PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

MAESTRÍA EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

ADMINISTRACIÓN DE CONTINUIDAD DEL NEGOCIO EN EL DEPARTAMENTO DE TI

WILSON OSWALDO JACOME CERDA

Trabajo previo a la obtención del Título de Magister en Gerencia de Tecnología de la Información

Quito DM., 2013

AGRADECIMIENTOS

A toda mi familia que ha estado presente en esta etapa tan importante de mi vida, a Dios que me ha acompañado en los momentos difíciles y ha sabido iluminar mi camino.

DEDICATORIA

A MIS PADRES

CONTENIDO

INDICE DE TABLAS

INDICE DE IMÁGENES E ILUSTRACIONES

INTRODUCCIÓN

La satisfacción del cliente se ha convertido en el centro de atención sobre el cual giran las diversas estrategias de negocios que buscan mantener a una organización fuerte y sostenible en el tiempo.

Hoy el mundo ha cambiado, la tecnología ha hecho que las necesidades de los consumidores cambien a otro ritmo y que busquen una atención distinta, adecuada y rápida, soluciones efectivas y productos apropiados; es decir, aquellas herramientas que les permitan lograr sus objetivos.

Sin embargo, esas herramientas deben brindar seguridad y tranquilidad al momento de enfrentar problemas y situaciones adversas a las cuales cualquier organización se encuentra expuesta. Lamentablemente han ocurrido problemas en diversas organizaciones porque no se han previsto planes de continuidad para poder contrarrestar las adversidades que se presentan inesperadamente.

Mediante el presente trabajo se busca principalmente demostrar que, para brindar confianza a los clientes es necesario contar con una administración de continuidad del negocio adecuada y probada; cuyo eje principal se basa en las herramientas y servicios que brinda el departamento de TI dentro de una organización. Dicha confianza generada en los clientes se ha convertido en el centro de atención sobre el cual giran las diversas estrategias de riesgos de las entidades financieras, tomando en cuenta la gran cantidad de eventos maliciosos y fraudes a los cuales se ve expuesto el cliente a diario.

Para cumplir con los objetivos propuestos, el presente trabajo se ha distribuido en seis capítulos:

- El primero brinda una introducción orientada al entendimiento de la Administración de Continuidad del Negocio y las Tecnologías de Información.

- En el segundo capítulo se analiza el entorno tanto mundial como local sobre la Administración de Continuidad del Negocio dentro de TI, así como la selección del caso de estudio del presente trabajo.
- El capítulo tres analiza la metodología a implementar así como el análisis de Impacto de Negocios generado dentro de la organización y sus resultados.
- En el cuatro se definen las estrategias de continuidad de TI a aplicar para los procesos definidos en el capítulo anterior.
- En el quinto capítulo se define y genera la administración de crisis dentro de la organización, así como el Rol que debe cumplir el departamento de TI dentro del mismo.
- En el último capítulo culmina la tesis con las conclusiones, recomendaciones y líneas de investigación

CAPÍTULO I: MARCO TEÓRICO

La planeación de Continuidad del Negocio es un proceso más que un proyecto; los planes desarrollados como parte de este proceso dirigirán la respuesta a incidentes, desde simples emergencias hasta desastres totales. La meta última del proceso es poder responder mejor a incidentes que puedan impactar en la gente, las operaciones y la capacidad de entregar bienes y servicios al mercado. Constantemente se experimentan situaciones de emergencia, directa o indirectamente, las cuales se manifiestan en respuestas equívocas ocasionadas por el temor, miedo o un extremo pánico. La buena aplicación de estos servicios y soluciones de continuidad y recuperación están pensados para garantizar una total disponibilidad de los procesos esenciales del negocio. Aunque las pérdidas por un desastre informático puedan ser muy importantes, cada vez son mayores los avances tecnológicos que permiten y hacen posible la recuperación en muy poco tiempo y a unos costes razonables, siendo sus ciclos de implantación cada vez más cortos.

1.1. Administración de Continuidad

1.1.1. Definición

Según el BCI (Business Continuity Institute) la Administración de Continuidad del Negocio es un proceso de administración holístico que identifica los potenciales impactos de amenazas en una organización, y provee un marco de trabajo que construye "resilencia"[1] y capacidad para conducir una respuesta efectiva que proteja los intereses de los participantes claves, su reputación y valor del negocio.

