Definición de un modelo para la implementación de planes de continuidad de TI que asegure la continuidad de los sistemas informáticos en las empresas

PRESENTADO PARA CUMPLIR CON LOS REQUISITOS FINALES PARA LA OBTENCIÓN DEL TITULO DE ADMINISTRADOR DE SISTEMAS INFORMÁTICOS

ESTUDIANTE

DANILO RAFAEL MARTÍNEZ BAQUERO

CÓDIGO: 602027001

DOCENTE:

MARIO CONTRERAS

UNIVERSIDAD SANTO TOMÁS

VICERRECTORÍA DE UNIVERSIDAD ABIERTA Y A DISTANCIA

ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS

BOGOTÁ, JUNIO 1 DE 2016

TABLA DE CONTENIDO

Índice de Tablas 3
Índice de Gráficas 4
1. INTRODUCCIÓN 7
2. UNIDAD 1 – DATOS GENERALES DEL PROYECTO 9
2.1. Titulo descriptivo del proyecto 9
2.2. El problema del proyecto 9
2.3. Objetivos 20
2.4. Justificación 21
2.5. Alcances y Delimitaciones 27
3. UNIDAD 2 – MARCO DE REFERENCIA 29
3.1. Antecedentes 29
3.2. Marco Teórico 31
3.3. Marco Conceptual 34
3.4. Marco metodológico 36
3.5. Cronograma de Actividades 39
4. UNIDAD 3 – DESARROLLO DEL PROYECTO 41
4.1. Análisis y Propuesta de Tecnologías y Productos – Análisis Sistémico 41
4.1.1 Antecedentes Técnicos 45
4.1.2 Ventajas del modelo 46
4.1.3 Estructura 46
4.1.4 Características 46
4.1.5 Proceso de Implementación 47
4.1.6 Funcionalidad 51
4.1.7 Impacto tecnológico 53
4.1.8 Impacto educativo 55
4.1.9 Impacto económico 55
4.2. Análisis Tecnológico 57
4.3. Análisis Financiero 61
4.4. Análisis Administrativo 68
5. CONCLUSIONES 72
6. ANEXOS 73

6.1. Contexto Histórico Social 73
6.1.1 Impacto social..... 76
6.1.2 Listado Equipamiento para sitio alterno 78
7. BIBLIOGRAFIA..... 81

Índice de Tablas

Tabla 1 Tabla de Regulaciones 26
Tabla 2 Marco Metodológico 37
Tabla 3 Cronograma de Actividades 40
Tabla 4 Matriz Impacto al Negocio BIA 40
Tabla 5 Matriz Análisis de Riesgos 53
Tabla 6 Capex-1 62
Tabla 7 Opex-1 63
Tabla 8 Opex-2 64

Índice de Gráficas

Imagen 1 Empresas sin planes de Continuidad..... 11

Imagen 2 Origen de las Interrupciones..... 12

Imagen 3 Origen de las Interrupciones. 13

Imagen 4 Reacción a los Incidentes..... 14

Imagen 5 Aplicabilidad de las normas..... 14

Imagen 6 El Costo de Las Interrupciones..... 15

Imagen 7 La Continuidad de las Operaciones 18

Imagen 8 Word Trade Center 23

Imagen 9 Solución de Monitoreo..... 24

Imagen 10 Inundación Universidad de la Sabana..... 25

Imagen 11 Tsunami en Japón 26

Imagen 12 Justificación de un plan de Continuidad..... 27

Imagen 13 Evolución de la Continuidad..... 31

Imagen 14 Metodología de la Continuidad..... 39

Imagen 15 Organización Sistémica sin Continuidad..... 43

Imagen 16 Organización Sistémica con continuidad en TI 44

Imagen 17 Organización Sistémica con Continuidad a todo nivel..... 45

Imagen 18 Modelo de Continuidad..... 46

Imagen 19 Modelo de Negocios 52

Imagen 20 La continuidad y sus niveles..... 56

Imagen 21 Las Opciones de Tecnología en la Continuidad 57

Imagen 22 El Rpo y el Rto 59

Imagen 23 La organización y la Continuidad 67

Imagen 24 Entrenamiento y Capacitación 70

Imagen 25: Evolución de la Continuidad 73

LISTA DE ABREVIATURAS

En este documento se utilizan las siguientes abreviaturas

TIC	Tecnologías de la Información y las Comunicaciones
ISO	Organización Internacional para la Estandarización
DRI	Instituto de recuperación ante desastres
BCM	Manejo de la continuidad del Negocio
TI	Tecnologías de la Información
BCP	Planeación de la continuidad del negocio
DRP	Plan de Recuperación ante Desastres
SGSI	Sistema de Gestión de la Seguridad de la Información
RPO	Punto de Recuperación Objetivo
RTO	Tiempo de Recuperación Objetivo
ITIL	Librería de Información de TI o de las tecnologías de la Información
BIA	Análisis de Impacto al Negocio
PYME	Pequeñas y Medianas Empresas

1. INTRODUCCIÓN

Las asignaturas de Proyecto de Tecnología I (Anteproyecto) y Proyecto II constituyen una base importante para que los estudiantes de Administración de Sistemas Informáticos cuenten con instrumentos de trabajo que les permitan intervenir en las soluciones a los problemas Informáticos que se ven enfrentados a diario.

El desarrollo de Proyectos Tecnológicos, requiere por parte de los estudiantes del programa tener el conocimiento necesario para poder aplicar las etapas en la elaboración y desarrollo de los mismos.

La identificación de problemáticas que puedan ser resueltas mediante la gestión de Proyectos Tecnológicos, es también, un aporte importante que el profesional en Administración de Sistemas Informáticos aplicará en su vida profesional.

Existe la necesidad de esquematizar todos los tópicos que se involucran en la búsqueda de soluciones a los problemas Informáticos, con la finalidad de organizar el trabajo en forma sistematizada que permita una reorientación sin pérdida de tiempo en la ardua tarea informática.

Este trabajo plantea o define una metodología ágil para que las empresas puedan construir su plan de continuidad de TI y de esta forma eliminar los riesgos que representa el no tener un plan de continuidad, que asegure la continuación de las operaciones en caso de un desastre o imprevistos.

El trabajo se desarrolla en tres grandes capítulos, en el primer capítulo se define la problemática, los objetivos del proyecto, la justificación del proyecto, se realiza un diagnóstico, se establecen unos alcances y delimitaciones y finalmente un cronograma macro de actividades o de trabajo.

En la segunda unidad se aborda el marco de referencia, el marco teórico, el marco conceptual y el marco metodológico.

En la tercera unidad se profundiza en el desarrollo del proyecto mediante un análisis sistémico, la definición del modelo de continuidad, como es el proceso de implementación, se analizan los diferentes impactos, como son el tecnológico, el impacto económico, se detalla el análisis financiero, el análisis administrativo y se finaliza con unas conclusiones y unos anexos con información importante.

En términos generales el trabajo es elaborado aplicando las normas técnicas APA.

2. UNIDAD 1 – DATOS GENERALES DEL PROYECTO

2.1. Titulo descriptivo del proyecto

Definición de un modelo para la implementación de planes de continuidad de TI que asegure la continuidad de los sistemas informáticos en las empresas.

2.2. El problema del proyecto

DESCRIPCIÓN DEL PROBLEMA INFORMÁTICO

Actualmente casi todas las empresas, compañías u organizaciones dependen prácticamente en su totalidad de los sistemas informáticos, esto se refiere a los servicios provistos por el área de TI al resto de la organización. Con toda seguridad se puede afirmar que si en algún momento los servicios de TI se vieran interrumpidos, la operación de la empresa se podría ver seriamente afectada al no contar las diferentes áreas de la organización, con el acceso a los datos o a la información y a los diferentes sistemas informáticos en los cuales se apoyan para llevar a cabo sus procesos del día a día.

Un ejemplo puntual de esto sería la operación de un banco, si un banco se viera afectado por la no disponibilidad de sus sistemas informáticos, sus agencias no podría atender al público, las personas no podrían retirar su dinero, los cajeros electrónicos no podrían entregar efectivo,

es decir, la razón de ser de un banco estaría comprometida seriamente y esto representaría perdidas millonarias.

Como se sabe, los datos o la información reposan en medios electrónicos, las transacciones se realizan por medio de los sistemas informáticos, entonces lo que hoy en día es prácticamente la revolución y la solución a muchos procesos que anteriormente se realizaban de manera manual y tomaban horas y días, el no disponer de estos servicios significa un problema serio que puede poner en riesgo la operación de la empresa y al final su continuidad en el mercado.

La misión de la organización es lograr las metas que se han fijado para un periodo en particular. Ser una organización exitosa, productiva y convertirse en un modelo operativo, pero para lograr lo anterior es necesario contar con unos sistemas informáticos que además de ser eficientes y efectivos, estén disponibles cuando se les necesita.

La anterior dependencia llevaría a tener que asegurar la disponibilidad constante de estos servicios informáticos para que las personas estén en capacidad de hacer bien su trabajo, poder ser productivos, lograr sus metas y que la misión de la organización se convierta en una realidad, surge entonces una pregunta importante:

¿Puede un plan alterno asegurar la disponibilidad de los servicios permitiendo suplir de manera efectiva fallas o eventos críticos de los sistemas?"

Este proyecto expone una metodología ágil para la implementación de planes de continuidad que efectivamente solventaran esta problemática o necesidad.

DIAGNÓSTICO

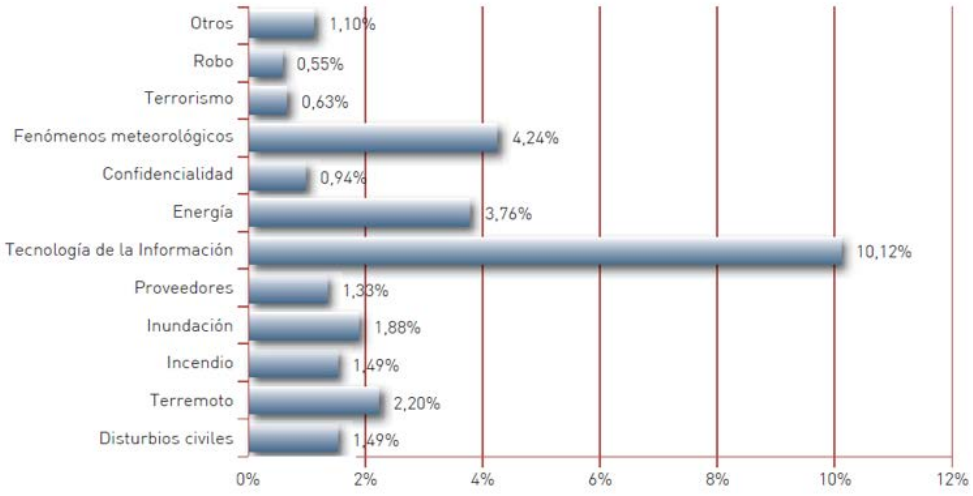
Para la ejecución de este diagnóstico se han realizado una serie de investigaciones, se ha trabajado con base en estadísticas de diferentes organismos internacionales y se ha elaborado un informe de cómo se encuentra el panorama en algunos países de America latina.

Según el artículo publicado por la revista digital “Expansión”, en agosto del año 2013, solo el 10% de las organizaciones y empresas radicadas en Mexico poseen un plan para la continuidad de sus operaciones en caso de imprevistos. De hecho, el mismo artículo menciona que alrededor de 2,500 comercios han quebrado debido a marchas, manifestaciones y otros en el distrito federal.

Imagen 1: Empresas sin planes de Continuidad

Hernández, I. (29 de 08 de 2013). *EMPRESAS, SIN UN PLAN ANTE CONTINGENCIAS*. Recuperado el 25 de 06 de 2017, de EXPANSIÓN, En alinza con CNN: http://expansion.mx/emprendedores/2013/08/28/empresas-sin-un-plan-ante-contingencias

La siguiente imagen muestra como la mayoría de imprevistos, paradas o interrupciones de las empresas tienen como origen diferentes tipos de eventos que se presentan en el área de TI, de allí la importancia de establecer un plan de continuidad de TI.



El estudio se ha realizado entre noviembre de 2011 y enero de 2012, y se ha contado con la respuesta de 685 ejecutivos de organizaciones ubicadas en más de cuarenta países, estando una cuarta parte de ellas ubicadas fuera de Estados Unidos de América. Los resultados mostrados están referidos exclusivamente a las empresas del sector asegurador, que suponen un 10,6% del total de compañías participantes en el estudio. La Tecnología de la Información es el principal elemento que desencadena la necesidad de activación de los planes de continuidad de negocio, incluyendo en este apartado, tanto las caídas de servicio programadas por actualizaciones, el mantenimiento y la gestión de cambios, así como las que no han sido programadas: ataques de virus, denegaciones de acceso o comunicaciones.

Imagen 2: Origen de las Interrupciones
Fuente: Estudio realizado por la empresa KPMG titulado “Global Business Continuity Management Program Benchmarking Study”

Por otro lado estadísticas de “GARTNER” del año 2010, reflejan la realidad en ese momento de cuáles eran las mayores causas de caída, indisponibilidades, fallas en los servicios y en general de porque las compañías se veían afectadas en su producción u operación.

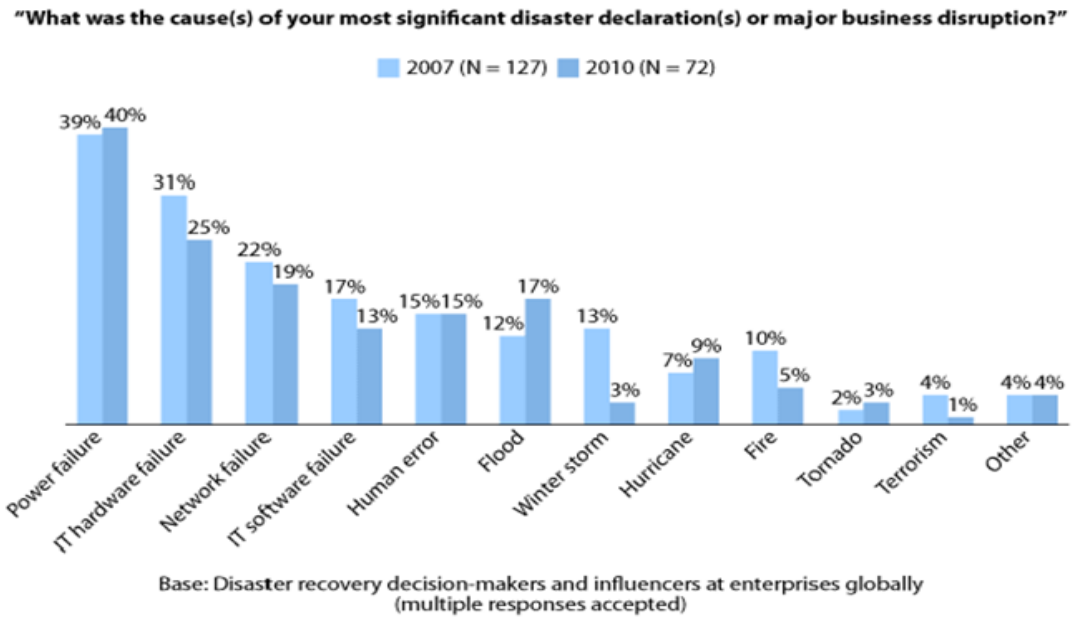
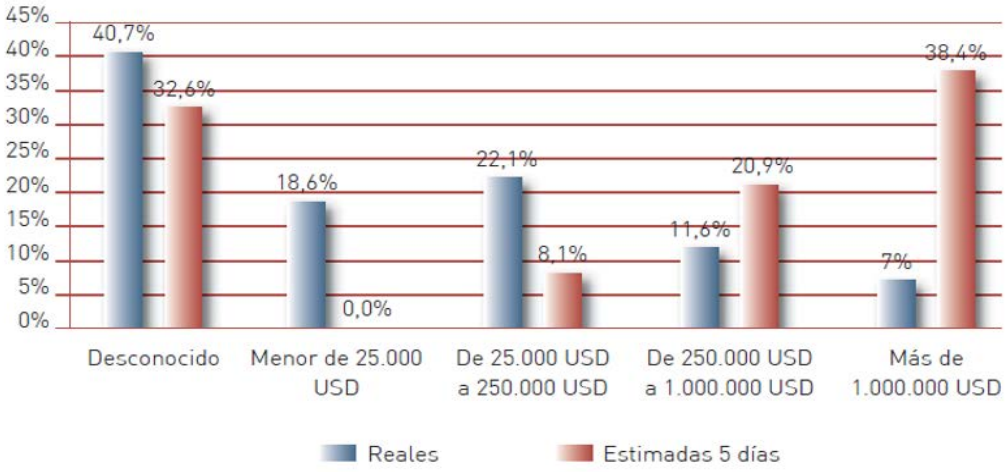


