UNIVERSIDAD APEC
UNAPEC

DECANATO DE INGENIERÍA E INFORMATICA
ESCUELA DE INFORMATICA

Implementación de un plan de Recuperación de Desastres para Empresas de Call Center en la República Dominicana. "Caso Stream Global Services"

Sustentantes:

Cristian Ariel Pérez Cleto **2000-2513**
Mario De Los Santos **2004-0124**

Asesores:

Ramón Gómez
Jacqueline Vega

Monografía para Optar por el Título de:
Ingeniero en Sistemas de Computación

Santo Domingo, D.N
Agosto, 2009

DEDICATORIA

A Dios por darme la luz durante todo este tiempo.

A mi madre Lucila Cleto y mi padre Francisco Pérez por todo el apoyo que siempre me han dado.

A mi esposa Yudilexy Polanco, mis hijos Cristian Emmanuel y Ryan Dariel, por ser mi inspiración y mi razón de existir.

A mis hermanos Randolph, Elizabeth y Wendy, por su lealtad y su apoyó incondicional y por estar conmigo en todos los momentos cuando los he necesitado.

Cristian Ariel Pérez Cleto

INDICE

RESUMEN

El objetivo principal de una empresa es buscar el éxito y cumplimiento de sus metas con el cliente y sus productos ofreciendo calidad y eficiencia, pero ninguna compañía está libre de riesgos, puede perder sus productos por un incendio, paralizar sus operaciones por atentados, entre otros riesgos.

Este trabajo consistió en el Diseño un Plan de Recuperación de Desastres que permita garantizar que los recursos tecnológicos no afecten los servicios que provee la empresa Stream Global Services al exterior y los procesos críticos internos operen a un nivel aceptable durante un evento de crisis y logren su normalidad después de ésta.

Durante la elaboración de este plan se definieron los conceptos que sirvieron como pautas para elaboración del plan de recuperación de desastres, además se Investigo la importancia que radica en el diseñar e implantar un DRP.

Por lo que se hizo una delimitación de los procedimientos del plan de recuperación de desastre, explicando lo que engloba cada fase durante el desarrollo de la misma, desde fase del análisis de impacto y de riesgos, precedidos por el el desarrollo del plan, hasta el desarrollo del mantenimiento y actualización del mismo.

En esta monografía también se describieron, analizaron y detallaron los procesos críticos que conforman la empresa, y que son de suma importancia para la sobre vivencia de esta en caso de desastres.

Por otra parte se realizó una lista activos, enfocando sus principales amenazas y vulnerabilidades con la finalidad de establecer su nivel de criticidad dentro de la organización y de esta forma determinar su nivel de riesgo en cada uno de ellos.

Se presentaron controles y medidas para mitigación de los efectos causados por un eventual desastre, mediante la adecuada planeación y control.

Finalmente se establecieron estrategias para la puesta en marcha del plan de recuperación de desastres en caso de ser activado.

INTRODUCCION

A medida que las empresas son más dependientes de la tecnología y luchan en escenarios complejos debido a la globalización, se hacen más susceptibles a que una serie de amenazas puedan penetrar sus vulnerabilidades y causarles daño, al grado de sacarlas de circulación.

Dentro de la Gestión de la Seguridad de la Información en una compañía es importante contar con un plan alternativo que asegure la continuidad de la actividad del Negocio en caso de que ocurran incidentes graves.

Tradicionalmente, los *Planes de Recuperación de Desastres*, denominados Planes de Contingencia en sus orígenes, están asociados a grandes compañías que necesitan reaccionar de forma inmediata ante cualquier evento que interrumpa sus servicios. La realidad es que cualquier compañía puede sufrir un incidente que afecte a su continuidad y, dependiendo de la forma en que se gestione dicho incidente, las consecuencias pueden ser más o menos graves.

Un Plan de Recuperación de Desastre se refiere a todo lo relacionado con la preparación y respuesta cuando un desastre sucede. El objetivo principal del mismo es la supervivencia de la organización centrándose principalmente en la recuperación de su infraestructura tecnológica.

Este estudio se centro en el diseño de un Plan de Recuperación de Desastres para una empresa de Call Center ubicada en el Distrito Nacional, Republica Dominicana.

En el mimos se incluyen los siguientes tipos de investigación: Documental, Descriptivo, Estudio de Campo e Histórico. Las técnicas empleadas para la recolección de las informaciones fueron a través de entrevistas a personas relacionadas con las empresas y expertos sobre el tema. También se aplicó la revisión literaria, ya que se investigó en libros, monografías, entre otras fuentes.

Algunos de los métodos utilizados en el estudio son: la observación en las instalaciones de la empresa investigada. Además, se llevaron a cabo diferentes análisis, tales como: de impacto, riesgo, entre otros; que son parte de la estructura de un plan de recuperación de desastres (DRP).

Cada capitulo se aborda de manera deductiva, partiendo de lo general a lo especifico, mostrando primero teorías generales sobre el plan de recuperación de desastres y luego analizando la situación de la empresa en cuestión.

Capitulo I.

Stream Global Services

Capitulo I.
STREAM GLOBAL SERVICES

En este capitulo se expone todo lo relacionado con la empresa objeto de este estudio, tales como, antecedentes, misión, visión valores, estructura organizacional, objetivos, entre otros. La mayoría de las informaciones presentadas fueron extraídas de la página virtual de la compañía aquí estudiada.

1.1 Antecedentes

Como empresa dedicada al negocio de Contact Centers en todo el mundo, Stream cuenta con una amplia experiencia, estabilidad y personal cualificado para llevar a cabo su misión corporativa de proporcionar experiencias excepcionales al cliente. En los últimos 20 años, Stream ha crecido como un socio, junto con los mercados de altas tecnologías a los que presta servicio, ya que entiende las necesidades de sus clientes y la importancia del servicio de atención al cliente en el ámbito del soporte técnico.

El resultado es el conocimiento integral que hoy tienen del negocio y su flexibilidad para afrontar nuevos desafíos.

La perspectiva de futuro de Stream incluye la expansión a nuevos países, la dedicación continua para lograr la satisfacción del cliente y la innovación de sus servicios de soporte.

Esta perspectiva los llevo a abrir sus instalaciones en la Republica Dominicana, con ya 3 sucursales en la Ciudad Capital, Stream Santo Domingo ofrecen una tentadora alternativa para los mercados en idiomas inglés y español. En Santo Domingo, la versatilidad es su punto fuerte pues ofrecen atención al cliente y asistencia técnica tanto en inglés como en español.

Sus tres (3) instalaciones en Santo Domingo ubicadas en San Isidro, Avenida Tiradentes y su ubicación dentro de Cyberpark (Parque Cibernético) aprovechan el hecho de que sea la mayor ciudad de la República Dominicana, con una población de 2,9 millones de habitantes. La alta tasa de alfabetización del país genera otra ventaja en una ciudad en la que se habla inglés extensamente. Asimismo, el gobierno local apoya la inversión nacional en educación y formación de la fuerza de trabajo.

1.2 Visión, Misión y Valores

1.2.1 Visión

La *visión* como estado futuro que se pretende alcanzar dentro de una organización debe enmarcar las metas y direcciones a seguir por esta[1].

[1] www.wikipedia.com

La visión de Stream es de ser la principal empresa de servicios de subcontratación, al integrar sus procesos de negocios a nivel global y de esta forma continuamente enriquecer las valiosas proposiciones de sus clientes.

1.2.2 Misión

Se entiende como *misión empresarial* "La definición específica de lo que la empresa es, de lo que la empresa hace (a qué se dedica) y a quién sirve con su funcionamiento. Representa la razón de ser de la empresa; orienta toda la planificación y todo el funcionamiento de la misma; y se redacta estableciendo: La actividad empresarial fundamental; El concepto de producto genérico que ofrece; El concepto de tipos de cliente a los que pretende atender"[2].

Stream Global Services posee como misión el continuamente proveer a sus clientes innovadoras soluciones de servicios para crear el valor máximo para sus consumidores.

1.2.3 Valores

Se entiende que el *valor* es una cualidad que permite ponderar el valor ético o estético de las cosas, por lo que es una cualidad especial que hace que las cosas sean estimadas en sentido positivo o negativo, estas cualidades son exactamente las que posee y busca mantener Stream Global Services y como parte de los valores que tratan de sostener dentro de la empresa poseen los siguientes:

[2] Diccionario de la Real Academia de la Lengua Española.

- Integridad y honradez
- Pasión por el éxito de sus clientes
- La constante búsqueda de la excelencia de servicio
- Innovación a través de sus prácticas empresariales y el servicio del cliente.
- Compromiso de proporcionar oportunidades de crecimiento personal y de liderazgo.
- Responsabilidad de crear valores para sus empleados, clientes, socios y accionistas.

1.3 Estructura Organizacional

La *estructura organizacional* no es más que la manera en que se dividen, agrupan y también coordinan las actividades de la organización en lo referente a las relaciones entre los gerentes y los empleados, entre gerentes y gerentes y entre empleados y empleados.

Debido a que Stream Global Services es una empresa intercontinental, con localidades a través de todo el mundo, es de sumo interés presentar la estructura organizacional de las instalaciones localizadas en el Parque Cibernético de Santo Domingo, ya que, estas son el objeto de estudio en este monográfico.

El gráfico a continuación muestra las diferentes posiciones existentes y el posible flujo de estas.

Figura 1.0 Estructura organizacional de Stream

1.4 Servicios

Las empresas de hoy en día deben centrarse en sus competencias clave, en incrementar la flexibilidad del soporte, en generar beneficios y en reducir los costes de gestión. Estos son los motivos que hacen que muchas empresas externalicen sus servicios de atención al cliente. Dentro de los mercados de alta tecnología a los que Stream presta servicio, estos objetivos tienen una especial

importancia debido a reducción de los márgenes de beneficio, a la creciente complejidad de los productos y al incremento del nivel de exigencia de los clientes.

El grafico a continuación muestra el núcleo de servicios ofrecidos por Stream.

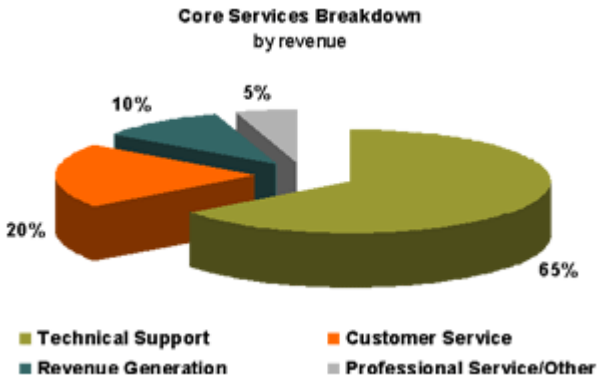


Figura 1.1 Detalle del núcleo de servicios ofrecidos por Stream

1.4.1 Descripción de los Servicios

Los servicios mostrados en la figura anterior se describen a continuación:

- *Soporte Técnico*

El Soporte técnico es un rango de servicios que proporcionan asistencia con el hardware o software de una computadora, o algún otro dispositivo electrónico o mecánico. En general, los servicios de soporte técnico tratan de ayudar al usuario a resolver determinados problemas con algún producto en vez de entrenar o personalizar.

Los profesionales de soporte técnico de Stream abarcan el 65% del total de servicios brindados por esta organización, estos reciben una extensa formación en los productos con los que trabajan, lo que les permite resolver los problemas del cliente de una forma inteligente y precisa.

- *Servicio de Atención al Cliente*

Se comprende como servicio al cliente la asistencia que presta una empresa para relacionarse con sus clientes y contestar cualquier pregunta que tengan estos.

Stream aplica a cada contacto los principios básicos de un gran servicio de atención al cliente, este mercado representa el 20% de sus servicios. Ya se trate de un servicio de activación de una cuenta, registro de un producto, solicitudes de suscripción o de cuentas, registro de clientes, entre otros.

- *Gestión de la Generación de Beneficios de Stream (RGM)*

En el cambiante panorama económico de los Contact Centers, la metodología de Gestión de la generación de beneficios de Stream se desmarca como una oportunidad creciente dentro de los mercados verticales. Sus clientes son capaces de compensar costes, alcanzar un equilibro y crear nuevos canales para generar beneficios.

Stream identifica las líneas de negocio de sus clientes que tienen mayor potencial para generar beneficios y crea soluciones personalizadas para la

satisfacción de sus necesidades, para alcanzar los objetivos económicos y desarrolla las habilidades necesarias para los programas de generación de beneficios.

Por ejemplo, el soporte a los productos de electrónica de consumo ofrece una oportunidad única para la venta de garantías. Al mismo tiempo que los profesionales de soporte resuelven problemas técnicos, utilizan la interacción con el cliente para resaltar los beneficios de una nueva garantía o de la ampliación de la que ya tenían.

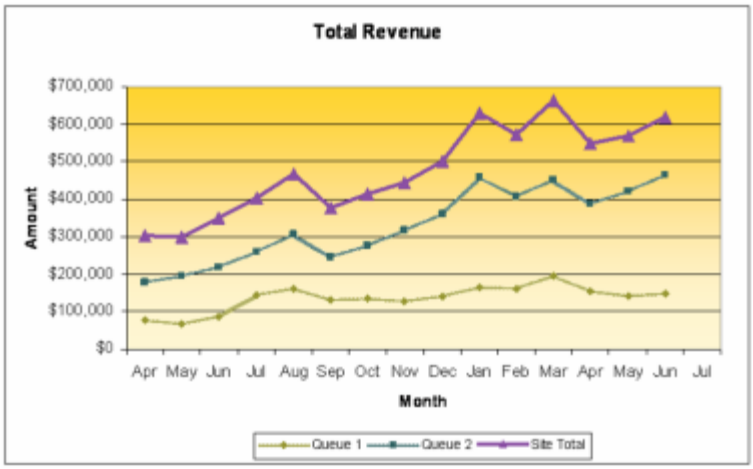


Figura 1.2 Grafico de generación de beneficios

- *Stream Smart Shore*

La localidad de una empresa es algo muy importante, esto envuelve las horas de operaciones en comparación con otro país que pudiera ser afectado por otra zona horaria. El poseer localidades en diferentes países permite a una empresa

cubrir los diferentes horarios de servicio al cliente vía telefónico que pudiese necesitar.

Los clientes de Stream tienen diferentes necesidades relativas al soporte: idiomas, satisfacción del cliente, balance de costes, continuidad de negocio y cobertura en distintas zonas horarias. En muchos casos, un sólo centro no puede hacer frente a todas estas necesidades. Stream Smart ShoreSM, que es la metodología de provisión global, busca la mejor solución geográfica y adecuan los objetivos sus clientes a las necesidades de los suyos.

Esta metodología tiene en cuenta una serie de variables que incluyen el tipo de servicio, el canal de contacto, la complejidad, la estabilidad del producto, entre otros. Algunos de los elementos fundamentales de Smart ShoreSM de Stream incluyen una conjunción de centros en la zona geográfica del cliente (onshore), en emplazamientos cercanos (nearshore) y en lugares más alejados que tienen muy en cuenta factores como el idioma, la afinidad cultural, las distintas zonas horarias y los objetivos generales del cliente a la hora de externalizar el servicio.

Capitulo II.

Plan de Recuperación de Desastres (DRP)

Capitulo II.
PLAN DE RECUPERACIÓN DE DESASTRES (DRP)

En la actualidad casi la totalidad de los productos y servicios que son solicitados por la sociedad son proporcionados por las organizaciones, para estas, es muy importante garantizar a sus clientes un adecuado nivel de seguridad, disponibilidad y confiabilidad de los procesos que son esenciales para el funcionamiento de su empresa, de tal manera que se asegure la continuidad de su negocio. Esta disponibilidad se puede ver afectada por factores accidentales, incidentales y humanos.

En el atentado del 11 de septiembre del 2001, un gran número empresas fracasaron por la falta de un plan de recuperación de desastres. Esto creó la necesidad de que actualmente las organizaciones estén implementando mecanismos y/o técnicas, que mitiguen los riesgos a los que se está expuesto, brindando una alta disponibilidad en las operaciones de su negocio

2.1 Concepto de DRP

Un plan de recuperación de desastres (DRP) se define como un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los servicios informáticos críticos en caso de contingencia. Su propósito es obtener un mapa de acciones que reduzcan “la toma de decisiones” durante las operaciones de recuperación, restáure los servicios críticos

rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costos y aumentado la efectividad.