[1] Capacidad de resistir eventos no programados que puedan afectar la continuidad de un negocio

Para que una Administración de Continuidad del Negocio pueda generar "resilencia" necesita identificar por adelantado los impactos potenciales de una gran variedad de eventos repentinos, los cuales permitan priorizar los esfuerzos requeridos de varias áreas especialistas encaminadas a recuperar sus funciones tales como seguridad, instalaciones y TI.

Aunque el término "resilencia" aplica a todos las escalas de respuestas a eventos no programados, la Continuidad de Negocio se encuentra enfocada al desarrollo de estrategias que permitan que una organización sobreviva a la pérdida parcial o total de su capacidad de operación. Esto implica por lo tanto sobrevivir a pérdidas de recursos tanto materiales como humanos. Debido a que la capacidad de reacción de la organización depende de la administración y operación de recursos humanos y materiales así como de la tecnología y las ubicaciones geográficas, dicha capacidad debe ser desarrollada a lo largo de toda la organización incluyendo proveedores, accionistas, clientes; con apoyo de la alta dirección.

De esta manera, el precursor de generar esta capacidad es la responsabilidad que tiene la alta gerencia con los intereses a largo plazo de todo el personal a su cargo, de sus clientes y de todos quienes dependen de la organización de alguna manera. Mientras es posible calcular las pérdidas financieras debido a interrupciones en el negocio, el impacto más significativo es usualmente el provocado por el daño en la reputación o la pérdida de confianza que resulta de la mala administración de un incidente. A diferencia de este efecto, se puede anotar que un incidente bien manejado en una organización puede mejorar la reputación y la confianza en el equipo directivo de la misma.

La competitividad creciente entre las organizaciones empresariales, las demandas cada vez más exigentes de clientes, o los requerimientos regulatorios cada vez más restrictivos, son factores que hoy en día fuerzan a las empresas a demostrar la resistencia de las actividades de negocio a permanecer activas ante cualquier contingencia grave. Una caída de la luz, una

inundación, un incendio o un robo han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas sean tan graves que afecten a la viabilidad del negocio. Son múltiples las organizaciones que, independientemente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestas y garanticen una alta disponibilidad en las operaciones de su negocio. De este modo, es necesario que las organizaciones establezcan una serie de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio en caso de tener que afrontar una contingencia grave.

De esta manera, la Administración de Continuidad del Negocio (BCM: Business Continuity Management) se convierte en una cultura organizacional que piensa en el antes, durante y después de un evento de crisis. La continuidad hace parte de los procesos de la compañía, es decir que todos los productos, procesos considerados como críticos dentro de la misma, siempre deberían considerar la perspectiva de la forman en la cual se va a garantizar la continuidad de estos.

1.1.2. Tendencias

"Eso nunca nos pasará a nosotros", "Nosotros sobreviviremos, siempre lo hemos hecho", "Somos demasiados grandes como para caer", "No somos un blanco terrorista" son respuestas frecuentes por empresarios cuando fueron cuestionados sobre su capacidad de resistir eventos catastróficos. Otros creen que sus compañías de seguros pagarán por estas catástrofes, lamentablemente la mayoría piensa que no han tenido tiempo para prepararse sobre algo que quizás nunca llegue a suceder. Lamentablemente el catálogo de empresas que

han desaparecido por una crisis externa sugiere que estas respuestas se basan en suposiciones totalmente falsas.

Si bien es cierto, las bombas, incendios e inundaciones capturan el 90% de los incidentes por los cuales podría atravesar una empresa, la mayoría de eventos que ponen en peligro una organización son "catástrofes silenciosas", las cuales no aparecen en los medios de comunicación, pero pueden tener un efecto devastador sobre la capacidad de una empresa para poder operar. Muchas de las causas están fuera del control de la organización y su respuesta y tiempo de interrupción dependen de los servicios de emergencia o proveedores.

