GUÍA METODOLÓGICA PARA EL DISEÑO DE UN PLAN DE CONTINUIDAD Y CONTINGENCIA DE T.I.

JUAN CAMILO BEDOYA MARTÍNEZ
DIEGO ALEXANDER RIOS

FUNDACIÓN UNIVERSITARIA LUIS AMIGO
ESCUELA DE POSGRADOS
ESPECIALIZACIÓN EN GERENCIA DE TECNOLOGÍA
MEDELLÍN
2012

GUÍA METODOLÓGICA PARA EL DISEÑO DE UN PLAN DE CONTINUIDAD Y CONTINGENCIA DE T.I.

JUAN CAMILO BEDOYA MARTÍNEZ
DIEGO ALEXANDER RIOS

Trabajo de Grado para optar el Título de:
Especialista en Gerencia de Tecnología

Asesor:
M.Sc. Byron Enrique Portilla Rosero

FUNDACIÓN UNIVERSITARIA LUIS AMIGO
ESCUELA DE POSGRADOS
ESPECIALIZACIÓN EN GERENCIA DE TECNOLOGÍA
MEDELLÍN
2012

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Mucho se ha avanzado desde las épocas en que los sistemas de información eran islas para atender cada requerimiento de un departamento en las organizaciones, en ese entonces el mayor problema era integrar la información para compartirla. Tanto se ha desarrollo este tema que en la actualidad se tienen soluciones que no solo integran aplicaciones de una organización o de una empresa, sino que incorporan el concepto amplio de la TIC´s (tecnologías de la información y de la comunicación) para entrar a formar parte de una cadena de valor.

Adicionalmente a la integración de los procesos que se ejecutan en línea y en tiempo real, las empresas dependen de sus sistemas de información para poder operar de manera eficiente. También dependen de los sistemas de información de sus aliados estratégicos para que las operaciones que hoy se efectúan en conjunto, tengan gran impacto y puedan influir positivamente en imagen y servicio.

Los cambios y avances tecnológicos dan una transformación al interior de las organizaciones lo que hace aun más necesario garantizar la disponibilidad de su servicio de información, no solo bajo planes de recuperación de desastres si no bajo procedimientos claros y precisos sobre la Continuidad del Negocio y la Contingencias necesarias para “no parar” y seguir operando ante una falla critica.

Un Plan de Continuidad y Contingencia presume la preparación y la acción que debe ejecutarse ante una incidencia que afecte la Disponibilidad del Servicio en un tiempo determinado, sobre el cual se declara la emergencia, y se ejecutan procedimientos que permiten que el servicio se restablezca en el menor tiempo posible. Una vez resuelta la emergencia, se disparan otra serie de procedimientos que vuelven la operación a su estado normal, procesos que pueden ser bastante tediosos de ejecutar, en especial cuando se trata de tener una mínima afectación sobre los usuarios y clientes.

El enfoque de un Plan de Continuidad y Contingencia se basa en la minimización del impacto que pueda ocasionar una falla o un evento mayor para la organización y está orientado a asegurar la continuidad del servicio cuya afectación incurre en la anormalidad de la operación del negocio y que pueda afectar de manera negativa financieramente, o en el deterioro de la imagen hacia el cliente y el entorno.

Un Plan de Continuidad tiene como prioridad restablecer en el menor tiempo los servicios críticos del Negocio, estos planes pueden incluir sitios alternos de procesamiento en caso tal de un evento nefasto, mientras que el Plan de

Contingencia se enfoca en la recuperación de un servicio, una actividad, un proceso, o información.

La interrupción del servicio no siempre requiere o involucra la invocación de un Plan de Continuidad, generalmente son las Contingencias las que proporcionan una solución directa a una falla o incidencia y según su naturalidad o prolongación se activa el Plan de Continuidad.

Para la elaboración y el desarrollo efectivo de un Plan de Continuidad y Contingencia se hace necesario Gestionar los Riesgos que puedan alterar la Operación y poder no solo identificarlos sino también poder medir su frecuencia y el impacto que estos puedan tener si se materializan desarrollando medidas de control para mitigarlos.

Hoy los riesgos son casi todos de muy alto impacto por las implicaciones que tienen en las organizaciones. Ya casi todas la organizaciones están expuestas a ataques de virus, problemas de seguridad informática, deficiencias en la calidad del software, almacenamiento inapropiado, arquitecturas tecnológicas complejas y hasta políticas poco efectivas para administrar los recursos de la organización que pueden incurrir o materializar una catástrofe y el impacto en el negocio de manera negativa; hasta se puede materializar una amenaza física como por ejemplo un incendio o un terremoto, siendo estos riesgos de menor frecuencia pero si de un impacto muy alto.

Un Plan de Continuidad y Contingencia tiene como objetivo tratar minimizar el tiempo de afectación del servicio teniendo presente que las Empresas desean un Nivel de Disponibilidad en sus servicios superior a un (99%), lo que implica que el sistema siempre estará disponible generando un gran compromiso de las áreas de tecnología para lograr estos niveles de disponibilidad.

Hoy la tecnología brinda diferentes posibilidades y alternativas en servicios y aplicaciones que bajo una adecuada planeación y estructuración de las redes, bases de datos y servidores pueden garantizar en un alto porcentaje el éxito de las organizaciones en cuanto a niveles de servicio y disponibilidad se refiere.

Los beneficios en la gestión eficaz un Plan de Continuidad y Contingencia desde su diseño, implementación, prueba y mejoramiento se reflejan en las organizaciones no solo entendimiento de las amenazas y vulnerabilidades si no también en el desarrollo de competencias, compromisos y dependencias que ofrecen confianza al interior y exterior de las mismas.

Un Plan de Continuidad y Contingencia involucra documentos y compromisos reflejados en procedimientos, políticas y responsabilidades no solo de las áreas de tecnologías de información sino también de toda la organización, generando una cultura en pro de la ejecución efectividad de estos planes.

Un Plan de Continuidad y Contingencia se apalanca sobre tecnologías emergentes (procedimientos de respaldo por periodos de tiempo programados, duplicidad de los sistemas, anillos redundantes, terceras copias, en los servidores y la infraestructura, entre otros), y debe incluir entre otros un plan de recuperación de desastres en el cual no se hará mucho énfasis ya que este es dirigido a desastres naturales o eventos de fuerza mayor sobre la infraestructura física de las empresas mientras que la objetividad del presente trabajo se enfoca en la recuperación de los servicios críticos de la organización en las TIC´s (tecnologías de la información y de la comunicación).

Sin embargo el desarrollo de un Plan de Continuidad y Contingencia, requiere del desarrollo de diferentes estrategias que deben implementarse y probarse mediante procedimientos establecidos ante una falla y después de la restauración.

La reanudación ante los eventos externos puedan tener un impacto muy relevante en cuanto al tiempo de recuperación, las organizaciones entonces deben crear conciencia y estar preparados para mantener los servicios críticos y tener ubicados todos los elementos necesarios ante una crisis o una incidencia de mayor o menor magnitud, siendo muy importante el compromiso y apoyo de las altas gerencias en todos los procesos.

Los Planes de Continuidad y Contingencia pueden ser costosos tanto desde la mima creación, puesta en marcha y mantenimiento para las organizaciones, pero se requieren de estudios de riesgos y balancear el costo de implementación de los Planes de Continuidad y Contingencia con el riesgo de no tenerlo.

INTRODUCCIÓN

Actualmente las personas laboralmente activas tienen alguna relación directa o indirecta con los servicios financieros de un banco o entidades que presten este fin, si se analiza que procesos y tecnologías se desarrollan mientras se está en el mercado y la entidad financiera en la cual se tiene el dinero no está en servicio, presenta una falla, y como usuarios se ha superado una larga fila de espera en la caja registradora; entonces podrían generarse un sin número de inconformidades que finalmente pueden influir negativamente en un deterioro en la imagen de la Entidad.

Pero si se va mas allá como lo expresa el Periódico expansión en un artículo del 23 de febrero de 2007: "Una caída en el fluido eléctrico, una inundación, un incendio, un pequeño corto circuito. Y es que todas las Empresas son susceptibles a sufrir un evento fortuito o intencionado, que afecten sus servicios informáticos. Estos fallos pueden causar pérdida de información valiosa, así como la interrupción de la actividad de la compañía lo que hace crucial la recuperación total de los datos una rápida disponibilidad de los dispositivos"[1].

Y es que como lo publica la Revista Éxito Empresarial en su ejemplar Numero 63 del año 2008 donde revela que según estudios del ICM Computer Group "un promedio del 20% de las organizaciones experimentara algún evento inesperado una vez, cada 5 años". Este mismo artículo, demuestra que las probabilidades son relativamente altas y que si las empresas no se preparan, el impacto de estos eventos pueden acabar con el negoció[2].

Es necesario para las compañías que proveen servicios a sus usuarios y clientes de manera permanente proveerse de herramientas y mecanismos basados en políticas, procedimientos, tecnologías y locaciones que permitan garantizar un servicio confiable, oportuno y disponible.

Con este propósito el presente proyecto tiene como fin proponer una guía metodológica que permita identificar los puntos más relevantes y que son necesarios para elaborar un Plan de Continuidad y Contingencia en las Organizaciones apoyados en la Norma BS 25777 y algunos conceptos generales de la Norma BS2599, si bien aunque este propósito puede diferir en conceptos por su amplia aplicación el objeto es facilitar la tarea de la incorporación de los contenidos de las normas mencionadas anteriormente y con la experiencia obtenida en empresas tecnológicas diseñar esta guía con las fases necesarias

que van desde el análisis de riesgos, identificación de servicios críticos, contingencias sobre procesos y continuidad del negocio.

Juan Gaspar Martínez en los objetivos de la guía para la elaboración del Plan de Continuidad del Negocio describe “Al igual que no hay dos Organizaciones iguales, no hay 2 Planes de Continuidad del Negocio iguales”[3]. Por tal motivo, la elaboración de esta guía describe como un equipo de ingenieros diseña una metodología práctica de como elaborar un Plan de Continuidad y Contingencia del Negocio para una organización y a su vez, esta permitiría a otras personas contar con modelo propuesto y tener una idea más clara de cómo iniciar su elaboración.

Conociendo este propósito se hace necesario resaltar que un Plan de Contingencia encierra el que hacer cuando un proceso falla y como dicha contingencia mitiga el riesgo al que se está expuesto cuando un proceso colapsa por cualquier razón. Por el contrario el Plan de Continuidad está orientado al mantenimiento de las operaciones críticas del negocio y como las Compañías pueden seguir operando en caso de desastre, una emergencia, un daño que represente para la organización trastornos en su operación cotidiana.

Actualmente muchas organizaciones dependen cada vez más de sus Servicios de Información unas más que otras y precisamente la búsqueda continua de mejorar sus servicios y procesos hacia sus clientes, ciudadanos si son entidades públicas o del gobierno por ejemplo son parte de los objetivos de un Plan de Contingencia y Continuidad ya que precisamente busca la continuidad del servicio y este resultado, se refleja en la satisfacción del cliente o usuario del servicio.

Es importante entonces que las empresas estén preparadas a un evento de riesgo que pueda perturbar sus operaciones, y como lo expresa la revisa Éxito Empresarial “Pocas son las empresas que se preparan para enfrentar estas situaciones, pues afirman que si en el pasado no han ocurrido, es poco probable que se presenten en el futuro. ¿Habrán pensado así las empresas ubicadas en el World Trade Center antes del 11 de septiembre de 2001?“[2].

Es ahí donde se requiere un Plan de Continuidad y Contingencia que permitirá a la Organización dar una respuesta oportuna, y coordinada ante una emergencia, falla, incidencia que afecta sus sistemas de información y por ende el servicio que presta al usuario o cliente.

Para dar una idea de la importancia de tener un (Plan de Continuidad y Contingencia PCN o BCM) según cifras del Emergency Management Forum (Estados Unidos), donde de cada 100 Empresas que afrontaron un desastre sin

contar con un PCN o BCM el 43% nunca reabrieron el negocio, el 51% sobrevive pero quedaron fuera del mercado después de 2 años y solo el 5 % logro sobrevivir a largo plazo[4].

A partir de estas cifras, se plantea la pregunta a la Organización, ¿Cuenta su compañía con un plan de Continuidad y Contingencia que le permita en un momento dado restablecer de manera inmediata u oportuna el servicio que presta a los usuarios o clientes de su organización ante una falla, incidencia, o evento de riesgo?