Imagen 3: Origen de las Interrupciones
Fuente: Informe Estadístico de GARTNER 2010

En esta gráfica se puede apreciar que la causa más común de fallas en los servicios de TI se encuentran relacionadas en primer lugar con fallas de potencia o energía, en segundo lugar con fallas en los equipos de TI (Servidores, almacenamientos etc.) y posteriormente con fallas del sistema de redes o “networking”, sin ser las demás causas menos importantes,

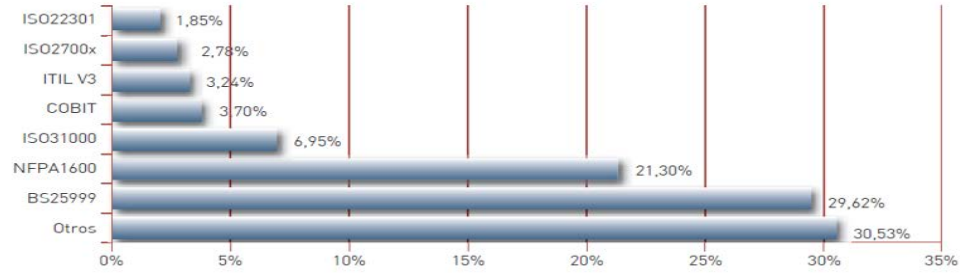
En la siguiente gráfica se observa que el costo que tienen que pagar las empresas luego de que este tipo de eventos se materialicen puede en algunos casos llegar a ser bastante altos.



Es significativo ver que el 40% de las organizaciones desconocen el coste económico de las pérdidas que les han supuesto los incidentes, mientras que también casi el 40% cuantifican las pérdidas por paralización del negocio durante cinco días en más de un millón de USD.

Imagen 4: Costo por los eventos
Fuente: Estudio realizado por la empresa KPMG titulado "Global Business Continuity Management Program Benchmarking Study"

La siguiente imagen refleja que estándar están utilizando hoy en día las organizaciones para trabajar los temas de continuidad en los estados unidos.



Se puede observar que un tercio de las compañías basan su sistema de gestión de la continuidad de negocio en estándares locales del país o estándares no específicos de continuidad de negocio (Otros). El elevado porcentaje de la aplicación del estándar NFPA1600 está motivado principalmente porque la mayoría de las compañías intervinientes en este estudio están localizadas en EE.UU. La normativa ISO22301, que sustituye a la BS25999, aparece con bajo porcentaje porque a la fecha del estudio estaba en fase de borrador (publicada en mayo 2012). También es destacable que casi un 7% de las compañías basan su sistema de gestión de continuidad de negocio en estándares relacionados principalmente con la tecnología (ITIL, COBIT).

Imagen 5: Aplicabilidad de las normas
Fuente: Estudio realizado por la empresa KPMG titulado "Global Business Continuity Management Program Benchmarking Study"

A continuación la empresa de investigación “Forrester” estima los costos de las interrupciones y fallas imprevistas a los que las empresas tienen que enfrentarse una vez experimenten algún tipo de interrupción grave.

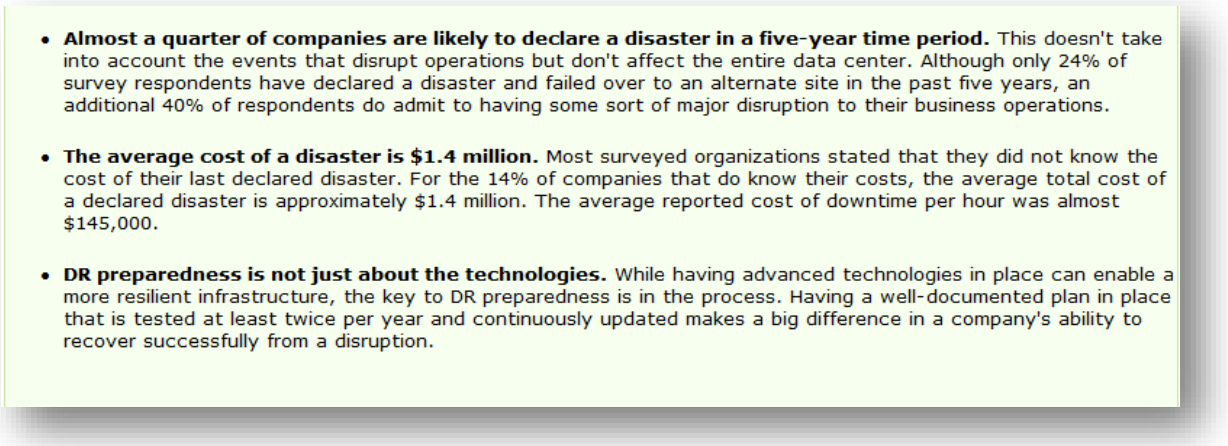


Imagen 6: El Costo de Las Interrupciones
Fuente: FORRESTER - White Paper Best Practices in Business Continuity 2011

De la imagen anterior se puede resumir, que un cuarto de todas las compañías encuestadas admiten haber declarado un evento de desastre en un periodo de 5 años lo cual no tiene en cuenta los diferentes eventos que en ese periodo se llegaron a dar en donde hubo interrupción de operaciones pero que no llegaron a afectar a todo el Centro de datos.

A pesar de que solamente el 24% de las compañías encuestadas declararon en algún momento una situación de desastre y tuvieron que activar su sitio alterno en los pasados 5 años un 40% adicional

de las compañías encuestadas admitieron haber tenido alguna clase seria de suspensión del servicio que llego a afectar las operaciones del negocio.

Un dato importantísimo a resaltar es que el costo promedio de un evento declarado como desastre asciende a la suma de 1.4 Millones de dólares sin embargo la mayoría de las empresas encuestadas respondieron que nunca supieron cuánto realmente perdieron en la última declaración de desastre.

Se calcula que el costo por un fuera del servicio por cada hora fue cercano a los $145.000 USD.

Lo que sí es importante, es que no basta tener la última tecnología de punta o la más costosa, lo que también importa es tener buenos y bien documentados planes de continuidad de negocios y que estos sean probados al menos 2 veces por año, esto es lo que marca la diferencia para que una compañía se pueda recuperar satisfactoriamente de una interrupción de sus servicios cualquiera que sea su causa.

PLANTEAMIENTO DEL PROBLEMA INFORMÁTICO

Tanto las estadísticas como los hechos del día a día confirman que la ausencia de planes de continuidad de TI es una deficiencia muchas veces de origen cultural u organizacional en cuanto a la permanencia de las empresas en el mercado.

Lo que se busca mediante la aplicación o la implementación de este modelo que se está proponiendo de plan de continuidad de TI es asegurar que las empresas estén preparadas para cualquier tipo de evento o amenaza previamente identificado y que pudiera llegar a materializarse. Estar preparado quiere decir, que de antemano ya estaría definido o documentado como proceder o reaccionar ante la consolidación de un riesgo.

Solo cuando se profundice en el tema de riesgos se podrá evidenciar que no todos los riesgos se pueden evitar, pero aun así, se les puede dar un manejo o tratamiento siempre y cuando este se tenga previamente identificado. De esto trata el plan de continuidad de TI, de identificar previamente a cuales riesgos está expuesta el área y de definir, documentar y prepararse para manejar dichos riesgos en caso de estos llegaran a materializarse.

SELECCIÓN DE LA SOLUCIÓN

El camino a seguir y que ha demostrado dar resultado en todas las empresas que han enfrentado interrupciones de servicio y que han sobrevivido a estos eventos con el mínimo impacto, es la implementación y puesta en marcha de un plan de continuidad de TI, que vaya acorde a los planes estratégicos del negocio.

El desarrollo de este tipo de planes, la identificación de las amenazas, el tener identificados los riesgos, la definición de estrategías, y un sitio alterno de recuperación en caso de que este aplique al tipo de organización, asegura la continuación de las operaciones en cualquier empresa.

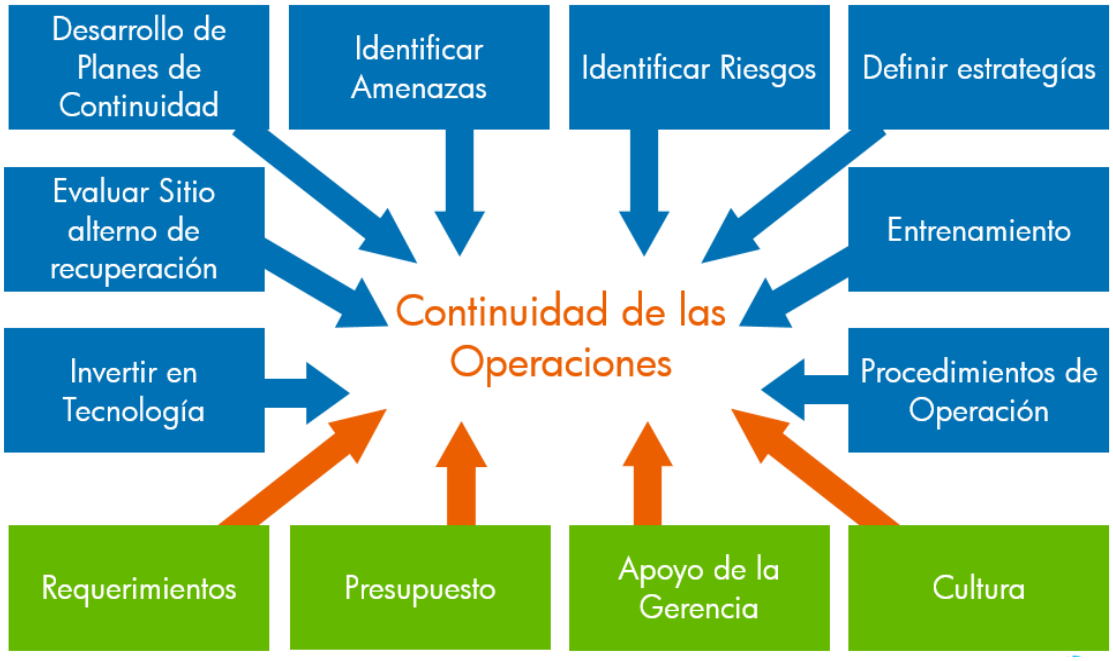


Imagen 7: La continuidad de las Operaciones
Fuente: Desarrollo Propio

Los objetivos anteriormente mencionados pueden lograrse mediante el estudio y la implementación de las normas ISO de gestión de seguridad de la información (ISO27001), ISO en continuidad de negocio (ISO22301), las buenas prácticas de ITIL, el modelo Cobit o la metodología existente de los entes reguladores a nivel mundial como lo son el DRI.

A nivel nacional el Ministerio de las Telecomunicaciones (MINTIC) y el Icontec también han desarrollado documentos referentes a la aplicación de metodología de este tipo, la propuesta del MINTIC se basa en el estándar británico BS25999 que en años recientes ha ganado mucho terreno, y en el caso del Icontec este instituto de normas técnicas ha desarrollado varias normas relacionadas con el tema de continuidad, por ejemplo la norma NTC-ISO 3100 para la gestión del riesgo y la norma 27001 que toca todo el tema de SGSI o sistema de gestión de seguridad de la información.

FORMULACIÓN DEL PROBLEMA DEL PROYECTO INFORMÁTICO

El modelo planteado subsanará la deficiencia que se tiene hoy en día en cuanto a la implementación de planes de continuidad de TI en las empresas, como ya se ha dicho, la situación problemática actual se genera por diversas razones, entre estas se encuentran falta de estrategia o de visión de la organización, la falta de controles, el no enfocarse en las causas raíces, por trabajar en los efectos o en las consecuencias, y por un manejo reactivo en vez de proactivo. Sin embargo, la implantación del modelo que se propone de continuidad de TI, llevará a cambiar la visión y estrategia de la organización, implementar nuevos controles, a trabajar con una visión proactiva para que los problemas potenciales puedan ser prevenidos por los miembros de la organización y que todo lo que pudiera llegar a ocurrir se encuentre siempre bajo control.

2.3. Objetivos

GENERAL

Proponer un modelo que atienda a necesidades específicas de las empresas y que garantice la continuidad de los servicios de Tecnologías de Información (TI), permitiendo la mitigación y reducción de los riesgos que afectan la disponibilidad de los sistemas informáticos, en conjunto y con el apoyo de las herramientas tecnológicas.

OBJETIVOS ESPECÍFICOS

Los objetivos específicos mediante la aplicación del modelo que se está proponiendo son los siguientes:

- Realizar una indagación sobre los modelos que sirven de soporte en la continuidad de los servicios de TI
- Identificar los riesgos potenciales a los cuales están expuestos los sistemas informáticos de la organización, permitiendo la construcción de la matriz de impacto al negocio
- Presentar el modelo que permita dar continuidad a la operación de la empresa y los servicios de TI, brindando estabilidad a las operaciones realizadas por los clientes
- Determinar los elementos técnicos, administrativos y financieros inmersos en la implementación de un modelo de continuidad de TI

Los objetivos financieros y económicos están directamente relacionados con los objetivos generales y específicos en la medida en que la organización lo que busca es eliminar la menor posibilidad de experimentar fuera de servicios, que a la larga significaran grandes pérdidas de dinero, de reputación y pérdida de clientes, viéndose seriamente comprometidas las metas financieras de la empresa y por ende su visión a largo plazo.

Los objetivos técnicos también van alineados a los objetivos de la gerencia de TI, ya que la gerencia de TI aspira a que sus sistemas sean unos sistemas de información altamente disponibles, altamente redundantes, sin puntos únicos de falla y que puedan estar operativos el 99.9999% del tiempo, por lo tanto, con los objetivos específicos se busca identificar aquellos puntos únicos de falla, aquellas amenazas, identificar riesgos y trabajar en busca de una solución para minimizar el impacto de los mismos.

Finalmente, los objetivos administrativos, que realmente se enfocan en la planeación estratégica para orientar el rumbo de la empresa, serán una realidad, ya que en la medida en que los sistemas de información sean más confiables, el foco de la dirección realmente será para la planeación estratégica.

2.4. Justificación

Según IBM, de las empresas que han tenido una pérdida principal de registros automatizados, el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años y sólo el 6 % sobrevivirá a largo plazo.

Durante el ataque terrorista más grande de la historia, las dos torres gemelas en Nueva York fueron derribadas por dos aviones comerciales, de las 493 compañías que operaban en las dos torres, o vieron afectadas seriamente su operación o quebraron definitivamente.

Imagen 7: Atentados Word Trade Center NY

(23 de 11 de 2011). *ATAQUE A TORRES GEMELAS*.

Recuperado el 25 de 06 de 2017, de Google: https://www.google.com.co/search?biw=1829&bih=861&tbm=isch&sa=1&q=imagenes+ataque+torres+gemelas

Fred Alger Management Company; perdió el 65% de sus empleados, sin embargo esta compañía pudo sobrevivir.

