ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TI DE UNA EMPRESA FARMACÉUTICA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

AUTOR:

LEIVA GARZÓN ANA LUCÍA

anyluleo@yahoo.com

DIRECTOR:

MSC. ING. RAÚL CÓRDOVA

mrcordova@server.epn.edu.ec

FEBRERO, 2008

DECLARACIÓN

Yo, Ana Lucía Leiva Garzón, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

_____

Ana Lucía Leiva Garzón

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Ana Lucía Leiva Garzón, bajo mi supervisión.

_____

Msc. Ing. Raúl Córdova
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por iluminar mi camino y acompañarme durante toda mi vida, brindándome la salud y la capacidad de asimilar satisfactoriamente los conocimientos hasta ahora obtenidos.

A los distinguidos profesores de la Escuela Politécnica Nacional por impartir sus conocimientos e inculcar valores éticos para ejercer con éxito la profesión, especialmente al Ing. Raúl Córdova por su excelente dirección del presente Proyecto de Titulación.

Un especial agradecimiento para el personal de IT de la Empresa Roche Ecuador S.A. por su colaboración para la realización de este trabajo.

DEDICATORIA

A mis Padres Rodrigo y Mary, quienes me han apoyado en cada paso de mi vida brindándome todo su amor y confianza, quienes me han dado el empuje y valor para seguir adelante en cada caída y han celebrado conmigo todos mis triunfos.

A mi hermana Karina, por sus consejos y su motivación incondicional, por ayudarme a ser mejor cada día.

Dedico este Proyecto de Titulación a mi familia, con el deseo de retribuir de alguna forma la confianza y cariño que han depositado en mí; este logro, para ellos.

A mi querido amigo de la Feria de Libros, por brindarme tantos momentos especiales y únicos.

CONTENIDO

Índice de Tablas

Índice de Figuras

RESUMEN

El presente proyecto de titulación propone el Desarrollo del Plan de Continuidad del Negocio para el Departamento de TI de una Empresa Farmacéutica, como una posible solución a la necesidad de las empresas de proteger sus recursos y darle continuidad de operaciones a sus principales actividades.

En el Capítulo 1 consta una descripción general de la empresa Roche Ecuador S.A., su principal actividad y su funcionamiento interno. También se describe su Departamento de TI, sus procesos, su estructura organizacional y un mapeo de servicios que soportan a las áreas del negocio; de manera que ayuda a tener una visión global del tipo de empresa, sus carencias y requerimientos de protección de recursos.

En el Capítulo 2 se desarrollan las cuatro etapas que propone ITIL para el diseño del plan de continuidad del negocio: Etapa de Iniciación, Etapa de Requerimientos y Estrategia, Etapa de Implementación y Etapa de Gestión Operativa. Dentro de estas etapas se elaboran tres documentos esenciales para la continuidad del negocio: Análisis de Impacto en el Negocio (BIA), Evaluación de Riesgos y Estrategias de la Continuidad. Adicionalmente se presentan los roles y responsabilidades del equipo de la continuidad, beneficios y posibles problemas al desarrollar el plan de continuidad del negocio.

En el Capítulo 3 se presenta un simulacro aplicado al Departamento de TI de Roche Ecuador S.A., para evaluar la eficacia del plan de continuidad del negocio propuesto, siguiendo las etapas de implementación: Respuesta Inicial y Notificación, Evaluación del Problema y Escalamiento, Declaración del Desastre, Plan de Implementación de Logística, Recuperación, y Normalización. Se evalúan parámetros de tiempo, costos y eficacia del plan propuesto y se presenta un análisis de resultados.

En el Capítulo 4 se presentan las conclusiones y recomendaciones emitidas durante el desarrollo del presente trabajo.

PRESENTACIÓN

El Plan de Continuidad del Negocio propuesto en este proyecto de titulación, empieza realizando un análisis situacional de la empresa farmacéutica Roche Ecuador S.A., describiendo su actividad principal en el mercado ecuatoriano, su misión y visión, su estructura organizacional y un análisis FODA de la misma. Se describe el funcionamiento del Departamento de TI, su esquema organizacional, sus áreas funcionales, la descripción de servicios que soporta TI a las áreas del negocio y un listado de procesos que el Departamento de TI gestiona internamente; éste análisis ayuda a obtener una visión global de sus carencias y requerimientos de continuidad ante cualquier tipo de desastre.

Para iniciar el diseño del Plan de Continuidad del Negocio enfocado al Departamento de TI de Roche Ecuador S.A., se definen las políticas, alcance y recursos disponibles, que sirven como lineamientos iniciales para su elaboración; luego se realiza un levantamiento de información dentro de la empresa para armar el documento base de la continuidad que es el Análisis de Impacto en el Negocio (BIA), donde se identifican los procesos críticos del negocio, se evalúa el impacto financiero y operacional de cada uno de ellos, se determinan los sistemas, aplicaciones y recursos de TI que soportan a los procesos críticos y acto seguido se determina el tiempo máximo que un proceso puede estar fuera de servicio sin que afecte significativamente al negocio.
Luego se realiza una Evaluación de Riesgos identificando posibles amenazas y consecuencias, en base al historial de ocurrencia de interrupciones y al entorno en el que opera la empresa, se proponen ciertas medidas de prevención y control de los riesgos. Con estos datos iniciales se definen las Estrategias de Continuidad, estableciendo las opciones aplicables de recuperación para la realidad de la empresa en estudio.

Luego se determina cuál será el equipo de la continuidad del negocio y las actividades que se deben realizar para la implementación del plan y se asignan los roles y responsabilidades a cada miembro del plan de continuidad.

Una vez culminadas las etapas del plan de continuidad del negocio se lo difunde a todos los miembros de la empresa concienciando a cada uno de ellos para fomentar la colaboración y participación con el plan de continuidad, mediante capacitaciones y por varios canales de comunicación.

Se refuerza éste estudio evaluando la efectividad del plan propuesto mediante un simulacro en el Departamento de TI de la empresa y se miden parámetros de tiempo, costos y efectividad, determinando así su aplicabilidad, este tipo de pruebas ayudan a mantener la vigencia del plan.

Finalmente, la elaboración del Plan de Continuidad del Negocio para TI de Roche Ecuador S.A., es un gran aporte para mitigar los riesgos originados por un desastre, por lo que en general, todas las empresas deberían darle importancia y crear sus propios planes de manera que estén preparados ante cualquier eventualidad.

CAPÍTULO 1. ANÁLISIS DE LA EMPRESA FARMACÉUTICA (ROCHE ECUADOR S.A.)

En este capítulo se realizará una descripción general de la Empresa Farmacéutica Roche Ecuador S.A., donde se aplicará el Plan de Continuidad del Negocio para el Departamento de Tecnologías de la Información.

1.1 DESCRIPCIÓN DE LA EMPRESA

1.1.1 LA COMPAÑÍA ROCHE

Roche es una empresa dedicada a brindar servicios de salud, se orienta principalmente a dar soluciones innovadoras en lo que se refiere a medicinas y equipos médicos. La empresa está operando aproximadamente desde hace 100 años enfocándose en el descubrimiento, desarrollo, fabricación y comercialización de nuevas soluciones para la atención médica.

Roche se preocupa de brindar a sus clientes una óptima calidad de vida, ofreciendo productos y servicios para el diagnóstico y tratamiento de enfermedades, además de poner énfasis en lo que se refiere a la prevención de las enfermedades.

1.1.2 MISIÓN, VISIÓN, OBJETIVOS ESTRATÉGICOS Y VALORES DE ROCHE

La información presentada a continuación acerca de la misión, visión, objetivos estratégicos y valores de la empresa, ha sido tomada de Roche Ecuador S.A., de documentos publicados en su página web[1].

[1] Pagina web de Roche Ecuador S.A.: http://www.roche.com.ec.

1.1.2.1 La Misión de Roche

La misión de la Compañía se enfoca en brindar soluciones médicas innovadoras y de alta calidad.
La misión de Roche es la siguiente:
Nuestro objetivo como empresa líder en el campo de la salud consiste en crear, producir y comercializar soluciones innovadoras de alta calidad para satisfacer necesidades médicas no cubiertas. Nuestros productos y servicios contribuyen a la prevención, el diagnóstico y el tratamiento de las enfermedades, incrementando así el bienestar y la calidad de vida. Las actividades de nuestra compañía están presididas por la responsabilidad y la ética, en el compromiso con un desarrollo sostenible y respetuoso con las necesidades de las personas, la sociedad y el medio ambiente.

1.1.2.2 La Visión de Roche

La visión de la Compañía se basa en tres aspectos importantes: Innovación, Rapidez y Crecimiento.

La visión de Roche es la siguiente:

- Crecer por encima del mercado.
- Optimizar la rentabilidad para garantizar un crecimiento sostenido.
- Ser reconocidos como la Compañía líder en servicio al cliente.
- Generar un ambiente que promueva el crecimiento, el desarrollo y la satisfacción de los empleados.

1.1.2.3 Los Objetivos Estratégicos de Roche

Roche enfatiza sus objetivos en el cliente, y en la innovación de sus productos, para llegar a ser superior a la competencia.

Los objetivos de Roche son los siguientes:

- Crecer en la áreas estratégicas de Roche por encima del mercado relevante, siendo financieramente flexibles y rentables.
- Crear valor a nuestros clientes cultivando la innovación y diferenciación permanente.
- Promover una cultura de Liderazgo que empodere a nuestros colaboradores y facilite la implementación y la toma de decisiones.

1.1.2.4 Los Valores de Roche

Los valores de Roche se presentan a continuación:
Éstos son los principios rectores de nuestra compañía. Queremos ser una empresa innovadora, que goce del orgullo de sus empleados y merezca la confianza permanente de sus socios.

- Servicio a los pacientes y los clientes
- Compromiso de responsabilidad
- Compromiso de rendimiento
- Compromiso con la innovación
- Perfeccionamiento continuo

1.1.3 LA PRESENCIA MULTINACIONAL DE ROCHE

La matriz de la Compañía Roche se encuentra en Basilea-Suiza (Basel-Switzerland) y las sucursales están distribuidas alrededor del mundo, con el fin de proporcionar un servicio excelente.

Roche está presente en aproximadamente 150 países y cuenta con la colaboración de alrededor de 74000 personas para su funcionamiento.

1.1.4 LA PRESENCIA DE ROCHE EN ECUADOR

La matriz de Roche en Ecuador se localiza en la ciudad de Quito y cuenta con sucursales en Guayaquil y Cuenca.

Roche Ecuador S.A. actualmente cuenta con la colaboración de aproximadamente 180 empleados quienes en su mayoría operan en la ciudad de Quito.

1.1.5 ESTRUCTURA ORGANIZACIONAL DE ROCHE

Las divisiones operativas que se destacan a nivel global en la empresa son:

- División Farma
- División Diagnóstica

Esta división se la puede apreciar en la Figura 1.1.

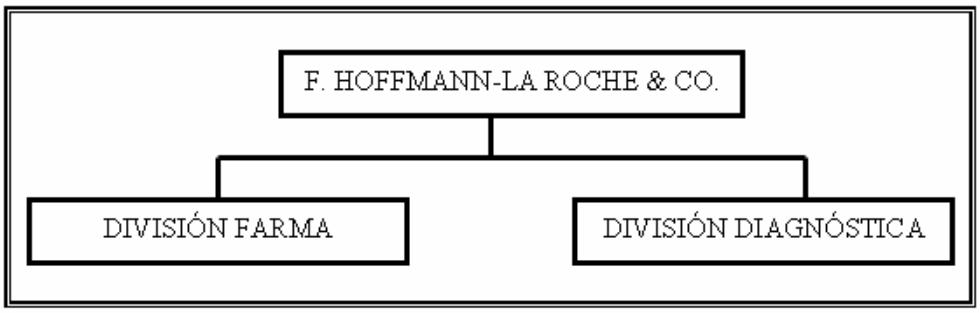

Figura 1.1 Estructura Organizacional de Roche
Fuente: Roche Ecuador S.A.

1.1.5.1.1 División Farma

Fritz Hoffmann fundó la compañía F. Hoffmann-La Roche & Co. en 1896, estaba convencido de la idea de elaborar productos de farmacia y comercializarlos en mercados internacionales, por lo que la innovación en los productos fue una las tendencias principales de la compañía, mediante lo cual Roche impone presencia en el mercado farmacéutico del área hospitalaria.

Se considera primordial la innovación continua en los nuevos medicamentos que ofrece Roche al paciente, aprovechando la medicina molecular.

1.1.5.1.2 División Diagnóstica

La división diagnóstica de Roche es líder mundial en diagnósticos in-vitro y ofrece una amplia gama de productos y servicios en todas las áreas médicas, Roche tiene una capacidad única en lo que se refiere a gente y tecnología para proveer soluciones innovadoras y rentables, investigación médica oportuna y fiable, diagnóstico de laboratorio y auto monitoreo del paciente.

Roche trabaja en diferentes países con clientes, investigadores, médicos y pacientes. Se dice que no hay laboratorio en el mundo que no contenga un producto de diagnóstico de Roche.

1.2 ANÁLISIS FODA DE LA EMPRESA

Tomando en cuenta el alcance del presente proyecto de titulación se enfoca el análisis FODA única y exclusivamente al Departamento de TI de Roche Ecuador S.A.

1.2.1 ANÁLISIS FODA DEL DEPARTAMENTO DE TI

Tomando en cuenta que actualmente la empresa en análisis no cuenta con un análisis FODA y que el plan de continuidad del negocio de este proyecto de titulación está orientado únicamente al Departamento de TI, se ha enfocado en identificar un FODA solamente para TI.

El análisis FODA del Departamento de TI ha sido elaborado con la colaboración de los miembros del Departamento de TI y se lo describe a continuación:

Fortalezas

- Se siguen estándares para los procedimientos que se realizan dentro del Departamento de TI.

- Se cuenta con personal calificado para administrar tanto los equipos como las aplicaciones requeridas por el negocio.
- Se tiene gran apertura para adoptar nuevas tecnologías de forma rápida.
- Los miembros del Departamento de TI tienen acceso a capacitación constante.
- Se tiene la posibilidad de escalar los problemas hacia las sucursales a nivel regional o mundial.
- Los miembros de TI tienen buena aceptación y percepción por parte de los usuarios.
- Liberación de actividades de soporte a usuarios, gracias a la buena capacitación que imparten.

Oportunidades

- El Departamento de TI de Roche Ecuador es partícipe de todos los proyectos regionales de la empresa.
- Tener acceso a tecnología de punta por los convenios que se tiene con varias empresas proveedoras de hardware y software.
- Tener acceso a capacitación de nuevas tecnologías con el fin de dar mejores soluciones al Departamento de TI.

Debilidades

- Acceder a los sistemas de manejo del negocio de manera remota y no de forma local, ya que se encuentran en otros países de Latinoamérica, y cuando ocurre un daño no se tiene control sobre estos sistemas para poder gestionar la reparación de acuerdo a las necesidades.
- Mantener la dirección de la administración de TI en Colombia, por lo que no existen controles adecuados.
- Administración de TI Ecuador desde la matriz ubicada en Quito hacia las sucursales de Cuenca y Guayaquil, ya que faltan recursos de personal para dar soporte en las sucursales de Ecuador.

- Falta de conocimiento total del negocio por parte del personal de TI.
- Falta de presupuesto para mejorar la infraestructura del Departamento.
- Falta de personal para cumplir con todas las funciones que requiere el Departamento.

Amenazas

- Plagio de soluciones informáticas, herramientas tecnológicas o métodos para llegar al cliente; por parte de la competencia.
- Inestabilidad política del país puede afectar a la organización en general.
- Problemas en los convenios existentes con los proveedores.

1.3 PROCESOS Y FUNCIONES DEL DEPARTAMENTO DE TI DE LA EMPRESA

1.3.1 EL DEPARTAMENTO DE TI (TECNOLOGÍAS DE LA INFORMACIÓN) DENTRO DE LA COMPAÑÍA

El área de Tecnologías de la Información de Colombia y Ecuador es gestionada por el Gerente de Informática, quien radica en Colombia.
La matriz de Roche Ecuador está en la ciudad de Quito.

El Departamento de TI ubicado en la matriz se encarga de dar soporte generalmente mediante vía remota a los usuarios de Guayaquil y Cuenca.

Las políticas informáticas se manejan de forma global, sin embargo se las ha adaptado según las necesidades y leyes de cada país.

Varios sistemas de información y aplicaciones que se utilizan en el Ecuador, se encuentran en Basilea, Argentina, Brasil y México, se accede a estas aplicaciones de forma remota. En Ecuador se encuentran instalados localmente pocos sistemas.

1.3.2 ESQUEMA ORGANIZACIONAL DEL DEPARTAMENTO DE TI

Cabe destacar que varios de los diagramas presentados en este proyecto de titulación se conservan en idioma inglés debido a que la empresa es multinacional y maneja estándares globales.

El Organigrama Estructural en el Departamento de TI de Roche Ecuador se representa en la Figura 1.2.

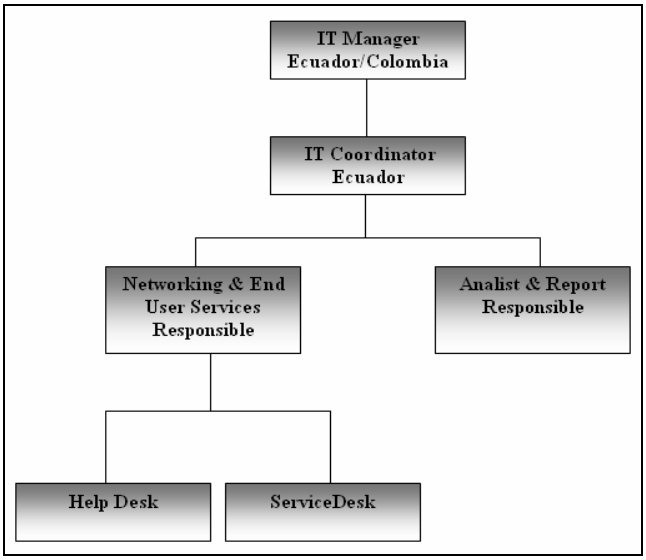

Figura 1.2 Organigrama Estructural del Departamento de TI de Roche[2]

1.3.3 ÁREAS ADMINISTRATIVAS DEL DEPARTAMENTO DE TI

De acuerdo a las políticas informáticas globales, el personal de TI en Ecuador se distribuye como se muestra en la Figura 1.3.

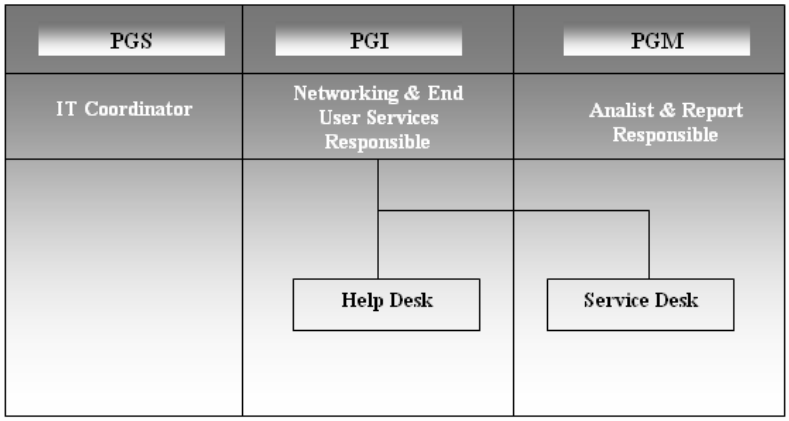

Figura 1.3 Áreas del Departamento de TI de Roche[3]

[2] Fuente: Roche Ecuador S.A.
[3] Fuente: Roche Ecuador S.A.

El Departamento de TI en Ecuador se divide en tres áreas importantes para desarrollar sus actividades:

- **PGS:** Supply Chain, Finance and Human Resources Information Management. (Gestión de Información de Recursos Humanos, Finanzas y Cadena de Suministro)
- **PGI:** Infrastructure Services and Operations. (Servicios de Infraestructura y Operaciones)
- **PGM:** Marketing and Sales Information Management. (Gestión de Información de Ventas y Marketing)

Donde:

PGS: Esta área se encarga de gestionar las Operaciones Técnicas, Finanzas y Recursos Humanos así como los principales clientes en la división Farma.
Proporciona servicios a los proyectos en ejecución para apoyar los nuevos requisitos comerciales y organizacionales que cambian rápidamente. PGS ayuda a mejorar la excelencia implementando soluciones innovadoras de TI. Además selecciona las aplicaciones comerciales más adecuadas de tecnología informática con el fin de mantener la ventaja competitiva de Roche, PGS cuenta con 380 expertos muy calificados para servir a los clientes comerciales en aproximadamente 23 sucursales de Farma alrededor del mundo.

El personal de PGS se encarga de gestionar lo siguiente dentro del Departamento de TI:

- El ERP
- La administración del Departamento de TI
- Reportar actividades a IT Manager Colombia/Ecuador.

La aplicación principal o ERP (Enterprise Resource Planning – Planificación de Recursos de la Empresa) de Roche es SAP (Systems, Aplications and Products -

Sistemas, Aplicaciones y Productos), esta aplicación se encuentra en Brasil y desde Ecuador se accede a ella de forma remota.

SAP es un software de planificación de recursos empresariales, en Roche se utiliza la versión R3 (Procesamiento en tiempo real en arquitectura de 3 capas: bases de datos, servidor de aplicaciones y cliente.)
Los módulos que conforman el SAP son:

- FI – Finance (Finanzas)
- HR - Human Resources (Recursos Humanos)
- LE - Logistics Execution (Ejecución de Logística)
- MM - Material Management (Gestión de Materiales)
- PM - Plant Maintenance (Mantenimiento de la Planta)
- PP - Production Planning (Planificación de Producción)
- SD - Sales & Distribution (Ventas y Distribución)

PGI: Esta área se encarga de la parte tecnológica y de dar soporte a usuarios. PGI es responsable de proporcionar la infraestructura informática y de dar apoyo a los usuarios que utilizan las aplicaciones comerciales de Roche, desde el uso de las herramientas del negocio hasta el uso del correo electrónico y herramientas de Office que ayudan a desarrollar las actividades y tareas del negocio de Farma.
Las personas están seguras de poder acceder a los sistemas e información que necesitan para realizar su trabajo contando con la colaboración del personal de PGI para brindarles soporte.
Al ser una empresa global, muchos de los servicios se necesitan 24 horas al día, 7 días a la semana y 365 días al año, por lo que exigen contar con un equipo especializado de profesionales. Se tiene empleados en más de 52 sitios de Farma, PGI global de Roche maneja más de 4000 servidores, provee servicios a más de 35000 usuarios de Farma y algunos servicios del core del negocio en la División Diagnóstica y provee de la infraestructura a más de 1200 aplicaciones.

El personal de PGI se encarga de gestionar los siguientes recursos:

- Equipos de Computación

- Redes/Networking
- Administración y mantenimiento de Servidores y Aplicaciones.
- Administración de Usuarios y Help Desk

En Roche Ecuador actualmente existen aproximadamente 150 equipos de computación, donde alrededor de 90 son computadores portátiles (Laptops) y 60 son computadores de escritorio (Desktops). Mantienen convenios con proveedores a nivel mundial, acuerdos que son regidos por la casa matriz de Roche.

Las Laptops se pueden dividir en dos tipos:
Mobiles: Son usadas dentro y fuera de la empresa por los usuarios.
Remotas: Se encuentran generalmente fuera de la ciudad de Quito, en las sucursales.
La nomenclatura utilizada para los equipos es la siguiente:

Laptop: RQUMWL###
Desktop: RQUMWD###

Las aplicaciones locales que posee Roche Ecuador se pueden clasificar en función de los servidores, como se describe en la Tabla 1.1:

Nombre del Servidor	Aplicación
RQUMSQ01	Servidor de Respaldos (Ghost)
RQUMSQ03	Servidor de Archivos Quito
RQUMSQ04	Servidor de Archivos Guayaquil
RQUMSQ06	Intranet
RQUMSQ10	Servidor de Archivos de Diagnóstica
RQUMSEM1	Servidor de Correo (Microsoft Exchange)
RQUMNALA	Servidor de Active Directory
RQUMSSWD01	Servidor de Distribución de Paquetes

Tabla 1.1 Aplicaciones Locales de Roche Ecuador S.A.[4]

[4] Fuente: Roche Ecuador S.A.

Con respecto a la red se puede mencionar que la mayor concentración de routers y switchs que conforman la red de cableado estructurado, se encuentra en el edificio principal de Roche en Quito. Se tiene conexión con las dos bodegas de Roche, también ubicadas en Quito, y otra con la sucursal de Guayaquil. La salida a Internet se la realiza mediante el túnel que sale a México. El diagrama red de Capa 1 se detalla en la Figura 1.4.

PGM: Esta área se encarga de manejar el Marketing y Venta de equipos médicos. PGM brinda apoyo a la parte de Marketing y Ventas de equipos que se lo hace al por mayor, ayuda a establecer una integración entre pacientes, médicos, farmacéuticos y comerciantes. También proporciona información a los clientes acerca de los productos Roche. PGM se enfoca en la gestión de las relaciones con los clientes, e-marketing y ventas, así como programas de apoyo a pacientes, dirigidas por médicos. Adicionalmente su función es realizar marketing estratégico para gestionar el ciclo de vida de los equipos y de los productos.

Existe personal responsable para cubrir cada área, optimizando el desempeño de las aplicaciones, brindando soporte a los usuarios y proporcionando la infraestructura necesaria para el desarrollo eficiente de las actividades propias de la empresa.

El personal de PGM se encarga de gestionar los siguientes recursos:

- Bases de Datos (Microsoft SQL, MySQL)
- Reportes (Visita médica, Call center, Ventas)

El sistema que ayuda a gestionar la visita médica es uno de los principales dentro de la empresa. El sistema Siebel utiliza como motor de base de datos SQL Server, y aquí se administra y se almacena datos sobre médicos y pacientes que adquieren los productos. El servidor de Siebel se encuentra en Brasil y se accede de forma remota. El personal de PGM se encarga de emitir los reportes para el área de Marketing y Ventas utilizando esta herramienta.

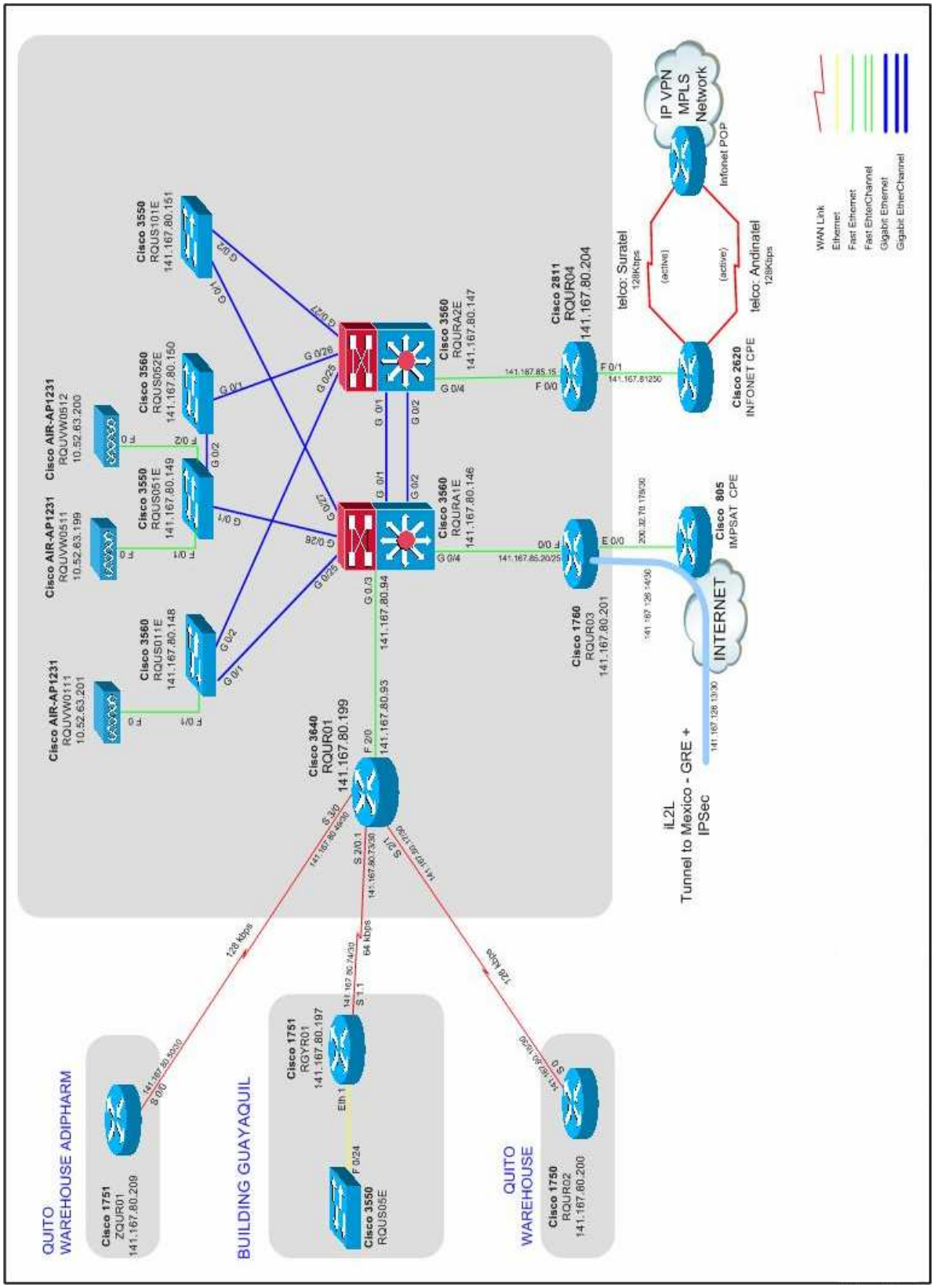

Figura 1.4 Diagrama de Red Capa 1.[5]

[5] Fuente: Roche Ecuador S.A.; Documentación de Networking & EUS Responsible

1.3.4 DESCRIPCIÓN DE LOS SERVICIOS QUE SOPORTA DEL DEPARTAMENTO DE TI.

En la tabla 1.2 se da una breve descripción de los servicios que soporta el Departamento de TI y la ubicación a la que se accede para utilizar cada uno de ellos:

SERVICIO DE TI	DESCRIPCIÓN	UBICACIÓN
SAP	Systems, Aplications and Products - Sistemas, Aplicaciones y Productos	Brasil
Microsoft Office Word	Herramientas de Oficina – Procesamiento de Texto	Local
Microsoft Office Excel	Herramientas de Oficina – Hoja de Cálculo	Local
Microsoft Office Power Point	Herramientas de Oficina – Manejo de Presentaciones	Local
Microsoft Office Outlook	Herramientas de Oficina – Administración de Correo Electrónico	Local
Intranet	Portal web interno de la empresa	Local
Servidor de Archivos	Partición disponible para almacenar información importante, se obtiene respaldos de forma periódica.	Local
Messenger Interno	Chat de comunicación interna de la empresa.	Argentina
Telefonía fija	Disponibilidad del servicio de teléfonos convencionales.	Local
Telefonía móvil	Disponibilidad del servicio de teléfonos celulares.	Local
IXOS	Sistema de almacenamiento de documentos escaneados.	Brasil
Internet	Red pública	Enlace a México y Enlace Local
Scanner	Digitalización de documentos	Local
Impresoras	Impresión de documentos	Local
Copiadora	Copiado de documentos	Local
Videoconferencia	Conferencias mediante televisión o computador	Local
Fax	Servicio de envío y recepción de documentos vía telefónica	Local
SISALEM	Sistema de Registro de Problemas para la División Diagnóstica y para control de sustancias psicotrópicas para la División Farma.	Local
Workflow	Control de Flujo de documentos de un proceso, maneja pasajes de avión, vacaciones de personal.	Brasil
IMS	Herramienta que genera información de venta de productos	Local
Siebel	Sistema para registrar pacientes, médicos, ventas, actividades de visitadores médicos.	Brasil
Net Meeting	Herramienta de apoyo para conferencias regional o internacional	Brasil

Live Meetings	Herramienta actualizada de apoyo a conferencias.	México
Teleconferencia	Conferencia mediante vía Telefónica	Local
VPN – Redes	Red virtual para acceder a la red interna desde fuera de la empresa.	Local con validación desde México
AutoCad	Herramienta de diseño gráfico	Local
Clarify Prisma / Call Center	Herramienta para el manejo de call center de la división Diagnóstica	Basilea
Enlaces Cableado	Red utilizando cable directo, cruzado, hub o switch.	Local
Enlaces Wireless	Red inalámbrica	Colombia
UPS	Corriente eléctrica de emergencia	Local
Central Telefónica	Servicio de telefonía fija y móvil	Local
Track IT	Sistema para gestión de Helpdesk	Local
VNC	Herramienta para asistencia remota a usuarios.	Local
Equipos de computación y componentes	Material necesario para administración del Departamento de TI	Local

Tabla 1.2 Descripción y Ubicación de Servicios soportados por el Departamento de TI.[6]

1.3.5 MAPEO DE SERVICIOS QUE SOPORTA EL DEPARTAMENTO DE TI A LAS ÁREAS DEL NEGOCIO.

En la tabla 1.3 se puede visualizar los Departamentos que conforman el plan de continuidad del negocio y los servicios de TI que utilizan.