La elaboración de un Plan de Continuidad y Contingencia, suministra a la compañía el respaldo no solo de Información, sino también de sus procesos cuando se presente alguna incidencia que afecte su continuidad y no solo requieren de políticas que afiancen sus procesos, es muy importante considerar el costo y las pérdidas posibles que pueden presentarse al tener una afectación en el servicio; lo que hace necesario entonces evaluar el entorno actual; considerar y clasificar sus vulnerabilidades.

Como indica ICM Computer Group (2004) evitar pérdidas de mercado, financieras, proteger los activos, la información, mitigar la publicidad negativa, cumplir con requerimientos legales exigidos, son solo algunos de los beneficios que se obtienen al implementar un Plan de Continuidad y Contingencia[2].

1

[1] (Arrieta, E - Revista, Adiós a los desastres informáticos disponible en, http://www.recoverylabs.com/prensa/2007/02_07_expansion.htm, 2007)
[2] (CEGESTI, Andrea Shum - Éxito Empresarial tomado de, http://www.cegesti.org/exitoempresarial/publicaciones/publicacion_63_150508_es.pdf, No. 63, 2008)
[3] (Martínez, 2006)
[4] (ESA Securtiy - Seguridad de la Información, www.esa-security.com, 2008)

OBJETIVO GENERAL

Proponer una guía metodológica que proporcione un esquema secuencial de contenidos de manera descriptiva, para facilitar la creación de un Plan de Continuidad y Contingencia con el apoyo en los estándares internaciones BS-25999 y BS 25777.

OBJETIVOS ESPECÍFICOS

- Describir cómo se pueden identificar, analizar y evaluar los riesgos a los que pueden estar expuestos los Sistemas de Información y el Impacto en el Negocio si los riesgos llegan a materializarse, como también las Vulnerabilidades las cuales se pueden convertir en factores de riesgo crítico.

- Identificar los Servicios Críticos y niveles de disponibilidad deseados con el fin de establecer los Planes de Continuidad y Contingencia según la incidencia o falla presentada.

- Diseñar planes de contingencia y continuidad a partir de un análisis y evaluación de riesgos, servicios críticos y niveles de disponibilidad.

CAPITULO 1. MARCO TEÓRICO Y ESTADO DEL ARTE

Las referencias teóricas se identifican en el desarrollo de metodologías que fueron evolucionando a raíz de acontecimientos nefastos como el ataque terrorista realizado a las Torres Gemelas el 11 de Septiembre de 2001 donde varias empresas fracasaron por la falta de un Plan de Continuidad del Negocio.

Através de los años la necesidad de poder seguir operando ante una falla de cualquier índole se ha convertido en requisito incluso exigido para ciertas empresas como lo son las financieras y del gobierno (Art 6, Ley 1369 de 2009), “Plan de continuidad del negocio es el conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción y el Plan de contingencia es el conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso” (Ministerio de las Tecnologías y las Comunicaciones, 2009), por lo que las empresas entonces han adoptado metodologías, normas y técnicas las cuales se han adoptado a sus procesos en la implementación de Planes de Continuidad y Contingencia.

La información obtenida para el desarrollo de esta guía de referencia se ha obtenido en la web basada en informe de entidades de estandarización internacional como BSI (British Standards Institution) Institución de Certificación a en el tratamiento de estándares que permiten obtener orientación y apoyo a los practicantes de la continuidad del negocio. El BSI cuenta actualmente con más de 7000 miembros en 100 países activos en un estimado de 2,750 organizaciones en los sectores privado, público y tercer lugar (BSi México, 2012).

La elaboración de un Plan de Continuidad y Contingencia también implica el Análisis de Vulnerabilidades y la identificación, valoración y controles de los Riesgos incluyendo más importantes que identifican las Compañías y pueden poner en riesgo la Operación del Negocio.

En el trabajo de (Baños & Carrera, 2010), se elabora un Plan de disponibilidad de TI para la empresa RELIANCE abarcando el estudio de los procesos de la empresa, su estructura, se describe el proceso de la elaboración del Plan de Disponibilidad y la Gestión del Análisis de Riesgo.

Otro trabajo importante es el de (Ochoa Vasquez, 2011), cuya finalidad fue elaborar una metodología para el desarrollo del Plan de Continuidad del Riesgo Operativo para el Banco Ecuatoriano de la Vivienda (BEV) incorporando diferentes estrategias prevención, respuesta, abarcando el Análisis de Riesgo y el Análisis de Impacto del Negoció (BIA).

En (Trujillo Ramírez, 2012) se presenta una descripción de las diferentes herramientas de TI para la Continuidad del Negocio resaltándose principalmente las Normas BS25999 y BS2577 las cuales son las normas mas importantes en cuanto a buenas prácticas se refiere para el desarrollo y la aplicación de los Planes de Continuidad y Contingencia, a su vez se pueden identificar en este trabajo diferentes estrategias usadas en las áreas de Tecnología para que los sistemas de información puedan seguir operando ante una falla entre las cuales esta la replicación de la bases de datos que consta de enviar transacciones de la base de datos principal a una secundaria.

En relación con este tema se han desarrollado otras tesis como la Propuesta de una metodología para elaborar un programa de continuidad del negocio en México (Morales, 2012) en la cual se incorporan para la Administración de la Continuidad del Negocio metodologías y estándares para su elaboración.

La elaboración de un Plan de Continuidad y Contingencia requiere de elementos importantes que van desde el Análisis de Riesgos, el Análisis de Impacto del Negocio, la Identificación de los Servicios o Elementos Críticos de la Organización para lo cual existen normas internacionales que proporcionan un conjunto de buenas prácticas para la creación de los Planes de Continuidad y Contingencia.

BSI British Standards es la entidad de normalización del Reino Unido, con una reputación de independencia, integridad e innovación en la creación de normas que fomentan las mejores prácticas reconocidas en el mundo entero. Desarrolla y comercializa normas y soluciones de estandarización que satisfacen las necesidades de las empresas y la sociedad, actualmente contempla las normas BS – 25999 y 25777-1 para la Gestión de la Continuidad del Negocio (BSi México, 2012).

La Norma BS – 25999 comprende 2 partes la primera de ellas publicada en el 2006 y la segunda en el 2007.

- La 1ra comprende unas recomendaciones y buenas prácticas, es simplemente un documento guía.

• La 2da es una especialización publicada el 20 de Noviembre de 2007 y proporciona los requisitos de un Sistema de Gestión de Continuidad del Negocio (SGNC).

Las características de la Norma BS – 25777-1 son muy importantes para el desarrollo de esta guía pues su finalidad es precisamente separa formalmente la Continuidad del Negocio de la Continuidad de TIC's (Tecnologías de Información - TI) porque si bien tienen interrelación con la Norma Bs – 25999 es indispensable separar la responsabilidad y la objetividad de las actividades.

Antes de esta separación las áreas de Tecnología Informática estaban inmersas en los Planes de Continuidad y no en todos los casos era solo exclusividad de las áreas de Tecnología e Información, a partir de estas premisas la British Standards Institution (BSI) en el 2006 con la colaboración de empresas del sector de TI crea un documento denominado PAS 77, cuyo documento contemplaba un código de buenas prácticas para crear Planes de Continuidad de Servicios de TI, donde inicialmente se concibió también 2 partes la BS 25777-1 que aborda los código de buenas prácticas sobre cómo realizar la gestión de la continuidad de servicios TI en una organización y la BS 25777-2, que especificaría los requisitos para implementar, operar, supervisar, revisar, probar, mantener y mejorar un sistema de gestión de continuidad de servicios TI, aunque según los expertos del sector de TI es posible que la segunda parte no se publique nunca o no se utilicé con frecuencia, gracias a las buenas especificaciones establecidas en la primera parte (BSi México, 2012).

La norma BS-25999 es un estándar el cual, establece mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio teniendo en cuenta los riesgos a los que se enfrenta una organización (Rodríguez Lache, 2009) y la Norma BS 25777 es un código de buenas prácticas que establece un marco y da las directrices generales para crear un plan de continuidad de servicios de tecnologías de la información (BSI British Standards - BS 25777, 2008).

La BS 25777-1 entró en vigor el 30 de Noviembre de 2008, esta contiene especificaciones particulares que permiten a las organizaciones constituir el (BCM Business Continuity Management - Administración de la Continuidad del Negocio), como un elemento importante para la gestión eficaz y prudente.

Esta Norma contempla las pautas que las organizaciones deben considerar para la elaboración de los Planes de Continuidad y Contingencia abarcando desde el compromiso y responsabilidades de la organización, la formación y

concientización de la implementación de la Gestión de Continuidad del Negocio hasta el mantenimiento, pruebas y revisiones de los Planes una vez se hayan implementado (BSI British Standards - BS 25777, 2008).

Cabe resaltar que las consideraciones contenidas en la norma las organizaciones pueden involucrarlas en sus procesos teniendo presente que dentro de la misma norma es primordial la identificación de los servicios críticos o actividades criticas y la respectiva evaluación de riesgos y las vulnerabilidades a las que pueden estar expuesta las organizaciones.

Tradicionalmente y mucho antes de las publicaciones de esta Norma y de la toma de conciencia a raíz de los nefastos desastres que fueron originados por el ataque del 11 de Septiembre en Nueva York, las estrategias se limitan solo a la recuperación después del evento, lo que finalmente llevaba a que los sistemas de tecnología, datos e información fueran restaurados con un tiempo posterior altamente tardío.

Hoy en día, la prevención del evento y la minimización del impacto tras un evento fallido son el principal enfoque que tiene un BCM (Business Continuity Management).

En (Martínez, 2006), se presenta una guía práctica en la cual se establecen las pautas y premisas de los impactos producidos por los desastres y las pérdidas en las que pueden incurrir las empresas tras eventos nefastos, como también contempla la evaluación de los elementos críticos y estrategias de recuperación necesarias.

Es fundamental para elaborar un Plan de Continuidad y Contingencia realizar un Análisis de Riesgos, en las organizaciones este proceso se conoce como Gestión del Riesgo ó Administración del Riesgo ya que contempla todo el proceso desde su identificación, valoración del riesgo y el impacto, medición, tratamiento y monitoreo.

La Norma (ICONTEC, 2011), define el riesgo como aquel efecto de incertidumbre sobre los objetivos, una desviación de aquello que se espera sea positivo, negativo, o ambos. La Norma también define que con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo los cambios en las circunstancias) y en la probabilidad (likelihood) que se utiliza para hacer referencia a la oportunidad de que algo suceda, esté o no este definido, medido o determinado subjetivamente, cualitativa o cuantitativamente, ó bien puede decirse o expresarse como frecuencia en un periodo determinado.

Para (Mejía Quijano, 2006) en su libro “Administración de riesgos. Un enfoque empresarial” resalta que la palabra “riesgo” viene del Italiano Risicare, que significa desafiar, retar, enfrentar, atreverse.

Otras definiciones de riesgo encontradas en este libro describen el riesgo como una probabilidad de pérdida, incertidumbre, dispersión del resultado actual con el esperado, amenaza evaluada en cuanto a posibilidad de ocurrencia y gravedad de consecuencia.

El riesgo en lo relacionado con la tecnología, se plantea directamente con la amenaza, y especificar el grado de exposición a la ocurrencia de una pérdida (riesgo de perder datos por virus informáticos, roturas de un disco, etc.)

De acuerdo con la ISO (Organización Internacional de Normalización) define el riesgo tecnológico como: “La probabilidad que una amenaza se materialice utilizando vulnerabilidad existente de un activo o de un grupo de activos, generando pérdidas o daños”.

Lo más importante es tener presente que el riesgo informático siempre va a estar presente y que se deben implementar los mecanismos necesarios para prevenirlos y permitir que la organización continúe con su normal funcionamiento si un evento de riesgo se materializa.

La elaboración y puesta en marcha de un Plan de Continuidad y Contingencia comprende entonces un Análisis de riesgos, Identificación de las Vulnerabilidades de la Compañía, la identificación de aquellos Servicios Críticos sobre los cuales se aplican los Planes de Continuidad y Contingencia, y los Niveles de Disponibilidad deseados para cada servicio crítico.