2.2 Cuando Aplicar un Plan de Recuperación de Desastres (DRP)

- Si falla alguno de sus sistemas críticos y/o si se contamina alguno de sus sistemas críticos con información no compatible proveniente del exterior.
- Si falla algún sistema de telecomunicaciones o enlace.
- Si falla alguno de sus proveedores informáticos clave.
- Si falla alguno de sus otros proveedores clave.
- Si falla algún servicio básico.
- Si se presentan fallas encadenadas y generalizadas
- Si colapsa el centro de cómputos.

2.3 Ventajas del Plan de Recuperación de Desastres (DRP)

- Señala los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Precisa a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Especifica los activos para priorizar su protección en caso de desastre.

- Contribuye una ventaja competitiva frente a la competencia.
- Promueve e implica a los recursos humanos de la compañía en las actividades de continuidad.

2.4 Fases del DRP

Para la realización del plan de resuperación de desastres se deben desarrollar las siguientes fases:

- *Fase 1:* Análisis de Riesgo y Evaluación de Riesgos.
- *Fase 2.* Selección de Estrategias.
- *Fase 3:* Desarrollo del DRP
- *Fase 4:* Programa de Capacitación y Concientización.
- *Fase 6 Plan de Comunicación Ante Crisis.*
- *Fase 7:* Pruebas y Ejercicios.
- *Fase 8:* Mantenimiento y Actualización.

Capitulo III.

Análisis de Impacto y Evaluación de Riesgos.

Capitulo III.
ANÁLISIS DE IMPACTO Y EVALUACIÓN DE RIESGOS.

Este capítulo comprende todo lo relacionado con la fase No.1 del Plan de Recuperación de Desastres, como es: el análisis de impacto y el análisis de riesgo. Primeramente, se abordarán las teorías que constituyen cada tema, para luego aplicar dicha fase a la empresa objeto de esta investigación.

3.1 Análisis de Impacto.

El Análisis de Impacto es esencial para establecer una estrategia de recuperación, que en principio dará continuidad a las actividades críticas y posteriormente al resto, si es posible.

El nivel de criticidad de una actividad dentro de la compañía se mide en función de lo dependiente de ella que es la organización y de lo que repercutiría su indisponibilidad. Dentro del análisis de impacto se distinguen las siguientes actividades:

1. *Relación de los Procesos:*

Los Procesos de negocios o simplemente procesos, son las actividades que una organización realiza para dar soporte a su principal propósito: Brindar y producir bienes y o servicios.

Se pueden dividir los procesos en operativos y procesos de soporte. Los *procesos operativos* son aquellos que guardan una relación directa con el cliente (comercial, facturación, almacenaje, atención al cliente, etc.). Los *procesos de soporte*, serían aquellos que facilitan los “recursos” para poder realizar los procesos operativos (recursos humanos, gestión financiera, etc.).

2. *Relación de las Aplicaciones.*

En este apartado debe recogerse el inventario de los recursos tecnológicos que soportan los procesos de la compañía, a fin de identificar aquellos que den soporte directo a los servicios críticos.

3. *Relación de Departamentos y Usuarios:*

Los procesos de la compañía están gestionados por departamentos/usuarios. Dentro del inventario de procesos es necesario conocer el personal involucrado en los mismos. Esta información puede obtenerse en las mismas entrevistas donde se recoge la información de los procesos existentes y de los elementos (hardware, software, etc.) que lo componen.

4. *Determinación de los Procesos Críticos.*

Aquí se evalúa el impacto económico y operacional concerniente al negocio en caso de no disponer del proceso analizado. Algunas formas que pueden ayudar a valorar las eventuales pérdidas pueden ser:

- Costo de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante.

- Ingresos dejados de percibir.

- Penalizaciones por incumplimiento de contratos con clientes.

- Gastos financieros.

Para simplificar esta valoración de los procesos se puede establecer una clasificación numérica, asignando mayor prioridad (p.e. 1) a aquellos procesos que se consideren más críticos y menor prioridad (p.e. 3) a aquellos que se consideren menos críticos.

5. *Periodo máximo de interrupción.*

Para cada proceso dentro del BIA, se necesita determinar el *Periodo Máximo de interrupción.*

El *Periodo Máximo de interrupción* se define como el tiempo en que después de que un proceso no se encuentra disponible crea consecuencias irreversibles y mayormente fatales para la empresa.

Este se encuentra formado por dos factores principales, el primero de estos es el RTO o Tiempo de recuperación objetivo que representa el periodo de tiempo en que la organización intenta tener devuelta en funcionamiento un proceso que fue

interrumpido, y el RPO o Punto de recuperación objetivo el cual se define como la máxima cantidad de data que se puede perder si un proceso es interrumpido y luego recuperado.

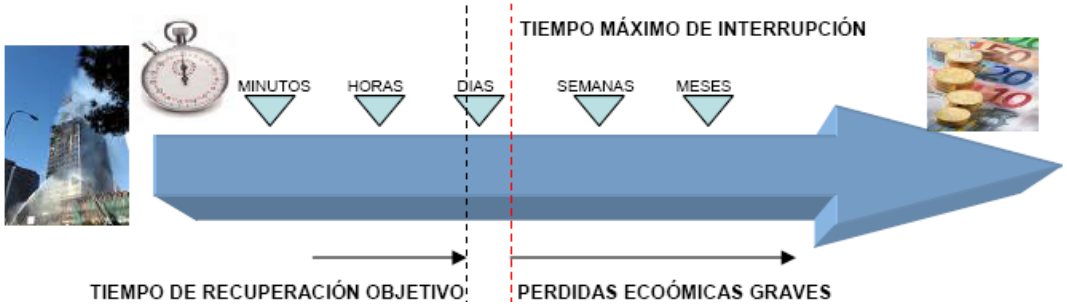


Figura 3.0 Tiempos de recuperación

3.1.1 Análisis de Impacto en Stream

En el análisis de impacto de le empresa sujeta a investigación se muestra una matriz que contiene todos los elementos esenciales del BIA en lo referente a los procesos críticos de esta, por ejemplo se realiza en esta tabla una pequeña descripción de esos procesos críticos, explicado el alcance y principales funciones de estos, también la frecuencia con la que son utilizados, sistemas que interactúan, entre otros elementos, esta composición de los elementos permite realizar un análisis más objetivo en todo lo que envuelven los procesos críticos de la empresa. La información que muestra la matriz del BIA fue producto de un levantamiento de información a los diferentes procesos de Stream (ver anexo IV Cuestionario para BIA).

Proceso	Descripción	Frecuencia de Uso	Sistema Interactúa	Equipo Necesario	Personal Critico	Suplidores	MTD	RTO	RPO	Costo Impacto por H/ D/ M	Nivel de Criticidad
Soporte al Producto del Cliente	Agente de la capacidad de mantener los niveles de servicio de contestador de teléfono y correo electrónico las solicitudes de apoyo.	Diario	AvayaCMS, Distribuidor Automático de Llamadas (ACD)	Servidores	Agentes de Atención al Clientes, Representantes de Tecnología Informática (TI)	Avaya	< 2 horas	1 hora	2 horas	2600 dólares por hora en promedio	1
Proceso de Apoyo: Tecnología Informática y Telecomunicaciones	Mantenimiento de la Tecnología Informática y de los Teléfonos	Diario	Window 2003 Server, SQL Server	Servidores y Teléfonos	Representantes de TI		2-4 horas	< 1hora	2 horas	1500 Dólares Por hora	2
Facilidades	Mantenimiento del Sistema del Edificio	Diario, Semanal, Bisemanal y Mensual	Maintance It	Servidores de aplicaciones, UPS, Plantas eléctricas	Personal de Mantenimiento	N/A	2horas a 4 días	<2 horas a 1 día	2 horas	250 Dólares	2
Nómina	Generar y distribuir nomina	Quincenal	Sage SP Nomina Plus 2009	Servidor y PC	Representante de Finanzas	Sage LTD.	24 a 72 horas	<24 horas	3 a 7 días	156.25 dólares por hora	3

3.2 Análisis de Riesgo

El Objetivo de este análisis es identificar y analizar los diferentes factores de riesgo que potencialmente podrán afectar a las actividades que se quiere proteger. La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el impacto que supondría para la organización. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado.

Un análisis de riesgo conlleva lo siguiente:

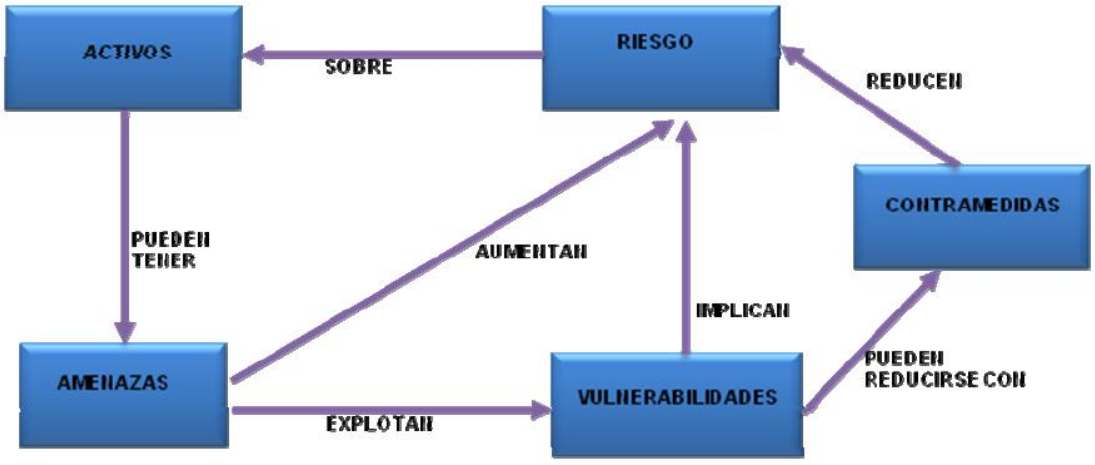


Figura 3.1 Componentes del análisis de riesgo

3.2.1 Análisis de Riesgo en Stream

3.2.1.1 Lista de Activos de Stream Global Services

En esta parte se presentan la lista de los recursos tecnológicos más importante de la organización.

La primera tabla muestra *los activos de hardware* con datos de importancia como son los distribuidores, modelos y ubicación de estos equipos. Estos datos son esenciales para la reacción en una situación de riesgo para Stream.

Lista de Inventario de Equipos				
Activos				
Hardware				
#	**Tipo de Hardware**	**Distribuidor**	**Modelo**	**Ubicación**
1	Servidor de Aplicaciones	Dell	PowerEdgeTM 2900 Servidor en torre de núcleo cuádruple con 2 sockets	Data Center
2	Servidor de Archivos	Dell	PowerEdgeTM 1900 Servidor en torre de núcleo cuádruple con 2 sockets	Data Center
3	PC's	Dell	Dell OptiPlex 740 Desktop	Producción / Oficinas
4	Servidor de Correo	Dell	PowerEdgeTM 1900 Servidor en torre de núcleo cuádruple con 2 sockets	Data Center
5	Sevidor de Internet	Dell	PowerEdgeTM 2900 Servidor en torre de núcleo cuádruple con 2 sockets	Data Center
6	Switch	Cisco	Catalyst 2948G-GE-TX Gigabit Ethernet	Data Center
7	Router	Cisco	Cisco Small Business 100 Series Router	Data Center
8	Call Manager	Avaya	Avaya Communication Manager 5.1	Data Center
9	Digital Telephone	Avaya	Avaya 2420	Producción / Oficinas

Esta segunda tabla tiene como base las *aplicaciones* principales que se encargan de envolver esos procesos que son de vital importancia dentro de Stream.

Aplicaciones		
Software	**Uso**	**Propietario**
SQL Server	Administrador de Base de Datos de Aplicaciones	Microsoft
CMS Monitoring Sys.	Sistema de Monitores de Actividad de Estaciones Avaya	Avaya
Administrative Tools	Sistema Basado en Web para la Gerencia	Microsoft

En esta tercera tabla el detalle realizado es el de los *Softwares* que son utilizados para el manejo de esos sistemas informáticos que dan soporte a la organización y que la indisponibilidad de estos conlleva un gran impacto.

Inventario de Software			
Sistemas Operativos			
Software	**Fabricante**	**Versión**	**Sistema**
Windows 2003 Server	Microsoft	2.06	Exchange
TFTP Server	Avaya	1.04	CMS Monitoring Sys.
Windows 2003 Server	Microsoft	2.06	FireWall System
Windows 2003 Server	Microsoft	2.06	Servidor de archivos / Aplicaciones

3.2.1.2 Identificación de Amenazas

Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios[3].

A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir de las más diversas fuentes. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

La siguiente ilustración clasifica las distintas amenazas:

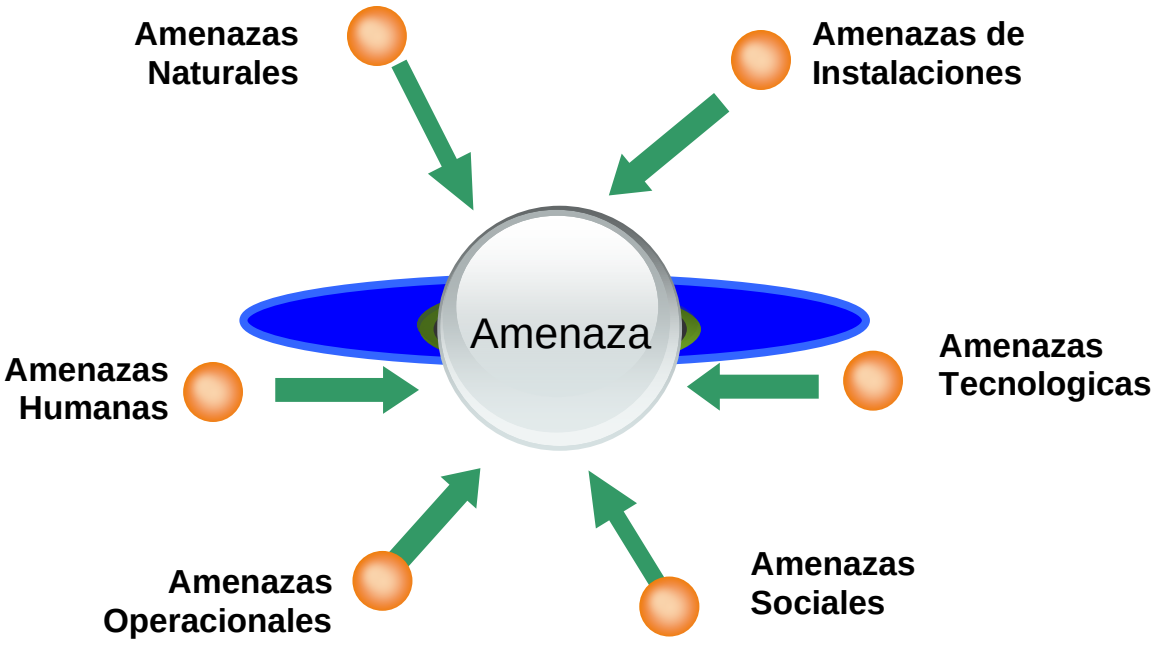


Figura 3.2 Clasificación de las amenazas

[3] Gómez, Ramón. Cátedra del Modulo Plan de Recuperación de Desastres. UNAPEC. 2009

Dependiendo de la organización y el proceso analizado, serán aplicables distintos tipos de amenazas. Las amenazas tienen una probabilidad de ocurrencia que depende de la existencia de una vulnerabilidad que pueda ser explotada para materializarse en un incidente. En el *anexo 2* se muestran algunos ejemplos de posibles amenazas.