En el manejo de cualquier evento que afecte a una organización, el éxito se juzga tanto por la respuesta técnica al mismo, así como la percepción sobre la gestión de la administración de dicho evento. En una investigación realizada por Knight y Pretty sobre métricas ("El impacto de las catástrofes en el valor de los accionistas", por Rory F. Knight y Deborah J. Pretty, 1996) se indica que las organizaciones afectadas por catástrofes se dividen en dos grupos: "Recuperadas" y "No Recuperadas". Cuando una organización ha afrontado con éxito una crisis, el valor de sus acciones ha aumentado en el largo plazo, en contraste con aquellas que se consideró no manejaron de forma adecuada la crisis, obtuvieron una disminución de sus acciones, y después de un año todavía no se habían recuperado. Una investigación más reciente ha demostrado que las organizaciones cuya mayor parte de su presupuesto es invertida en Administración de Riesgos, BCM y Gobernabilidad (Estrategia) son las más rentables en su sector, lo que nos permite concluir que el BCM es una inversión y no un gasto.

El principal objetivo del BCM es asegurar que la organización posea una respuesta a las crisis más importantes que puedan amenazar a su supervivencia. Si bien es cierto, esta razón debería ser la más importante para implementar un BCM en una organización, existen otros

beneficios que se pueden obtener al adoptar el BCM como una disciplina de gestión tales como:

- Algunas empresas deben respetar y obedecer requisitos legales y reglamentarios ya sea específicamente para BCM o más general sobre "Gestión de Riesgos" como parte de requisitos de su gobierno corporativo o estatal.
- Un plan de BCM es apropiado para satisfacer tanto los requisitos y respuestas a riesgos específicos, así como a la "conciencia" de riesgo" de una organización.
- Las empresas que brindan servicios a otras empresas han utilizado al BCM como una ventaja competitiva para obtener nuevos clientes y para mejorar sus cualidades como una demostración más adecuada de "atención al cliente".
- Un examen exhaustivo de la empresa por medio de una Evaluación de Impacto sobre el negocio usada en el BCM puede poner en relieve las ineficiencias en el mismo y centrarse en prioridades que sin dicho ejercicio no podrían haber sido evidenciadas.
- Las organizaciones que proporcionan bienes y servicios reconocen que mantener a los clientes a través de un servicio confiable es más barato que recuperarlos después de una interrupción.

Según la encuesta conducida por la Price Waterhouse Coopers en el año 2012 en lo referente a la seguridad de información (ver Figura 1.1) se puede evidenciar que la Administración de Continuidad es el segundo factor que motiva a las empresas a invertir en medidas de seguridad de información. Esto nos demuestra la relevancia que ha obtenido en el mercado este tema y como poco a poco empieza a ganar protagonismo dentro del mercado internacional.