CAPITULO 2. ANÁLISIS DE RIESGOS Y VULNERABILIDADES

Según la Norma (ICONTEC, Gestión del Riesgo. Principios y directrices NTC-ISO 31000, 2011). “Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si ellas lograran o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el Riesgo”

Para (Mejía Quijano, 2006) los riesgos se clasifican en cuatro grupos principales:

- Riesgos del Entorno: el entorno de una organización abarca muchos elementos e impacta con los niveles culturales de la región donde se encuentran diferentes según la región donde se instala la empresa.

- Riesgos asociados por la naturaleza: estos riesgos están relacionados con los fenómenos climáticos, huracanes, lluvias, inundaciones, terremotos, epidemias, virus etc; Y los que las organizaciones pueden generar y afectar el medio ambiente.

- Riesgos asociados al País, la región o la ciudad donde se encuentra ubicada la organización. Dependiendo de una serie de ítems económicos, políticos, etc. Aumenta o disminuye el nivel de riesgo.

- Riesgos Asociados al sector económico y de la industria, se debe tomar en cuenta las campañas que puedan tener los competidores que son a veces de desprestigio, espionaje, etc.

Desde la perspectiva de la empresa se tienen un sin número de riesgos, que se generan por el entorno que influye en la empresa, además del desarrollo normal de las actividades, entre estos se destacan distintos tipos de riesgo que afectan a una empresa de distintas formas:

- Riesgo de reputación: Se trata de pérdida de credibilidad y confianza por parte de la sociedad bien sea por fraudes, insolvencias, conductas erróneas por parte de los empleados, etc. Este riesgo causa pérdidas principalmente en lo que respecta a la disminución de demanda del producto que ofrece la organización.

- Riesgo puro y especulativo: el primero origina pérdidas como es el caso de un incendio o una inundación; en el segundo se da por malas inversiones financieras.

- Riesgo de mercado: Son inversiones financieras mal realizadas, pero sólo en el caso de inversiones en el bolsa, y malas inversiones con insumos y productos.

- Riesgo de crédito: Es un riesgo definido como la pérdida de dinero, cuando un cliente falla en pagos a la organización; otro ejemplo de este es también es la insolvencia en CDT's bonos de deuda entre otros.

- Riesgo tecnológico: se plantea directamente con la amenaza, y el grado de exposición a la ocurrencia una pérdida (riesgo de perder datos por virus informáticos, roturas de un disco, etc.).

- Riesgo físico: Es el riego que afecta no sólo el recurso humano, sino también las instalaciones y todo lo que se encuentra dentro de la organización.

Para trabajar con los procesos en la Administración de los Riesgos, se tiene que tener en siempre presente, que además de los procesos operados en una organización, cada proyecto nuevo a realizarse debe contemplar la evaluación de los riesgos, puede resultar que el proyecto no puede hacerse o debe tener modificaciones para que pueda ser realizado.

A continuación se presentan las etapas para la administración de los riesgos empresariales figura 1, (ICONTEC, 2011):

a. Identificación de los riesgos.

b. Calificación de los riesgos.

c. Evaluación de los riesgos.

d. Diseño de medidas de tratamiento.

e. Implementación de las medidas.

f. Monitoreo y evaluación.

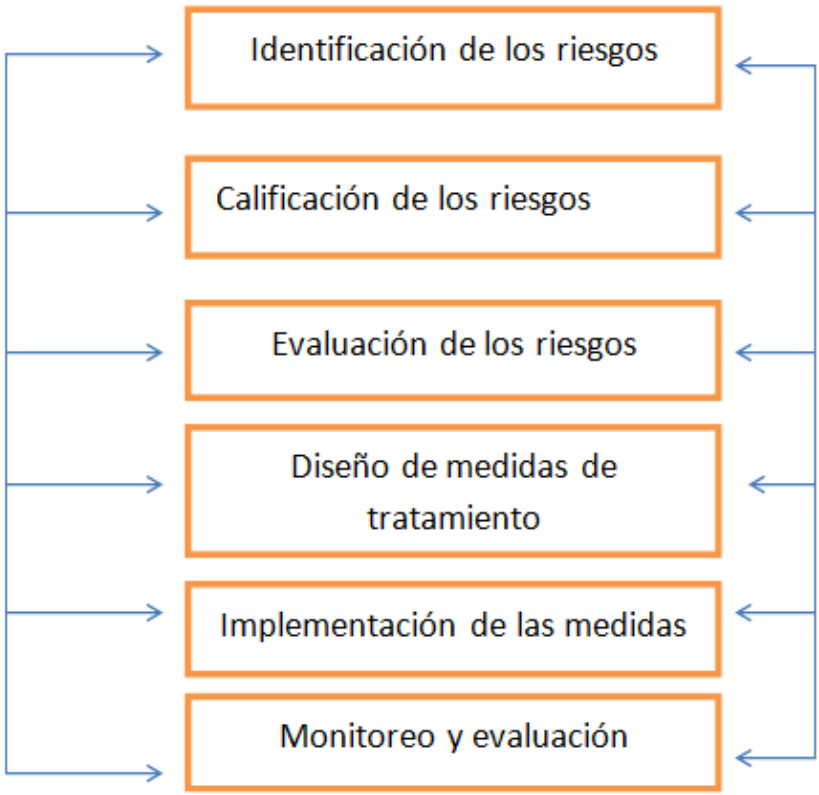

Figura 1. Etapas de la Administración del riesgo (Mejía Quijano, 2006)

2.1 IDENTIFICAR Y ANALIZAR LOS RIESGOS

Gran parte del éxito de tener un Plan de Continuidad y Contingencia tiene que ver la identificación de los riesgos, al identificarlos, analizarlos y evaluarlos se puede concebir a que se está expuesto y que controles se debe implementar con el fin de mitigarlos o asumirlos si este riesgo al materializarse no causa un efecto mayor.

Si bien la creación y la aplicación de procesos de manera eficiente mitigan el impacto si un riesgo llega a materializarse es importante valorar el impacto riesgo por mínimo que parezca.

La identificación de los riesgos es una de las etapas más determinantes en lo que tiene que ver con la administración de los riesgos. En este punto la organización y

sus empleados se dan cuenta de aquellas situaciones y peligros potenciales a los que se pueden tener y cómo actuar cuando estos se presenten.

“Entre los métodos de identificación de riesgos, se puede encontrar una gran variedad, como el método Hazop, el árbol de fallas, el árbol de eventos y otros incluidos en las diferentes metodologías de identificación y evaluación de riesgos.

Cualquiera de las herramientas o métodos utilizados tiene como propósito establecer los posibles eventos que puedan presentarse y afectar de algún modo el cumplimiento de los objetivos, bien sea del proceso, del proyecto, la actividad, la unidad del negocio o el ámbito en el que se realiza la identificación de los riesgos” (Mejía Quijano, 2006).

Lo que en definitiva se busca con esta primera etapa es dejar claro las alternativas que ayudan a prevenir que haya riesgos en la empresa, bajar el número de las ocurrencias y disminuir las consecuencias cuando estos se presenten.

Una vez identificados los riesgos se deberá determinar la magnitud, es decir, expresar que tan significativos son para la empresa. Es así como se tendrá que identificar la probabilidad del riesgo y el impacto que este pueda tener.

Existen distintas maneras para establecer la calificación de un riesgo:

Según (Mejía Quijano, 2006), estos pueden ser cualitativos o cuantitativos, los primeros, definen rangos de variables cualitativas como alto, medio o bajo y de igual manera su impacto grave, leve, entre otros. Los segundos, se orientan a representaciones matemáticas donde los valores de las variables pueden establecer tendencias y definir viabilidades. Un riesgo también puede ser defiinido a través de variables semi-cuantitativas en las cuales se enlazan las dos anteriores.

Una vez identificados los riesgos y al clasificarlos se puede tener una idea más clara de que elementos se deben fortalecer, la “Perdida del servicio prestado al usuario o cliente por fallas en los sistemas de información” es un riesgo que puede afectar a la organización, al clasificarlo se puede decir que dicho riesgo puede ser operativo ya que afecta directamente la operación de la compañía, o bien podría materializarse como riesgo financiero ya que incurre en costos por perdida de servicio y disponibilidad, este mismo riesgo afecta el cumplimento y se materializa directamente en Tecnología por lo que también es un riesgo tecnológico, esta consideración se conoce un factor de riesgo.

La clasificación de los riesgos depende de la naturaleza de cada negocio y cada empresa, su análisis y evaluación depende las condiciones que se establezcan según sus servicios y el impacto considerable que pueden causar un riesgo de llegar a materializarse.

2.2 EVALUACIÓN Y VALORACIÓN DEL RIESGO

En esta etapa se estudia las calificaciones que entregan los riesgos en la etapa de identificación y se determina la situación en la que se encuentra la organización respecto a los riesgo; por medio de la evaluación se facilita el diseño de planes de manejo de acuerdo con un rango de prioridades, definidas en relación con la gravedad de los riesgos previamente identificados.

Aquí, se debe utilizar un modelo que permita clasificar cada riesgo de acuerdo con su naturaleza, en un rango que represente el grado de exposición de la organización ante el riesgo. Es así como se usan criterios que pueden establecer de acuerdo con el nivel de tolerancia del riesgo, definido por los altos mandos de la empresa. Según (Mejía Quijano, 2006), los niveles pueden pasar por ser aceptables cuando es un riesgo de peligro muy bajo, hasta inaceptable cuando es tan peligroso que debe ser evitado y contralado rápidamente

En este parte es fundamental que la empresa sea consciente que las mediciones deben ser consecuentes con la realidad de sus actividades, procesos y procedimientos que desarrolla, una valoración inadecuada podría ocasionar que un riesgo sea controlado de manera eficiente y en el peor de los casos ni siquiera se identifique.

2.3 DISEÑO DE MEDIDAS DE TRATAMIENTO DE LOS RIESGOS

Cuando se haya realizado la identificación y la evaluación de los riesgos, se toma la decisión de cuáles medidas se van a tener. Es decir se obtienen las medidas de control de riesgos como: evitar y prevenir y las de medidas de financiamiento como: aceptación, retención o transferencia. Estas medidas servirán como los parámetros para el tratamiento ante cualquier riesgo (Mejía Quijano, 2006).

A continuación se detalla cada uno de estos parámetros:

- Evitar: es no emprender un nuevo proyecto evaluado como no viable, eliminando la actividad que genera un riesgo o sustituyéndola por otra que no sea tan peligrosa o que no produzca tantas pérdidas.

- Prevenir: se toman medidas en que la probabilidad que un riesgo ocurra disminuya. Algunas medidas de prevención se ven enfocadas en el diseño de procedimientos, políticas de selección, capacitación y entrenamiento del personal de la empresa.

- Proteger: se diseñan medidas que deben actuar sobre los recursos amenazados (personas, materiales, información, entre otros) para evitar pérdidas en el evento de que un riesgo se haga presente. El caso concreto de la protección se ve como por ejemplo el plan de manejo de crisis es una herramienta para proteger la organización.

- Transferir: es trasladar las pérdidas a otras empresas, a través de la elaboración de arreglos por medio de contratos de seguros; en esta medida el asegurador se hace responsable de aquellas pérdidas que se tengan por cuenta de los riesgos. Otra manera de transferencia de riesgos se hace mediante el outsourcing o la contratación de actividades tales como: servicios de alto riesgo, transporte, vigilancia, entre otros.

- Aceptar: asumir las consecuencias que implica un riesgo cuando se presenta. Los riesgos se aceptan cuando la frecuencia es baja y el impacto es leve, y por ende no hay peligro en lo que tiene que ver con la estabilidad de la organización. La aceptación de un riesgo se hace de manera muy crítica cando en el mercado no hay medidas que se adoptan para la aceptación del mismo.

- Retener: a través de la creación de un fondo, de una cuenta de gasto, etc. responder de manera inmediata por las pérdidas causadas debido a la aparición de un riesgo.

En la Implementación de las medidas de tratamientos de riesgos se pretende dejar claros los planes y las acciones que corresponden a cada proceso, proyecto o unidad de negocio donde se analizó previamente los riesgos.

Ante todo se necesita establecer un programa que garantice que los planes se aprueben, se analicen y se les asigne prioridades en su implementación: tales como fechas límite, personas responsables y los recursos que se necesitan para ser llevados a cabo como se muestra en la figura 2 (Mejía Quijano, 2006).