Tablas de Amenazas Stream

Del listado de Amenazas fueron marcadas las que pueden afectar a Stream en su situación actual. Para ello se uso la siguiente escala de valoración para la probabilidad y el impacto:

Probabilidad Calificación		**Evaluación de impacto**	
Puntuación	**Nivel**	**Puntuación**	**Nivel**
1	Muy alta	1	Terminal
2	Alto	2	Devastadores
3	Medio	3	Crítica
4	Bajo	4	Controlable
5	Muy baja	5	Muy pequeña

- *Evaluación de Desastres Naturales*

Se examinan cada amenaza potencial de desastre natural. El enfoque que se realiza es en base a la interrupción de la empresa que pudiera resultar de cada tipo de desastre. Las amenazas de desastres naturales con mayor potencial son las siguientes:

Amenazas Naturales	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Tornado	5	1-5	Tornados no se han producido en esta región.
Huracán / tormenta-huracán Nivel fuertes vientos	4	4-5	Apagón, Daños a la Propiedad, inundaciones
Inundación	3	4-5	Problemas de transporte, problemas de aparcamiento, Daños a la Propiedad
Terremoto	3	1-5	Interrupción infraestructura, daños a la propiedad, problemas de transporte, de seguridad para empleados
Tormentas eléctricas	3	4-3	Apagón, Daños a la Propiedad, seguridad de los empleados.
Fuego	4	1-5	Apagón, Daños a la Propiedad, seguridad de los empleados.
Contaminación y los peligros ambientales	3	1-5	Daños a la Propiedad, seguridad de los empleados.
Epidemia	3	1-5	Niveles de personal podría ser afectado por una epidemia generalizada. Esto tendría consecuencias para los niveles de servicio.

- *Evaluación de las amenazas humanas*

En esta parte se evalúan las potenciales amenazas pero en el ámbito humano, cuales son los posibles escenarios donde un proceso de la empresa se puede ver afectado por una interrupción causada en base a una amenaza humana.

Amenazas Humanas	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Disputas laborales / Acción Industrial	5	4	No ha habido ninguna actividad laboral en el Parque Cibernético-SD2. Disputas laborales impactan los Niveles de Servicio
Incendio provocado	5	1-5	No han tenido una incidencia de este tipo, pero el Impacto dependerá de la severidad del fuego.
Robo	2	5	Los incidentes de robo en el ciberespacio Park - SD2 han variado desde pequeños a los sistemas informáticos, sin embargo el impacto directo en la empresa ha sido menor.
Acto de guerra	5	1-5	No han tenido un acto de este tipo en la República Dominicana hace ya muchos años. El impacto dependerá de la gravedad.
Acto de sabotaje	5	1-5	Nunca se ha presentado esta situación pero su impacto dependerá de la gravedad.
Acto de terrorismo	5	1-5	El impacto dependerá de la gravedad.

- *Evaluación de las amenazas en las instalaciones*

Aquí se examinan y evalúan las amenazas con mayores posibilidades de ocurrencia en el plantel de Stream. Los potenciales desastres que pueden ocurrir en caso de la pérdida de las utilidades o servicios de Stream.

Amenazas a las instalaciones	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Falta de energía eléctrica	1	1-3	Fallo de alimentación en el Parque Cibernético - SD2 solo impacta a la empresa si los generadores de emergencia no entran en funcionamiento inmediatamente al ocurrir el evento. Los niveles de servicio se ven interrumpidos.
Pérdida de suministro de agua	3	4	Cualquier pérdida de agua sería temporal y manejable, a menos que parte de una mayor escala de desastres (terremotos etc)
Interrupción de los servicios de comunicaciones	3	4-3	Pérdida del servicio telefónico impacta de inmediato los niveles de servicio.
Pérdida de drenaje / eliminación de desechos	4	4	Pérdida de drenaje sería temporal y manejable, a menos que parte de una mayor escala de desastres (terremotos etc)
Falta de aire acondicionado	3	4	Fracaso de las unidades individuales puede ser compensada por otras unidades en el edificio. Fracaso general de nivel de servicio podría generar interrupciones si el edificio llega a estar demasiado calientes para los agentes a trabajar de manera eficaz. Las unidades podrían ser sustituidas o reparadas rápidamente.
Avería de los equipo (con exclusión de hardware de TI)	3	5-4	En función de nivel de impacto a la construcción de infraestructuras. Es improbable que tenga un impacto en los niveles de servicio.

- *Evaluación de incidentes serios con los sistemas de información*

Los escenarios con mayor posibilidad que podrían afectar a la empresa en caso de que suceda un incidente con los sistemas de información son los siguientes:

Potencial de los Desastres	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Crimen Cibernético	3	4	Podría crear interrupción a los sistemas de TI e impactar los niveles de servicio.
Pérdida de registros o datos	3	4	Podría crear interrupción a los sistemas de TI e impactar los niveles de servicio.
Revelación de información sensible	3	4	Depende de la naturaleza de la información.
Fallo del sistema TI	3	3-4	Impacta temporalmente los niveles de servicio. Existen copias de seguridad de los sistemas disponibles.

- *Evaluación de otras amenazas*

Existen otras amenazas que poseen un nivel de impacto considerable en la empresa en caso de ocurrir, ejemplo de dichas amenazas de describen en la tabla a continuación.

Potencial de los Desastres	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Reglamento de Salud y Seguridad	4	5	Sin efecto sobre los niveles de negocios.
La moral de los empleados	3	4-5	Podrían tener un impacto en el nivel de personal y el afectar los niveles de servicio.
Las fusiones y adquisiciones	4	5	Poco o ningún impacto a nivel de servicios
Publicidad negativa	4	5	Poco o ningún impacto de nivel de servicio.

3.2.1.3 Evaluación de Vulnerabilidades

Las *vulnerabilidades* son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves en una compañía. Las vulnerabilidades en sí mismas no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo[4].

La vulnerabilidad se asocia a la incapacidad de resistencia cuando se presenta un fenómeno amenazante.

[4] Gregory, Meter. IT Disaster Recovery Planning for Dummies. Editora Wiley Publishing, Inc. S.n.e . Indiana. 2008.

En el *anexo 3* se muestran algunos ejemplos de vulnerabilidades.

Vulnerabilidades Stream

Durante la identificación de las vulnerabilidades de la empresa Stream Global Services se pudo observar que estas provienen de múltiples fuentes, a continuación se muestra una lista de vulnerabilidades recogida durante la investigación.

- Falta de mantenimiento de los equipos.
- Ventanas del Data Center con Cristales muy Frágiles.
- Suministro Eléctrico Redundante Poco Eficiente.
- Ausencia del Sistema de Extinción Automática de Fuegos/ Humos en el Data Center.
- Falta de Motivación de los Empleados.
- Educación Inadecuada del Personal en Virus y Troyanos.
- Carencia Dispensario Médico Cerca de las Facilidades.
- Política de Seguridad de la información Inadecuada.
- Ausencia de Pruebas de Copia de Respaldo.
- Descarga Incontrolada y mal uso de Software de Internet.

En función de las Vulnerabilidades que se han encontrado, se establecieron algunos escenarios en que estas pudiesen convertirse en un incidente de seguridad.

ESCENARIOS	NIVEL DE PROTECCIÓN	RESPUESTA
Ventanas del Data Center con Cristales muy Frágiles	Existe una revisión periódica de las ventanas ante y durante la temporada Ciclónica	No periódicamente
Cableado Deteriorado en Varias Terminales	Se revisan estos detalles durante el mantenimiento a los equipos	Pocas Veces
Suministro Eléctrico Redundante Poco Eficiente	Están las unidades actuales de generación y UPS en capacidad de suministrar energía de manera ininterrumpida	No
Política de Seguridad de la información Inadecuada	¿Existe una clasificación de la información adecuada al nivel de confidencialidad de los datos?	No en todos los casos
Educación Inadecuada del Personal en Virus y Troyanos	La compañía provee algún tipo de información sobre los efectos que estos males pudieran causar	No
Ausencia de Pruebas de Copia de Respaldo	Existe una política de prueba de copias de seguridad de los datos	No
Carencia Dispensario Medico Cerca de las Facilidades	Provee la compañía alternativas para mitigar el efecto en caso de cualquier emergencia medica	No

3.2.1.4 Evaluación del Riesgo

Riesgo es la posibilidad de que se produzca un impacto determinado en la organización. El riesgo calculado es simplemente un indicador ligado al impacto y la probabilidad de que una amenaza suceda[5].

[5] Brigham, Eugene. Fundamentos de Administración Financiera. Editora Thomson. Décima Edición. México. 2005.

El siguiente cuadro muestra una relación entre las diferentes amenazas a los activos tomando en cuenta el impacto y la probabilidad, para de esta forma medir el nivel de Priorización.

Activo	Amenaza	Vulnerabilidades	Impacto	Probabilidad	Medición	Priorización
Central Telefónica	Falla del hardware, fallas del proveedor de servicios Vandalismo.	Suministro eléctrico ineficiente, seguridad débil.	5	2	10	A
Servidor de Aplicaciones	Virus, Perdida de Energía, Hackers, Inundaciones.	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado.	3	2	6	C
Computadoras	Virus, Vandalismo, perdida de Energía.	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	3	2	6	C
Servidor de Correo	Virus, Perdida de Energía, Hackers, Inundaciones.	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	4	2	8	B
Línea RDSI de comunicaciones	Fuego, fallas del proveedor de servicios, Vandalismo	Falta de extintores automáticos, suministro eléctrico ineficiente, seguridad débil.	5	2	10	A
Routers	Virus, Perdida de Energía, Hackers	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	4	2	8	B
Switchs	Virus, Perdida de Energía, Hackers	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	3	2	6	C
Sistema de CCTV	Perdida de Energía, Vandalismo, Error Humano	Falta de extintores automáticos, suministro eléctrico ineficiente, seguridad débil.	1	2	2	D
Base de datos de la empresa	Falla en el Software, Perdida de Datos, Manipulación de Datos	Falta de prueba de copias de respaldo, seguridad lógica débil, antivirus desactualizado	3	2	6	C
Personal	Epidemia, huelgas, problemas con el trasporte, Desmotivación	Falta de motivación, dispensario medico muy lejos, diferencia	4	3	12	A

		de ideas				
Software de Aplicaciones	Fallas en la Red, Falla de integridad Datos, Fallas de Software	Falta de prueba de copias de respaldo, seguridad lógica débil, antivirus desactualizado	2	2	4	D
Teléfonos	Error Humano, Vandalismo, Falla de la red	Desmotivación de los empleados, suministro eléctrico inadecuado	4	2	8	B
Base de datos de Clientes	Falla en el Software, Perdida de Datos, Manipulación de Datos	Falta de prueba de copias de respaldo, seguridad lógica débil, antivirus desactualizado	3	2	6	C
UPS	Fallas Eléctricas, fuego, Vandalismo	Falta de extintores automáticos, falta de mantenimiento de los equipos	3	2	6	C
Generadores Eléctricos	Fuego , Error Humano, Falta de Mantenimiento	Falta de extintores automáticos, falta de mantenimiento de los equipos.	4	2	8	B
Software de OS	Falla en la red, Hackers, Virus, error Humano	Falta de prueba de copias de respaldo, seguridad lógica débil, antivirus desactualizado	3	2	6	C
Call Manager	Falla del Hardware, Vandalismo, perdida de Energía	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	4	2	8	B
Servidor de internet	Virus, Perdida de Energía, Hackers, Inundaciones	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	3	2	6	C
Base de Datos de Aplicaciones	Falla en el Software, Perdida de Datos, Manipulación de Datos	Falta de prueba de copias de respaldo, seguridad lógica débil, antivirus desactualizado	2	2	4	D
Servidor de Archivos	Virus, Perdida de Energía, Hackers, fallas del Hardware, Inundaciones	Suministro eléctrico ineficiente, seguridad lógica débil, antivirus desactualizado	2	3	6	C

3.2.1.5 Evaluación de Contramedidas

Para reducir los niveles de riesgos se utilizan los siguientes controles o medidas de seguridad.

Medidas para garantizar de prueba de copias de seguridad de los datos:

- Desarrollar un procedimiento para realizar pruebas de copias de seguridad.
- Probar las copias de seguridad con frecuencia mediante la restauración real de los datos en una ubicación de prueba.
- Establecer hojas de checklist en donde se establezca la periodicidad con que se realizan estas pruebas, nombre de quien las realizan, entre otros.
- Se asegurará de que los medios de copia de seguridad y los datos copiados están en buenas condiciones, lo cual garantizará un nivel de confianza que resultará útil durante una crisis real.
- Documentar posibles problemas que se presenten durante el ejercicio.

Controles para evitar el ataque de virus y troyanos:

- Tener un antivirus actualizado al día.
- Actualización del sistema operativo y programas de sus posibles vulnerabilidades críticas, estas actualizaciones se realizarán en los sitios oficiales.

- Contar con un firewall con capacidad de análisis SMTP, que intercepte los archivos adosados de tipo ejecutable que comúnmente son usados como cargas útiles de virus.
- Educar a los usuarios en cuanto al peligro de descargar el software de fuentes no confiables. Configure su firewall para bloquear la descarga de archivos ejecutables desde Internet vía HTTP.
- Asegurar parchear las computadoras tan rápidamente como sea posible, es una buena prevención contra cualquier virus, gusanos o ataques de troyanos.
- Establecer políticas claras sobre el empleo de software no autorizado en el lugar de trabajo.
- Mantener al día al personal del área de tecnología en lo referente a nuevos "brotes" de virus peligrosos y establecer métodos de actuación, de esta forma puede evitar que estos impacten en la organización y puedan causar daños mayores.

Medidas para eficientizar el suministro de energía redundante:

- Priorizar los servicios que requieran el uso de energía redundante.
- Crear mecanismos para el ahorro de energía cuando se este usando el UPS o los generadores.
- Analizar los requerimientos de potencia actuales y futuros.
- Determinar el tiempo máximo de respaldo de energía requerido.

- Establecer políticas de mantenimiento para las unidades de energía redundante.
- Garantizar soporte técnico (antes, durante y después de la instalación los generadores y UPS).

Controles para el acceso a la información:

- Crear y mantener perfiles de seguridad para todos los usuarios con base en sus roles y responsabilidades.
- Establecer mecanismos de autentificación eficientes para el acceso a sistemas críticos.
- Limitar el acceso del usuario a únicamente a los recursos que requiere para desarrollar su trabajo.
- Revisar los derechos de acceso de usuarios periódicamente.
- Instalar mecanismos que limiten el número de intentos fallidos para autenticarse en el sistema.
- Establecer una longitud mínima de password, así como la combinación de letras mayúsculas y minúsculas, números y signos.
- Solicitar a todos los usuarios firmar un acuerdo de uso apropiado antes de que tengan acceso al equipo, red y sus recursos.

Medidas para ser tomadas en cuenta en las instalaciones durante la temporada ciclónica y ante la llegada de la misma:

- Realizar inspecciones minuciosas de las instalaciones físicas y los alrededores y preparar un informe detallado sobre todo aquello que requiera reparación para corregir toda deficiencia que pueda representar un riesgo para la vida humana y la propiedad.
- Determinar la necesidad de planchas de metal o paneles protectores para asegurar áreas vulnerables en las instalaciones.
- Monitorear los boletines de la oficina nacional de meteorología y otras fuentes oficiales.
- Informar al personal para que se mantenga en estado de alerta y, de creerlo necesario, permitir regresar a sus hogares a todo el personal que no tenga asignaciones dentro del plan de emergencia de la empresa.
- Proveer orientación al personal que esta laborando sobre de contingencia a seguir en caso de ser impactados.
- Desconectar los interruptores de energía eléctrica.
- Mover el equipo electrónico a áreas que estén lejos de las ventanas, colocarlo sobre escritorios u otros muebles y cubrirlo con material impermeable.
- Colocar paneles de huracanes en las ventanas y puertas de cristal según estén disponibles.

Capitulo IV.
Desarrollo Estrategias.

Capitulo IV.
DESARROLLO ESTRATEGIAS.

En este capitulo se detallan los aspectos que involucran la fase No.2 del plan objeto de este estudio. Se seleccionarán los métodos operativos alternativos (estrategias) que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en la organización. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto. La estrategia debe estar enfocada en los procesos críticos del negocio para garantizar la viabilidad de la empresa.

4.1 Consideraciones

Dependiendo de las necesidades de cada compañía, en cuanto a tiempos de recuperación, costes económicos, recursos, entre otros, deberá considerarse los siguientes factores antes de seleccionar un plan estratégico determinado:

1. *Ubicación y superficie requerida:*
    - Espacio suficiente.
    - Zonas acondicionadas para acoger a personal.
2. *Recursos técnicos necesarios:*
    - Hardware.
    - Software.
    - Comunicaciones.
    - Datos de respaldo.