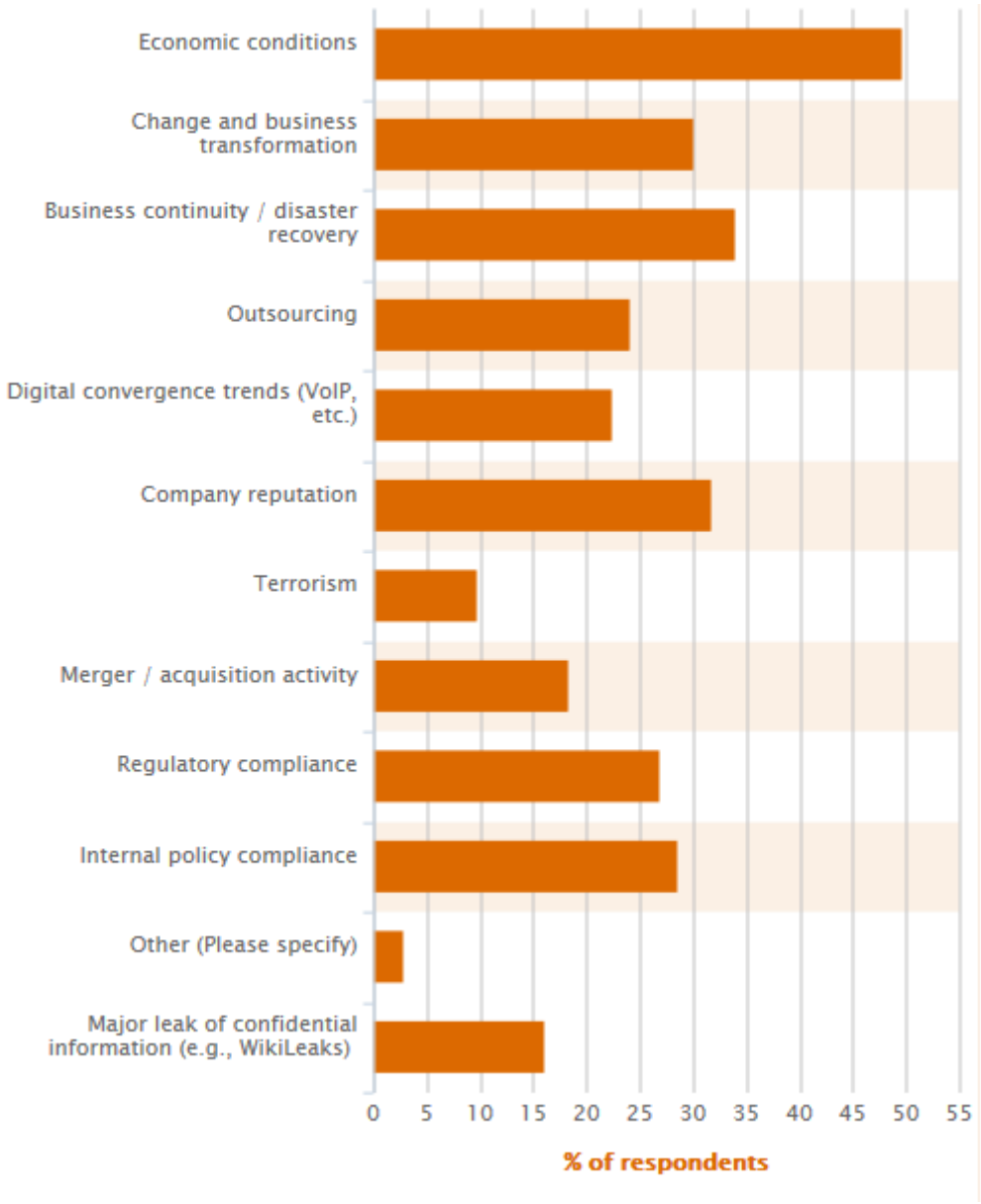

Ilustración 1. Motivos de Inversión en Seguridad de Información. Fuente: Price Waterhoouse Coopers 2012

Las propuestas para evitar interrupciones y asegurar una reducción aceptable de riesgo asociados al funcionamiento de una empresa han sido numerosas. Los Planes de Recuperación de Desastres (DRP: Disaster Recovery Plan) fueron los primeros instrumentos desarrollados en ese sentido hace más de 20 años, superados una década después por los planes de Continuidad de Negocios (BCP: Business Continuity Plan). En la actualidad los instrumentos empleados han equilibrado la fuerte carga tecnológica que caracterizaba a los planes anteriores para enfrentarse con los demandas operativas de las organizaciones.

La propuesta actual de un BCM asume principios tales como alinearse con los objetivos de la organización integrándose directamente en la empresa y conformar procesos en constante evolución. Esta tendencia permite que los planes desarrollados dentro de un BCM se ajusten al dinamismo de la empresa para adecuarse a las mutaciones del mapa de riesgos, el cual es constantemente afectado por cambios que deben ser analizados y tratados consecuentemente.

En el Ecuador, lamentablemente la mayoría de las empresas toma en cuenta el factor económico a la hora de decidirse por una solución a un potencial problema, ya que debería ser administrador por medio de la generación de una norma o política que obligue a las mismas a la realización de un Plan de Continuidad de Negocios. Sin embargo, en el ámbito de las entidades financieras el panorama se enmarca de una manera más adecuada y controlada.

Hoy en día las empresas pioneras en la preocupación por la continuidad del negocio son las instituciones que participan del sistema financiero de los países. Esto se produce básicamente por el énfasis que el Comité de Basilea[2] le ha dado al tema en los últimos años en su segundo acuerdo sobre capital. De acuerdo a esto, aquellas empresas que sean menos cuidadosas en la implementación de sus planes de continuidad deberán comprometer más capital para sus operaciones. De tal manera, el público y el mercado podrá conocer cuáles serán las empresas más exitosas en el control de riesgos, y podrá decidir si maneja sus operaciones financieras con empresas más seguras o empresas más riesgosas, lo cual le permitirá negociar diferentes condiciones para sus operaciones.