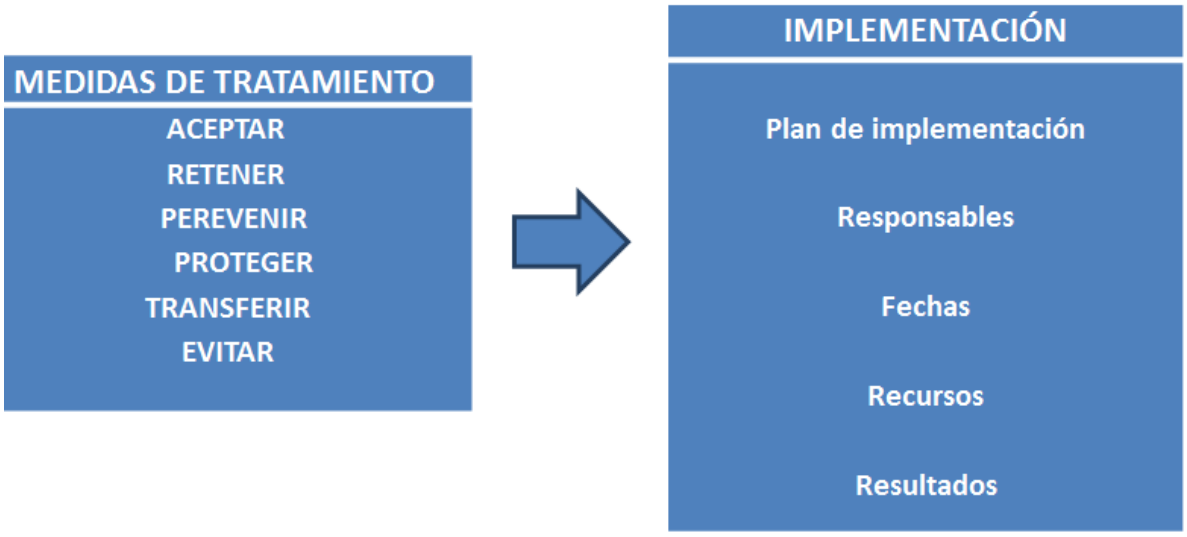

Figura 2. Implementación de medidas de tratamiento de riesgos (Mejía Quijano, 2006).

2.4 MONITOREO Y EVALUACIÓN DE RIESGOS

El monitoreo y la evaluación de los riesgos, se generan cambios que en el futuro afectan a la organización y a su entorno, porque traen no sólo nuevas oportunidades, sino también nuevos riesgos.

Otro aspecto del porqué de la realización del monitoreo y la evaluación de riesgos, es que con ésta medida se puede revisar las decisiones tomadas y encontrar los errores en la identificación y evaluación de riesgos, lo cual permite enrutar nuevamente el plan de implementación. En la figura 3. Se presenta un modelo de monitoreo y evaluación presentado en (Mejía Quijano, 2006).

En esta parte, lo que se necesita es tener claros los indicadores de riesgo acorde a la frecuencia y ocurrencia de los mismos además de tener en cuenta el impacto y las consecuencias. Además, se debe tener en cuenta lo que tiene que ver con la autoevaluación, por medio de ésta, se realiza un diagnóstico sobre la aplicación, y se vigila se cuenten con todos los elementos necesarios para que el análisis de riesgo sea exitoso. Finalmente, se tiene la evaluación independiente, la cual puede ser realizada por un auditor interno o por uno externo. Es así como al final se complementa la autoevaluación y la etapa de monitoreo de los riesgos lo que permite que se tenga un mejoramiento continuo.

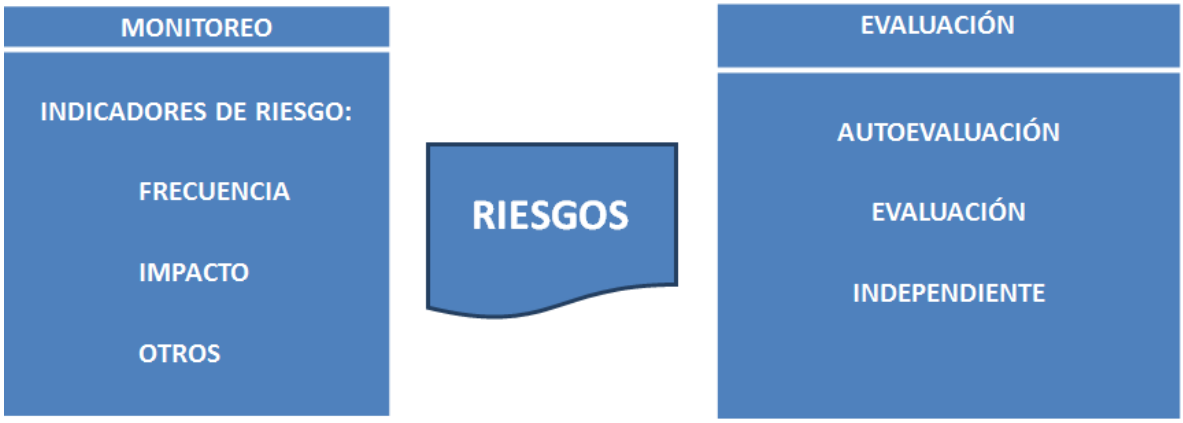

Figura 3. Evaluación y monitoreo de los riesgos (Mejía Quijano, 2006).

2.5 ANÁLISIS DE VULNERABILIDADES

La seguridad es un factor muy importante y es un aspecto cambiante en las organizaciones por lo tanto, no solo es importante identificar los riesgos sino también realizar periódicamente análisis de vulnerabilidades por medio de pruebas de penetración las cuales nos permiten identificar las brechas de seguridad.

Es fundamental definir el alcance de estas pruebas ya que pueden ser realizadas por proveedores de manera interna y externa, en este sentido la confidencialidad prima un papel importante. En este punto en especial se considera importante definir una política de aplicación de estas pruebas y considerar un plazo de tiempo para aplicar los parches y actualizaciones sugeridas para mejorar la seguridad en las brechas encontradas en el análisis. Por lo tanto, se sugiere generar un Informe destinado a gerentes informáticos donde se puede tener una vista instantánea y real del estado de seguridad de la infraestructura analizada y un informe mucho mas detallado que evidencia las distintas vulnerabilidades.

CAPITULO 3. IDENTIFICACIÓN DE LOS SERVICIOS CRÍTICOS

Al conocer los riesgos y sus vulnerabilidades las compañías pueden realizar un mejor control y desarrollo de estrategias en sus Planes de Continuidad y Contingencia relacionados con las con las TIC´s (Tecnologías de la información y la comunicación).

La identificación de servicios críticos realizado por una empresa puede abarcar no solo el software principal sino también un conjunto de componentes entre los cuales se pueden incluir servidores, enlaces de comunicación y base de datos criticas.

En la figura 4, se muestra el proceso de identificación de los servicios críticos, aquí, se reúne los elementos necesarios y útiles para que una empresa puede concebir de manera eficiente las estrategias para el diseño de los Plan de Continuidad y Contingencia del Negocio, es decir que este punto es muy importante para poder establecer a que servicios y procesos se les realiza un Plan de Continuidad y cuales un Plan de Contingencia, teniendo presente que la Continuidad se establece sobre los servicios críticos y la Contingencia sobre un proceso, actividad o elemento especifico.

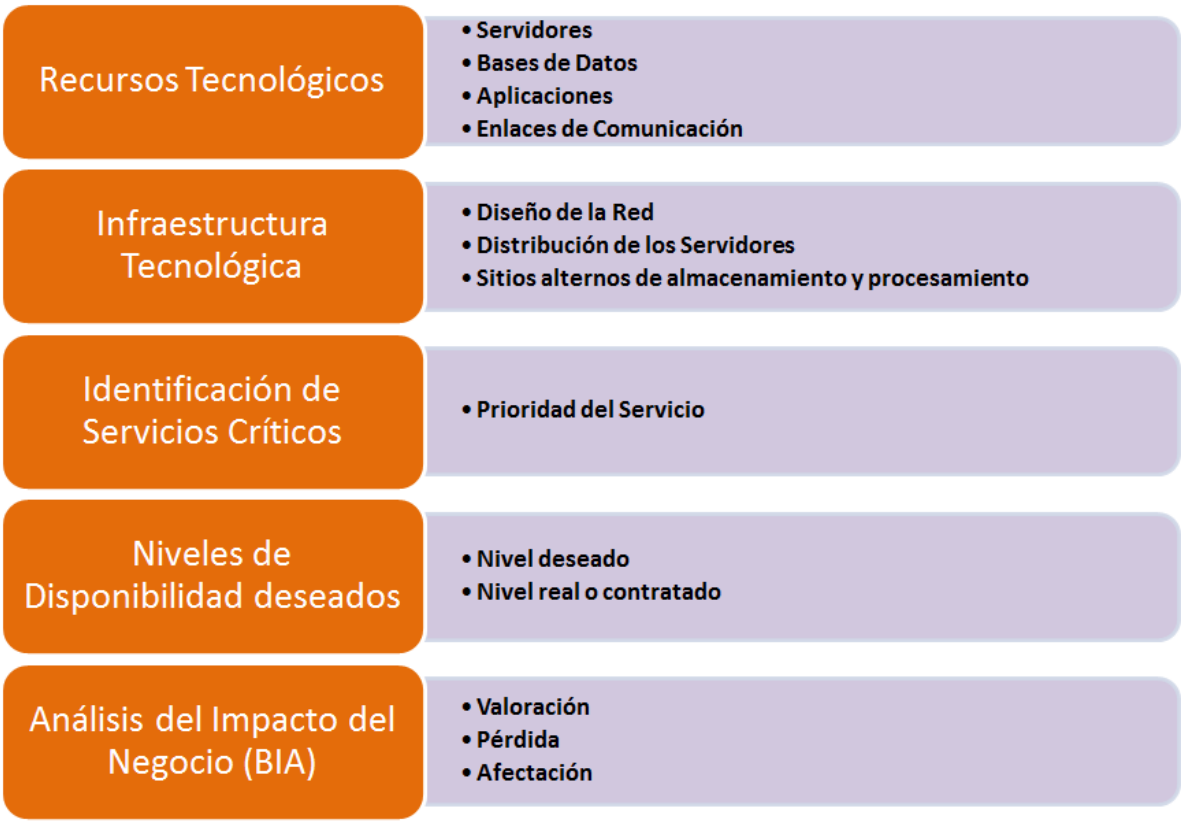

Figura 4. Proceso de identificación de los servicios críticos

3.1 RECURSOS TECNOLÓGICOS

Un Recurso Tecnológico, es el medio que se vale de la tecnología para lograr un propósito. Estos pueden ser tangibles como un servidor o intangibles como una aplicación. La identificación de los recursos tecnológicos dimensiona la magnitud y la trascendencia que tiene la aplicación de los planes de continuidad y contingencia de las empresas por lo tanto es importante tener un control preciso de los activos tecnológicos entre los cuales están: servidores, bases de datos, aplicaciones, hardware, dispositivos de almacenamiento, licencias, entre otros.

Las áreas de TI deben identificar que recursos tecnológicos tienen relación con los servicios críticos de la compañía. La figura 5, muestra como cada elemento identificado desde un comienzo, establece su objetividad hacia el servicio y de esta manera define que recursos operan como en modo critico para la organización a nivel operativo y cuales son contingencia de estos servicios principales.

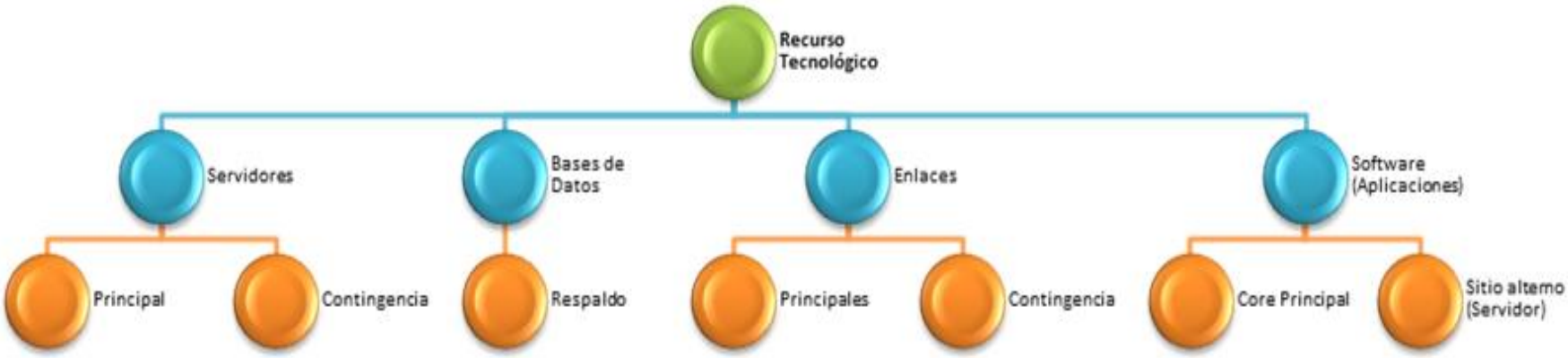

Figura 5. Recursos tecnológicos

La tabla 1, presenta un ejemplo de cómo podría relacionarse los elementos y servicios con activos y cuáles de ellos operan como alternativa ante una falla. En la columna de Servicio se puede visualizar el Core (Activo) y un servidor igual Core (Pasivo) el cual es la Contingencia.

