de negocio, mediante el mirroring de la información en un sitio alterno.

El objetivo de la justificación es explicar de manera convincente por qué y el para de la selección de un plan de recuperación ante desastres.

6.3.1 Descripción de problema

Una empresa municipal ha venido sufriendo varios inconvenientes en los 2 últimos años, entre los más potenciales es la perdida y energía que ha afectado en varias ocasiones a su infraestructura tecnológica e incluso teniendo que reemplazar en distintas ocasiones discos duros que se han dañado a causa de los apagones sufridos. Esto ha producido alteraciones y pérdida significativa de sus datos.

6.4 OBJETIVOS

6.4.1 Objetivo General ¿Por qué se hace?

Se lo realiza con el objetivo de determinar y mitigar los riesgos que presenta actualmente la empresa. Es por ello, que se pretende utilizar la estrategia de replicación mediante la adquisición de un sitio alterno que permita respaldar y proteger datos, procesos críticos que impidan afectar la continuidad del negocio en la organización.

6.4.2 Objetivo Especifico ¿Para qué se hace?

Para prevenir la pérdida de información y reducir el tiempo mínimo de inactividad en los procesos y operaciones críticos.

6.5 ANÁLISIS DE FACTIBILIDAD

Una vez realizadas las pruebas respectivas para asegurar el funcionamiento del plan de recuperación se procedió a realizar un pequeño simulacro después de la jornada normal de trabajo, la misma que consistió en apagar los equipos del sitio principal con el objetivo de tomar el control sobre las operaciones y servicios replicados en el sitio alterno.

Objetivos Previos	Resultados Obtenidos
1. Minimizar riesgos y amenazas	1. Minimización de costos operativos
2. Protección de la información	2. Minimización y reducción de espacio físico usado por los servidores
3. Reducir el tiempo de inactividad	3. Reducción considerable del RPO y RTO
4. Evaluación de interrupciones y daños	4. Administración flexible y centralizada
5. Determinar servicios y procesos críticos	5. Alta disponibilidad y escalabilidad
6. Determinación del impacto operacional	

6.6 FUNDAMENTACIÓN

Para la realización de este proyecto se basó en el estándar ISO/IEC 24762:2008 y el estándar de buenas prácticas BS 2777:2008 que facilita el proceso de desarrollo de un plan de recuperación ante desastres.

ANÁLISIS

6.6.1 Fase de análisis y evaluación de riesgos

Una vez terminada la fase de planificación se procederá con la fase de evaluación en donde involucra la identificación de amenazas tanto internas como externas, las mismas que puedan ocasionar la interrupción de las operaciones normales del

negocio y la perdida de los procesos y actividades críticas de la organización . En esta fase se plantea la toma de medidas y priorización de planes de acción de gestión de riesgo, planes de las actividades de misión crítica, dependencias, fallas y análisis del impacto y efecto que ocasionaría en el caso de la pérdida total o parcial de los procesos críticos de la organización.

En esta fase es importante considerar el análisis del impacto al negocio conocido como (BIA – Business Impact Analysis), el mismo que tiene un enfoque a dos objetivos que son:

- ✓ RPO (Punto Objetivo de Recuperación): Es el punto en el cual fueron interrumpida las operaciones de los sistemas debido a un siniestro.
- ✓ RTO (Tiempo Objetivo de Recuperación): Es el tiempo que se estima para que las operaciones y procesos críticos estén en funcionamiento nuevamente. (Crump, 2014)

Ilustración 13 - Tiempos y puntos objetivos de recuperación

Nivel de RTO	Intervalo de Recuperación
1	Menor a 2H
2	De 2H a 24H
3	De 24H a 40H
4	De 2Dias a 5Dias
5	Mayor a 5 Días

Fuente: (Securityartwork, 2012)

El objetivo de definir el BIA en la etapa de análisis y evaluación de riesgo es permitir la identificación de los riesgos asociados con el evento previo a su ocurrencia para intentar mitigarlos. Al momento de diseñar un informe para desarrollar el análisis del impacto del negocio hay que tomar las siguientes recomendaciones: (Mendoza, 2014)

- ✓ Definir la frecuencia de utilización del proceso.
- ✓ Determinar si el proceso es considerado crítico.
- ✓ Considerar el tiempo de inactividad de dicho proceso.
- ✓ Evaluar y determinar el periodo máximo de interrupción.
- ✓ Determinar la compatibilidad de versiones en las aplicaciones.
- ✓ Detectar indicadores y medidas de desempeño existentes.
- ✓ Considerar procedimientos alternos.
- ✓ Verificar la efectividad de procedimientos alternativos.
- ✓ Estimar los recursos mínimos en la recuperación.
- ✓ Definir los posibles impactos y eficiencia operativa.
- ✓ Determinar responsables de las operaciones individuales.

6.6.2 Determinación de funciones de criticidad de servicios y recursos

En este punto se debe listar todas las funciones y servicios del área que se pretende tomar como referencia, en este caso es el datacenter de la empresa municipal, para determinar los recursos computacionales considerados como críticos. Se debe tomar en consideración el tiempo máximo que se debe de esperar para la subida y reanudación de los servicios y procesos.

6.6.3 Identificación, análisis y evaluación de riesgos

Para establecer la probabilidad de ocurrencia e impacto que podría generar un riesgo se exponen los siguientes gráficos en donde se toma en consideración las vulnerabilidades versus las pérdidas que pueden desencadenar dichos riesgos. (Freitas, 2009)

Tabla 4 - Probabilidad de ocurrencia de un riesgo

PROBABILIDAD DE OCURRENCIA

NIVEL	FRECUENCIA	DETALLE
1	Irregular	Muy pocas veces puede ocurrir
2	Improbable	Podría ocurrir en algún instante
3	Regular	Puede ocurrir en algún momento
4	Probable	Tiene probabilidad que ocurra con mayor frecuencia
5	Certero	Se da el caso de ocurrencia del evento

Elaborado por: Autor

Tabla 5 - Impacto potencial del riesgo

IMPACTO POTENCIAL

NIVEL	VALOR	DETALLE
1	Insignificante	Sin daños y muy baja pérdida económica.
2	Menor	Daños menores, primeros auxilios, pérdida económica media.
3	Moderado	Se requiere atención, perjuicios medios, tratamiento médico.
4	Elevado	Se presta mayor atención, pérdida de producción, mayor prejuicio, pérdida económica mayor.
5	Caótico	Inactividad completa, muerte, pérdidas económicas extremas.

Elaborado por: Autor

6.6.4 Matriz de riesgos

La importancia del diseño de la matriz de riesgo radica en un diagnóstico real de la empresa o negocio y predice en qué estado se encuentra actualmente la organización, de esta manera se brinda el principal elemento requerido para tomar

decisiones y proporciona de una visión global e integral de la verdadera situación, la cual le permite definir medidas necesarias para enfrentar situaciones de riesgos, minimizar sus efectos y reaccionar oportunamente con efectividad.

El nivel de probabilidad de los riesgos detectados anteriormente y la incidencia en la empresa municipal se los puede establecer con rangos de valores que permitan identificar los riesgos siendo los de mayor criticidad de nivel [5] y los de menor nivel [1] en la infraestructura organizacional. Como de muestra en el siguiente gráfico:

Ilustración 14 - Parámetros de medición de riesgos y Amenazas

		Criminalidad			**Riesgos físicos**					**Negligencia**		
Elementos implicados	Magnitud del daño	Virus	Accesos no autorizados	Mal uso de la información	Fuego	Inundaciones	Terrorismo	Fallas Eléctricas	Terremotos	Mantenimiento	Puertos abiertos	Exponer contraseñas
Servidores	alto	3	3	2	5	4	4	3	4	4	3	4
Enlaces de red	muy alto	2	3	3	5	4	4	5	2	5	4	4
Sistema Eléctrico	alto	1	5	1	5	4	3	5	2	4	1	1
Ordenadores	bajo	2	2	3	5	4	3	2	1	1	1	1
Información	muy alto	3	5	5	5	4	5	1	3	3	4	2
Edificación	moderado	2	2	1	5	4	3	4	4	3	1	1

Elaborado por: Autor

IMPACTO:
1= Insignificante
2= Menor
3= Moderado
4= Elevado
5= Catastrófico

PROBABILIDAD:
1= Muy Baja
2= Baja
3= Medio
4= Alto
5= Muy Alto

6.6.5 Análisis de control de riesgos

Al haber determinado el análisis y la evaluación de riesgos, ahora se determinara el análisis de control de riesgos, en donde se pretende describir estrategias para tratar de minimizar y mitigar los riesgos que están presentes en los procesos y de esta manera poder reanudarlos.

En muchas ocasiones se da el caso, que pese a las medidas que se adoptan para el control de riesgos igual puede ocurrir un desastre, es por ello que hay que estar preparado para diversas situaciones adversas que se puedan presentar.

6.6.6 Definición de estrategias para el control de riesgos

Como primer paso es la determinación de estrategias como un mecanismo de seguridad y protección para tratar de reducir el porcentaje de criticidad que tenga un evento y mantener el control sobre los mismos. Podemos destacar cuatro principales estrategias:

1 **Evitar el riesgo:** Quizás esta opción es para muchos desestimada porque si el nivel de riesgo es muy alto va a resultar insensato tratar de evitarlo, pero si se plantea de otra manera tal como adquisición de un sitio alterno, es una de las mejores opciones para evitar pérdidas e inactividad en las operaciones y contar con un presupuesto anual para invertir en tecnología.

2 **Minimizar el riesgo:** Si bien es cierto el riesgo es dependiente de la probabilidad de ocurrencia y a su vez del impacto, para mayor comprensión se puede exponer de la siguiente manera:

[Probabilidad = muy probable] x [Impacto=Alto] = [Riesgo = Alto]

Una manera de minimizar el riesgo es contar con equipos redundantes los cuales permitan tener alta disponibilidad en los procesos.

3 **Absorber las perdidas:** Es decir asumir perdidas, A manera de ejemplo, en la empresa municipal existe la probabilidad de perdidas eléctricas de 10 veces anualmente en esa zona, lo que implicaría que uno de cada de 10 años la perdida de energía eléctrica puede afectar de manera muy negativa a sus equipos de

comunicación y obviamente la perdida de información. Es por situaciones como estas, es necesario un presupuesto destinado para futuros inconvenientes

4 **Transferir el riesgo:** Supongamos que la empresa municipal se ha gastado el presupuesto que tenía destinado para la inversión de tecnología en otras cosas de mayor prioridad y resulta que a dos de sus empleados les robaron sus laptops y entre otros activos de la empresa, podemos contratar un seguro de cobertura por robo.

6.6.7 Técnicas de la Administración de riesgos

La administración de riesgos hoy se puede considerar como un área especial y funcional de la organización, por lo cual a medida que transcurren los años se ha venido formalizando sus técnicas y principios de manera formidable teniendo un alto índice de importancia para minimizar los riesgos que se puedan generar. Se pueden destacar las siguientes técnicas:

No arriesgar mucho por poco: Esta técnica es razonable en relación entre el costo y el riesgo, hace saber cuándo los riesgos pueden sobrepasar los límites estimados de daño y cuando la pérdida es relativamente grande a los beneficios adquiridos por dicho bien o servicio.

Contemplar diferencias: Esa técnica sugiere la probabilidad de pérdida medible, le permite el poder decidir qué hacer sobe un riesgo en particular.

No arriesgar más de lo establecido: Es una de las técnicas más importantes que permite establecer las medidas de acción específicas, se pueden tomar el caso de una pérdida potencial de la infraestructura total y por lo general estas suelen ser devastadoras y fuera del alcance de la organización. En muy pocas ocasiones puede darse el caso que están tengan un menor impacto financiero.

6.6.8 Sistemas de registros de gestión de riesgos

En una empresa donde su nivel de transaccionalidad y ejecución de procesos es bastante grande hay que tomar en cuenta que la información dicha compañía es la materia prima de toda la lógica del negocio, es por ello que es imprescindible contar

con registros y estadísticas de todos los elementos involucrados con los sistemas de información tales como : (Grupo-epm)

- ✓ Cumplimiento de estándares nacionales e internacionales
- ✓ Alineación con auditoria basada en riesgos
- ✓ Administración centralizada de registros y control de riesgos
- ✓ Reportes de ofertas y seguros
- ✓ Administración centralizada por políticas y registros de seguridad
- ✓ Seguimiento y monitoreo
- ✓ Diseño de tablas estadísticas de valoración de riesgos

6.6.9 Análisis y evaluación del impacto del negocio

Una vez examinado el análisis de control de riesgos, se procede a determinar las actividades de misión crítica que permitan categorizar los procesos del negocio, de esta manera permitir la definición de las causas, efectos y las acciones pertinentes por el tipo de desastre ocurrido.