Otro de los aspectos que ha influido en que las entidades financieras hayan incrementado el presupuesto dedicado a la Gestión de Continuidad de Negocio fue el impacto que supuso el

[2] Denominación al Comité de Supervisión Bancaria de Basilea (BCBS) cuya función es fortalecer la solidez de los sistemas financieros.

"11S"[3], los numerosos desastres naturales, y por el cybercrimen y su imparable evolución. En 2007, el cambio de ciclo económico parece haber marcado un nuevo período, en el que la mayor parte de las preocupaciones es la crisis crediticia, más acentuada en el mercado estadounidense, pero cuyas consecuencias han salpicado a todo el planeta. En dicho contexto la Continuidad de Negocios está tomando fuerza como medida eficaz de reducción de riesgo.

Desde octubre del 2005 está disponible en el website de la Superintendencia de Bancos y Seguros del Ecuador (SBS) la resolución No. JB-2005-834 para la gestión y administración del riesgo operacional. En esta resolución de aproximadamente 19 páginas y 146 controles, el equipo técnico de la Superintendencia ha organizado un conjunto de mejores prácticas para mitigar o controlar los riesgos que forman base del riesgo operacional. En lo referente a la Continuidad de Negocio se define el siguiente punto:

Aspecto Mayor	Breve Descripción
Continuidad del Negocio (sección IV)	Planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. Proceso de administración de la continuidad de negocios

En la actualidad es tan importante para las entidades de control que los organismos que se encuentran bajo su jurisdicción acaten la implementación de Continuidad de Negocios; a tal punto que en una carta enviada por la SBS el 24 de Agosto del 2011 dirigida a todo el sistema financiero nacional, se especifica que: " Se recuerda e instruye a las instituciones financieras

[3] Término que hace referencia a los atentados terroristas sufridos en Estados Unidos por miembros de la organización Al-Qaeda mediante secuestros de aviones de línea para ser impactados contra varios objetivos

la necesidad de implementar los planes de contingencia y de continuidad, determinados en la Norma invocada en la Aplicación de la Ley General de Instituciones del Sistema Financiero"

1.1.3. Metodologías Disponibles

Cuando se habla sobre Administración de Continuidad del Negocio, el núcleo del concepto se enfoca en todos los procesos que se deben ejecutar para asegurar la supervivencia de una empresa o institución en caso de que esta se viera sometida a una interrupción no deseada de su negocio y por ende de su funcionamiento.

Citando las cifras descritas por el Emergency Management Forum (Estados Unidos), de cada 100 empresas que afrontan un desastre sin contar con una Administración de Continuidad, 43% nunca reabren el negocio, 51% sobrevive, pero están fuera del mercado en 2 años y solo el 6% logra sobrevivir a largo plazo.

Es por este motivo que el mundo ha tomado conciencia sobre la importancia de tener normas, estándares y un consenso de buenas prácticas en lo referente a la Administración de continuidad del Negocio, entre las cuales se puede citar las siguientes:

1.1.3.1. British Standards Institute (BSI): BS 25999-1 BS 25999-2

Es un estándar británico desarrollado en un inicio como un Plan de Continuidad de Negocio (BCP) y luego expandido a una Administración de Continuidad de Negocio (BCM) creado y mejorado por un grupo de expertos de relevancia mundial en los sectores de la industria. Se trata de una norma certificable; es decir, que entrega una certificación a quienes comprueben conocimiento y práctica de la misma; en el cual se tienen en cuenta tanto los recursos humanos, como las infraestructuras, la información vital, las tecnologías de información y los equipos que la soportan.

La norma consiste en una serie de recomendaciones o buenas prácticas para facilitar la recuperación de los recursos antes mencionados en caso de que se presente una crisis, y fue dividida en dos partes:

- BS 25999-1 : (2005) Documento orientativo que proporciona las recomendaciones prácticas para el BCM
- BS 25999-2 : (2006) Establece los requisitos para un sistema de Administración de Continuidad de Negocio (BCM): es la parte certificable a través de la implementación, auditoría y certificación