SERVIDORES										
FISICOS										
CÓDIGO	SEDE	UBICACIÓN	SERVICIO	SISTEMA OPERATIVO	Marca y Modelo	Caracteristicas Generales			Promedio de Carga Procesamiento	Porcentaje Almacenamiento Disponible
						Procesador	Disco Duro	Memoria		
SER003	MEDELLÍN	DATACENTER	CORE SERVICE (ACTIVO)	WINDOWS SERVER 2008	Servidor en rack PowerEdge R520	E5-2400 del procesador Intel® Xeon®	2TB (Hasta 24 TB)	32 GB (Hasta 192 GB)	25%	65%
SER004	MEDELLÍN	DATACENTER	CORE SERVICE (PASIVO)	WINDOWS SERVER 2008	Servidor en rack PowerEdge R520	E5-2400 del procesador Intel® Xeon®	2TB (Hasta 24 TB)	32 GB (Hasta 192 GB)	9%	65%

Tabla 1. Ejemplo de relación activo, pasivo

3.2 INFRAESTRUCTURA TECNOLÓGICA

La adecuada estructuración de la red y el diseño de la misma es importante para tener claridad sobre qué servicios y en que elementos se aplica la Contingencia y sobre cuales la Continuidad, tener una noción gráfica de esta infraestructura permite identificar de manera mas ágil el origen de una incidencia, dimensionar su afectación y brindar un soporte oportuno a la operación afectando mínimamente la disponibilidad.

En la figura 6, se presenta un ejemplo de servidores principales del Core del Negocio ubicados en el DataCenter Medellín, los cuales tienen un conjunto de equipos de similar configuración que comparten servicios comunes o que uno soporta al otro en caso de presentarse una incidencia.

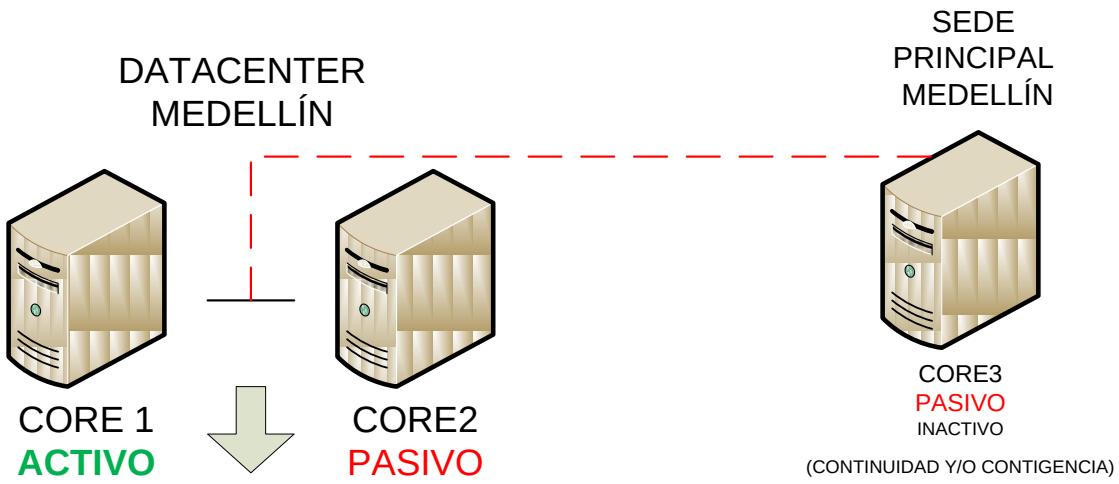

Figura 6. Ejemplo de una estructura y distribución de servidores

En la grafica anterior, se puede identificar un Servidor Core3 que es igual a los del DataCenter como aplicación al Plan de Continuidad, es decir si por algún evento de fuerza mayor el DataCenter no es Operativo se puede restaurar el Servicio desde otra sede diferente que se tenga establecido dentro del Plan de Continuidad como Sitio alterno de procesamiento.

Otros Servidores para otros servicios no tan críticos se pueden ubicar en otras locaciones y tener ubicaciones de respaldó con las mismas configuraciones previo

análisis de todas las partes involucradas en el servicio prestado a los clientes de una organización.

La figura 7, muestra la forma como una empresa puede identificar sus enlaces principales y sus enlaces de contingencia. Aquí, se visualizan 4 sedes de una empresa y su servicio principal en un DataCenter. De color rojo, el enlace principal y de color azul la contingencia de cada canal con un proveedor diferente enrutando todo el tráfico de la red al sitio alterno de procesamiento.

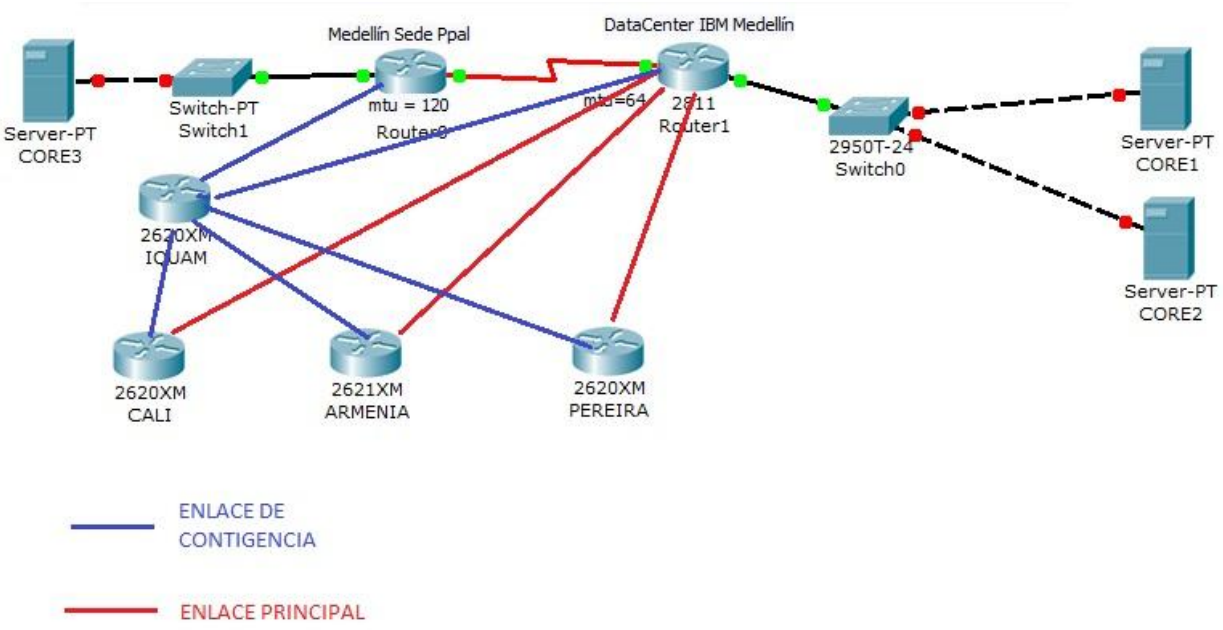

Figura 7. Ejemplo de enlaces y comunicaciones

Es importante para toda organización tener claro los alcances y la disponibilidad ofrecida por los proveedores, identificar de manera precisa las diferentes alternativas o caminos cuando un enlace falle.

3.3 IDENTIFICACIÓN DE SERVICIOS CRÍTICOS

La identificación de Servicios Críticos permite tener claridad sobre la importancia de las aplicaciones y de los elemento de TI, cada compañía puede identificar sus servicios críticos y clasificarlos según sus escalas de medición.

No se descarta la importancia de los demás servidores pero la finalidad de identificar los servicios críticos es precisamente preservar la continuidad del negocio y clasificarse según su prioridad por tiempo de respuesta en la solución de una incidencia o por el impacto que ejerza el servicio sobre el negocio.

3.4 NIVELES DESEADOS DE DISPONIBILIDAD

Los niveles de disponibilidad deseados se establecen según la criticidad de los servicios, en este sentido los niveles de disponibilidad pueden depender de factores internos o bien externos como por ejemplo las incidencias que los proveedores puedan tener en sus sistemas influyendo directamente el servicio que se presta.

Si bien las áreas de tecnología conjuntamente con la gerencia establecen los niveles de disponibilidad deseados, es necesario identificar los riesgos y tener claridad con los acuerdos definidos con los terceros.

Un nivel de disponibilidad deseado debe convertirse en un objetivo claro para lograr la estabilidad del servicio y de esta manera estratégicamente lograr mantener un nivel de disponibilidad superior al 90% siendo este porcentaje algo hipotético ya que cada organización lo establece según sus análisis.

Si bien aunque toda organización desearía tener una disponibilidad del 100% difícilmente se puede garantizar, aun más cuando la tecnología puede fallar en cualquier momento.

La Disponibilidad se puede medir por horas y generalmente se mide mensualmente, al mes se tendrá 720 horas. A partir de este dato, se puede establecer los niveles deseados.

Estos niveles, se aplican sobre los servicios, aplicaciones, comunicaciones definiendo, su hora y porcentaje.

En la Tabla 2., se presenta un ejemplo de la identificación de los servicios críticos en un Empresa.

El análisis periódico de estas mediciones es un factor relevante para la toma de decisiones en cuanto al mejoramiento continúo del servicio de TI se refiere, su análisis permite no solo comprometer a la organización a lograr los niveles

deseados sino también establecer un compromiso con proveedores y miembros directos e indirectos de la organización.

NIVELES DE DISPONIBILIDAD DESEADOS					
SERVICIOS					
CÓDIGO	SERVICIO	DISPONIBILIDAD DESEADA /MES Base: 720 Horas Mes		DISPONIBILIDAD ACORDADA /MES Base: 720 Horas Mes	
		En Horas	Porcentaje	En Horas	Porcentaje
SVC001	XXXXXXXXX	718	99,72%	710	98,61%
SVC002	XXXXXXXXX	600	83,33%	650	90,28%
SVC003	XXXXXXXXX	690	95,83%	700	97,22%
SVC004	XXXXXXXXX	700	97,22%	715	99,31%
SVC005	XXXXXXXXX	700	97,22%	710	98,61%
SERVIDORES					
CÓDIGO	SERVICIO	DISPONIBILIDAD DESEADA /MES Base: 720 Horas Mes		DISPONIBILIDAD ACORDADA /MES Base: 720 Horas Mes	
		En Horas	Porcentaje	En Horas	Porcentaje
SER001	XXXXXXXXX	710	98,61%	700	97,22%
SER002	XXXXXXXXX	710	98,61%	710	98,61%
SER003	XXXXXXXXX	718	99,72%	710	98,61%
SER004	XXXXXXXXX	718	99,72%	710	98,61%
SER005	XXXXXXXXX	708	98,33%	700	97,22%

Tabla 2. Niveles deseados de disponibilidad.

Sobre cada servicio crítico se sugiere implementar un procedimiento o Plan de Contingencia ó Continuidad según las características de disponibilidad y tanto actividades como responsabilidades de cada proceso.

3.5 ANÁLISIS DEL IMPACTO DEL NEGOCIO (BIA)

El Análisis del Impacto en el negocio (BIA – Business Impact Analysis) consiste en técnicas y metodologías usadas para identificar, cuantificar y calificar los impactos de negocio y sus efectos en una organización en caso de pérdida o interrupción de los servicios críticos, la clave para realizar este análisis es tomar el negocio como un todo y no como componentes aislados.