Verizon Communication; se vio impactada seriamente quedando sin servicio lo siguiente:

- 5 conmutadores de telecomunicación
- 10 torres del sistema de telefonía celular

- 300.000 líneas de voz
- 3.6 millones de circuitos ubicados en el área
- Los centros de conmutación de AT&T y Sprint en el WTC fueron destruidos

Solo 3 semanas después de esto Verizón se había recuperado de los daños en un 80%.

Imagen 8: Reacción a los incidentes

(23 de 11 de 2011). *ATAQUE A TORRES GEMELAS*.

Recuperado el 25 de 06 de 2017, de Google: https://www.google.com.co/search?biw=1829&bih=861&tbm=isch&sa=1&q=imagenes+ataque+torres+gemelas

Nokia & Ericsson son dos compañías reconocidas mundialmente pero tenía un proveedor común de chips que vio afectada su producción de tarjetas por un incendio, gracias a que Nokia tenía un plan de continuidad claramente definido, y este plan incluía a otros proveedores pudo sobrevivir y no incumplir a sus clientes, pero lo mismo no paso con Ericsson quien termino retirándose definitivamente del mercado de telefonía celular.

Universidad de la Sabana Bogotá; debido a las inundaciones del rio Bogota, la universidad no pudo continuar dando clases en su sede y tuvo pérdidas cuantiosas debido al daño de gran cantidad de equipo de tecnología como computadores y equipos de comunicaciones entre otros, el resultado fue miles de estudiantes afectados y sin poder asistir a clases.

Imagen 9: Inundación Universidad de la Sabana

(29 de 12 de 2011). *IMÁGENES INUNDACIÓN UNIVERSIDAD DE LA SABANA*. Recuperado el 25 de 06 de 2017, de Google: http://www.google.com.co/search?q=imagenes+inundacion+universidad+sabana

- Terremoto y Tsunami en Japón
- Miles de Víctimas mortales
- Declaración de emergencia en la central nuclear FUKUSHIMA
- Incendio en el edificio de turbinas de la central nuclear de Onagawa
- La red de transporte japonesa sufrió innumerables daños
- Suspensión de servicios en aeropuertos
- Cierre temporal de fábricas automotoras como Toyota, Nissan y Honda con pérdidas millonarias

Imagen 10: Tsunami en Japón

(15 de 04 de 2011). *IMÁGENES TSUNAMI EN JAPON*. Recuperado el 25 de 06 de 2017, de Google: https://www.google.com.co/search?biw=1829&bih=861&tbm=isch&sa=1&q=imagenes+tsunami+en+japon

La lista de ejemplos como estos son interminables pero el mensaje principal es, que quien sobrevive a cualquier tipo de eventos son aquellas empresas que estaban preparadas de antemano con un plan claramente definido de continuidad de negocios o de continuidad de TI, de allí la importancia de contar con planes de continuidad de negocios o de TI.

Debido a lo anterior las organizaciones están ya comenzando a solicitar planes de continuidad de negocios a sus proveedores como un prerrequisito para poder establecerse como socios comerciales en el mercado.

Hoy en día son muchas las organizaciones que podrían llegar a tomar la decisión de no establecer vínculos comerciales con determinados socios de negocios o proveedores de materia prima, si estos no certifican, o demuestran tener o estar trabajando en sus respectivos planes de continuidad, resulta entonces claro que esto es un beneficio para quien lo tiene y una desventaja para quien no los tiene.

La siguiente imagen muestra que es lo que motiva a las empresas a comenzar a implementar un plan de continuidad.

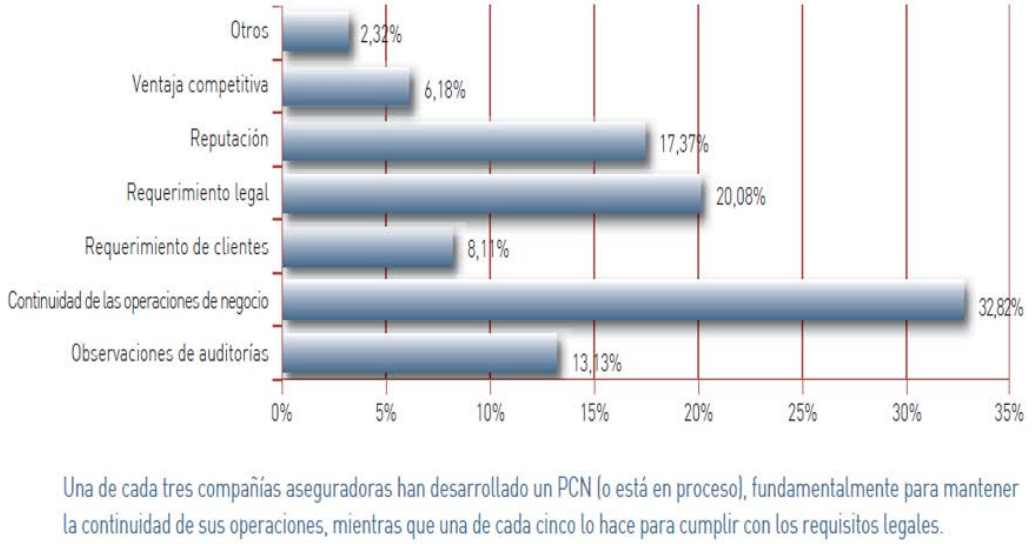


Imagen 11: Justificación de un plan de Continuidad
Fuente: 2012 - Estudio realizado por la empresa KPMG titulado "Global Business Continuity Management Program Benchmarking Study"

Debido a que una de las razones de implementar un plan de continuidad de TI o de la siguiente fase que es la continuidad del negocio, son los requerimientos legales, en Colombia hay dos regulaciones claras que vienen de la "Superfinanciera" y que aplica para todas aquellas organizaciones financieras o bancarias.

País origen	Metodología Estándar Guía	Desarrollada por:	Propósito	Fecha
UK	ISO27001. Information Security Management	British Standards Institute (BSI)	Estándares para el desarrollo, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). A.14 Gestión de la Continuidad del Negocio	2005
UK	ITIL. IT Infrastructure Library's Service Delivery Management practices	Office of Governement Commerce	Lineamientos para mantener la continuidad de servicios de tecnología.	2007
Colombia	SARO	SuperFinanciera	Reglas relativas a la administración del riesgo operativo. 3.1.3.1 Administración de la continuidad del negocio	2006
Colombia	Circular 052	SuperFinanciera	3.2.3 Exigir que los terceros dispongan de planes de contingencia y de continuidad debidamente documentados	2007

Tabla 1: Tabla de Regulaciones
Fuente: Ministerio de Comunicaciones (Mintic)

2.5. Alcances y Delimitaciones

Este proyecto tiene como propósito establecer y proporcionar un modelo o metodología ágil de continuidad de TI para que las organizaciones puedan iniciar la implantación de un proyecto de este tipo sin alejarse de las prácticas que existen en el mercado, como son las normas ISO de la familia 27000 relacionadas con los sistemas de gestión de seguridad de la información (SGSI) y las mejores prácticas del "Disaster Recovery Institute" (DRI) o sea una combinación de seguridad de la información y continuidad de negocios.

Los lineamientos, recomendaciones e información en general aquí plasmados no pretenden reemplazar cualquier otra fuente de información experta en el tema de seguridad de la información y/o continuidad de negocios sino servir de apoyo con base en la experiencia que se tiene en continuidad de TI.

Existen muchas otras fuentes de información al respecto, como por ejemplo las normas ISO 27000 y toda la información generada por las dos instituciones que a nivel mundial son las rectoras del tema de continuidad como son el DRI (Disaster Recovery Institute) y el BCM (Bussiness Continuity Institute).

Si bien, el proyecto tiene como alcance el área de TI, lo que quiere decir que se plantea un plan de continuidad de TI y no del negocio en su totoalidad, también es muy cierto que el proyecto influencia o se relaciona con toda la compañía u organización ya que TI es un área que actúa como soporte para que las demás áreas puedan llevar a cabo sus labores y/o cumplir con sus objetivos, luego serán beneficiarias las diferentes áreas que TI soporta dentro de la organización.

Para llevar a cabo un plan de continuidad de TI se debe contar con el apoyo irrestricto de la gerencia, este tipo de procesos no nacen y se maneja solamente en torno al área de TI, se necesita el apoyo total de la gerencia y de los líderes de las demás áreas de la compañía u organización.

Un proyecto de esta envergadura es muy variable en tiempo y en alcance y tiene mucho que ver con la compañía en donde se quiera aplicar, con el tamaño de la misma y con su complejidad organizacional.

El momento de emprender un proyecto de este tipo dependerá de la visión de la organización y del impulso de la dirección de TI, se podría decir que es ya una realidad que toda empresa necesita al menos indagar a cuales riesgos está expuesta y determinar el impacto de la consolidación de esos riesgos para evaluar si continua con todo el proceso de la continuidad, teniendo en cuenta que la información es uno de los activos más valiosos de la organización.

El establecimiento de los planes de continuidad de TI podría llevarse a cabo y en paralelo con otros proyectos de implementación de seguridad de la información.

Finalmente y como parte de los entregables, la aplicación de este proyecto generará la cultura de la seguridad y continuidad dentro de la organización así como los planes y/o procedimientos escritos de cómo proceder ante la consolidación de cualquier evento que ponga en riesgo la continuidad del área de TI y los efectos a que esto conlleve.

Al finalizar la implantación de un proyecto de este tipo, la organización no verá una retribución económica inmediata, resultado de esta inversión realizada pero si tendrá como retribución la seguridad de que sus servicios y su plataforma tecnológica son altamente disponibles, lo cual asegurara la continuidad de las operaciones, generara confianza tanto en el cliente interno como

en el cliente externo, generará reputación y buena imagen en el mercado y más importante que minimizara las grandes pérdidas resultado de no tener un plan de continuidad.

3. UNIDAD 2 – MARCO DE REFERENCIA

3.1. Antecedentes

Debido a todo lo que anteriormente se ha venido exponiendo, es que muchas empresas desde hace muchos años vieron la necesidad inicialmente de definir o tener “Planes de Contingencia” o lo que se llamaba en su momento como planes alternos o “Plan B”, posteriormente esto evolucionó a tener un plan de recuperación ante desastres o DRP, después y dada la importancia del tema se hizo necesario mirar hacia otras áreas de la compañía es decir que los planes de contingencia deberían de abarcar los diferentes procesos críticos de la compañía por lo que nace el plan de continuidad del negocio o “BCP” y hoy en día, en donde se ve que el proceso no puede ser algo puntal en el tiempo sino continuo ya hablamos de la Administración de la continuidad del negocio o BCM (Administración de la Continuidad del Negocio).

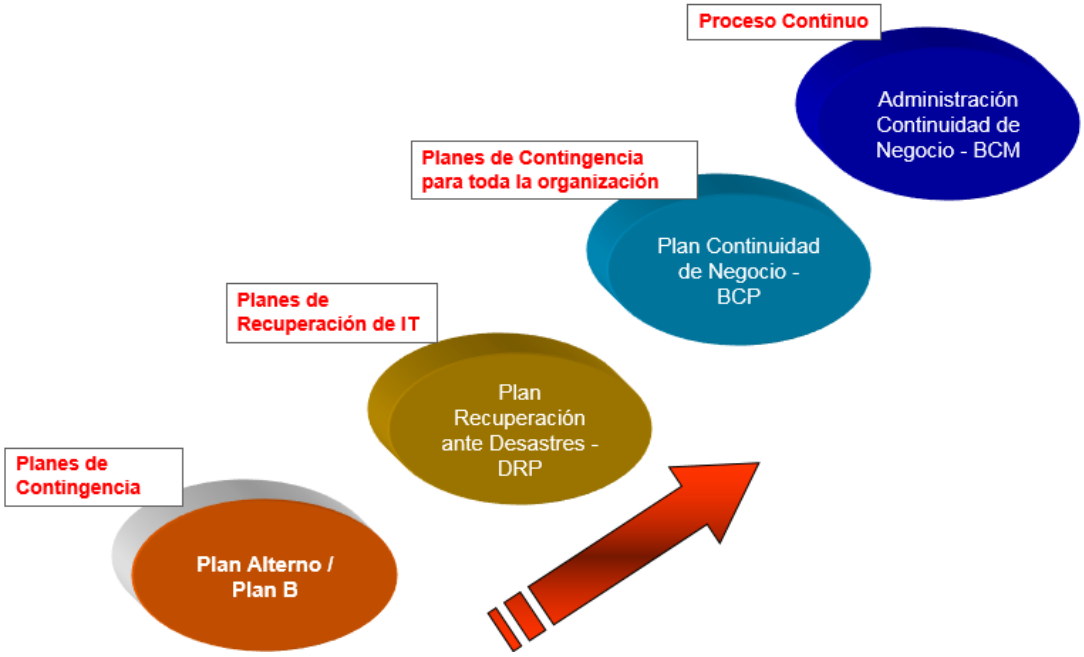


Imagen 12: Evolución de la Continuidad
Fuente: Hewlett Packard - Disaster Recovery Readiness Document

Ahora, cuál sería el costo para las empresas que no tengan implementado un plan de continuidad (BCP) o la administración de la continuidad del negocio "BCM"? Los hechos y lo que vemos continuamente demuestran que las organizaciones terminan teniendo perdidas millonarias y otras en corto o mediano plazo terminan desapareciendo.

Hoy en día empresas prestadoras de servicios como las compañías de telefonía o como los bancos entre otras, son empresas pioneras en los temas de alta disponibilidad y continuidad de los servicios.

Muchas empresas comenzaron a trabajar en continuidad porque el gobierno mediante regulaciones les exigían tener asegurada la información y la prestación de los servicios, en caso

contrario podrían hacerse acreedoras a altas multas y/o penalidades sino hay continuidad en la prestación de los servicios.

De todo esto surge la necesidad de las empresas de tener planes de continuidad definidos, probados y en funcionamiento para sus servicios considerados como críticos.

3.2. Marco Teórico

La solución al problema se abordara aplicando el modelo propuesto de continuidad de TI que incluyen máximo unas 10 prácticas a seguir. Dentro de las prácticas más relevantes para la implementación del proyecto se encuentran:

a) Administración e inicio del proyecto

   En esta primera fase se trata de hacer ver a la empresa la necesidad de implantar un plan de continuidad de TI, hay que involucrar, convencer y lograr el apoyo de la alta Gerencia, establecer el comité del proyecto y hacer un presupuesto de los costos para la ejecución del proyecto, realizar el "kickoff" del proyecto o arranque del mismo, hay que tener el compromiso de todas las áreas de la organización, finalmente emitir reportes continuos de avance del proyecto.

b) Evaluación de Riesgos y Controles

   Es muy claro que un riesgo es aquel que proviene del interior o del exterior y que al final son una amenaza para el logro de los objetivos del negocio.

La evaluación de riesgos es entonces la identificación de las exposiciones externas o internas que presenta la compañía.

Existen amenazas físicas y lógicas, físicas como los terremotos, inundaciones, incendios etc. y las lógicas como los virus, fallas del software o de las aplicaciones.

En resumen, podemos concluir que la evaluación del riesgo es la consideración del daño sobre el negocio que puede llegar a producir una amenaza, la probabilidad de que una amenaza se llegue a hacer una realidad y las medidas adoptadas para lograr mitigar los riesgos previamente identificados.

c) Análisis de Impacto al Negocio (BIA)

El BIA es la elaboración de una matriz con los procesos críticos del negocio y cuál sería el impacto al negocio en caso de falla o no ejecución de uno de esos procesos críticos debido a fallas en TI.

Aquí se evalúan cuáles son los efectos de las interrupciones, daños o impacto al negocio.

También se evalúa cual es el impacto financiero de las posibles interrupciones.