1.1.3.2. Singapore Standard: SS 540

Es un estándar publicado en Singapur en el año 2008, el cual establece un marco de trabajo para que una organización pueda analizar sus estrategias, procesos y procedimientos. Este estándar hace énfasis en la capacidad de resistir una crisis en una empresa por medio de la protección de sus activos críticos tales como recurso humano y su entorno tanto intangible como físico. Se centra en la administración de la continuidad y la recuperación de las funciones críticas del negocio aplicables tanto a pequeñas como a grandes organizaciones. El estándar intenta cumplir los siguientes puntos:

- Proveer una política para prevenir, preparar y responder ante eventos que afecten a una organización
- Proveer objetivos, procedimientos y procesos que permitan lograr las políticas antes mencionadas
- Proveer a la organización una capacitación y fortaleza para enfrentar crisis
- Proveer un sistema de monitoreo y revisión del desempeño de la organización
- Proveer una mejora continua del proceso de administración de la continuidad

1.1.3.3. ISO/PAS 22399:2007

Publicada en el año 2007 y actualizada en marzo del 2011, provee una guía general para organizaciones ya sean privadas, gubernamentales y no gubernamentales, la cual les permite desarrollar su propio criterio de desempeño para la preparación contra incidentes y continuidad de la operación. Entrega las bases para entender, desarrollar e implementar la continuidad de operaciones y servicios dentro de la organización y proveer confianza en sus negocios, comunidad, clientes.

Este estándar es aplicable a todos los tipos de organizaciones y presenta los principios generales y los elementos para preparar a dichas empresas contra incidentes que eviten la continuidad de las operaciones. La extensión de esta aplicación dependerá de factores tales como las políticas de la organización, la naturaleza de sus actividades, sus productos y servicios, y sus ubicaciones geográficas

1.1.3.4. Australian and New Zealand Business Continuity Management Standard: AS/NZS 5050:2010

Este estándar fue preparado por el Comité OB-007 de estándares de Nueva Zelandia y Australia en el año 2010, enfocado bajo el esquema de Administración de Riesgos, el cual permite mantener la continuidad de los negocios a través de la administración adecuada de los riegos asociados con la interrupción de las empresas.

El enfoque de la administración de riesgos asociados con la interrupción del negocio fue hecho por intermedio de la norma AS/NZS ISO 31000:2009 “Administración de Riesgos, Principios y Guías” dando particular énfasis en los eventos de interrupción, su impacto y probabilidad, así como la capacidad de la organización de administrar los mismos.

La administración efectiva de este tipo de riesgos requiere de un conocimiento profundo de los objetivos de la organización, su ambiente de operación y sus dependencias. La aplicación de este estándar se recomienda sea parte integral de la administración de los riesgos de la organización, lo cual debe ayudar a reducir su ocurrencia y su impacto, los cuales al ser materializados pueden ocasionar la interrupción de toda la organización.

1.1.3.5. ISO 22301 BCM Standard

Este estándar se constituye en la publicación más actual en lo referente a especificaciones de la Administración de Continuidad del Negocio; apenas el 16 de Mayo del 2012 fue su publicación oficial cuyo nombre completo es: "ISO 22301:2012 Societal Security – Business Continuity Management Systems - Requeriments". Como se ha descrito en el presente trabajo, este constituye uno más de los 100 estándares de BCM disponibles en el mercado, su particularidad nace de que al ser un estándar ISO tiene más credibilidad porque ha sido desarrollador por un grupo de expertos en dicho dominio.

La ISO ha determinado que la norma 22301 es aplicable en su implementación para cualquier país, y por lo tanto también puede ser auditable, tal como lo es la norma BS 25999-2 descrita anteriormente; sin embargo, al ser un resultado de una racionalización de todos los puntos de vista y otros estándares como entrada, alguna terminología de la norma ISO es más orientada al negocio y por lo tanto sus requerimientos son menos ambiguos que la BS 25999-2.

Este nuevo estándar representa una mejora sobre la 25999-2 en áreas tales como respuesta a desastres y comunicación de crisis, y es mucho más robusta en el uso del ciclo de administración de sistemas "PLAN-DO-CHECK-ACT" [4]. Esto también permite que el

[4] El ciclo PDCA, también conocido como "Círculo de Deming o circulo de Gabo" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.

modelo de gobierno de la organización en lo referente a la continuidad del negocio se centre en el programa de BCM como tal, a consecuencia de ello las organizaciones deberán ser más rigurosas en su implementación. A diferencia de la 25999-2 que se centra únicamente en las acciones de prevención y mitigación de riesgos.