Tabla 6 - Evaluación del impacto del negocio

Evaluación del impacto del negocio				
Escenario de perdida	Causas	Efectos	Impacto %	Que hacer
Perdida de 2 discos duros del sistema de almacenamiento	Apagón eléctrico	Perdida de datos	Mayor 50%	Compra y remplazo de los discos afectados
…				

Elaborado por: Autor

Evaluar y tomar en consideración los siguientes planes de acción propuestos: (ISO)

1. Tener contemplado las pérdidas potenciales y tratar de minimizarlas.
2. Identificar controles para reducir o prevenir pérdidas potenciales.
   - ✓ Protección Física y lógica de activos.
   - ✓ Establecer la localización de los activos.

3. Evaluar y seleccionar la mejor medida adoptada para evitar pérdidas.
4. Valorar la garantía que ofrecen los controles y medidas para evitar pérdidas.
5. Examinar las actividades de recolección de datos.
6. Acudir a los registros e inventario de activos y procesos críticos del negocio.
7. Evaluar las causas y efectos de las interrupciones, daños e imprevistos.
8. Establecer y categorizar las funciones y registros críticos.
9. Definir los tiempos de reemplazo de los activos afectados.
10. Establecer escalas tiempos de recuperación y solicitud de recursos.

El objetivo de realizar el análisis de evaluación del impacto del negocio es para:

1. Determinar las áreas , funciones y procesos expuestos a interrupciones
2. Identificar las dependencias de los procesos
3. Analizar el impacto económico que causan las interrupciones
4. Analizar la carga operacional que causan las interrupciones
5. Estimar y contemplar los tiempos de inactividad
6. Graduar y medir el impacto del RTO y RPO
7. Establecer los recursos esenciales en la restauración de las operaciones
8. Medir y considerar los recursos que son críticos

6.4 DISEÑO

6.6.10 Análisis del Diseño del plan de recuperación

En esta etapa se analizara, determinará y definirán las alternativas de recuperación, políticas y preparación alternas del centro de datos de la empresa municipal, además se debe identificar las estrategias y medios de almacenamiento de respaldos optimas considerando la replicación de datos de un sitio alterno versus un servicio de recuperación de desastres basado en cloud.

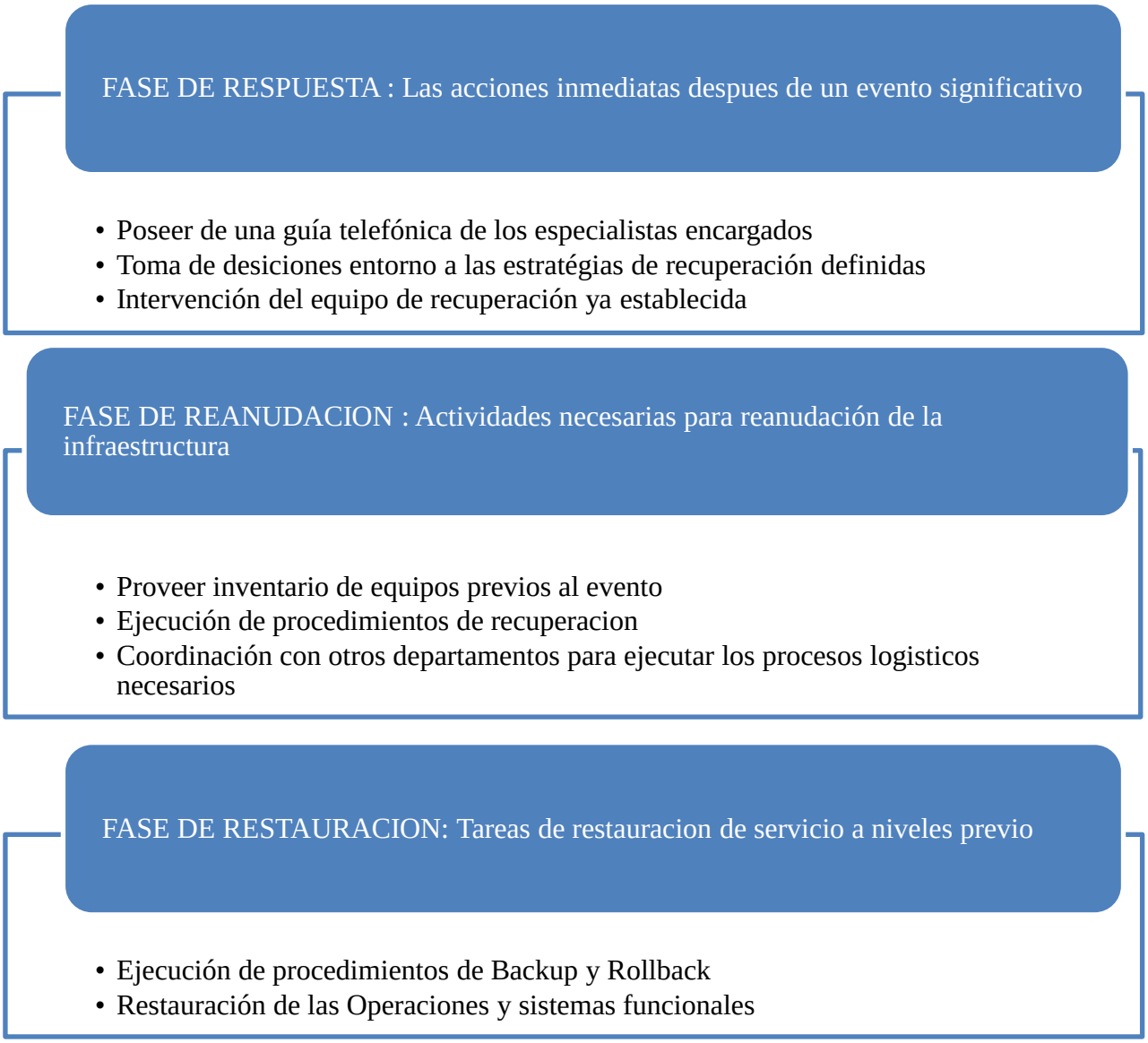
En esta fase se identificara y verificara el inventario de equipos físicos que se tienen actualmente en el sitio principal frente a los que se vayan a solicitar para el sitio alterno, con el objetivo de tener la replicación y datos actualizados.

Además establecer la definición de los procedimientos de recuperación teniendo en cuenta la calidad del servicio, la tolerancia a fallos y la alta disponibilidad.

6.6.11 Diseño de procedimientos de recuperación.

Se tiene como propósito realizar el análisis de diseño del proceso de recuperación de desastres (DRP) el mismo que consta de tres fases bien asentadas que son: La fase de respuesta, la reanudación y la restauración. Estas fases deben ser gestionadas de manera simultánea a los procedimientos de recuperación de la continuidad del negocio (BCP), correspondientes en el siguiente gráfico.

Ilustración 15 - Fases del proceso de una recuperación ante desastres



Elaborado por: Autor

6.6.12 Consideración de procedimientos de recuperación

Una vez que ya se tiene determinado el proceso o procedimientos de emergencia a seguir, es necesario determinar las respectivas consideraciones que se deben llevar acabo para la recuperación de las operaciones de un centro de datos:

Infraestructura:

- ✓ Adecuación y ambiente idóneo para edificar el sitio alterno
- ✓ Hardware solicitado para replicar los procesos servicios del sitio principal
- ✓ Software solicitado para replicar los procesos servicios del sitio principal
- ✓ Cableado solicitado para replicar los procesos servicios del sitio principal
- ✓ Sistema de Backup para la recuperación de la información

Estrategias de recuperación del Data Center:

- ✓ Procedimientos de recuperación manuales (No recomendable)
- ✓ Cold Sites (Aún no están listos para operar) / Hot Sites (Listo para operar inmediatamente) / Warm Sites (Listo para operar a pocas horas)
- ✓ Almacenamiento en la nube
- ✓ Mirror Sites (Sincronizado con el sitio principal – Listo para operar inmediatamente)
- ✓ Acuerdos empresariales recíprocos

Calidad de Servicio

- ✓ Alta disponibilidad (Equipamiento redundante)
- ✓ Tolerancia a fallos (Fuentes redundantes o aprovisionamiento eléctrico)
- ✓ Balanceo de Carga (Comparte carga de trabajo y mejora el desempeño)

6.6.13 Elaboración de Políticas del plan de recuperación de desastres

Se realiza con el objetivo de formalizar los objetivos y alcances que va a contener el plan, así como las responsabilidades, funciones y roles de los integrantes de cada equipo de trabajo (networking, infraestructura, sistemas eléctricos, Data & Backup, DBA), dirigido por el líder designado para la continuidad del negocio y el apoyo de la toma de decisiones de la gerencia general.

Adicionalmente se puede emitir un documento sencillo, claro y preciso en donde se exponen a nivel estratégico los objetivos y se establecen con exactitud los puntos claves aplicados en la elaboración del plan de recuperación.

Finalmente la persona o el equipo encargado en el proceso del plan de recuperación debe aplicar sus conocimientos y habilidades como Project Manager, para coordinar y programar fechas, presupuestos, plazos e indicadores de éxitos, con el fin de cumplir y satisfacer las políticas determinadas en el documento descrito anteriormente.

El equipo designado para el plan de recuperación debe cumplir fielmente las siguientes responsabilidades:

- ✓ Coordinar y programar plazos por cada fase del proyecto.
- ✓ Administrar el alcance, objetivos, estrategias, políticas y actividades críticas.
- ✓ Exponer el proceso a seguir a la alta gerencia y a departamentos vinculados con el plan.
- ✓ Determinar y delimitar el presupuesto para comenzar el proceso.
- ✓ Mantener controlado los aspectos críticos que surjan en el proyecto.
- ✓ Acogerse a recomendaciones idóneas y eficientes de los especialistas.

6.6.14 Escenarios de recuperación (sitio alterno vs recuperación por cloud)

La empresa municipal debe escoger el escenario que más se ajuste a su presupuesto y a su core de negocio, ellos han determinados dos posibles métodos o solución de recuperación entre ellas está la recuperación de desastres por sitio alterno y la otra es un servicio de recuperación por cloud, se pretende analizar y determinar los dos métodos exponiendo las ventajas y desventajas de cada uno de ellos.

Plan de recuperación tradicional (Sitio Alterno):

1 Bajo costo con referencia a servicios de cloud.
2 Inversión inicial elevada (Equipos, cableado, sistema eléctrico, implementación de servicios, etc…)
3 Tiempo de reanudación de las operaciones considerable y en algunos casos inmediatos.
4 Costos de mantenimiento del sitio alterno.

Plan de recuperación en la nube (Cloud):

1 Costo dependiendo de la capacidad de almacenamiento en la nube, modelo pago por uso.
2 Costos elevados con respecto al plan de recuperación tradicional.
3 Seguridad Gestionada.
4 Mantenimiento de especialistas en distintos ámbitos tecnológicos , servicio 24 x 7
5 Centros de proceso de datos con infraestructuras redundantes para ofrecer alta disponibilidad.
6 Fiabilidad y agilidad en la recuperación.

6.6.15 Evaluación del Diseño del plan de recuperación

Una vez que se ha analizado y considerado políticas, procedimientos, escenarios y estrategias del diseño para un plan de recuperación es necesario evaluar el mismo con el objetivo de escoger la mejor estrategia de recuperación para el diseño de un DRP.

- ✓ Identificar estrategias de reanudación y evaluación de daños
- ✓ Definir procedimientos de control de activos
- ✓ Elaboración de un esquema o bosquejo de las actividades
- ✓ Definir e identificar un formato de la estructura principal para su posterior replicación
- ✓ Definir estrategias para asegurar la protección de los datos
- ✓ Administración de procesos logísticos y estratégicos
- ✓ Establecer e identificar lugares aptos para la replicación y recuperación de los datos
- ✓ Responder ante la activación del desastre
- ✓ Identificar alternativas de recuperación
- ✓ Recuperación y reanudación de las operaciones sensibles

6.6.16 Evaluación del sitio alterno

La adopción de un sitio alterno es una de las estrategias más utilizadas y recomendadas por las empresas hoy en día, pero muchas veces dependen del índice económico que estas manejen. En el caso de tener un sitio alterno primeramente se debe evaluar la ubicación geográfica con respecto al sitio principal, luego evaluar las instalaciones físicas tales como (localidad, Cableado eléctrico, temperatura, dispositivos contra incendio, dispositivos de acceso, etc.…) y lo necesario que permita mantener el centro de datos seguro.