En resumen, también se define cual es el tiempo máximo que un servicio podría no estar operando sin que llegue a afectar negativamente a la operación de la empresa.

d) Desarrollo de Estrategias de Continuidad de TI

Se trata de definir una(s) estrategia(s) de continuidad para la(s) posible(s) falla(s) de los procesos críticos del negocio ya identificados en la matriz BIA, es decir cómo se piensa reaccionar ante la consolidación de un determinado evento que afecta la operación de la empresa.

Hay que presentar cual es análisis costo beneficio de una estrategia específica.

En caso de que una estrategia sea activar un sitio alterno para la continuidad de las operaciones, hay que evaluar las modalidades de sitios alternos para poder seguir operando así como todo el equipamiento.

e) Construcción de los planes de continuidad

En el punto anterior se define solamente cual sería la estrategia a aplicar, en este punto de la construcción del plan ya se detalla cómo y mediante que recursos se lograra la activación de la estrategia seleccionada.

f) Implementación del DRP

Luego de las fases anteriores, es posible obtener como resultado que uno o algunos de los procesos críticos del negocio necesite continuidad de computo por lo que se hace necesario contar con un sitio alterno de procesamiento para poder dar continuidad a esos procesos críticos, de aquí nace la necesidad de contar con un sitio alterno de procesamiento, con un plan de recuperación ante un desastre, es decir cómo vamos a dar servicio desde el sitio remoto, cuando, en qué condiciones, porque, por cuanto tiempo, cuando sería el regreso etc.

g) Mantenimiento al plan de continuidad

Esta práctica es muy importante y está relacionada con la actualización de los planes, el mundo de TI cambia mucho en su configuración, nuevos servicios son implementados, nuevas aplicaciones, nuevos equipos etc. Si un plan de continuidad no se actualiza pierde vigencia ya que al momento de su aplicación no será consistente y por lo tanto no se podrá cumplir con el objetivo y los resultados podrían ser gravísimos y costosos.

h) Pruebas y Simulacros

Para asegurar que las estrategias definidas y que el plan de continuidad construido y documentado sea consistente se hace necesario realizar simulacros de fallas y probar el plan tal como se encuentra documentado para establecer que efectivamente las operaciones se pueden restablecer en forma y en tiempo, aquí es donde se puede llegar a detectar que algo en el plan necesita ser reconsiderado, ajustado y perfeccionado.

3.3. Marco Conceptual

Lo que plantea este proyecto es un modelo de continuidad para TI que vaya alineado con el plan de continuidad del negocio o de la organización, es importante el manejo y dominio de los siguientes conceptos (entre otros) durante el ciclo de vida del proyecto.

EL RIESGO: El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas, los riesgos siempre están presentes pero se pueden llegar materializar o no.

LA AMENAZA: Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando se dan ciertas condiciones el riesgo podría materializarse y convertirse en una amenaza. Se puede considerar que es la materialización del riesgo.

LA VULNERABILIDAD: Está muy relacionado con el riesgo y con la amenaza, se define como el grado de exposición de un sujeto, objeto o sistema.

FACTORES DE RIESGO: Son todas las cosas que hacen aumentar la probabilidad de dañar los puntos más vulnerables de un sistema.

ANALISIS DE RIESGOS: Es la temprana acción que se puede tomar para conocer, identificar, clasificar, y atenuar o evitar las consecuencias o efectos del mismo.

SITIO ALTERNO: Es el centro de cómputos de contingencia en donde se tienen equipos de similares características y que en algún momento entraran a proveer los servicios que estaban siendo provistos por los equipos del sitio principal y que por la materialización de un riesgo quedo fuera de servicio por un periodo de tiempo.

ALTA DISPONIBILIDAD: Disponibilidad es una característica de diseño y arquitectura que mide el grado con el que los recursos de los sistemas están activos y disponibles para su uso por el usuario final. En resumen la Alta disponibilidad nos asegura que nuestros sistemas, ante posibles fallos, seguirán estando disponibles para su uso.

REDUNDANCIA: Es cuando los componentes de nuestros sistemas se encuentran duplicados con el objeto de suplir una función en caso de falla del primero.

PLAN DE RECUPERACION DE DESASTRE: Es un documento donde reposan los procedimientos o paso a paso para poner en práctica y recuperarse de una situación o eventos que genero una indisponibilidad de los sistemas o de la operación de una compañía.

3.4. Marco metodológico

A continuación se presenta cual será el paso a paso o la metodología para llevar a cabo cada etapa del proyecto.

ACTIVIDADES / OBJETIVOS	ESTRATEGIAS	RECURSOS
Conseguir Soporte y/o Apoyo de la Gerencia	Justificar Proyecto y presentarlo a la gerencia con costo beneficio	Gerencia de TI, Líder De Continuidad
Conseguir recursos para el proyecto	Justificar Proyecto y presentarlo a la gerencia con costo beneficio	Gerencia de TI, Líder De Continuidad
Realizar el análisis de riesgos	Mediante reuniones y revisión de procesos	Gerente del Proyecto Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio
Identificar procesos críticos y crear matriz BIA	Mediante reuniones y revisión de procesos	Gerente del Proyecto Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio
Desarrollo de estrategias de continuidad	Mediante reuniones y revisión de procesos	Gerente del Proyecto Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio
Desarrollo del plan de continuidad de TI	Mediante reuniones y revisión de procesos	Gerente del Proyecto Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio

ACTIVIDADES	ESTRATEGIAS	RECURSOS
Mantenimiento al plan de continuidad de TI	Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio	Gerente del Proyecto Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio
Simulacros y pruebas del plan de continuidad	Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio	Administradores de las plataformas Gerencia de TI Lideres de los procesos Críticos Líder de Continuidad del Negocio

Tabla 2: Marco Metodológico
Fuente: Desarrollo propio

La metodología utilizada para la ejecución del presente proyecto ha sido analítica y de campo

- Investigación Analítica: Se realizó una investigación sobre la implementación de la continuidad en algunos países de America latina y estados unidos para tener indicadores al respecto.
- Investigación de Campo: La investigación de campo se realizó a través de visitas hechas a diferentes compañías y a conclusiones obtenidas de la observación.

Imagen 13: Metodología propuesta para la continuidad
Fuente: Desarrollo propio

En el diagrama anterior se observa el orden de ejecución de las diferentes actividades y como el mantenimiento al plan de continuidad y las pruebas y simulacros son actividades que deberán estarse ejecutando continuamente ya que los cambios que se den en la configuración actual podrían dejar desactualizados los planes y por ende las pruebas podrían llegar a fallar.

Finalmente una de las prácticas tiene que ver con la retroalimentación se lleva a cabo mediante el uso de reportes e indicadores que deberán ser enviados a la gerencia sobre el resultado de las pruebas y simulacros o también luego de la consolidación de eventos reales que tiene que ver con el resultado de la activación de los planes de continuidad.

3.5. Cronograma de Actividades

A continuación el cronograma de actividades relacionadas con la puesta en marcha del modelo que se está proponiendo, es importante tener en cuenta que los tiempos pueden variar dependiendo del tamaño y complejidad de la organización.

OBJETIVOS	ACTIVIDAD	TIEMPO	RECURSOS
IDENTIFICACION DE SPONSORES	Conseguir apoyo de la gerencia para el proyecto	2 Semanas	Líderes de áreas y de procesos BCP MGR, BCP Consulting
RIESGOS	Realizar sesiones de identificación de riesgos	2 Semanas	Líderes de áreas y de procesos
	Documentar riesgos con probabilidad y criticidad	1 semana	Líderes de áreas y de procesos
MATRIZ BIA	Revisión e identificación de procesos críticos del negocio	2 Semanas	Líderes de áreas y de procesos BCP MGR, BCP Consulting
	Documentar riesgos con probabilidad y criticidad	1 Semana	Líderes de áreas y de procesos BCP MGR, BCP Consulting
ESTRATEGIAS	Definir estrategías de recuperación	1 Semana	Líderes de áreas y de procesos BCP MGR, BCP Consulting
	Documentar estrategías	1 Semana	Líderes de áreas y de procesos BCP MGR, BCP Consulting
PROCEDIMIENTOS	Desarrollo del plan y aplicación del modelo	4 Semanas	BCP MGR, BCP Consulting
PLAN DE CONTINUIDAD	Actualización del plan	3 Semanas	BCP MGR, BCP Consulting
ENTRENAMIENTO	Coordinación con autoridades externas	2 Semanas	BCP MGR, BCP Consulting

OBJETIVOS	ACTIVIDAD	TIEMPO	RECURSOS
MANTENIMIENTO	Realizar simulacros, pruebas y ejercicios	3 Semanas	Líderes de áreas y de procesos BCP MGR, BCP Consulting
COMUNICACIÓN	Sensibilización y capacitación	2 Semanas	BCP MGR, BCP Consulting

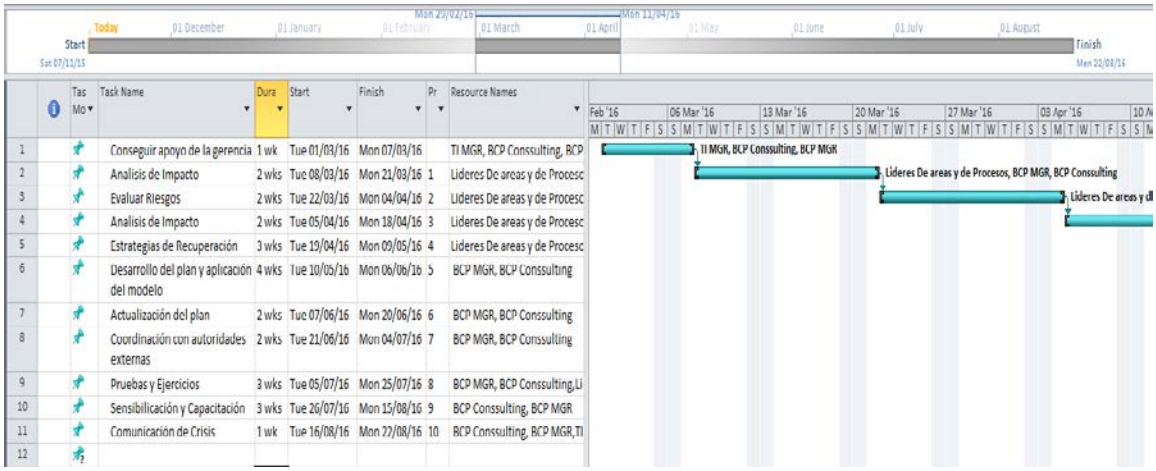


Tabla 3: Cronograma de Actividades
Fuente: Elaboración Propia

4. UNIDAD 3 – DESARROLLO DEL PROYECTO.

4.1. Análisis y Propuesta de Tecnologías y Productos – Análisis Sistémico

La organización nace, crece, se vuelve más compleja, sus partes interaccionan y su ciclo de vida es extenso.

“Toda empresa u organización se puede ver como un sistema abierto con características comunes a un organismo vivo, ya que solo puede existir mediante el intercambio con su ambiente”…. Miller y Rice

Imagen 14: Organización Sistémica sin Continuidad
Fuente: Desarrollo propio

A partir de la anterior afirmación, se muestra inicialmente un mapa sistémico de la organización sin la integración con la continuidad, aquí se aprecia como la organización es un sistema que tiene sus entradas que son los insumos, las materias primas etc. y que mediante una serie de procesos produce unos productos y servicios, sin embargo, también se observa como la organización está propensa a amenazas y riesgos que vienen del ambiente circundante y que podrían afectar sus productos y servicios y por ende su reputación en el mercado.

Imagen 15: Organización Sistémica con Continuidad en TI
Fuente: Desarrollo Propio

Este mapa sistémico de la organización refleja como una organización que ha implementado planes de continuidad de TI o alrededor de aquella tecnología que apoya los demás procesos de la organización está más preparada para afrontar muchos de los riesgos y amenazas que vienen del

exterior y en esta medida llegar a generar mayor confianza entre sus clientes produciendo y entregado los mismos productos y servicios pero siendo ya una organización más confiable y con mayor resiliencia a los ojos de sus clientes y de la competencia misma cuando la comparamos con ellos.

Imagen 16: Organización Sistémica con Continuidad a todo nivel
Fuente: Desarrollo Propio

Un paso más adelante es la implementación de la práctica de la continuidad en toda la organización, en todos sus procesos y en todas la áreas del negocio, es un paso mucho más adelante es una evolución a la que habría que llegar para generar todavía más valor a la empresa, el alcance que hemos dado en el presente proyecto es continuidad de TI pero la organización no debe perder de vista implementar la continuidad en toda la organización.

4.1.1 Antecedentes Técnicos

Las distintas actividades van en secuencia, cada actividad tendrá un tiempo de ejecución que dependerá del tipo y tamaño o de la complejidad de la organización.

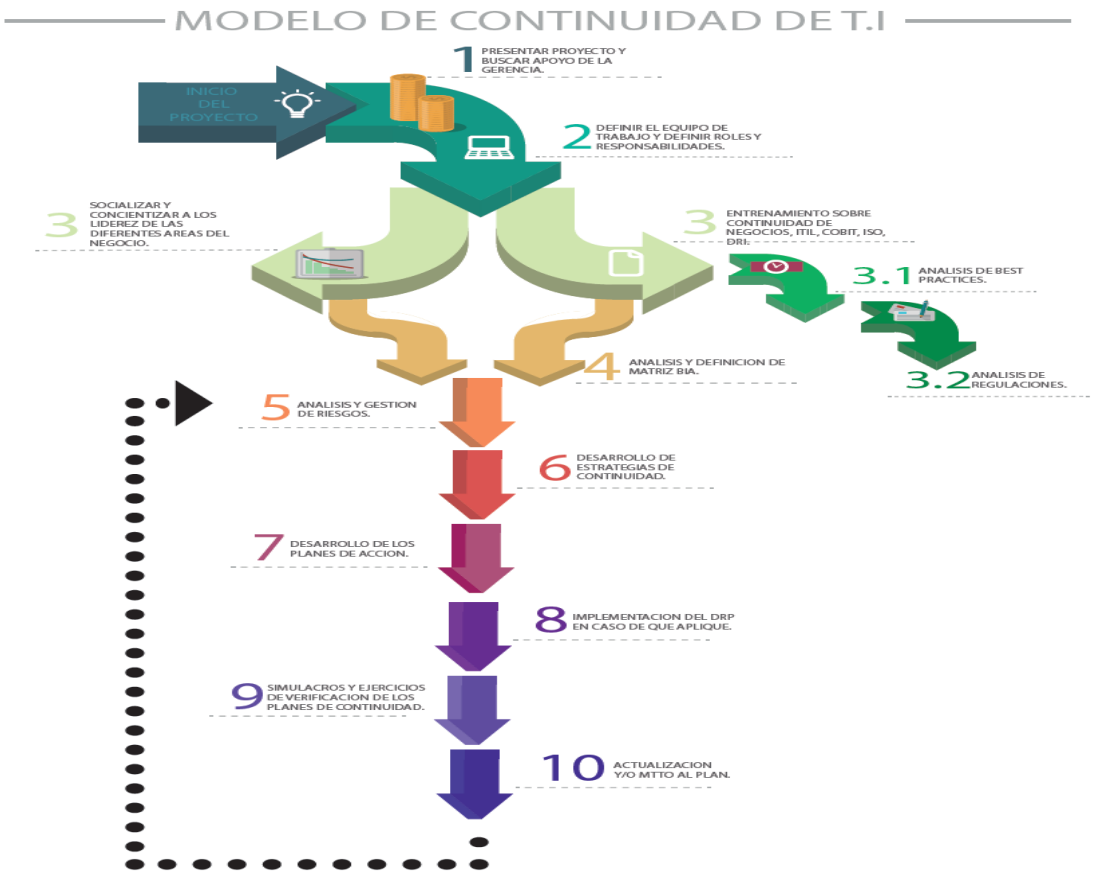


Imagen 17: Modelo de Continuidad Propuesto
Fuente: Desarrollo propio

El modelo como todo sistema se retroalimenta el mismo, esto se hace cuando lleguen los periodos de cambios, sea que estos se den en la infraestructura, en los procesos, en las personas, resultado de los ejercicios de mantenimiento y pruebas del plan y su posterior actualización en los respectivos documentos.