DEPARTAMENTO	SERVICIO DE TI
Finanzas	SAP
	Microsoft Office • Excel • Power Point • Outlook
	Intranet • Finanzas • Formularios
	Servidor de Archivos
	Messenger Interno
	Telefonía fija y móvil
	IXOS • Cuentas por Pagar
	Internet
	Scanner
	Impresora
	Copiadora
	Videoconferencia

[6] Fuente: Roche Ecuador S.A.

Estudios Clínicos	Intranet • Reservaciones • Workflow • Formularios
	Micosoft Office • Excel • Word • Power Point • Outlook
	Telefonía Fija y Móvil
	Messenger Interno
	Impresora
	Fax
	Videoconferencia
Registro Sanitario	SAP • Precios • Ingreso • Planes Comerciales
	Microsoft Office • Excel • Word • Outlook
	Internet
	Telefonía Fija y Móvil
	Messenger Interno
	Video Conferencia
	Intranet • Formularios
	SISALEM • Reportes Psicotrópicos
Ventas	Microsoft Office • Excel • Word
	Internet
	Workflow
	Telefonía Fija y Móvil
	Siebel • Reportes • Consultas
	SAP • Facturación • Devoluciones • Inventario • Clientes
	Impresora
	Videoconferencia
Marketing	IMS
	Internet
	Microsoft Office • Excel • Power Point • Outlook

	Siebel • Reportes
	Telefonía fija y móvil
	Messenger Interno
	Call Center
	Videoconferencia
	Scanner
	Intranet
	Net Meeting
Logística	Microsoft Office • Excel • Word • Outlook
	SAP • Productos
	Live Meetings
	Videoconferencia
	Teleconferencia
	Internet
	Intranet • Información Casa Matriz • Formularios
	Impresora
	Telefonía fija y móvil
Recursos Humanos	Intranet • Finanzas • Recursos Humanos
	Microsoft Office • Excel • Word • Outlook
	Telefonía fija y móvil
	Messenger Interno
	SAP
	Internet
	Videoconferencia
	Impresoras
	Servidor de Archivos
	Scanner
	Performance Scord Card

Administración y Finanzas – Diagnóstica	SAP • Cobranzas • Facturación • Cartera • Liberación de Pedidos • Órdenes de Compra
	Internet
	Messenger interno
	Telefonía fija y móvil
	Microsoft Office • Excel • Power Point • Outlook
	Impresoras
Servicio Técnico - Diagnóstica	Intranet • Grips
	Microsoft Office • Outlook
	SISALEM
	VPN – Redes
	AutoCad
	Clarify Prisma / Call Center
	Telefonía Fija y Móvil
	Messenger Interno

Tabla 1.3 Catálogo de Servicios que soporta el Departamento de TI.[7]

1.3.6 LISTADO DE PROCESOS DEL DEPARTAMENTO DE TI

Los principales procesos que desarrolla el Departamento de TI se describen a continuación:

Proceso de TI	Descripción	Periodicidad
Creación de Usuarios	El proceso de creación de usuarios consiste en solicitar permisos y cuentas de usuario a Registration Desk de México para agregar nuevas cuentas de usuario. Servicios utilizados: Microsoft Outlook, Internet, Enlaces.	El proceso de creación de usuarios se lo realiza cuando es necesario permitir el acceso a los diferentes sistemas, de forma general a personal nuevo. Responsable: Networking & EUS Services Responsible Ec.

[7] Fuente: Roche Ecuador S.A.

Obtención de Backups	El proceso de obtención de backups consiste en sacar un respaldo de las unidades de red y de los servidores que contienen aplicaciones locales que utilizan base de datos. Servicios utilizados: Servidor de Archivos, Enlaces.	El proceso de obtención de backups se lo realiza diariamente en cintas magnéticas de la información de las unidades de red. Responsable: Networking & EUS Services Responsible Ec, Analist & Report Responsible Ec.
Mantenimiento de Comunicaciones	El proceso de mantenimiento de comunicaciones consisten en realizar las reparaciones correspondientes o prevenir cualquier daño de los equipos de comunicación, revisarlos y conservarlos limpios de acuerdo a las políticas de TI. Servicios utilizados: Equipos de computación y componentes, Central telefónica, Enlaces cableado, Enlaces wireless, VPN redes, Telefonía fija y móvil, Videoconferencia.	El proceso de mantenimiento de telecomunicaciones se lo realiza de forma periódica y en caso de daños se contacta a los proveedores. Responsable: Networking & EUS Services Responsible Ec.
Mantenimiento de Hardware	El proceso de mantenimiento de hardware consiste en realizar las reparaciones correspondientes o prevenir cualquier daño del hardware, revisarlos y conservarlos limpios de acuerdo a las políticas de TI. Servicios utilizados: scanner, impresoras, copiadora, fax, UPS, equipos de computación y componentes.	El proceso de mantenimiento de hardware se lo realiza de forma periódica y en caso de daños se contacta a los proveedores para aplicar garantía o soporte técnico. Responsable: Networking & EUS Services Responsible Ec.
Mantenimiento de Software	El proceso de mantenimiento de software consiste en realizar las actualizaciones correspondientes a las aplicaciones utilizadas, mediante el envío de paquete por la red. Servicios utilizados: Microsoft Office, IMS,.	El proceso de mantenimiento de software se lo realiza al menos semanalmente o cuando así lo indica la matriz de cada aplicación. Networking & EUS Services Responsible Ec, Analist & Report Responsible Ec, IT Coordinator.
Adquisición de Equipos	El proceso de adquisición de equipos consiste en obtener los equipos que sean necesarios con el fin de no mantener en la empresa equipos obsoletos sino que tengan un excelente funcionamiento. Servicios utilizados: equipos de computación y componentes.	El proceso de adquisición de equipos se lo realiza periódicamente, aplicando acuerdos a nivel mundial con los proveedores y dependiendo de las políticas de vida útil de los equipos. Responsable: Networking & EUS Services Responsible Ec, IT Coordinator.
Adquisición de Software	El proceso de adquisición se software consiste en actualizar las aplicaciones utilizadas de acuerdo a las políticas que rige TI de casa matriz. Servicios utilizados: Microsoft Office, IMS.	El proceso de adquisición de software se lo realiza bajo las políticas globales que determina la matriz de la empresa (ERP, Base de Datos, Sistemas Locales). Responsable: Networking &

		EUS Services Responsible Ec, IT Coordinator.
Soporte a Usuarios	El proceso de soporte a usuarios consiste en brindar ayuda a los usuarios en el manejo de aplicaciones y equipos computacionales. Servicios utilizados: telefonía fija y móvil, central telefónica, Track IT, VNC.	El proceso de soporte a usuarios se lo realiza de manera constante con el fin de garantizar los servicios que provee TI. Responsable: Networking & EUS Services Responsible Ec, Service desk, Help desk.
Capacitación a Usuarios	El proceso de capacitación a usuarios consiste en realizar cursos, talleres, e-learnings con el fin de que los usuarios aprendan a usar las nuevas aplicaciones con las que se cuenta para un mejor desempeño del negocio. Servicios utilizados: Microsoft Office.	El proceso de capacitación a usuarios se lo realiza cuando existe la necesidad de que los usuarios tengan conocimiento de herramientas informáticas. Responsable: Todos los miembros de TI.
Administración de Base de Datos	El proceso de administración de base de datos consiste en mantener actualizadas las ases de datos con los datos proporcionados por los usuarios, realizar un monitoreo constante de la base, obtener reportes y backups. Servicios utilizados: bases de datos de aplicaciones; SAP, Siebel, IMS, Call center.	El proceso de administración de la Base de Datos se la realiza constantemente dado que se emiten diferentes tipos reportes diariamente. Responsable: Analist & Report Responsible Ec.
Mantenimiento y Soporte del ERP (SAP)	El proceso de mantenimiento y soporte de SAP consiste en brindar apoyo a los usuarios en el manejo de todos los módulos de SAP usados en el Ecuador, con el fin de explotar su utilidad. Servicios utilizados: SAP.	Los procesos de mantenimiento y soporte de SAP se lo realiza de forma constante dado que varias áreas de la empresa utilizan este sistema. Responsable: IT Coordinator.
Administración Web	El proceso de administración de la parte Web de la empresa consiste en la actualización y mantenimiento de Intranet y Extranet de la empresa. Servicios utilizados: Internet, Intranet.	El proceso de administración web se lo realiza de forma constante dado que por la actividad principal del negocio se utiliza frecuentemente publicidad y marketing. Responsable: Help desk.
Manejo de cableado y equipos eléctricos	El proceso de mantenimiento de cableado y equipos eléctricos consiste en verificar su correcto funcionamiento. Servicios utilizados: UPS, equipos de computación y componentes.	El proceso de manejo de cableado y equipos eléctricos se lo realiza constantemente con el fin de mantener los equipos prendidos y conectados a la red de la empresa. Responsable: Networking & EUS Services Responsible Ec, Help desk.

Tabla 1.4 Procesos del Departamento de TI

CAPÍTULO 2. ELABORACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO

En este capítulo se realizará la elaboración del Plan de Continuidad del Negocio para el Departamento de Tecnologías de la Información de Roche Ecuador S.A.

Para desarrollar el Plan de Continuidad se utilizarán las mejores prácticas de ITIL en lo que se refiere a gestión de la continuidad tomando en cuenta que los miembros del Departamento de TI de Roche Ecuador S.A. así lo han solicitado ya que se platearon como objetivo que desde el año 2007 se incorpore a su Departamento este modelo de gestión de servicios de TI además de certificar a su personal.

El objetivo principal de la gestión de la continuidad es "asegurar la continuidad en los sistemas de TI ante cualquier eventualidad, basado en el establecimiento de medidas preventivas"[8].

Las etapas que propone ITIL para la gestión de continuidad son las que se muestra en la Figura 2.1.

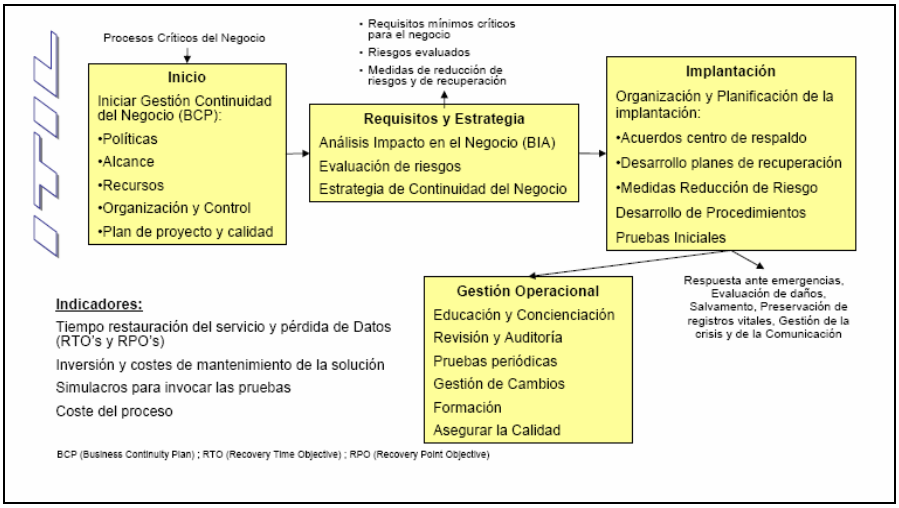

Figura 2.1 Esquema del Plan de Continuidad del Negocio propuesto por ITIL.[9]

[8] https://www.fdi.ucm.es/libre/formativas/ITILSopraProfit.pdf
9 Fuente: https://www.fdi.ucm.es/libre/formativas/ITILSopraProfit.pdf

Sin embargo de acuerdo a las necesidades de la empresa, éste esquema se lo ha adaptado de la siguiente manera con el fin de que sea aplicable a la realidad del Departamento de TI de Roche Ecuador S.A. y que sea práctico para su implementación, el esquema que se utilizará para el desarrollo del Plan de Continuidad se muestra en la Figura 2.2.

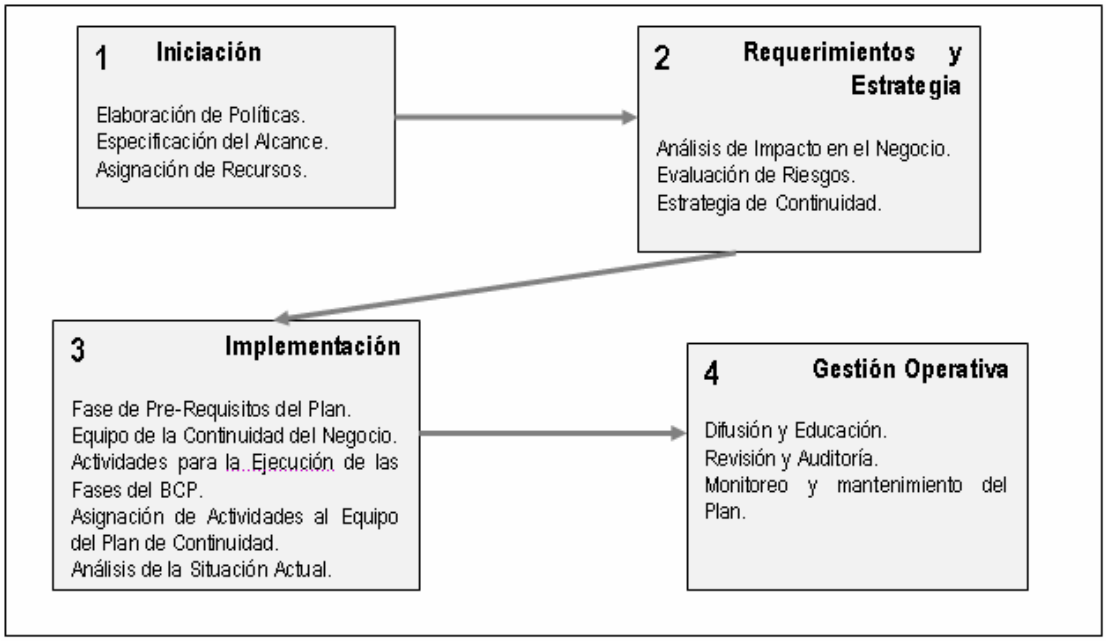

Figura 2.2 Esquema adaptado del Plan de Continuidad del Negocio propuesto por ITIL.[10]

2.1 ETAPA DE INICIACIÓN

La etapa de Iniciación comprende 3 aspectos importantes para elaborar el plan de continuidad:

Las políticas: donde se definen los acuerdos entre la compañía y la/las personas que diseñarán el plan.

El alcance: donde se definen los temas a tomar en cuenta en el plan de continuidad.

Los recursos: donde se asignan los recursos financieros, tecnológicos y humanos para lograr un diseño óptimo del plan de continuidad para el Departamento de TI.

[10] Fuente: https://www.fdi.ucm.es/libre/formativas/ITILSopraProfit.pdf. Adaptado por: Ana Lucía Leiva Garzón

2.1.1 ELABORACIÓN DE POLÍTICAS

Las políticas del plan de continuidad del Departamento de TI consisten en definir acuerdos de nivel de servicio entre los miembros o responsables del Departamento y el equipo de diseño y elaboración del plan de continuidad, de tal forma que se desarrolle el proceso con total normalidad rigiéndose a los acuerdos realizados. A continuación se definen las implicaciones de la política de continuidad:

- Los miembros del Departamento de TI de la empresa deberán comprometerse a colaborar y a participar activamente en la elaboración del plan de continuidad brindando toda la información necesaria que el equipo del plan requiera para realizar sus tareas.
- Los miembros del equipo de continuidad que elabora el plan de continuidad del negocio se comprometen a manejar con estricta confidencialidad la información que les sea proporcionada y referente a la empresa.
- El Departamento de TI de la empresa determinará personas claves de la empresa quienes serán los que proporcionen la mayor cantidad de la información que se requiere para elaborar el plan de continuidad.
- Se requieren al menos 4 personas que conformen el equipo de diseño y elaboración del plan de continuidad del negocio, por la gran cantidad de información que se debe manejar.
- Se deben firmar acuerdos de nivel de servicio y de compromiso entre los miembros del Departamento de TI y el equipo de diseño y elaboración del plan de continuidad.

2.1.2 ESPECIFICACIÓN DEL ALCANCE

El Plan de Continuidad del Negocio para el Departamento de TI pretende establecer los lineamientos generales que se deben seguir para continuar operando a pesar de que suceda algún tipo de desastre.

Se cubrirá el ciclo de vida del plan de continuidad del negocio que propone ITIL con sus cuatro etapas, tomando en cuenta los servicios estratégicos y los procesos críticos del Departamento de TI. El alcance del Plan de continuidad depende también de las expectativas del negocio y de los recursos disponibles para su inversión.

Se incluye también procedimientos para el mantenimiento constante de las estrategias de continuidad con el fin de tener siempre el plan vigente.

2.1.3 ASIGNACIÓN DE RECURSOS

La Gestión de la Continuidad del Servicio está destinada al fracaso si no se asigna una cantidad suficiente de recursos. Su dimensión depende de su alcance y sería absurdo y contraproducente establecer una política ambiciosa que no dispusiera de los recursos necesarios. También se debe tomar en cuenta que una emergencia no es el mejor momento para estudiar documentación y manuales.

Debido a que la asignación de recursos se la realiza en base a los estudios que se debe hacer para el plan de continuidad, en este ítem se describen los recursos disponibles en el Departamento de TI de Roche Ecuador S.A.

Actualmente no hay recursos asignados para la Gestión de La Continuidad del negocio dentro del Departamento de TI de Roche Ecuador S.A.

Los recursos con los que se cuenta en el Departamento de TI son:
Recursos Financieros: Existe un presupuesto anual que asigna el área de informática global a Ecuador para invertirlo en recursos computacionales.
Recursos Humanos: Al momento existen 5 personas en el Departamento de TI, quienes se encargan de la gestión del Departamento y de que marchen bien los servicios que se proporciona a todas las áreas de la empresa.
Recursos Tecnológicos: Una de las ventajas que tiene el Departamento de TI Ecuador es que en la parte tecnológica puede disponer de todos los recursos que

requiera así como su mantenimiento y soporte, en el tema tecnológico casa matriz se encarga de apoyar a todos y cada uno de los países con el fin de crear facilidad en las labores que realizan sus empleados.

Recursos de Logística: Muchos de los servicios de logística actualmente son contratados mediante outsourcing debido a la falta de personal en el Departamento de TI.

2.2 ETAPA DE REQUERIMIENTOS Y ESTRATEGIA

2.2.1 ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

El Análisis de Impacto en el Negocio consiste en una secuencia de pasos que interactúan con el fin de identificar el impacto de la interrupción en el negocio y de determinar los requerimientos necesarios para recuperar los procesos críticos del negocio una vez ocurrido el desastre.

En el Análisis de Impacto en el Negocio se desarrollarán los siguientes aspectos:

- Objetivos, alcance y suposiciones
- Identificar funciones y procesos
- Evaluar el Impacto financiero y operacional
- Identificar Procesos críticos del negocio
- Identificar MTD’s y Priorizar los Procesos del Negocio
- Identificar Sistemas y Aplicaciones Críticas de TI
- Determinar RTO y WRT
- Determinar RPO
- Análisis del daño que causa la interrupción de un proceso

Para la obtención de datos que se requieren para elaborar el diseño del plan de continuidad se utilizó una combinación de encuestas y entrevistas, las cuales se realizaron a los Gerentes de Departamento de Roche Ecuador S.A. El formato de estas encuestas se encuentra en el Anexo 1 del documento: Formato para Catálogo de Servicios; donde constan los siguientes datos: Servicios soportados por TI, Tiempo máximo que el departamento puede estar sin el servicio y

Criticidad del servicio para cada departamento evaluado. Estos datos se utilizarán especialmente a lo largo del desarrollo del análisis de impacto.

2.2.1.1 Objetivos y Alcance del BIA

2.2.1.1.1 Objetivos

- Identificar el impacto de una interrupción en el negocio.
- Definir los lineamientos para recuperar los procesos críticos del negocio una vez ocurrida la interrupción.
- Emitir información gerencial para la toma de decisiones.
  - Áreas de misión crítica del Negocio
  - Impacto operacional de la interrupción del negocio.
  - Deficiencias en las capacidades actuales de recuperación.
- Usar los resultados del BIA para estimaciones de BCP (Business Continuity Plan).

2.2.1.1.2 Alcance

El BIA que se desarrollará en éste ítem está enfocado única y exclusivamente al Departamento de Tecnologías de la Información de Roche Ecuador S.A. Se realizará el análisis del impacto que provoca un desastre y las posibles medidas que se tomarán para recuperar sistemas, recursos y datos.

2.2.1.1.3 Suposiciones

Es necesario asumir ciertas suposiciones las cuales ayudan a caracterizar los potenciales eventos de interrupción y las capacidades de recuperación de la compañía. Las suposiciones para el BIA[11] son:

- Si la interrupción ocurre en ocasiones donde el procesamiento es máximo.
- Si no existe facilidad de recuperación alterna de TI.
- Si no existe un área de trabajo u oficina alterna.
- Si no existe facilidad para operar y producir de forma alterna.

---

[11] Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

- Si el sitio afectado se vuelve inaccesible una vez ocurrida la interrupción.
- Si el sitio afectado se vuelve accesible después de un periodo de tiempo después de ocurrida la interrupción.
- Si el personal clave no se encuentra disponible en el momento de la interrupción.

2.2.1.2 Identificar Funciones y Procesos

Esta etapa consiste en identificar las funciones y procesos de la compañía, donde:
Funciones: Son los departamentos que conforman la compañía, ejemplo: Finanzas, Ventas, TI, etc.
Procesos: Son las actividades que los empleados de la compañía realizan en cada uno de sus departamentos, ejemplo: En Finanzas se realiza Facturación, Administración de Cuentas por Pagar y Cuentas por Cobrar, Comunicación con Bancos, Proveedores y Clientes, etc.

Los Departamentos que intervienen en el plan de continuidad son:

- Finanzas
- Estudios Clínicos
- Registro Sanitario
- Ventas
- Marketing
- Logística
- Recursos Humanos
- Administración y Finanzas – Diagnóstica
- Servicio Técnico - Diagnóstica
- IT

Las funciones y procesos de Roche Ecuador se detallan en la tabla 2.1.

FUNCION DEL NEGOCIO	PROCESO DEL NEGOCIO
Finanzas	Facturación
	Administración de Cuentas por Pagar y Cuentas por Cobrar
	Comunicación con Bancos, Proveedores y Clientes
	Alineamiento del Área de Finanzas con Colombia y Consultas Regionales e Internacionales
Estudios Clínicos	Supervisión de efectos adversos de medicamentos
	Investigación de nuevas aplicaciones de medicamentos
	Alineamiento del Área de Estudios Clínicos con Colombia y Consultas Regionales e Internacionales
Registro Sanitario	Legalización de productos en instituciones correspondientes
	Fijación de precios de productos
	Alineamiento del Área de Registro Sanitario con Colombia y Consultas Regionales e Internacionales
Ventas	Generación de Órdenes de Venta
	Generar Reporte de Ventas
	Visita Médica
	Alineamiento del Área de Ventas con Colombia y Consultas Regionales e Internacionales
Marketing	Promocionar Productos
	Promover Programas de Apoyo para Médicos y Pacientes
	Administración de los Call Center
	Alineamiento del Área de Marketing con Colombia y Consultas Regionales e Internacionales
Logística	Importación de productos
	Distribución de productos
	Almacenamiento de productos
	Reportes de Stock y de Importaciones
	Alineamiento del Área de Logística con Colombia y Consultas Regionales e Internacionales
Recursos Humanos	Selección de Personal
	Evaluación de Desempeño de Personal(Performance Scord Card)
	Alineamiento del Área de RRHH con Colombia
Administración y Finanzas – Diagnóstica	Facturación
	Administración de Cuentas por Pagar y Cuentas por Cobrar
	Comunicación con Bancos, Proveedores y Clientes
	Alineamiento del Área de Administración y Finanzas de Diagnóstica con Regionales
Servicio Técnico – Diagnóstica	Mantenimiento y Reparación de Equipos de Laboratorio
	Administración de Bases de Datos de Clientes
TI	Creación de Usuarios

	Obtención de Backups
	Mantenimiento de Comunicaciones
	Mantenimiento de Hardware
	Mantenimiento de Software
	Adquisición de Equipos
	Adquisición de Software
	Soporte a Usuarios
	Capacitación a Usuarios
	Administración de Base de Datos
	Mantenimiento y Soporte del ERP (SAP)
	Administración Web
	Manejo de cableado y equipos eléctricos

Tabla 2.1 Funciones y Procesos de la Compañía.[12]

2.2.1.3 Evaluar el Impacto Financiero y Operacional

En esta etapa se evalúa el impacto financiero y operacional asumiendo que ocurra una interrupción o desastre. La parte financiera del plan de continuidad será evaluado de manera cualitativa en todos los casos, debido a que las cifras reales representan información confidencial de la compañía, política que es regida por casa matriz.

2.2.1.3.1 Evaluación del Impacto Financiero

Para poder realizar la evaluación del impacto financiero se debe hacer la siguiente pregunta: Cuál sería la magnitud del impacto de la pérdida financiera si los procesos del negocio fuesen interrumpidos por un desastre?

En la tabla 2.2 se define el impacto financiero por cada proceso del negocio, en caso de ocurrir un desastre.

El impacto financiero se evalúa en el momento más crítico de cada función del negocio. En este caso los valores se especifican de manera cualitativa, dado que no es posible obtener cifras exactas en dólares americanos por el grado de confidencialidad que rige la empresa, a continuación se describen los valores

[12] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

utilizados en pérdidas por día de ganancias por concepto de ventas, se pueden definir los siguientes rangos:

Impacto 0: no hay pérdidas: 0 días

Impacto 1: bajo: 1-4 días

Impacto 2: medio: 5-10 días

Impacto 3: alto: más de10 días

Cabe destacar que la tabla 2.2 es un extracto de la tabla mostrada en el Anexo 2: Evaluación del Impacto Financiero, donde consta el impacto financiero de todas las funciones del negocio:

FUNCION DEL NEGOCIO	PROCESO DEL NEGOCIO	IMPACTO FINANCIERO
Finanzas	Facturación	3
	Administración de Cuentas por Pagar y Cuentas por Cobrar	3
	Comunicación con Bancos, Proveedores y Clientes	2
	Alineamiento del Área de Finanzas con Colombia y Consultas Regionales e Internacionales	1

Tabla 2.2 Evaluación del Impacto Financiero.[13]

A continuación se da una breve explicación del análisis de los valores ubicados en el impacto financiero para cada uno de los procesos realizados en los diferentes departamentos de la compañía:

Se dice que el proceso de Facturación tiene un impacto financiero de 3, debido a que si no se factura no hay ingresos monetarios a la empresa, por consiguiente se produce falta de pago a proveedores y empleados, quedan impagos los créditos que la empresa ha adquirido, lo que produce falta de credibilidad con los bancos, posibles procesos legales y falta de dinero circulante para realizar actividades internas de la empresa, como promoción de productos, adquisición de suministros, importación y distribución de productos, etc. Como se puede

[13] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

observar la detención del proceso de facturación puede producir un caos en el desarrollo de las actividades de la empresa por lo tanto se considera crítico.

Se dice que el proceso de Administración de Cuentas por Pagar y Cuentas por Cobrar tiene un impacto financiero de 3, dado que si no se lleva un manejo adecuado registrando de manera estricta cada uno de los movimientos puede producir el mismo impacto que el proceso de facturación porque están ligados directamente.

Se dice que el proceso de Comunicación con Bancos, Proveedores y Clientes tiene un impacto financiero de 2 debido a que hay varios medios por los que se puede acceder a información de Bancos, Proveedores y Clientes, está comunicación se puede ser vía telefónica, por correo electrónico, accesos mediante sitios web, en caso de haber problemas en todos estos medios, la comunicación puede darse personalmente, transportándose al lugar requerido.

2.2.1.3.2 Evaluación del Impacto Operacional

El impacto operacional se puede dar por la alteración de los niveles normales de diferentes factores como: suficiencia del servicio prestado, eficacia del servicio, satisfacción del cliente, imagen que proyecta la compañía, confianza del cliente, control de la compañía, ética y moral, posicionamiento en el mercado, dinero circulante en la empresa, etc.

La tabla 2.3, es un extracto de la tabla mostrada en el Anexo 3: Evaluación del Impacto Operacional; donde se han tomado tres factores representativos y diversos para evaluar el impacto operacional: Flujo de Caja, Satisfacción del Cliente y Posicionamiento en el Mercado, los cuales cubren diferentes áreas de la empresa.

El impacto operacional puede ser medido con los siguientes valores:

0: no produce impacto

1: bajo impacto

2: impacto medio

3: alto impacto

FUNCION DEL NEGOCIO	PROCESO DEL NEGOCIO	CLASIFICACIÓN DEL IMPACTO OPERACIONAL		
		Flujo de Caja	**Satisfacción del Cliente**	**Posicionamiento en el Mercado**
Finanzas	Facturación	3	1	2
	Administración de Cuentas por Pagar y Cuentas por Cobrar	3	3	3
	Comunicación con Bancos, Proveedores y Clientes	0	3	3
	Alineamiento del Área de Finanzas con Colombia y Consultas Regionales e Internacionales	2	0	0

Tabla 2.3 Evaluación del Impacto Operacional.[14]

Al Flujo de Caja se le asigna un valor Alto, dado que el movimiento financiero es frecuente y de uso delicado, por el tipo y tamaño de la empresa.

Con respecto al indicador de Satisfacción del Cliente se lo puede valorar como Bajo debido a que la parte financiera como lo es facturación es independiente del servicio al cliente, sin embargo la disponibilidad de dinero podría influir de manera indirecta en los servicios que se le ofrece al cliente como por ejemplo el financiamiento de los programas de salud que patrocina la empresa.

Se le asigna un valor Medio al indicador del Posicionamiento en el Mercado porque la interrupción de operaciones al producir la falta de disponibilidad de dinero se ve afectada el área de Marketing, dejando de promocionar y difundir información acerca de los productos, lo cual puede bajar el nivel de posicionamiento de los productos y de la empresa como tal en el mercado, logrado hasta entonces.

[14] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

2.2.1.4 Identificar Procesos Críticos del Negocio

Para definir los procesos críticos del negocio se analizan varios criterios cuyos valores fueron evaluados en la etapa anterior y que constan en la tabla 2.3.
Un proceso es crítico si:

- En el impacto financiero se tiene un valor de 2 o 3.
- Si en el impacto operacional existen al menos dos valores “Alto”.
- Si en el impacto operacional existen al menos un valor “Alto” y un valor “Medio”.

Si se da una valoración cuantitativa entre 0 y 3 a los indicadores del impacto operacional, de la siguiente manera:
Ninguno: 0: no produce impacto
Bajo: 1: bajo impacto
Medio: 2: impacto medio
Alto: 3: alto impacto
Se suman los valores del impacto financiero y operacional para sacar un total que servirá para evaluar el tiempo máximo que un proceso pude estar fuera de operaciones.

Una vez definidos los criterios, se realiza una revisión para identificarlos, estos resultados se presentan en la Tabla 2.4.