6.6.17 Evaluación del hardware y software

Los equipos físicos y la información son los implementos necesarios para cumplir con el objetivo de recuperación. Es por tal razón que hay que evaluar la infraestructura física actual en el centro de datos principal, evaluar la capacidad de almacenamiento actual y evaluar supuestos que permitan contener con toda esa carga de información y que obviamente se va a mantener en crecimiento constante. En cuanto al software se debe evaluar la compatibilidad de los sistemas operativos, sistemas de archivos (Filesystems), con las aplicaciones que son usadas internamente en la empresa municipal.

6.6.18 Evaluación de respaldos

Los respaldos o sistemas de respaldos deben descargar la información más reciente y actualizada sobre los equipos que van a servir de contingencia en un sitio alterno, influye mucho el hecho de adoptar y calendarizar estratégicamente políticas de respaldos y recuperación de los datos.

6.6.19 Evaluación de restauración de datos y procesos

Al realizar la restauración de los datos y procesos se deben considerar y verificar que se encuentren actualizados, para evitar pérdidas potenciales de información y evitar modificar la lógica del negocio.

6.6.20 Evaluación de sistemas de comunicación

Es de importancia contar con un enlace dedicado en los equipos de comunicación, si se adopta la estrategia de respaldos por sitio alterno ya que va hacer el medio por el cual se tenga replicada la información más reciente y evitar cuellos de botella y congestionamientos en la red administrativa.

COMPROBACIÓN Y VERIFICACIÓN

Con el objetivo de asegurar la eficacia y el funcionamiento del plan de recuperación, se debe evaluar el equipo y el personal que se encuentra encargado de cada una de las actividades críticas, realizando la demostración del funcionamiento de las aplicaciones, disponibilidad de servicios de red y fidelidad de los datos. Tomando como referencia el estándar ISO/IEC 24762:2008 y la documentación de buenas prácticas BS 25777:2008; de esta manera poder identificar los fallas y problemas para corregirlos con los estándares ya antes mencionados.

6.6.21 Descripción de pruebas

La descripción de pruebas ayuda a la coordinación y documentación de las actividades a realizar para hacer valida la evaluación de los resultados. Se puede crear escenarios de prueba que permita entender el correcto funcionamiento de los procesos del negocio, el apoyo de la alta gerencia y personal de TI juega un papel importante en el periodo de pruebas para dejar en constancia el estado en que se dejaran las aplicaciones una vez concluido el plan de recuperación y para dotar de recomendaciones para evitar problemas futuros.

6.6.22 Definir escenarios de pruebas

Es necesario tener identificado el ambiente de pruebas, la periodicidad con que estas se den y la elección de responsables para una mejor administración de plan de pruebas de recuperación, además es necesario incluir al equipo encargado del plan, equipo logístico en fin el personal de TI. Para asegurar la factibilidad del plan y adoptar medidas necesarios para poder mitigar problemas que se susciten en el periodo de recuperación.

6.6.23 Ejecución de las pruebas

Una vez que se analizó y planifico anteriormente los ambientes de pruebas, ahora se debe poner en marcha la etapa de ejecución, utilización de los resultados obtenidos anteriormente, las mejoras y adecuaciones más convenientes propuestas en el plan. Se debe controlar las fechas de ejecución, los resultados obtenidos y la selección de los responsables encargados de hacer dichas pruebas.

Al realizar dichas pruebas se puede tomar en cuenta las respectivas consideraciones:

- ✓ Verificar el grado de madurez del plan de continuidad y recuperación ante desastres.
- ✓ Gestionar y seleccionar las mejores estrategias de recuperación de información.
- ✓ Evaluar al personal y grupo de trabajo de la recuperación.
- ✓ Analizar y gestionar los procesos de misión crítica y viabilidad de las estrategias.
- ✓ Control y coordinación de las operaciones a nivel operacional y táctico.
- ✓ Definir escenarios y ambientes de pruebas de desastres
- ✓ Definir y coordinar tiempos para el mantenimiento de pruebas.
- ✓ Identificar fallas y determinar recomendaciones.
- ✓ Ensayar desarrollar simulacros anuales para comprobar el nivel factibilidad del plan.

FASE DE AUDITORÍA Y MANTENIMIENTO

Esta es la etapa final del plan de recuperación, es donde se llevan a cabo la estrategia de continuidad del negocio relacionadas con el plan de recuperación ante desastres, permitiendo identificar y sobre todo evaluar el buen uso de la norma y metodologías aplicada durante todo el desarrollo de las actividades.

6.6.24 Auditoria del plan de recuperación

Es donde se revisa la utilización de las buenas prácticas de la metodología y estándares propuestos, además se evalúa las técnicas, estrategias y recomendaciones definidas en el proceso del plan de recuperación y se gestiona la documentación de

los procesos del plan de acción, una vez aprobado la auditoria se pasa al siguiente nivel que es la definición de políticas de mantenimiento.

6.6.25 Definición de políticas de mantenimiento

La definición de políticas de mantenimiento se da por la necesidad de mejora del plan de recuperación y tiene su origen básicamente en las observaciones y recomendaciones detectadas en la auditoria, por lo que se realiza un listado que describa e indiquen las causas de su modificación, el detalle o descripción del elemento que fue expuesto al cambio, indicar fechas de modificación, personal involucrado en el proceso de modificación y actualización e incluir los resultados obtenidos para analizar si fue viable su modificación .

6.6.26 Ejecución de estrategias de mantenimiento

Para poner en ejecución el mantenimiento y actualización del plan, es necesario que se actualice y documente los cambios realizados con el fin de que se conozcan los detalles y motivos de las modificaciones logradas. Para poner en acción las estrategias de mantenimiento se debe examinar y considerar algunos aspectos:

- ✓ Planificar y mantenerse al tanto de las modificaciones a realizar.
- ✓ Verificar si los cambios van a afectar en algo el proceso del plan de recuperación actual.
- ✓ Aplicar estándares definidos por la auditoria.
- ✓ Establecer políticas, estrategias, prioridades y objetivos.
- ✓ Analizar el impacto de las modificaciones a realizar.
- ✓ Documentar y controlar las actividades y procedimientos realizados en proceso de modificación.

En este capítulo se realizó el análisis y la evaluación de las fases y procedimientos que debe cumplir un plan de recuperación.

En el siguiente capítulo se desarrollara el diseño de la metodología propuesta, usando como referencia la norma ISO/IEC 24762:2008 y la aplicación de buenas prácticas de recuperación con la norma BS 2777:2008; además se tomara en cuenta las estrategias y recomendaciones provistas en este capítulo con el fin de cumplir con los objetivos previstos.

6.7 PROPUESTA TÉCNICA

La propuesta técnica es el documento donde se va a poner en constancia los procesos operativos, los objetivos y alcances del proyecto de un plan ante desastres. En esta propuesta se pone en consideración los siguientes puntos:

A) Introducción

En los dos últimos años la empresa municipal ha venido experimentando diversos inconvenientes, entre estas fallas eléctricas, mal mantenimiento técnico y un mal uso de recursos, las mismas que han afectado en cierta parte su infraestructura tecnológica. Es por esta razón que la directiva organizacional ha tomado la decisión de contar con un plan recuperación ante desastres, que les permita restablecer rápidamente sus operaciones de misión crítica y evitar pérdidas significativas de sus datos.

B) Objetivos y Alcances del proyecto

El objetivo principal del proyecto es evitar la pérdida de información y la reanudación de sus procesos en cuestión de horas, el alcance de proyecto estará basado en el estándar ISO/IEC 24762 el mismo que ofrece la opción de adoptar un centro de datos alterno que les brinde la seguridad y confianza necesaria para mantener la continuidad del negocio.

C) Descripción del proyecto

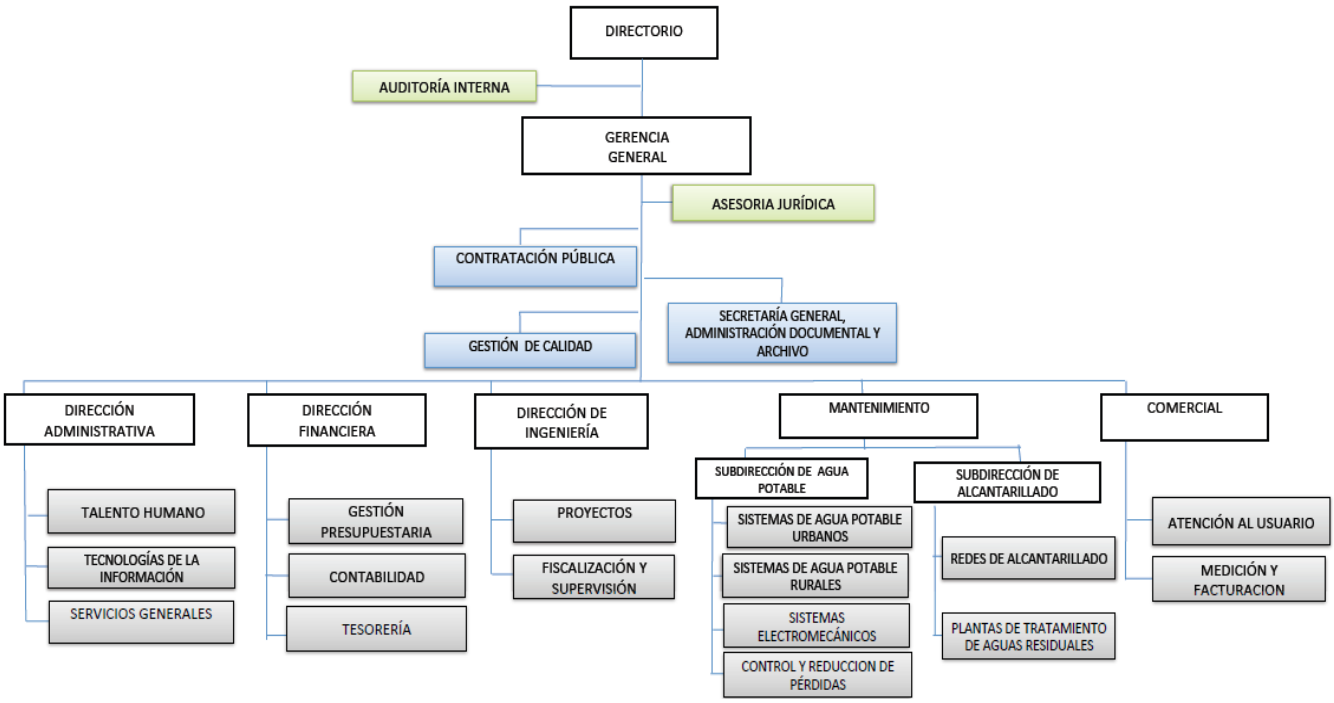
Basado en antecedentes previos, se pudo determinar que la infraestructura actual del centro de datos principal se encuentra virtualizado, para no alterar el modelo o metodología actual, se pretende realizar la instalación de un software o producto de la misma línea de virtualización conocido como VCenter Recovery Manager, este software le permite mantener sincronizada y replicada la información en ambos sitios y de esta manera minimizar el RTO y RPO que surgen al momento de enfrentar la recuperación de un centro de datos.

6.7.1 Desarrollo y diseño del plan de recuperación ante desastres

1. Conociendo el ambiente organizacional

Como primer paso debe realizar la identificación de la estructura organizacional de la empresa municipal, la misma ayudará a ubicar los departamentos a los que el datacenter proveerá de los servicios que se desean respaldar y de la misma manera conocer dónde y a quien se deberá entrevistar y pedir información para poder desarrollar el plan de recuperación.