4.1.2 Ventajas del modelo

La ventaja de este modelo es que es un modelo altamente efectivo y busca no ser complejo en exceso. Para facilitar su implementación, lleva un orden lógico en cuanto a las actividades y va acorde a las mejores prácticas del mercado en cuanto a continuidad de TI. Este modelo no recomienda que el cliente debe fielmente seguir una metodología puntal o específica, EJ: Cobit en vez de las normas ISO, o ITIL en vez de la metodología del DRI, en realidad todas las metodologías o frameworks son válidas y han demostrado tener mucha madurez y efectividad, la empresa está en libertad de apoyarse en una metodología o un estándar especifico de la industria si esto le llega a generar más valor o si con esto llegase a sentirse más cómodo, o si por el contrario quiere profundizar mucho más en una práctica especifica de las ya mencionadas, como por ejemplo "manejo de riesgos". Si dentro de la empresa ya hay personal con experiencia en Itil sería de mucho valor el aprovechar ese conocimiento e incorporarlo en la implementación.

4.1.3 Estructura

Es la identificación de las partes o módulos que componen el modelo

4.1.4 Características

Esta propuesta metodológica está compuesta de personas, procesos, procedimientos y tecnología.

El modelo está planteado mediante una serie de pasos, procesos o tareas que deberán seguirse de manera secuencial porque es el orden de "facto" que llevaran al éxito del proyecto, por ejemplo

no podemos comenzar a definir nuevos roles o responsabilidades si previamente no tenemos el soporte y/o el aval de la alta gerencia para la ejecución del proyecto.

Para llevar a cabo un análisis de riesgos es necesario haber definido anteriormente cuales son los servicios críticos de la empresa sobre los cuales nos vamos a enfocar, recordemos que los servicios críticos son aquellos que necesitamos darle continuidad, ya que ante la ausencia de ellos es cuando la empresa deja de ser efectiva, productiva, y comienza con incumplimientos y/o genera insatisfacción y perdida de reputación lo que al final conlleva a perdidas.

El modelo se lleva a la práctica como cualquier otro proyecto, mediante la definición de objetivos, unos requerimientos, unos entregables, un cronograma de trabajo, unos responsables, etc. La diferencia es que generalmente los proyectos tienen un comienzo y un final, pero la aplicación de este modelo es una tarea continua ya que la organización es cambiante en el tiempo, razón por lo cual no hay que dejar de hacer revisión y mantenimiento a los planes y/o estrategias de continuidad, así como también la ejecución de los simulacros y/o ejercicios que se recomiendan llevar a la práctica al menos una o dos veces al año.

4.1.5 Proceso de Implementación

El responsable de iniciar o arrancar con la puesta en marcha o con llevar a la práctica el modelo de continuidad de TI es precisamente el líder o gerente del área de TI de la organización.

Probablemente la idea surja como uno de los prerrequisitos para cumplir con la visión de la empresa y sea este una pieza más del engranaje, probablemente al gerente de TI le sea encomendada la responsabilidad de iniciar con este proyecto, de todas formas es el responsable de TI quien debe comenzar con el proceso.

Lo primero que el gerente de TI debe hacer es la presentación del proyecto a la gerencia donde principalmente se muestren los objetivos, los beneficios, mostrar la problemática y cuál sería la solución, esto debe ir acompañado de un análisis costo beneficio y mostrar claramente a lo que está expuesto la empresa en caso de no ejecutar el proyecto o posponerlo a largo plazo.

Una vez se cuente con el aval de la alta gerencia para continuar con el proyecto se debe designar los roles y responsabilidades, es decir debe haber oficialmente un líder de continuidad, una persona que sea responsable del proyecto de principio a fin, es un como un punto focal “Focal Point”, de ahora en adelante este personaje será el responsable del plan de continuidad y tiene la responsabilidad de llevar el modelo a la práctica.

Este líder de continuidad comenzará a trabajar con los líderes de las demás áreas de negocio, tiene como objetivos socializar el proyecto y crear conciencia sobre el mismo desde todas las áreas de la empresa.

Definir que insumos necesita, sea en capacitación para él o para algunos miembros de su equipo, computadores, papelería para la construcción de formatos etc.

Así mismo será quien se encargue de reunir a los demás líderes de otras áreas para comenzar a definir y documentar cuales son los procesos críticos del negocio y cuáles son los riesgos a los que están expuestos, es decir construir la matriz de impacto al negocio en caso de que esta todavía no exista (Matriz BIA).

Luego de tener construida la matriz BIA se procederá con el análisis de riesgos en torno a los procesos de la matriz BIA y a definir el “tratamiento” que se le da a cada riesgo.

Hay muchos formatos para la matriz BIA, un ejemplo de matriz BIA es el que se relaciona a continuación:

CATEGORIA	SERVICIO	APLICACIÓN	RPO	RTO	CRITICIDAD
Administracion de Cliente	Administracion Base Datos de Clientes	SISTEM1	1 hora	1 hora	alta
		BUKQRY	1 hora	1 hora	alta
		BANCOHORA	1 hora	1 hora	alta
	Comunicaciones Con El Cliente	ATH	1 hora	1 hora	alta
		VIVIENDA	2 horas	2 horas	alta
		LATINA	2 horas	2 horas	alta
		MONITOR TRANSACCIONES	2 horas	2 horas	alta
		JUSTOA HORA	2 horas	4 horas	baja
		PAGINAS AZULES	2 horas	4 horas	baja
	Extractos	sesquinet	30 Mins	4 horas	baja
		oracle	30 Mins	4 horas	baja
		SQL	30 Mins	1 hora	alta
	Gestion de Relaciones con los Cliente	telco	30 Mins	1 hora	alta
		canales	50 mins	1 hora	alta
		Listas Apoyo	50 mins	30 mins	critica
		BI	45 Mins	30 mins	critica
		BI	1 hora	30 mins	critica
		todo1	1 hora	30 mins	critica
		Siebel	45 Mins	30 mins	critica

Tabla 4: Matriz BIA
Fuente: Elaboración Propia

Se coloca uno a uno los servicios prestados por el área de TI, con su aplicación correspondiente y la categoría de servicio al que pertenece, igualmente se coloca el RPO y el RTO máximo permitido y con esta matriz se procederá a definir las estrategias y planes de continuidad para los servicios de criticidad alta y crítica.

Del análisis de riesgo saldrán muchas ideas, opiniones planes etc., la idea es construir estrategias a seguir en caso de que un riesgo se llegase a consolidar.

Hay muchas formas de hacer un análisis de riesgos y muchas fuentes que pueden ser consultadas para generar una matriz de riesgos, un ejemplo de esta matriz es el que se muestra a continuación

RIESGO	PROBABILIDAD DE OCURRENCI	IMPACTO	SEVERIDAD (PROBABILIDAD X IMPACTO)
Falla UPS Datacenter	2 - posible	4 - grande	8 - Medio
Falla Canales de Comunicación	3 - Muy probable	4 - grande	12 - Alto
Falla Energía	2 - posible	15 - excesivo	30 - alarmante
Falla del Core Switch	1 - excepcional	4 - grande	5 - medio
Falla Aires Acondicionados	2 - posible	3 - moderado	6 - medio
Incendio	1 - excepcional	15 - excesivo	15 - muy alto
Falla Generador	2 - posible	3 - moderado	6 - medio
Corrupción de Data	1 - excepcional	15 - excesivo	15 - muy alto
	1 - exepcional	1 - insignifican	1 - 4 bajo
	1 - improbable	2 - pequeño	5 - 10 medio
	2 - probable	3 - moderado	11 - 15 alto
	3 - muy probable	4 - grande	16 - 25 muy alto
	4 - casi seguro	15 - excesivo	25 - 35 alarmante

Tabla 5: Matriz de Riesgos
Fuente: Elaboración Propia

Básicamente consiste en enumerar uno a uno los riesgos que se logren identificar, colocarle una probabilidad de ocurrencia más un impacto y la severidad será el resultado de multiplicar la probabilidad por el impacto, obviamente el desarrollo de estrategías será principalmente para los servicios que resulten con una mayor severidad, es decir alta o muy alta.

La elaboración de los planes de acción son documentos donde se describe el cómo, cuándo, el que, etc. son detalles de los pasos a seguir, como actuar, bajo la dirección de quien, a quien llamar, como se decreta una emergencia, como se activa la contingencia, etc.

En caso de que en la definición de estrategias se haya definido que hay que tener un sitio alterno como contingencia y por ende un DRP (Disaster Recover Plan) o plan de recuperación ante desastres se deberá evaluar bajo que modalidad de las disponibles se puede llegar a implementar.

Una vez definidas las estrategias, los planes de acción, el DRP, en caso de que este se haya considerado, se deberán contemplar simulacros o ejercicios para validar que los planes de acción y las estrategias son consistentes, esto se debería hacer una o dos veces por año dependiendo de los cambios que se hayan dado a nivel de procesos o de infraestructura en la empresa.

El resultado de los ejercicios se deberá analizar, confrontar, cuáles fueron los resultados, si es necesario modificar algo que no funciona, etc. La idea es ir perfeccionando los planes y las estrategias.

Como resultado de lo anterior se deberán actualizar los planes de acción constantemente.

4.1.6 Funcionalidad

El modelo funcionara en la medida en que cuente con el soporte continuo de la alta gerencia, en la medida en que se defina claramente el alcance, las metas y los objetivos que se buscan.

Como ya mencionamos es importante contar con apoyo, es necesario entrenar al personal, es importante concientizar al personal involucrado y socializar el proyecto.

Este es un modelo que se podría implementar y llevar a la práctica en un promedio de 6~12 meses sin DRP, cuando la definición de estrategias arrojan que es necesario implementar un DRP este podría conllevar a más tiempo porque este viene siendo otro proyecto en donde hay que contemplar el sitio alterno, los equipos (hardware), software y/o licenciamiento adicional, canales de comunicación, personal adicional, más costos de administración y/o mantenimiento etc.

Generalmente la implementación de un DRP como resultado de la implementación de un plan de continuidad de TI o de negocios conlleva a una inversión muy grande, algunas empresas del sector obligatoriamente tienen que implementar un DRP como por ejemplos los bancos o empresas del

sector financiero ya que hay regulaciones del gobierno que obligan a esto, otras que no forman parte del sector financiero igualmente necesitan contar con un DRP que garantice la continuidad de sus operaciones en un sitio alterno.

Lo más importante del modelo es llegar a la parte de matriz BIA e identificación de riesgos porque en la medida en que estos se logren identificar se podría implementar algún tipo de acción que de una u otra forma logre minimizar el efecto de los mismos.

Se debe tener en cuenta que el rol de “Líder de Continuidad” no solamente es por el tiempo de la duración del proyecto en sí, esta figura deberá existir por siempre, sea que la persona esté dedicada a esta función exclusivamente o que sea solo una parte de sus funciones en general.

Hay eventos externos que podrían conllevar a la actualización de las estrategias y/o planes de acción y son las nuevas regulaciones del gobierno o los cambios que se den en el área de IT o en la organización en general.

A continuación se observa gráficamente mediante “Canvas” el modelo del negocio.

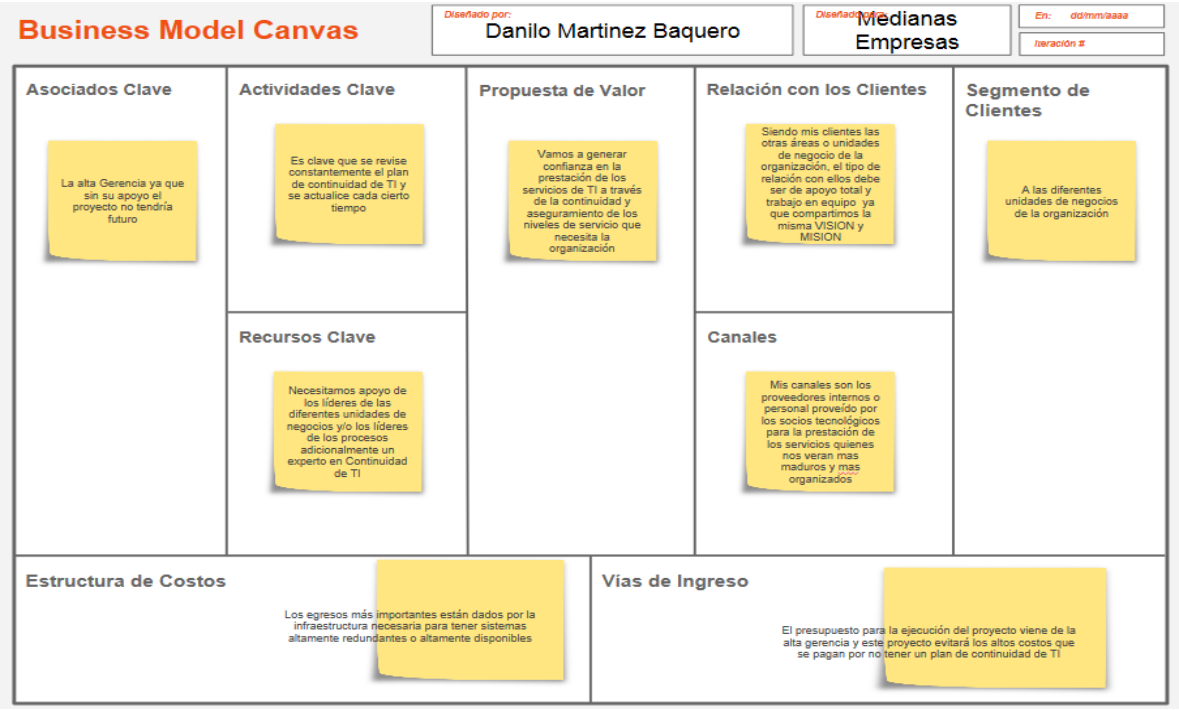


Imagen 19: Modelo de Negocios
Fuente: Desarrollo Propio

4.1.7 Impacto tecnológico

El impacto tecnológico podría resultar alto en la medida en que las estrategias que resulten luego de hacer el análisis de riesgos contemplen la adquisición de nueva tecnología para de esta forma garantizar la continuidad de los servicios críticos de la organización, mediante la aplicación de sistemas altamente redundantes, o a prueba de fallos, se buscaría así eliminar o minimizar los puntos únicos de fallas.

Hay que hacer una buena inversión en tecnología cuando de la definición de las estrategias surja la necesidad de implementar un sitio alterno y un completo plan de recuperación, esto implica adquirir tecnología, hardware y software, sistemas de monitoreo, y prácticamente duplicar algunos

sistemas que a hoy en día están funcionando, esta es la única manera de garantizar casi al 100% la continuidad en caso de eventos altamente críticos.

Sin embargo aquí lo importante es que esto no debe percibirse como un gasto sino como una inversión, se está invirtiendo para tener una compañía más segura, en la cual tanto los proveedores como los clientes puedan confiar y establecer relaciones comerciales.

Dentro de la adquisición y/o arrendamiento que habría que hacer para garantizar continuidad se encuentran entre otros

- Sitio alterno (estructura física) dotado de lo siguiente
- Servidores
- Desktops y laptops
- Almacenamiento
- Sistema de respaldo
- Equipos de comunicaciones
- Teléfonos
- Canales de comunicación
- Sistemas de replicación de datos constante al sitio alterno
- Software
- Licencias
- Sistema contra incendios
- Sistemas de alarmas
- Sistema de video vigilancia

4.1.8 Impacto educativo

Si bien, el personal de TI podría llegar a tener algunos conocimientos sobre el tema de continuidad se hace necesario desarrollar estos conocimientos a profundidad en algunos de los empleados para que igualmente ellos “repliquen” estos conocimientos sobre el resto de la comunidad involucrada en el desarrollo de los planes.