Este análisis también tiene en cuenta el RTO (Recovery Time Objetive) que es aquél tiempo entre el punto de interrupción y el punto en el cuál la se cuenta con la

disponibilidad del servicio, el RPO (Recovery Point Objetivo) es el punto en cuál fueron interrumpidas las operaciones debido a la ocurrencia de un evento (Rodríguez Lache, 2009).

Después de realizarse un previa gestión del riesgo donde se identifican aquellos riesgos que pueden afectar los servicios críticos del negocio, se estable una probabilidad de ocurrencia la cual es valorada por cada Compañía, esta probabilidad puede medirse por número de eventos al año o al mes y se le da una valoración la cual es el nivel de importancia cuantitativa de ese riesgo.

Las tabla 3 y 4 muestran un ejemplo para establecer la probabilidad de ocurrencia de un riesgo y la medición del impacto respectivamente.

TABLA DE PROBABILIDAD			
ESCALA	PROBABILIDAD	NÚMERO DE EVENTOS	VALORACIÓN
IMPROBABLE	Entre el 0% y el 3%	Entre 0 y 10 eventos en un año	1
REMOTO	Entre el 4% y el 6%	Entre 0 y 10 eventos en un año	2
OCACIONAL	Entre el 7% y el 9%	Entre 0 y 10 eventos en un año	3
FRECUENTE	Entre el 10% y el 15%	Entre 0 y 10 eventos en un año	4
CONSTANTE	Entre el 16% y el 100%	Entre 0 y 10 eventos en un año	5

Tabla 3. Ejemplo para establecer un riesgo.

TABLA DE IMPACTO				
ESCALA	OPERACIONAL	ECONÓMICO	IMAGEN	VALORACIÓN
INSIGNIFICANTE	Interrupción entre 2 y 5 minutos	Perdidas hasta $ 1'000.000	No afecta las relaciones con el Cliente	1
MODERADO	Interrupción entre 6 minutos y 1 hora	Perdidas entre un $ 1'000.000 y $ 5'000.000	Puede afectar las relaciones con el cliente pero es manejable.	2
GRAVE	Interrupción entre 1 hora y 12 horas	Perdidas entre un $ 5'000.001 y $ 25'000.000	Afecta la relación con los clientes.	3
CRÍTICO	Interrupción entre 13 horas y 24 horas	Perdidas entre un $ 25'000.001 y $ 125'000.000	Afecta la relación con los clientes y nuevos proyectos.	4
CATASTRÓFICO	Interrupción entre 24 horas y 3 días	Perdidas entre un $ 125'000.001 y $ 780'000.000	Afecta la relación con los clientes y nuevos proyectos.	5

Tabla 4. Ejemplo para la medición del impacto.

CAPITULO 4. PLANES DE CONTINUIDAD Y CONTINGENCIA

Los Planes de Continuidad a diferencia de un Plan de Contingencia están orientados al mantenimiento de las operaciones criticas necesarias para continuar operando después un incidente no planificado. (BSI British Standards - BS 25777:2008, 2008).

El Plan de Continuidad del Negocio de las TIC´s (tecnologías de la información y de la comunicación) son parte integral en la estrategia en los servicios de gestión de las TIC´s que son alineados con la estrategia organizacional.

La Continuidad en las TIC´s se basa en seis principios fundamentales según la Norma (BSI British Standards - BS 25777:2008, 2008) y presentados en la figura 8:

a) Proteger: proteger el ambiente de las TIC de incidentes, fallas e interrupciones, mejorando la capacidad de recuperación de los servicios de TIC para mantener los niveles deseados para una organización.

b) Detectar: detectar los incidentes en la primera oportunidad minimizará el impacto en los servicios, reducirá el esfuerzo de recuperación, y preservará la calidad del servicio.

c) Reaccionar: reaccionar a un incidente de la manera más adecuado dará lugar a una recuperación más eficiente y reducirá al mínimo cualquier tiempo de inactividad.

d) Recuperar: identificar e implementar la estrategia de recuperación adecuada, garantizará la pronta reanudación de los servicios y mantendrá la integridad de los datos, entendiendo las prioridades de recuperación, permite que los servicios más críticos sean reintegrados primeramente. Los servicios de una naturaleza menos crítica pueden ser reintegrados posteriormente en unas circunstancias, no en todas.

e) Operar: la ejecución en modo de recuperación de desastres en las TIC, hasta el retorno a la operatividad normal.

f) Retornar: la elaboración de una estrategia para cada plan de continuidad de las TIC, que permita a una organización migrar de vuelta de un modo de recuperación

de desastres de las TIC a una posición en la que puede soportar la actividad comercial de la Organización.

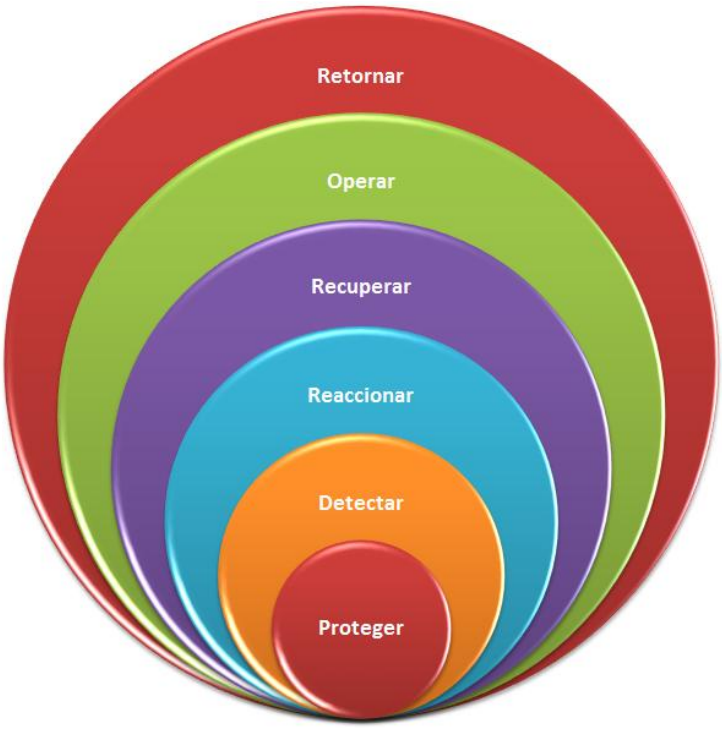

Figura 8. Principios fundamentales para la continuidad en las TIC's (BSI British Standards - BS 25777:2008, 2008)

La incorporación de un Plan de Continuidad y Contingencia abarca entonces los elementos descritos en los capítulos anteriores 2 y 3 respectivamente, la figura 9. muestra los elementos necesarios para su eficiente desarrollo.

Figura 9. Hacia la continuidad del negocio

4.1 TIEMPO OBJETIVO DE RECUPERACIÓN

El Objetivo de Tiempo de Recuperación (OTR), es el tiempo fijado para la reanudación del servicio entregado y ofrecido después de un incidente (BSI British Standards - BS 25777:2008, 2008).

Es recomendable que este tiempo sea fijado según la experiencia recopilada en incidentes anteriores y ser muy consecuentes en los tiempos fijados, para no desbordar los tiempos e incurrir en tiempos objetivos que tal vez no se van a conseguir por una planificación desacertada. Además, es ideal establecer un tiempo según la criticidad del servicio y el tipo de incidencia ya que estos 2 elementos proporcionan y determinan que el plan debe seguirse según los procedimientos establecidos por la compañía.

La tabla 5., presenta un ejemplo de cómo una compañía puede identificar los servicios críticos y (OTR), que se establecen asociados a una posible incidencia.

OBJETIVO TIEMPO DE RECUPERACIÓN (OTR)				
SERVICIOS				
CÓDIGO	**SERVICIO**	**INCIDENCIA**	**Tiempo de solución esimado a incidencia**	**OTR - Objetivo de Tiempo de Recuperación**
			En Minutos	**En Minutos**
SVC001	XXXXXXX	Bloqueo del Servicio	5	15
		Alto Performance del Servidor	8	15
		Problemas de Replicación de la Base de Datos	5	15
SERVIDORES				
CÓDIGO	**SERVICIO**	**INCIDENCIA**	**Tiempo de solución esimado a incidencia**	**OTR - Objetivo de Tiempo de Recuperación**
			En Minutos	**En Minutos**
SER003	XXXXXXX	Daño en Hardware	25	20
		Alto Performance del Servidor	10	15
		Denegación de Servicio por incidencia de seguridad	20	15
SER004	XXXXXXX	Daño en Hardware	25	15
		Alto Performance del Servidor	10	15
		Denegación de Servicio por incidencia de seguridad	20	15
COMUNICACIONES				
CÓDIGO	**SERVICIO**	**INCIDENCIA**	**Tiempo de solución esimado a incidencia**	**OTR - Objetivo de Tiempo de Recuperación**
			En Minutos	**En Minutos**
ENL001	XXXXXXX	Dispositivos de Comunicaciones	10	15
		Ultima milla	10	15
		Daño en tramos de fibra	10	15
ENL002	XXXXXXX	Dispositivos de Comunicaciones	10	15
		Ultima milla	10	15
		Daño en tramos de fibra	10	15

Tabla 5. Ejemplo de OTR

Es importante resaltar que se puede establecer un tiempo de solución a una incidencia y si este tiempo es superado puede contemplarse la invocación de un Plan de Contingencia hacia un Plan de Continuidad en el sitio alterno.

El OTR no contempla en la norma si este tiempo es tomado sobre la solución a la incidencia o si involucra la invocación del Plan de Contingencia abarcando el tiempo total que se tomo la reanudación del servicio una vez se vio suspendido.

Un ejemplo es presentado en la figura 10.

4.2 PUNTO OBJETIVO DE RECUPERACIÓN

El (OPR) Punto Objetivo de Recuperación es punto referido a los datos y es aquella instancia en que los datos deben ser recuperados con el fin de reanudar los servicios de TIC.

Este tiempo puede utilizarse al definir la disponibilidad de los datos cuando se presenta una incidencia, sin embargo este tiempo es de consideración de la Empresa a la hora de aplicar sus estimaciones ya que pueden reunirse los criterios de servicio y datos en un mismo tiempo (OTR) (BSI British Standards - BS 25777:2008, 2008).

4.3 ALTERNATIVAS A FALLOS

Las alternativas a fallos permiten tener claridad de que hacer o que alternativa tomar ante la ocurrencia de un evento o incidencia.

Estas alternativas pueden quedar consignadas en el desarrollo de las actividades de cada procedimiento en los Planes de Contingencia o bien relacionar cada incidencia con una alternativa ante esa falla, por ejemplo si se presenta un problema que afecte la red local cableada una alternativa es habilitar la Red Inalámbrica para dar disponibilidad.

Las alternativas a fallos pueden incorporarse en las estrategias de cada Plan de Continuidad y Contingencia o bien dentro de la descripción de cada actividad de los planos bajo la responsabilidad de un miembro de TI.