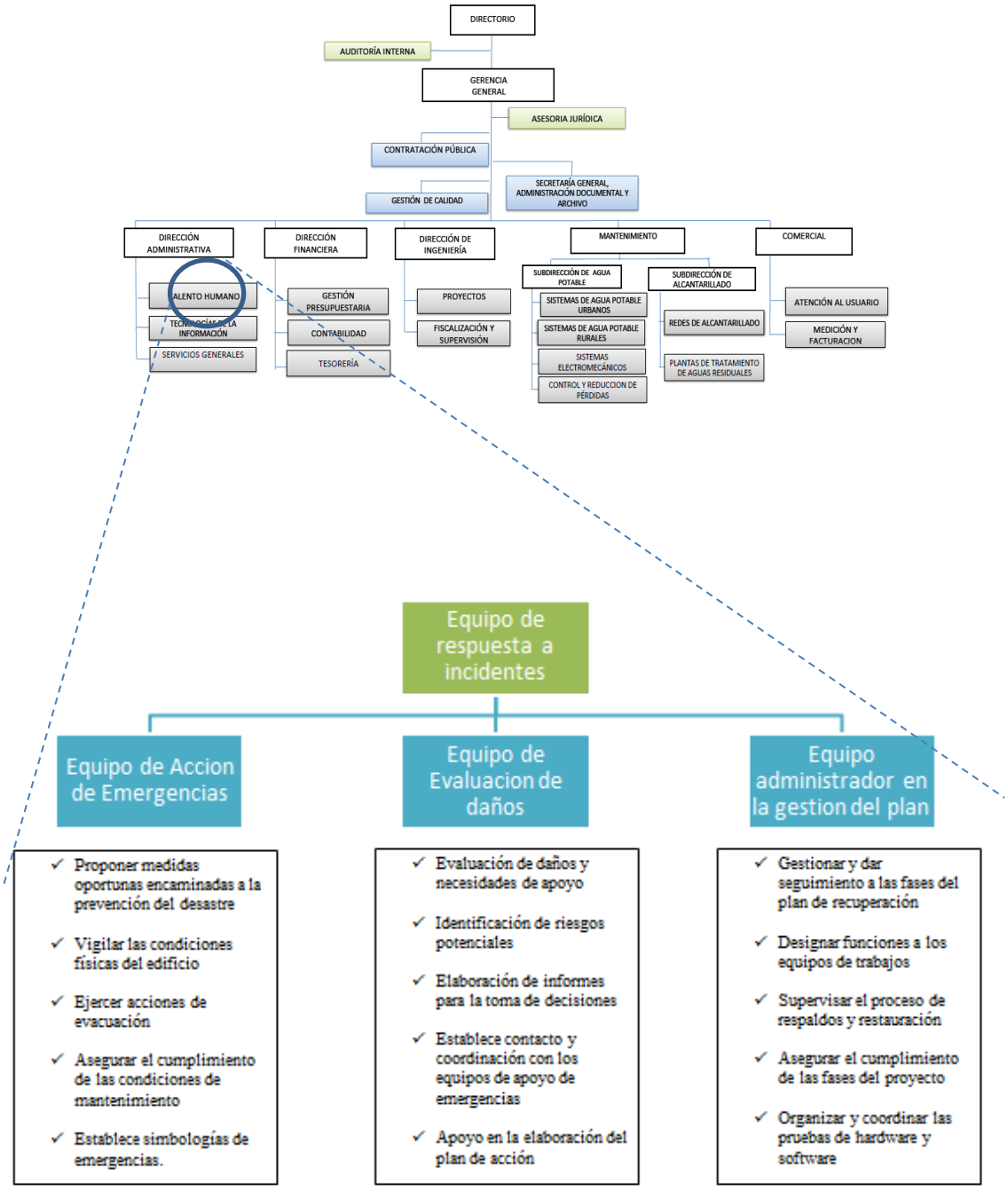
Ilustración 16 - Organigrama general de la empresa de objeto de estudio



Elaborado por: Autor

Una vez que se haya detectado el área principal en donde se va a desarrollar el plan de recuperación, deberá seleccionar un equipo lider que este al mando y le sirva de apoyo en las situaciones de emergencias y eventos que pongan en riesgo la informacion de la organización .

Ilustración 17 - Organigrama de las areas funcionales de Apoyo



Elaborado por: Autor

2. Definición de objetivos y alcance de incidentes

Se definen las funciones que cada equipo de acción debe cumplir para alcanzar los objetivos planteados.

Tabla 7 - Definición de objetivos de los equipos de emergencia

EQUIPO	OBJETIVOS	ALCANCE	AMBIENTE
Acción de Emergencias	Proporciona medidas oportunas encaminadas a la prevención del desastre	Acciones para tratar de minimizar el riesgo.	✓ Fallas Eléctricas ✓ Fallas ✓ Virus informáticos ✓ Fallas en instalaciones ✓ Fugas de gas ✓ Fallas en los equipos
Evaluación de Daños	Identifica los riesgos potenciales y establece contacto con los equipos de apoyo del plan de acción	Acciones para evaluar los daños de tipo operacional, financiera, recursos humanos y tecnología.	✓ Se determina después de haberse suscitado el desastre
Administración y gestión de emergencias	Brinda y ejecuta el seguimiento de las fases del plan de recuperación	Acciones destinadas ara las recuperaciones las operaciones críticas del negocio.	✓ Inundaciones ✓ Terremotos ✓ Incendios ✓ Tornados ✓ Erupciones volcánicas ✓ Huelgas ✓ Terrorismo ✓ Fallas en los equipos ✓ Fallas en los enlaces de comunicación

Elaborado por: Autor

3. Identificación de servicios y recursos críticos

En esta etapa se pretende listar los servicios y recursos críticos que se deben priorizar en el centro de datos determinados en la empresa municipal y a su vez definir los tiempos máximos de recuperación (RTO) para la reanudación de los servicios.Donde **EAE** – EQUIPO DE ACCION DE EMERGENCIAS ; **EED** - EQUIPO DE EVALUACION DE DAÑOS ;**EAGE** –EQUIPO ADMINISTRADOR Y GESTION DE EMERGENCIAS.

Tabla 8 - Identificación de servicios y recursos críticos

SERVICIOS	RECURSOS CRÍTICOS		
	Prioridad	Áreas de Apoyo	RTO
Sistemas telefónicos	Media	EAE	2 días
Redes locales	Alta	EAE - EED	2 días
Redes WAN	Muy alta	EAE - EED	2 días
Red Wireless	Media	EAE - EED	1 día
Internet	Alta	EAE	1 día
Infraestructura Física	Muy alta	EAE – EED - EAGE	1 semana
Correo Electrónico	Alta	EAE – EED	1 día
Hardware	Muy alta	EAE – EED	1 semana
Base de datos	Muy alta	EAE – EED - EAGE	3-4 días
Sistema Operativo	Media	EAE	2 días
Firewalls	Media	EAE	1 día
Sistemas Eléctricos	Muy alta	EAE – EED - EAGE	3-4 días
Sistemas de Backup	Muy alta	EAE – EED - EAGE	4 días
Servicios de Antivirus	Bajo	EAE	1 día

Elaborado por: Autor

4. Identificación, análisis y evaluación de la probabilidad de ocurrencia

En esta etapa se pretende identificar la probabilidad de ocurrencia de los posibles riesgos y el impacto potencial que ocasionaría en la empresa municipal.

Tabla 9 - Detección de amenazas, probabilidad y nivel de impacto

Categoría	Probabilidad de ocurrencia	Impacto
AMENAZAS TECNICAS		
1. Fallas sistemas eléctricos	85%	5
2. Fallas sistemas de respaldos	95%	5
3. Fallas sistemas de comunicación	75%	4
4. Fallas en las instalaciones	80%	4
5. Fallas de Hardware y Software	85%	5
6. Fallas en equipos	90%	4
AMENAZAS HUMANAS		
7. Huelgas	70%	2
8. Robo	60%	5
9. Terrorismo	50%	3
10. Ingeniería Social	85%	4
11. Accidentes	99%	5
AMENAZAS NATURALES		
12. Inundaciones	60%	5
13. Terremotos	85%	5
14. Incendios	90%	5
15. Rayos	70%	3
16. Erupciones Volcánicas	40%	2
17. Avalanchas	15%	3
18. Tornados	30%	3
19. Nevada	10%	2

Elaborado por: Autor

Tabla 10 - Matriz de evaluacion de los riesgos

Tabla de Matriz de Riesgo					
Probabilidad de Ocurrencia	Impacto Potencial				
	1	2	3	4	5
10%		19	17		
20%					
30%			18		
40%		16			
50%			9		
60%					8,12
70%		7	15	3	
80%				4,10	1,5,13
90%				6	2,14
100%					11
CATEGORIZACION DE LOS NIVELES DE RIESGOS					
Bajo	Medio	Alto	Muy alto	Caótico	

Elaborado por: Autor

Tabla 11 - Cuadro integral de la probabilidad de riesgo en la empresa municipal

Nivel de riesgo de la empresa municipal			
Valor	**Nivel**	**Riesgo**	**Descripción**
1	Bajo	17,19	Sin daños
2	Medio	9,16,18	Daños a baja escala, primeros auxilios, pérdidas económicas bajas
3	Alto	7,15	Se requiera atención ,perdidas económicas medias
4	Muy Alto	3,8,12	Daños evidentes, pérdida de producción, pérdidas económicas altas
5	Caótico	1,2,4,5,6,10,11,13,14	Inactividad completa, perdidas extremas

Elaborado por: Autor

5. Prevención y control de riesgos

En esta etapa se determina las estrategias a utilizar en los riesgos detectados anteriormente y encontrar la manera de prevenirlos.

Tabla 12 - Prevención y control de riesgos

Escenario de Riesgo	Consideraciones de control de riesgos
Desastres Naturales	✓ Contratación de Polizas de Seguros ✓ Brigadas de emergencias ✓ Detección de rutas de evacuación ✓ Aprovisionamiento de presupuestos anuales
Fallos de Hardware	✓ Reemplazo de equipos obsoletos ✓ Verificacion de tecnologia redundate ✓ Monitoreo de deteccion de fallas en servidores ✓ Mantenimiento correctivos y preventivos ✓ Analisis de ambiente y acondicionamiero fisico de la infraestructura
Fallos de Software	✓ Verificacion de compatibilidad entre tecnologias ✓ Detección de cambios en la configuración de las aplicaciones ✓ Determinar puntos de restauración y rollback
Interrupciones de Energia	✓ Disponibilidad de fuentes de energia redundantes ✓ Equipos de proteccion de corriente alterna ✓ Obtencion de lamparas de iluminacion para emergencias ✓ Considerar balanceo de carga energetico
Fallos en comunicaciones	✓ Requerir personal de soporte tecnico ✓ Mantenimiento preventivo y correctivo en equipos de comunicación
Fallos humanos	✓ Capacitaciones constantes del personal ✓ Contratación de especialistas para cada area ✓ Definición de funciones del personal
Fallos en respaldos	✓ Establecer politicas de resplados ✓ Coordinar y candelarizar tareas de respaldos

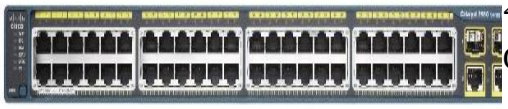
	✓ Mantenimiento y soporte de equipos de almacenamiento ✓ Configuración de aprovisionamiento de discos ✓ Documentación actualizada de procedimientos de respaldos
Incendios	✓ Contratación de Polizas de Seguros ✓ Contar con Brigadas de emergencias ✓ Evitar y mantener alejado material tóxico ✓ Contar con detectores de humos ✓ Botones de alertas y emergencias
Accesos no autorizados	✓ Administración y configuración de firewall ✓ Dispositivos de seguridad fisica (Biométricos) ✓ Detección y administración de puertos abiertos ✓ Administrar policas de acceso ✓ Control y manejo de bitácoras de registros

Elaborado por: Autor

6. Identificación de recursos de hardware actuales

Tabla 13 - Recursos actuales de Hardware

HARDWARE ACTUAL		
Recursos	**Detalles**	**Aplicación**
	6 x BL460c Blade , Discos SAS160GB C/U– 2Procesadores , 64 GB RAM	Active Directory Correo Web
	P2000 G3 – 12 Discos SAS de 600 GB C/U, 2 Procesadores 64GB RAM	Aplicaciones,SAP Sistemas AXIS (interno)