3. *Recursos humanos requeridos*

    - Recursos materiales y de infraestructura.
    - Servicios auxiliares necesarios
    - Tiempos de activación
    - Costo

4.2 Selección de la Estrategia

Para el desarrollo de las estrategias a seguir por la empresa Stream Global Services se tomará como base los procesos críticos enlistados en el BIA, RPO, RTO, MTD de cada uno y los sistemas de TI que sustentan a dichas actividades.

Los siguientes escenarios serán considerados para el desarrollo de las estrategias:

Escenario 1: Infección por Virus en Servidores y Computadores.

Estrategia:

1. Desinfección del virus a través de un antivirus.
2. Restauración de archivo en caso de pérdida de datos
3. Recuperación por medio de los warmsite

Escenario 2: Pérdida de Base de Datos

Estrategias:

1. Recuperación por medio de Back-up.

2. Recuperación por medio de los warmsite.

Escenario 3: Falla de la Energía Eléctrica.

Estrategias:

1. Activar sistemas redundantes.
2. Acuerdo con suministro eléctrico de terceros.

De las alternativas existentes en el mercado se recomienda un acuerdo con la compañía llamada el *NAP del Caribe* para el arrendamiento de un Warm sites para el data center, de esta manera Stream garantizará una rápida recuperación de sus procesos críticos y el servicio brindado a sus clientes, sin que el impacto de un incidente tuviera consecuencias catastróficas para la compañía.

Además, se sugiere una línea de comunicación dedicada RDSI redundante, de modo que si la existente dejase de funcionar la sugerida tomase el control y las comunicaciones no se afectarían.

Listado de diferentes proveedores de servicio de Warm sites y su costo:

Nombre del Proveedor	Tipo de Servicio	Localidad	Costo Total Mensual Warm Site
NAP del Caribe	HotSide/ Warm Site	Santo Domingo	$100,000
Integrity Data C.O.	HotSide/ Warm Site	California	$200,000
Prime Soluctions S.A.	HotSide/ Warm Site	España	$185,000

Tabla que recoge la relación entre el Tiempo Objetivo de recuperación y la solución de continuidad más adecuada a este Objetivo*:*

Tiempo Objetivo de Recuperacion	Internas	Tipo de Servicio
Meses	Reconstrucción / Realojamiento	----------
Semanas	Edificios prefabricados On-Site	Contratación de unidades móviles o prefabricados
Días	Recuperación “in situ” trabajo en casa	Subcontratación de procesos en oficinas móviles
Inmediato	Localizaciones diversas para la misma función	Cambio de funcionamiento a un centro de respaldo subcontratado Hot side, Warm site, Cold site

Nota:

- Hot sites: Normalmente esta configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.
- Warm sites: En esta opción no se incluyen servidores específicos de alta capacidad.
- Cold sites: En esta opción sólo se tiene aire acondicionado, potencia, enlaces de telecomunicaciones, y otros.

4.3 Prioridades de Recuperación

Una vez seleccionada la estrategia se procede al desarrollo de la misma, en donde se priorizan los procesos de acuerdo a su nivel de importancia para las operaciones del negocio.

En la siguiente tabla muestra una recomendación para la recuperación de los procesos:

Proceso	Sistema	RTO Acordado	Prioridad de Recuperación	Estrategia Acordada
Soporte al Producto del Cliente	AvayaCMS, Distribuidor Automatizo de Llamadas (ACD)	< 1hora	1	Warm Site
Proceso de Apoyo: Tecnología Informática y Telecomunicaciones	Window 2003 Server, SQL Server	< 1hora	2	Warm Site RDSI
Nomina	Sage SP Nómina plus 2009	<24 horas	3	Warm Site

4.4 Infraestructura y Recursos Tecnológicos para el Warm Site

La infraestructura y recursos tecnológicos que requerirá el Warm Site del *NAP del Caribe* serán:

1. *Infraestructura*
    - Climatización permanente entre 18º-22º con una humedad relativa de 50 %.
    - Alimentación eléctrica ininterrumpida por medio de generadores y UPS.

- Sistema de extinción automático/manual se basa en la inundación total (gas FE-13) de la sala.
- Control de acceso seguro.
- Suelo técnico antiestático.

2. *Hardware*
    - *Un servidor para aplicaciones PowerEdgeTM 2900 Servidor en torre de núcleo cuádruple con 2 sockets.*
    - Un servidor de correo y de archivos PowerEdgeTM 1900 Servidor en torre de núcleo cuádruple con 2 sockets
    - Un call manager Avaya comunication 5.1
    - Equipos para la interconexión del hardware y redes.
3. *Sistemas Operativos*
    - Windows 2003 Server2.06
    - TFTP Server 1.04
4. *Procedimiento de Respaldo*
        - Copia de data incremental cada 25 minutos
        - Copia de data diferencial cada tres días
        - Copia de toda la data cada 5 días los viernes en la noche.
        - Toda la data debe estar protegida y encriptada.
5. *Comunicaciones*
    - Línea de comunicación redundante RDSI de acceso primario.

Capitulo V.
Desarrollo del DRP

Capitulo V.
DESARROLLO DEL DRP

En este capítulo se desarrolla la Fase No.3 del DRP, en donde se detallan los procedimientos que se utilizarán para la recuperación ante un evento que cause la interrupción de las operaciones del negocio en Stream Global Services.

5.1 Objetivos.

El *objetivo* se define como las metas a corto y a largo plazo que se desean alcanzar[6]. Los objetivos trazados que debe cumplir el plan son los siguientes:

- Definir los equipos de trabajo necesarios para el desarrollo del Plan.
- Establecer responsabilidades y funciones de cada uno de los equipos.
- Identificar dependencias orgánicas entre los diferentes equipos.
- Desarrollar de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Definir Los procedimientos de actuación ante incidentes.
- Establecer estrategia de vuelta a la normalidad.

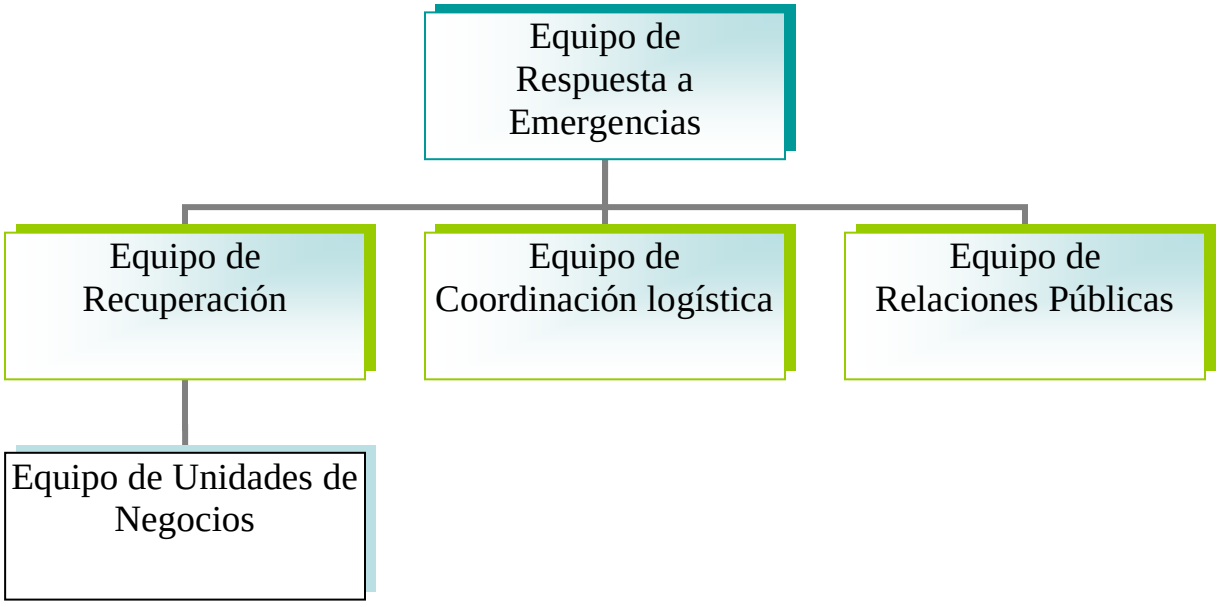
5.2 Organización de los Equipos.

En esta parte se procederá a la organización de los equipos formados por el personal clave de Stream Global Services, estos se encargarán de la activación

[6] Gregory, Meter. IT Disaster Recovery Planning for Dummies. Editora Wiley Publishing, Inc. S.n.e . Indiana. 2008

y desarrollo del Plan de Recuperación. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan.

5.2.1 Organigrama de los Equipos del Pan de Recuperación de Desastres:



5.2.2 Equipo de Respuesta a Emergencias

Listado de integrantes del equipo

Responsable del Equipo	Nombre: Brad Spencer Posición: Director del Site Teléfono Móvil: 809-435-5467 Teléfono Residencia: 809-778-4534
Miembros del Equipo	Nombre: Luís Ruiz Posición: Director de Operaciones Teléfono Móvil: 829-323-4583 Teléfono Residencia: : 809-768-4230 Nombre: Porfirio Estrada Posición: IT Manager Teléfono Móvil: 829-456-3453 Teléfono Residencia: : 809-598-4364 Nombre: Maria Vargas Posición: Gerente de Recursos Humanos Teléfono Móvil: 809-345-5433 Teléfono Residencia:809-590-3456

Punto de reunión del equipo de respuesta a emergencias: mediante consenso de los miembros se acordó como punto de operaciones la residencia del director del site, la misma es de fácil acceso para todos, pero en caso de no poder llegar a esta como segunda opción se usará la residencia del gerente de IT. Una vez activado el plan el equipo de respuesta a emergencias deberá reunirse para afrontar la situación y comunicar a los responsables de los equipos del comienzo de las actividades del plan.

5.2.3 Equipo de Recuperación

Listado de integrantes del equipo

Miembros del Equipo	Nombre: Mariano Castillo Posición: IT Supervisor Teléfono Móvil: 829-345-4411 Teléfono Residencia: 809-599-1245 Responsabilidades: Coordinador del Personal Técnico Nombre: Roberto Ramírez Posición: Analista IT Teléfono Móvil: 809-412-4355 Teléfono Residencia: 809-543-3489 Responsabilidades: Encargado de Aplicaciones Nombre: Héctor Rivas Posición: Técnico de IT Teléfono Móvil: 829-435-8760 Teléfono Residencia: 809-699-0978 Responsabilidades: Encargado de Sistemas Operativos Nombre: José Mesa Posición: Técnico de IT Teléfono Móvil: 829-635-8062 Teléfono Residencia: 809-689-1938 Responsabilidades: Encargado de Seguridad Lógica

El equipo de recuperación de Stream Global Services es el autorizado de ejecutar todo el proceso de recuperación para reponer los servicios en el las facilidades del NAP del CARIBE, para ello se realizarán los ejercicios siguientes:

- El equipo se transportará al centro de respaldo ubicado en el NAP del CARIBE.
- Se pondrán en marcha por orden de criticidad los sistemas que soportan el soporte al producto del cliente, el proceso de apoyo: tecnología informática y telecomunicaciones y la nómina.
- Para la puesta en marcha de los sistemas se tomará el último backup realizado en Stream a los sistemas.
- Confirmación y operatividad de los servicios restaurados.

5.2.4 Equipo de Coordinación Logística

Listado de integrantes del equipo

Integrantes del Equipo	Nombre: Marta Feliz Posición: Gerente de Finanzas Teléfono Móvil: 809-457-8923 Teléfono Residencia: 809-345-3790 Nombre: Porfirio Estrada Posición: Gerente de Calidad Teléfono Móvil: 829-450-5490 Teléfono Residencia: 809-690-0018

El equipo de coordinación logística de Sream será el responsable de todo lo concerniente a:

- Atender las necesidades logísticas del personal de la organización involucrados en el DRP. (Transporte de personas, transporte de materiales, etc.)
- Gestionar el suministro de comida al personal implicado.
- Contactar con los proveedores de la organización para solicitar material necesario que indiquen los responsables de la recuperación.

Listado de Proveedores de Stream Global Services.

Avaya	Nombre de Contacto: Derek Rice Teléfono: 718-366-4040
Dell	Nombre de Contacto: Steven Falmer Teléfono: 407-573-1234
Telecom	Nombre de Contacto: Albert Contreras Teléfono: 716-345-7890
NAP del CARIBE	Nombre de Contacto: Bienvenido Riveras Teléfono: 809-476-3030
Codetel	Nombre de Contacto: Antonio Valdez Teléfono: 809-220-1125

5.2.5 Equipo de Relaciones Públicas

Listado de integrantes del equipo.

Integrantes del Equipo	Nombre: Josefina Padilla Posición: Coordinadora de Recursos Humanos Teléfono Móvil: 829-334-6589 Teléfono Residencia:809-580-1034 Nombre: Wendy Grullón Posición: Encargada de Contabilidad Teléfono Móvil: 829-884-1559 Teléfono Residencia: 809-590-3014

Este equipo será responsable de comunicación una vez activado el plan.

Formato usado por Stream para la Difusión de Información a los afectados

5.2.6 Equipo de Unidades de Negocios

Listado de integrantes del equipo.

Integrantes del Equipo	Nombre: Marcos Pérez Posición: Supervisor de Producción Teléfono Móvil: 809-333-6789 Teléfono Residencia: 809-236-3639 Nombre: Luisa Almonte Posición: Supervisora de Producción Teléfono Móvil: 829-880-4562 Teléfono Residencia: 809-964-7459

Equipo responsable de probar los procesos críticos y reportar en caso de anomalías.

5.3 Acciones del Plan

En esta parte se muestran las acciones a tomar por parte de los equipos durante la ejecución del DRP.

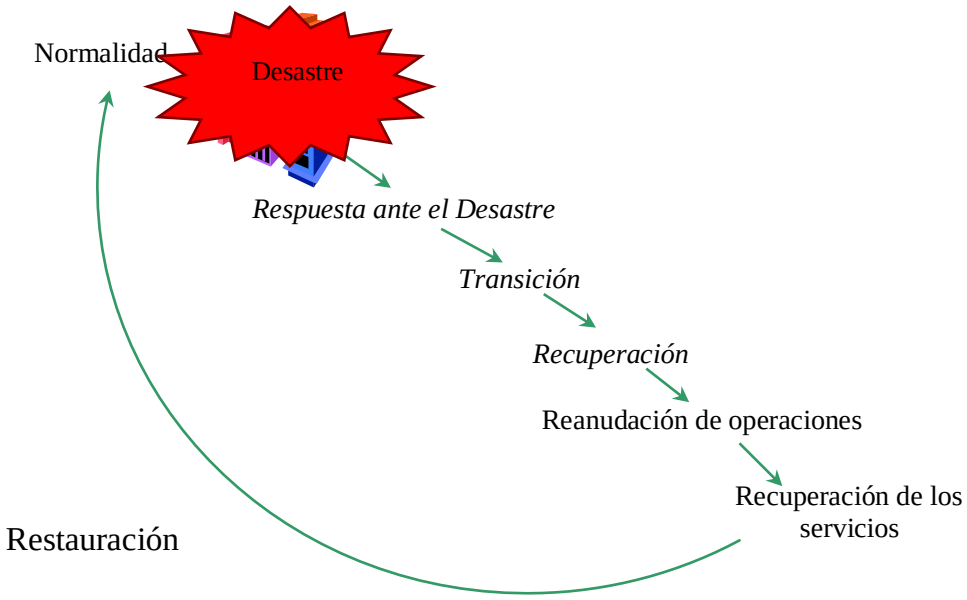


Figura 4.0 Acciones en el Desarrollo del Plan.

5.3.1 Respuesta ante el Desastre

Una vez haya ocurrido el desastre el equipo de respuesta a emergencia evaluará la situación con toda la información del incidente y luego, se ventilará si se activa o no el plan.