FUNCION DEL NEGOCIO	**PPROCESO DEL NEGOCIO**	**Impacto Financiero**	**Impacto Operacional**			**Total Puntos (Financiero + Operaciona)**
			Flujo de Caja	**Satisfacción del Cliente**	**Posicionamiento en el Mercado**	
Finanzas	Facturación	3	3	1	2	9
	Administración de Cuentas por Pagar y Cuentas por Cobrar	3	3	3	3	12
Estudios Clínicos	Supervisión de efectos adversos de medicamentos	2	1	3	3	9

Registro Sanitario	Legalización de productos en instituciones correspondientes	3	3	3	3	12
	Fijación de precios de productos	3	0	3	3	9
Ventas	Generación de Órdenes de Venta	3	3	3	3	12
	Visita Médica	3	1	3	3	11
Marketing	Promocionar Productos	3	3	3	3	12
	Promover Programas de Apoyo para Médicos y Pacientes	3	2	3	3	11
	Administración de los Call Center	3	3	3	3	12
Logística	Importación de productos	3	3	3	3	12
	Distribución de productos	3	3	3	3	12
Recursos Humanos	Selección de Personal	2	0	3	2	7
Administración y Finanzas – Diagnóstica	Facturación	3	3	1	2	9
	Administración de Cuentas por Pagar y Cuentas por Cobrar	3	3	3	3	12
Servicio Técnico – Diagnostica	Mantenimiento y Reparación de Equipos de Laboratorio	3	2	3	3	11
	Administración de Bases de Datos de Clientes	3	2	3	1	9

Tabla 2.4 Procesos Críticos del Negocio.[15]

En la columna del total de puntos en el proceso de facturación el resultado es de 9, debido a que se suman el impacto financiero y los tres valores del impacto operacional, de la siguiente manera:

[15] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Impacto financiero: 3
Impacto operacional, Flujo de Caja: 3
Impacto operaciolnal, Satisfacción del Cliente:1
Impacto operacional, Posicionamiento de Mercado: 2
Total puntos para el proceso de facturación es 9

Es importante mencionar que para el Departamento de TI cambian las acciones de los procesos en el momento del desastre, ejemplo:
Un proceso crítico de TI es la Obtención de Backups cuando se está en operaciones normales, sin embargo cuando ha ocurrido el desastre, no se considera crítico obtener un backup sino utilizar y recuperar los backups que se ha obtenido anteriormente, por lo que es importante tener en cuenta este factor, en la tabla 2.5 se da una breve especificación del cambio de acción de los procesos de TI.

Procesos en Operaciones Normales	Descripción del proceso una vez ocurrido el desastre
Obtención de Backups	Recuperación, utilización de Backups
Mantenimiento de Comunicaciones	Recuperación de las comunicaciones
Mantenimiento de Hardware	Recuperación de Sistemas, Servidores, PC's.
Mantenimiento de Software	
Soporte a Usuarios	Soporte a Usuarios
Administración de Base de Datos	Recuperar las Bases de Datos, e información en general
Mantenimiento y Soporte del ERP (SAP)	Recuperación de los enlaces locales (dado el caso) para el acceso al ERP, ubicado en Brasil.

Tabla 2.5 Especificación de Procesos Críticos del Departamento de TI en un Desastre

2.2.1.5 Identificar Sistemas y Aplicaciones Críticas de TI por Proceso del Negocio

Cuando un sistema o aplicación de TI soporta un proceso crítico del negocio, es decir, un proceso de la empresa, se lo denomina crítico.

Los procesos críticos del Departamento de TI se detallan en la Tabla 2.6 que es un extracto de la tabla mostrada en el Anexo 4: Sistemas, Aplicaciones y Recursos Críticos del Departamento de TI.

FUNCION DEL NEGOCIO	PROCESO DEL NEGOCIO	SISTEMAS, APLICACIONES Y RECURSOS CRÍTICOS DE IT
Finanzas	Facturación	SAP
		Intranet • Finanzas • Formularios
		Microsoft Office Excel
		Microsoft Office Outlook
		Telefonía
		Servidor de Archivos
		Impresora
		Copiadora
		Fax
	Administración de Cuentas por Pagar y Cuentas por Cobrar	SAP
		IXOS • Cuentas por Pagar
		Intranet • Finanzas • Formularios
		Microsoft Office Excel
		Microsoft Office Outlook
		Telefonía
		Servidor de Archivos
		Impresora
		Copiadora

Tabla 2.6 Sistemas, Aplicaciones y Recursos Críticos del Departamento de TI.[16]

2.2.1.6 Identificar MTD's

Cuando ya se conocen los procesos críticos del negocio se define el Maximum Tolerable Downtimes (MTD). El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio.

[16] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Ejemplo:
Cuanto tiempo puedo estar sin facturar, es decir, sin operaciones en mi área?

La estimación del MTD está basada en el valor del total de puntos, resultante de la suma del el impacto financiero e impacto operacional, por lo tanto, la escala de tiempos que se utiliza para dar valores del MTD a cada proceso del negocio es la siguiente, realizando la equivalencia de la manera indicada en la tabla 2.7:

A. De 1 a 24 horas
B. De 25 a 48 horas
C. De 49 a 72 horas
D. De 73 horas a 5 días
E. De 6 a 15 días
F. De 16 a 30 días

Total puntos (Impacto financiero+impacto operacional)	**MTD**
12	A
11	B
10	C
9	D
8	E
7	F

Tabla 2.7 Escala de Equivalencia para Definición de MTD's

Los valores del MTD se describen en la Tabla 2.8 que es un extracto de la tabla mostrada en el Anexo 5: Definición de MTD, Maximum Tolerable Downtimes.

FUNCION DEL NEGOCIO	**PROCESO DEL NEGOCIO**	**MTD**
Finanzas	Facturación	D
	Administración de Cuentas por Pagar y Cuentas por Cobrar	A

Tabla 2.8 Definición de MTD.[17]

En el proceso de Facturación se ha definido un MTD de D donde el tiempo máximo que puede la empresa estar sin realizar el proceso de facturación está en

[17] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

un rango de 73 horas a 5 días ya que afecta significativamente a toda la compañía.

Al proceso de Administración de Cuentas por Pagar y Cuentas por Cobrar se le ha asignando un MTD de A donde el tiempo máximo que la empresa puede operar sin inconvenientes hasta que este proceso vuelva a la normalidad es menor a 24 horas.

2.2.1.7 Determinar RTO y WRT

En este paso se necesita obtener el Requerimiento de Tiempo para la Recuperación, de forma general se refiere a la longitud de tiempo disponible para recuperarse desde el momento de la interrupción y consta de varios componentes que son detallados a continuación, la definición de estos indicadores ha sido tomada de Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004:

RTO (Recovery Time Objective): Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción.
Ejemplo:
Cuanto tiempo me demoro recuperando el Internet para volver a operaciones normales?
La escala que se utilizará para este indicador es la siguiente:

A. De 1 a 24 horas
B. De 25 a 48 horas
C. De 49 a 72 horas
D. De 73 horas a 5 días
E. De 6 a 15 días
F. De 16 a 30 días
G. De 31 a 60 días

WRT (Work Recovery Time): Indica el tiempo disponible para recuperar los datos perdidos, trabajo retrasado y datos capturados manualmente una vez que los sistemas o recursos son recuperados.

Ejemplo:

Si se me han perdido los datos de SAP en el desastre, cuánto tiempo me demoro recuperando los datos, el trabajo retrasado y digitalizando los datos que he registrado manualmente?

Los valores de WRT se evaluarán para los servicios de TI que aplique este indicador, es decir, en los sistemas y aplicaciones en los que se almacenen datos.

Para evaluar los tiempos RTO que se requiere para la recuperación de sistemas y recursos críticos se estima primero el tiempo que toma las actividades prioritarias de TI con el fin de que a partir de estas actividades base se puedan recuperar los demás recursos, La escala para este indicador se la valora en función del tiempo.

Actividad	RTO
Recuperar el enlace de red interno (LAN)	24 horas
Recuperar el enlace de red externo (WAN)	12 horas
Recuperar Servidor Dominio (Active Directory)	24 horas
Recuperar Servidor Exchange	48 horas
Recuperar Servidor de Intranet	48 horas
Recuperar Servidor de Archivos	72 horas
Recuperar Servidor de Bases de Datos (SQL Server, MySQL)	48 horas
Central Telefónica	8 horas

Tabla 2.9 Definición de RTO para TI.[18]

Los valores de RTO y WRT de los procesos y servicios de TI se pueden visualizar en la Tabla 2.10 que es un extracto de la tabla mostrada en el Anexo 6: Definición de Requerimiento de Tiempo de Recuperación (RTO y WRT).

FUNCION DEL NEGOCIO	PROCESO DEL NEGOCIO	PROCESOS Y SERVICIOS DE TI	RTO	WRT
Finanzas	Facturación	SAP	2 horas	4 horas

[18] Fuente: Miembros del Departamento de TI de Roche Ecuador y sus Proveedores

		Intranet • Finanzas • Formularios	1 hora	--
		Microsoft Office Excel	3 horas	1 hora
		Microsoft Office Outlook	3 horas	4 horas
		Telefonía	2 horas	--
		Servidor de Archivos	1 hora	2 horas
		Impresora	2 horas	--
		Copiadora	1 hora	--
		Fax	1 hora	--
	Administración de Cuentas por Pagar y Cuentas por Cobrar	SAP	2 horas	4 horas
		IXOS • Cuentas por Pagar	2 horas	1 hora
		Intranet • Finanzas • Formularios	1 hora	--
		Microsoft Office Excel	3 horas	1 hora
		Microsoft Office Outlook	3 horas	4 horas
		Telefonía	1 hora	--
		Servidor de Archivos	1 hora	1 hora
		Impresora	1 hora	--
		Copiadora	1 hora	--

Tabla 2.10 Definición de Requerimiento de Tiempo de Recuperación (RTO y WRT).[19]

En el proceso de Facturación se le ha calificado al sistema SAP con un RTO de 2 horas y un WRT de 4 horas. SAP utiliza principalmente el personal de Finanzas, para recuperar SAP se debe tomar en cuenta que es responsabilidad del Departamento de TI recuperar y verificar el correcto funcionamiento del enlace Ecuador-Brasil, pero la recuperación del sistema en si, en caso de haber colapsado, es responsabilidad del personal de TI de Roche Brasil recuperarlo. Estimando que en Brasil SAP funcione correctamente y una vez recuperado el enlace Ecuador-Brasil, se estima un tiempo de 2 horas en instalar el cliente de

[19] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

SAP y verificar su funcionamiento. El WRT tiene un valor de 4 horas debido a qe en SAP se registran una serie de transacciones del procesos de Facturación, en este tiempo se ingresarán los datos recolectados manualmente mientras duró la recuperación del sistema.

2.2.1.8 Determinar RPO

Es importante determinar la tolerancia que tiene el negocio para la pérdida de datos como resultado de un desastre o interrupción, para esto se define el RTO, la definición de este indicador ha sido tomada de Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004.

RPO (Recovery Point Objective): Es la magnitud de los datos perdidos en términos de un período de tiempo que puede ser tolerado por un proceso del negocio.
Ejemplo:
En SAP, datos perdidos de máximo cuantos días u horas puedo tolerar?
Si me demoro una hora en realizar una actividad y máximo puedo tolerar la pérdida de la mitad de los datos procesados, el RPO sería de media hora.
La escala que se utilizará para este indicador es en función del tiempo.

Los valores del RPO constan en la Tabla 2.11 que es un extracto de la tabla mostrada en el Anexo 7: Definición del RPO, Recovery Point Objective.

FUNCION DEL NEGOCIO	PROCESO DEL NEGOCIO	PROCESOS Y SERVICIOS DE IT	RPO
Finanzas	Facturación	SAP	1-2 horas
		Intranet • Finanzas • Formularios	--
		Microsoft Office Excel	menos de 30
		Microsoft Office Outlook	30-60 min
		Telefonía	--
		Servidor de Archivos	menos de 30 min
		Impresora	--

		Copiadora	--
		Fax	--
	Administración de Cuentas por Pagar y Cuentas por Cobrar	SAP	menos de 30 min
		IXOS • Cuentas por Pagar	30-60 min
		Intranet • Finanzas • Formularios	--
		Microsoft Office Excel	30-60 min
		Microsoft Office Outlook	menos de 30 min
		Telefonía	--
		Servidor de Archivos	30-60 min
		Impresora	--
		Copiadora	--

Tabla 2.11 Definición del RPO, Recovery Point Objective.[20]

En SAP para el proceso de facturación se define un RPO de 1-2 horas, ya que representan datos importantes donde se manejan grandes cantidades de dinero.

2.2.1.9 Análisis del daño que causa la interrupción de un proceso

Es importante determinar las consecuencias de la interrupción de un sistema, recurso o servicio soportado por el Departamento de TI con el fin de tener idea del impacto que se produce en el negocio si hay una paralización de operaciones. En la tabla 2.12 se da una breve descripción de las consecuencias de la detención de los servicios de TI y donde se encuentra ubicado.

Servicio de TI	Consecuencia	Ubicación
SAP	Si se interrumpe el sistema SAP, se detiene la facturación, la generación de órdenes de venta. Dado que SAP es el ERP de la empresa, varias áreas utilizan distintos módulos esenciales para el core del negocio.	Brasil

[20] Estructura de la Tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Microsoft Office Excel	La interrupción de Excel provoca que los usuarios no puedan elaborar varios reportes que lo realizan manualmente.	Local
Microsoft Office Power Point	El daño de Power Point provoca que los usuarios no puedan elaborar presentaciones para las frecuentes reuniones que programan.	Local
Microsoft Office Outlook	El daño de Outlook provoca que los usuarios no puedan tener comunicación con otros usuarios locales, regionales e internacionales, gran parte de la información es transmitida por e-mail.	Local
Intranet	El daño de la Intranet provoca que los usuarios no puedan ver y utilizar información publicada, formularios, datos financieros, enlaces a páginas de Roche de otros países.	Local
Servidor de Archivos	El no tener acceso a las unidades de red provoca que los usuarios no puedan ni guardar ni acceder a sus datos. Se tiene respaldos periódicos de estas unidades, se almacena información relevante.	Local
Messenger Interno	El daño del Messenger interno provoca que los usuarios no puedan comunicarse con otros usuarios locales, regionales e internacionales, Sirve como medio alternativo del e-mail.	Argentina
Telefonía fija y móvil	El daño o interrupción de la telefonía fija y móvil provoca que los usuarios no tengan salida telefónica interna y externa de la empresa, miembros de la empresa se comunican constantemente con visitadores médicos (en Roche Ecuador S.A. se los denomina Representante de Producto), quienes realizan su labor fuera de la empresa.	Local
IXOS	Si se detiene el sistema IXOS no se pueden enviar documentos de finanzas, ni documentos escaneados, debido a que mediante este sistema se transfieren de manera rápida los documentos al servidor ubicado en Brasil.	Brasil
Internet	El enlace a México permite la conexión a la red de la compañía, si se cae el enlace no se puede acceder a la información interna de la empresa.	Enlace a México
	El enlace local permite la navegación rápida en el Internet sin que sea necesario entrar a la red de la empresa, por lo tanto si no se tiene este servicio no se podría acceder de	Enlace Local

	manera rápida al Internet.	
Scanner	El daño del servicio de scanner provoca que los usuarios retrasen el envío de sus informes (documentos digitalizados), dado que las actividades de Ecuador están alineadas a las de Colombia.	Local
Impresoras	El daño del servicio de impresión provoca que los registros de documentos no queden archivados, solicitudes pendientes, invitaciones a eventos de promoción de productos y documentos en general.	Local
Copiadora	El daño del servicio de fotocopiado provoca que los usuarios no puedan respaldar documentos necesarios para el cumplimiento de sus funciones.	Local
Videoconferencia	El daño de la videoconferencia provoca que los usuarios no puedan tener reuniones que generalmente la hacen con usuarios regionales o internacionales, tal que no puedan intercambiar información importante para el desarrollo de la compañía.	Local
Fax	El daño o interrupción del servicio de fax provoca que los usuarios no puedan intercambiar información que se la considera urgente para realizar sus funciones.	Local
SISALEM	La detención de operaciones del sistema SISALEM produce que la división Diagnóstica de Roche no pueda registrar los problemas e inconvenientes que presentan los equipos médicos en los hospitales, se deja de llevar el registro y seguimiento desde la notificación del daño hasta su solución. De igual forma se deja de llevar el control de las sustancias psicotrópicas en la división Farma.	Local
Workflow	El daño del Workflow produce que no se lleve un registro de los pasajes de avión, vacaciones, viáticos, e información de políticas para la administración del personal de la empresa.	Brasil
IMS	Si no está disponible el sistema IMS no se puede contar con reportes de ventas para toar decisiones gerenciales para el área de Ventas de la empresa.	Local
Siebel	El daño del sistema Siebel provoca la falta de reportes periódicos para los usuarios, el registro de actividades de los visitadores médicos, médicos y pacientes que compran ciertos medicamentos.	Brasil

Net Meeting		Si no se tiene disponible el Net Meeting no se puede utilizarlo como medio de comunicación para conferencias regionales e internacionales.	Brasil
Live Meetings		Si no se tiene disponible el Live Meetings no se puede utilizarlo como medio de comunicación para conferencias regionales e internacionales.	Mexico
Teleconferencia		El daño o interrupción del servicio de teleconferencia provoca que los usuarios no puedan intercambiar información con usuarios regionales o internacionales, existen otros medio para este tipo de comunicación.	Local
SQL Server		Si no se tiene disponible la base de datos SQL Server no se puede registrar, consultar o eliminar información de hospitales, médicos, pacientes.	Local/Brasil
Oracle		Si no se tiene disponible la base de datos de Oracle el cual se conecta con el sistema SISALEM, no se puede registrar, consultar o eliminar los problemas suscitados con los equipos médicos.	Basilea- Suiza
VPN – Redes		Si no se tiene disponible la VPN, el personal de la empresa no podría acceder a la red interna desde fuera de ella.	Local
AutoCad		El daño o interrupción del AutoCad provoca que los usuarios no puedan realizar sus diseños de los equipos médicos de la división Diagnóstica.	Local
Clarify Prisma / Call Center		Si se produce un daño o interrupción en el sistema Clarify Prisma no se podría registrar las llamadas y datos de los clientes que se comunican al call center de la división Diagnóstica.	Basilea
Enlaces	Cableado	El daño o interrupción de la red de cableado estructurado provoca que los usuarios no puedan acceder a varios servicios como Internet, Intranet, información de unidades de red; ya que están fuera de la red de Roche Ecuador S.A.	Local
	Wireless	El daño o interrupción de la red de inalámbrica provoca que los usuarios no puedan acceder a varios servicios como Internet, Intranet, información de unidades de red; ya que están fuera de la red de Roche Ecuador S.A.	Colombia
Fluído Eléctrico		La interrupción o falta del servicio de fluído eléctrico provoca que los usuarios no tengan acceso a sus Desktops, poco tiempo disponible para usar sus laptops, no tendrían	Local

	servicio de impresión, copiado, scanneado, fax y luz.	
Central Telefónica	El daño o interrupción de la central telefónica provoca que los usuarios no puedan comunicarse vía telefónica con usuarios locales, regionles e internacionales. Existen otros medios de comunicación.	Local
Track IT	El daño o interrupción del Track IT provoca que los helpdesk no puedan registrar las actividades de sopote a usuarios y dar seguimiento a sus problemas para controlar el tiempo que se requiere solucionarlos.	Local
VNC	El daño o interrupción del VNC provoca que los HelpDesk no puedan dar asistencia remota a los usuarios que tienen problemas con su computador.	Local
Equipos de computación y componentes	El daño o la falta de equipos de computación y sus componentes provocan retraso en el trabajo de los miembros del Departamento de TI y de los usuarios de toda la compañía.	Local

Tabla 2.12 Consecuencias de la interrupción de los Servicios de TI.[21]

2.2.2 EVALUACIÓN DE RIESGOS

Para el plan de continuidad es necesario realizar un análisis de los riesgos que pueden afectar a una compañía, identificando las amenazas y sus consecuencias, de tal manera que en base a estos datos se puedan establecer las opciones de recuperación necesarias para mitigar los riesgos.

En la evaluación de riesgos se desarrollarán los siguientes puntos:

- Evaluación de Riesgos
  - Identificar el origen de la amenaza
  - Identificar la amenaza como evento
  - Identificar las Consecuencias de la amenaza
  - Identificar Probabilidad de Ocurrencia de la amenaza.
- Evaluación de las Opciones de Control de Riesgos
- Costos de Evaluación del Control de Riesgos.

---

[21] Fuente: Departamento de TI de Roche Ecuador S.A.

- Decisiones del Control de Riesgos

2.2.2.1 Identificación de Riesgos

Es importante tomar en cuenta que los riesgos constan de varios componentes, ilustrados en la Figura 2.3:

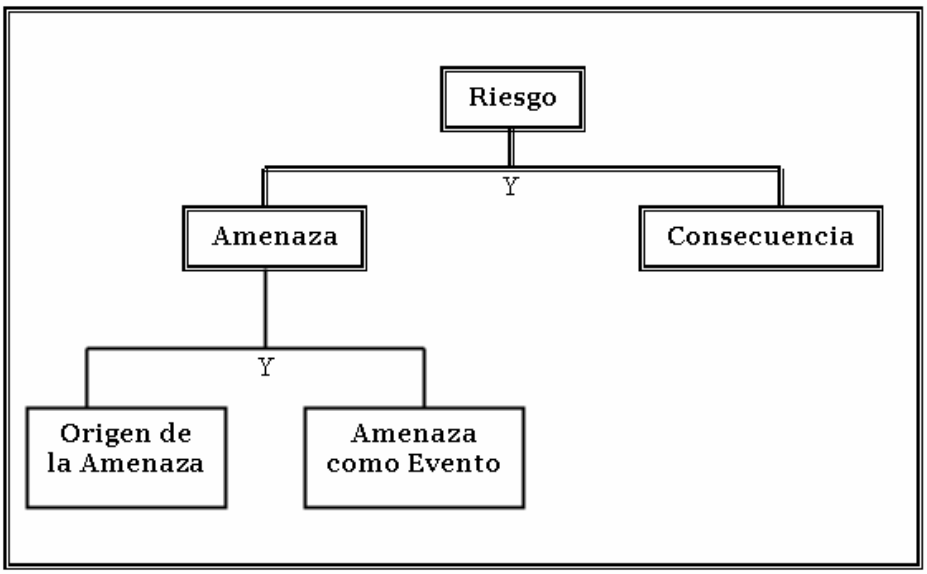

Figura 2.3 Componentes de un Riesgo.[22]

El riesgo se compone de dos partes: Amenaza y Consecuencia, donde la Amenaza consta de su origen y del evento como tal.
Ejemplo:
Origen de la Amenaza: Lluvias fuertes
Amenaza como Evento: Suspensión del Fluído Eléctrico
Consecuencia: Equipos de la empresa apagados, retrasos de trabajo.

2.2.2.2 Identificar el origen de la amenaza

Esta fase consiste en identificar la fuente que origina la amenaza para la organización. Las amenazas pueden ser de tipo natural, técnico y humano. En la Tabla 2. 11 se presenta un listado de las posibles amenazas para la compañía:

---

[22] Fuente: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

ORIGEN DE LA AMENAZA		
Amenazas Naturales	**Amenazas Técnicas**	**Amenazas Humanas**
Incendio	Interrupción de Energía eléctrica	Hackers
Terremoto/Temblor	Daño del Disco Duro del Computador	Virus de Computadoras
Vientos fuertes	Falla de los Servidores	Robo
Erupción Volcánica	Virus en las Aplicaciones de Software	Vandalismo
Epidemia de enfermedades mortales	Fallas del Aire Acondicionado (calentamiento de los equipos)	Terrorismo
Diluvio	Fallas en el servicio de voz o comunicación de datos	Accidentes en el trabajo
Ola de Calor (Corriente Cálida del Niño)	Fugas de Agua o Gas	Violencia de reglas en el lugar del trabajo
	Escasez de Energía	Complot (desastres provocados intencionalmente)
	Fallas o daño en la red	Huelgas
	Caída de un avión	Guerra
	Desastre nuclear	

Tabla 2.13 Tipos de Amenazas.[23]

2.2.2.3 Identificar la amenaza como evento

En esta fase se identifica la amenaza como un evento, se deriva del origen de una amenaza identificada. En la Tabla 2.14 es un extracto del Anexo 8: Amenazas como Eventos; donde se visualizan las amenazas como un evento.

Origen de la Amenaza	Amenaza como Evento
Incendio	Pérdida de Equipos
	Pérdida de Sistemas
	Pérdida de Recursos
	Pérdida de Información
	Ingreso inaccesible al edificio
	Falta de Energía Eléctrica
	Falta de disponibilidad de Comunicaciones
Fallas del Aire Acondicionado (calentamiento de los equipos)	Daño de los Equipos
	Falla en los Sistemas
	Ingreso inaccesible al edificio
	Falta de Energía Eléctrica
	Falta de disponibilidad de Comunicaciones
Hackers	Vulnerabilidad de los Sistemas
	Vulnerabilidad de la información
	Retrasos de Trabajo
	Fallos en la comunicaciones
	Acceso no autorizado a los sitios web

[23] Fuente: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Robo	Pérdida de Equipos
	Pérdida de Sistemas
	Pérdida de Recursos
	Pérdida de Información
	Retrasos de Trabajo
Complot (desastres provocados intencionalmente)	Retrasos de Trabajo
	Pérdida de Información
	Pérdida de Equipos

Tabla 2.14 Amenazas como Eventos.[24]

2.2.2.4 Identificar las Consecuencias de la amenaza

En este punto se identifica la consecuencia de la amenaza, esta consecuencia representa el segundo componente del riesgo, también se determina el recurso crítico que se ve afectado directamente por la amenaza, estos datos se detallan en la Tabla 2.15 que es un extracto de la tabla mostrada en el Anexo 9: Consecuencias de las Amenazas.

Origen de la Amenaza	Amenaza como Evento	Recurso Crítico	Consecuencia
Incendio	Quema de Equipos	Equipos de Computación	Equipos fuera de funcionamiento, apagados, dañados.
	Pérdida de Sistemas	Software/Programas	Software inaccesible, retrasos de trabajo e inconvenientes en la actividad principal del negocio.
	Pérdida de Recursos	Personal Hardware Sistemas Información Implementos computacionales, electrónicos, eléctricos, repuestos y de limpieza y Material de oficina	Recursos no disponibles para realizar actividades laborales y operacionales.
	Pérdida de Información	Información	Inaccesibilidad de información vital para la compañía, pérdida de información de los usuarios, produce retrasos de trabajo o inconvenientes en la actividad principal del negocio.

[24] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

	Ingreso inaccesible al edificio	Empresa - Departamento de TI	Los usuarios no tienen acceso a la red de la empresa, a sus computadores, a su información.
	Falta de Energía Eléctrica	Equipos de Computación, equipos eléctricos. Sistemas, Aplicaciones.	Los usuarios no pueden usar sus equipos de computación, retrasos de trabajo.
	Falta de disponibilidad de Comunicaciones	Telefonía, Redes, Radios, Messenger Interno	Los usuarios pierden la comunicación nacional, regional e internacional; con clientes, proveedores y colegas.

Tabla 2.15 Consecuencias de las Amenazas.[25]

2.2.2.5 Determinar la Probabilidad de Ocurrencia de la Amenaza

A continuación se presenta la Tabla 2.14 donde se analiza la probabilidad de ocurrencia de una amenaza, este indicador ayuda a tomar decisiones de la forma de mitigación de los riesgos que afectan al Departamento de TI; se analizan dos factores el ambiente o entorno donde se encuentra el edificio dentro del país y el histórico de los desastres suscitados, para esto se tiene la siguiente escala, donde se ha tomado un rango de análisis de historial de 9 años y se lo ha dividido en subrangos de 3 años, la escala mostrada en la Figura 2.4 consiste en que si ha ocurrido una amenaza en un rango de 3 años la probabilidad de ocurrencia es alta, si ha ocurrido en un Arango de 6 años la probabilidad es media y si la amenaza ha ocurrido en un rango de 9 años la probabilidad de ocurrencia es baja:

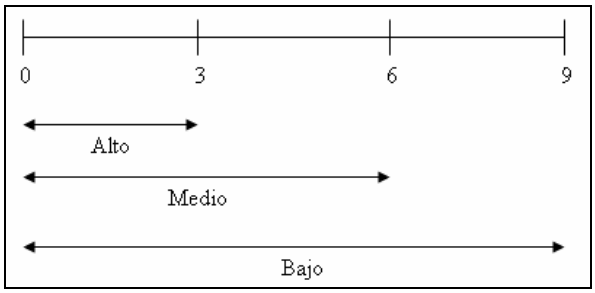

Figura 2.4 Escala para obtener la Probabilidad de Ocurrencia de la Amenaza

[25] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Amenazas	Probabilidad de Ocurrencia de la Amenaza
Incendio	Medio
Terremoto/Temblor	Bajo
Vientos fuertes	Bajo
Erupción Volcánica	Medio
Epidemia de enfermedades mortales	Bajo
Diluvio	Bajo
Ola de Calor (Corriente Cálida del Niño)	Bajo
Interrupción de Energía eléctrica	Alto
Daño del Disco Duro del Computador	Alto
Falla de los Servidores	Medio
Virus en las Aplicaciones de Software	Alto
Fallas del Aire Acondicionado (calentamiento de los equipos)	Alto
Fallas en el servicio de voz o comunicación de datos	Alto
Fugas de Agua o Gas	Bajo
Escasez de Energía	Bajo
Fallas o daño en la red	Medio
Caída de un avión	Bajo
Desastre nuclear	Bajo
Hackers	Alto
Virus de Computadoras	Alto
Robo	Medio
Vandalismo	Bajo
Terrorismo	Bajo
Accidentes en el trabajo	Bajo
Violencia de reglas en el lugar del trabajo	Bajo
Complot (desastres provocados intencionalmente)	Bajo
Huelgas	Bajo
Guerra	Bajo

Tabla 2.16 Análisis Probabilidad de Ocurrencia de una Amenaza

2.2.2.6 Evaluación de las Opciones de Control de Riesgos

Las opciones de control de riesgo se dividen en cuatro categorías:
Aceptación del Riesgo: Consiste en aceptar el riesgo y no hacer nada.
Anulación del Riesgo: Consiste en anular el riesgo totalmente.
Reducción del Riesgo: Consiste en reducir el riesgo a niveles aceptables.
Transferencia del Riesgo: Consiste en transferir el riesgo a otra entidad u organización.

Evaluar las opciones de control de riesgos consiste en no utilizar la categoría de Aceptación del Riesgo donde se deje de hacer esfuerzos por reducir o eliminar los riesgos, sino que se debe procurar llegar a la categoría donde se anule el riesgo en la medida que sea posible.

En la Tabla 2.17 que es un extracto del Anexo 10: Opciones de Control de Riesgos; se presenta la categoría de las opciones de control de riesgos.

Origen de la Amenaza	Opción de Control de Riesgo	Categoría del Control de Riesgo
Incendio	Alarma de incendios y extintores.	Reducción del Riesgo.
	Tener seguros contra incendios.	Transferencia del Riesgo.
	Protección del cuarto frío con material aislante.	Anulación del Riesgo.

Tabla 2.17 Opciones de Control de Riesgos.[26]

La opción de implementar una Alarma contra incendios y un sistema de extintores se la puede catalogar como Reducción de riesgo, ya que es una opción que no elimina totalmente sino que solamente ayuda a prevenir o detectar a tiempo un incendio.

La opción de Tener seguros contra incendios se la cataloga como Transferencia del Riesgo debido a que se tercializa el servicio, comúnmente denominado outsourcing, donde la empresa proveedora se encarga de reponer los recursos perdidos, dependiendo del tipo de seguro contratado.

La opción e Protección del cuarto frío con material aislante es una categoría de Anulación del riesgo debido a que si ocurre algún incendio, la parte protegida con el material especial se conservará intacto, para lo cual se toma en cuenta también la magnitud del incendio.

2.2.2.7 Costos de Evaluación del Control de Riesgos.

Esta etapa consiste en realizar un análisis del costo que se genera al implementar la opción para controlar el riesgo que amenaza al normal desempeño de las operaciones de la compañía.

---

[26] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

La escala está dada de acuerdo al presupuesto anual asignado para el Departamento de TI, la escala utilizada es la siguiente:

Alto: costo alto

Medio: costo medio

Bajo: costo bajo

En la Tabla 2.18 que es un extracto del Anexo 11: Costos de la Evaluación de Control de Riesgos, donde se muestra el costo de cada opción.

Origen de la Amenaza	**Opción de Control de Riesgo**	**Categoría del Control de Riesgo**	**Costo**
Incendio	Alarma de incendios y extintores.	Reducción del Riesgo.	Bajo
	Tener seguros contra incendios.	Transferencia del Riesgo.	Medio
	Protección del cuarto frío con material aislante.	Anulación del Riesgo.	Alto
Terremoto/Temblor	Alarma de detección de sismos.	Reducción del Riesgo.	Bajo
	Tener seguros contra sismos.	Transferencia del Riesgo.	Medio
	Que la estructura del edificio sea antisísmica.	Reducción del Riesgo.	Alto

Tabla 2.18 Costos de la Evaluación de Control de Riesgos.[27]

La opción de Alarma de incendios y extintores tiene un costo bajo tomando en cuenta que solamente se requiere una inversión inicial y un mantenimiento mínimo, se debería adquirir un detector de altas temperaturas y revisarlo frecuentemente que su funcionamiento sea correcto.

La opción de Seguros contra incendios tiene un valor Medio debido a que se debe pagar un valor mensual de tal manera que cubra los bienes que el Departamento de TI desee asegurar, mientras mayores bienes se desee recuperar, mayor será la cuota mensual a pagar a la aseguradora.