	P2000 G3 – 24 Discos SAS 300GB c/u ; 64 GB RAM , 2 procesadores	Documentos y registros de contratacion publica
	Store works – 25 Discos SAS de 600 GB c/u	Transacciones contables y facturacion electrónica
	Storage Works MSL2024	Respados con cintas LTO 4 y 5
	Cisco Pix 506 - Firewall	Proteccion perimetral Proteccion Interna y externa
	Switch HP JE006A – 24 Puertos y 4 Puertos Gbits	Conectividad con servidores y sistemas de almacenamiento
	2 x Switch cisco Catalyst 2960 – 48 puertos	Conectividad para usuarios
	4 x Cisco Aironet 1041N Wireless – Access Point	Conectividad inalámbrica
	Cisco 881 - Router	Conectividad WAN con ISP

Elaborado por: Autor

7. Identificación de Software actual

Tabla 14 - Recursos de Software actual

SOFTWARE ACTUAL	
Software	**Aplicación**
Sistemas Operativos	Windows 2008R2 – Active Directory – Sistema AXIS Centos 5 – Red Hat 4
Unidad de Respaldos	HP Data Protector
Web	CMS Joomla 3.x
Antivirus	ESET Endpoint Secure 5
SAP	ERP

Elaborado por: Autor

8. Análisis Costo / Beneficio para sitio alterno

Tabla 15 - Costo de Compra Hardware para sitio Alterno

COMPRA DE HARDWARE PARA SITIO ALTERNO				
Sitio	SERVIDORES - STORAGE			
	Equipos	Costo-Compra	Mantenimiento Anual	TOTAL
Alterno	3	$1570	$1250	$5960
Sucursales	0	0	0	
Sitio	CONFIGURACIONES DE ALMACENAMIENTO			
	Equipos	Costo-Compra	Mantenimiento Anual	TOTAL
Alterno	2	$1550	$3200	$6300
Sucursales	0	0	0	
Sitio	EQUIPAMIENTO ELECTRICO (UPS)			
	Equipos	Costo-Compra	Mantenimiento Anual	TOTAL
Alterno	1	$3550	$2500	$6050
Sucursales	0	0	0	
TOTAL :				$18310

Elaborado por: Autor

Tabla 16 – Arriendo de hardware para sitio alterno

ARRIENDO DE HARDWARE PARA SITIO ALTERNO				
Sitio	SERVIDORES - STORAGE			
	Equipos	Costo-Arriendo	Mantenimiento Anual	TOTAL
Alterno	3	$1050	$1250	$4400
Sucursales	0	0	0	
Sitio	CONFIGURACIONES DE ALMACENAMIENTO			
	Equipos	Costo-Arriendo	Mantenimiento Anual	TOTAL
Alterno	2	$1550	$2500	$5600
Sucursales	0	0	0	
Sitio	EQUIPAMIENTO ELECTRICO (UPS)			
	Equipos	Costo-Arriendo	Mantenimiento Anual	TOTAL
Alterno	1	$2500	$4000	$6500
Sucursales	0	0	0	
TOTAL :				16500

Elaborado por: Autor

Según el análisis de costos anterior muestra una pequeña diferencia entre la compra y arriendo de un sitio alterno del cual se determinó :

Qué es mucho mejor realizar la compra de los equipos que elegir la opción de arriendo ya que es más alto el costo de mantenimiento como servicio y los equipos aun así siguen siendo propiedad del arrendatario.

Los valores anteriormente citados son proformas que realizo la empresa municipal para determinar y escoger la opción más convenientes para la adquisición de un sitio alterno.

Los costos son un pocos elevados, pero se encuentran considerados la compra de los discos SAS y discos SSD (estado sólido) para la configuraciones de arreglo de disco del sistema de almacenamiento.

9. Preparación del centro de datos alterno

Una vez que se ha tomado en consideración todo lo necesario para adoptar un sitio alterno para que la empresa que es objeto de estudio pueda proteger su información y poder reanudar rápidamente sus actividades. Tomando en cuenta la garantía de funcionamiento ,alta disponibilidad y escalabilidad .

Debe estar previsto de las respectivas seguridades y cumplimiento de estándares en la creación de centro de datos.

Ilustración 18 - Sistemas de Suministro de Energía

Elaborado por: Autor

Ilustración 19 - Sistemas de Seguridad

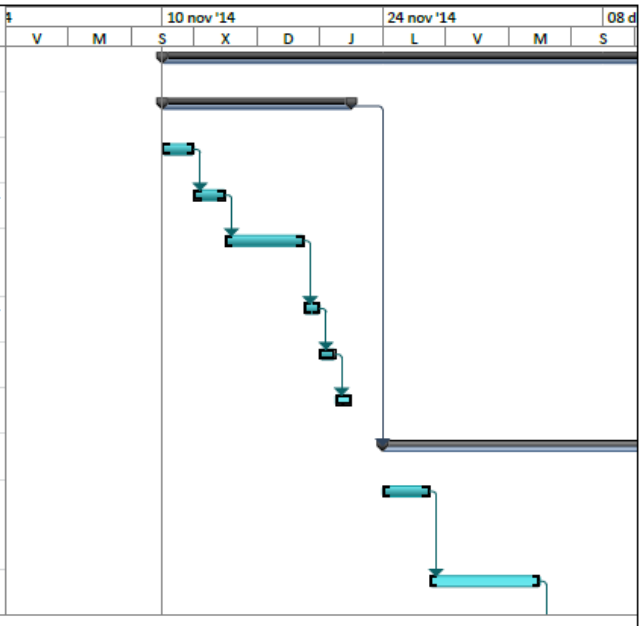
Elaborado por: Autor

6.8 PROPUESTA OPERATIVA

Se determina el tiempo de ejecución de cada una de las tareas a desarrollar en el plan de recuperación ante desastres.

Ilustración 20 – Tiempo de ejecución del proyecto A

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
1		Plan de Recuperacion ante Desastres	75 días	lun 10/11/14
2		Fase de Planificación	10 días	lun 10/11/14
3		Conocer el medio ambiente general	2 días	lun 10/11/14
4		Identificar la estructura organizacional	2 días	mié 12/11/14
5		Definir equipo de recuperacion y asignar responsabilidades	3 días	vie 14/11/14
6		Determinar la problemática	1 día	mié 19/11/14
7		Definir los objetivos y alcance del proyecto	1 día	jue 20/11/14
8		Aprobación del plan por parte de la alta gerencial	1 día	vie 21/11/14
9		Fase de Análisis y Evaluación	20 días	lun 24/11/14
10		Identificación y determinacion de procesos y servicios críticos	3 días	lun 24/11/14
11		Identificación de riesgos y vulnerabilidades	5 días	jue 27/11/14



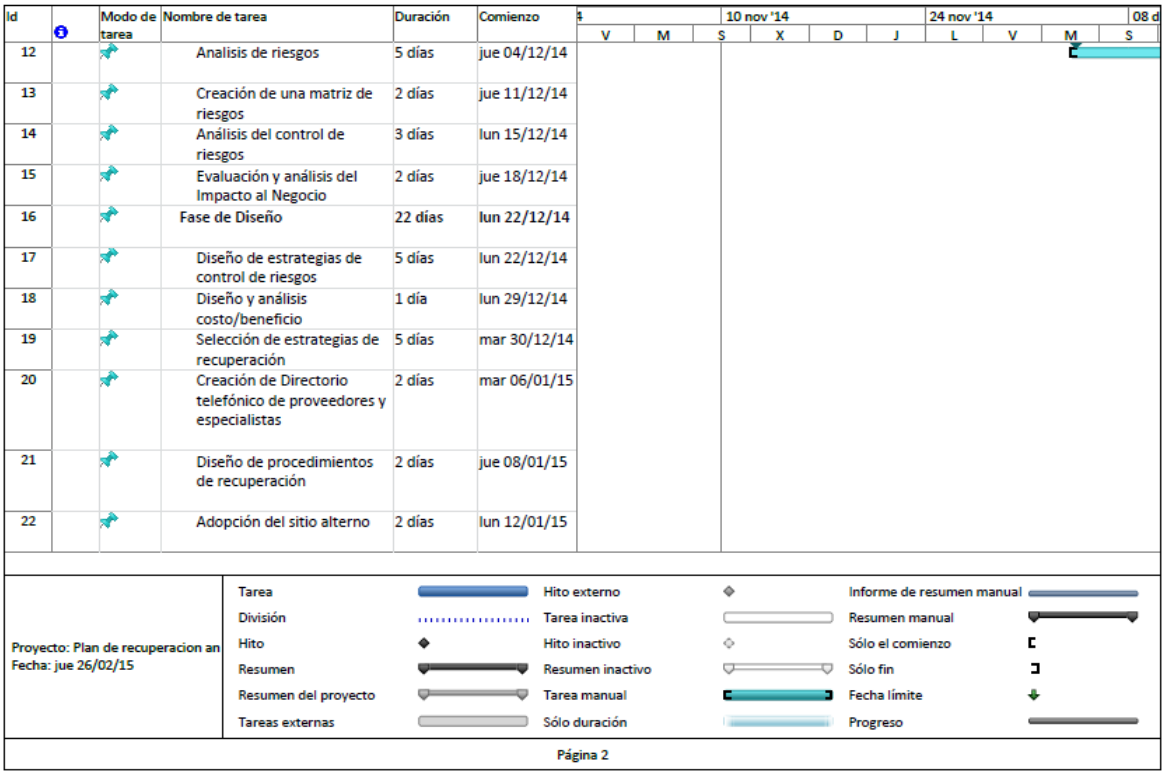
Proyecto: Plan de recuperacion an
Fecha: jue 26/02/15

Tarea · División · Hito · Resumen · Resumen del proyecto · Tareas externas
Hito externo · Tarea inactiva · Hito inactivo · Resumen inactivo · Tarea manual · Sólo duración
Informe de resumen manual · Resumen manual · Sólo el comienzo · Sólo fin · Fecha límite · Progreso

Página 1

Elaborado por: Autor

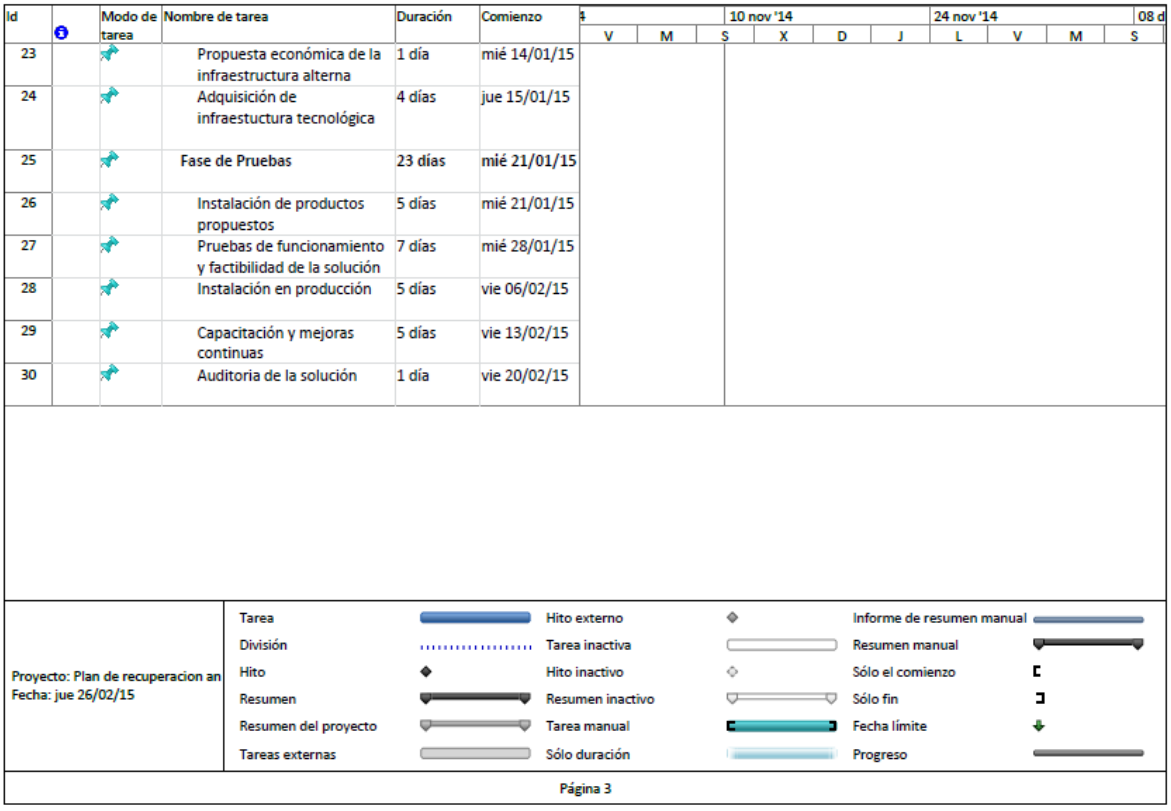
Ilustración 21 – Tiempo de ejecución del proyecto B