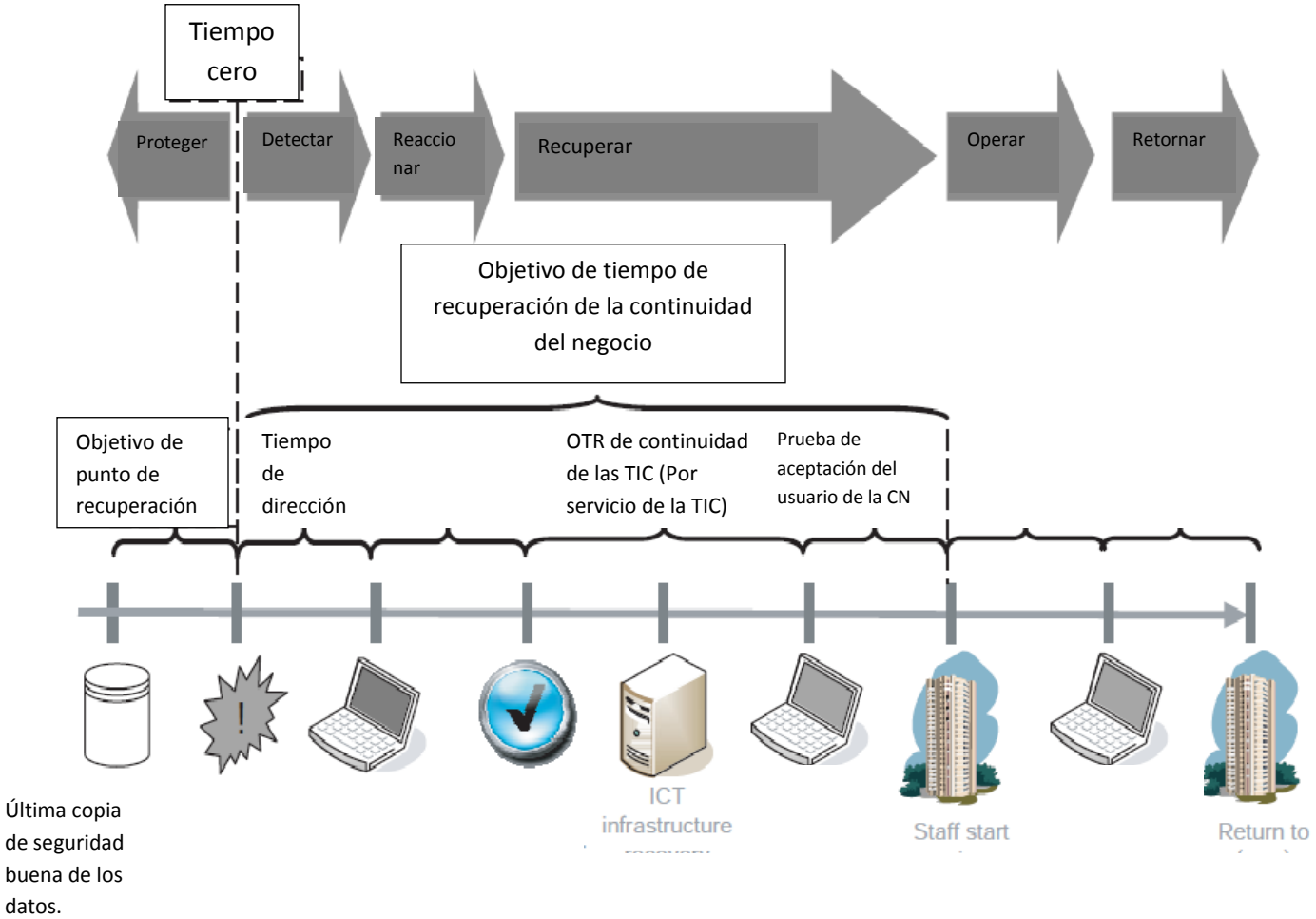

Figura 10. Escalas de tiempo claves en la gestión de continuidad de las TIC's (BSI British Standards - BS 25777:2008, 2008).

4.4 PLANES DE CONTINUIDAD DEL NEGOCIO

EL Plan de Continuidad del Negocio abarca una colección de documentos y procedimientos que deben estar disponible para su uso en caso de incidencia y que su correcta ejecución, permite a la organización seguir ofreciendo sus actividades críticas en un nivel aceptable definido, la estructuración inadecuada puede incurrir en un riesgo humano que afecte la Continuidad del Servicio o retrase la normalización de las actividades propias del Negocio.

Se debe definir el alcance del plan de continuidad, definir las responsabilidades y los procedimientos de ejecución ante una incidencia (BSI British Standards - BS 25777:2008, 2008).

4.4.1 Alcance

El propósito y el alcance de cada plan deben estar definidos y acordados por la alta gerencia, cada plan debe indicar con claridad la intención y lo que se quiere lograr.

Un ejemplo puede ser el siguiente:

"El Plan de Continuidad del Negocio se aplica para los Servicios Críticos de la Compañía X, solo aplicará en primera instancia los Servidores y Servicios Críticos y, en segunda instancia los Servicios secundarios".

4.4.2 Definición de Responsabilidades

Las funciones y responsabilidades de las personas y los equipos que tienen autoridad tanto en toma de decisiones y de ejecución después de un incidente deben estar documentadas.

Las responsabilidades son muy necesarias a la hora de planificar cualquier actividad no solo los planes de contingencia, para efectos de hacer alusión se desarrolla un ejemplo de un formato creado en el cual se pueden relacionar las responsabilidades según el cargo o la actividad a desarrollar. La tabla 6., permite identificar las responsabilidades de la gerencia entre las cuales puede estar por ejemplo:

- Designar las personas con la antigüedad y autoridad suficiente para ser responsable de la Implementación de los Planes de Continuidad y Contingencia.

PLANES DE CONTINUIDAD Y CONTIGENCIA			
MATRIZ DE RESPONSABILIDADES			
AREA			ELEMENTO DE APLICACIÓN
TECNOLOGÍA INFORMATICA			SERVICIOS CRÍTICOS
CARGO	**ACTIVIDAD**	**PROCEDIMIENTO**	**DESCRIPCION DE LA ACTIVIDAD**
Gerente de TIC	1	GR-PR001	Definir junto con las aaraes de TIC´s el alcance de la continuidad objetivos y obligaciones , incluyendo las obligaciones legales y reglamentarias.
	2		Definir y estandarizar el los de riesgo, según su nivel, tomando encuentra los
	3		La gerencia debe establecer y demostrar una política clara de gestión sobre la continuidad del servicio de TIC, esta se debe referir a los procedimientos que sean Diseñados y Documentados me manera clara y controlada según las personas involucradas en el proceso.
	4		Establecer lineamientos y políticas que estén acorde con las metas y objetivos estratégicos de la organización.
	5		Analizar los reportar de los cambios significativos en los servicios.
	6		La gerencia debe administrar eficientemente los recursos, debe proporcionarle los recursos necesarios para implementar, operar y mantener la continuidad de la gestión de las TIC, dichas funciones deben de estar respectivamente documentadas y autorizadas y respaldas por la alta gerencia.
	7		La dirección debe designar una persona con idoneidad y con experiencia para la implementación de las políticas sobre la gestión de continuidad.
	8		Asegurar que la organización incorpore programas de capacitación constantes sobre gestión de continuidad de las TIC en sus operaciones, rutinas y procesos de gestión de manera que se conviertan en el eje central para la continuidad del negocio de las TIC
CONTROL DE DOCUMENTO			**FECHA DE ELABORACIÓN**
ELABORÓ			**APROBÓ**
JUAN CAMILO BEDOYA			DIEGO RIOS

Tabla 6. Responsabilidades de la gerencia

4.4.3 Invocación al Plan de Continuidad

El tiempo perdido durante una respuesta no puede ser recuperado, por lo tanto la invocación del Plan de Continuidad debe contener unos protocolos de comunicación externos e internos bien definidos, no solo en caso de incidencia

sino también actividades programas de actualización y mantenimiento, entre los cuales pueden incluirse:

- Motivo de la incidencia (Externo)

- Tiempo estimado de solución (Externo)

- Invocación del Plan de Continuidad (Interno o Externo)

4.4.4 Procedimientos de Ejecución

La ejecución de los procedimientos a seguir para la recuperación del servicio debe contemplar una lista de actividades para recuperar los datos, los servicios y la red, como por ejemplo:

- Soporte de accesos remotos.

- Restablecimiento de la información del usuario.

- Actividades de recuperación de la red, las bases de datos.

- Ubicaciones alternativas de almacenamiento de datos.

- Procedimientos de Copias de Seguridad.

Los procedimientos deben ser claros y detallados, en el siguiente ejemplo se muestra un procedimiento creado con las actividades a ejecutar ante una incidencia que involucra seguir operando desde un sitio alterno, en él se visualizan además los responsables de su ejecución, como se presenta en la tabla 7.

4.5 PLANES DE CONTINGENCIA

Los Planes de Contingencia se pueden aplicar a cualquier proceso, actividad, elemento, servicio, información que permita en un momento determinado contar con una disponibilidad precisa de ese elemento, proceso o servicio.

GT-PR-004		PLANES DE CONTINUIDAD Y CONTIGENCIA
VERSIÓN	FECHA	
1.0	13-ago-12	

OBJETIVO DEL PROCEDIMIENTO
Garantizar la Continuidad del Servicio ofrecido por la Cooperativa Antioqueña en los tiempos estimas de recuperación tras fallas tecnicas o incidencias que conlleven a el traslado del servicio a un sitio alterno
ALCANCE Y APLICABILIDAD
El procedimiento debe aplicarse cuando según el análisis del personal responsable de TI establezca que es necesario trasladar los servicios al sitio alterno, o si se presenta un falla o incidencia mayor en el Centro de Computo o bien cuando los Niveles de OTR son elevados y no hay solución a una incidencia en los servicios críticos.

AREA	TECNIOLOGIA INFORMÁTICA	ELEMENTO DE APLICACIÓN	CONTINUIDAD DEL NEGOCIO

DESCRIPCIÓN DE ACTIVIDADES			
ACTIVIDAD NUMERO	**ACTIVIDAD**	**RESPONSABLE DE LA ACTIVIDAD (Quién lo hace)**	**DESCRIPCIÓN DE LA ACTIVIDAD**
1	Identificación de Incidencia con Servicios	Coordinador de TI	Se debe identificar y documentar de manera precisa la incidencia presentada por la cual se debe seguir el Paln de Continuidad.
2	Documentar el Plan de Acción	Coordinador de TI	Se debe Documentar de manera precisa cada una de las configuraciones y cambios pertinentes en las configuracion y plasmarlas en el plan de acción.
3	Coordinar enrutamiento de Comunicaciones al Sitio Alterno	Coordinador de TI	Coordinar con los Proveedores de comunicaciones los enrutamientos pertinentes para que el tráfico de datos se direccione al Sitio Alterno, el tráfico recibido a la IP 200.76.34.56
4	Verificar integridad de Servicios de Servidor Alterno	Coordinador de TI	Verificar la integridad y actulizaciones de las Bases de Datos y las aplicaciones del Servidor.
6	Iniciar Servios en Servidor Alterno	Coordinador de TI	Verificados los enlaces de comunicaciones se inicia el Servicio en Sitio Alterno

CONTROL DE DOCUMENTO		
ELABORÓ	**REVISÓ**	**APROBÓ**
JUAN CAMILO BEDOYA	DIEGO RIOS	EDITH LOBOS

Tabla 7. Procedimiento para ejecutar el plan de continuidad

A diferencia del Plan de Continuidad la Contingencia se aplica constantemente, se puede decir que si un enlace de comunicaciones presenta fallas se tiene otro enlace para restablecer los servicios y garantizar la Continuidad lo que se denomina Contingencia. El Conjunto de actividades previas de análisis, procesos y procedimientos que se tiene que llevar a cabo para solucionar una incidencia es lo que se denomina Plan de Contingencia.

Las bases de datos por seguridad y disponibilidad deben tener una copia preferiblemente al día y según la identificación e importancia que esta tenga y que sea definido por la Compañía con datos actualizados por lo que la Contingencia en este caso depende de una estrategia adoptada por que bien podría utilizarse una copia diaria, por horas o una replicación que consiste en sincronizar las bases de datos cada minuto.

Este ultimo punto referido a las base de datos como muchos otros que las compañías determinen según su infraestructura hace parte de un sin numero de procedimientos contemplados dentro de los Planes de Continuidad y Contingencia.

4.5.1 Alcance

El alcance de los Planes de Contingencia se establece según los procesos, servicios de cada organización siendo importante que al identificar los servicios críticos y no críticos cada uno de ellos tenga una Contingencia definida y un conjunto de actividades que llevadas a cabo eficientemente minimizan la afectación del servicio y agilizan la solución a ciertos incidentes.

4.5.2 Procedimientos de Ejecución

A diferencia de los Planes de Continuidad los procedimientos de un Plan de Contingencia pueden ser más numerosos ya que cada procedimiento se asocia a un compuesto de la infraestructura técnica y operativa de la organización o hasta un mismo proceso.

La tabla 8, ilustra un ejemplo de un procedimiento de Contingencia en este caso específico para las copias de respaldo de las Bases de Datos.