Como ya se ha mencionado hay muchas prácticas y normas internacionales que posiblemente ya se utilicen como parte de otros proyectos u operación en esta empresa, ejemplo el tema de mesa de ayuda apoyado en Itil, en ese caso sería una buena práctica seguir complementando con ese estándar el tema de continuidad si fuera necesario.

Igualmente el personal luego de recibir la capacitación, de desarrollar los conocimientos y ponerlos en práctica buscara obtener las debidas certificaciones en la materia lo que generan aún más valor para ellos y para la empresa.

Lo anterior también significa un diferenciador cuando hay que compararse contra la competencia.

Para socializar y concientizar a la población hay que implementar una serie de actividades que conlleven precisamente a que el personal piense de otra forma en cuanto a la continuidad, esto también es un esfuerzo desde el punto de vista educativo porque se trata de “educar” a los empleados.

4.1.9 Impacto económico

Como ayuda económicamente esta propuesta de un modelo de continuidad a la empresa?

Antes de responder a esta pregunta sería también importante indagar cómo afectaría económicamente a la empresa el hecho de no tener aplicado un modelo o una metodología de

continuidad de negocios. Como ya se ha mencionado anteriormente las consecuencias van desde la perdida de dinero, pérdida de confianza, pérdida de clientes, reducción del valor de la empresa, pérdida de credibilidad y en el peor de los caso la quiebra absoluta.

Emprender y llevar a la práctica un proyecto de este estilo necesita una inversión como todo proyecto, pero es algo que a corto, mediano y largo plazo valoriza a la empresa y evita que la misma enfrente penalidades impuestas generalmente por los entes reguladores, pero lo más importante es que la empresa se vuelve más atractiva, es más valorada, genera confianza y al final los clientes gustan de hacer negocios con este tipo de empresas que demuestran madurez y respaldo.

4.2. Análisis Tecnológico

Las soluciones de continuidad, recuperación ante desastres o alta disponibilidad que involucren un sitio alterno como estrategia de la continuidad se deben manejar como una sola entidad y no como piezas separadas unas de otras, tal como se puede ver gráficamente en la siguiente figura.

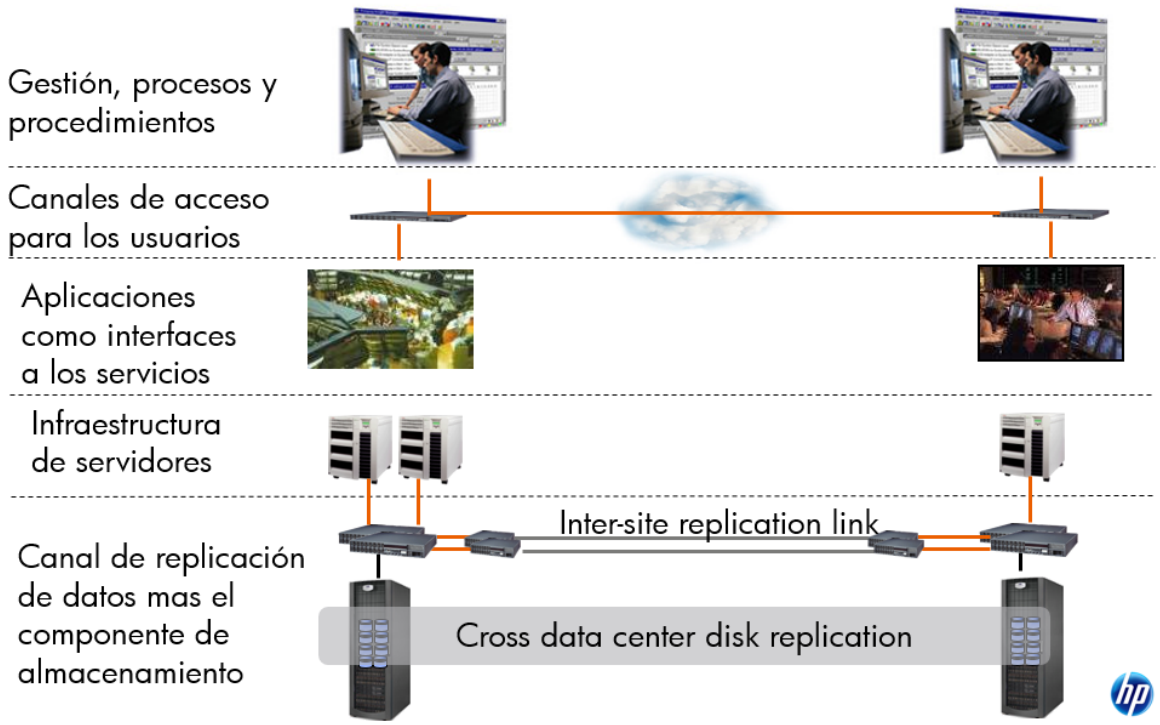


Imagen 18: La continuidad y sus niveles
Fuente: Hewlett Packard Disaster Recovery Readiness Document

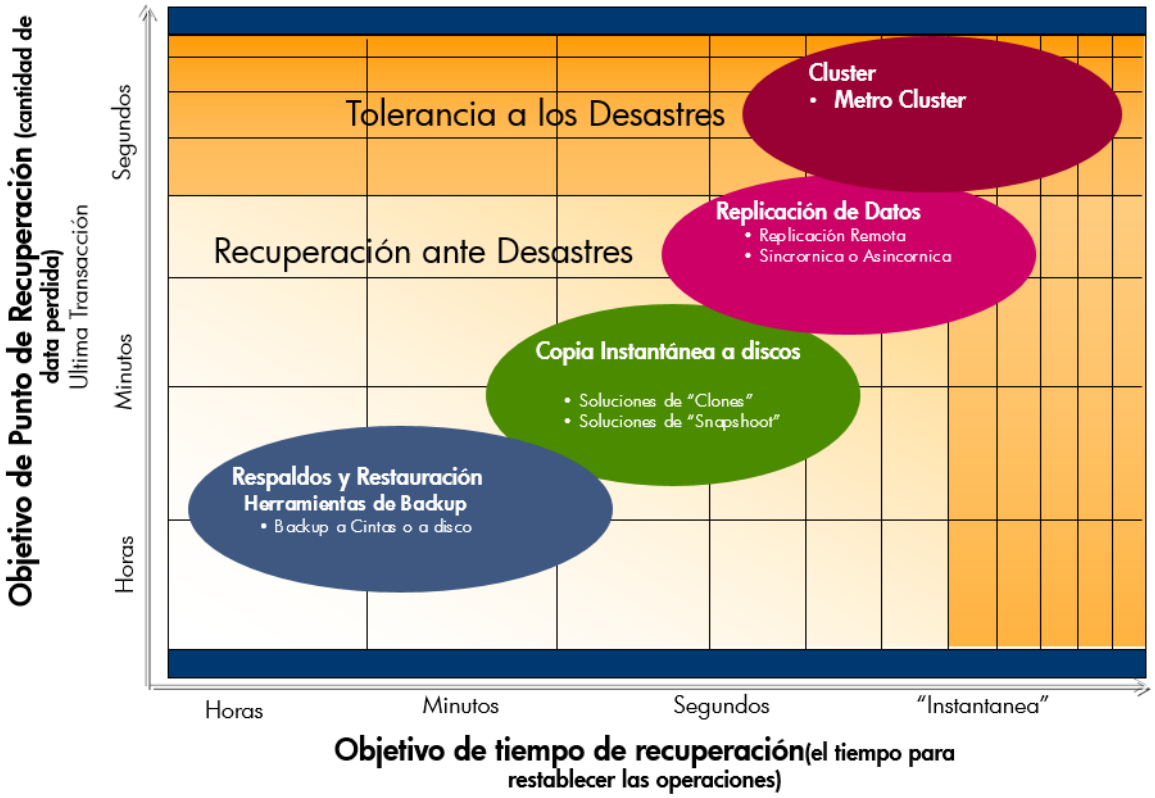


Imagen 21: Las Opciones de Tecnología en la Continuidad
Fuente: Desarrollo Propio

Independientemente de la razón que conlleve a la implementación de un sitio alterno de contingencia, siempre es importante tener presente los siguientes conceptos.

RPO=”Recovery Point Objetive” o Punto de recuperación establecido
RTO=”Recovery Time Objetive” o Tiempo de recuperación establecido

El punto de recuperación establecido o RPO (siglas en inglés) tiene que ver con; “a qué punto hay recuperarse en el tiempo”, es decir, si el desastre en el sitio principal ocurrió a las 12:00pm, los enlaces, los canales, la infraestructura, trabajan tan eficientemente que pudieron replicar toda la data antes del desastre e inclusive las ultimas transacciones hasta unos minutos antes del desastre. Lo anterior es uno de varias escenarios, también hay casos en donde el RPO necesario pudiera

estar cercano a cero, todo esto dependerá de la infraestructura con que se disponga, pero obviamente un RPO cercano a cero necesitaría una mayor inversión al tener que involucrar más tecnología de punta.

Por el contrario echar mano a las estrategias de respaldo hace que el RPO se aleje y se establezca ya no en segundos y minutos sino en horas.

El tiempo de recuperación establecido tiene que ver con el tiempo que la organización invierte en restablecer los servicios en el sitio alterno, igualmente esto podría ser horas, minutos o segundos, ser muy automático o ser muy manual, igualmente dependerá de la tecnología, en el caso de soluciones (hardware y software) de "clustering" la restauración de los servicios desde el sitio alterno podría ser en segundos o minutos, en caso de no contar con este tipo de soluciones y tener que utilizar procedimientos manuales para restablecer los servidores en el sitio alterno esto podría llegar a tomar horas.

Nuevamente llegar a disponer de soluciones "automáticas" como cluster (o metro cluster) necesita de una alta inversión en tecnología.

La siguiente gráfica representa con más detalle lo mencionado anteriormente

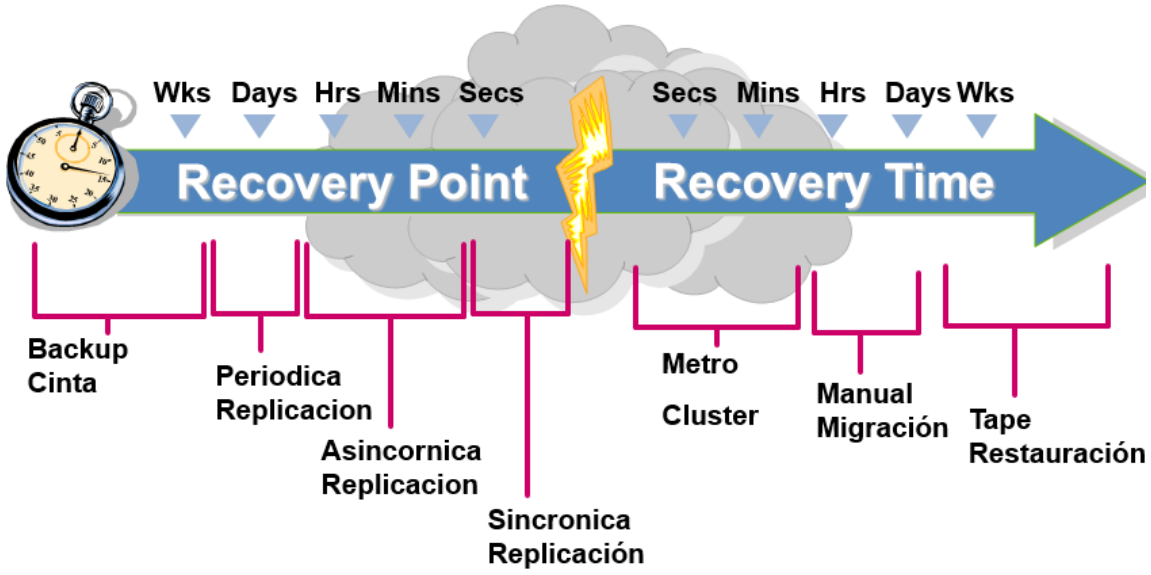


Imagen 22: El Rpo y el Rto
Fuente: Hewlett Packard Disaster Recovery Readiness Document

Tal como se ha visto anteriormente, el disponer de un sitio alterno podría asegurar a la organización la continuidad de sus operaciones en segundos, minutos, horas o días.

4.3. Análisis Financiero

El siguiente análisis financiero para este proyecto, no busca mostrar si la propuesta es una opción viable o no para una empresa en particular, y esto debido a que el modelo o metodología no está planteado para una empresa en particular, no se cuenta con datos financieros específicos para llegar a una conclusión de ese tipo ya que la presente propuesta como se ha indicado desde un principio, es para que pueda ser utilizada por cualquier empresa u organización.

Lo que si busca el análisis financiero es mostrar las diferentes opciones que una empresa tiene para contar con un sitio alterno ante desastres desde donde pueda continuar sus operaciones.

Las dos opciones planteadas, están basadas en modalidad de gastos OPEX y CAPEX es decir optar por pagar un monto periódico (mensual, bimestral, semestral etc.) Por todos los servicios recibidos (la infraestructura y ciertos servicios) u optar por comprar infraestructura y solamente pagar arriendo de algunos servicios como "área blanca", canales de comunicaciones entre otros y pagar el mantenimiento de los equipos.

Opción de compra de equipo (CAPEX), esta opción si bien evita tener que pagar un costo mensual ya que la infraestructura es propia, implica pagar un costo adicional por ser dueño de la propiedad, estos son costos como garantía extendida, mantenimiento, si la infraestructura se vuelve insuficiente hay que ir a un proceso de compra el cual no garantiza tener los equipos en el corto tiempo etc.

ITEM	PERODICIDAD	IMPORTE
Servidores X86 (10)	UNA SOLA VEZ (CAPEX)	$ 150.000.000
Almacenamiento (50 teras)	UNA SOLA VEZ (CAPEX)	$ 100.000.000
Equipo de Redes (5 Switches)	UNA SOLA VEZ (CAPEX)	$ 50.000.000
Software (Base de datos y Middleware)	UNA SOLA VEZ (CAPEX)	$ 30.000.000
Infraestructura de Respaldos (Librería Backup y Software)	UNA SOLA VEZ (CAPEX)	$ 20.000.000
Canal de Comunicación (200mb)	MENSUAL (OPEX)	$ 3.500.000
Arriendo de Area Blanca (Incluye Power, Cooling, racks, Sistema contra incendios)	MENSUAL (OPEX)	$ 24.000.000
	TOTAL SIN TCO	$ 377.500.000

Tabla 6: Capex-1

Fuente: Desarrollo Propio

Esta es una cotización basada en 10 servidores de rango medio, con 50 terabytes de almacenamiento en SAN (Compartido), 5 Switches Lan a 1Gb, una infraestructura de respaldo con una librería de 4 drives LTO6 y software de respaldo y el arriendo de la llamada “área blanca” para tener los equipos instalados.

Si la empresa no quiere incurrir en grandes inversiones para no endeudarse o para no quedarse sin capital puede optar por la opción de OPEX (1) en donde no compra los equipos pero hay un proveedor que pone a disposición la infraestructura con un costo mensual sea que lo use o no lo use, es decir sea que se presente un evento o no en donde tenga que operar desde el sitio alterno.

SI bien es una opción que a simple vista haría que cualquier decisión se oriente por CAPEX ya que se paga menos al momento de adquirir los equipos y los mismos son propios, es importante tener en cuenta que aquí con OPEX (1) no hay gastos de TCO (Total Cost of Ownership) o costo

total de propiedad, lo cual hace que esta segunda opción sea muy atractiva al momento de hacer los cálculos financieros. Los equipos siempre están disponibles pero pueden ser compartidos con otros clientes, es decir no son equipos dedicados y esperando todo el tiempo por un evento de continuidad de un cliente especifico.