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
12		Analisis de riesgos	5 días	jue 04/12/14
13		Creación de una matriz de riesgos	2 días	jue 11/12/14
14		Análisis del control de riesgos	3 días	lun 15/12/14
15		Evaluación y análisis del Impacto al Negocio	2 días	jue 18/12/14
16		**Fase de Diseño**	**22 días**	**lun 22/12/14**
17		Diseño de estrategias de control de riesgos	5 días	lun 22/12/14
18		Diseño y análisis costo/beneficio	1 día	lun 29/12/14
19		Selección de estrategias de recuperación	5 días	mar 30/12/14
20		Creación de Directorio telefónico de proveedores y especialistas	2 días	mar 06/01/15
21		Diseño de procedimientos de recuperación	2 días	jue 08/01/15
22		Adopción del sitio alterno	2 días	lun 12/01/15

Elaborado por: Autor

Ilustración 22 – Tiempo de ejecución del proyecto C



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
23		Propuesta económica de la infraestructura alterna	1 día	mié 14/01/15
24		Adquisición de infraestuctura tecnológica	4 días	jue 15/01/15
25		**Fase de Pruebas**	**23 días**	**mié 21/01/15**
26		Instalación de productos propuestos	5 días	mié 21/01/15
27		Pruebas de funcionamiento y factibilidad de la solución	7 días	mié 28/01/15
28		Instalación en producción	5 días	vie 06/02/15
29		Capacitación y mejoras continuas	5 días	vie 13/02/15
30		Auditoria de la solución	1 día	vie 20/02/15

Elaborado por: Autor

6.9 PROPUESTA ECONÓMICA

Tomando en consideración los presupuestos que maneja anualmente la empresa, se determinó que la solución más eficiente y económica seria contar con servidores que cumplan con las mismas características de su sistema de almacenamiento, por lo general siempre se visualiza que el centro de datos alterno tiene que ser una copia del centro de datos principal, pero hay que considerar que lo importante no es poseer la misma infraestructura física , lo importante es que la infraestructura a implantar sea robusta y que tenga la capacidad necesaria de aguantar el nivel de procesamiento y almacenamiento que genera la empresa a diario. Es por este motivo que se recomienda la virtualización, la misma que es considerada por abaratar costos relacionados con el número de equipos físicos, minimización de tiempos de recuperación y recursos que influyen en un centro de datos.

Este es el listado de equipos propuestos para ofrecer la solución de recuperación ante desastres.

HP P2000 Modular Smart Array 3.5-in Drive Bay Chassis (LFF)	1	$1.718,57
HP P2000 G3 MSA Fibre Channel Controller	2	$4.357,14
HP P2000 Dual I/O LFF Drive Enclosure, twelve 3.5" drive bays	1	$3.548,57
HP P2000 600GB 6G SAS 15K rpm LFF Dual Port Enterprise Hard Drive	12	$5.965,71
HP P2000 2TB 6G SAS 7.2K LFF (3.5 inch) DP MDL HDD	12	$5.948,57
LC-LC Multi-Mode OM3 Fibre Channel Cable 2m	2	$428,57
HP 3 year 4 hour 24x7 MSA2000 G3 Arrays Proactive Care Service	1	$3.752,86
TOTAL:		$25.720,00

HP DL380p Gen8 E5-2650v2 25SFF US (2) Intel Xeon 8-CoreE5-2650 v2 (2.6GHz) / 20MB L3 cache / 32GB (2x16GB) PC3-14900R RDIMM /HP FlexFabric 10Gb 2-port 533FLR-T Adapter / HP Smart Array P420i/2GB FBWC (RAID 0/1/1+0/5/5+0/6/6+0) / 25 SFF SAS/SATA HDD bahias / No soporta DVD interno / (6) slots PCIe 3.0 / (2) 750W Fuentes de poder CS Platinum+ Hot Plug / (6) Ventiladores (N+1 redundancia) / Rack (2U) / 3 años en piezas, mano de obra, on site	1	$8.197,14
HP 16GB 2Rx4 PC3-14900R-13 Kit	8	$2.697,14
HP Ethernet 1Gb 4-port 331T Adapter	1	$280,00
HP Insight Control E-LTU	1	$538,57
HP 82E 8Gb 2-port PCIe Fibre Channel Host Bus Adapter	1	$2.142,86
HP 3y CTR DL38x(p) Foundation Care Service	1	$976,04
HP 300GB 6G SAS 10K 2.5in SC ENT HDD	2	$748,57
HP 12.7mm SATA DVD RW Jb Kit	1	$98,57
TOTAL :		$15.678,90

HP A5120-24G 24 puertos 10/100/1000 + 4 puertos duales Giga o SFP+Módulo de expansión para 2 puertos +1 RJ45 consola	2	$2.934,29
HP 3y 24x7 HP 51xx Swt products FC SVC	2	$1.840,00
TOTAL:		$4.774,29

VMware vSphere 5 Essentials Plus Kit for 3 hosts (Max 2 processors per host)	1	$6.144,91
Production Support/Subscription VMware vSphere 5 Essentials Plus Kit for 3 years	1	$4.563,60
TOTAL:		$10.708,51

VMware vCenter Site Recovery Manager 5 Standard (25 VM Pack)	1	$6.664,39
Production Support/Subscription for VMware vCenter Site Recovery Manager 5 Standard (25 VM Pack) for 3 years	1	$4.949,32
TOTAL:		$11.613,70

Servicios	1	$14.285,71
TOTAL:		$14.285,71

Rack y PDU	1	$3.571,43
Memorias	10	$6.428,57
Discos P2000 600GB 6G SAS 10K 2.5in DP ENT HDD	9	$4.975,71
Acometida eléctrica	1	$2.857,14
TOTAL:		$2.857,14

UTM	1	$5.714,29
TOTAL:		$5.714,29

TOTAL DEL PROYECTO: $106.327,76

6.10 ADMINISTRACIÓN

La administración del proyecto va a quedar al mando del grupo o el individuo que haya designado para la recuperación de las operaciones. Esta persona o grupo responsable del plan debe coordinar cada una de las actividades con los encargados de cada área con el objetivo en común de restaurar los procesos y servicios desde el sitio alterno hasta que se recupere o se estabilice la situación en el sitio principal.

La gerencia juega un papel importante, en el apoyo y la aprobación de la toma de decisiones y estrategias definidas previamente contempladas en el plan de recuperación.

BIBLIOGRAFÍA

Acronis. (2014). *www.acronis.com*. Obtenido de http://www.acronis.com/es-mx/resource/solutions/backup/2005/incremental-backups.html

Arend, C. (Enero de 2008). *ASTIC*. Obtenido de Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas: http://www.astic.es/sites/default/files/IDCBullStorage.pdf

BSCCONSULTORES. (febrero de 2010). *BSCCONSULTORES*. Obtenido de http://www.bscconsultores.cl/descargas/D.5%20%20Continuidad%20del%20Negocio%20y%20%20recuperacin%20de%20desastres%20ISACA.pdf

CIIFEN. (s.f.). *Ciifen*. Obtenido de http://www.ciifen.org/index.php?option=com_content&view=category&id=84&layout=blog&Itemid=111&lang=es

Crump, G. (22 de enero de 2014). *Storage Wiss*. Obtenido de http://storageswiss.com/2014/01/22/backup-basics-what-do-slo-rpo-rto-vro-and-gro-mean/

EMC2. (s.f.). *EMC2*. Obtenido de http://mexico.emc.com/corporate/glossary/disaster-recovery.htm

FeedBack-Networks. (2013). *FeedBack-Networks*. Obtenido de http://www.feedbacknetworks.com/cas/experiencia/sol-preguntar-calcular.html

Freitas, V. D. (Abril de 2009). *scielo*. Obtenido de http://www.scielo.org.ve/scielo.php?pid=S1690-75152009000100004&script=sci_arttext

Granada, L. F. (Octubre de 2012). *Universidad Militar Nueva Granada.* Obtenido de http://repository.unimilitar.edu.co/bitstream/10654/10790/1/TRABAJO%20DE%20GRADO%20ESPECIALIZACION%20EN%20ALTA%20GENERENCIA%20UMNG.pdf

Grupo-epm. (s.f.). *OSE*. Obtenido de http://www.ose.com.uy/descargas/pfe/taller_gestion_de_riesgos/grupo_epm_sistema_gestion_integral_riesgos.pdf

HP. (Marzo de 2011). *hp*. Obtenido de http://hp.com/support/manuals

HP. (2015). *shopping1.hp.com*. Obtenido de http://shopping1.hp.com/is-bin/INTERSHOP.enfinity/WFS/WW-USSMBPublicStore-Site/en_US/-/USD/ViewApplication-DisplayCachedWelcomePage

Ibarra, J. A. (2008). *CCISA*. Obtenido de Consultoría en Comunicaciones e Informática: http://www.ccisa.com.mx/InfoCCISA/Archivo/PlanesdeContingenciaLatinCACS2004.pdf

INTECO. (20 de Noviembre de 2007). *INTECO*. Obtenido de www.incibe.es: https://www.incibe.es/file/t2sHW92KsAV506ZWcHTKRg

ISO. (s.f.). *www.iso.org*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:24762:ed-1:v1:en

J., H. C., & K., B. Z. (2000). *A Primer for Disaster Recovery Planning in an IT Environment.* London: Idea Group Publishing.

Jenny Caicedo. (19 de Octubre de 2012). *Oocities*. Obtenido de http://www.oocities.org/es/jjcaicedop1/ges/Trabajo2/Cambio_T2.htm

Jiménez, M. P. (2014). *Diccionario de administración y finanzas.* EE.UU.: Palibrio LLC.

Mendoza, M. Á. (6 de Noviembre de 2014). *Welivesecurity*. Obtenido de http://www.welivesecurity.com/la-es/2014/11/06/business-impact-analysis-bia/

RED HAT. (s.f.). *Red Hat*. Obtenido de https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/s2-disaster-recovery-sites.html

Serrano, E. R. (11 de abril de 2005). *www.aporrea.org.* Obtenido de http://www.aporrea.org/actualidad/a13255.html

Softland. (2012, Agosto 7). *www.backup4all.com*. Retrieved from http://www.backup4all.com/kb/backup-types-115.html

Tittel, K. L. (14 de Noviembre de 2013). *CIO*. Obtenido de http://www.cio.com/article/2381021/best-practices/how-to-create-an-effective-business-continuity-plan.html

Vigo Jaccottet, C. A. (Marzo de 2010). *Facultad de Ciencias Economicas y de Administacion de Uruguay.* Obtenido de http://www.ccee.edu.uy/bibliote/monografias/2010/M-CD4039.pdf

vmware. (n.d.). *book.itep.ru*. Retrieved from http://book.itep.ru/depository/recovery/eBook_A_Guide_to_Moderin_IT_Disaster_Recovery.pdf

Webber, M. W. (2004). *The Disaster Recovery Handbook.* United States of America: AMACOM.