La opción de Protección del cuarto frío con material aislante tiene costos altos ya que la instalación y mantenimiento de este tipo de material requiere mucho cuidado y vigilancia constante.

[27] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

2.2.2.8 Decisiones del Control de Riesgos

Se analizarán las amenazas que tienen una probabilidad de ocurrencia de valor "Alto" y "Medio".

Para tomar la decisión acerca de la mejor opción de riesgo, se toma en cuenta que sería ideal anular el riesgo por completo al menor costo posible, debido a que hay que tomar en cuenta que se debe contrarrestar varios riesgos y que no se puede enfocar todos los recursos económicos a uno solo, sino tratar de abarcar a la gran mayoría especialmente a los que tienen mayor probabilidad de ocurrencia.

Un factor que ayuda a tomar una decisión adecuada es definir la prioridad de decisión de una opción ya que en algunos casos se puede tener varias opciones, para esto se define:

1: Prioridad Alta

2: Prioridad Media

3: Prioridad Baja

En la Tabla 2.19 que es un extracto del Anexo 12: Costos de la Evaluación de Control de Riesgos, se muestra la prioridad de decisión para cada opción de control de riesgo para implementar de acuerdo a varios factores que se puedan tomar en cuenta.

Origen de la Amenaza	Opción de Control de Riesgo	Categoría del Control de Riesgo	Costo	Prioridad de Decisión
Incendio	Alarma de incendios y extintores.	Reducción del Riesgo.	Bajo	2
	Tener seguros contra incendios.	Transferencia del Riesgo.	Medio	1
	Protección del cuarto frío con material aislante.	Anulación del Riesgo.	Alto	3

Tabla 2.19 Decisiones del Control de Riesgos.[28]

Se define como prioridad 1 a tener un seguro contra incendios debido a que es más factible recuperar un porcentaje de los recursos, de acuerdo al tipo de seguro

[28] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

contratado, antes que perder los recursos en su totalidad. Mientras que es preferible anular por completo el riesgo, también se debe tomar en cuenta los costos, en este caso implementar una protección con material aislante es una medida bastante costosa. Y sería recomendable implementar alarmas contra incendios como prioridad 2 o en una segunda etapa del plan de recuperación.

2.2.3 ESTRATEGIA DE CONTINUIDAD DEL NEGOCIO

La estrategia de continuidad del negocio consiste en identificar lo que se requiere para la recuperación y evaluar las mejores opciones para hacerlo.
Los puntos que se desarrollarán en la Estrategia de Continuidad del Negocio son:

- Identificación de Requerimientos de Recuperación
- Identificación de opciones de Recuperación
- Evaluación de Opciones Aplicables
- Evaluación Costo-Capacidad
- Consideraciones para las estrategias de recuperación

2.2.3.1 Identificación de Requerimientos de Recuperación

Para identificar los requerimientos de recuperación se pueden distinguir las siguientes áreas que deben ser recuperadas:

- Área de Trabajo
- Sistemas de IT e Infraestructura
- Datos e información crítica

Área de Recuperación: Área de Trabajo

Categorías de Requerimiento de Recuperación:

- Área de trabajo u oficina Alternativa para administración de la crisis

Área de Recuperación: Sistemas de TI e Infraestructura

Categorías de Requerimiento de Recuperación:

Se han clasificado los recursos de TI en las siguientes categorías:

- Sistemas críticos TI
- Enlaces de Datos
- Enlaces de Voz
- Servidores
- Recursos

La Tabla 2.20 indica la clasificación de los recursos en las categorías mencionadas, donde cada uno de los servicios que se necesite recuperar, entra a una de las categorías definidas de recuperación:

Sistemas críticos de TI	**Enlaces de Datos**	**Enlaces de Voz**	**Servidores**	**Recursos**
SAP	Messenger Interno	Telefonía fija	Intranet	Scanner
Microsoft Office Word	IXOS	Telefonía móvil	Servidor de Archivos	Impresoras
Microsoft Office Excel	Internet	Teleconferencia	Internet (local)	Copiadora
Microsoft Office Power Point	SISALEM	Central Telefónica	Servidor de Archivos	Videoconferencia
Microsoft Office Outlook	Workflow		Servidor de Dominio	Fax
IMS	Siebel		Servidor de Correo	Fluído Eléctrico
AutoCad	Net Meeting		Servidor de Bases de Datos	Equipos de computación y componentes
Track IT	Live Meetings			
VNC	VPN – Redes			
	Clarify Prisma / Call Center			
	Enlaces Cableado			
	Enlaces Wireless			

Tabla 2.20 Clasificación de Servicios de TI en Categorías de Recuperación

Área de Recuperación: Datos e Información Crítica

Categorías de Requerimiento de Recuperación:

- Almacenamiento de datos e información crítica en otro sitio.
- Bases de Datos

2.2.3.2 Identificación de opciones de Recuperación

Entre las opciones de recuperación pueden estar las siguientes:

Pre-Establecido: donde los sistemas son adquiridos e instalados antes del desastre y son usados únicamente para propósitos de recuperación.
Pre-Acordado: donde un acuerdo es realizado con un proveedor que garantice la entrega de los sistemas requeridos dentro de un período de tiempo convenido a partir del desastre.
Adquirir según se requiera: donde los sistemas requeridos son solicitados a un proveedor después de ocurrido desastre.

2.2.3.2.1 Área de Recuperación: Área de Trabajo

Categorías de Requerimiento de Recuperación:

a) Área de trabajo u oficina Alternativa para administración de la crisis

Opciones de Recuperación

a) Área de trabajo u oficina Alternativa para administración de la crisis.

En la Tabla 2.21 se muestran las opciones de recuperación para el área de trabajo que se usará como lugar alternativo para administrar la recuperación.

Categoría de Opción de Recuperación	Opción de Recuperación	Descripción de la Opción
Establecimiento Comercial	Sitio Móvil	Un sitio móvil es un establecimiento de recuperación alternativo en un vehículo. Este vehículo es pre-configurado con escritorios, sillas, hardware,

		software, datos y equipos de voz y comunicaciones.
	Sala de Conferencias de un Hotel	Una sala de reuniones o conferencias de un hotel debidamente preparada con equipos y materiales de oficina, comunicaciones de red, líneas telefónicas.
	Sitio Fijo	Una oficina disponible contratada a un proveedor, debidamente preparada con equipos y materiales de oficina, comunicaciones de red, líneas telefónicas.
Establecimiento propio de la compañía	Sitio alternativo propio de la compañía o sucursal.	Una oficina propia de la compañía o sucursal debidamente preparada con equipos y materiales de oficina, comunicaciones de red, líneas telefónicas.
Casas de los Empleados	Casa usada como oficina	Una casa o parte de ella, propia de un empleado del Departamento de TI, preparada con equipos y materiales de oficina, comunicaciones de red, líneas telefónicas.
Método de Adquisición de Recurso Crítico	Pre-Establecido	Establecimiento adquirido antes del desastre y preparado exclusivamente para recuperación.
	Pre-Acordado	Establecimiento adquirido a un proveedor que garantice su debido funcionamiento en un período de tiempo convenido entre las partes, a partir del desastre.
	Adquirir según se requiera	Solicitar una oficina o establecimiento cuando ocurra el desastre según las necesidades del momento.

Tabla 2.21 Opciones de Recuperación para el Area de Trabajo.[29]

2.2.3.2.2 Área de Recuperación: Sistemas de TI e Infraestructura

Categorías de Requerimiento de Recuperación:

a) Sistemas críticos IT
b) Enlaces de Datos
c) Enlaces de Voz
d) Servidores
e) Equipos Críticos y Recursos

Opciones de Recuperación

a) Recuperación de Sistemas críticos IT

En la Tabla 2.22 se muestran las opciones de recuperación para los sistemas de TI e Infraestructura.

Categoría de Opción de Recuperación	Opción de Recuperación	Descripción de la Opción
Método de Adquisición de	Pre-Establecido	Los sistemas son adquiridos e instalados antes de que ocurra un desastre y usados

[29] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Recurso Crítico		solamente con propósitos de recuperación.
	Pre-Acordado	Se realiza un acuerdo con un proveedor que garantice la entrega de los sistemas requeridos dentro del tiempo acordado después de la interrupción.
	Adquirir según se requiera	Los sistemas son solicitados al proveedor según sean requeridos una vez ocurrida la interrupción.

Tabla 2.22 Opciones de Recuperación para Sistemas de TI e Infraestructura[30]

b) Recuperación de Enlaces de Voz y Datos

En la Tabla 2.23 se muestran las opciones de recuperación para los enlaces de voz y datos.

Categoría de Opción de Recuperación	Opción de Recuperación	Descripción de la Opción
Método de Adquisición de Recurso Crítico	Pre-Establecido	Los enlaces son adquiridos e instalados antes de que ocurra un desastre y usados solamente con propósitos de recuperación.
	Pre-Acordado	Se realiza un acuerdo con un proveedor que garantice la recuperación de los enlaces requeridos dentro del tiempo acordado después de la interrupción.
	Adquirir según se requiera	Los enlaces son solicitados al proveedor según sean requeridos una vez ocurrida la interrupción.

Tabla 2.23 Opciones de Recuperación para Enlaces de Voz y Datos.[31]

c) Recuperación Servidores

En la Tabla 2.24 se muestran las opciones de recuperación para de los servidores.

Categoría de Opción de Recuperación	Opción de Recuperación	Descripción de la Opción
Método de Adquisición de Recurso Crítico	Pre-Establecido	Los servidores son adquiridos e instalados antes de que ocurra un desastre y usados solamente con propósitos de recuperación.
	Pre-Acordado	Se realiza un acuerdo con un proveedor que garantice la entrega de los servidores

[30] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

[31] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

		requeridos dentro del tiempo acordado después de la interrupción.
	Adquirir según se requiera	Los servidores son solicitados al proveedor según sean requeridos una vez ocurrida la interrupción.

Tabla 2.24 Opciones de Recuperación para Servidores[32]

En el Departamento de Roche Ecuador, los servidores tienen un estándar definido por casa matriz, tanto para hardware como para software. Tomando en cuenta que se usa una herramienta para obtener imágenes de las estaciones de trabajo cada cierto tiempo con el fin de mantener respaldo de la configuración de cada una de ellas, cabe destacar que esto no se lo hace para servidores, sin embargo este procedimiento sería recomendable con el fin de optimizar tiempos de recuperación para los servidores.

d) Recuperación de Equipos Críticos y Recursos

En la Tabla 2.25 se muestran las opciones de recuperación para equipos críticos y recursos.

Categoría de Opción de Recuperación	Opción de Recuperación	Descripción de la Opción
Adquirir según se requiera	Adquisición de Equipos	Los equipos son adquiridos según se requiera una vez ocurrido el desastre.
	Adquisición de partes	Las partes de equipos son adquiridas según se requiera una vez ocurrido el desastre.
Pre-Establecido	Contratos de mantenimiento de servicios para salvamento y recuperación	Los acuerdos de salvamento y recuperación de algún daño en los equipos y recursos son establecidos con un proveedor antes de que ocurra el desastre.
	Mantenimiento de backups de partes críticas en un establecimiento alternativo	Un proveedor de las partes críticas las almacena como respaldo en un sitio alterno, antes de que ocurra el desastre.
	Mantenimiento de backups de equipos críticos en un establecimiento alternativo	El equipo crítico es almacenado como respaldo antes de que ocurra el desastre.

Tabla 2.25 Opciones de Recuperación Equipos Críticos y Recursos.[33]

[32] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

[33] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Casa matriz de Roche exige estándares de hardware y software para los computadores por lo que se debe tomar en cuenta estos lineamientos para la adquisición de los recursos necesarios para la recuperación.

2.2.3.2.3 Área de Recuperación: Datos Críticos

Categorías de Requerimiento de Recuperación:

a) Almacenamiento de datos críticos en otro sitio.

Opciones de Recuperación

a) Almacenamiento de datos críticos en otro sitio.

En la Tabla 2.26 se muestran las opciones de recuperación para almacenamiento de datos críticos en el sitio alternativo.

Categoría de Opción de Recuperación	Opción de Recuperación	Descripción de la Opción
Frecuencia de backups de datos	Continuo	Los datos son respaldados de forma continua en un establecimiento alternativo utilizando replicación en tiempo real y técnicas de obtención de backups.
	Diario	Los datos son respaldados una vez al día
	Semanal	Los datos son respaldados una vez a la semana
	Mensual	Los datos son respaldados una vez al mes.
Tipos de Backups	Completas	Un backup normal o completo de todas las filas
	Incrementales	Un backup solamente de las filas ingresadas o modificadas a partir de la fecha del último backup incremental.
	Diferenciales	Un backup solamente de las filas ingresadas o modificadas a partir de la fecha del último backup completo.
Métodos para Obtención de Backups	Arreglo de discos remoto	Se obtiene una imagen o espejo de los datos en un establecimiento alternativo para proveer disponibilidad continua usando tecnologías tales como ruteador de transacciones y sistemas propietarios redundantes tolerantes a fallos
	Alta disponibilidad de Clustering	Este método usa software y hardware basado en equipos organizados en una WAN(Wide Area Network) que pueden ser reemplazados automáticamente a un equipo con fallas.
	Almacenamiento en la Red	Alta rapidez y alto desempeño en la red que conecta los computadores con diferentes sistemas operativos para comunicarse con

		un dispositivo de almacenamiento.
	Almacenamiento virtual	Combinación de múltiples dispositivos de almacenamiento dentro de un dispositivo lógico virtual que puede ser administrado de manera centralizada, y es presentado como una unidad de almacenamiento.
	Arreglo de Discos	Un controlador sobre un disco primario de escritura o un controlador sobre un disco secundario en modo síncrono.
	Disco secundario	Los cambios de los datos de un disco primario son continuamente capturados en un log el cual es registrado en el disco de un servidor secundario en modo asíncrono.
	Aplicaciones o Utilitarios basados en replicación de datos	Aplicaciones o Utilitarios envía los datos del servidor primario a un servidor de aplicaciones en un sitio alternativo.
	Cajas fuertes electrónicas	Los respaldos son creados automáticamente en una caja fuerte ubicada donde un proveedor.
	Tareas programadas remotamente	Logs transaccionales o tareas programadas son enviadas a un establecimiento de recuperación alternativo.
	Cintas de Backup	Los respaldos transaccionales se almacenan en cintas magnéticas.
Establecimiento Alternativo de Almacenamiento	Establecimiento comercial de almacenamiento de datos	Sitios de almacenamiento remoto ofrecidos por un proveedor comercial para almacenar los datos registrados en dispositivos para backups. El sitio es relativamente seguro y con un ambiente confiable.
	Establecimiento de almacenamiento remoto de datos, propio de la compañía.	Sitio de almacenamiento remoto de la compañía donde los datos son almacenados en dispositivos para backups. El sitio es relativamente seguro y con un ambiente confiable.

Tabla 2.26 Opciones de Recuperación de almacenamiento de Datos Críticos en el Sitio Alternativo.[34]

b) Almacenamiento de los registros físicos en un sitio alternativo.

En la Tabla 2.27 se muestran las opciones de recuperación para Almacenamiento de registros físicos en un Sitio Alternativo.

Categoría de Opción de Recuperación	**Opción de Recuperación**	**Descripción de la Opción**
Frecuencia de los backups	Diariamente	Los registros son respaldados una vez al día
	Semanalmente	Los registros son respaldados una vez a la semana

[34] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

	Mensualmente	Los registros son respaldados una vez al mes
	Anualmente	Los registros son respaldados una vez al año
Dispositivos de almacenamiento	Microfilm	Diferentes tipos de dispositivos de almacenamiento son necesarios para obtener los backups
	Disco Óptico	
	Cintas Magnéticas	
	Discos	
	CDs	
Salvamento y Métodos de restauración	Contratos Pre-Acordados con un proveedor para salvamento y restauración de operaciones	Un acuerdo o contrato es establecido con un proveedor para salvar y restaurar los registros dañados, hasta antes de la interrupción
	Contratos según se requiera para salvamento y restauración	Un acuerdo o contrato es establecido con un proveedor para salvar y restaurar los registros dañados, después de la interrupción
Establecimiento Alternativo de Almacenamiento	Establecimiento comercial de almacenamiento de información.	Sitios de almacenamiento remoto ofrecidos por un proveedor comercial para almacenar los datos registrados en dispositivos para backups. El sitio es relativamente seguro y con un ambiente confiable.
	Establecimiento de almacenamiento remoto de información, propio de la compañía.	Sitio de almacenamiento remoto de la compañía donde los datos son almacenados en dispositivos para backups. El sitio es relativamente seguro y con un ambiente confiable.

Tabla 2.27 Opciones de Recuperación para Almacenamiento de Registros Físicos en el Sitio Alternativo.[35]

2.2.3.3 Evaluación de Opciones Aplicables

Esta fase consiste en evaluar las opciones que se podrían aplicar de acuerdo a la realidad del día día de la compañía. Donde en la columna de aplicación de la tabla 2.25 se muestra las siguientes posibles opciones:

Adecuada

Recomendable

No recomendable

No aplica

Mientras que en la columna de Prioridad de Implementación se pueden medir con niveles de prioridad para tener abiertas las opciones según costos y factibilidad de la empresa, la forma de avaluación es la siguiente:

---

[35] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

1: Prioridad Alta

2: Prioridad Media

3: Prioridad Baja

4: Ultima Prioridad

5: No concuerda con los Objetivos

En la Tabla 2.28 que es parte del Anexo 13: Evaluación de Opciones Aplicables, se muestran el tipo de aplicación y la prioridad de implementación de las opciones de recuperación para Almacenamiento de registros físicos en un Sitio Alternativo.

Categoría de Opción de Recuperación	Opción de Recuperación	Aplicación	Prioridad de Implementación
Establecimiento Comercial	Sitio Móvil	No aplica	5
	Sala de Conferencias de un Hotel	Recomendable	3
	Sitio Fijo	Recomendable	2
Establecimiento propio de la compañía	Sitio alternativo propio de la compañía o sucursal.	Adecuada	1
Casas de los Empleados	Casa usada como oficina	Recomendable	4
Método de Adquisición de Recurso Crítico	Pre-Establecido	Adecuado	3
	Pre-Acordado	Recomendable	4
	Adquirir según se requiera	No recomendable	5

Tabla 2.28 Evaluación de Opciones de Recuperación Aplicables para Almacenamiento de Registros Físicos en el Sitio Alternativo.[36]

La opción más recomendable y adecuada es mantener un sitio alternativo propio de la compañía donde se tenga recursos ya disponibles que servirían solamente para la recuperación, estos recursos podrían ser utilizados mientras se les de un mantenimiento constante para verificar su correcto funcionamiento en todo momento, tal que cuando ocurra el desastre se los utilice única y exclusivamente para operaciones de recuperación. Los costos serían graduales y como se lo implementaría con anticipación resulta económico para la empresa.

[36] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

La segunda opción aplicable es tener un recontrato de un sitio fijo implementado con todos los recursos necesarios de tal forma que inmediatamente después del desastre se pueda usar el sitio para administrar la recuperación, esto también puede incurrir en costos bajos debido a que es previa contratación para lo cual se puede llamar a licitación y escoger la opción más conveniente.

La contratación de la Sala de Conferencias de un Hotel tiene una prioridad de 3 debido a que no todos los hoteles tienen implementados los recursos necesarios para una recuperación, y los costos pueden ser altos dependiendo de los días que pueda extenderse el uso de la misma.

La opción que se ha determinado con una prioridad de 4, la casa de alguno de los empleados, es poco adecuada debido al espacio reducido, gran inversión para implementación de recursos requeridos para la recuperación y pérdida de tiempo para iniciar la administración de recuperación.

La opción de un sitio móvil es la ultima prioridad por el hecho de que los costos de implementación y mantenimiento resultan muy altos, es difícil encontrar un lugar donde guardar el vehículo de manera que este protegido, y es menos confiable utilizar en estos casos la comunicación móvil por las interferencias, cuando en realidad se requiere comunicación confiable.

2.2.3.4 Evaluación Costo-Capacidad

Una vez que se han definido las opciones aplicables en el Departamento de TI de Roche Ecuador S.A., se procede a evaluar los costos en términos cualitativos dado el grado de confidencialidad que mantiene la empresa, además de los esfuerzos que cada opción de recuperación requiere para ser satisfactoria. El propósito de esta evaluación es seleccionar la opción de recuperación que más se acople a las necesidades de la compañía.

Parámetros a evaluarse:

Esfuerzo: Estima el grado de esfuerzo que se requiere para recuperarse.

Calidad: Estima la calidad del servicio, información, rapidez asociados a la opción.

Confiabilidad: Estima como satisface las necesidades de contabilidad que requiere la empresa.

Control: Estima el nivel de control que la empresa tiene una vez implementada la opción de recuperación.

Seguridad: Estima factores de seguridad física y de información de cada opción.

La escala cualitativa para valorar estos factores es la siguiente:

Alto

Medio

Bajo

No aplica

2.2.3.4.1 Área de Recuperación: Área de Trabajo

Categorías de Requerimiento de Recuperación:

a) Área de trabajo u oficina Alternativa para administración de la crisis

Opciones de Recuperación

a) Área de trabajo u oficina Alternativa para administración de la crisis

En la Tabla 2.29 que es parte del Anexo 14: Evaluación Costo-Capacidad, se muestra el análisis costo-capacidad de las opciones de recuperación del Area de Trabajo.

Categoría de Opción de Recuperación	**Opción de Recuperación**	**Costo-Capacidad**					
		Esfuerzo de Recuperación	Calidad	Confiabilidad	Control	Seguridad	Costo
Establecimiento Comercial	Sitio Móvil	Alto	Baja	Baja	Bajo	Baja	Alto
	Sala de Conferencias de un Hotel	Medio	Media	Media	Medio	Alta	Medio
	Sitio Fijo	Bajo	Alta	Alta	Alto	Alta	Medio
Establecimiento propio de la compañía	Sitio alternativo propio de la compañía o sucursal.	Bajo	Alta	Alta	Alto	Alta	Bajo

Casas de los Empleados	Casa usada como oficina	Alto	Baja	Baja	Medio	Alta	Alto
Método de Adquisición de Recurso Crítico	Pre-Establecido	Bajo	Alta	Alta	Alto	Alta	Bajo
	Pre-Acordado	Medio	Alta	Media	Medio	Media	Medio
	Adquirir según se requiera	Alto	Baja	Baja	Bajo	Baja	Alto

Tabla 2.29 Evaluación Costo-Capacidad para la Opción de Recuperación del Area de Trabajo.[37]

Para el Caso de un Sitio Móvil se evalúa al Esfuerzo de Recuperación como Alto debido a que el espacio para el numero de personas que administraría la recuperación es reducido, la Calidad es Baja por el grado de implementación que se requiere para la recuperación, la Confiabilidad es Baja porque se requiere precisión en los enlaces y al ser en un vehiculo seria móvil, el Control es Bajo porque es consecuencia de de la confiabilidad con respecto a los enlaces, la Seguridad es Baja porque es un sitio móvil y se debe tener alto cuidado cuando haya movilización, el costo es alto porque requiere gran inversión para implementar los recursos necesarios para la recuperación.

Para el Caso de un Sitio alternativo propio de la compañía o sucursal, se evalúa al Esfuerzo de Recuperación como Bajo debido a que se puede implementar con antelación todos los recursos necesarios para la recuperación, la Calidad es Alta porque la implementación de los recursos se lo haría con licitaciones para encontrar las mejores opciones, la Confiabilidad es Alta porque se tendría precisión en los enlaces y se tendría monitoreo constante de los recursos, el Control es Alto porque sería factible el mantenimiento ya que por estándares de la empresa son constantes, la Seguridad es Alta porque se tendría protegidos los recursos tanto de hardware como software, el Costo es Bajo porque como se lo implementa con anticipación se puede escoger los recursos tal que resulte económico.

[37] Estructura de la tabla tomada de: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

2.2.3.5 Consideraciones para las estrategias de recuperación

- Considerar un sitio alternativo para administrar la recuperación, tal que no sea afectado por el mismo desastre.
- Considerar que debe haber facilidades para que las personas claves que forma el equipo de administración de la recuperación, puedan llegar al sitio alternativo.
- Reducir los costos, re localizando el sitio alternativo a uno menos costoso, una vez que se tenga el control de la interrupción.
- Asegurar que las facilidades de recuperación de TI sean adecuadas, que tengan controles, protección, seguridad.
- Asegurar que los proveedores que proporcionan las facilidades de recuperación de TI sean lo suficientemente confiables para cubrir el soporte técnico necesario.
- Para los sistemas que deben ser recuperados en menos de 8 horas es recomendable utilizar la estrategia pre-establecida de recuperación, donde los sistemas son adquiridos antes de cualquier desastre.
- Para los sistemas que deben ser recuperados en menos de 72 horas es recomendable utilizar la estrategia pre-acordada de recuperación, donde los sistemas son adquiridos en un tiempo determinado una vez que ocurra la interrupción.
- Para los sistemas que deben ser recuperados en un tiempo mayor a 72 horas es recomendable utilizar la estrategia de adquirir según se requiera, donde los sistemas son adquiridos después del desastre.
- Usar sistemas de reemplazo en las áreas donde sea posible.
- Asegurar que los sistemas de red, voz y datos y equipos tengan suficiente capacidad de recuperación.

2.3 ETAPA DE IMPLEMENTACIÓN

2.3.1 FASE DE PRERREQUISITOS PARA IMPLEMENTACIÓN DEL PLAN

2.3.1.1 Equipo de Recuperación Inicial

Una vez ocurrido un desastre se asume que la persona encargada de liderar la recuperación del departamento de TI que es IT Coordinator, convoca inicialmente solo a los miembros del departamento de TI para realizar la evaluación del sitio afectado, una vez realizada la evaluación se procederá a decidir si es necesario llamar al todo el equipo del plan de continuidad.

2.3.1.2 Centro de Reunión Alternativo en caso de desastre

De acuerdo al tipo de desastre se tienen las siguientes prioridades de puntos de encuentro para reunión de los miembros de TI, dados los siguientes casos:

Si el sitio de desastre es accesible, reunirse en:

1. Matriz - 5to Piso
2. Matriz – Sala de Reuniones 6to Piso
3. Matriz – Sala de Reuniones Planta Baja

Si el edificio es inaccesible, reunirse en:

1. Sucursal - Bodega Farma
2. Sucursal – Bodega Diagnóstica
3. Centro de Administración contratado.

Si el desastre afectó toda la ciudad, reunirse en:

1. Sucursal – Guayaquil
2. Sucursal - Cuenca

2.3.1.3 Acuerdos con Proveedores

Se asume que el Departamento de TI de Roche ya tiene implementados acuerdos con proveedores para que proporcionen los recursos necesarios en caso de desastre en los tiempos pre-acordados.

2.3.1.4 Requerimientos Tecnológicos

Se asume que se están trasladando constantemente los backups fuera de la matriz del Departamento de TI y que se cuenta con personal 24/7 en el proveedor para que entreguen los backups a las personas autorizadas en el momento que se requiera, o en su defecto, que sean entregados a personas de Roche con autorización de los representantes legales para realizar esta actividad.

2.3.2 EQUIPO DE LA CONTINUIDAD DEL NEGOCIO[38]

Para poder implementar el plan de continuidad del negocio para el Departamento de TI se debe definir el equipo que se encargará de la recuperación y del retorno a operaciones normales de las actividades del Departamento de TI. El número de miembros del equipo de recuperación depende de del alcance y la complejidad del plan. Para el caso del Departamento de TI de Roche Ecuador S.A. los miembros del equipo serán las 5 personas que conforman el Departamento de TI, por el tamaño y las actividades que realiza la empresa, se puede contar también con el apoyo de al menos tres personas del Departamento de TI de Roche Colombia que apoyen la gestión de Ecuador debido a que la administración de informática tanto de Colombia como de Ecuador es gestionada desde Colombia.

La estructura que debe tener el equipo del plan de continuidad del negocio se muestra en la figura 2.5:

---

[38] Fuente: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004. Abstract de Business Continuity Team, pag. 143, 144, 145, 146, 147 y 148.

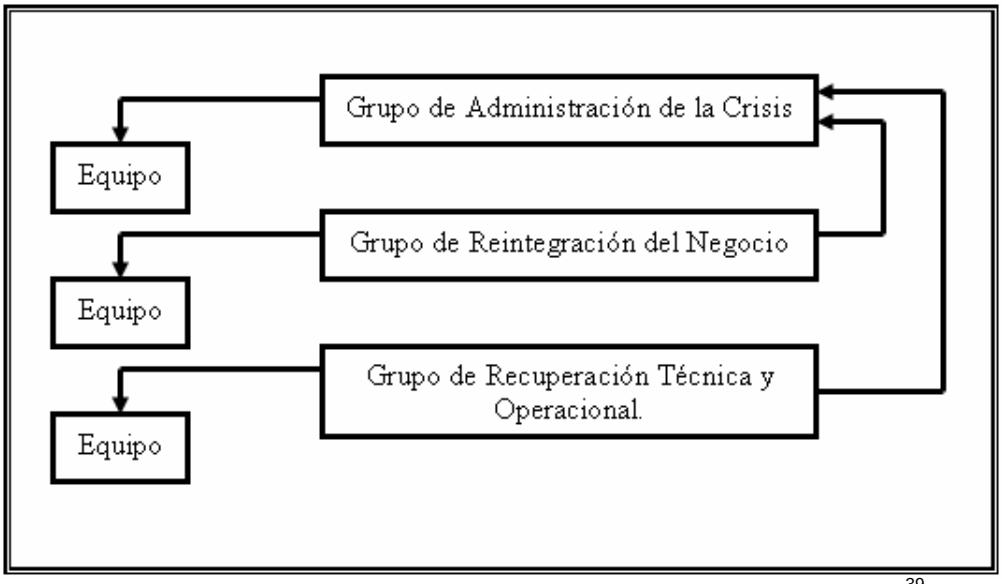

Figura 2.5 Estructura del Equipo del Plan de Continuidad del Negocio.[39]

Grupo de Administración de la Crisis: consiste en los siguientes roles:

Equipo de Administración de la Crisis (CMT-Crisis Management Team): se encarga de administrar y controlar el plan de continuidad del negocio, del plan de respuesta de emergencia y del plan de comunicación de la crisis. Inmediatamente después de ocurrida la crisis el CMT se traslada al centro de administración del desastre, dado el caso al sitio alternativo predeterminado. El CMT es el equipo autorizado de invocar al plan de continuidad del negocio en caso de ser necesario.

Coordinador de la Continuidad del Negocio (BCC-Business Continuity Coordinator): se encarga de supervisar las siguientes fases del plan de continuidad: respuesta inicial y notificación, evaluación de problemas y escalamiento declaración del desastre, plan de implementación de logística, rcuperación y reintegración y normalización.

Equipo de Evaluación de Daños (DAT-Damage Assessment Team): es el equipo en cargado de realizar la evaluación de los daños inmediatamente ocurrido el desastre de acuerdo a los parámetros establecidos en el plan y en base a estos datos estimar el tiempo que tomará la recuperación.

---

[39] Fuente: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004

Equipo de Notificación (NT-Notification Team): es el equipo encargado de convocar al personal responsable de la ejecución del plan de continuidad, la convocatoria se la debe realizar de acuerdo a los procedimientos preestablecidos en el plan.

Equipo de Respuesta de Emergencia (ERT-Emergency Response Team): Se encarga de gestionar la integridad de vidas humanas, recursos y entorno del Departamento de TI, presta auxilio facilitando la evacuación y brinda asistencia médica.

Equipo de Comunicación de la Crisis (CCT-Crisis Comunication Team): Es el equipo responsable de proveer información a todo el personal, esta información debe ser consistente, veraz, oportuna y exacta.

Equipo de Logística y Suministro de Recursos (RPLT-Resource Procurement and Logistics Team): es el equipo encargado de proveer de manera oportuna, confiable y segura los recursos necesarios para que se cumpla el proceso de recuperación.

Equipo de Evaluación de Riesgos (RAM-Risk Assessment Team): es el equipo responsable de evaluar y controlar los riesgos, mitigándolos y tomando en cuenta asuntos legales y seguridad para lograrlo.

Grupo de Reintegración del Negocio: consiste en los siguientes roles:

Equipo de Administración de Usuarios (UMT-User Management Team): es el equipo encargado de mediar o interactuar entre los usuarios y el equipo técnico de la recuperación.

Equipo de Unidades del Negocio (BUT-Business Unit Team): es un equipo conformado por una persona clave de cada función del negocio, cada uno de ellos evalúa las necesidades de su área y las comunica al equipo de recuperación.