El siguiente checklist muestra la lista de actividades que se realizaran durante este proceso:

Checklist #1

Responsables	Acciones:
Equipo de respuesta a emergencias	1. Coordinar la respuesta inicial y la utilización de procedimientos establecidos para proteger la vida y minimizar los daños. ☐ 2. Calcular los daños. ☐ 3. Evaluar posible activación del plan de recuperación. ☐ 4. Convocar a los equipos correspondientes para comenzar el Proceso. ☐ 5. Proporcionar un aviso oficial. ☐ 6. Comenzar la recuperación de desastres de la forma establecida. ☐ 7. Suministrar las informaciones pertinentes correspondientes sobre la situación por los canales correspondientes. ☐ 8. Establecer un informe de evaluación de las perdidas. ☐

5.3.2 Transición

Una vez convocados todos los equipos y puesto en marcha el plan, el equipo de logística es el encargado de coordinar el traslado del personal correspondiente a las instalaciones del NAP del CARIBE, además es el encargado de gestionar todo el material necesario para poner en funcionamiento el centro de recuperación (cintas de backup, documentación, etc.)

5.3.3 Recuperación

Cuando el equipo de recuperación llegue al NAP del Caribe y los materiales estén listos, deben verificar rápidamente el estado de los equipos y luego iniciar con las instalaciones de las aplicaciones.

Una vez instalada las aplicaciones, se procederá a cargar el backup más reciente de la data y verificar que esta información este correcta. Luego el encargado de seguridad lógica verificará que toda la data que se este procesando en este nuevo sitio tenga las garantías necesarias y que los equipos tengan un alto nivel de seguridad establecidos para no ser atacados por hackers, virus y otros.

El siguiente checklist muestra las actividades a realizar el el warmsite del NAP de Caribe:

Checklist #2

Responsables	Acciones:
Equipo de Recuperación	1. Recibir notificación del equipo de respuesta a emergencias. ☐ 2. Comenzar las actividades de recuperación. ☐ 3. Iniciar los preparativos del Warmsite. ☐ 4. Confirmar condiciones del Warmsite ☐ 5. Verificar servidores y sistemas operativos. ☐ 6. Instalar aplicaciones correspondientes. ☐ 7. Cargar base de datos y restaurar el último backup. ☐ 8. Verificar si la información es correcta. ☐ 9. Verificar la seguridad lógica de Warmsite. ☐ 10. Activar Warmsite. ☐

5.3.4 Restauración

El orden de recuperación de las aplicaciones se hará de acuerdo a la criticidad de los sistemas: soporte al producto del cliente, sistemas de apoyo: tecnología informática y telecomunicaciones y la nómina.

Los dos primeros sistemas deben recuperarse en un plazo no mayor de 24 horas después del desastre, los demás pueden esperar un plazo de no mayor a las 48 horas siguientes.

Una vez los sistemas restaurados, el equipo de unidades de negocio realizará las comprobaciones necesarias que certificarán que dichos sistemas funcionan de manera satisfactoria y así continuar dando el servicio.

5.3.5 Vuelta a la Normalidad

En esta parte se plantearán las diferentes estrategias y acciones para recuperar la normalidad total del funcionamiento de la organización.

Se efectuaran las siguientes actividades:

- Asegurar que todos los equipos estén en su estado normal para su funcionamiento.
- Iniciar los preparativos para regresar las instalaciones de Stream.
- Activar el centro de datos de la empresa.
- Desactivar el warmsite
- Emitir comunicado.

Escenario #1: lista de actividades a realizar en caso de un virus en el sistema.

Checklist #3

Amenaza	Acciones:
Virus en el sistema	1. Notificar al personal de TI encargado. ☐ 2. Detectar e identificar el virus y equipos afectados. ☐ 3. Proceder a desinfectar los archivos infectados, eliminar el virus. ☐ 4. Aplicar parches correspondientes. ☐ 5. Evaluar daños en el sistema. ☐ 6. Restaurar archivos en caso necesario. ☐ 7. Notificar al equipo de recuperación. ☐ 8. Evaluar necesidad de activar warmsite. .☐

Escenario # 2: lista de actividades a realizar en caso de una pérdida de la base de datos.

Checklist # 4

Amenaza	Acciones:
Pérdida de Base de Datos	

1. Notificar al personal de TI encargado. ☐

2. Confirmar la perdida de información. ☐

3. Cargar el último Back-up. ☐

4. Restaurar la data perdida. ☐

5. Confirmar restauración e integridad de datos. ☐

6. Evaluar y documentar daños. ☐

7. Notificar al equipo de recuperación. ☐

8. Evaluar necesidad de activar warmsite. . ☐

Escenario # 3: lista de actividades a realizar en caso de una falla en la energía eléctrica.

Checklist # 5

Amenaza	Acciones:
Falla de Energía Eléctrica	1. Notificar al personal de mantenimiento encargado. ☐ 2. Verificar que el sistema redundante se haya activado de inmediato y sin problemas. ☐ 3. Activar generador de emergencia. ☐ 4. Verificar que todos los equipos estén funcionando ☐ 5. Contactar la generadora para saber la hora que se restablecerá el servicio ☐ 6. Evaluar necesidad de contratar generador a terceros. ☐ 7. Notificar al equipo de recuperación. ☐ 8. Evaluar necesidad de activar warmsite. ☐

Capitulo VI.

Programa de Capacitación y Concientización.

Capitulo VI.
PROGRAMA DE CAPACITACIÓN Y CONCIENTIZACIÓN.

En este capitulo se expone lo relacionado a la Fase No.4 del DRP, en el mismo se presentan las diferentes acciones que se desarrollarán para capacitar y concienciar al personal de Stream Global Services.

6.1 Programa de Capacitación y Concientización. Generalidades

Para preparar un programa de capacitación y concientización se deben seguir los siguientes pasos:

- Definir objetivos de concientización y entrenamiento
- Desarrollar e implementación de los programas de entrenamiento.
- Desarrollar programas de concientización.
- Identificar otras oportunidades de educación.

6.2 Definición de Objetivos de Concientización y Entrenamiento.

El objetivo principal del Plan de Concientización y Entrenamiento es:

“Crear una cultura pro-activa hacia los desastres y que el personal este consciente de las posibles repercusiones de los mismos dentro de la organización”.

Otros objetivos más específicos son:

- Capacidad de reacción frente a un desastre.
- Disponer de las informaciones y recursos necesarios para enfrentar el posible desastre.
- Conocer la lista de emergencias a contactar en el momento de daño.

6.3 Desarrollo Programa de Entrenamiento y Concientización.

Es necesario si no obligatorio comenzar el entrenamiento desde que el empleado es reclutado. El entrenamiento de los empleados en Stream particularmente aquellos que deben formar parte del equipo de emergencia es un requerimiento a ser completado lo más pronto posible. Se sugiere el siguiente esquema para introducir los empleados hasta la velocidad de reacción o conocimiento requerida en los procedimientos de recuperación:

Procedimiento de revisión - una semana: una de las primeras asignaciones para los nuevos miembros del personal es la revisión de todos los documentos del procedimiento para la recuperación de desastres.

Análisis del impacto sobre la empresa: los nuevos miembros del personal deben leer el análisis del impacto sobre la empresa para ayudarles a ver el panorama sobre los procesos críticos del negocio.

Recorridos: invitar a los nuevos miembros del personal a realizar recorridos, incluso si son sólo observadores. Un paseo de observación los expone a la idea detrás del BIA, los planes y los procedimientos de recuperación.

Simulaciones: este paso servirá para conocer qué tipo de habilidades de gestión y de liderazgo posee el personal existente en caso de emergencias.

Simulaciones paralelas: la participación de nuevos miembros del personal en estas pruebas sirve para extender la experiencia alrededor de los otros empleados, ya que nunca se sabe quien estará disponible para ayudar en un desastre real, por lo que mientras más número de personas que tengan experiencia práctica, mejor.

Meta formal: motivar a la incorporación de todo el personal en la planificación de la recuperación de desastres.

Capacitación formal e informal: Introducir al personal a la cultura de la recuperación de desastres en la planificación de la organización mediante la creación de clases de formación y colocación de carteles con mensajes referentes al DRP.

6.4 Identificación de otras Oportunidades de Educación.

Los miembros del equipo de emergencia se podrían enviar a tomar conferencias internacionales sobre el manejo de crisis, mitigación de riesgos, entre otros.

Además, se podría otorgar acreditaciones de cursos sobre planificación de desastres.

A continuación se muestra la tabla del plan de actividades a desarrollar durante la sesiones de entrenamiento.

Conferencia/Sesión de entrenamiento

Patrocinado por: **Stream Global Services**

	Lunes	Martes	Miércoles	Jueves	Viernes
9:00-9:30	Introducción al DRP	Que es el BIA?	Prevención	Organigrama empresarial	Ventajas de la experiencia
9:30-10:30	Necesidades y beneficios de la recuperación de desastres	Entendiendo su propósito, y enfoque	Estrategias de protección de claves	Equipos de emergencia	Simulación de Escenario de emergencia
10:30-10:45	*Receso*	*Receso*	*Receso*	*Receso*	*Receso*
10:45-11:15	Efectos de un Desastre	Activos mas importantes "Personas, Procesos, TI"	Ayuda de escritorio	Lista de contactos	Inundaciones
11:15-11:45	Desastres menores		Reportar incidentes	Cuando llamar a quien?	Tormentas
11:45-1:15	*Almuerzo*	*Almuerzo*	*Almuerzo*	*Almuerzo*	*Almuerzo*
1:15-1:45	Como un desastre podría afectar su organización	Amenazas, riesgos y vulnerabilidades	Detectar situación	Liderazgo en desastres	Incendios
1:45-2:15			Control de acceso	Trabajo en equipo	Terremotos
2:15-2:30	*Receso*	*Receso*	*Receso*	*Receso*	*Receso*
2:30-3:00	Rol de la prevención	Escenarios de desastres	Confidencialidad de información de la empresa	Puesta en marcha del plan	Salidas de emergencia
3:00-3:30				Sitios alternos	Importancia del tiempo
3:30-3:45	*Receso*	*Receso*	*Receso*	*Receso*	*Receso*
3:45-4:15	Rol de la planeación	Errores humanos	Hackers, virus, E-mails, USB, CD's, Chateo y mas	Transición	Donde ubicarse
4:15-4:45		Como reaccionar frente a un desastre		Vuelta a la normalidad	Poder de la calma
4:45-5:00	Prevención en casa		Como protegerse	Preservando el plan	Compromiso individual

Capitulo VII

Plan de Comunicación Ante Crisis

Capitulo VII
PLAN DE COMUNICACIÓN ANTE CRISIS

Un plan de comunicación de crisis es un documento que contiene los procedimientos internos y externos que las organizaciones deben preparar ante un desastre. Este plan debe estar coordinado con los demás planes para asegurar que sólo comunicados aprobados sean divulgados y que solamente personal autorizado sea el responsable de responder las diferentes inquietudes y de diseminar los reportes de estado al personal y al público.

A través de la comunicación de crisis es posible indicar el equipo involucrado en la toma de decisiones, establecer las líneas de comunicación a seguir, los voceros responsables con quienes centralizar la difusión de la información así como las estrategias de relaciones públicas a seguir con las audiencias involucradas como medios de comunicación, autoridades, público afectado, empleados, comunidad en general, etc. que le permitan a la organización ser un emisor ágil y confiable, que proporcione de manera consistente datos verificados, evite especulaciones y vacíos que serían llenados por rumores o información imprecisa.

7.1 Objetivos:

- Indicar las líneas y flujos de comunicación que prevalecerán durante una crisis
- Definir los miembros del comité de crisis
- Establecer los pasos de acción de cada miembro del comité

- Ofrecer las posiciones oficiales pre-elaboradas de acuerdo al tipo de crisis

7.2 Plan de Comunicación de Crisis de Stream Global Services

Tan pronto como se produzca la crisis o se sospeche que se produce, el equipo relaciones públicas deberá ser notificado por el equipo de respuesta a emergencias, y provisto de la siguiente información:

1. ¿Qué ha sucedido?
2. ¿Cuando sucedió?
3. ¿Hay algún empleados o del público en cualquier peligro?
4. ¿Quiénes son los afectados?
5. ¿Qué materiales, de personal y suministros están disponibles?

Con esta información, el equipo de relaciones públicas de Stream determinará un modo de comunicación y empezar a preparar una declaración que incluya todos los hechos que se han confirmado. Esta declaración será actualizada a medida que más información esté disponible. Una vez aprobada la declaración se pondrá a disposición de los medios de comunicación y otros afectados.

La cobertura de los medios de comunicación determinan en gran medida de cómo los clientes, los empleados y el público percibe la empresa en una crisis. Todos los miembros de los diferentes equipos deben comprometerse a la comunicación clara y abierta. Se informará al público de los hechos tan pronto como sea posible y con honestidad

Formato usado por Stream para la Difusión de Información a los afectados.

Afectados por la Interrupción	Persona Responsable de Coordinar las Comunicaciones		
	Nombre	**Posición**	**Detalles de Contacto**
Clientes			
Gerencia y Empleados			
Proveedores			
Medios			
Otros			

Si alguien del equipo de relaciones públicas recibe una llamada telefónica de un miembro de los medios de comunicación o de algún cliente en relación con la crisis que se esta tratando o de otro tema que podría dar lugar a una publicidad negativa. Debe tomar las siguientes medidas para la gestión de la situación:

- No divulgar cualquier información o hacer una declaración si previo consenso de todos los miembros del comité.
- No dar opinión personal o especular sobre lo que se piensa puede ser verdadero o falso.
- Tener la información acabada y bien detallada de modo que a la hora de su difusión esta no se preste a mal entendido ni manipulación por parte de los afectados.

7.3 Formulario de Información para los Medios de Comunicación

Llamada recibida por: _____

Fecha: _____

Hora: _____

1. Nombre del reportero:
_____

2. Nombre de la institución: _____

3. Teléfono #: _____

4. Motivo de la llamada: _____

5. Preguntas especifica para la persona a entrevistar:
_____

_____

6. Solicitud: conferencia de prensa _____ Entrevista _____

Capitulo VIII.
Pruebas y Ejercicios

Capitulo VIII.
PRUEBAS Y EJERCICIOS

La fase No.5 del DRP consiste en la realización de ensayos para verificar la operabilidad del plan. En este capitulo se exponen los diferentes métodos de pruebas sugeridos para Stream Global Services.

8.1 Pruebas y Ejercicios. Conceptualización.

El plan de recuperación de desastres no se encuentra del todo completo hasta no ser verificado mediante exitosas pruebas que demuestren el buen funcionamiento de este y que aseguren la viabilidad de las estrategias de solución adoptadas.

Realizar pruebas se ha convertido en parte natural del ciclo de vida de la mayoría de los esfuerzos por realizar desarrollo tecnológicos, por ejemplo desarrollo de software, procesos y también el plan de recuperación de desastres, a continuación se muestra una grafica que representa el ciclo de vida de un DRP.

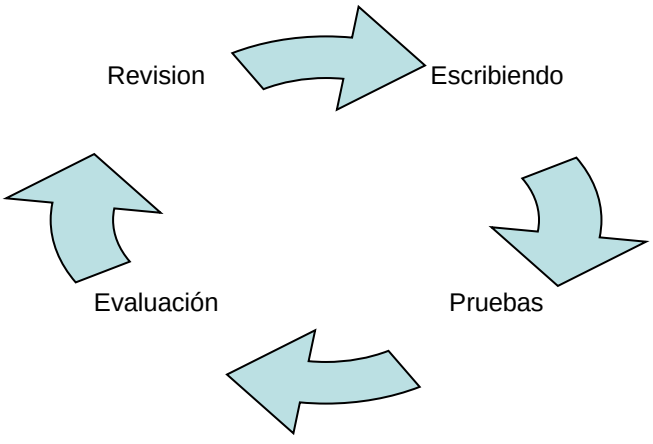


Figura 7.0 Ciclo de vida de un DRP.

8.1.1 Objetivos

Un Plan de Pruebas tiene como objetivos:

• Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la compañía.

• Probar la efectividad y los tiempos de respuesta del Plan para comprobar que están alineados con la definición realizada en el diseño.

• Identificar las áreas de mejora en el diseño y ejecución del Plan.

• Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.

• Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.