ITEM	PERODICIDAD	IMPORTE
Servidores x86 (10)	MENSUAL (OPEX)	$ 15.000.000
Almacenamiento (50 teras)	MENSUAL (OPEX)	$ 10.000.000
Equipo de Redes (5 Switches)	MENSUAL (OPEX)	$ 5.000.000
Software (Base de datos y Middleware)	MENSUAL (OPEX)	$ 3.500.000
Infraestructura de Respaldos (Librería Backup y Software)	MENSUAL (OPEX)	$ 2.500.000
Canal de Comunicación (200mb)	MENSUAL (OPEX)	$ 3.500.000
Arriendo de Area Blanca (Incluye Power, Cooling, racks, Sistema contra incendios)	MENSUAL (OPEX)	$ 15.000.000
	TOTOAL MENSUAL	$ 54.500.000

Tabla 7: Opex-1
Fuente: Elaboración Propia

Es importante hacer claridad que si se llega a presentar un evento con un cliente específico el proveedor automáticamente preparara otra infraestructura similar para el evento en que se llegue a presentar otra necesidad al mismo tiempo con otro cliente.

Por último, la opción de OPEX-2 permite pagar una cantidad semanal solamente en el evento de activación del servicio, no hay costo por TCO pero la infraestructura no está disponible de

inmediato, es decir el proveedor establece un tiempo para alistar esta infraestructura desde el momento que el cliente genera la solicitud, es decir el proveedor podría establecer que tendrá la infraestructura lista en 30 o 48 horas lo cual podría no ser viable para algunas empresas debido al alto RTO y el RPO también es alto pues no hay replicación continua y el cliente tendría que usar sus respaldos para hacer Restauración de la información y poder dar servicio.

ITEM	PERODICIDAD	IMPORTE
Servidores x86 (10)	SEMANAL (OPEX)	$ 10.000.000
Almacenamiento (50 teras)	SEMANAL (OPEX)	$ 6.500.000
Equipo de Redes (5 Switches)	SEMANAL (OPEX)	$ 3.500.000
Software (Base de datos y Middleware)	SEMANAL (OPEX)	$ 2.500.000
Infraestructura de Respaldos (Librería Backup y Software)	SEMANAL (OPEX)	$ 1.750.000
Canal de Comunicación (200mb)	SEMANAL (OPEX)	$ 2.500.000
Arriendo de Area Blanca (Incluye Power, Cooling, racks, Sistema contra incendios)	SEMANAL (OPEX)	$ 10.000.000
	TOTOAL SEMANAL X EVENTO	$ 36.750.000

Tabla 8: Opex-2
Fuente Elaboración Propia

El análisis muestra que la opción de OPEX es mucho más económica y manejable debido a que no todas las empresas disponen de capital para hacer una inversión de capital que a veces resulta ser muy sustancial y además de eso los gastos adicionales generados del costo total de propiedad

por lo que se opta por un gasto mensual que viene a ser un gasto operativo y que resulta ser más manejable para algunas empresas.

Por último, este análisis se basa en un análisis con una infraestructura muy específica, hay que tener en cuenta que en la medida en que se requiera más infraestructura los costos pueden ser más elevados.

Solamente CAPEX y OPEX-1 permiten tener una replicación constante garantizando un RPO cercano a cero.

Este análisis financiero busca más que todo mostrar las diferentes opciones disponibles en el mercado, los SLAs, y los costos a los que habría que incurrir.

A manera de información es importante tener en cuenta la terminología técnica en cuanto a las diferentes opciones disponibles en el mercado y por las cuales se puede optar.

- Hot Site; se refiere a un sitio o área de computo listo para operar en muy pocas horas o minutos ya que tiene toda la infraestructura, la data ha estado replicándose, los servidores y equipos de comunicaciones se encuentran listos y solamente se están en espera de la declaración de emergencia para abandonar el sitio primario o para hacer el "switch" desde el sitio primario al sitio alterno, en este caso referenciado como "Hot Site"
- Warn Site; se refiere a un sitio o área de computo que puede comenzar a operar en menos de un día ya que se encuentra parcialmente configurado, con conexiones de red y equipo de cómputo.
- Cold Site; se refiere a un sitio o área de computo que puede tardar en operar más allá de un día pues si bien tiene cierta infraestructura básica es necesario instalar algunos equipos,

comenzar a restaurar data desde los respaldos y esta tarea podría llegar a estimarse en varios días dando servicio progresivamente.

Por último y llegado el momento de evaluar la viabilidad financiera de la implementación de este tipo de proyectos y teniendo la información financiera de la empresa específica con que se quiere trabajar se hace muy importante realizar la estimación mediante algunas herramientas como son la TIR y el VPN, para esto presentamos una breve reseña de estos dos métodos estimativos tal como aparecen expuestos en el documento de "Metodología de Proyectos" que nos ha sido entregada como insumos para la ejecución del proyecto.

MÉTODO DEL VALOR PRESENTE NETO (VPN)

El método del Valor Presente Neto es muy utilizado por dos razones, la primera porque es de muy fácil aplicación y la segunda porque todos los ingresos y egresos futuros se transforman a pesos de hoy y así puede verse fácilmente, si los ingresos son mayores que los egresos. Cuando el VPN es menor que cero implica que hay una pérdida a una cierta tasa de interés o por el contrario si el VPN es mayor que cero se presenta una ganancia. Cuando el VPN es igual a cero se dice que el proyecto es indiferente. La condición indispensable para comparar alternativas es que siempre se tome en la comparación igual número de años, pero si el tiempo de cada uno es diferente, se debe tomar como base el mínimo común múltiplo de los años de cada alternativa.

En la aceptación o rechazo de un proyecto depende directamente de la tasa de interés que se utilice. Por lo general el VPN disminuye a medida que aumenta la tasa de interés.

METODO DE LA TASA INTERNA DE RETORNO

Este método consiste en encontrar una tasa de interés en la cual se cumplen las condiciones buscadas en el momento de iniciar o aceptar un proyecto de inversión. Tiene como ventaja frente a otras metodologías como la del Valor Presente Neto (VPN) o el Valor Presente Neto Incremental (VPNI) porque en este se elimina el cálculo de la Tasa de Interés de Oportunidad (TIO), esto le da una característica favorable en su utilización por parte de los administradores financieros.

La Tasa Interna de Retorno es aquélla tasa que está ganando un interés sobre el saldo no recuperado de la inversión en cualquier momento de la duración del proyecto. En la medida de las condiciones y alcance del proyecto estos deben evaluarse de acuerdo a sus características, con unos sencillos ejemplos se expondrán sus fundamentos. Esta es una herramienta de gran utilidad para la toma de decisiones financiera dentro del sistema y organización

COSTO ANUAL UNIFORME EQUIVALENTE (CAUE)

El método del CAUE consiste en convertir todos los ingresos y egresos en una serie uniforme de pagos. Obviamente, si el CAUE es positivo, es porque los ingresos son mayores que los egresos y por lo tanto, el proyecto puede realizarse; pero, si el CAUE es negativo, es porque los ingresos son menores que los egresos y en consecuencia el proyecto debe ser rechazado.

4.4. Análisis Administrativo

Como se había mencionado previamente, la implementación de la continuidad de TI hace que surja la necesidad de contar con nuevos roles en la organización, y uno de los más importantes roles, sea que se esté hablando de la continuidad de TI o se esté hablando de la continuidad del negocio, este rol será el de "Líder de Continuidad".

Imagen 23: La organización y la Continuidad
Fuente: Elaboración Propia

Con relación al diagrama anterior se hace importante resaltar que el comité de manejo de crisis debe estar conformado por personas claves y con cierta autonomía en la toma de decisiones, generalmente este está conformado por el Gerente de TI, por el gerente general, por los gerentes o líderes de las principales unidades de negocios de la organización, son ellos los que en determinado momento tomaran decisiones ante la materialización de ciertas eventos, producto de amenazas que se hayan materializado y que dictaran los pasos a seguir, por ejemplo una decisión podría ser activar el DRP y dar servicio desde el sitio alterno.

El grupo de respuesta a emergencias o de evaluación de daños, también son personajes que ya tienen una función específica dentro de la organización y que solamente durante una crisis entrarían a hacer una evaluación especifica de los daños que se han presentado para rendir un informe muy puntal.

El líder de continuidad debería ser una persona dedicada solo a esta función, esta es una función importante que necesita dedicación de tiempo casi que completo, sea que estemos hablando de la continuidad del negocio o de la continuidad de TI esta es una posición dentro de la organización que deberá iniciar con el proyecto y tiene entre otras las siguientes responsabilidades.

- Es quien inicia el proyecto mostrando la necesidad de contar con un programa de continuidad de TI o del negocio
- Presenta y obtiene el apoyo por parte de la gerencia del proyecto de continuidad.
- Guiar a los patrocinadores en la definición de objetivos, en la estructura del programa, en las políticas y en la administración de los factores críticos de éxito.

- Definir los requerimientos de presupuesto para la puesta en marcha del programa o del proyecto
- Coordinar y administrar la implementación del programa de continuidad de TI de principio a fin
- Hacer seguimiento y supervisar continuamente la efectividad del programa
- Medir, mostrar métricas y reportar a la gerencia general los avances y/o el estado general del proyecto

Debido a que hay nuevos roles, y que uno de los objetivos es concientizar o socializar la importancia de la continuidad con muchas personas o roles claves dentro de la organización, es importante establecer los requerimientos en cuanto a capacitación que existen alrededor del tema.

El DRI establece una ruta de entrenamiento y certificación que a continuación se expone a manera de información, para los profesionales que deseen incursionar en el tema de continuidad, y de esta forma estar alineados a las prácticas internacionales. Así mismo poder transferir sus conocimientos a los demás miembros de la organización.

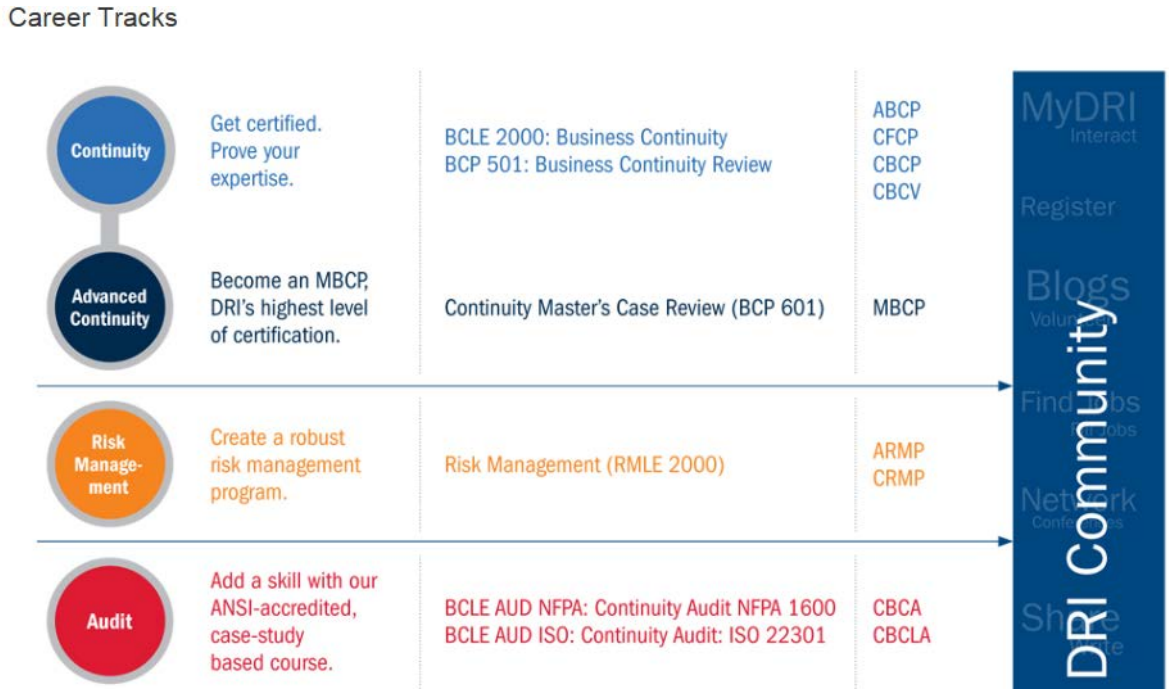


Imagen 24: Entrenamiento y Capacitación

(2017). *Certification*. Recuperado el 25 de 06 de 2017, de DRI International Inc: https://www.drii.org/certificationoverview

El área administrativa de la organización debe ser involucrada en los planes de continuidad porque hay algunas funciones que deberán estar claramente definidas para manejar el tema de la continuidad como por ejemplo:

- Transporte, comida, alojamiento en caso de darse la declaratoria de emergencia real y tener que operar desde el centro alterno, todo esto teniendo en cuenta la ubicación física del sitio designado como contingencia
- Proveer los elementos de comunicación necesarios (teléfonos)
- Organizar juntas, minutas, comunicados de prensa (en caso de que aplique)

5. CONCLUSIONES

Mediante este proyecto se plantea entonces la presentación de un modelo para la implementación de planes de continuidad de TI, con el apoyo obviamente de los sistemas informáticos que sirven de soporte para la puesta en marcha de los planes de continuidad de TI. Cuando se habla del apoyo de los sistemas informáticos, esto se refiere al uso de tecnología, hardware, software, canales de comunicación, licenciamiento e infraestructura de cómputo en general.

Una de las claves del éxito en la implementación del plan de continuidad es lograr identificar claramente todos los riesgos a los cuales está expuesta la organización, si uno de los riesgos es pasado por alto quiere decir que al momento de materializarse posiblemente no estarán preparados para enfrentarlo y/o darle el manejo apropiado.

Al final lo que se busca es que la empresa no se vea afectada por la materialización de un riesgo y que debido a esto tenga que verse enfrentada a una parada de sus operaciones lo cual podría llegar a representar grandes pérdidas financieras y generar desconfianza en los socios de negocios,.

La matriz BIA igualmente debe reflejar exactamente los servicios críticos, y ser actualizada como mínimo cada 6 meses para que se mantenga acorde a la realidad.

Las estrategias y planes de continuidad igualmente deben revisarse cada 6 meses como mínimo ya que los cambios que se den en la organización o en las configuraciones de TI pueden ir dejando desactualizado las estrategias y los planes.

Además de las pérdidas financieras hay algo muy valioso que hay que cuidar y es la imagen y la reputación de la empresa en el mercado, esta imagen y esta reputación se ha cultivado durante

mucho tiempo pero podría verse seriamente afectado en un solo momento en caso de no tener definidas las estrategias y los planes de continuidad.

Si bien en los cronogramas se establecieron unos tiempos más o menos estándar esto puede variar y dependerá del tamaño de TI en la organización y de la organización misma.

Los resultados obtenidos luego de aplicar esta metodología deberían estar relaciones con los objetivos propuestos del proyecto, esto garantizaría buenos resultados.

6. ANEXOS

6.1. Contexto Histórico Social

La propuesta de desarrollo de este modelo de continuidad de TI surge a raíz de la necesidad que tienen hoy en día las empresas en cuanto a minimizar los riesgos a los que el negocio se encuentra expuesto, así mismo evaluar el impacto al negocio de las posibles interrupciones de los servicios de TI, también de la necesidad de establecer estrategias de continuidad que vayan acorde a los planes de continuidad del negocio y finalmente como consecuencia de casos muy conocidos que se suceden alrededor del mundo debido a desastres naturales o de ataques inescrupulosos.