Grupo de Recuperación Técnica y Operacional: consiste en los siguientes roles:

Equipo de Recuperación Técnica (ITTRT-IT Technical Recovery Team): se enfoca en cumplir los siguientes roles:

a. Equipo de Sistemas Operativos/Plataformas
b. Equipo de Redes y Telecomunicaciones

c. Equipo de Sistemas de Bases de Datos
d. Equipo de Aplicaciones
e. Equipo de Sistemas de Backups
f. Equipo de Controles de Seguridad
g. Equipo de Integración y Pruebas

Equipo de Salvatage y Restauración de Registros Vitales (Vital Records Salvage and Restoration Team): se encarga de recuperar los registros dañados, de aplicar los procedimientos para restaurar los registros a condiciones normales.
Equipo de Recuperación de Backups de Registros Críticos y Datos (Data and Critical Record Backup Retrieval Team): Es el equipo encargado de recuperar las copias de los backups de sistemas operativos, aplicaciones, datos, registros críticos, manuales y documentación necesaria para la recuperación. Es también responsable de la protección y seguridad de los dispositivos que contienen los backups durante la recuperación.
Equipo de Coordinación de Soporte (Administration Support Coordination Team): es el equipo de apoyo para los miembros de la recuperación, contacta a proveedores, alimentación, hospedaje, transportación y demás actividades de soporte.

2.3.3 EQUIPO DE LA CONTINUIDAD DEL NEGOCIO PARA EL DEPARTAMENTO DE TI DE ROCHE ECUADOR S.A.

Para el caso de Roche al existir 5 personas que conforman el departamento de TI y 3 personas de apoyo, cada miembro debe cumplir una o varias tareas por lo que el equipo se distribuye de la siguiente manera:

- **IT Manager Ecuador/Colombia**
  a. Equipo de Administración de la Crisis
  b. Coordinador de la Continuidad del Negocio
  c. Equipo de Notificación
- **IT Coordinator Ecuador**
  a. Equipo de Administración de la Crisis

b. Coordinador de la Continuidad del Negocio
c. Equipo de Notificación
d. Equipo de Integración y Pruebas

- **Networking & End User Services Responsible Ecuador**
  a. Equipo de Evaluación de Daños
  b. Equipo de Evaluación de Riesgos
  c. Equipo de Respuesta de Emergencia
  d. Equipo de Redes y Telecomunicaciones
  e. Equipo de Administración de Usuarios
  f. Equipo de Sistemas de Backups
  g. Equipo de Salvatage y Restauración de Registros Vitales
  h. Equipo de Recuperación de Backups de Registros Críticos y Datos

- **Networking & End User Services Responsible Colombia/Ecuador**
  a. Equipo de Sistemas Operativos/Plataformas
  b. Equipo de Redes y Telecomunicaciones
  c. Equipo de Sistemas de Backups
  d. Equipo de Controles de Seguridad
  e. Equipo de Salvatage y Restauración de Registros Vitales
  f. Equipo de Recuperación de Backups de Registros Críticos y Datos

- **Analist & Report Responsible Ecuador**
  a. Equipo de Evaluación de Daños
  b. Equipo de Evaluación de Riesgos
  c. Equipo de Sistemas Operativos/Plataformas
  d. Equipo de Sistemas de Bases de Datos
  e. Equipo de Salvataje y Restauración de Registros Vitales
  f. Equipo de Recuperación de Backups de Registros Críticos y Datos

- **Analist & Report Responsible Colombia/Ecuador**
  a. Equipo de Sistemas de Bases de Datos
  b. Equipo de Integración y Pruebas

c. Equipo de Salvatage y Restauración de Registros Vitales
d. Equipo de Recuperación de Backups de Registros Críticos y Datos

- **Help Desk**
  a. Equipo de Respuesta de Emergencia
  b. Equipo de Logística y Suministro de Recursos
  c. Equipo de Administración de Usuarios
  d. Equipo de Coordinación de Soporte

- **Service Desk**
  a. Equipo de Respuesta de Emergencia
  b. Equipo de Comunicación de la Crisis
  c. Equipo de Logística y Suministro de Recursos
  d. Equipo de Administración de Usuarios
  e. Equipo de Salvatage y Restauración de Registros Vitales
  f. Equipo de Aplicaciones

- **Personas clave de cada Función del Negocio (10 miembros)**
  a. Equipo de Unidades del Negocio

- **Personal Adicional Recomendado (al menos 5 personas conformadas por proveedores, personal outsourcing,etc.)**
  a. Equipo de Redes y Telecomunicaciones
  b. Equipo de Aplicaciones
  c. Equipo de Coordinación de Soporte
  d. Equipo de Sistemas de Backups
  e. Equipo de Controles de Seguridad
  f. Equipo de Integración y Pruebas
  g. Equipo de Salvatage y Restauración de Registros Vitales
  h. Equipo de Recuperación de Backups de Registros Críticos y Datos

Se han distribuido los roles de la manera antes mencionada tomando en cuenta las funciones que cumplen dentro de la empresa o por su conocimiento acerca de

las actividades del negocio. Por lo que los equipos quedarían conformados como indica la Figura 2.6:

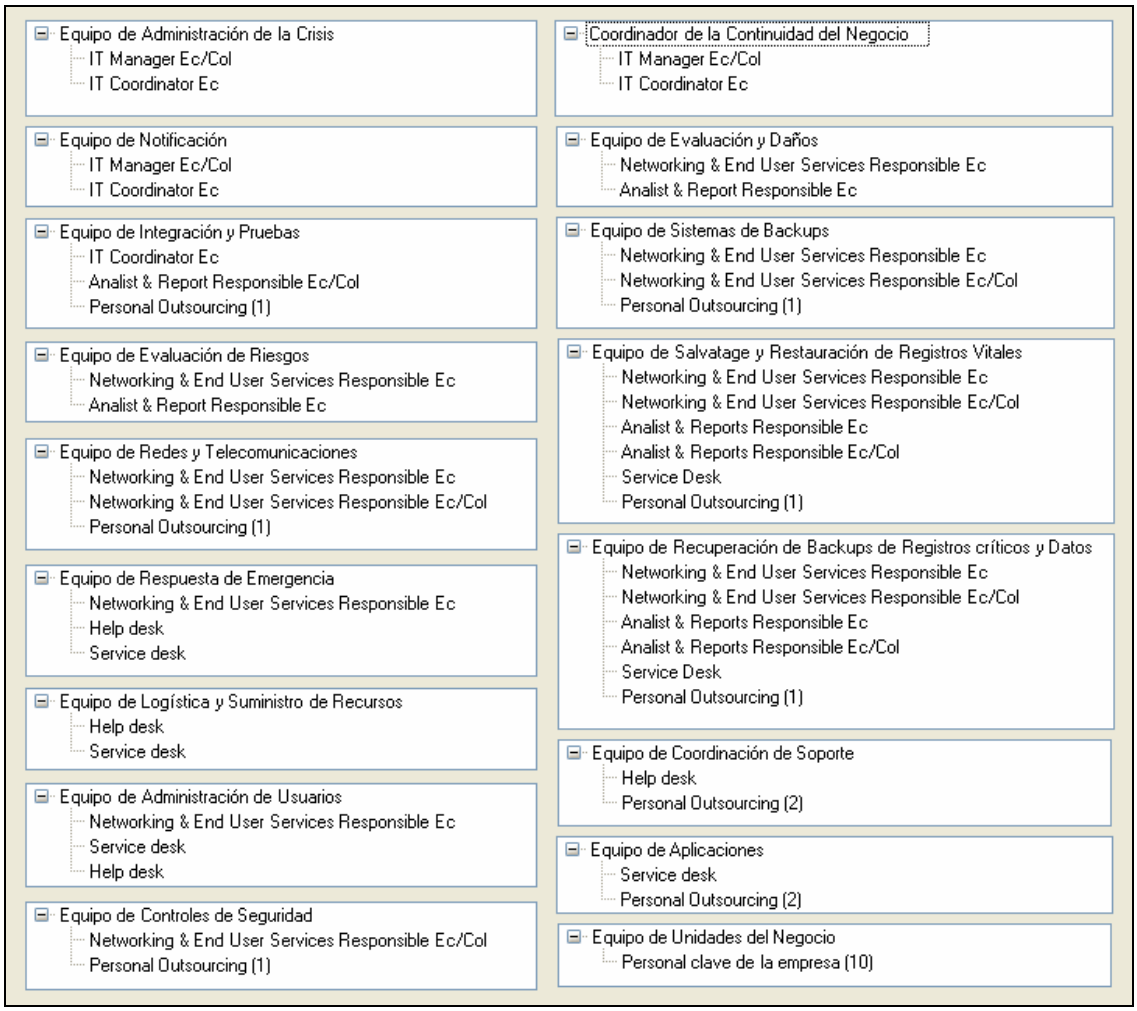

Figura 2.6 Distribución de los Equipos del Plan de Continuidad del Negocio

Si bien debería existir un equipo para cada parte de la recuperación de un desastre, dado el alcance, la asignación de recursos y el tamaño del Departamento de TI; se ha repartido varias tareas para una sola persona, a su vez dada la magnitud de la empresa y su número de usuarios se ha estimado conveniente añadir al equipo del plan de continuidad 5 personas adicionales a los miembros del Departamento de TI, este personal agregado pueden ser proveedores, o personal tercializado contratado específicamente para conformar el equipo de recuperación de manera inmediata una vez ocurrido el desastre.

El equipo de la continuidad del negocio se formará de acuerdo al tipo de desastre que se produzca, ya que de acuerdo a la magnitud del desastre se debe

determinar la necesidad de que todos o parte de los miembros del equipo actúen en la recuperación; por lo tanto los miembros del plan actuarán en la recuperación de acuerdo a la Tabla 2.30.

Impacto / Miembro	No Impacto	Bajo	Medio	Alto
IT Coordinator EC		x	x	x
Analist & Report Responsible Ec		x	x	x
Networking & EUS Responsible Ec	x	x	x	x
Service Desk	x	x	x	x
Help Desk	x	x	x	x
IT Manager Co/Ec			x	x
Analist & Report Responsible Co/Ec				x
Networking & EUS Responsible Co/Ec				x
Personal Clave del Negocio (10)				x
Personal Outsourcing (5)			x	x

Tabla 2.30 Matriz Equipo-Impacto

2.3.4 INFORMACIÓN DE CONTACTOS

Se debe definir una estructura jerárquica que represente la secuencia de llamadas que se debe hacer en caso de desastre entre los miembros del plan de continuidad, para el Departamento de TI de Roche Ecuador S.A. se define la estructura de llamadas en la Figura 2.7:

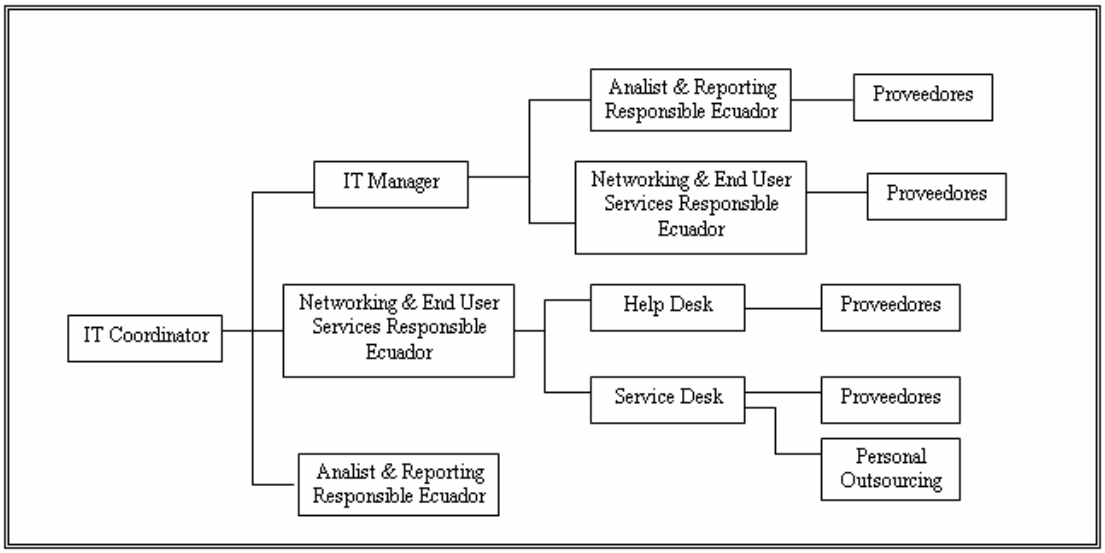

Figura 2.7 Estructura Jerárquica de Llamadas Telefónicas

En el plan de continuidad debe estar registrada la siguiente información de cada miembro que conforma el equipo de la continuidad del negocio, en el Anexo 15: Datos Personales de Miembro del equipo Plan de Continuidad, se puede ver el formulario de cada miembro del equipo donde consta su información personal:

- Nombre del Equipo
- Nombre del Miembro del Equipo
- Rol o Cargo del Miembro del Equipo
- Número de Teléfono de la Oficina, extensión.
- Número del Teléfono Celular
- Dirección de la Casa
- Número de Teléfono de la Casa
- Dirección de e-mail
- Nombre de un miembro suplente, quien realice las funciones del miembro oficial en caso de estar ausente.

En este documento no se ha publicado la información personal de cada miembro del equipo del plan de continuidad del negocio, debido a que ese tipo de información se lo maneja de manera confidencial y dentro de la empresa, adicionalmente esta información se la debe actualizar de manera constante por la variabilidad de las personas en sus cargos. La plantilla donde se puede llenar la

información de los proveedores se puede ver en el Anexo 16: Datos de Proveedores.

2.3.5 ACTIVIDADES PARA LA EJECUCIÓN DE LAS FASES DEL BCP[40]

El plan de continuidad del negocio tiene como objetivo seguir una serie de pasos que ayudarán a manejar de forma óptima la administración de un desastre minimizando el tiempo de recuperación y retorno a la normalidad de las actividades del negocio, en este caso restablecer lo antes posible los recursos de computación y comunicaciones, para que los usuarios puedan operar de forma normal, dentro de lo que dependa del Departamento de TI. Las actividades que se especifican en cada fase han sido tomadas como referencia del libro Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004, y adaptadas para el caso que se está analizando.

A continuación se detallarán los pasos a seguir en cada fase del plan de continuidad.

2.3.5.1 Respuesta inicial y Notificación

Esta etapa inicia inmediatamente después de sucedido el desastre, se evalúa el impacto de los daños, todos los miembros del plan de continuidad son notificados y el plan es activado.
Para mantener el orden y la calma, para que cada miembro sepa lo que tiene que hacer, se han definido las siguientes actividades para esta fase:

1. Definir el lugar de reunión del equipo de continuidad.
2. Cada miembro del equipo recibe la alerta de desastre, utilizando el árbol de contactos.

---

[40] Fuente: Syed, Akhtar; Syed, Afsar; Business Continuity Planning Methodology; 2004. Activities for BC Plan Execution Phases. Actividades selecciónadas según la aplicabilidad a la empresa Roche Ecuador S.A.

3. Notificar a las proveedores acerca del daño, en caso de de ser necesario.
4. Acceder a la documentación del plan de continuidad del negocio.
5. Determinar si el establecimiento es accesible.
6. Si el desastre ocurre en horas no laborables, trasladarse al establecimiento de manera inmediata.
7. Evaluación preliminar de los daños.
8. Evaluación preliminar de las causas de los daños.
9. Evaluación del impacto del desastre.
10. Preparar un reporte preliminar del desastre y sus problemas.
11. Notificar a los miembros del plan de recuperación.

El informe preliminar de la magnitud del impacto de los daños y sus causas proporcionará una idea global del problema, se pueden utilizar los datos obtenidos en esta etapa una vez llenado el check list del plan de continuidad ya que ahí consta la información necesaria para construir el informe preliminar de la falla.

2.3.5.2 Evaluación del Problema y Escalamiento

La etapa 2 consiste en dos partes, la primera es determinar la magnitud del problema basado en el reporte preliminar, la segunda parte consiste en decidir si se pasa o no de manera inmediata a la siguiente fase.
Las actividades a seguir para esta etapa son:

1. Recepción del reporte preliminar del problema.
2. Revisión de la magnitud y del impacto de los daños en el reporte preliminar del problema.
3. Inspeccionar el sitio del desastre para evaluar detalladamente el impacto causado por la interrupción.
4. Evaluar la interrupción de los procesos y el daño en los equipos y recursos en general. Apoyarse completando el Anexo 17: Análisis de Impacto en el Negocio.
5. Estimar las pérdidas financieras, para esto se puede utilizar una lista de chequeo de recursos, elaborada previamente. Apoyarse completando el Anexo 18: Evaluación de Pérdidas Financieras.

6. Estimar el impacto del desastre basado en los registros del plan, catalogando al desastre como bajo, medio o alto.
7. Si esto no impacta a lo procesos críticos se debe continuar el monitoreo de la situación, de lo contrario continuar a la siguiente fase del plan de ejecución.
8. Evaluar los riesgos que implica el desastre. Apoyarse completando el Anexo 19: Evaluación de Riesgos.
9. Preparar un informe detallado del problema.
10. El equipo de notificación debe comunicar al personal clave, los temas que contiene el informe detallado del problema.

2.3.5.3 Declaración del Desastre

La decisión de declarar un desastre está basada en el informe de la evaluación detallada del problema. Se puede seguir las siguientes actividades:

1. Revisar el informe detallado del problema, analizando magnitud del desastre, los riesgos e impactos de los daños.
2. Revisar las opciones de recuperación disponibles en la sección de la estrategia de recuperación del plan de continuidad. Apoyarse en el Anexo 20: Estrategias de recuperación.
3. Decidir la mejor opción de recuperación para la situación actual.
   a. Preparar la declaración de desastre.

   Apoyarse en el Anexo 21: Declaración de Desastre.

2.3.5.4 Plan de implementación de Logística

En esta etapa se prepara el entorno para que el establecimiento de recuperación tenga todos los recursos necesarios para empezar la recuperación y la normalización de operaciones. Para lo cual se tiene las siguientes actividades:

1. Ordenar o adquirir hardware y software, en caso de ser necesario.
2. Ordenar o adquirir equipos de voz y datos, en caso de ser necesario.
3. Ordenar o adquirir impresoras, faxes y copiadoras, en caso de ser necesario.

4. Ordenar o adquirir cintas magnéticas y discos duros, en caso de ser necesario.
5. Obtener formularios necesarios para continuar con los procesos manualmente.
6. Enviar los documentos claves al sitio alternativo incluyendo el plan de continuidad del negocio.
7. Recibir los equipos y recursos en el sitio alternativo.
8. Preparar todo el sitio de manera rápida para iniciar la administración de la recuperación.

Para preparar adecuadamente el sitio de la recuperación, se debe asegurar que las personas que van a administrar la recuperación tengan la disponibilidad y facilidades para transportarse al sitio, para lo cual las actividades siguientes apoyan a cumplir este requerimiento:

1. Identificar quienes están disponibles para realizar las operaciones de recuperación.
2. Identificar quienes se transportarán hacia el sitio alternativo, desde donde y cuanto tardarán.
3. Identificar quienes trabajarán en el sitio original si éste es accesible.
4. Identificar los recursos requeridos, tales como laptops, copias del plan de continuidad, hacer un listado de equipos.
5. Proveer los recursos necesarios.
6. Proveer la información necesaria para que todos los miembros puedan llegar al sitio alternativo, así como contactos administrativos y técnicos del sitio.
7. Mantener contacto permanente con las personas que proveen las facilidades del sitio para coordinar el entorno y configuraciones que se requiera para la recuperación.

2.3.5.5 Recuperación

Las áreas de recuperación que se deben tomar en cuenta en esta fase son:

1. Si la recuperación es en el Sitio principal de la empresa, es decir, el sitio afectado.

2. Si la recuperación es en el Establecimiento de recuperación alternativo para TI, sucursal de la empresa.
3. Si la recuperación es en un Centro de Administración, contratado.

Las actividades de recuperación son manejadas por el Equipo Técnico y Operacional de Recuperación, este equipo es el responsable de salvaguardar los recursos de TI y los datos y registros principales.

2.3.5.5.1 Si la recuperación es en el Sitio principal de la empresa, es decir, el sitio afectado.

En este caso la recuperación se puede dividir en cuatro partes: Preparación, Inspección y Evaluación, Salvatage y Restauración y Transportación.

Preparación

Se pueden seguir las siguientes actividades:

a. Asegurar todos los equipos que se ha solicitado y que han llegado al sitio del desastre, la empresa.
b. Asegurar al equipo de recuperación de TI.
c. Revisar detalladamente el reporte del problema.
d. Revisar la confiabilidad de los procesos y procedimientos.

Inspección y Evaluación

Se pueden seguir las siguientes actividades:

a. Inspeccionar el área de TI, como agua, gas, electricidad, etc.
b. Inspeccionar que no haya presencia de gases, químicos, cables sueltos, etc. para protección de recursos.
c. Inspeccionar los recursos y datos críticos, en caso de ser accesibles.
d. Evaluar el potencial de daños orientado a evitar deterioros mayores.
e. Determinar las opciones de protección de recursos.
f. Determinar el tiempo disponible para aplicar los procedimientos para prevenir deterioros mayores.
g. Elaborar de informe de resultados de esta fase.

Salvataje y Restauración

Se pueden seguir las siguientes actividades:

a. Adquirir protección especial para los recursos, tanto como sea necesario.
b. Ejecutar los procedimientos para evitar deterioros mayores, por ejemplo, controlar la humedad, la temperatura; con el fin de proteger los datos y registros críticos.
c. Si es necesario, colocar en otro piso o edificio los principales recursos, que contiene la información vital de la empresa.
d. Aplicar los procedimientos de restauración de recursos.
e. Elaborar de informe de resultados de esta fase.

Transportación

Se pueden seguir las siguientes actividades:

a. Determinar la ubicación a donde se transportará los recursos críticos.
b. Conseguir el transporte, tenerlo listo.
c. Transportar los recursos al sitio determinado, de acuerdo a los procedimientos predeterminados.

2.3.5.5.2 Si la recuperación es en el Establecimiento de recuperación alternativo para TI, sucursal de la empresa.

Las actividades en este caso se pueden dividir en tres partes: Preparación, Organización de Sistemas e Infraestructura, Restauración de Aplicaciones Críticas de TI.

Preparación

Se pueden seguir las siguientes actividades:

a. Asegurarse de que el personal de recuperación haya llegado al sitio alternativo.
b. Asegurarse de que todo el personal esté conciente del Requerimiento de tiempo de Recuperación, que se compone de: MTD’s, RTO’s, RPO’s y WRT’s.

c. Asegurarse de que todo el personal tenga disponible el listado de procedimientos para la recuperación.
d. Asegurarse de que todos los recursos estén disponibles en el sitio y revisar su confiabilidad y correcta configuración.
e. Recibir los dispositivos de backups y revisar su integridad.
f. Revisar la integridad de todos los recursos recibidos en el sitio alternativo, como: documentación, equipos, implementos de red, etc.

Organización de Sistemas e Infraestructura

Se pueden seguir las siguientes actividades:

a. Verificar que todos lo equipos necesarios estén completo y disponibles para su utilización.
b. Prender los equipos.
c. Instalar sistema operativo, parches y configurar cada máquina.
d. Revisar el entorno que rodea la infraestructura de red y de sistemas de TI.
e. Revisar el diagrama de red y verificar la correcta conexión de enlaces, servidores, routers, etc.
f. Asegurar que los equipos críticos como los servidores estén conectados a la red.
g. Revisar que los equipos de red estén correctamente configurados.
h. Correr los procesos de configuración y controladores.
i. Instalar las aplicaciones correspondientes en cada servidor.
j. Verificar el correcto funcionamiento de las aplicaciones necesarias.
k. Restaurar los datos de la red utilizando los backups.
l. Restaurar la seguridad de los sistemas, incluyendo firewall.
m. Redireccionar el enlace de la red hacia el sitio alternativo de recuperación.
n. Realizar pruebas de conectividad de la red.

Restauración de Aplicaciones Críticas soportadas por TI, para clientes.

Se puede seguir las siguientes actividades:

a. Verificar la conectividad de los equipos.
b. Revisar las prioridades de recuperación y los MTD’s que constan en el plan de continuidad.

c. Iniciar la restauración de cada sistema y sus aplicaciones de acuerdo a las prioridades de recuperación y a los procedimientos que se debe seguir.
d. Asegurarse de tener levantadas y disponibles las cuentas de usuario.
e. Asegurarse de que las claves de acceso están habilitadas correctamente.
f. Restaurar los sistemas operativos mediante imagen (Backup de cada máquina).
g. Configurar los sistemas operativos.
h. Restaurar las aplicaciones mediante los backups.
i. Verificar el correcto funcionamiento de las aplicaciones.

2.3.5.5.3 Si la recuperación es en un Centro de Administración, contratado.

Se puede seguir las siguientes actividades:

a. Asegurar que todos los miembros del equipo hayan llegado al centro de administración.
b. Revisar que los requerimientos, equipos y recursos estén acorde a las necesidades.
c. Asegurar la existencia y disponibilidad de energía eléctrica, comunicaciones, etc.
d. Inspeccionar los equipos recibidos en el centro de administración siguiendo un checklist para verificación de inventario.
e. Arreglar y asignar áreas de trabajo como escritorios a cada miembro según se requiera.
f. Proveer una laptop a cada miembro del equipo, donde estén almacenados archivos, presentaciones y anexos del plan de continuidad.
g. Instalar y configurar computadores de escritorio, impresoras y otros recursos en caso de ser necesario.

2.3.5.6 Normalización

El objetivo de esta fase es retornar a las condiciones que se estaba operando antes de ocurrir el desastre.

Esta fase consta de cuatro etapas: Determinación del Sitio, Reparaciones, Preparación y Transición.

Determinación del Sitio

Se pueden seguir las siguientes actividades:

a. Revisar la inspección y resultados de la evaluación preparada por el grupo de recuperación técnica y operacional en la fase de recuperación.
b. Determinar la viabilidad de retornar al sitio original de la empresa.
c. Analizar la posibilidad de trasladarse a un sitio menos costoso.

Reparaciones

Se pueden seguir las siguientes actividades:

a. Aprobar la reparación del sitio afectado por el desastre.
b. Contratar personal para reparar el sitio afectado.
c. Supervisar reparaciones.
d. Obtener los permisos gubernamentales requeridos para la reconstrucción del sitio afectado.
e. Revisar el inventario de equipos dañados para reemplazarlos y ordenar los equipos requeridos.
f. Recibir e inspeccionar los equipos solicitados a proveedores.
g. Instalar la energía eléctrica y cables de la red.
h. Instalar líneas telefónicas.
i. Instalar configurar y probar los computadores, impresoras, teléfonos, faxes, etc.
j. Suministrar implementos de oficina.

Preparación

Se pueden seguir las siguientes actividades:

a. Revisar el diagrama de red y verificar la correcta conexión de enlaces, servidores, routers, etc.
b. Instalar los sistemas.

c. Asegurar que los sistemas y aplicaciones críticas de TI estén conectados a la red de la empresa.
d. Revisar el correcto funcionamiento de la red y las configuraciones.
e. Correr los procesos de configuración de controladores.
f. Restaurar los datos de la red utilizando los backups.
g. Restaurar la seguridad de los sistemas, incluyendo firewall.

Transición

Se pueden seguir las siguientes actividades:

a. Determinar el marco de tiempo para la transición.
b. Notificar al equipo el cronograma de transición y asignar actividades.
c. Preparar un backup completo del sitio de recuperación alternativo.
d. Preparar los registros para el nuevo sitio o sitio original.
e. Transferencia del equipo del plan de continuidad, los backups y registros desde el sitio alternativo al sitio original.
f. Restaurar los sistemas de TI, aplicaciones y datos en el sitio original.
g. Verificar el correcto funcionamiento de la red y aplicaciones y la consistencia de los datos levantados, comparando los datos del sitio original contra los del sitio alternativo.
h. Redireccionar los enlaces de voz y datos al nuevo sitio o al sitio original.
i. Proveer de nuevos registros de usuario y contraseña a los usuarios.
j. Distribuir la información restablecida.
k. Registrar el funcionamiento normal de operaciones.
l. Iniciar procedimientos normales de obtención de backups.
m. Brindar asistencia técnica mediante help desk.
n. Concluir las operaciones en el sitio alternativo de recuperación, destruir o trasladar al sitio original los registros y documentos confidenciales que se han almacenado en el sitio alternativo. Concluir contratos de alquiler del sitio alternativo y realizar los pagos respectivos si es el caso.

2.3.6 ASIGNACIÓN DE ACTIVIDADES AL EQUIPO DEL PLAN DE CONTINUIDAD

En la Tabla 2.31 es un extracto del Anexo 22: Matriz Actividad-Responsable, donde se presenta una matriz de Actividades o asignadas a cada miembro del equipo del plan de continuidad, de acuerdo a su conocimiento y a sus funciones dentro del negocio.

Actividad / Responsable	IT Manager	IT Coordinator	Networking & End User Services Responsible Ec.	Networking & End User Services Responsible Col/Ec.	Analist & Report Responsible Ec.	Analist & Report Responsible Col/Ec.	Help Desk	Service Desk	10 Personas clave de la Empresa	Personal outsourcing
Recuperar el enlace de red interno (LAN)			x	x						x
Recuperar el enlace de red externo (WAN)			x	x						x
Recuperar Servidor DNS			x	x						x
Recuperar Servidor Exchange			x	x						x
Recuperar Servidor de Intranet							x			x
Recuperar Servidor de Archivos			x	x						x
Recuperar Servidor de Bases de Datos					x	x				x
Central Telefónica										x
SAP		x								
Microsoft Office Word								x		x
Microsoft Office Excel							x	x		x
Microsoft Office Power Point							x	x		x
Microsoft Office Outlook							x	x		x
Messenger Interno							x	x		x
Telefonía fija										x
Telefonía móvil										x
IXOS							x	x		x
Internet			x	x						x
Scanner							x	x		x
Impresoras							x	x		x
Copiadora							x	x		x
Videoconferencia							x	x		x

Fax							x	x		x
SISALEM							x	x		x
Workflow			x	x						x
IMS							x	x		x
Siebel					x	x				x
Net Meeting							x	x		x
Live Meetings							x	x		x
Teleconferencia							x	x		x
VPN – Redes							x	x		x
AutoCad							x	x		x
Clarify Prisma / Call Center							x	x		x
UPS			x	x						x
Track IT							x	x		x
VNC			x	x						x
Equipos de computación y componentes			x	x			x	x		x
Apoyar al equipo de recuperación	x	x							x	x
Actividades de Logística	x	x								x
Escalar Requerimientos	x	x	x	x	x	x	x	x	x	x
Toma de Decisiones	x	x								
Gestión financiera de recuperación	x	x								

Tabla 2.31 Matriz Actividad/Responsable

2.3.7 ANÁLISIS DE LA SITUACIÓN ACTUAL

Es importante para todos los miembros de la organización y en especial para los Gerentes y miembros de TI tener clara la información que se presenta a continuación, que es un extracto del Análisis de Impacto, Evaluación de Riesgos y Estrategias de Continuidad.

2.3.7.1 Procesos Críticos del Negocio

A continuación se presentan los procesos críticos del negocio y el tiempo máximo que pueden estar fuera de servicio con el fin de no afectar la actividad principal de la empresa:

Menos de 24 horas

Administración de Cuentas por Pagar y Cuentas por Cobrar – Finanzas

Legalización de productos en instituciones - Registro Sanitario
Generación de Órdenes de Venta - Ventas
Promocionar Productos – Marketing
Administración de los Call Center – Marketing
Importación de productos –Logística
Distribución de productos - Logistica
Administración de Cuentas por Pagar y Cuentas por Cobrar – Administración y Finanzas Diagnóstica.

Entre 25 y 48 horas
Visita Médica – Ventas
Promover Programas de Apoyo para Médicos y Pacientes – Marketing

Entre 73 horas y 5 días
Facturación - Finanzas
Supervisión de efectos adversos de medicamentos – Estudios Clínicos
Fijación de precios de productos – Registro Sanitario
Facturación - Administración y Finanzas Diagnóstica.
Administración de Bases de Datos de Clientes – Servicio Técnico Diagnóstica

Entre 16 y 30 días
Selección de Personal

2.3.7.2 Medidas de Reducción de Riesgos

Las medidas más adecuadas para reducir los riesgos con el fin de evitar desastres y que deberían tomar en cuenta los responsables del Departamento de TI son las siguientes, destacando que los riesgos analizados a continuación son los que mayor probabilidad de ocurrencia tienen.

Para reducir el riesgo de un Incendio

- Tener seguros contra incendios.

- Alarma de incendios y extintores.
- Protección del cuarto frío con material aislante.

Para reducir el riesgo de un Erupción Volcánica

- Tener seguros contra erupción volcánica.
- Ubicar el Departamento de TI en un piso alto del edificio.
- Estructura del edificio aislante al calor.