GT-PR-005		PLANES DE CONTINUIDAD Y CONTIGENCIA
VERSIÓN	FECHA	
1.0	13-ago-12	

OBJETIVO DEL PROCEDIMIENTO			
Realizar copias de Respaldo las cuales pueden ser utlizadas como Contingencia ante una falla inesperada en hardware.			
ALCANCE Y APLICABILIDAD			
Todas las Bases de Datos de la Organización			
AREA	Tecnologías de Información	**ELEMENTO DE APLICACIÓN**	Contingencia sobre Bases de Datos
DESCRIPCIÓN DE ACTIVIDADES			
ACTIVIDAD NUMERO	**ACTIVIDAD (Describir que se hace)**	**RESPONSABLE DE LA ACTIVIDAD (Quién lo hace)**	**DESCRIPCIÓN DE LA ACTIVIDAD**
Mensual	Copias de respaldo de la informacion para las Bases de Datos y de los Servidores	Cordinador de TI	Respaldo total del disco y del sistema Operativo;Depende la Volatilidad de la Informacion o de la modificaciones (Nuevas versiones, Parches o Rotacion de cuentas de acceso, etc), generar duplicidad y terceras copias de las Base de datos en general, verificar el estado de los disco duros.
Semanal			* Respaldo total de la información (Los fines de semana se realiza un respaldo de toda la informacion de la semana, en algunos casos se respaldan los directorios de los usuarios y privilegios de acceso). *Verificar el logs de errores en caso de errores reportar el responsable, revision del antivirus.
Diario	Realizar respaldo Diario de la Base Datos		Se recomienda realizar este respaldo diario para evitar perdida de informacion y esto no tenga impactos negativos en la organizacion
CONTROL DE DOCUMENTO			
ELABORÓ		**REVISÓ**	**APROBÓ**
JUAN CAMILO BEDOYA		DIEGO RIOS	ESTELLA GÓMEZ

Tabla 8. Procedimiento de contingencia para el respaldo de bases de datos

4.6 AUDITORIA Y REVISIONES PERIÓDICAS

Las Directivas deben asegurarse que la gestión de continuidad de las TIC sea revisada periódicamente y de manera planificada. Estas revisiones pueden tomar la forma de auditorías internas o externas, autoevaluaciones.

Es conveniente que las evaluaciones brinden oportunidades de mejoramiento y conlleven a la necesidad de cambios para una óptima gestión y respuesta en la gestión de continuidad del negocio, por lo tanto, es importante que los resultados de las revisiones sean claramente documentados (BSI British Standards - BS 25777:2008, 2008).

Es importante tener presente entonces en un proceso de auditoria o revisión aspectos como:

- Cumplimiento de los niveles de servicio

- Capacidad de los proveedores para mantener los niveles de servicio acordados.

- Retroalimentación sobre las observaciones encontradas.

- Estado y control de las acciones preventivas y correctivas.

- Medidas de seguimientos por parte de la dirección.

- Evaluación y análisis del riesgo residual.

4.7 PRUEBAS Y EJERCICIO

Los Planes de Continuidad y Contingencia de una organización no pueden ser fiables hasta no ser probados o ejecutados.

Es recomendable realizar periódicamente y como tiempo ideal cada 3 o 6 meses pruebas de Continuidad sobre el sitio alterno y con un tiempo menos prolongado pruebas de continuidad específica sobre los servicios y enlaces de comunicación.

La continuidad de los ejercicios dentro del programa se debe definir la frecuencia, el alcance y el formato de cada ejercicio de prueba, dentro de estas pruebas es importante considerar los siguientes elementos:

- Recuperación de datos: Recuperar los datos o archivos de bases de datos después de incidente.

- Recuperar los servicios de un servidor.

- Pruebas de red (Verificación de los enlaces).

4.7.1 Informes y seguimientos.

Al finalizar las pruebas o la misma ejecución de los Planes de Continuidad y Contingencia se deben revisar las conclusiones, ser revisadas y seguirlas. Estos informes pueden incluir entre otros:

- Recopilación de los resultados mismos de las pruebas o ejecución de los planes de manera detallada y por actividades ejecutadas.

- Analizar los resultados obtenidos tomando como referencia los niveles de disponibilidad deseados y los Objetivos de tiempo de recuperación (OTR).

- Identificar los vacios u observaciones de mejora.

- Consignar las acciones de mejora del ejercicio.

- Evaluar la resiliencia que es la capacidad de recuperarse ante una eventualidad que afecte los servicios de TIC’s

4.7.2 Control de la documentación.

Se debe establecer un control sobre la documentación de la gestión de Continuidad. Dentro de este control es recomendable asegurar que:

- Los documentos publicados sean previamente aprobados.

- Los documentos deben ser revisados y actualizados como sea necesario.

- Se deben identificar los cambios y los estados de revisión actuales de los documentos.

- Contar con la disponibilidad pertinente de los documentos.

- identificar los documentos de uso externo e interno.

CONCLUSIONES

- Se hace esencial que las Organizaciones implementen medidas apropiadas para responder ante los riesgos identificados y posteriormente clasificados según el grado de peligro que puedan presentar, la clasificación asignada a los riesgos permite su respectiva evaluación y por ende el diseño de las medidas apropiadas para tratarlos ejerciendo control sobre la efectividad de las mismas las cuales hacen parte de los procesos de la organización.

- Las amenazas hacen parte del entorno de las áreas de TI en las Organizaciones, aunque no solo áreas de TI en sí, toda la Organización esta expuesta a amenazas que pueden afectar la seguridad de la Información y por ende puede generar traumatismos en los servicios críticos si llegan a ser efectivas, es muy importante que las Organizaciones cuenten con los procedimientos y políticas que contrarresten estas amenazas.

- Los Planes de Continuidad y Contingencia implica que en las Organizaciones inmersas en estos procesos estas se hagan más organizadas y conscientes de la importancia que tienen la correcta implementación, prueba y ejercicio estos planes. Por lo tanto un control y conocimiento de los servicios críticos de la compañía y un dimensionamiento claro de sus niveles deseados disponibilidad dará lugar a un alcance muy bien definido cuando los procedimientos sean ejecutados.

- Es sumamente importante que el diseño de un Plan de Continuidad y Contingencia este fuertemente ligado al negocio, a sus expectativas buscando en todo momento que los servicios de TI funcionen sin interrupciones, de manera fiable y cumpliendo en todo momento con los acuerdo de disponibilidad deseados por la Organización.

- A mayor sea el tiempo de indisponibilidad o interrupción de un servicio critico mayores son las perdidas económicas y de imagen a las que pueden estar expuestas las Organizaciones.

- No solo las herramientas modernas y la última tecnología garantizan Niveles de disponibilidad deseados en los Sistemas de Información, se debe contar una correcta gestión de estos elementos contando con un diseño eficiente en infraestructura, servicios, planes de recuperación y objetividad clara en los procesos.

- Toda empresa se enfrenta a constantes cambios, por lo que debe mejorar cada día sus procesos identificando aquellas acciones correctivas las cuales con posterioridad se convite en fuente de prevención ante un riesgo de ocurrencia que pueda afectar el servicio que presta la Organización, es decir que los procesos maduran en sus resultados con la constante puesta en marcha de pruebas y ejercicios mas aún con la experiencia recopilada ante una situación de falla real.

- No mas importante deja de ser el Compromiso de la toda la Organización durante la puesta en marcha de un Plan de Continuidad y Contingencia, esta responsabilidad recae en todos y cada uno de los miembros de la compañía visionando en todo momento fomentar una cultura alrededor de las estrategias adoptadas por las áreas de TI, las gerencias y las personas involucradas en los procesos.

RECOMENDACIONES

- Se recomienda contar con métricas con las cuales se puedan llevar históricos en los tiempos de respuesta ante una falla o incidencia, esta información será útil para que una vez identificada la incidencia el tiempo de solución sea cada vez menor.

- Se recomienda también que las personas inmersas en los procesos tanto de implementación, puesta en marcha y mantenimiento de los Planes de Continuidad y Contingencia tengan una visión clara de la magnitud del impacto que puede tener la afectación del servicio, este conocimiento le permite establecer prioridades no solo de atención si no una respuesta mas efectiva solicitada a un tercero o proveedor si es del caso.

- Es recomendable que exista en relación a la disponibilidad de los servicios de TI otras disciplinas que puedan soportar o servir en un momento dado en la ejecución de un Plan de Continuidad y Contingencia, estas pueden ser, entre otras:

    - Gestión de la Capacidad, orientado al conocimiento de la capacidad de los Recursos de TI como por ejemplo capacidad de almacenamiento en un servidor.

    - Gestión de Aplicaciones, permite concebir las versiones de software que tienen las Compañías en diferentes ambientes ya sean de producción o pruebas de desarrollo.

    - Gestión de la Configuración, relacionado con aquellos elementos de conocimiento general en TI que permiten relacionar los cambios en los sistemas en mejoramiento y cambio de versiones o actualizaciones.

    - Gestión de Incidentes, proceso que permite a la organización tener documentada una incidencia lo que permitirá mitigar riesgos o minimizar el tiempo de solución a una incidencia si es repetitiva.

ANEXOS

BIBLIOGRAFÍA

(UADY), U. A. (2008). *Plan de Contigencias.* Yucatán, México.

Arrieta, E - Revista, Adiós a los desastres informáticos disponible en, http://www.recoverylabs.com/prensa/2007/02_07_expansion.htm. (23 de Febrero de 2007). Adiós a los desastres informáticos. (http://www.recoverylabs.com/prensa/2007/02_07_expansion.htm, Ed.) *Adiós a los desastres informáticos*, Pág. 20.

Baños, J. E., & Carrera, P. (2010). *Elaboración del Plan de Disponibilidad de TI para la Empresa RELIANCE.* Quito, Ecuador.

BSI British Standards - BS 25777. (2008). *BS 25777:2008.* London: BSI Group Headquarters.

BSI British Standards - BS 25777:2008. (2008). *BS 25777:2008.* London: BSI Group Headquarters.

BSi México. (04 de Mayo de 2012). *BS 25999 Continuidad del Negocio*. Recuperado el 17 de 07 de 2012, de http://www.bsigroup.com.mx/es-mx/

CEGESTI, Andrea Shum - Éxito Empresarial tomado de, http://www.cegesti.org/exitoempresarial/publicaciones/publicacion_63_150508_es.pdf. (No. 63, 2008). Continuidad del negocio: ¿cómo seguir operando a pesar de los eventos inesperados? *Éxito Empresarial*, 4.

Coopers, Price Waterhouse - Riesgo Operacional, Hot Topics. Año 3. Edición Especial. (2007). *Riesgo Operacional.* Argentina: Hot Topics. Año 3. Edición Especial.

Corrales, Dra. Martha - Contingencias y recuperación de desastres, Universidad Virtual del Tecnológico de Monterrey. (2005). *Contingencias y recuperación de desastres.* Universidad Virtual del Tecnológico de Monterrey: Diplomado de Gobierno Electrónico.

ESA Securtiy - Seguridad de la Información, www.esa-security.com. (30 de Diciembre de 2008). *ESA Securtiy - Seguridad de la Información.* Recuperado el 04 de Febrero de 2012, de www.esa-security.com

ICONTEC. (2011). *Gestión del Riesgo. Principios y directrices NTC-ISO 31000.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

ICONTEC. (2011-02-16). *Gestión del Riesgo Vocabulario GTC 137.* Bogotá: Instituto Colombiano de Normas Técnicas y Certificación.

III, R. H.-U. (Mayo 2010). *Planes de Contigencia y su auditoría.* Madrid.

Introducción al riesgo informático - Leonardo Sena y Simón Tenzer. (Agosto, 2004). *Introducción al riesgo informático.*

Mapfre, E. C.-S. (2 - 2006). Gerencia de riesgos informáticos. *Trébol, N° 39*, 10.

Martínez, J. G. (2006). *Planes de Contigencia. La Continuidad del Negocio en las Organizaciones.* Buenos Aires: Editorial Díaz de Santos.

Mejía Quijano, R. C. (2006). *Administración de riesgos Un enfoque empresarial.* Medellín: Universidad EAFIT Escuela de Administración.

Ministerio de las Tecnologías y las Comunicaciones. (2009). *Ley 1369.* Bogotá D.C.

Morales, Y. L. (02 de Agosto de 2012). Propuesta de una metodología para elaborar un programa de Continuidad del negocio en México. *Instituto Politécnico Nacional*. México, D.F.

Ochoa Vasquez, M. E. (2011). *Metodología para el desarrollo del Plan de Continuidad de Riesgo Operativo del Banco Ecuatoriano de la Vivienda (BEV).* Ecuador.

Rodríguez Lache, E. Y. (2009). Plan de Continuidad - BS 25999. *Resumen - Este artículo trata sobre el estándar BS 25999*, 12.

Trujillo Ramírez, C. R. (2012). *Herramientas de TI para la Continuidad del Negocio.* Guatemala.