• Concienciación y formación para los empleados a través de la realización de pruebas.[7]

8.1.2 Tipo de pruebas

Las pruebas de un plan de recuperación de desastres deben tener dos características principales:

[7] Del Pino Jiménez, Laura. Guía de Desarrollo de un Plan de Continuidad de Negocio. Escuela Universitaria de Informática de la Universidad Politécnica de Madrid. Madrid. 2007.

Realismo: La ventaja de las pruebas se reduce con la selección de escenarios ficticios. Aquí radica la importancia de reproducir escenarios que proporcionen un nivel de entrenamiento adecuado a las situaciones de riesgo.

Exposición Mínima: Las pruebas deben diseñarse de forma que impacten lo menos posible en el negocio, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible para el negocio.

En algunos casos puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocio. Por eso, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo.

8.1.3 Ejercicios Técnicos

Los ejercicios en si representan los diferentes escenarios que se pueden realizar para la evaluación de estas pruebas comprendidas por sus dos características básicas, realismo y exposición mínima.

Los ejercicios de pruebas se componen pero no se limitan a:

- Orientaciones.
- Simulaciones.
- Simulaciones parciales.
- Funcional.
- Ejercicios paralelos.

Este tipo de ejercicio requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado.

Algunos ejemplos de elementos verificados durante un ejercicio de simulación son:

- Procedimientos de emergencia.
- Métodos alternativos.
- Líneas de telecomunicaciones de backup.
- Procedimientos de notificación Vendedores / Clientes.
- Capacidad y rendimiento del hardware.
- Portabilidad del software.
- Accesibilidad al centro de respaldo.
- Movilización de los equipos de trabajo.
- Recuperación de ficheros y documentación almacenados en lugar externo.
- Recuperación de datos.

8.2 Pruebas y ejercicios en Stream

Todos los equipos son responsables de estar familiarizados con el DRP, y se reunirán cada trimestre para revisar el manual y sugerir las actualizaciones de acuerdo a los cambios en la infraestructura física y organizacional como los cambios de personal, cambios de política, de comunicación, entre otros. Las actualizaciones son completadas por el Coordinador en del DRP y debería producirse en los siguientes casos:

1. Revisión trimestral de las reuniones.
2. Después de cada caso de emergencia.
3. Después de los cambios en el personal clave.

El administrador del DRP se encargará de coordinar reuniones trimestrales de los diferentes equipos, otras reuniones necesarias, y preparar planes de evacuación y la construcción de lugares designados para los equipos y de los miembros del Equipo de Respuesta de Emergencia para atender en caso de una evacuación.

Todos los equipos llevarán a cabo ejercicios de los procedimientos del DRP en un mínimo de dos veces al año. A pesar que los Ejercicios no implicarán a toda la población del lugar, los miembros de los equipos de respuesta y todo el personal administrativo que no estén incluidos en un equipo de respuesta deben participar. A lo largo del año diferentes niveles de los ejercicios se llevarán a cabo por los diferentes equipos. Mientras que el equipo de respuesta podrá llevar a cabo ejercicios limitados a funciones o de escala completa, los otros equipos realizarán pruebas principalmente de mesa. En Stream serán completados dos ejercicios cada año. Acontecimientos reales se consideran como ejercicios.

8.2.1 Tipos de ejercicios a realizar

Orientación - La orientación es una introducción o revisión de los procedimientos del plan, la organización o ideas sobre el DRP. Un ejemplo de ello es la presentación de un panorama general de gestión de crisis de un sitio / programa de recuperación del negocio.

Simulación parcial – En esta actividad se pone a prueba, se desarrolla o se da mantenimiento a una sola fase de respuesta de emergencias o de procedimientos de recuperación. Un ejemplo de esto son los ejercicios de comunicación entre los diferentes equipos de emergencias o también la simulación de un incendio.

Esta será la primera a prueba a ser realizada por el equipo de TI, dirigida por el gerente de TI, aquí se comprobaran las siguientes partes del plan.

Perdida accidental de información

Antes de realizar esta prueba el gerente de TI debe presentar el presupuesto a ser requerido para la realización de esta prueba al director del site. Aquí presentara todos los detalles de la prueba a ser realizada.

Se someterán a prueba tanto el software de Back up como los discos y cintas utilizadas para back up, tomando solo una de estas y dejando la otra en funcionamiento en la empresa para así no dejarla sin ningún tipo de almacenamiento alterno, lo primero a realizar es la comunicación de esta a

prueba al proveedor de servicios en el sitio alterno para que esté al tanto de la prueba y tenga todos sus equipos listos y en espera de nuestro equipo.

Este equipo seleccionado por el gerente de TI, se trasladara al sitio alterno con los discos de back up del site completo para verificar el buen funcionamiento de estos. Serán 4 integrantes lo que se encargaran de realizar la prueba, uno de ellos tendrá la responsabilidad de documentar todos los resultados de la prueba y determinar las partes funcionales y notificar que necesita mejoras.

Antes de poner en prueba el buen funcionamiento estos deben verificar la compatibilidad de versión de los diferentes software que están envueltos y la correcta conectividad de la red disponible en el sitio alterno, luego poner en marcha los discos de back up y verificar el buen funcionamiento de toda la data. Las anotaciones deben ser realizadas en el mismo momento de ser realizada la prueba.

Ejercicio sobre mesa – Este ejercicio esta destinado a ser una prueba de bajo estrés y costos, es una prueba que se realiza con lentitud y precisión con el propósito de clarificar los roles y responsabilidades en respuesta a un desastre mayor. Los eventos en este tipo de ejercicio no son visibles, ya que son presentados y analizados sólo en papel. El movimiento del personal también es presentado en papel solamente.

Funcional – Ejercicios funcionales están designados para familiarizar a los miembros de los diferentes equipos con cual es su rol y responsabilidad dentro de un ambiente simulado de desastre. Todo es realizado sólo a nivel de documentación, y no es necesario movilizar al personal de la empresa en este tipo de ejercicios.

Simulaciones – Este ejercicio busca las respuestas por parte de los miembros de los diferentes equipos a un escenario simulado. Debido a la relación de generación de beneficios y continuidad de negocios que posee Stream. Una simulación completa esta prohibida de tener algún tipo de costo en referencia a la productividad de la empresa. Una versión modificada será realizada involucrando al equipo de emergencia y miembros de la alta gerencia de Stream.

Capitulo IX.

Mantenimiento y Actualización del Plan.

Capitulo IX.
MANTENIMIENTO Y ACTUALIZACIÓN DEL PLAN.

En este capítulo se aborda la última fase se detallan los diferentes procedimientos para favorecer el mantenimiento y la actualización del Plan de Recuperación de Desastres propuesto para Stream.

9.1 Generalidades del Proceso de Mantenimiento y Actualización.

Todo plan debe tener una estrategia de apoyo que contribuya a su mantenimiento y vigencia. Los objetivos de este proceso se pueden enunciar como sigue:

- Desarrollar de los procedimientos de mantenimiento del Plan de Recuperación.
- Diseñar de la estrategia de mantenimiento y actualización.

9.1.1 Consideraciones a tomar en cuenta al momento de las Actualizaciones

- Cambios en el personal clave.
- Cambios en el organigrama (Ej. Creación de nuevas posiciones);
- Cambios de dirección / teléfono de algún componente del equipo de recuperación.
- Cambios en cualquier equipo o dispositivo informático incluido dentro del esquema de recuperación.

- Cambio en algún procedimiento.
- Reubicación de instalaciones.
- Nuevos proveedores para los recursos críticos.
- Cambios en la configuración de los sistemas o los dispositivos de almacenamiento (Storage).
- Cambios en la configuración de comunicaciones o de las redes.

9.1.2 Elementos mínimos a tener en cuenta en las revisiones del plan:

- Requerimientos operacionales.
- Requerimientos de seguridad.
- Procedimientos técnicos.
- Hardware, software y otros equipos (tipos, especificaciones y cantidad).
- Nombres e información de contacto de los miembros de los equipos de recuperación.
- Nombres e información de contacto de los proveedores.
- Archivos vitales (impresos y electrónicos).
- Necesario realizar manteamientos al DRP y de esta manera conservarlo como un documento vivo y no obsoleto en caso de emergencias.

9.2 Plan de Mantenimiento y Actualización de Stream.

Debido a que las organizaciones son entes cambiantes en una constante búsqueda de la eficientización de sus procesos y actualización de sus activos

informáticos para que den mejor repuestas a las necesidades planteadas es necesario trazar estrategias de mantenimiento y actualización.

En Stream para dar respuesta a esta necesidad el plan a seguir es el siguiente en lo referente al *mantenimiento* y *Actualización*:

En las reuniones pautadas a ser realizadas cada trimestre los miembros de los diferentes equipos del DRP deben realizar recomendaciones para la actualización del DRP de acuerdo los cambios en la infraestructura física y organizacional.

Una actualización de la lista de contacto debe ser realizada cada 90 días para asegurar que toda la información de los contactos es correcta y funcional. Una auditoria a mayor escala de toda la información y funciones debe completarse una vez al año para asegurar la actualización de todos los procesos que lo requieran. En caso de ponerse en marcha el plan de recuperación de desastre y uno de los miembros de los diferentes equipos no se encuentra disponible, el administrador del DRP es responsable de asumir las responsabilidades de esa persona o de asignar esa funciona a otra.

CONCLUSION

Con la implementación de un Pan de Recuperación de Desastres (DRP) cualquier empresa sin importar la industria a la que pertenece asegura su continuidad y sobre vivencia. Con el mismo se logra la protección no sólo de vidas humanas sino también de equipos tecnológicos reduciendo la confusión en tiempo de crisis para así tomar decisiones mucho más efectivas, igualmente ayuda a recuperar de forma oportuna las áreas críticas del negocio mitigando los riesgos, protegiendo a los activos.

Hoy en día los negocios son más y más dependientes de la tecnología, ya que la gran mayoría de las organizaciones tienen sus sistemas productivos y financieros automatizados y computarizados. De esta forma es crucial contar con un plan para sostener el flujo de los negocios ante siniestros que imposibiliten el uno de dichos recursos.

En el estudio realizado se demostró el hecho de que Stream actualmente necesita implementar un plan de recuperación efectivo para garantizar la continuidad de sus procesos críticos durante un eventual desastre, la misma en caso de no seguir las recomendaciones realizadas podría mermar sus operaciones de manera definitiva, con el seguimiento de las pautas presentadas el poder de reacción y sobre vivencia ante cualquier desastre incrementa y disminuye los efectos causados por estos. De la misma manera se realizaron estudios que ayudan a la solución mas optima en lo referente a costo, eficacia y

prontitud, ya que se analizaron los procesos que representan la vida misma de la empresa.

El presente estudio muestro las pautas para la implementación y puesta en marcha del plan de recuperación desastre, y también el mantenimiento que debe darse a este como un documento vivo y de gran importancia para la compañía.

Con todos los factores expuestos, entendemos, el plan de recuperación de desastres aplicado sobre el negocio no debe sólo responder a la pregunta de cuánto necesito invertir en infraestructuras de respaldo sino que debe servirnos para determinar qué grado de respaldo que debemos proporcionar a nuestros sistemas e infraestructuras que apoyan la organización.

RECOMENDACIONES

A través de los resultados obtenidos durante el plan se sugiere lo siguiente para Stream:

1. Debe aplicarse el DRP a los diferentes procesos existentes en una empresa de Call Center para garantizar la sobre vivencia de esta ante un desastre.

2. Poner en práctica evaluaciones periódicas de los diferentes factores tecnológicos, climáticos, humanos, políticos y económicos que afectarían el normal desenvolvimiento de la empresa, para analizar si las medidas consideradas en el DRP son aún vigentes o deben ser actualizadas.

3. Debe considerarse el plantear escenarios de desastre que servirán de base al momento de determinar las alternativas viables para la recuperación.

4. La alta gerencia de Stream debe estar disponible para decidir la activación del plan y tomar las decisiones no previstas en un tiempo oportuno y con la seriedad que el caso amerita, pues alguna desconsideración de algún análisis y estimaciones de costos puede provocar un caos a la empresa en el momento que llegue a materializarse el desastre.

UNIVERSIDAD APEC
UNAPEC

FACULTAD DE HUMANIDADES Y CIENCIAS
DECANATO DE INFORMATICA

IMPLEMENTACIÓN DE UN PLAN DE RECUPERACION DE DESASTRES PARA EMPRESAS DE CALL CENTER EN LA REPÚBLICA DOMINICANA. "CASO STREAM GLOBAL SERVICES"

Sustentantes:
Cristian Ariel Pérez Cleto **2000-2513**
Mario De Los Santos **2004-0124**

Asesor:
Ramón Gómez

Anteproyecto de la Monografía para Optar por el Título de:
INGENIERO EN SISTEMAS DE COMPUTACIÓN

Distrito Nacional, República Dominicana
Junio 2009

Índice

Pag.

1. SELECCIÓN DE TITULO Y DEFINICIÓN DEL TEMA

1.1 Titulo:

Implementación de un plan de recuperación de desastres para empresas de call center en la república dominicana. "caso Stream Global Services"

1.2 Definición del Tema:

Peter Gregory (CISA, CSISP) en su libro "Plan de recuperación de Desastre" (IT Disaster Recovery Plannning) define como recuperación de desastres todo lo relacionado con la preparación y respuesta cuando un desastre sucede. El objetivo principal del mismo es la supervivencia de la organización.[8]

En un mundo en miras a una globalización cada vez más amplia, y una expansión cada vez mayor de los países que ofrecen servicios de subcontratación (outsourcing), definido por la enciclopedia libre "Wikipedia" como el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

Un plan de recuperación de desastres, es una rama especifica de un plan de continuidad de negocios sólo que el mismo aboga por preservar la infraestructura tecnológica en las organizaciones.

La eficacia de un buen plan de recuperación de desastres con políticas y procedimientos previamente establecidos y probados garantizará la entrega de los servicios necesarios que se requieren en los procesos críticos de la empresa para la continuidad y supervivencia de las operaciones del negocio en un momento dado.

Este trabajo se centrará en el desarrollo de un plan estructurado de recuperación de desastres para la empresa Stream Global Services, la cual cuenta con 3 sucursales en Santo Domingo y la misma es una de las empresas que mayor crecimiento de su generó en estos momentos.

[8] Peter Gregory (2008). IT Disaster Recovery Planning for Dummies. Wiley Publishing, Inc.

2. PLANTEAMIENTO DEL PROBLEMA

Si una persona se remonta a los antecedentes históricos del mundo, encontraría un sinfín de casos en los que han ocurrido desastres de todo índole, no sólo de la naturaleza sino también provocados por personas. Algunos ejemplos de los primeros que se podrían citar son: fuegos, inundaciones, huracanes, temblores, erupciones, entre otros. Mientras que de los segundos, se pueden mencionar: retaliaciones, incidentes de seguridad, fallas de equipos, interrupciones eléctricas, sabotaje, terrorismo, huelgas, entre otros.

Los eventos antes mencionados tienen el potencial de infligir no sólo daños a edificios sino también a equipos y sistemas tecnológicos; ocasionando la interrupción del ritmo normal de las operaciones de las organizaciones. Por tal razón, muchas empresas a nivel mundial se han preocupado por desarrollar planes para auxiliarse con herramientas que le permitan garantizar una rápida vuelta a la normalidad ante la presencia de cualquier eventualidad, por lo tanto, el hecho de diseñar y preparar un plan de recuperación de desastres no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, la búsqueda de mecanismos de seguridad para proteger a la información de las diversas amenazas a las que se ve expuesta y supone un importante avance a la hora de superar todas aquellas adversidades.

Sin embargo, en empresas ubicadas en países en desarrollo sólo se preocupan en gran medida por establecer políticas de protección y seguridad a sus equipos tecnológicos muy pobres.

Stream Global Services con 3 sucursales ubicadas en el Distrito Nacional del país, es de sumo intereses analizar y desarrollar nuevos planes de recuperación de desastres para dichas empresas con miras a preservar y garantizar sus recursos informáticos ante hechos potencialmente devastadores, no solo de índole natural o humano sino también como de origen técnico (fallas del hardware, del software, con el suministro de energía, etc.). Y es casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden llegar a ser catastróficas para los intereses de cualquier organización.