Para reducir el riesgo de una Interrupción de Energía eléctrica

- Contar con UPS
- Contar con un proveedor de energía eléctrica, adicional.
- Contar con una planta generadora de energía eléctrica, propia.

Para reducir el riesgo de un Daño del Disco Duro del Computador

- Evitar movilización frecuente y brusca de los equipos.
- Mantener sistemas de prevención: sistema de aire acondicionado, sistema de limpieza, etc.

Para reducir el riesgo de una Falla de los Servidores

- Evitar movilización frecuente y brusca de los equipos.
- Mantener sistemas de prevención: sistema de aire acondicionado, sistema de limpieza, etc.
- Proporcionar mantenimiento constante de hardware y software en los servidores.
- Contar con sistemas de arreglos de discos.

Para reducir el riesgo de un Virus en las Aplicaciones de Software

- Mantener políticas de seguridad.
- Contar con uno o más programas antivirus y actualizarlos constantemente.
- Mantener una estructura adecuada de los servidores, para entrada y salida de información de la empresa.

Para reducir el riesgo de Fallas del Aire Acondicionado (calentamiento de los equipos).

- Mantenimiento constante del sistema de aire acondicionado.
- Alarmas en caso de daños en el sistema de aire acondicionado.

Para reducir el riesgo de Fallas en el servicio de voz o comunicación de datos

- Mantenimiento constante de los enlaces de voz y datos
- Contar con estructuras/topologías adecuadas de acuerdo a lo requerido y a políticas de casa matriz.
- Controles de envío de paquetes: cantidad, tipo de paquetes, peso, frecuencia, etc.

Para reducir el riesgo de Fallas o daños en la red

- Mantenimiento constante de los enlaces de voz y datos
- Contar con estructuras/topologías adecuadas de acuerdo a lo requerido y a políticas de casa matriz.
- Controles de envío de paquetes: cantidad, tipo de paquetes, peso, frecuencia, etc.

Para reducir el riesgo de Hackers

- Mantener políticas de seguridad.
- Mantener una estructura adecuada de los servidores, para entrada y salida de información de la empresa.

Para reducir el riesgo de un Virus de Computadoras

- Mantener políticas de seguridad.
- Contar con uno o mas programas antivirus y actualizarlos constantemente.
- Mantener una estructura adecuada de los servidores, para entrada y salida de información de la empresa.

Para reducir el riesgo de un Robo

- Contar con seguridades en las puertas, sistemas de alarmas contra robos, etc.

- Contratar servicio de vigilancia en el edificio, y los pisos que ocupa la empresa.
- Contar con cámaras de vigilancia en el edificio, y los pisos que ocupa la empresa.

2.3.7.3 Estrategias de Recuperación

Las estrategias de recuperación que más se adaptan a la realidad actual de la empresa son las siguientes:

Opciones aplicables para Sitio Alternativo de Recuperación

- Sitio alternativo propio de la compañía o sucursal.
- Si se requiere recuperar dentro de la ciudad, un centro de administración contrado, sala de conferencias de un Hotel.

Opciones aplicables para Recuperación de Sistemas críticos TI

- Pre-Establecido: mantener copias e imágenes de los sistemas críticos de TI como backups en el sitio alternativo y adicionalmente como servicio contratado de almacenamiento donde un proveedor.
- Pre-Acordado: mantener acuerdos con proveedores de tal manera que una vez ocurrido el desastre, la persona responsable de TI de Roche notifique al proveedor y éste se comprometa a entregar los recursos solicitados en el tiempo acordado en los contratos.

Opciones aplicables para Recuperación de Enlaces de Voz y Datos

- Pre-Establecido: mantener disponibles equipos de red y rutas alternativas de enlaces como backups en el sitio alternativo y adicionalmente como servicio contratado de almacenamiento donde un proveedor.
- Pre-Acordado: mantener acuerdos con proveedores de tal manera que una vez ocurrido el desastre, la persona responsable de TI de Roche notifique al proveedor y éste se comprometa a proporcionar enlaces alternativos en el tiempo acordado en los contratos.

Opciones aplicables para Recuperación de Servidores

- Pre-Establecido: mantener copias e imágenes de los servidores como backups en el sitio alternativo y adicionalmente como servicio contratado de almacenamiento donde un proveedor.
- Pre-Acordado: mantener acuerdos con proveedores de tal manera que una vez ocurrido el desastre, la persona responsable de TI de Roche notifique al proveedor y éste se comprometa a entregar los servidores solicitados en el tiempo acordado en los contratos.
- Adicionalmente se sugiere obtener imágenes de respaldos de los servidores para optimizar el tiempo de recuperación.
- Se debe tener equipos de respaldo almacenados en Bodega listos para ser utilizados en caso de desastre y que contengan las aplicaciones necesarias para subir los respaldos solamente, además de cumplir con los estándares que exige casa matriz.

Opciones aplicables para Recuperación de Equipos Críticos y Recursos

- Pre-Establecido: mantener copias e imágenes de los equipos como backups y recursos en general en el sitio alternativo y adicionalmente como servicio contratado de almacenamiento donde un proveedor.

Opciones aplicables para Recuperación de Datos Críticos

Frecuencia de Obtención de Backups

- Diario
- Continuo

Tipos de Backups

- Completos
- Diferenciales

Métodos para Obtención de Backups

- Arreglo de Discos
- Cintas de Backups
- Replicación en sitio remoto

Opciones aplicables para Almacenamiento de Datos Críticos

Frecuencia de Almacenamiento de Backups en otro sitio

- Diario
- Semanal

Dispositivos de Almacenamiento

- Cintas Magnéticas
- Discos Duros

Salvamento y Métodos de Restauración

- Contratos Pre-Acordados con un proveedor para salvamento y restauración de operaciones.
- Contratos según se requiera para salvamento y restauración.

Establecimiento alternativo de almacenamiento

- Establecimiento comercial de almacenamiento de información y
- Establecimiento de almacenamiento remoto de información, propio de la compañía.

2.3.7.4 Asignación de Recursos para la Recuperación

Recurso	Cantidad
Servidores	6
Laptops	13
Equipos de Red e implementos	2 equipos adicionales por cada enlace
PC´s con Red	10
Teléfonos Celulares	23
Teléfonos Fijos	5
Memorias Flash (1Gb)	23
Impresoras	2
Copiadora	1
Fax	1

Tabla 2.32 Asignación de Recursos

Es recomendable tener un equipo de respaldo por cada uno de los servidores existentes, de tal manera que la recuperación sea óptima en el tiempo, y sobretodo es recomendable disponer de imágenes de respaldo de cada uno de los servidores de igual forma que se lo maneja con las estaciones de trabajo. Se requiere varios equipos de red adicionales tomando en cuenta que al ser un daño menor se puede reemplazar con piezas o armar la red mínima necesaria con los equipos de respaldo.

2.3.8 CONTROL DE CAMBIOS DEL BCP

El control de cambios se basa en los procesos, tecnología y personal. Los cambios deben ser sincronizados para asegurar la recuperación de información. Los cambios del plan deben ser controlados mediante procedimientos de tal manera que se mantenga íntegro. Se puede seguir el siguiente procedimiento para realizar un control de cambios adecuado:

1. Revisar el requerimiento de cambio, se debe definir un grupo e personas que realicen las revisiones al menos cada 2 meses.
2. Determinar la naturaleza del cambio, puede ser de procesos, tecnología, personas, etc.
3. Determinar las partes del pan que han sido afectadas por el nuevo cambio.
4. Identificar a las personas responsables de las áreas afectadas en el plan, quien debe realizar un nuevo documento donde se modifiquen los nuevos procedimientos a seguir o actualizar los datos correspondientes y sus anexos. Se debe versionar los documentos.
5. Revisar en la documentación del plan las dependencias, conflictos e inconsistencias.
6. Culminar la documentación con firmas y sellos de las personas autorizadas, en este caso estos cambios deberían ser aprobados por IT Manager Colombia/Ecuador y por IT Coordinator Ecuador.
7. Realizar pruebas de validez del plan, para verificar que los nuevos cambios apliquen a la situación actual.
8. Distribuir y difundir la nueva versión del plan de continuidad.

2.4 ETAPA DE GESTIÓN OPERATIVA

En la etapa de gestión operativa se analizan aspectos importantes tales como la difusión del plan de continuidad, el entrenamiento a los miembros de la empresa,

realizar una revisión del plan en caso de no haber tomado en cuenta ciertos factores y realizar pruebas sobre el plan.

2.4.1 DIFUSIÓN Y EDUCACIÓN

Una vez culminado el diseño del plan de continuidad, se lo debe difundir a todos los miembros del Departamento de TI, y a los miembros de la empresa, pues es necesario que todos presten su colaboración para que la empresa vuelva a operar normalmente y lo antes posible cuando ocurra un desastre.
Existen diferentes formas de difundir el plan de continuidad mediante las siguientes estrategias apoyadas con documentación apropiada y presentaciones ilustrativas:

- Charla de Concientización a los Gerentes mediante un análisis costo-beneficio.
- Charla de Concientización al personal de la Empresa para que se involucren y colaboren activamente en el plan de continuidad.
- Reuniones informativas
- Carteleras digitales informativas
- Talleres de simulación para probar el plan
- E-mails informativos
- Publicación del plan de continuidad en la Intranet
- Elaborar y publicar un e-learning

Cabe destacar que se debe dar una capacitación diferente a los miembros de TI, a las personas clave de la empresa y a los usuarios de la empresa; esto se debe a que existen varios niveles de participación de las personas de la empresa en el plan de continuidad.
El tipo de información que se debe difundir va de acuerdo al personal que va dirigido:

<u>Miembros de TI</u>

Para los miembros de TI más que una difusión del plan se requiere una capacitación, entrenamiento, simulacros y sobretodo que cada miembro del equipo esté al tanto de todos los procesos de recuperación. Cada miembro de TI debe conocer la ubicación de toda la documentación necesaria para implementar el plan en caso de desastre, los documentos de registro de procedimientos de configuración de la red, de levantamiento d backups, etc; y deben conocer los roles y actividades que debe cumplir cada uno de ellos.

Personal Clave de la Empresa

El personal clave de la empresa debe mantenerse al tanto de los procedimientos de recuperación ante un desastre ya que son partícipes activos del plan de continuidad, es el personal que debe informar constantemente a los miembros que conforman su área de trabajo debido a que el equipo del plan de continuidad será al personal clave a quienes informarán de los avances de la recuperación, el personal clave guiará al personal de su área mientras se restablecen las operaciones normales del Departamento de TI.

Usuarios de la Empresa

El equipo del plan de continuidad del negocio en conjunto con los miembros de TI debe difundir el plan de continuidad a todos los usuarios de la empresa dándoles a conocer los lineamientos generales del plan e informarles acerca de las actividades en las cuales pueden participar con el fin de realizar con eficacia y rapidez la recuperación colaborando con el equipo de recuperación.

De manera general a todos los miembros de la organización se debe difundir al menos la siguiente información:

1. Entorno del Plan de continuidad, ver Figura 2.8.

Figura 2.8 Elementos que incluyen el Plan de Continuidad

2. Objetivos y Alcance del Plan de Continuidad. Objetivos ver figura 2.9.

Figura 2.9 Objetivos del Plan de Continuidad

Alcance ver figura 2.10.

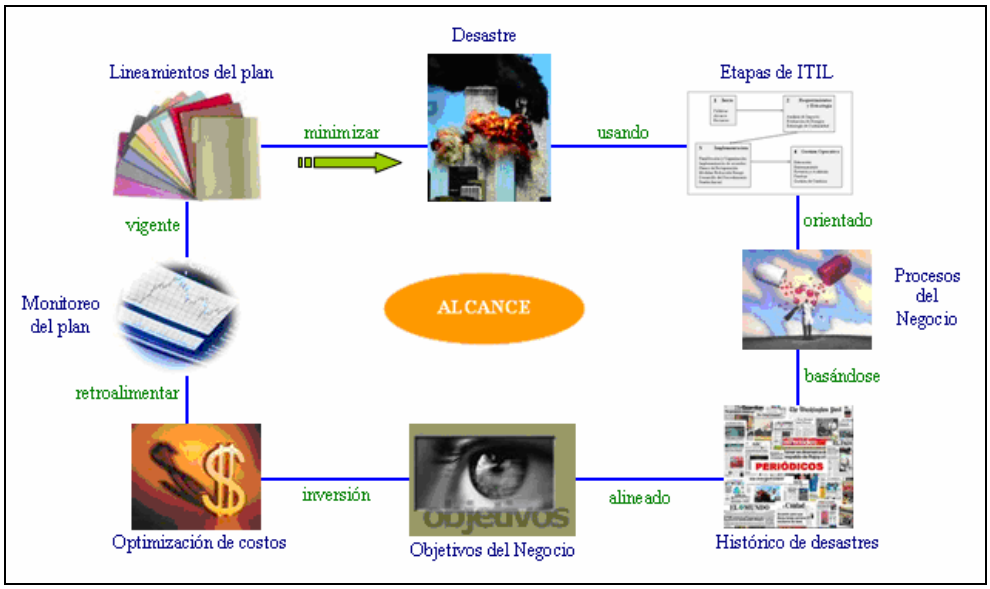

Figura 2.10 Alcance del Plan de Continuidad

3. Etapas de la Implementación del Plan de Continuidad, ver Figura 2.11.

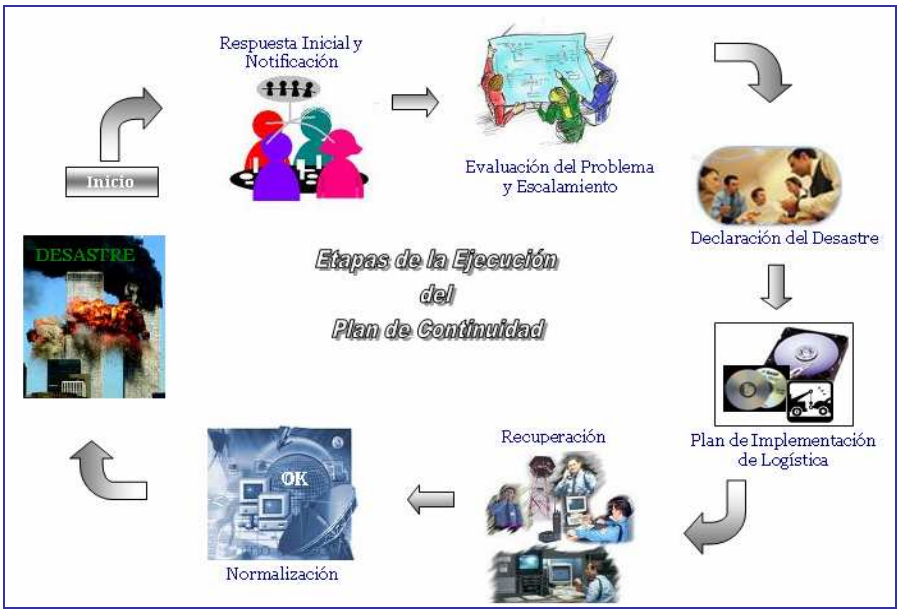

Figura 2.11 Etapas de Implementación del Plan de Continuidad

4. Resumen del Análisis de Impacto: ver sección 2.3.7.1: Procesos Críticos del Negocio.
5. Las Medidas de Reducción de Riesgos: ver sección 2.3.7.2: Medidas de Reducción de Riesgos.

6. Las Estrategias aplicables a la empresa: ver sección 2.3.7.3: Estrategias de Recuperación.
7. Explicación de pruebas y simulacros: se explica en la sección 2.4.3: Monitoreo y Mantenimiento del Plan de Continuidad.

2.4.2 REVISIÓN Y AUDITORÍA

Es necesario realizar las revisiones del plan de continuidad periódicamente con el fin de mantenerlo vigente y adecuado a las condiciones reales de la empresa. En muchas ocasiones el dinamismo del entorno en el que se encuentra la línea del negocio de la empresa obliga también al Departamento de TI a mantener sus servicios en constante cambio, por lo que es importante realizar revisiones al menos cada 2 meses.

Asegurar un plan de continuidad actualizado debe ser una de las prioridades para el Departamento de TI y difundir esta idea a todos los miembros de la organización especialmente a los Gerentes de Área, haciendo énfasis en que es importante para la organización invertir en un plan que asegure la continuidad de los procesos para que sigan operando sin interrupciones severas y evitando que el desastre produzca pérdidas financieras altas.

Se recomienda que se realicen auditorias periódicas realizadas por expertos con el fin de mantener la eficacia del plan y que ayuden al Departamento de TI mediante una visión global a identificar las falencias encontradas.

En las revisiones se pueden verificar los siguientes entregables:

- Objetivos y Alcance del plan de continuidad.
- Análisis de Impacto
- Evaluación de Riesgos
- Estrategias de Continuidad
- Decisiones de Recuperación
- Administración del Sitio Alternativo
- Medidas de Reducción de Riesgos
- Actividades del Plan a seguir

- Registro de Pruebas
- Recomendaciones de Auditoría.

Adicionalmente se recomienda verificar:

- Que los backups se estén almacenando fuera del sitio principal de la empresa.
- Que los backups obtenidos se puedan restaurar, es decir, que funciones correctamente.
- La documentación de configuración de la red y restauración de backups.
- Los contratos con los proveedores se encuentren vigentes y con todos los requerimientos necesarios.

2.4.3 MONITOREO Y MANTENIMIENTO DEL PLAN DEL CONTINUIDAD

Una vez finalizado el diseño del plan de continuidad es importante realizar pruebas con el fin de verificar la validez de sus procedimientos.

Se recomienda hacer los simulacros al menos cada 6 meses.

La prueba más eficaz para evaluar la efectividad del plan es un simulacro, donde se monte un escenario y se apliquen los procedimientos necesarios para la recuperación. En los simulacros se debe realizar lo siguiente:

1. Definir un escenario con determinadas condiciones.
2. Definir fecha y hora para realizar el simulacro, éste debe ser debidamente planificado.
3. Llegada la fecha y hora, iniciar las actividades del plan, y tomando decisiones de acuerdo a las condiciones predeterminadas.
4. Registrar los tiempos que se han tomado para la recuperación total del Departamento de TI.
5. Registrar todos los problemas e inconvenientes encontrados durante el proceso de recuperación.
6. Se deben medir parámetros de tiempo, costos y efectividad del plan, donde:
   a. Los parámetros de tiempo consisten en medir cuánto tiempo toma realizar cada actividad para la recuperación del desastre.

b. Los parámetros de costos consisten en cuantificar el dinero que se ha invertido en la recuperación.
c. Los parámetros de efectividad del plan ayudan a medir si éste se encuentra acorde a la realidad de la empresa, para esto se puede medir los siguientes indicadores: Tiempo de paralización de operaciones del negocio por el desastre, Tiempo de retrasos de trabajo, Porcentaje de usuarios afectados por el desastre, Número de procesos críticos afectados por el desastre, Esfuerzo invertido por los miembros de TI, Integridad de la información recuperada, Número de recursos de personal adicionales para la recuperación, MTD, RTO, WRT, RPO.

7. Una vez terminado el simulacro, realizar una reunión donde se discutan los problemas suscitados, los inconvenientes encontrados, falencias e inconsistencias del plan que no se adecúen a la realidad.
8. Realizar los cambios necesarios en el plan en caso de ser necesario, siguiendo los procedimientos de control de cambios del plan de continuidad.

Se sugiere también que se realicen auditorias por uno o varios expertos en Business Continuity Plan, para realizar la ser revisiones y sugerencias que sean necesarias, con el fin de mantener un plan eficaz de recuperación.

2.5 ROLES Y RESPONSABILIDADES

Se puede definir los siguientes roles en el proceso de recuperación ante un desastre: el equipo del plan de continuidad, los miembros de TI, los usuarios, los proveedores, personal temporal contratado (outsourcing).
Para cada uno de los roles se pueden definir varias responsabilidades de manera general:

2.5.1 EQUIPO DEL PLAN DE CONTINUIDAD

Las principales responsabilidades del equipo de continuidad son:

- Asegurar la recuperación de las actividades en el menor tiempo posible.

- Asegurar la restauración del sitio original afectado en el menor tiempo posible.
- Asegurar que los datos recuperados sean consistentes.
- Proteger los recursos asignados para la recuperación.
- Proporcionar los recursos de TI a las personas clave de cada función del negocio para continuar sus actividades si entre sus actividades incluyen procesos críticos del negocio.
- Registrar acuerdos con proveedores, pagos, negociaciones con las aseguradoras, adquisición de recursos, etc.
- Informar a los miembros de la empresa acerca de la situación de recuperación y sus avances.
- Tomar en cuenta dos aspectos: eficacia para la recuperación y optimización de costos de la recuperación.
- Verificar el correcto funcionamiento de los sistemas, aplicaciones, recursos y consistencia de datos una vez que se haya retornado a operaciones.
- Realizar simulacros y pruebas periódicamente del plan para mantenerlo vigente.

2.5.2 MIEMBROS DE TI

Generalmente la mayoría o la totalidad de los miembros de TI participan también como miembros del plan de continuidad, adicionalmente los miembros que no constan en el equipo del plan tienen las siguientes responsabilidades:

- Estudiar previamente el plan de continuidad para apoyar las actividades en caso de desastre.
- Colaborar activamente en la elaboración e implementación del plan cuando sea necesario.
- Ser mediadores entre el equipo del plan de continuidad y los miembros de la empresa y comunicar las necesidades de las partes.
- Colaborar en las actividades de recuperación del sitio original, como configuraciones, instalaciones, etc.
- Difundir el plan de continuidad mientras sea posible, con el fin de que los miembros de la empresa estén al tanto de estas actividades.

2.5.3 USUARIOS DE LA EMPRESA

Las principales responsabilidades de los usuarios de la empresa son:

- Colaborar en lo que sea posible en la recuperación del plan de continuidad.
- Informarse de la situación de recuperación y sus avances.
- Estudiar el plan de continuidad en caso de ser un usuario que realice actividades de un proceso crítico.
- Informar sus propias necesidades de TI a la persona clave del área a la que pertenece, para que sean transmitidos al equipo de recuperación.
- Tener en cuenta que el equipo del plan de continuidad se encargará de recuperar los recursos que soporta TI al negocio, mas no de la recuperación del negocio.

2.5.4 PROVEEDORES

Las principales responsabilidades de los proveedores son

- Cumplir con los acuerdos realizados previamente acerca de los equipos y tiempos de entrega.
- Proporcionar equipos de alta calidad que el personal de la empresa ha solicitado.
- Disponibilidad de suministrar equipos backup en caso de fallos de los equipos proporcionados.

2.5.5 PERSONAL TEMPORAL CONTRATADO (OUTSOURCING)

Las principales responsabilidades del personal contratado son:

- Informarse del rol y de las actividades que deben cumplir dentro del plan de continuidad.
- Prestar sus servicios con alta disponibilidad de colaboración en la implementación del plan.
- Compromiso de mantener la confidencialidad de la información que se le otorga, ya que son datos críticos y propios de la empresa.

2.6 BENEFICIOS Y POSIBLES PROBLEMAS

2.6.1 BENEFICIOS DE IMPLEMENTAR EL PLAN DE CONTINUIDAD

- Alinear los objetivos de TI con los objetivos del Negocio.
- Garantizar la continuidad de operaciones sin que el negocio se vea afectado significativamente por el desastre.
- Evitar pérdidas mayores en caso de ocurrir un desastre.
- Protección de la información ante un desastre, que es el activo intangible mas importante de una empresa.
- Lograr un equilibrio entre retardo de retorno a operaciones y costos de inversión, en un desastre.
- Reducir y mitigar los riesgos que puedan afectar al negocio.
- Reducir las pérdidas por interrupción de los procesos ante un desastre.
- Servicios de TI acorde con las necesidades del negocio con respecto al mercado y sus clientes.
- Evitar la pérdida de confianza de los clientes.
- Aseguramiento de los procedimientos de obtención de backups de manera periódica.
- Convenios preestablecidos con proveedores para entrega de recursos computacionales en tiempos acordados.
- Integrar estrategias, personal, procesos y tecnología.
- Mantener documentación actualizada de la empresa en caso de que las personas responsables de la información, no estén disponibles.
- Identificar las debilidades que tiene el Departamento de TI en los servicios que proporciona al negocio.
- Determinar posibles amenazas al negocio y al Departamento de TI.
- Permite conocer la situación actual de la empresa ante un desastre, mediante las pruebas del plan.
- Establece el plan de acción a corto, mediano y largo plazo, para darle continuidad al negocio.

2.6.2 POSIBLES PROBLEMAS AL IMPLEMENTAR EL PLAN DE CONTINUIDAD

- Falta de personal disponible para asumir responsabilidades para implementar el plan de continuidad en caso de desastre.
- Cumplimiento de procedimientos excesivamente burocráticos, como firmas de acuerdos entre el equipo del plan de continuidad y la gerencia o responsables de la empresa, alargando la gestión del plan de continuidad.
- Miembros del Departamento de TI o del equipo del plan de continuidad que no tengan el suficiente conocimiento de los procedimientos de servicio de TI.
- Si los objetivos del plan de continuidad no han sido bien definidos y difundidos entre todo el personal correspondiente.
- Plantearse objetivos del plan de continuidad poco realistas o inalcanzables, como tiempos de recuperación muy cortos.
- Plantearse beneficios a muy largo plazo, ya que se puede implementar varias fases del plan de continuidad, unas a corto plazo y otras a largo plazo.
- Si el Departamento de TI no está alineado con las necesidades del negocio, el plan de continuidad perdería su enfoque y objetividad.
- Si el plan de continuidad no se puede implementar correctamente si existen factores externos que lo impidan como por ejemplo un desastre que caotice la ciudad.
- Que tanto los miembros de TI como los usuarios de la empresa no estén concientes de la importancia que tiene el plan de continuidad para la empresa.

CAPÍTULO 3. EVALUACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO PROPUESTO

Para realizar la evaluación del plan de continuidad propuesto se registrarán los datos de un simulacro que ha sido planificado con los miembros del Departamento de TI de la empresa Roche Ecuador S.A. con el fin de identificar las falencias del plan y realizar una retroalimentación del mismo para lograr que sea efectivo ante cualquier tipo de desastre. Es conveniente realizar varios simulacros para poder abarcar de manera global la recuperación de desastres y superar los inconvenientes presentados en cada uno de ellos.

3.1 PARÁMETROS A EVALUAR

En el simulacro se evaluarán parámetros de tiempo y costos utilizando el plan y sin utilizarlo, para realizar una comparación y analizar los resultados que cada uno genera. Así mismo se evaluarán parámetros propios del plan para definir si es efectivo, a éstos parámetros se los denomina parámetros de efectividad del plan de continuidad.

3.1.1 PARÁMETROS DE TIEMPO

Los parámetros que se muestran a continuación se evaluarán en función del tiempo.

- Tiempo de obtención de un servidor con capacidades similares al servidor de archivos: tiempo que transcurre desde que se ha solicitado al proveedor un equipo o recurso hasta que es entregado.
- Tiempo de instalación y configuración del sistema operativo: Tiempo que transcurre desde que inicia hasta que finaliza la instalación del sistema operativo utilizado en Roche Ecuador S.A. para los servidores.
- Tiempo de Instalación y configuración de Impresoras: Tiempo que toma instalar un aproximado de 10 impresoras.
- Tiempo de Instalación y configuración de herramienta Legato Networker 7.2. (Solicitud a Roche Brasil): Tiempo que transcurre desde que se solicita la

instalación y configuración de la herramienta Legato a Brasil hasta que éste se lo ha realizado en el servidor de Ecuador.

- Tiempo para sacar al servidor de archivos anterior del dominio: Tiempo que trascurre mientras se deshabilita del dominio el servidor de archivos dañado.
- Tiempo para cambiar el nombre del Servidor para redireccionarlo: Tiempo que transcurre mientras se habilita el nuevo servidor de archivos en el dominio.
- Tiempo para reiniciar el servidor: Tiempo que se requiere para reiniciar al servidor para que reconozca la nueva configuración.
- Tiempo para cargar el backup: Tiempo que transcurre desde que inicia hasta que finaliza la obtención del backup, en un servidor determinado.
- Tiempo para validar los permisos de las carpetas y archivos: Tiempo que toma revisar los permisos de carpetas y archivos validado acceso según el perfil.
- Tiempo para verificar el buen funcionamiento del servicio: verificar que los datos estén completos y que sean confiables para su utilización.
- Total Tiempo de recuperación: Tiempo total que ha transcurrido desde el inicio hasta el final de la recuperación. Suma de los tiempos anteriores.

3.1.2 PARÁMETROS DE COSTOS

Los parámetros que se muestran a continuación se evaluarán en función de costos.

- Costo de un servidor con capacidades similares al servidor de archivos: Costo en dólares de un servidor de las mismas capacidades del servidor de archivos que ha sufrido el daño.
- Costo de un sistema de aire acondicionado temporal: costo en dólares de la medida de reducción del riesgo de forma temporal mientras reparan o adquieren un nuevo sistema de aire acondicionado.
- Costo de reparación del aire acondicionado afectado o adquisición de uno nuevo: costo en dólares de la mano de obra de reparación o adquisición del aire acondicionado definitivo.

- Costo de consultoría de Proveedores en caso de haber utilizado este servicio: costo de la evaluación y asesoría que realizan los proveedores en caso de daños que TI no pueda resolver.
- Total Costo de recuperación: el total de costo de recuperación en dólares. Suma de los costos anteriores.

3.1.3 PARÁMETROS DE EFECTIVIDAD DEL PLAN DE CONTINUIDAD.

Los parámetros de efectividad se muestran a continuación, de acuerdo a lo establecido en la sección 2.4.3: Monitoreo y Mantenimiento del Plan de Continuidad.

: .

- Tiempo de paralización de operaciones del negocio por el desastre: Tiempo que el desastre ha afectado al negocio manteniendo los servicios paralizados.
- Tiempo de retrasos de trabajo: Los retrasos de trabajo que han sufrido los usuarios a causa de la paralización de los servicios.
- Número de usuarios afectados por el desastre: Número de usuarios que se ven afectados por la paralización de servicios.
- Número de procesos críticos afectados por el desastre: Número de procesos críticos del negocio que se ven afectados por la paralización de servicios.
- Esfuerzo invertido por los miembros de TI: el esfuerzo medido en horas/hombre para la recuperación.
- Confiabilidad e Integridad de la información recuperada: porcentaje de la integridad de la información una vez recuperada, ayudan a medir los usuarios.
- Número de recursos de personal adicionales para la recuperación: número de personas que se necesitaron para la recuperación, adicionales a los miembros de TI.
- Maximum Tolerable Downtimes (MTD): El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio.
- RTO (Recovery Time Objective): Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción.

- WRT (Work Recovery Time): Indica el tiempo disponible para recuperar los datos perdidos, trabajo retrasado y datos capturados manualmente una vez que los sistemas o recursos son recuperados.
- RPO (Recovery Point Objective): Es la magnitud de los datos perdidos que pueden ser tolerados por un proceso del negocio en términos de un período de tiempo.

3.2 EVALUACIÓN

Para la evaluación se describen los escenarios que se proponen para la recuperación utilizando el plan propuesto y sin utilizarlo, con el objetivo de realizar una comparación efectiva y obtener recomendaciones importantes para mejorar la gestión de la continuidad del negocio en caso de desastres posteriores en el Departamento de TI de Roche Ecuador S.A.

Para realizar esta comparación se ejecuta el plan de continuidad para el caso de la caída del servidor de archivos, la implementación del plan para este simulacro se describe a continuación:

3.2.1 SUPOSICIONES

3.2.1.1 Antecedentes de la Ejecución del Plan de Continuidad

- Se asume que el simulacro se realizará sobre una caída del servidor de archivos.
- Se asume que el plan inicia un lunes a primera hora de la mañana.
- Se asume que se ha capacitado y entregado previamente el plan a todos los miembros del Departamento de TI, que son:
  - IT Coordinator
  - Networking & End User Services Responsible Ecuador
  - Analist & Report Responsible Ecuador

  - Help Desk
  - Service Desk
- Se asume que se ha notificado la fecha y hora del simulacro a todos los miembros de la empresa.

3.2.1.2 Caída del Servidor

- Se asume que ha ocurrido un daño en el sistema de aire acondicionado y por consiguiente quedó totalmente afectado el arreglo de discos del servidor de archivos, en este servidor también se encuentran instaladas las impresoras. Cabe destacar que los demás servidores resistieron el calentamiento y se encuentran en perfectas condiciones.
- Se asume que se perdió toda la información del servidor de archivos y que no se puede acceder al servidor.
- El backup de datos se almacena en las cintas todas las noches, el backup empieza a realizarse de manera automática y tiene una duración aproximada de 3 horas.
- Se asume que se utiliza una cinta de backup por día.