Hace unos 20 años las empresas optaban como contingencia la adopción de políticas de respaldos de la información en diferentes tipos de medios magnéticos, esto si bien resultaba efectivo para salvaguardar los datos, no garantizaba una rápida recuperación, tal vez hace 20 años, el dedicarle un día entero a la recuperación era algo aceptado y normal, pero hoy en día la situación es más

exigente, en años recientes las empresas han buscado alternativas para lograr esa alta disponibilidad que garantice la continuidad de los servicios críticos como por ejemplo las soluciones de cluster, sistemas altamente redundantes etc. Sin embargo hoy en día es claro que la verdadera continuidad se consigue mediante el uso de un sitio alterno y separado geográficamente del sitio primario, puede ser en otra zona de la ciudad, en otra localidad, en otro país o en lo que hoy llaman “la nube”.

Lo anterior surge de los tiempos que la empresa se pone a si misma o que le impone el gobierno o sus clientes, de aquí salen unos nuevos términos como son el RPO (Recovery Point Objetive) o el punto de recuperación como objetivo, es decir a qué punto se van a recuperar, si el sitio primario desapareció y hay que ir al sitio alterno a qué punto se podrían recuperar, a hace 5 minutos? A 1 hora? A 6 horas? Entre más largo sea el punto de recuperación más delicada se vuelve la situación porque se ha podido perder mucha información vital.

Otro término es el de RTO (Recovery Time Objetive) o el tiempo de recuperación como objetivo, es decir cuánto tiempo tomara nuevamente dar servicio desde otro sitio? Es automático? Es manual y toma minutos, horas o días? Igualmente entre más tiempo pase más delicado se vuelve la situación.

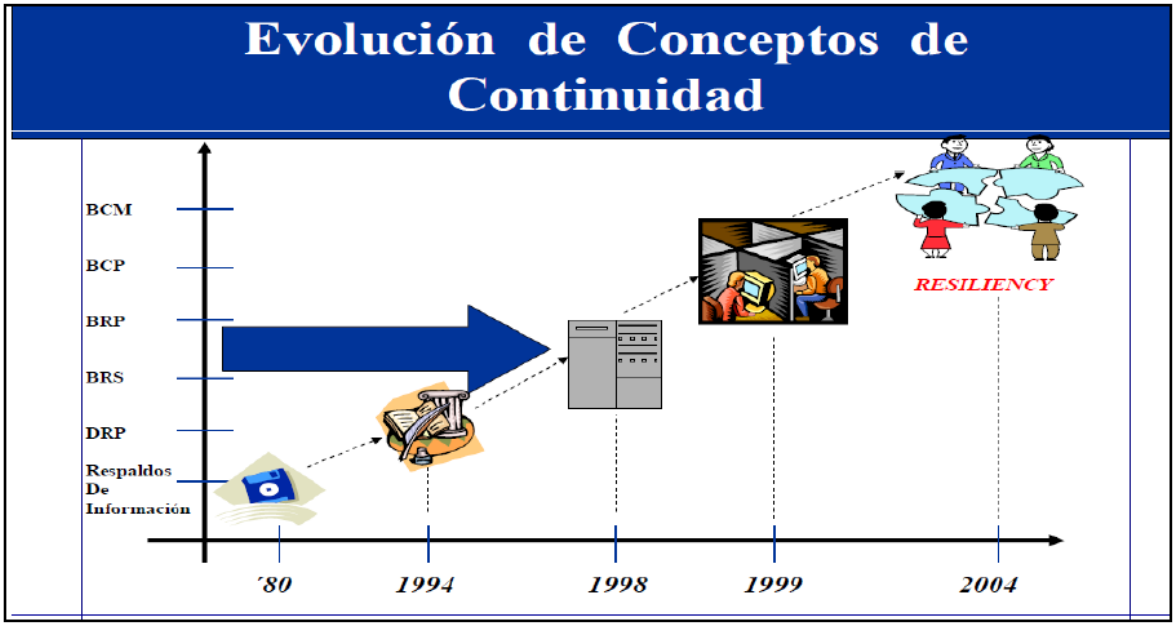


Imagen 25: Evolución de la Continuidad

(2017). *Continuidad*. Recuperado el 25 de 06 de 2017, de Universidad Católica de Colombia: http://repository.ucatolica.edu.co/simple-search?query=continuidad

Lo cierto es que hoy en día las empresas no pueden dejar de operar sin sus sistemas críticos de información.

A través de la historia, las empresas, con el avance de la tecnología han podido planear, analizar y llevar a la práctica diferentes tipos de estrategias que les permitan de una u otra forma enfrentar y salir "airosos" en muchos casos de los eventos que siempre están presentes en el ecosistema.

El modelo propuesto viene básicamente de la experiencia, del contacto con muchas organizaciones, de tener la oportunidad de percibir sus problemas y el manejo que le han dado a sus experiencias, además de trabajar o tener algún tipo de relación con múltiples empresas en donde se hace evidente los problemas y la búsqueda de soluciones. Han sido alrededor de 20 años teniendo contacto con todo tipo de empresas, viendo sus problemas más críticos de perdida de

información y viendo como la mayoría tiene por costumbre trabajar reactivamente en vez de proactivamente.

6.1.1 Impacto social

El impacto social se puede medir como negativo, positivo o nulo.

Definitivamente el impacto social positivo que tiene la implementación de este tipo de proyectos es grande, por el contrario se han visto casos de empresas que al desaparecer dejan una cantidad de personal cesante, lo cual impacta no solo a los empleados directos sino a los indirectos y a todas las personas que de una u otra forma dependen de estas.

Este tipo de proyectos generan confianza en la población, un ejemplo contrario y reciente, es el incendio en la central hidroeléctrica de Guatape en nuestro país, que dejo por fuera la central y Colombia se vio al borde de una crisis energética donde toco empezar a comprar energía a los vecinos y el país expuesto al riesgo de apagones y/o restricciones diarias a la población.

Cuando una empresa cuenta con planes de contingencia para eventos previamente identificados esto crea menos impacto social y genera más confianza.

El establecimiento de planes de continuidad de TI implica el establecimiento de nuevos roles y responsabilidades tanto en el área de TI como en las diferentes áreas claves de la organización, específicamente estamos hablando de aquellos roles que hoy en día que actúan como líderes o dueños de los procesos críticos así como también a la alta gerencia. Lo anterior quiere decir que dependiendo del tamaño de la empresa y su complejidad el organigrama debería mostrar un área de función como lo es la continuidad del negocio y/o de TI.

Al conformarse un equipo de trabajo dedicado exclusivamente a la implementación y seguimiento continuo del plan de continuidad basado en este modelo se crean posiciones nuevas dentro de la organización lo que resulta en requerir más mano de obra.

El establecimiento del modelo generara nuevas políticas y lineamientos acordes a los fines que se persiguen, el personal recibe capacitación, la visión de la empresa tiene más sentido o tendría que reevaluarse debido a los efectos positivos de la implementación del modelo de continuidad que asegura y da larga vida a las operaciones de la empresa, al menos esta resulta blindada a muchos de los eventos que podrían acabar con otras empresas al no adoptar un modelo similar.

6.1.2 Listado Equipamiento para sitio alterno

Este es un listado ejemplo de equipos a adquirir para tener na solución de almacenamiento y respaldo en el sitio alterno, siempre estará sujeta a las necesidades reales de cada organización.

Product Number	Opt Code	Product Description	Qty	Product
A8G55AAE		HP Backup Navigator 10-49TB SW E-LTU	35	Backup
TD586EAE		HP Data Protector 9.00 Eng SW E-Media	1	Backup
TF542AAE		HP DP perTB 10-49TB SW E-LTU	35	Backup
QU625A		HP MSL6480 Scalable Base Module	1	Backup
HA114A1	5UE	HP StoreEver MSL6480 Base M Startup SVC	1	Backup
C0H28A		HP MSL LTO-6 Ultr 6250 FC Drive Upg Kit	4	Backup
TC443AAE		HP MSL6480 Data Ver for 100 Cart E-LTU	1	Backup
TC444AAE		HP StoreEver MSL6480 CV-TL E-LTU	1	Backup
TC445AAE		HP StoreEver MSL6480Tapeassure Adv E-LTU	1	Backup
H1K94A3	QC1	HP MSL TapeAssure Adv Lic SW Supp	1	Backup
H1K94A3	QC6	HP MSL6480 Base Support	1	Backup
H1K94A3	QC8	HP MSL6480 Cmand Vew TL SW Sup	1	Backup
H1K94A3	SQ3	HP MSL6480 Data Verification SW Support	1	Backup
BB878A		HP StoreOnce 4500 24TB Backup	2	Backup
BB881A		HP StoreOnce 4500/4700 24TB Upgrade Kit	1	Backup
BB909A		HP StoreOnce 4500 48TB Upgrade Kit	1	Backup
H1K94A3	28A	HP StoreOnce43/45/4700 Cap Upg Kit Supp	1	Backup
H1K94A3	9LA	HP StoreOnce 41/4500 Backup System Supp	2	Backup
H1K94A3	ST7	HP StoreOnce 4500 48TB Upgrade Supp	1	Backup
HA113A1	5KK	HP StoreOnce Basic Installation SVC	4	Backup
HA124A1	55Q	HP Startup StoreOnce Backup System SVC	1	Backup
HA124A1	55R	HP Startup StoreOnce Additional SVC	1	Backup
HA124A1	5UZ	HP StoreOnce Cap Kit Startup SVC	1	Backup

Product Number	Opt Code	Product Description	Qty	Product
E7X02A		HP 3PAR StoreServ File Cntl v2 Strg	1	Storage
656596-B21		HP Ethernet 10Gb 2P 530T Adptr	2	Storage
656596-B21	0D1	Factory integrated	2	Storage
AJ763B		HP 82E 8Gb Dual-port PCI-e FC HBA	1	Storage
AJ763B	0D1	Factory Integrated	1	Storage
H1K94A3		HP 3Y 6 hr CTR Proactive Care SVC	1	Storage
H1K94A3	SQ0	HP 3 Par StoreServ FileControllerv2 Supp	1	Storage
HA114A1		HP Installation and Startup Service	1	Storage
HA114A1	5AM	HP StoreEasy 1000/3000 Startup SVC	1	Storage
E7X67A		HP 3PAR StoreServ 7200c 2N Fld Int Base	1	Storage
QR486A		HP 3PAR 7000 4-pt 8Gb/s FC Adapter	2	Storage
E7X49A		HP M6710 1.2TB 6G SAS 10K 2.5in HDD	12	Storage
E7Y55A		HP M6710 480GB 6G SAS 2.5in cMLC SSD	4	Storage
E7X64A		HP M6710 SFF(2.5in) SAS Fld Int Drv Encl	1	Storage
HA114A1		HP Installation and Startup Service	1	Storage
HA114A1	5TP	HP Startup 3PAR 7200 2-Nd Strg Base SVC	1	Storage
HA114A1	5TT	HP Startup 3PAR 7000 FC Adapter SVC	2	Storage
HA114A1	5TV	HP Startup 3PAR 7000 2U SAS Enclosre SVC	1	Storage
E7X49A		HP M6710 1.2TB 6G SAS 10K 2.5in HDD	12	Storage
E7Y55A		HP M6710 480GB 6G SAS 2.5in cMLC SSD	4	Storage
QR516B		HP 3PAR 7000 Service Processor	1	Storage
BC745BAE		HP 3PAR 7200 OS Suite Base E-LTU	1	Storage
BC746AAE		HP 3PAR 7200 OS Suite Drive E-LTU	48	Storage
BC747AAE		HP 3PAR 7200 Replication Ste Base E-LTU	1	Storage
BC748AAE		HP 3PAR 7200 Replication Ste Drive E-LTU	48	Storage
BC767BAE		HP 3PAR 7200 Reporting Suite E-LTU	1	Storage
BD268AAE		HP 3PAR 7200 Data Opt St v2 Base E-LTU	1	Storage
BD269AAE		HP 3PAR 7200 Data Opt St v2 Drive E-LTU	48	Storage

BD362AAE		HP 3PAR StoreServ Mgmt/Core SW E-Media	1	Storage
BD363AAE		HP 3PAR OS Suite E-Media	1	Storage
BD365AAE		HP 3PAR Service Processor SW E-Media	1	Storage
BD373AAE		HP 3PAR Reporting Suite E-Media	1	Storage
H8B37A3		HP 3Y 6 hour CTR Proactive Care Adv SVC	1	Storage
H8B37A3	RD0	HP 3PAR 7200 OS Suite Base LTU Supp	1	Storage
H8B37A3	RD1	HP 3PAR 7200ReplicationSuiteBaseLTU Supp	1	Storage
H8B37A3	RDB	HP 3PAR 7200 Reporting Suite LTU Supp	1	Storage
H8B37A3	RZ5	HP 3PAR 7000 Service Processor Supp	1	Storage
H8B37A3	S6L	HP 3PAR 7200 OS Suite Drive LTU Supp	48	Storage
H8B37A3	S6M	HP 3PAR 7200 Replic Suite Drive LTU Supp	48	Storage
H8B37A3	S7B	HP 3PAR 7200 DataOpt St v2 Base LTU Supp	1	Storage
H8B37A3	S7C	HP 3PAR 7200 Data Opt St v2 Drv LTU Supp	48	Storage
H8B37A3	TPJ	HP 3PAR 7000 480GB SAS cMLC SSD HW Supp	8	Storage
H8B37A3	TRE	HP 3PAR StoreServ 7200c2NStrgbase HWSupp	1	Storage
H8B37A3	WSF	HP 3PAR Internal Entitlement Purpose	4	Storage
H8B37A3	WUT	HP 3PAR 7000 Drives over 1TB Support	24	Storage
H8B37A3	WUW	HP 3PAR 7000 Drive Enclosure Support	1	Storage
H8B37A3	WUX	HP 3PAR 7000 Adapter Support	2	Storage
H5M58A		HP 4.9kVA 208V 20out NA/JP bPDU	4	Storage
HA113A1		HP Installation Service	1	Storage
HA113A1	5BW	ProLiant Add On Options Installation SVC	4	Storage
HA124A1		HP Technical Installation Startup SVC	1	Storage
HA124A1	5TM	HP Startup 3PAR 7000 Reporting Ste SVC	1	Storage
HA124A1	5UG	HP Startup 3PAR 7000 Data Opt Ste v2 SVC	1	Storage
UW316AS		HP Proactive Select Service	1	Storage
HK696A1		HP 1Y Proactive Select 10 Credit SVC	4	Storage
HK696A1	2BT	HP Proactive Select Credit SVC	4	Storage
U4VT2AS		HP PCA Proactive Credits Per Year SVC	10	Storage
E7X02A		HP 3PAR StoreServ File Cntl v2 Strg	2	Storage

656596-B21		HP Ethernet 10Gb 2P 530T Adptr	2	Storage
656596-B21	0D1	Factory integrated	2	Storage
AJ763B		HP 82E 8Gb Dual-port PCI-e FC HBA	2	Storage
AJ763B	0D1	Factory Integrated	2	Storage
H1K94A3		HP 3Y 6 hr CTR Proactive Care SVC	1	Storage
H1K94A3	SQ0	HP 3 Par StoreServ FileControllerv2 Supp	2	Storage
HA114A1		HP Installation and Startup Service	1	Storage

7. BIBLIOGRAFIA

HERKENS, Gary. Gestión de Proyectos. McGraw Hill. Madrid, 2003

GALLARDO CERVANTES, Juan. Formulación y evaluación de proyectos de inversión: un enfoque de sistemas. McGraw-Hill. México. 1998.

SAPAG CHAIN, Nassir, Reinaldo. Fundamentos de preparación y evaluación de proyectos. Tercera edición. Editorial Mc Graw Hill. España, 1995.

MÉNDEZ LOZANO, Rafael Armando. Formulación y evaluación de proyectos. Fotolito Herbol Ltda. Segunda Edición. Colombia. 2000.

HERNANDEZ HERNANDEZ, Abraham, Formulación y Evaluación de Proyectos de Inversión.Thomson.México, 2001.