La empresa Stream Global Services en la actualidad no cuenta con las adecuadas estrategias, técnicas, procedimientos y usos orientados a prevenir, controlar y evaluar los efectos producidos por cualquier tipo de siniestro. Esta empresa cuenta en estos momentos con planes de backup, recuperación de data y varios sistemas alternos que en caso de emergencia son puestos a operar para mantener parcialmente algunos procesos críticos, pero el tiempo de

respuesta a estas eventualidades no es satisfactorio. Como ejemplo a lo antes mencionado se puede citar el hecho de que en esta se han observado casos en que el sistema de energía eléctrica se ha suspendido por un tiempo prolongado llevando al fallo de los sistemas de UPS y generadores eléctricos, los cuales han ocasionado el cese de las operaciones completas de la empresa, y teniendo como resultado perdidas cuantitativas en un corto periodo de tiempo.

Además, la compañía no cuenta con un equipo formado y entrenado para casos de recuperación de desastres propiamente dicho. Estos elementos mencionados pueden en un momento dado ocasionar, si sucede un siniestro, indisponibilidad, falta de Integridad y confidencialidad, replicación y pérdida de control de acceso a la data de la organización. Además la eventual pérdida de los sistemas de comunicaciones y redes de la empresa.

Estos males impactan grandemente la imagen interna y externa de la empresa, la credibilidad de los clientes corporativos y la competitividad en el mercado.

Es por todo lo antes mencionado que la finalidad de este estudio es el diseño de un plan de recuperación de desastres para dicha empresa; a fin de que la misma continúe sus operaciones pese a cualquier desastre.

3. OBJETIVOS DE LA INVESTIGACIÓN

3.1 Objetivo General:

Diseñar un plan de recuperación de desastres que permita garantizar que los recursos tecnológicos no afecten los servicios que provee la empresa Stream Global Services al exterior y los procesos críticos internos operen a un nivel aceptable durante un evento de crisis y logren su normalidad después de ésta.

3.2 Objetivo Específicos:

Definir a que se llama plan de recuperación de desastres.

Investigar la importancia de diseñar e implantar un plan de continuidad de negocios.

Delimitar y describir los procedimientos de un plan de continuidad de negocios.

Explicar que engloba el concepto plan de recuperación de desastres; definir sus ventajas y desventajas.

Proteger y conservar los activos de TI de la empresa de riesgos, desastres naturales o actos mal intencionados.

Mitigar los efectos causados por un eventual desastre, mediante la adecuada planeación y control.

Investigar los procesos de negocio que se realizan en la compañía.

Establecer la relación de aplicaciones que soportan los procesos de la compañía.

Determinar los niveles aceptables de riesgos y las alternativas.

Investigar los lineamientos estratégicos de Stream.
(Misión, visión, valores, estructura organizacional y situación actual).

4. JUSTIFICACIÓN DE LA INVESTIGACION

4.1 Justificación Teórica

Basado en las diferentes teorías que se han escrito sobre planes de recuperación de desastres podemos resaltar las ventajas descritas por Laura del Pino Jiménez en su guía de desarrollo de un plan de continuidad de negocio, tales como identificar los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización, obligar a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.

Además prevenir o minimizar las pérdidas para el negocio en caso de desastre, clasificar los activos para priorizar su protección en caso de desastre y finalmente aportar una ventaja competitiva frente a la competencia.[9]

4.2 Justificación Metodológica

Básicamente en el presente estudio se utilizarán los lineamientos ofrecidos por los planes de continuidad de negocios. Debido a que los planes de recuperación de desastres son una parte esencial de los mismos. Solo que estos se enfocan en la preservación de los equipos tecnológicos.

4.3 Justificación Práctica

Un plan de recuperación de desastres forma parte de un programa del todo relacionado con sus partes determinado por los requerimientos del negocio. Este proporciona un medio probado para enfrentar crisis derivadas de desastres.

Con la implementación del mismo cualquier empresa sin importar la industria a la que pertenece asegura su continuidad y sobre vivencia. Con el mismo se logra la protección no sólo de vidas humanas sino también de equipos tecnológicos reduciendo la confusión en tiempo de crisis para así tomar decisiones mucho más efectivas, igualmente ayuda a recuperar de forma

[9] Laura Del Pino Jiménez (2007). Guía de desarrollo de un plan de continuidad de negocios. Madrid, España: Universidad Politécnica de Madrid.

oportuna las áreas críticas del negocio mitigando los riesgos, protegiendo a los activos.

Se debe tener en cuenta que en la actualidad la productividad de las empresas se basa en una gran proporción en sus equipos tecnológicos. Una falla en cualquiera de estos puede ocasionar perdidas incalculables. De ahí radica la importancia de tener un plan de recuperación de desastres en el área tecnológica.

5. TIPO (S) DE LA INVESTIGACIÓN:

Las técnicas de investigación utilizadas para el desarrollo del tema serán las siguientes:

- Documental: Se analizara información de fuentes escritas sobre diferentes tipos de planes de recuperación de desastres en el área de tecnología (datos de la empresa, búsquedas en Internet con la finalidad de obtener información actualizada del tema, revistas, consultas de libros, etc.).

- Descriptiva: En esta etapa de la investigación se trataran los rasgos, cualidades y características de lo que será el desarrollo de un modelo de plan de recuperación de desastres.

- Estudio de caso: Cuyo resultado será la implementación de un plan de recuperación de desastres en el área de tecnología. La empresa escogida es Stream Global Services, específicamente sus sucursales localizadas en la República Dominicana y es en donde demostraremos los beneficios que este plan ofrece.

- Histórico: Ya que se harán menciones de desastre ocurridos relacionados con el objeto de este estudio.

6. MARCO DE REFERENCIA:

6.1 Marco Teórico:

Plan de Continuidad del Negocio (BCP) es el resultado de la aplicación de una metodología interdisciplinaria, llamada Cultura BCM, usada para crear y validar planes logísticos para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción o desastre. Estos planes son llamados Planes de Continuidad del Negocio.

En lenguaje sencillo, BCP es el cómo una organización se prepara para futuros incidentes que puedan poner en peligro la organización y su misión básica a largo plazo.

Un Plan de Continuidad de Negocio, a diferencia de una Plan de recuperación de desastres, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado.

Un plan de recuperación de desastres consiste en la identificación de aquellos sistemas de información y/o recursos informáticos aplicados que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la organización, con el propósito de estructurar y ejecutar aquellos procedimientos y asignar responsabilidades que salvaguarden la información y permitan su recuperación garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible y a unos costos razonables.

El plan de recuperación de desastres debe cubrir todos los aspectos que se van a adoptar tras una interrupción, lo que implica suministrar el servicio alternativo y para lograrlo no solo se deben revisar las operaciones cotidianas, sino que también debe incluirse el análisis de los principales distribuidores, clientes, negocios y socios, así como la infraestructura en riesgo. Esto incluye cubrir los siguientes tópicos: hardware, software, documentación, talento humano y soporte logístico; debe ser lo más detallado posible y fácil de comprender.

Se puede considerar como un desastre la interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede

remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Ejemplos obvios son los grandes incendios, las inundaciones, los terremotos, las explosiones, los actos de sabotaje, etcétera.

Estadísticas recientes sobre los tipos más comunes de desastres que ocurren muestran que el terrorismo, los incendios y los huracanes son las causas más comunes en muchos países.[10]

Terrorismo: 17.5%
Incendios: 17.5%
Huracanes y tornados: 14.0%
Terremotos: 10.5%
Interrupción del suministro de energía eléctrica: 9.5%
Errores en el software: 8.8%
Inundación: 7.0%
Errores en hardware: 5.3%
Interrupción de servicio en la red: 3.5%
Rotura de tuberías: 3.5%
Otros: 2.9%

Las consecuencias de estos incidentes sobre las organizaciones que no tienen un plan de continuidad de negocio pueden llegar a ocasionar incluso el cierre de las mismas. Se puede tomar como ejemplo las siguientes cifras:

- Un 43% de las organizaciones después de un accidente no podrán continuar sus operaciones viéndose obligadas a cerrar.

- Un 80% tendrán que hacerlo en menos de 13 meses.

- Un 53% de los clientes de estas organizaciones no recuperarán las pérdidas causadas por los daños derivados.

- Un 50% se verán forzadas a cerrar antes de cinco años después del desastre.

A pesar de que los efectos inmediatos de un desastre aparentemente son la pérdida de beneficios por la parada de actividad puntual y la incapacidad para proveer servicios críticos, no son éstos los efectos más perniciosos que un incidente de este tipo provoca.

[10] Cámara de comercio de Londres (2007).

Otros efectos derivados que pueden causar un gran impacto en la compañía son la pérdida de reputación de cara a los clientes, o la pérdida de ventaja competitiva con otras compañías.

Casos en los que se requiere aplicar un plan de recuperación de desastres:

- Si falla alguno de sus sistemas críticos y/o si se contamina alguno de sus sistemas críticos con información no compatible proveniente del exterior.
- Si falla algún sistema de telecomunicaciones o enlace.
- Si falla alguno de sus proveedores informáticos clave.
- Si falla alguno de sus otros proveedores clave.
- Si falla algún servicio básico.
- Si se presentan fallas encadenadas y generalizadas

6.2 Marco Conceptual:

Para entender lo que es un plan de recuperación de desastres del área de tecnología es necesario aclarar todos los conceptos, equipos y términos que se manejan, ya que esta es un área nueva a nivel tecnológico donde los términos no son comunes ni claros.

Backup (Copia de seguridad): Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento.

BC: Continuidad de negocio, concepto para seguir con las operaciones de una empresas a pesar de cualquier emergencia o contingencia (Business continuity).

BCP: Plan consultivo de continuidad de negocio.

BD: Abreviatura de bases de datos.

Bóveda: Almacenamiento de data a través de cintas, cartuchos, discos, etc.

Call Center: También llamado Centro de Llamadas o Centros de Atención es el departamento de una empresa en donde se atienden y procesan las comunicaciones telefónicas con los Clientes.

Caso de Negocio: consiste en saber cuanto se invierte y cuando se gana en determinado proyecto.

Cold Site: venta de espacio electrónico en los equipos del IDC.

Contingencia: Posibilidad o riesgo de que suceda una cosa.

Continuidad: Duración o permanencia de una cosas sin interrupción.

Desastre: es un hecho natural o provocado por el hombre que afecta negativamente a la vida, al sustento o industria desembocando con frecuencia en cambios permanentes en las sociedades humanas, ecosistemas y medio ambiente.

DPL: Enlacé dedicado de comunicaciones de 128 Mbps.

DR: Es el resguardar solamente la data de los sistemas de computo.

DRI: Instituto de recuperación de desastre el cual impone la reglas y estatus de esta manera de trabajo.
DRP: Plan Consultivo de recuperación de desastre.

Hardware: corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Hold Site: venta exclusiva de espacio fisco y electrónico.

HW: abreviatura de Hardware.

Implementación: Formas y métodos para llevar a cabo algo.

Outsourcing: (subcontratación) es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

Plan: un modelo sistemático que detalla qué tareas se deben llevar a cabo para alcanzar un objetivo, para lo cual se establece metas y tiempo de ejecución.

Plan de Continuidad del Negocio: es el resultado de la aplicación de una metodología interdisciplinaria, llamada Cultura BCM, usada para crear y validar planes logísticos para la practica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción o desastre.

Plan de Contingencia Tecnológico: Este Plan, es un subconjunto y complemento necesario para el Plan de Continuidad de Negocio, está enfocado a resolver las contingencias tecnológicas (escenarios de falla) que impidan entregar los servicios informáticos necesarios que requieren los procesos críticos del Negocio.

SF: abreviatura de Software.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.

Sistema: es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

UPS(Uninterruptible Power Supply): Sistema de alimentación ininterrumpida). Un UPS es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

Workgrup Space: espacio de trabajo que se ofrece a los clientes en caso de que no puedan operar desde sus oficinas, esto incluye: Teléfono, PC, Oficinas, Fax, etc.

6.3 Marco Espacial

Esta propuesta tiene como escenario la empresa de Call Center Stream Global Services ubicada en el Distrito Nacional, Republica Dominicana, específicamente todo lo que abarca sus recursos tecnológicos, sistemas de información y telecomunicación.

6.4 Marco Temporal

El estudio tiene como limite temporal el año 2009. Ya que es en este que se espera llevar a cabo el diseño del plan de contingencia.

7. MÉTODOS, PROCEDIMIENTOS Y TÉCNICAS.

7.1 Métodos

Para recabar las informaciones necesarios para el desarrollo de la presente investigación se utilizarán los siguientes métodos:

- Método de Observación: se utilizara para visualizar internamente la situación actual en lo que respecta a la seguridad de los sistemas y equipos tecnológicos dentro de la empresa a investigar.

- Método Deductivo: Ya que se partirá de premisas generales (Lineamientos de que se basa el plan de recuperación de desastres) hasta llegar a premisas particulares (Diseño del plan de recuperación de desastres).

- Método de Análisis: Se utilizara este método en el proceso de conocimiento en donde se identificaran cada una de las parte que conforman un plan de recuperación de desastres del área de tecnología

- Técnica de la entrevista: Se realizarán entrevistas a profesionales capacitados del área de TI de las diferentes sucursales de la empresa Stream Global Services, además se consultaron otros profesionales del área de sistemas de la universidad APEC.

7.2 Procedimientos:

Los procedimientos que se implementaran para el desarrollo de la investigación estarán basados en los pasos establecidos para el diseño del plan de recuperación de desastres.

8. TABLA DE CONTENIDO

3.2 Selección de la Estrategia

3.3 Desarrollo de la Estrategia de Recuperación

3.4 Infraestructura y Recursos Tecnológicos para el Warm Site

Capitulo IV. Desarrollo del Plan

4.1 Objetivos.

4.2 Organización de los Equipos.
- 4.2.1 *Equipo de Respuesta a Emergencias*
- *4.2.2 Equipo de Recuperación*
- *4.2.3 Equipo de Coordinación Logística*
- *4.2.4 Equipo de Relaciones Públicas*
- *4.2.5 Equipo de Unidades de Negocios*

4.3 Acciones del Plan
- 4.3.1 Respuesta ante el Desastre
- 4.3.2 Transición
- 4.3.3 Recuperación
- 4.3.4 Restauración
- 4.3.4 Vuelta a la Normalidad

Capitulo V. Capacitación y Concientización.

5.1 Programa de Capacitación y Concientización. Generalidades

5.2 Definición de Objetivos de Concientización y Entrenamiento.

5.3 Desarrollo Programa de Entrenamiento y Concientización.

5.4 Identificación de otras Oportunidades de Educación.

Capitulo VI. Pruebas y Ejercicios

6.1 Pruebas y Ejercicios. Conceptualización.
- 6.1.1 Objetivos
- 6.1.2 Tipo de pruebas
- 6.1.3 Ejercicios Técnicos

9. FUENTES DE INFORMACION

Libros:

Gregory, Peter (2008). IT Disaster Recovery Planning. Indiana, USA. Willey Publishing, Inc.

Del Pino Jiménez, Laura (2007). Guía de desarrollo de un plan de continuidad de negocio. Madrid, España. Escuela Universitaria de Informática.