3.2.2 ESCENARIOS DEL SIMULACRO

Se realizará un simulacro de desastre el cual consiste en la caída del servidor de archivos que se ha originado por un calentamiento del equipo a causa del daño del sistema de aire acondicionado. Los servidores restantes no han sufrido daños y se encuentran operando de manera normal; el servidor de archivos ha sufrido un daño en el arreglo de discos por la alta temperatura. La falta de disponibilidad del servidor de archivos ha causado la pérdida de información alojada en el servidor, sin embargo se asume que el desastre ocurrió un lunes en la madrugada y que tiene disponibles las cintas con los backups obtenidos automáticamente del día viernes y que almacenaron en la caja fuerte del Departamento de TI y otra copia se transportó a donde el proveedor contratado para almacenamiento de backups, de acuerdo a las políticas manejadas por el Departamento de TI. Cabe

destacar que todas las opciones de recuperación están basadas en los documentos de procedimientos donde constan datos como:

- Configuraciones de los servidores, sistemas, bases de datos, conexiones de redes, etc.
- Descripción del funcionamiento de los procesos que dependen de TI y los propios.
- Políticas para manejo de los procedimientos.

A continuación se describen las acciones generales que se realizarán para el levantamiento del servicio afectado por el desastre, en el escenario donde se utiliza el plan y en el escenario donde se realiza la recuperación sin implementar ningún plan.

3.2.2.1 Escenario Sin Plan de Continuidad

Se realizan las siguientes acciones en caso de no implementar ningún plan de continuidad:

1. Obtener un servidor con capacidades similares al servidor de archivos actual que ha sufrido el daño, es decir, solicitar al proveedor un equipo.
2. Recibir el equipo solicitado.
3. Configurar equipo:
   a. Instalar y configurar el sistema operativo.
   b. Instalar y configurar Aplicaciones e Impresoras.
   c. Gestionar la instalación y configuración de la herramienta para subir el backup: Legato Networker 7.2.
4. Recuperar las cintas correspondientes al último backup obtenido:
   a. Revisar las cintas de backup en la caja fuerte del Departamento de TI.
5. Preparar la Herramienta Legato Networker para cargar el backup de archivos.
6. Renombrar al Servidor nuevo:
   a. Cambiar el nombre del Servidor nuevo para redireccionarlo.
   b. Cambiar dirección IP al servidor nuevo.
   c. Reiniciar el servidor.

7. Cargar el backup.
8. Revisar permisos de los usuarios sobre las carpetas en base a los registros de perfil de cada usuario y departamento de la empresa.
9. Tiempo para verificar el buen funcionamiento del servicio.

3.2.2.2 Escenario Con Plan de Continuidad

Se realizan las siguientes acciones en caso de implementar el plan de continuidad propuesto:

1. Recuperar las cintas correspondientes al último backup obtenido:
   a. Revisar las cintas de backup en la caja fuerte del Departamento de TI.
2. Preparar la Herramienta Legato Networker para cargar el backup de archivos.
3. Renombrar al Servidor nuevo:
   a. Cambiar el nombre del Servidor nuevo para redireccionarlo.
   b. Cambiar dirección IP al servidor nuevo.
   c. Reiniciar el servidor.
4. Cargar el backup.
5. Revisar permisos de los usuarios sobre las carpetas en base a los registros de perfil de cada usuario y departamento de la empresa.
6. Tiempo para verificar el buen funcionamiento del servicio.

3.2.3 EJECUCIÓN DEL PLAN DE CONTINUIDAD

Utilizar el Check List con las actividades generales que se deben seguir en caso de desastre, ver Anexo 1 del Plan de Continuidad del Negocio para el Departamento de TI de Roche Ecuador S.A.: Check List del Plan de Continuidad del Negocio aplicado al simulacro, el check list representa un documento de apoyo para las personas encargadas de la recuperación ya que ayudará a recordar los lineamientos a seguir, sin omitir tarea alguna para poder reestablecer los servicios de manera rápida y sobretodo para ir registrando los avances de la recuperación, de tal forma que al final se haga un recuento que sirva para retroalimentar al plan para evitar desastres mayores.

Cabe destacar que el check list está basado en las actividades del plan de continuidad.

A continuación se detallarán los pasos a seguir en cada fase del plan de continuidad.

3.2.3.1 ETAPA 1: RESPUESTA INICIAL Y NOTIFICACIÓN

En esta etapa se registra la siguiente información:

1. Registrar la/las personas que notaron el desastre.

Identificar a la persona que se dio cuenta de la ocurrencia del desastre, fecha y hora.

Es este caso se dio cuenta del desastre el Networking & End User Services Responsible a las 8:H00 del día lunes y él notificó lo ocurrido a IT Coordinator.

2. Definir el lugar de reunión del equipo de continuidad.

Debido a que el desastre no es grave se define que el lugar de reunión es en el quinto piso de la matriz de la empresa en el mismo Departamento de TI por lo que si es accesible.

IT Coordinator Networking & En User Services Responsible hacen un análisis breve y general del desastre.

Se define cual fue el desastre: El servidor de archivos no funciona correctamente, sin embargo, se ha determinado que el grado de severidad del impacto es bajo, tomando en cuenta que según los valores predefinidos en la evaluación del impacto financiero que costa en el BIA, un desastre se puede catalogar como: no hay pérdidas, impacto bajo, impacto medio o impacto alto, en función de las pérdidas financieras por día de ganancias por concepto de ventas y tomando en cuenta que la base de tiempo estimado para recuperar un servidor de archivos es 72 horas; El impacto bajo se encuentra dentro del rango de pérdidas financieras de 1 a 4 días.

3. Cada miembro del equipo recibe la alerta de desastre, utilizando el árbol de contactos.

En este punto es necesario también definir si es necesario o no convocar a los demás miembros del plan de continuidad.

Por lo tanto no es necesario convocar a más miembros para ejecutar el plan de continuidad dado que los miembros del Departamento de TI pueden resolver el problema. Por consiguiente, para la recuperación, el equipo del plan de continuidad del negocio está conformado por:

1. IT Coordinator Ecuador
2. Networking & End User Services Responsible Ecuador
3. Analist & Report Responsible Ecuador
4. Help Desk
5. Service Desk

Se convoca a los demás miembros del Departamento de TI, utilizando los datos que deberían tener registrados en la plantilla del Anexo 15: Datos personales de los Miembros del Plan de Continuidad del Negocio y del árbol de llamadas que deben realizar los miembros, el árbol de llamadas se encuentra en la Figura 2.6: Estructura Jerárquica de Llamadas Telefónicas, dentro de la Etapa de Implementación del Plan de Continuidad del Negocio.

Nota: En este proyecto de titulación no se publican los datos personales de los miembros de la empresa ni de sus proveedores ya que representa información reservada de la misma.

4. Convocar a proveedores o personal externo para asesoramiento, en caso de ser necesario.

De acuerdo al desastre ocurrido y a los daños que ha causado, se evalúa la posibilidad de llamar a los proveedores en el caso de que los propios miembros de TI no puedan resolver el problema.

En este caso, se convoca al proveedor del Aire Acondicionado para la respectiva revisión y reparación, donde se deberá aplicar la garantía del recurso dañado ya que para este tipo de equipos se tiene convenios de mantenimiento constante y dependiendo del tipo de equipo se los debe tener asegurados. En el Anexo 16:

Datos de Proveedores, se encuentra una plantilla donde se puede llenar los datos de personales de los proveedores del Departamento de TI, con el fin de tener disponible la información y ubicarles en caso de que sea necesario.

5. Acceder a la documentación del plan de continuidad del negocio.

El plan de continuidad se encuentra disponible en:

a. La red: Servidor de Archivos
b. Enlace mediante la Intranet
c. En la máquina local de cada usuario.
d. En la flash memory personal de cada miembro de la empresa, especialmente de los miembros de TI.
e. Documentación impresa (dentro y/fuera de la empresa).
f. Email corporativo y personal de los miembros de la empresa.

Obtener el plan de continuidad de la ubicación que sea más sencilla acceder.

6. Determinar si el establecimiento es accesible.

Se debe definir, de acuerdo al desastre, si el edificio es accesible si hasta esta etapa no se han podido obtener los datos anteriores del desastre. Se debe determinar si el desastre es repetitivo, como por ejemplo cuando ocurre un terremoto puede haber replicación, de manera que pueda continuar afectando a los recursos del Departamento de TI.
En este caso el edificio de la matriz de la empresa se encuentra en perfectas condiciones. El desastre, si es que no se controla, puede seguir afectando a los recursos de TI por el aumento de temperatura.

7. Determinar hora y condiciones del desastre.

Si el desastre ocurre en horas no laborables, trasladarse al establecimiento de manera inmediata.

En este caso se percataron del desastre el lunes a las 8:H00 cuando empezaron su jornada laboral.

8. Evaluación preliminar de los daños, Evaluación preliminar de las causas de los daños.

De forma general y para cualquier tipo de desastre, los miembros del Departamento de TI deben realizar las siguientes actividades:

a) Realizar una inspección general del desastre:
   a. Dirigirse al cuarto frío para revisar los servidores.
   b. Verificar que todos los servidores estén prendidos.
   c. Revisar el correcto funcionamiento de sistema operativo y aplicaciones de los servidores.
   d. Revisar el log de cada uno de los servidores.
   e. Revisar los logs de la obtención del último backup que debía realizarse de forma automática.
   f. Revisar que en las cintas se haya cargado correctamente el backup de datos.
   g. Verificar que las computadoras de los usuarios tengan acceso a todas las herramientas que usan a diario y que la información esté disponible.
b) Buscar pistas que puedan ayudar a definir la causa del desastre.
   a. Verificar si hay algún tipo de amenaza natural, tecnológica o humana.
   b. Revisar de forma general las conexiones eléctricas, fugas de agua o gas, etc.
   c. Asegurar que la amenaza no siga afectando los recursos del Departamento de TI, tal que pueda seguir afectándolo.
c) Asegurar los recursos del Departamento de TI.
   d. Verificar que la amenaza no siga produciendo daños en los recursos del Departamento de TI.

9. Preparar un reporte preliminar del desastre y sus problemas.

Para tener una idea totalmente clara del desastre y sus causas, se debe completar la primera etapa de implementación del plan de continuidad del negocio: Respuesta Inicial y Notificación, constituyendo este documento el Informe Preliminar de Falla.

10. Notificar a los miembros del plan de recuperación.

Inmediatamente elaborado el informe preliminar de la falla, IT Coordinator Ecuador debe comunicar el inconveniente a todos los miembros del Departamento de TI, para que de manera inmediata cada uno de ellos empiecen a realizar sus funciones de acuerdo a los roles del plan de continuidad.

Revisar sección 2.5 de Roles y responsabilidades generales en la Etapa de Gestión Operativa del Plan de Continuidad del Negocio y actividades específicas en la Etapa de Implementación.

Para este caso los roles y responsabilidades son:

a) IT Coordinator Ecuador

- Notificar a las personas clave de la empresa acerca del daño ocurrido.
- Coordinar actividades de administración de la continuidad del negocio.

- Analizar si los archivos no disponibles afectan a la operación de SAP.

b) Networking & End User Services Responsible Ecuador

- Coordinar la recuperación del servidor.
- Coordinar la restauración de los backups.
- Monitorear el proceso de recuperación del servidor.

c) Analist & Report Responsible Ecuador

- Analizar si los archivos no disponibles afectan a la operación de aplicaciones que involucren Reportes o Bases de Datos como Siebel.
- Apoyar a Networking & End User Services Responsible Ecuador en las actividades de recuperación.

d) Help Desk

- Comunicarse con Proveedores en caso de ser necesario.
- Encargarse de coordinar la transportación del backup desde la Bodega hasta la matriz de la empresa.

e) Service Desk

- Soporte a usuarios mientras se normalizan operaciones para minimizar el impacto del desastre.
- Apoyar a a Networking & End User Services Responsible Ecuador y a Analist & Report Responsible Ecuador en sus actividades.

3.2.3.2 ETAPA 2: EVALUACIÓN DEL PROBLEMA Y ESCALAMIENTO

La etapa 2 consiste en dos partes, la primera es determinar la magnitud del problema basado en el reporte preliminar, la segunda parte consiste en decidir si se pasa o no de manera inmediata a la siguiente fase.

Las actividades a seguir para esta etapa son:

1. Recepción del reporte preliminar del problema.

Esta fase aplica en el caso de contar con un equipo numeroso de continuidad del negocio, cuando un equipo transfiere a otro equipo el siguiente paso del proceso de recuperación.

Sin embargo como el área afectada es la de infraestructura y redes, el encargado de los procedimientos de recuperación del servidor es Networking & End User Services Responsible, pasa el check list a Help desk para que continúe con la documentación, as dos personas deben trabajar en conjunto.

2. Evaluar la interrupción de los procesos y el daño en los equipos y recursos.

Determinar los procesos que fueron afectados, las áreas de TI que fueron afectadas, los equipos que fueron afectados así como los recursos en general, los sistemas e infraestructura de red. Estos datos debe ser registrados en el Anexo 17-A: Análisis de Impacto en el Negocio.

3. Estimar las pérdidas financieras, para esto se puede utilizar una lista de chequeo de recursos, elaborada previamente.

Se deben evaluar las pérdidas financieras que se dieron por el desastre ocurrido, estos datos se debe registrar en el Anexo 18-A: Evaluación de Pérdidas Financieras.

4. Estimar el impacto del desastre basado en los registros del plan, catalogando al desastre como bajo, medio, alto o crítico.

De cuerdo al análisis realizado en el Informe preliminar de Falla se cataloga al desastre como nivel medio, debido a que por un lado se ve afectada la información personal de cada usuario, lo que produce retrasos de trabajo a la empresa. Por otro lado la información es recuperable, en caso de que la información se hubiese perdido totalmente se catalogaría al desastre como crítico.

5. Determinar si se debe continuar o no a la siguiente fase.

Si este desastre no impacta a lo procesos críticos se debe continuar el monitoreo de la situación, de lo contrario continuar a la siguiente fase de ejecución del plan de continuidad.

Al ser un desastre que afecta procesos críticos, de acuerdo al Informe de Análisis de Impacto, se debe continuar con la siguiente fase del plan.

El informe detallado del problema debe proveer la siguiente información.

1. Nivel del desastre.

Nivel de desastre

2. Estimación de pérdidas financieras.

Total Pérdidas

3. El origen del daño, es decir, la amenaza.

Origen del daño

4. La magnitud del daño, especificando:
    a. Áreas de TI afectadas por el desastre.
    b. Los sistemas e infraestructura de TI afectados.
    c. Cuántos y cuales procesos críticos fueron afectados.

El informe detallado del problema consiste realizar la especificación y justificación del Informe Preliminar de Falla una vez terminada la recuperación, por lo que representan datos certeros más no los estimados inicialmente.

1. Condiciones físicas del Departamento de TI.

Evaluar en qué estado se encuentra el Departamento de TI.

Para este caso el Departamento tiene condiciones óptimas.

2. Presencia de factores contaminantes como gases.

Detectar presencia de gases tóxicos y otros que puedan contaminar a las personas.

En este caso no existen factores contaminantes.

3. Riesgos que implica el desastre.

Evaluar si el desastre continúa provocando riesgos para personas y recursos de TI.

Para este caso:

Riesgos Tecnológicos: puede seguir afectando a los demás servidores.

Riesgos Humanos: ninguno.

Llenar Anexo 19-A: Evaluación de Riesgos

4. Estimación del tiempo de recuperación.

Para recuperar el servidor de archivos se requiere aproximadamente 1 día laborable, 8 horas, utilizando el plan de continuidad propuesto.

3.2.3.3 ETAPA 3: DECLARACIÓN DEL DESASTRE

La decisión de declarar un desastre está basada en el informe de la evaluación detallada del problema. Se puede seguir las siguientes actividades:

1. Revisar las opciones de recuperación disponibles en la sección 2.2.3 de la estrategia de continuidad del negocio.

Llenar Anexo 20-A: Estrategias de Recuperación.doc

2. Decidir la mejor opción de recuperación para la situación actual.

De acuerdo a los costos presentados en el Informe de Evaluación de Pérdidas Financieras y procurando el menor tiempo posible.

3. Preparar la declaración de desastre, que deberá contener lo siguiente:
   a. Anuncio oficial del desastre.
   b. Fecha y Hora del desastre.
   c. Categorizar el desastre en niveles entre bajo, medio o alto.
   d. Seleccionar las opciones de recuperación.
   e. Informe de la situación de recuperación.
   f. Estimación del tiempo de recuperación.
   g. Nombre de la autoridad que declara el desastre.
   h. Notificar y declarar el desastre a toda la organización.

Utilizar y llenar el Anexo 21: Declaración de Desastre

3.2.3.4 ETAPA 4: PLAN DE IMPLEMENTACIÓN DE LOGÍSTICA

En esta etapa se prepara el entorno para que el establecimiento de recuperación tenga todos los recursos necesarios para empezar la recuperación y la normalización de operaciones. Para lo cual se tiene las siguientes actividades:

1. Ordenar o adquirir hardware y software, en caso de ser necesario.

Solicitar a los proveedores los recursos que requieren ser reemplazados.
Para este caso: No Aplica

2. Ordenar o adquirir equipos de voz y datos, en caso de ser necesario.

Solicitar a los proveedores los recursos que requieren ser reemplazados.
Para este caso: No Aplica

3. Ordenar o adquirir impresoras, faxes y copiadoras, en caso de ser necesario.

Solicitar a los proveedores los recursos que requieren ser reemplazados.
Para este caso: Gestionar la adquisición de un sistema de aire acondicionado temporal de manera urgente.

4. Ordenar o adquirir cintas magnéticas y discos duros, en caso de ser necesario.

Solicitar a los proveedores los recursos que requieren ser reemplazados.
Para este caso: No Aplica

5. Obtener formularios necesarios para continuar con los procesos manualmente.

En caso de que los procesas puedan seguir operando manualmente, se debe obtener formularios ya realizado previamente de acuerdo a los procedimientos de TI y continuar con los procesos.
En este caso se requiere formularios para registrar los problemas de help desk.

6. Evaluar si es necesario trasladarse a un sitio alternativo para la recuperación.

En este caso no es necesario trasladarse a otro sitio debido a que en general el Departamento de TI se encuentra en óptimas condiciones para seguir operando y administrando la crisis desde el lugar.

7. Enviar los documentos claves al sitio alternativo incluyendo el plan de continuidad del negocio.

En este caso:No Aplica

8. Recibir los equipos y recursos en el sitio alternativo.

En este caso:No Aplica

9. Preparar todo el sitio de manera rápida para iniciar la administración de la recuperación.

Se debe preparar que esté listo y disponible el personal, las instalaciones estén adecuadas, las conexiones, hardware, software, recursos generales, documentación.

En este caso:No Aplica

3.2.3.5 ETAPA 5: RECUPERACIÓN

3.2.3.5.1 Si la recuperación es en el Sitio principal de la empresa, es decir, el sitio afectado.

En este caso la recuperación se puede dividir en cuatro partes: Preparación, Inspección y Evaluación, Salvataje y Restauración y Transportación.

- **Preparación**

Se puede seguir las siguientes actividades:

1. Asegurar todos los equipos que se ha solicitado y que han llegado al sitio del desastre, la empresa.

Verificar que todo esté funcionando correctamente.

En este caso: No aplica

2. Asegurar al equipo de recuperación de TI.

Verificar que tanto el hardware y software de la empresa estén listos para la recuperación. Revisar gases tóxicos, cables sueltos, fugas, desastre repetitivo, etc.

- **Inspección y Evaluación**

Se puede seguir las siguientes actividades:

1. Inspeccionar el área de TI, como agua, gas, electricidad, etc.

En este caso: No existen riesgos para el personal, solamente riesgos tecnológicos de calentamiento de los servidores mientras se repare el sistema de aire acondicionado.

2. Inspeccionar que no haya presencia de gases, químicos, cables sueltos, etc. para protección de recursos.

En este caso: Gestionar la reparación del aire acondicionado y utilizar el aire acondicionado temporal.

3. Inspeccionar los recursos y datos críticos, en caso de ser accesibles.

Asegurarse de que los demás servidores estén funcionando correctamente tomando en cuenta las siguientes actividades para monitoreo:

a. Dirigirse al cuarto de servidores para revisar los servidores.
b. Verificar que todos los servidores estén prendidos.
c. Revisar el correcto funcionamiento de sistema operativo y aplicaciones de los servidores.
d. Revisar el log de cada uno de los servidores.
e. Verificar que las computadoras de los usuarios tengan acceso a todas las herramientas que están vinculadas a los demás servidores.
f. Determinar las opciones de protección de recursos.

En este caso:

a. Contratar un sistema de aire acondicionado temporal.
b. Obtener ventiladores de manera inmediata.
c. Gestionar la reparación del aire acondicionado actual.
d. Aplicar contratos pre-acordados con proveedores para entrega de recursos.

4. Determinar el tiempo disponible para aplicar los procedimientos para prevenir deterioros mayores.

En cualquiera de las opciones elegidas debería ser un tiempo no mayor a 1 hora, mientras se deben apagar los servidores.

- **Salvataje y Restauración**

Se puede seguir las siguientes actividades:

1. Adquirir protección especial para los recursos, tanto como sea necesario.

En este caso: Se tiene disponible al menos una opción para contrarrestar la temperatura del cuarto de servidores.

2. Ejecutar los procedimientos para evitar deterioros mayores, por ejemplo, controlar la humedad, la temperatura; con el fin de proteger los datos y registros críticos.

En este caso:

   a. Gestionar la logística de recepción de equipos y personal de reparación.
   b. Implantar los equipos de aire acondicionado, con la ayuda de proveedores.
   c. Prender los servidores.

3. Si es necesario, colocar en otro piso o edificio los principales recursos, que contiene la información vital de la empresa.

En este caso: No es necesario movilizar los equipos.

4. Aplicar los procedimientos de restauración de recursos.

En este caso:

1. Recuperar las cintas correspondientes al último backup obtenido:
   a. Revisar las cintas de backup en la caja fuerte del Departamento de TI, o
   b. Trasladar las cintas de backup desde donde el proveedor hasta el Departamento de TI.
2. Preparar la Herramienta Legato Networker para cargar el backup de archivos.
3. Cargar el backup.
4. Renombrar al Servidor nuevo:
   a. Cambiar el nombre del Servidor nuevo para redireccionarlo.
   b. Cambiar dirección IP al servidor nuevo.
   c. Reiniciar el servidor.
5. Revisar permisos de los usuarios sobre las carpetas en base a los registros de perfil de cada usuario y departamento de la empresa.

- **Transportación**

Se puede seguir las siguientes actividades:

1. Determinar la ubicación a donde se transportará los recursos críticos.

En este caso: No Aplica

2. Conseguir el transporte, tenerlo listo.

En este caso: No Aplica

3. Transportar los recursos al sitio determinado, de acuerdo a los procedimientos predeterminados.

En este caso: No Aplica

3.2.3.6 ETAPA 6: NORMALIZACIÓN

El objetivo de esta fase es retornar a las condiciones que se estaba operando antes de ocurrir el desastre.

Esta fase consta de cuatro etapas: Determinación del Sitio, Reparaciones, Preparación y Transición.

- **Determinación del Sitio**

No es necesario determinar el sitio en este caso dado que se está administrando la recuperación en el Departamento de TI en la matriz.

- **Reparaciones**

Se pueden seguir las siguientes actividades:

a. Contratar personal para reparar el sitio afectado.

En este caso: Si la opción que se ha elegido es diferente a gestionar la reparación del aire acondicionado, empezar a realizarla en esta fase.

b. Supervisar reparaciones.

En este caso: Help desk es la persona encargada de la supervisión de esta reparación.

c. Obtener los permisos gubernamentales requeridos para la reconstrucción del sitio afectado.

En este caso: No aplica

d. Revisar el inventario de equipos dañados para reemplazarlos y ordenar los equipos requeridos.

En este caso: Un servidor con similares características al servidor de archivos que sufrió el daño.

e. Recibir e inspeccionar los equipos solicitados a proveedores.

En este caso: El encargado de revisar el estado de los equipos solicitados es Networking & End User Services Responsible Ecuador.

f. Instalar configurar y probar los computadores, impresoras, teléfonos, faxes, etc.

En este caso:

a. Verificar que la información sea accesible para todos los usuarios.
b. Verificar el buen funcionamiento del servicio de impresiones.
c. Brindar el soporte necesario a los usuarios y gestionar cualquier inconveniente.

g. Suministrar implementos de oficina.

En este caso: No aplica

- **Preparación**

Se pueden seguir las siguientes actividades:

a. Revisar el diagrama de red y verificar la correcta conexión de enlaces, servidores, routers, etc.

Verificar el correcto funcionamiento de los servicios que presta TI al negocio.

b. Instalar los sistemas.

En este caso: No aplica

c. Asegurar que los sistemas y aplicaciones críticas de TI estén conectados a la red de la empresa.

Verificar el correcto funcionamiento de software en general.

d. Revisar el correcto funcionamiento de la red y las configuraciones.

Verificar el correcto funcionamiento de las conexiones de red.

e. Correr los procesos de configuración de controladores.

En este caso: No aplica

f. Restaurar los datos de la red utilizando los backups.

Preparar los recursos necesarios para la migración de los datos al equipo nuevo adquirido para el retorno a operaciones normales.

g. Restaurar la seguridad de los sistemas, incluyendo firewall.

Verificar permisos de usuarios para los archivos restaurados.

- **Transición**

Se pueden seguir las siguientes actividades:

a. Determinar el marco de tiempo para la transición.

Retornar a operaciones normales una vez que se tenga disponible el equipo, esto incluye sistema operativo y aplicaciones instaladas y realizadas todas las configuraciones necesarias; tomaría un lapso de aproximadamente 8 horas, las cuales pueden ser totalmente transparentes al usuario dado que incluso se puede realizar la migración al servidor nuevo en la noche.

b. Notificar al equipo el cronograma de transición y asignar actividades.

Los roles y responsabilidades son los mismos que al momento de la recuperación debido a que las actividades fueron asignadas acorde con los conocimientos y funciones que desempeñan dentro de la empresa cada uno de ellos.

c. Preparar un backup completo del sitio de recuperación alternativo.

Una vez que se ha cargado el backup de las cintas en el servidor alternativo, se debe obtener un backup con el fin de tener seguridad de los datos.

En este caso: No Aplica

d. Preparar los registros para el nuevo sitio o sitio original.
    a. Registrar los cambios que se han realizado con respecto a configuraciones y utilización de equipos.
    b. Asegurar que quede actualizada la configuración vigente.

En este caso: No Aplica

e. Transferencia del equipo del plan de continuidad, los backups y registros desde el sitio alternativo al sitio original.

En este caso: No Aplica

f. Restaurar los sistemas de TI, aplicaciones y datos en el sitio original.

En este caso: No Aplica

g. Verificar el correcto funcionamiento de la red y aplicaciones y la consistencia de los datos levantados, comparando los datos del sitio original contra los del sitio alternativo.

Esta actividad es gestionad por Help desk y Service desk.

h. Redireccionar los enlaces de voz y datos al nuevo sitio o al sitio original.

Configuraciones del servidor, las mismas que se realizaron al momento de la recuperación.

i. Proveer de nuevos registros de usuario y contraseña a los usuarios.

Actualizar o crear los permisos de usuarios en caso de que se hayan perdido.

j. Distribuir la información restablecida.

IT Coordinator debe notificar el retorno a operaciones normales.

k. Registrar el funcionamiento normal de operaciones.

Documentar el procedimiento realizado. Las actividades que se realizaron en la etapa de normalización. Utilizar los datos de la etapa de normalización del check list del plan de continuidad del negocio.

l. Iniciar procedimientos normales de obtención de backups.

Preparar la herramienta para obtener los backups de forma normal y automáticamente, como antes del desastre.

m. Brindar asistencia técnica mediante help desk.

Durante la recuperación y retorno a operaciones normales el área de Soporte a usuarios deben atender los requerimientos de los usuarios y registrando los problemas que se presenten.

En este caso:

a. Retrasos de trabajo en los usuarios por la necesidad de consultar archivos personales.
b. Configurar impresoras en cada máquina.
c. Proveer de impresoras conectadas directamente a cada impresora.

n. Concluir las operaciones en el sitio alternativo de recuperación.

Destruir o trasladar al sitio original los registros y documentos confidenciales que se han almacenado en el sitio alternativo.

Concluir contratos de alquiler del sitio alternativo y realizar los pagos respectivos si es el caso.

Registrar las facturas en el centro de costos del Departamento de TI, previa aprobación de IT Coordinator.

En este caso: No Aplica

Cabe destacar que varios de los pasos a seguir en este plan se los puede implementar de manera paralela con el fin de optimizar tiempos de recuperación y no necesariamente secuencial, esto depende de la disponibilidad de tiempo de los miembros del plan.

Las diferencias entre un escenario y otro radican en tiempos de recuperación, costos y aspecto generales de efectividad del plan de continuidad, como se va analizar a continuación:

3.2.3.7 Tiempo que se ha invertido durante la recuperación del desastre.

En la Tabla 3.1 se presenta la comparación de los tiempos de recuperación con y sin plan de continuidad:

Parámetros	Sin Plan de Continuidad	Con Plan de Continuidad
Tiempo de obtención de un servidor con capacidades similares al servidor de archivos.	15 días	1 hora
Tiempo de instalación y configuración del sistema operativo.	3 horas	0 horas
Tiempo de Instalación y configuración de Impresoras.	1 hora	0 horas
Tiempo de Instalación y configuración de herramienta Legato Networker 7.2. (Solicitud a Roche Brasil)	1 día	0 días
Tiempo para sacar al servidor de archivos anterior del dominio.	5 minutos	5 minutos
Tiempo para cambiar el nombre del Servidor para redireccionarlo.	0 minutos	5 minutos
Tiempo para reiniciar el servidor.	0 minutos	15 minutos
Tiempo para cargar el backup.	6 horas	6 horas
Tiempo para validar permisos de acceso en carpetas y archivos.	1 hora	1 hora
Tiempo para verificar el buen funcionamiento del servicio.	1 hora	1 hora
Total Tiempo	16 días, 12 horas, 5 minutos	9 horas y 25 minutos
Tiempo aproximado	17 días ≈480 horas	10 horas

Tabla 3.1 Parámetros de Tiempo de la Evaluación del Simulacro

3.2.3.8 Costos generados por el desastre.

En la Tabla 3.2 se presenta la comparación de los costos de recuperación con y sin plan de continuidad:

Parámetros	Sin Plan de Continuidad	Con Plan de Continuidad
Costo de un servidor con capacidades similares al servidor de archivos.	USD 8000	USD 0
Costo de un sistema de aire acondicionado temporal.	USD 500	USD 500
Costo de reparación del aire acondicionado afectado o adquisición de uno nuevo.	USD 2000	USD 0 (garantía)
Costo de consultoría de Proveedores en caso de haber utilizado este servicio.	USD 200	USD 0
Total Costo	USD 10700	USD 500

Tabla 3.2 Parámetros de Costos de la Evaluación del Simulacro

3.2.3.9 Parámetros de efectividad del Plan de Continuidad.

En la Tabla 3.3 se presenta la comparación de parámetro del plan de continuidad:

Parámetros	Con Plan de Continuidad
Tiempo de paralización de operaciones del negocio por el desastre.	8 horas (paralización parcial)
Tiempo de retrasos de trabajo.	4 horas
Porcentaje de usuarios afectados por el desastre.	75%
Número de procesos críticos afectados por el desastre.	10
Esfuerzo invertido por los miembros de TI.	50 horas/hombre
Integridad de la información recuperada.	99% (1 % si se daño algún archivo antes del desastre)
Número de recursos de personal adicionales para la recuperación.	0 personas
Maximum Tolerable Downtimes (MTD). El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio.	Los procesos críticos que tienen MTD=A, donde 1≤A≤24horas
RTO (Recovery Time Objective): Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción.	72 horas base (más una hora por proceso afectado).
WRT (Work Recovery Time): Indica el tiempo disponible para recuperar los datos perdidos, trabajo retrasado y datos capturados manualmente una vez que los sistemas o recursos son recuperados.	Para servidor de archivos 2 horas. Para impresoras no aplica.
RPO (Recovery Point Objective): Es la magnitud de los datos perdidos que pueden ser tolerados por un proceso del negocio en términos de un período de tiempo.	Los datos perdidos que pueden ser tolerados en función del tiempo es de 30 minutos. Para impresoras no aplica.

Tabla 3.3 Parámetros de Efectividad del Plan de Continuidad del Negocio

3.3 RESULTADOS DE LA EVALUACIÓN

Como ya se ha mencionado, el simulacro ayuda a retroalimentar el plan de continuidad apoyando así a su efectividad.

EL simulacro de la caída del servidor ha dado como resultado varios valores en parámetros de tiempo, costos y efectividad del plan de tal forma que ayudan a evaluar si el plan es aplicable a la realidad de la empresa y su entorno de operaciones.