Westen, C. V. (2010). *itc*. Obtenido de International Institute for Geo - information Science and earth: http://www.itc.nl/external/unesco-rapca/Presentaciones%20Powerpoint/10%20Sensores%20Remotos%20para%20Manejo%20de%20Desastres/Sensores%20Remotos%20para%20Manejo%20de%20Desastres.pdf

ANEXOS

ANEXO 1 - Plantilla para la recuperación de equipos de información

SISTEMA	Sistema SAP - EMASAPSERVER

RESUMEN	Sistema de aplicación SAP
SERVIDOR EN PRODUCCION	Ubicación: Centro de datos Modelo de servidor: P2000 G3 Sistema operativo: Windows Server 2003 CPU: 2 – XEON Memoria: 64 GB Disco total: 600 TB Identificador del sistema: Sistema SAP DNS Principal: 192.20.9.10 DNS Secundario:192.20.9.10 Dirección IP: 192.20.10.250
SERVIDOR DEL SITIO	EMASAPSERVER
APLICACIONES	Servidor de Aplicaciones , SAP
SERVIDORES ASOCIADOS	Servidores DNS , ORACLE

CONTACTOS CLAVE	
Proveedor de hardware	Ing. Helio Terán
Dueños del sistema	Propiedad de la empresa pública
Propietario de la base de datos	Ing. Roberto Cabrea
Propietarios de aplicaciones	Ing. Ismael Ruiz
Proveedores de software	Ing. Joselyn García
Almacenamiento fuera del sitio	Ing. Michael Garcés
Servicios de red	Ing. Joe Benítez

SISTEMA DE PROCEDIMIENTO DE DRP	**DETALLES**
ESCENARIO 1 Pérdida de la red	----------
ESCENARIO 2 Pérdida de Hardware	Pérdida de un Disco en Raid 0+1 Reemplazar el disco en Spare

ADDENDUM

CONTACTOS	N° TELEFONO
Ing. Roberto Cabrea	09-85544028
Ing. Ismael Ruiz	09-53176312
Ing. Joe Benítez	09-89521445
Ing. Joselyn García	09-43512498

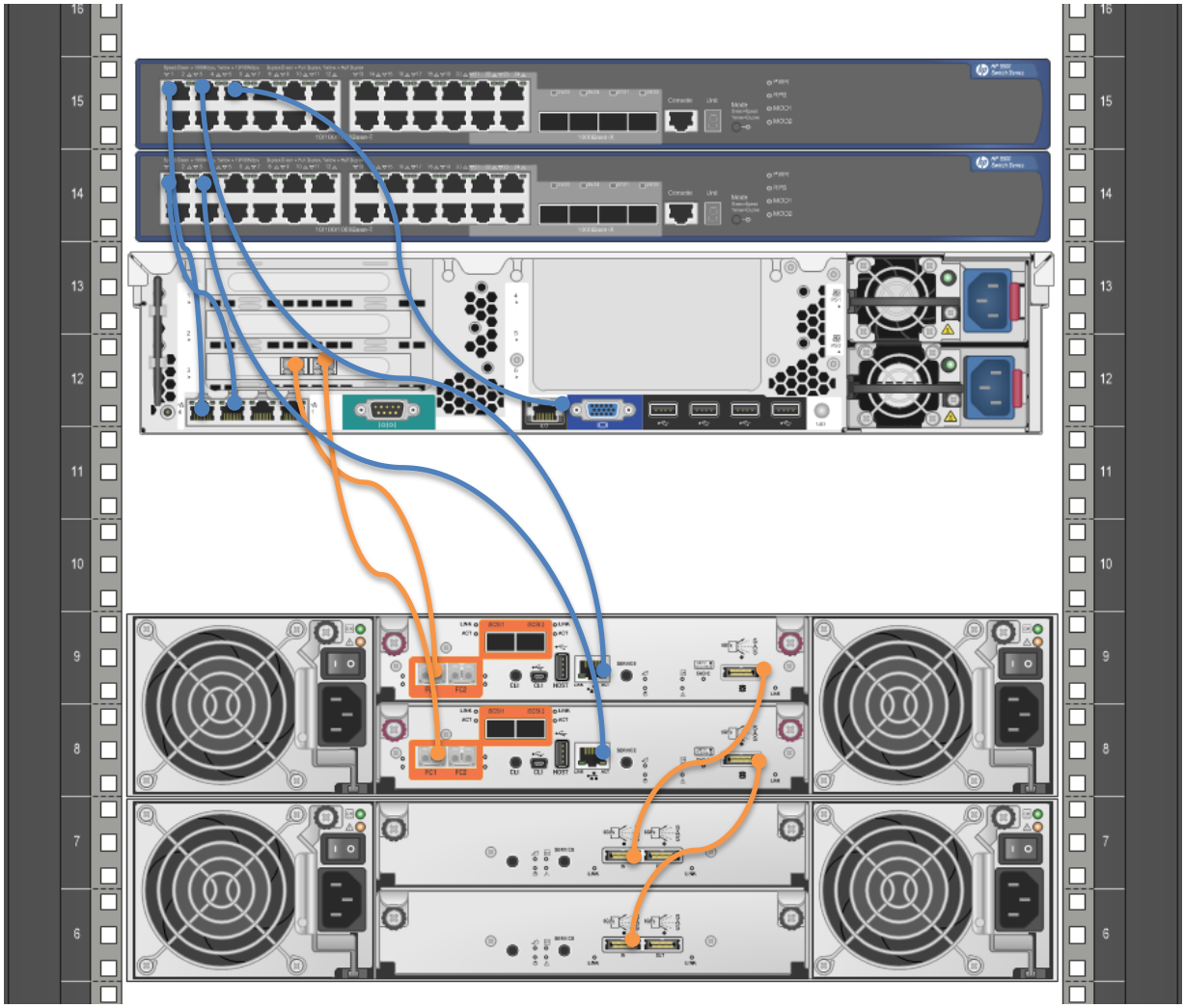
FILE SYSTEMS [10/Marzo/2015]

Sistema de archivos Filesystems mínimo para crear y restaurar desde una copia de: [1 Filesystems]	Filesystems : PRODUCCION kbytes Habilitados : 134895276 kb usados: 55 % Utiliza montado en: EMASAPSERVER
Otros archivos críticos para modificar	----------
Directorios necesarios para crear	/mnt/db/release ; /etc/sys/status/
Para restaurar los archivos críticos	----------
Archivos secundarios para restaurar	----------
Otros archivos para restaurar	----------

SISTEMA DE APOYO	DETALLES
Activos críticos de la red	Switch Core
Interfaces críticas	Eth0 ; FC 0 ; FC 1 ; ILO
Para restaurar los archivos críticos	----------
Servicios críticos de la red para restaurar	DNS, HTTP, PROXY SQUID
Otros servicios	EMAIL

ANEXO 2 - Conexiones Física del Sitio Alterno – VCenter Site Recovery Manager

Ilustración 23 – Conexiones físicas del rack en el sitio alterno



Elaborado por: Autor

ANEXO 3 - Encuestas previo al diseño del plan de recuperación ante desastres

ENCUESTA DE ANALISIS PARA UN PLAN DE RECUPERACION ANTE DESASTRES

1. ¿ Que método de respaldos es utilizado actualmente en la empresa municipal?

- ☐ Backup por cintas
- ☐ Backup por mirroring de discos
- ☐ Backup en medios extraíbles
- ☐ Backup en la nube

2.¿Con cuanta frecuencia se realizan los respaldos en la empresa?

- ○ Diario
- ○ Semanal
- ○ Quincenal
- ○ Mensual

3.¿De que manera se administran los respaldos y restauración de los datos?

- ☐ Full Backup
- ☐ Incremental
- ☐ Diferencial
- ☐ Desconosco

4.¿Conoce usted los riesgos a los que se enfrenta actualmente la empresa?

- ○ Apagones eléctricos
- ○ Infraestructura antigua
- ○ Virus
- ○ Insuficiente métodos de respaldos

5.¿Conoce si la empresa posee un presupuesto destinado para restauración de la infraestructura en el caso de suscitarse el siniestro?

- ○ Si
- ○ No
- ○ Desconosco

6.¿Cuál de las siguientes opciones, piensa usted que es una forma estratégica de mantener almacenada de la información?

- ○ Sitio alterno
- ○ Sitio Arrendado
- ○ Servicios en la nube
- ○ Otros

7.¿Cuál es el tiempo prudencial que considera la empresa para restablecer sus operaciones?

- ○ Menor a 12 dias
- ○ Mayor a 12 horas
- ○ Mayor a 1 dia
- ○ Mayor a 1 semana

8.¿Qué grado de importancia tiene la obtención de un plan de recuperación?

- ○ Muy Significativo
- ○ Significativo
- ○ Considerable
- ○ Sin importancia

9.¿A escuchado de este tipo de herramientas de backup de información que sirven como técnicas útiles a nivel empresarial?

- ○ a. Symantec –NetBackup
- ○ b. HP Data Protector
- ○ c. IBM Tivoli Storage Flas Copy Manager
- ○ d. EMC NetWorker
- ○ e. vMware Site Recovery Manager

10.¿La empresa está preparada para afrontar las diversos situaciones de desastres tales como?

- ○ Inundaciones
- ○ Incendios
- ○ Terremotos
- ○ Incendios
- ○ Ninguno de los anteriores

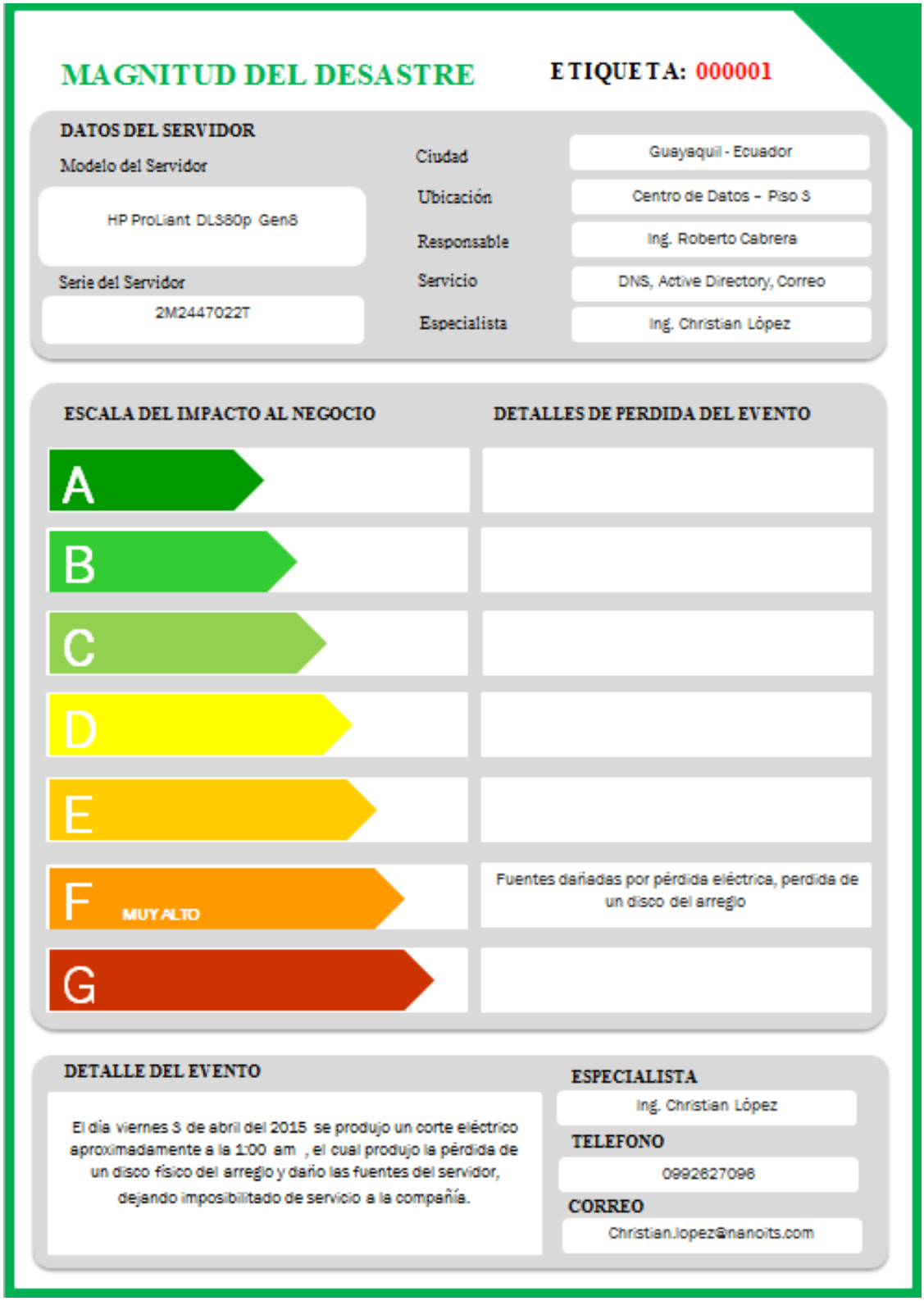
11.¿Que tan beneficioso considera el adoptar un plan de recuperación ante desastres?

	1	2	3	4	5	
Irrelevante	○	○	○	○	○	Muy Indispensable

12.¿Según los antecedentes en la empresa ,con cuanta urgencia considera el desarrollo de el plan ante desastres?