Referencias Electrónicas:

Como elaborar un Plan de Contingencia
Miércoles, 4 Junio 2008 en Noticias Tecnológicas, Sistemas de Información
http://www.abartiateam.com

Plan de Contingencia
http://integrity.abast.es

Metodología de Análisis de Riesgos OCTAVE
www.cert.org

Metodología de Análisis de Riesgos MAGERIT
www.csi.map.es

Revista de Continuidad de Negocio
http://www.contingencyplanning.com

Portal de Business Continuity Plan
http://www.globalcontinuity.com

Business Continuity Institute
http://www.thebci.org/pas56.htm

Información y guías sobre Continuidad
http://www.disaster-recovery-guide.com

Mejores prácticas en Seguridad Informática
http://www.nist.org

Anexo II

AMENAZAS
DESASTRES NATURALES
Huracanes
Inundaciones
Incendios
DAÑOS ACCIDENTALES
Fuego fortuito
Inundaciones
Fallo del aire acondicionado
Exceso de humedad
Humo, gases tóxicos
Subida de tensión
Fallo de suministro eléctrico
Fallo de la UPS
Accidentes del personal
Capacidad inadecuada de las comunicaciones
Fallo/degradación del hardware
Fallo/degradación de las comunicaciones
Errores de operación
Fallos en las copias de seguridad
Fallos de los sistemas de autenticación/autorización
Pérdida de confidencialidad
Incumplimientos legales
ATAQUES INTENCIONADOS
Explosivos
Fuego intencionado
Accesos no autorizados al edificio
Actos de vandalismo
Radiaciones electromagnéticas
Robos intencionados
Manipulación de datos/software
Manipulación de hardware
Uso de software por personal no autorizado
Acceso no autorizados a datos de la compañía
Software malicioso
Robo de equipos
Robo de documentos

Robo de software
Descarga de software no controlada
Interceptación de las líneas de comunicación
Manipulación de las líneas de comunicación
Abuso de privilegios de acceso
Introducción de virus en los sistemas
Troyanos
Ataques por ingeniería social
Bombas lógicas
Ataques de denegación de servicio
Errores intencionados
Copias incontroladas de documentos/software/datos
Errores en el mantenimiento
Corrupción de datos
Incumplimientos legales intencionados

Anexo III

VULNERABILIDADES
Existencia de materiales inflamables como papel o cajas
Cableado inapropiado
Ancho de banda inapropiado
Suministro eléctrico inapropiado
Mantenimiento inapropiado del servicio técnico
Ausencia de mantenimiento
Educación inadecuada del personal en virus y malware
Políticas de firewall inadecuadas
Política de seguridad de la información inadecuada
Ausencia de política de seguridad
Derechos de acceso incorrectos
Ausencia de un sistema de extinción automática de fuegos/humos
Ausencia de backup
Ausencia de control de cambios de configuración eficiente y efectiva
Ausencia de mecanismos de identificación y autenticación
Ausencia de política de restricción de personal para uso licencias de software
Ubicación física en un área susceptible de desastres naturales
Carencia de software antivirus
Descarga incontrolada y uso de software de Internet
Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales
Protección física de equipos inadecuada
Personal sin formación adecuada
Incumplimientos legales (LOPD, Ley Sarbanes Oxley, etc.)
Definición de privilegios de acceso inadecuada
Ausencia de un Plan de recuperación de incidentes

Anexo IV

Cuestionario BIA

Datos básicos del proceso y de su dueño

Frecuencia del proceso

Períodos de tiempo críticos

Tiempo máximo de interrupción

Volumen de trabajo del proceso

Indicadores y medidas de desempeño existentes

Impactos: Financiero, cliente interno, cliente externo, eficiencia operativa, aspectos legales, imagen - reputación y en general para la organización como negocio.

Dependencias internas y externas

Aplicaciones informáticas que lo soportan

Procedimientos alternos existentes o sugeridos

Efectividad de los procedimientos alternos

Registros vitales de cada proceso

Complejidad de recuperación de las dependencias evaluadas

Recursos mínimos para la recuperación de cada dependencia.

Anexo V

Leyendas:

PROBABILIDAD	
Puntuación	**Nivel**
5	Muy alto
4	Alto
3	Medio
2	Bajo
1	Muy bajo

IMPACTO	
Puntuación	**Nivel**
5	Terminal
4	Devastador
3	Critico
2	Controlable
1	Irritante

PRIORIZACION	
Puntuación	**Nivel**
10-12	A
8-9	B
6-7	C
5-1	D

Anexo VI

ESCALA DE UN TERREMOTO[11]

Escala de Intensidad Rossi-Forel	Escala de Intensidad Mercalli Modificada	Magnitud (Escala Ritcher)	Aceleración Máxima del Terreno(G's)
I	I No sentido.	< 2.3	< 0.002
II	II. Sentido solamente por algunas personas en posición de descanso, especialmente en pisos altos. Objetos suspendidos oscilan un poco.	2.3 - 2.9	0.002 - 0.003
III	III Sentido en el interior. Muchas personas no lo reconocen como un temblor. Automóviles parados se balancean. Vibraciones como el paso de un camión pequeño. Duración apreciable.	3.0 - 4.1	0.004 - 0.007
IV	IV Sentido en el interior por muchos, en el exterior por pocos. Ventanas, platos, puertas vibran. Las paredes crujen. Vibraciones como el paso de un camión grande; sensación de sacudida como de un balón pesado. Automóviles parados se balancean apreciablemente.	3.7 - 4.2	0.015 - 0.02
V	V Sentido por casi todo el mundo; muchos se despiertan. Algunos platos, ventanas, etc. se rompen; algunas casas de mampostería se agrietan. Objetos inestables volcados. Los péndulos de los relojes se detienen. Las puertas se balancean, se cierran, se abren. Arboles, arbustos sacudidos visiblemente.	4.3 - 4.9	0.03 - 0.04
VI	VI Sentido por todos; muchos se asustan y corren al exterior. Es difícil andar. Ventanas, platos y objetos de vidrio se rompen. Algunos muebles pesados se mueven; se caen algunas casas de mampostería; chimeneas dañadas. Daños leves.	5.0 - 5.6	0.06 - 0.07

[11] http://redsismica.uprm.edu/spanish/informacion/sisnotas_tam.php

VII	VII Todo el mundo corre al exterior. Daños muy pequeños en edificios de buen diseño y construcción; leve a moderado en estructuras bien construidas; considerable en las mal construidas; algunas chimeneas se rompen. Sentido por conductores.	5.7 - 6.2	0.1 - 0.15
VIII	VIII Daño leve en estructuras especialmente diseñadas para terremotos; considerable hasta con colapso parcial en edificios corrientes; mayor en estructuras pobremente construidas. Los paneles de las paredes se salen de los marcos. Se caen chimeneas, monumentos, columnas y paredes. Se viran muebles pesados. Pequeños corrimientos de arena y fango. Cambios en el caudal de fuentes y pozos. Difícil conducir.	6.3 - 6.9	0.25 - 0.3
IX	IX Daño considerable en estructuras de diseño y construcción buena, estructuras bien diseñadas, desplazadas de sus cimientos; mayor en edificios corrientes con colapso parcial y total. Amplias grietas en el suelo. Eyección de arena y barro en áreas de aluvial. Tuberias subterráneas rotas.	7.0 - 7.6	0.5 - 0.55
X	X Algunas estructuras bien construidas en madera y puentes destruidos, la mayoría de las construcciones y estructuras de armazón destruidas con sus cimientos. Grietas grandes en suelo. Deslizamientos de tierra, agua rebasa las orillas de canales, ríos, lagos, etc. Arena y barro desplazados lateralmente. XI Colapso de la mayoría de las estructuras de cemento y hormigón. Puentes y otras vías de transporte seriamente afectadas. XII Pérdida total en la infraestructura. Grandes masas de rocas desplazadas. Objetos pesados lanzados al aire con facilidad.	7.7 - 8.2 8.3 - 9.0 > 9.0	> 0.6

Anexo VII

ESCALA DE INTENSIDAD DE HURACANES
SAFFIR- SIMPSON[12]

CATEGORÍA	VIENTOS (KPH)	DAÑOS	EJEMPLOS
I	119-153	Se producen daños en casas móviles, árboles. Algunos inundaciones costeras en carreteras. Marea de tormenta entre 4 y 5 pies sobre lo normal.	JEANNE, 2004 ELOISA 1975
II	154-177	Marea de tormenta entre 6 y 8 pies. Algunos techos, puertas y ventanas sufren daños. Considerables daños en postes eléctricos y árboles. Inundaciones en rutas de evacuación antes de llegar el centro del huracán. Pequeñas embarcaciones son desplazadas.	FLORA 1963 BEULAH 1967
III	178-209	Marea de tormenta entre 9 y 12 pies. Algunos daños estructurales en pequeñas residencias y en edificios. Daños considerables a postes eléctricos y árboles con amplio follaje. Casas móviles y construcciones deficientes son destruidas. Fuertes rompientes pueden provocar daños en estructuras pequeñas cerca de la costa. Terrenos por debajo de 5 pies con respecto a nivel medio del mar pueden ser inundados tierra adentro. Deben procederse a evacuar personas en alto riesgo.	GEORGES, 1998
IV	210-249	Mareas de tormenta entre 13 y 18 pies sobre lo normal. Daños extensos en pequeñas residencias. Postes y árboles son derribados. Inundaciones en las vías de escape dificultan las evacuaciones entre 3 y 5 horas antes de la llegada del fenómeno.	SAN ZENON, 1930 INEZ,, 1966
V	249 O MAS	Mareas de tormenta generalmente mayores de 18 pies. Daños severos a gran parte de residencias y edificios industriales. Casas móviles totalmente destruidas.	DAVID, 1979

[12] Oficina nacional de meteorología de la Republica Dominicana ONAME.

ANEXO VIII

MEDIDAS DE PRECAUCIÓN PARA MITIGAR LOS EFECTOS DE UN TERREMOTO[13]

Recuerde, un terremoto de gran intensidad puede afectar a Puerto Rico en cualquier momento. Tome las siguientes medidas de precaución para evitar la muerte, heridas y daños a la propiedad.

AHORA

1. Desarrolle una conciencia sísmica.
2. Haga una inspección minuciosa de su casa y lugar de trabajo/estudio para determinar si hay peligros estructurales.
3. Asesórese con un ingeniero para asegurar la estabilidad estructural durante un terremoto.
4. Construya en terreno firme.
5. Identifique y tome medidas para reducir los peligros que hay en su hogar, vecindario y centro de trabajo/estudio.
6. Ancle los muebles potencialmente inestables a la pared o al piso.
7. Sujete muebles y enseres con ruedas al piso y las paredes
8. Asegure las puertas de los gabinetes y enseres.
9. Asegure firmemente los objetos colgantes del techo.
10. Remueva objetos pesados de lugares altos.

---

[13] Red sísmica política de privacidad univ. De puerto rico recinto de mayagüezwdt copyrights 2005

11. Aleje las camas de lugares peligrosos.
12. Sujete los tanques de gas fluído y calentadores de agua a la pared.
13. Use tubos de materiales flexibles.
14. Mantenga las salidas libres.
15. Adquiera un seguro adecuado contra terremoto.
16. Prepare un plan de contingencia para su familia/hogar y lugar de trabajo/estudio.
17. Haga un duplicado de las llaves de su hogar y vehículo.
18. Mantenga una linterna con baterías de repuesto al lado de su cama.
19. Mantenga un radio portátil con baterías.
20. Coloque un extintor de incendios en un sitio accesible.
21. Mantenga una reserva adecuada de alimentos.
22. Guarde una reserva abundante de agua.
23. Mantenga en un lugar accesible una caja de herramientas.
24. Esté preparado para suministrar primeros auxilios y asegúrese de tener suficientes medicinas.
25. Guarde los documentos importantes en una caja de seguridad.
26. Para los salones de clases y lugares de trabajo, preparar una mochila de seguridad. Las mismas deben incluir suministros para primeros auxilios (alcohol, antiséptico, betadina, gazas, etc.), radio, linterna, baterías para radio y linterna, marcadores, libreta, guantes, y otras cosas que entienda sean necesarias.

27. Desarrolle un plan con sus vecinos para enfrentar terremotos.
28. Haga una evaluación de los recursos del vecindario.
29. Prepara a sus niños para enfrentarse a un terremoto.
30. Oriente a las personas con impedimentos.
31. No debe dejar realengos los animales domésticos.
32. Conduzca y practique simulacros contra terremotos en su hogar y lugar de trabajo/estudio.
33. Si vive o trabaja en un edificio alto, prepárese para oscilaciones fuertes.
34. Conozca rutas alternas.

DURANTE

1. Reaccione con prontitud.
2. Ordene repetidamente a la tierra que pare de temblar.
3. Si está dentro de su casa u otra edificación, quédese ahí y muévase a un lugar seguro.
4. Manténgase alejado de objetos peligrosos y protéjase contra los que caigan.
5. No corra. En la mayoría de los casos es más seguro quedarse adentro que tratar de salir.
6. No use el elevador o trate de salir por las escaleras durante el terremoto.
7. Detenga su automóvil y permanezca en el.
8. Si está fuera, quédese ahí, alejándose de postes, árboles y edificios.

9. Si está en un sillón de ruedas, quédese en él y trate de esquivar objetos que puedan estar cayendo.

DESPUÉS

1. Aléjese del mar.
2. Mantenga la calma, tome unos momentos para pensar las consecuencias de lo que vaya a hacer.
3. Implante su plan de emergencia familiar y comunal.
4. Haga una rápida inspección inicial por si hay heridos o gente atrapada.
5. Póngase ropa adecuada.
6. Verifique si hay incendios.
7. No haga llamadas innecesarias.
8. Si detecta escapes de gas, cierre la válvula principal, abra las ventanas y salga de la edificación.
9. Desconecte el servicio eléctrico si hay daño en el sistema eléctrico de la propiedad.
10. No toque cables o postes eléctricos que hayan caído al suelo.
11. Disponga adecuadamente de sustancias peligrosas que se hayan derramado.
12. Examine el sistema sanitario.
13. Abra la pluma de agua fría y almacene agua en los lavabos y bañeras.
14. Inspeccione su casa cuidadosamente por si hay daños estructurales.
15. Tenga cuidado al abrir las puertas del mobiliario.

16. Sintonice el sistema de radiodifusión de emergencia.
17. No salga a novelerear.
18. Esté preparado para más temblores.
19. Si usted es lisiado y está atrapado, llame o haga ruido para recibir ayuda.
20. Si usted es sordo o tiene problemas auditivos, atraiga la atención de otros.
21. Ayude a las personas con impedimentos visuales.
22. Coopere con la Defensa Civil y otras autoridades de emergencia y seguridad pública.

ANEXO IX

Teléfonos de Emergencias

INSTITUCIONES	SERVICIOS	SALUD
Policía Nacional	Tricom	Cruz Roja
(809) 682-5423	(809) 476-6000	(809) 682-4545
Ayuntamiento DN	Codetel	Movimed Área Metropolitana
(809) 535-1181	(809) 220-1111	(809) 532-0000
Defensa Civil SD	Apolo Taxi	Hospital Darío Contreras
(809) 472-8614	(809) 537-7771	(809) 596-3686
Migración	Meteorología	Centro Médico UCE
(809) 688-5075	(809) 788-1122	(809) 592-1409
Palacio de Justicia	Aeronáutica Civil	H. F. Moscoso Puello
(809) 221-6400	(809) 221-7909	(809) 681-2913
Fiscalía Nacional	Bomberos	H. L.E. Aybar (Morgan)
(809) 688-1372	(809) 682-2000	(809) 684-3478
Control de Drogras	CDE	H. Salvador B. Gautier
(809) 221-4166	(809) 535-1100	(809) 565-3171
ProFamilia	CAASD	H. Padre Billini
(809) 689-0141	(809) 562-3500	(809) 686-2833
		H. Psiquiátrico
		(809) 559-8475
		H. Robert Reid Cabral
		(809) 533-1111
		Plaza de la Salud
		(809) 565-7477
		Matern. del La Altagracia
		(809) 686-6376
		Rehabilitación
		(809) 689-7151
		Centro Antirrábico
		(809) 681-1637

BIBLIOGRAFIA

Libros:

Gregory, Peter (2008). IT Disaster Recovery Planning. Indiana, USA. Willey Publishing, Inc.

Del Pino Jiménez, Laura (2007). Guía de desarrollo de un plan de continuidad de negocio. Madrid, España. Escuela Universitaria de Informática.

Referencias Electrónicas:

Como elaborar un Plan de Contingencia
Miércoles, 4 Junio 2008 en Noticias Tecnológicas, Sistemas de Información
http://www.abartiateam.com

Plan de Contingencia
http://integrity.abast.es

Metodología de Análisis de Riesgos OCTAVE
www.cert.org

Metodología de Análisis de Riesgos MAGERIT
www.csi.map.es

Revista de Continuidad de Negocio
http://www.contingencyplanning.com

Portal de Business Continuity Plan
http://www.globalcontinuity.com

Business Continuity Institute
http://www.thebci.org/pas56.htm

Información y guías sobre Continuidad
http://www.disaster-recovery-guide.com

Mejores prácticas en Seguridad Informática
http://www.nist.org