A continuación se hará un análisis de los parámetros determinados tomando en cuenta que se los compara aplicando el plan y sin aplicarlo, para definir las ventajas y desventajas de su ejecución en el Departamento de TI de Roche Ecuador:

3.3.1 PARÁMETROS DE TIEMPO

Tiempo de Obtención de un servidor con capacidades similares al servidor de archivos: Si se aplica el plan de continuidad el servidor de reemplazo, en caso de daño del principal, estaría ya preparado con antelación, como es un gasto inútil el hecho de tener un servidor sin utilizarlo, podría servir para respaldos de imágenes de computadores portátiles o de escritorio, de tal manera que solamente se tomaría 1 hora en prepararlo con el espacio suficiente para utilizarlo como reemplazo del servidor de archivos, ya sea depurando información o sacándola en otro disco adicional.

Si no se aplica plan de continuidad alguno, en el momento del desastre los miembros de TI tendrían que dedicarse a conseguir un servidor con capacidades similares al servidor de archivos, esto tomaría mucho tiempo ya que los proveedores de hardware generalmente no tienen disponibles en stock servidores con características determinadas, sino que los ensamblan, configuran o traen del exterior bajo pedido del cliente, por lo tanto se estima un promedio de 15 días hasta poder conseguir un servidor que pueda soportar la funcionalidad que debe tener un servidor de archivos y de impresoras.

Tiempo de instalación y configuración del sistema operativo: Debido a que el Departamento de TI debe utilizar estándares de hardware y software regidos por casa matriz, se debe tomar en cuenta que el sistema operativo que se utiliza tanto para estaciones de trabajo como para servidores está adaptado exclusivamente para Roche, por lo tanto no es posible instalar cualquier sistema operativo. Al aplicar el plan de continuidad se tiene el sistema operativo ya instalado y configurado con anterioridad en el servidor disponible para desastres por lo que al momento de la recuperación no tomaría tiempo en realizar esta actividad. En el caso de no aplicar ningún plan, una vez que se ha obtenido un servidor, toma aproximadamente 3 horas en instalar y configurar el sistema operativo.

Tiempo de instalación y configuración de Impresoras: Al aplicar el plan de continuidad no tomaría tiempo para instalar y configurar impresoras ya que

estarían preparadas desde antes de la ocurrencia del desastre en el servidor adicional. Si no se aplica plan alguno tomaría aproximadamente 1 hora instalar las impresoras en el servidor nuevo.

Tiempo de Instalación y configuración de herramienta Legato Networker 7.2.: La instalación y configuración de la herramienta para obtener respaldos la configuran desde Brasil, por lo que si no se aplica un plan de continuidad la demora entre la solicitud a Brasil y la preparación de la herramienta es de 24 horas. Si se aplica el plan no se necesitaría tiempo para esta actividad.

Tiempo para sacar al servidor de archivos anterior del dominio: en el caso de que el servidor de archivos que ha sufrido el daño aún esté dentro del dominio, se debe deshabilitarlo para incluir al servidor de reemplazo. Esta tarea toma aproximadamente 5 minutos, con o sin plan de continuidad.

Tiempo para cambiar el nombre del Servidor para redireccionarlo: en el caso de no implementar un plan no se requiere este paso por lo que no se invierte tiempo para esta actividad. Al aplicar el plan de continuidad este paso toma aproximadamente 5 minutos, esta tarea consiste en cambiar el nombre del servidor (Ejm. Servidor 1) de reemplazo por el nombre que del servidor de archivos que sufrió el daño (Ejm. Servidor 3).

Tiempo para reiniciar el servidor: En el caso de no implementar un plan esta actividad no toma tiempo alguno porque se la omite porque al servidor se le configura desde cero. Si se ejecuta el plan de continuidad se reinicia el servidor que se ha asignado como de archivos (servidor de reemplazo), con el fin de que se efectúen las nuevas configuraciones realizadas.

Tiempo para cargar el backup: El tiempo que se requiere para cargar el backup del servidor de archivos, utilizando o no, el plan de continuidad es de aproximadamente 6 horas, ya que el servidor de archivos tiene un contenido de aproximadamente 500 GB.

Tiempo para validar permisos de acceso en carpetas y archivos: El tiempo que se requiere para validar permisos en carpetas y archivos del servidor es de 1 hora aproximadamente, se utilice o no, el plan de continuidad. Esta tarea consiste en revisar y activar los permisos necesarios de las carpetas y archivos para que puedan acceder los usuarios de forma individual o por Departamento.

Tiempo para verificar el buen funcionamiento del servicio: Sea que se utilice o no, un plan de continuidad se debe invertir al menos 1 hora para monitorear el correcto funcionamiento y acceso a los archivos que han sido restaurados, de manera que se asegure la confiabilidad e integridad de los mismos.

Total Tiempo de Recuperación: Si no se implementa un plan de continuidad, el tiempo de recuperación es de 16 días, 12 horas, 5 minutos. Si se aplica el plan de continuidad propuesto la recuperación del servidor de archivos tomaría 9 horas y 25 minutos.

Tiempo aproximado: Tomando en cuenta que para gestionar las actividades de logística, comunicaciones, acuerdos, etc. puede tomar tiempo adicional, se aproxima y se tienen los siguientes tiempos: Sin aplicar el plan la recuperación toma aproximadamente 17 días. Aplicando el plan de continuidad propuesto la recuperación del servidor de archivos toma aproximadamente 10 horas. Ver Figura 3.1.

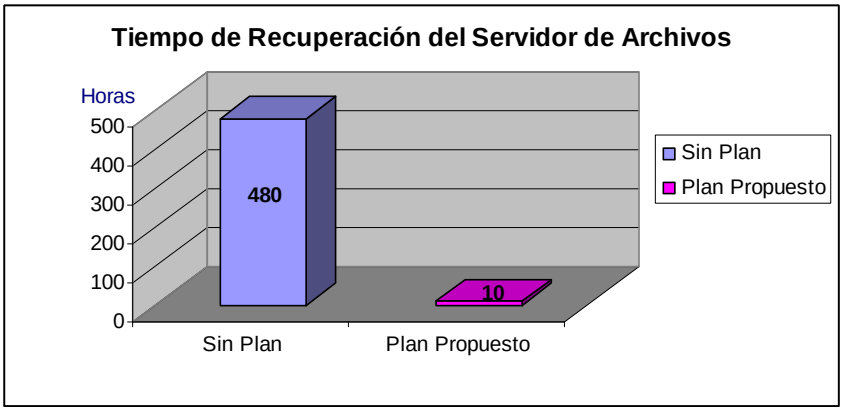

Figura 3.1 Tiempo de Recuperación del Servidor de Archivos

Si se toma en cuenta un tiempo óptimo de adquisición del servidor de archivos en el caso de no implementar un plan, se presume un tiempo no menor a 2 días, en

este caso la recuperación sería aproximadamente 4 días, este tiempo sigue siendo mucho mayor en comparación a 10 horas de recuperación utilizando el plan de continuidad. Por lo tanto este parámetro depende de la rapidez con la que el proveedor pueda conseguir un servidor adecuado.

Cabe destacar que mientras más rápido los proveedores puedan conseguir los equipos solicitados, mayores son los costos. Por consiguiente los factores: tiempos y costos resultan ser directamente proporcionales, a mayor rapidez de entrega del equipo, mayor costo.

Por otra parte la solicitud a Brasil de la instalación y configuración de la herramienta Legato para Backups, toma un tiempo de aproximadamente 1 día, sin embargo, ésto depende de la disponibilidad del personal de Roche Brasil para atender esta petición.

3.3.2 PARÁMETROS DE COSTOS

Costo de un servidor con capacidades similares al servidor de archivos: El costo aproximado de la adquisición de un servidor de características similares al servidor de archivos es de USD 8000, de acuerdo a los valores vigentes actualmente en el mercado. En cambio, si se aplica el plan de continuidad propuesto, en el momento de la recuperación no se invierte costo alguno, la inversión sería con antelación y a largo plazo.

Costo de un sistema de aire acondicionado temporal: Debido a que es necesario controlar el desastre sin que sus secuelas sigan afectando a los demás recursos de TI, en este caso, controlar la temperatura por el daño del aire acondicionado, se debe adquirir o alquilar un aire acondicionado temporal mientras se repara el sistema de aire acondicionado de planta o se adquiere uno nuevo según el tipo de daño. Por lo tanto de cualquier manera si se implementa o no el plan propuesto se debería invertir en controlar el daño, por lo que se estima un aproximado de USD 500.

Costo de reparación del aire acondicionado afectado o adquisición de uno nuevo: Para recuperar el sistema de aire acondicionado que ha sufrido un daño se tiene la opción de mandar a repararlo o adquirir uno nuevo. En el caso de no utilizar un plan se estima aproximadamente USD 2000, y al usar el plan de continuidad no tendría costo debido a que se aplicaría la garantía ya se lo tendría asegurado y se realizaría su mantenimiento constantemente.

Costo de consultoría de Proveedores en caso de haber utilizado este servicio: Tomando en cuenta que cualquier proveedor al realizar una asesoría cobra un aproximado de USD 200 dependiendo del tipo de servicio que presten a la compañía. Si se aplica el plan de continuidad, teniendo documentados todos los procesos y procedimientos a seguir en caso de daños, la situación puede ser controlada por los miembros de TI, evitándose los costos por concepto de consultoría.

Total Costo: Si se toman n cuenta los factores anteriores que se requieren para la recuperación se puede observar que utilizando el plan propuesto la inversión es de USD 500, en cambio si no se tiene un plan de continuidad el costo es de USD 10700 aproximadamente. Ver Figura 3.2.

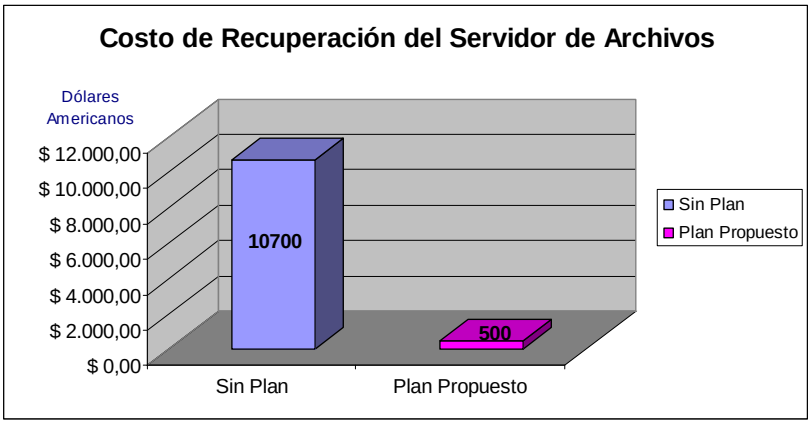

Figura 3.2 Costos de Recuperación del Servidor de Archivos

Los costos estimados en este análisis están tomados de acuerdo a los costos vigentes en el mercado, a los proveedores con los que tiene acuerdos la empresa y a los estándares que rige casa matriz.

Se puede notar la gran diferencia de costos que se generan al utilizar un plan de continuidad, pues uno de los objetivos del plan de continuidad es tratar de minimizar los costos al momento de la recuperación, constituyendo este factor como clave en la decisión de implementación de un plan que aparte de ayudar a dar continuidad al negocio, tenga costos bajos.

3.3.3 PARÁMETROS DE EFECTIVIDAD DEL PLAN DE CONTINUIDAD

Tiempo de paralización de operaciones del negocio por el desastre: Se estima 8 horas de paralización de actividades en el negocio, sin embargo este tiempo se lo denomina parcial debido a que las funciones de los usuarios no están basadas en su totalidad en los archivos que almacenan en el servidor, una buena parte de los archivos los tienen guardados en sus herramientas de gestión de e-mail o en su máquina local, además dependiendo de la fecha de modificación de los archivos requeridos se pueden levantar los archivos más importantes para los usuarios, obteniéndolos directamente de cintas de backup anteriores. Ver Figura 3.3.

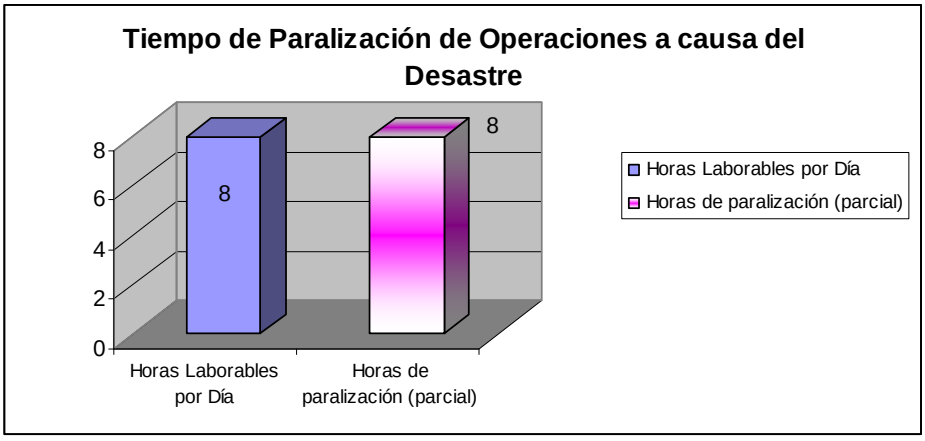

Figura 3.3 Tiempo de Paralización de Operaciones a causa del Desastre

Tiempo de retrasos de trabajo: Una vez especificado que las horas de paralización no es de manera absoluta sino relativa, se puede estimar que el tiempo de retrasos de trabajo que el desastre ha producido es de 4 horas. Ver Figura 3.4.

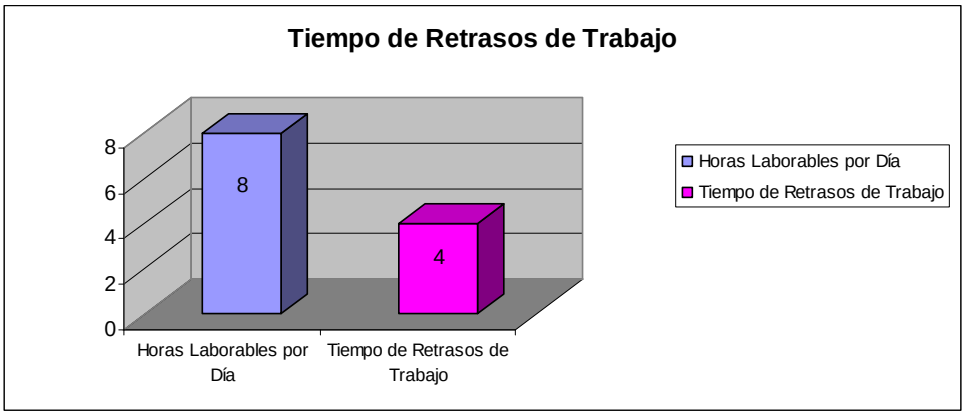

Figura 3.4 Tiempo de Retrasos de Trabajo

Porcentaje de usuarios afectados por el desastre: Casi la totalidad de los usuarios utilizan como lugar de almacenamiento seguro el servidor de archivos ya que están concientes de que esta información es respaldada diariamente. Tomando en cuenta que los Visitadores Médicos por su tipo de trabajo almacenan sus archivos en su herramienta de gestión de e-mail o en su máquina local, se estima que un 75% de usuarios se ven afectados por la caída del servidor de archivos. Ver Figura 3.5.

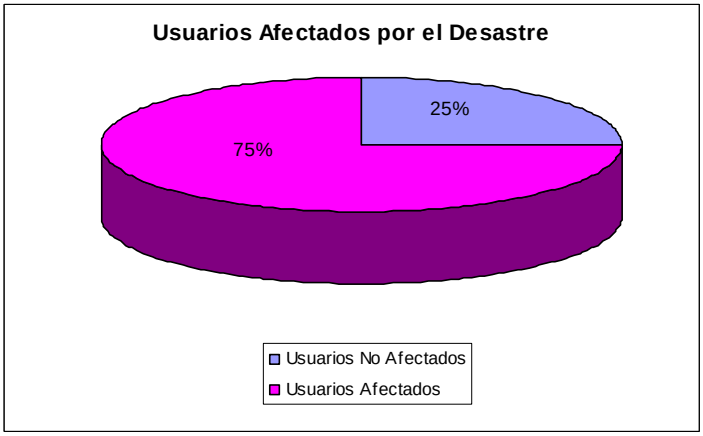

Figura 3.5 Usuarios Afectados por el Desastre

Número de procesos críticos afectados por el desastre: Los procesos críticos definidos son 17, de los cuales 10 utilizan en sus procedimientos el almacenamiento de información en el servidor de archivos o el servicio de impresiones. Ver Figura 3.6.

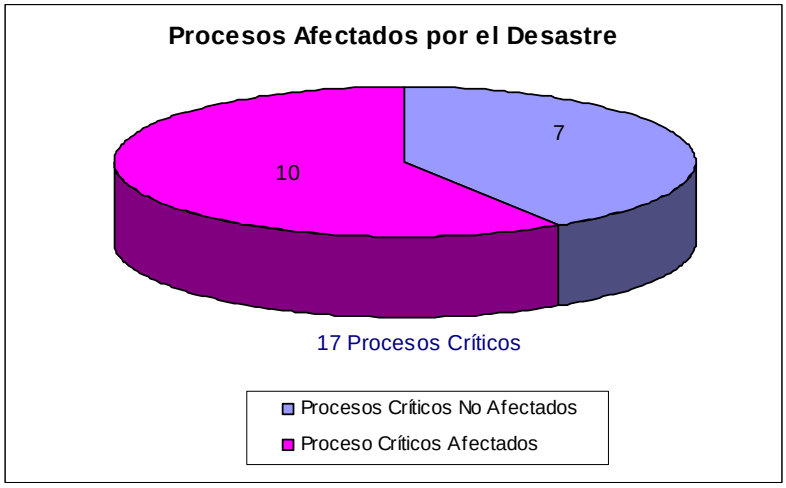

Figura 3.6 Procesos Afectados por el Desastre

Esfuerzo invertido por los miembros de TI: Debido a que el esfuerzo se mide en horas/hombre se tiene en cuenta que para la recuperación del servidor de archivos participan los 5 miembros de TI, y se toman 10 horas para la recuperación, se tiene como esfuerzo realizado un total de 50 Horas/Hombre.

Integridad de la información recuperada: En el caso de que el backup haya sido restaurado exitosamente y sin ningún inconveniente se puede deducir que la integridad de la información es de un 99%, donde el 1% restante representa la probabilidad de que algún archivo se haya dañado antes del desastre o algún tipo de error al restaurar el backup. Ver Figura 3.7.

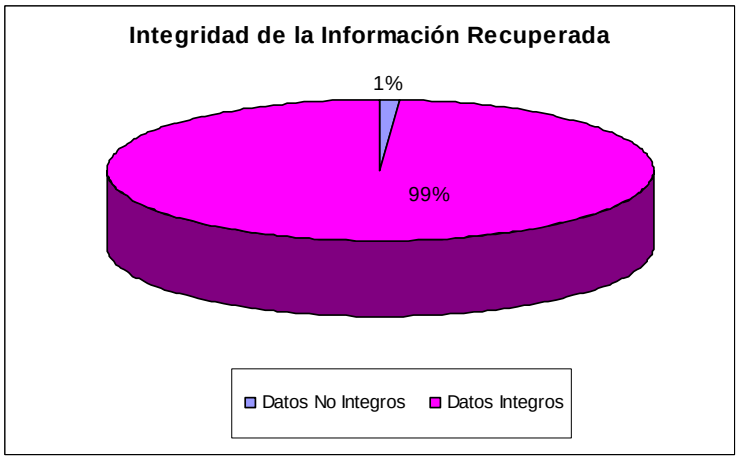

Figura 3.7 Integridad de la Información Recuperada

Número de recursos de personal adicionales para la recuperación: No se ha requerido personal adicional para el caso de la caída del servidor debido a que se tiene información disponible acerca de los procesos y procedimientos, tal que cualquier miembro del Departamento de TI está capacitado para realizar cualquier función dentro de esta recuperación gracias a la documentación de configuraciones existente.

Maximum Tolerable Downtimes (MTD). El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio: Varios de los procesos críticos del negocio que se ven afectados por el desastre de la caída del servidor de archivos e impresiones tienen un MTD de "A", donde A=1-24 horas que el servicio puede estar fuera de operaciones. Entonces, si la recuperación del desastre toma aproximadamente 10 horas, todos los MTD para cada procesos afectado, cumplen con el tiempo de recuperación, demostrando así que el tiempo de recuperación no sobrepasa el MTD de cada proceso, al no aplicar el plan, el tiempo de recuperación no cumple con los MTD de procesos, de tal manera que no satisface el tiempo de restauración del servicio en el rango de tiempo estimado para que no afecte las actividades principales del negocio. Ver Figura 3.8.

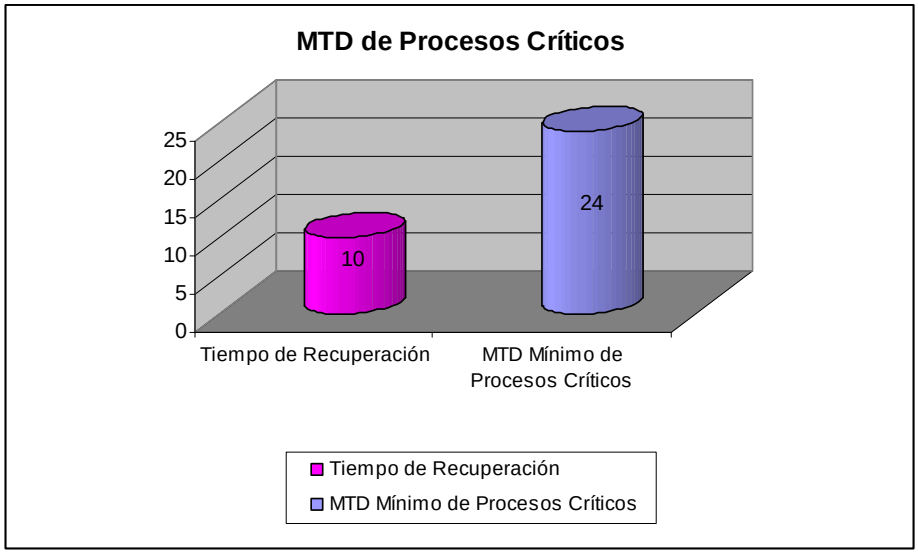

Figura 3.8 MTD de Procesos Críticos

RTO (Recovery Time Objective): Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción: El tiempo mínimo en el que se puede recuperar el servidor de archivos e impresiones sin aplicar ningún plan y siguiendo los procedimientos actuales es de 72 horas, más la demora de recuperar cada proceso afectado en el caso de que se requieran otros recursos adicionales. Por lo tanto el tiempo de recuperación aplicando el plan satisface el RTO base de recuperación. Ver Figura 3.9.

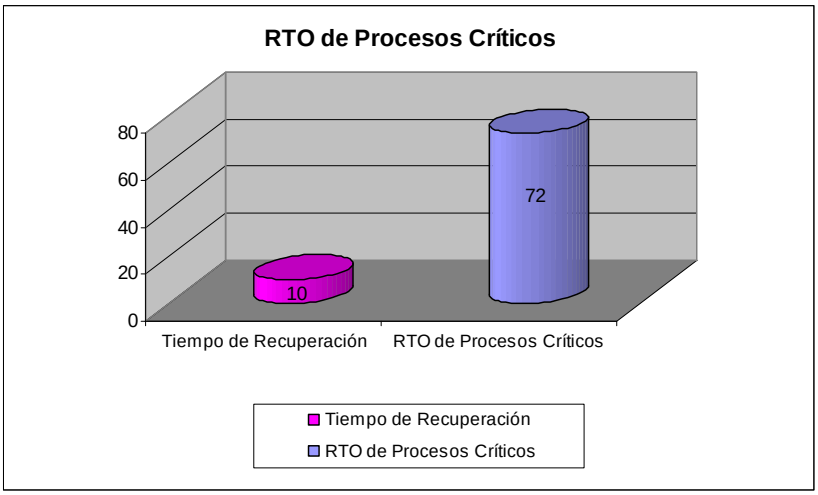

Figura 3.9 RTO de Procesos Críticos

WRT (Work Recovery Time): Indica el tiempo disponible para recuperar los datos perdidos, trabajo retrasado y datos capturados manualmente una vez que los sistemas o recursos son recuperados: Para el caso de la caída del servidor de archivos no se requiere recuperar datos de forma manual, a excepción de que entre los archivos almacenados en el mismo se encuentren algún tipo de formulario y que lo usen frecuentemente, de todas maneras el tiempo que tomaría compensar el retraso de trabajo sería no mas de 2 horas.

RPO (Recovery Point Objective): Es la magnitud de los datos perdidos que pueden ser tolerados por un proceso del negocio en términos de un período de tiempo: La pérdida de datos que puede ser tolerada por la caída del servidor en función del tiempo es de 30 minutos, es decir, se puede perder los datos elaborados o modificados hasta 30 minutos antes del desastre. Si la recuperación no abarca este lapso empiezan a existir retrasos de trabajo. De acuerdo al

simulacro realizado, los datos han sido recuperados exitosamente y en su totalidad.

De manera general el simulacro de la caída del servidor de archivos a ayudado a determinar las ventajas que puede aportar al negocio un plan de continuidad, existen varias opciones de recuperación, las cuales pueden acortar tiempos de retorno a la normalidad, en este caso se debe llegar a un equilibrio entre tiempo y costos, ya que estos factores son directamente proporcionales, de manera que puedan satisfacer las necesidades que tiene la empresa de seguir operando en sus principales actividades.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

El diseño e implementación del plan de continuidad del negocio aplicado al Departamento de TI de Roche Ecuador S.A. ha dado como resultado las siguientes conclusiones y recomendaciones:

4.1 CONCLUSIONES

- El plan de continuidad del negocio para un Departamento de TI debe estar enfocado a la recuperación de los procesos críticos del negocio.

- La base fundamental para lograr un plan de continuidad de alta calidad y efectividad es el Análisis de Impacto en el Negocio (BIA).

- A mayor cantidad de tiempo de paralización de operaciones, mayores son las pérdidas en el negocio, mientras que si se realizan inversiones y planificaciones de actividades para volver a la operación normal, los costos de recuperación disminuyen.

- Para lograr alcanzar un Plan de continuidad del negocio que sea exitoso, se requiere la participación activa de cada uno de los miembros de la empresa.

- Para lograr una aceptación total del Plan de Continuidad del Negocio se requiere convencer al área gerencial, mediante un análisis costo – beneficio, es decir, los costos de recuperación de un desastre son mayores que la implementación de medidas de prevención.

- El plan de continuidad debe ser considerado como un proceso global de la empresa que debe ser retroalimentado, mejorado y actualizado constantemente.

4.2 RECOMENDACIONES

- Se recomienda al Departamento de TI tener equipos de respaldo ya preparados en hardware y software, especialmente de los servidores, para minimizar el tiempo de recuperación en caso de caída de alguno de ellos.

- Se recomienda que se utilice una herramienta que ayude a obtener imágenes de servidores como respaldo en caso de que ocurra un desastre.

- Se recomienda mantener el plan de continuidad actualizado mediante revisiones cada 6 meses y simulacros anuales, con el fin de mantener vigentes todas sus actividades.

- Se recomienda al Departamento de TI de Roche Ecuador S.A. utilizar los equipos de recuperación en otros procesos que no sean críticos, cuando no se los utilice en casos de desastre.

BIBLIOGRAFÍA

Libros y Manuales

- Santa Monica Consulting S.A.. Fundamentos de ITIL para la Gestión de Servicios de TI. Manual de Formación Versión 1.4. ARTUTA. Argentina. 2002.

- Syed, Akhtar; Syed, Afsar. Business Continuity Planning Methodology. 2004

- Fulmer, Kenneth L. Business Continuity Planning: A Step by Step Guide. Tercera Edición. Philip Jan Rothstein, FBCI, Editor. Brookfield-USA. Oct 2004.

Artículos y Direcciones Electrónicas

- MARTÍN, Aurelio. Alta Disponibilidad Plan de Contingencia. http://www.aslan.es/boletin/boletin39/siemens.shtml. 28 de Diciembre del 2006.

- HIDALGO MATEOS, José Luis. La continuidad del negocio y la seguridad;un reto y una necesidad. http://www.belt.es/expertos/experto.asp?id=2503. 28 de Diciembre del 2006.

- SOPRA PROFIT. ITIL (Information Technology Infrastructure Library). https://www.fdi.ucm.es/libre/formativas/ITILSopraProfit.pdf. 22 de Abril del 2007.

- SUN MICROSYSTEMS. ITIL IT Infrastructure Library, Las Mejores Prácticas para la Gestión de Servicios de TI en su Organización. https://www.sun.es/services/itil. 22 de Abril del 2007.

- OSIATIS. ITIL Gestión de Servicios TI. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_continuidad_del_servicio. 22 de Abril del 2007.

- ANONIMO. Uti. http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=2428, 28 de Diciembre de 2006.

- STROHOL SYSTEMS. Business Continuity Planning & Disaster Recovery Software and Services. http://www.strohl.com. 19 de Junio del 2007.

- COMUNIDAD BCM. Comunidad BCM de Iberoamérica. http://www.comunidadbcm.com. 11 de Julio del 2007

- EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A. Business Continuity Plan. http://eficienciagerencial.com. 23 de Enero del 2008.

Tesis

- Diego Xavier Torres Ripalda; Metodología para la Preparación de un Plan de Recuperación de Aplicaciones Críticas y Datos en casos de Desastres. EPN, Quito, 1998
- Naranjo Elicio, Rómulo Paspuel; Sistema Informático de Apoyo a la Administración de Planes de Contingencia SICOB; EPN; Quito; 2002
- José Villagómez, Mario Molina; Análisis de la Aplicabilidad de los Planes de Contingencia en las Unidades Informáticas de Quito; EPN; Quito; 2000
- Larrea Jimena, Hugo Montesdeoca; Diseño del Sistema de Seguridad y del Plan de Contingencia para la Interconexión entre Regionales y Matriz de una Empresa Comercializadora; EPN; Quito; 2002
- Jorge Meza, Jonny Sandoval; Desarrollo de un Modelo de Plan Estratégico de Tecnologías de Información para el Sector Público Ecuatoriano. Caso de Estudio Ministerio de Turismo; EPN; Quito; 2003

ANEXOS

Anexos Impresos[41]

- **Anexo 25:** Plan de Continuidad del Negocio para el Departamento de TI de Roche Ecuador S.A.

Anexos Digitales

Los anexos digitales se encuentran en el cd que se adjunta a este proyecto de titulación.

- **Anexo 1:** Formulario para Catálogo de Servicios
- **Anexo 2:** Evaluación del Impacto Financiero
- **Anexo 3:** Evaluación del Impacto Operacional
- **Anexo 4:** Sistemas, Aplicaciones y Recursos Críticos del Departamento de TI
- **Anexo 5:** Definición de MTD, Maximum Tolerable Downtimes
- **Anexo 6:** Definición de Requerimiento de Tiempo de Recuperación (RTO y WRT)
- **Anexo 7:** Definición del RPO, Recovery Point Objective
- **Anexo 8:** Amenazas como Eventos
- **Anexo 9:** Consecuencias de las Amenazas
- **Anexo 10:** Opciones de Control de Riesgos
- **Anexo 11:** Costos de la Evaluación de Control de Riesgos
- **Anexo 12:** Decisiones de Control de Riesgos
- **Anexo 13:** Evaluación de Opciones Aplicables
- **Anexo 14:** Evaluación Costo-Capacidad
- **Anexo 15:** Datos Personales de Miembro del Equipo Plan de Continuidad
- **Anexo 16:** Datos de proveedores
- **Anexo 17:** Análisis de Impacto en el Negocio
- **Anexo 17-A:** Análisis de Impacto en el Negocio; aplicado al simulacro
- **Anexo 18:** Evaluación de Pérdidas Financieras
- **Anexo 18-A:** Evaluación de Pérdidas Financieras; aplicado al simulacro
- **Anexo 19:** Evaluación de Riesgos

---

[41] Los archivos impresos se encuentran desde la página 152.

- **Anexo 19-A:** Evaluación de Riesgos; aplicado al simulacro:
- **Anexo 20:** Estrategias de Recuperación
- **Anexo 20-A:** Estrategias de Recuperación; aplicado al simulacro:
- **Anexo 21:** Declaración de Desastre
- **Anexo 21-A:** Declaración de Desastre; aplicado al simulacro
- **Anexo 22:** Matriz Actividad-Responsable
- **Anexo 23:** Certificados emitidos por la Empresa ROCHE ECUADOR S.A.: certificados emitidos por IT Coordinator y Networking & EUS Responsible.
- **Anexo 24:** Plan de Continuidad del Negocio para el Departamento de TI de Roche Ecuador S.A.