	1	2	3	4	5	
Baja	○	○	○	○	○	Alta

ANEXO 4 - Evaluación de pérdidas ante desastres



MAGNITUD DEL DESASTRE

ETIQUETA: 000001

DATOS DEL SERVIDOR

Modelo del Servidor: HP ProLiant DL380p Gen8

Serie del Servidor: 2M2447022T

Ciudad: Guayaquil - Ecuador

Ubicación: Centro de Datos – Piso 3

Responsable: Ing. Roberto Cabrera

Servicio: DNS, Active Directory, Correo

Especialista: Ing. Christian López

ESCALA DEL IMPACTO AL NEGOCIO	DETALLES DE PERDIDA DEL EVENTO
A	
B	
C	
D	
E	
F MUY ALTO	Fuentes dañadas por pérdida eléctrica, perdida de un disco del arreglo
G	

DETALLE DEL EVENTO

El día viernes 3 de abril del 2015 se produjo un corte eléctrico aproximadamente a la 1:00 am , el cual produjo la pérdida de un disco físico del arreglo y daño las fuentes del servidor, dejando imposibilitado de servicio a la compañía.

ESPECIALISTA

Ing. Christian López

TELEFONO

0992627096

CORREO

Christian.lopez@nanoits.com

ANEXO 5 - Instalación de la infraestructura Virtual

INSTALACIÓN DE VMWARE VCENTER – VSPHERE REPLICATION

1.1 Requisitos mínimos de hardware

Tabla 17 – Requisitos mínimo de hardware

Hardware	Requisitos
Procesador	Procesador Intel o AMD x86 con dos o más núcleos lógicos, cada uno con una velocidad de por lo menos 2 GHz. El procesador Intel Itanium (IA64) no es compatible. Es posible que los requisitos para el procesador sean mayores si la base de datos se ejecuta en la misma máquina.
Memoria	4 GB de RAM. Los requisitos de RAM pueden ser mayores si su base de datos se ejecuta en la misma máquina. VMWare Virtual Center Management Web Services requiere entre 512 Mb y 4.4 GB de memoria adicional. La memoria máxima de Web Services JVM puede especificarse durante la instalación, según el tamaño del inventario.
Almacenamiento en disco	4 GB. Los requisitos del disco pueden ser superiores si vCenter Server database se ejecuta en la misma máquina. En vCenter Server 5.0, el tamaño predeterminado para registros vCenter Server es 450 MB, superior al de vCenter Server 4.x. Asegúrese de que el espacio del disco asignado a la carpeta de registros sea suficiente para este aumento.
Requisitos de disco de Microsoft SQL Server 2008 R2 Express	Se necesitan más de 2 GB de espacio libre en el disco para descomprimir el archivo de instalación. Aproximadamente 1.5 GB de estos archivos se eliminan una vez que se completa la instalación.
Conexiones de red	Se recomienda una conexión de 1 Gbit.

Fuente: **(vmware, 2014)**

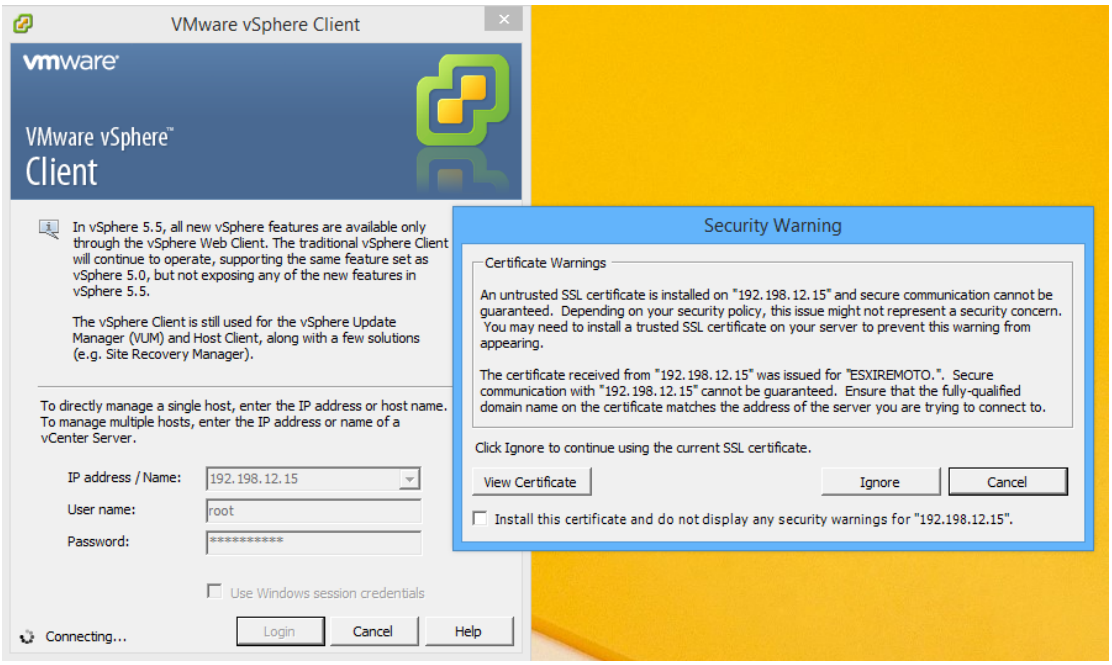
1.2 Requisitos del Sistema Operativo

VCenter Server 5.0 requiere un sistema operativo de 64 bits y no puede ser instalado en un sistema operativo de 32 bits. Al realizar la instalación, debe asegurarse de que su sistema operativo tenga 64 bits de capacidad. Para obtener más información, consulte *Operating System Compatibility for vSphere Client, vCenter Server, and VMware vCenter Update Manager* en vSphere Compatibility Matrixes.
Estos sistemas operativos son admitidos por:

- Microsoft Windows Server 2003 Standard, Enterprise o Datacenter SP2 64bit
- Microsoft Windows Server 2003 Standard, Enterprise o Datacenter R2 64bit
- Microsoft Windows Server 2008 Standard, Enterprise o Datacenter SP2 64bit
- Microsoft Windows Server 2008 Standard, Enterprise o Datacenter R2 SP1 64bit
- Microsoft Windows Server 2008 Standard, Enterprise o Datacenter R2 64bit
- Microsoft Windows Server 2008 Standard, Enterprise o Datacenter SP1 64bit

1.3 Configuraciones de red

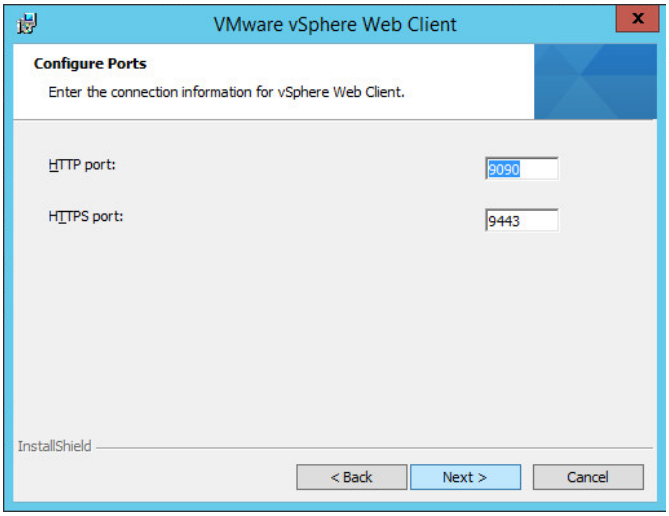
DESCRIPCIÓN	IPV4	GATEWAY	NETWORK MASK	DNS
ESXI 5.5 Remoto	**192.198.12.15**	**192.198.12.252**	**255.255.255.0**	**192.198.12.21**
Vsphere VCenter 5.5	**192.198.12.16**	**192.198.12.252**	**255.255.255.0**	**192.198.12.21**
ESXI 5.5 Principal	**192.198.12.4**	**192.198.12.252**	**255.255.255.0**	**192.198.12.21**
vSphere Replication	**192.198.12.0**	**192.198.12.252**	**255.255.255.0**	**192.198.12.21**
OVF Template	**192.198.12.242**	**192.198.12.252**	**255.255.255.0**	**192.198.12.21**

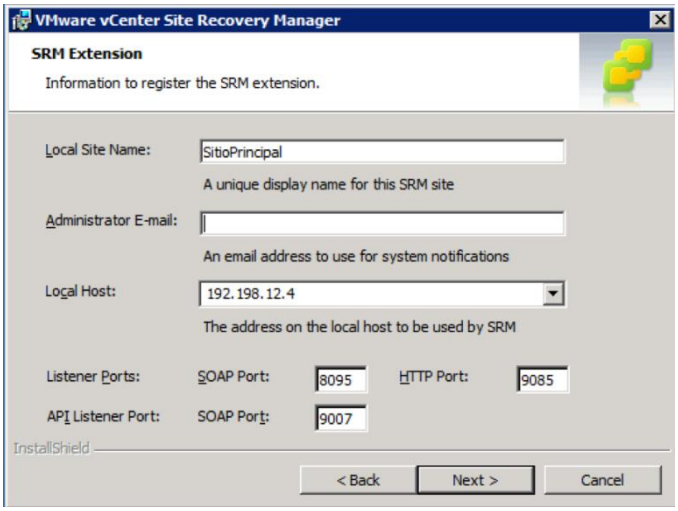


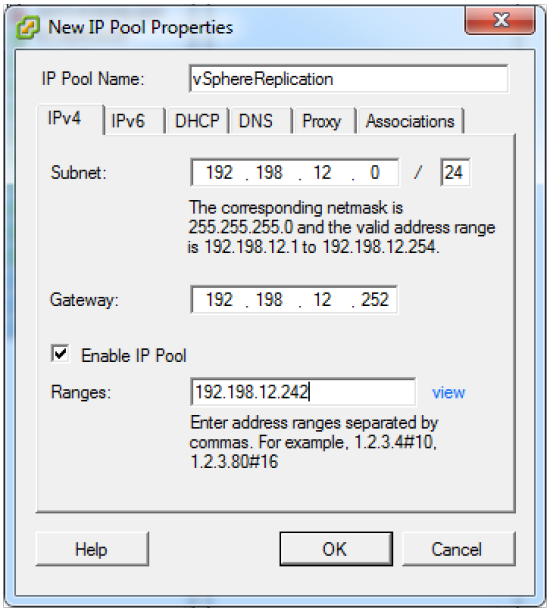
SOAP Port: 8095 – 9007

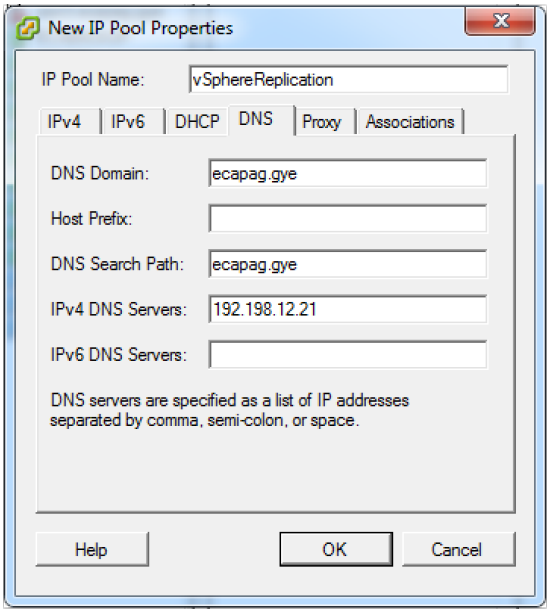
HTTP Port: 9085 - 9090

HTTPS VCenter Port: 9443









ANEXO 6 – Certificado de Participación en el Proyecto

EMAPAG-EP
ENTE MUNICIPAL DE REGULACIÓN Y CONTROL

Guayaquil, 10 de abril de 2015

CERTIFICADO

Certifico que el proyecto para la elaboración de un plan de recuperación ante desastres (DRP), cuya finalidad consiste en replicar la información hacia un sitio alterno para mantener activos los servicios y evitar la pérdida de datos en la Empresa Municipal de Agua Potable y Alcantarillado de Guayaquil (EMAPAG EP) el mismo que se encuentra en funcionamiento, fue diseñado e implementado como tema de tesis por el Sr. BYRON VICENTE NIETO MUÑOZ,

Atentamente,

Ing. Roberto Cabrera A.
Jefe de Tecnologías de la información

Av. Francisco de Orellana s/n y Miguel H. Alcívar, Mezzanine, Centro Empresarial Las Cámaras
PBX: (593-4) 2681315 • Fax: (593-4) 2682225 • www.emapag-ep.gob.ec