1.2. Tecnologías de Información

La utilización de tecnología, específicamente computadoras y ordenadores electrónicos, son usados para el manejo y procesamiento de información; es decir, la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

Los orígenes de la TI (Tecnologías de Información) son recientes, aunque el nombre de tecnología de información se remonta a los años 70, y su utilización en los negocios se remonta a mediados del siglo XX, durante la segunda guerra mundial. Sin embargo, ha sido en los últimos 20 años donde ha alcanzado niveles de uso y aplicaciones tan variadas y ubicuas, que se ha convertido en un área de gran amplitud e impacto en todos los aspectos de la vida cotidiana – incluyendo la gerencia de cualquier empresa, en la cual hoy en día es casi indispensable.

Este término se origina del inglés "information technology", cuando el administrador de computadoras Jim Domsic lo hace conocido en noviembre de 1981, con el objetivo de modernizar el término "procesamiento de datos" (data processing).

De todas maneras en el Diccionario de inglés de Oxford se cita un texto de 1958 que empleaba la palabra "information technology".

1.2.1. Definición

El concepto de Tecnologías de Información según González Gisbert indica: "El conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información".

Si se centra en la definición que de tecnología hacen Harvey Brooks y Daniel Bell: "el uso de un conocimiento científico para especificar modos de hacer cosas de un modo reproducible", se podría decir que las Tecnologías de Información, más que herramientas generadoras de productos finales, son procesos científicos cuyo principal objetivo son la generación de conocimientos, que a la postre incidirán en los modos de vida de las sociedades, no sólo en un ámbito técnico o especializado, sino principalmente en la creación de nuevas formas de comunicación y convivencia global. Dicho entendimiento se encuentra mejor concebido en la definición que hace Bologna y Walsh en el año de 1997 sobre las TI: “aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información, por lo tanto la Tecnología de Información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones”

La tecnología de la información no es un fenómeno tan nuevo como muchas personas creen. El proceso de construir artefactos (en el sentido más amplio del término) que favorezcan la preservación y circulación de información, con el fin de que se pueda transformar en conocimiento útil, ha sido una actividad constante desde los inicios de la palabra escrita. Lo novedoso hoy es el hecho de haber puesto juntos numerosos recursos tecnológicos que generan una sinergia comunicativa sin precedentes: palabra escrita; registros orales y visuales; dispositivos masivos de almacenaje con capacidades de ordenar, organizar y transformar información; dispositivos potentes de transmisión y comunicación;

disponibilidad casi universal de estos recursos; desaparición de los condicionantes de tiempo y espacio.

Se podría establecer un punto de semejanza entre la revolución de las Tecnologías de la Información y la Revolución Industrial, cuya principal diferencia reside en la materia prima de su maquinaria; es decir, se pasó de una eclosión social basada en los usos de la energía a una sociedad cuyo bien primordial ha pasado a ser el conocimiento y la información. Pueden ser incluidas en esta gran área de las ciencias, la microelectrónica, la computación (hardware y software), las telecomunicaciones y (según opinión de algunos analistas) la ingeniería genética. Esta última, por decodificar, manipular y reprogramar la información genética de la materia viviente.

Desde un punto de vista histórico, la revolución de las Tecnologías de la Información marca un momento crucial y decisivo en la sociedad mundial, pues ha penetrado en todas las áreas de vida humana, no como agente externo, sino como un motor que genera un flujo activo en las interrelaciones sociales.

Durante la última década del siglo pasado, mucho se habló sobre una nueva era de oscurantismo informativo, ocasionado por esta suerte de carrera contra reloj por la adquisición y generación de información y conocimientos. Sin embargo, las nuevas tecnologías de la información, representan una oportunidad singular en el proceso de democratización del conocimiento, pues los usuarios pueden tomar el control de la tecnología, que usan y generan, y producir y distribuir bienes y servicios. Podría pensarse que las TI han abierto un territorio en el cual la mente humana es la fuerza productiva directa de mayor importancia en la actualidad.

Por lo tanto, el ser humano es capaz de convertir su pensamiento en bienes y servicios y distribuirlos no ya en una frontera local, sino globalmente. Las TI han modificado sustancial e irrevocablemente, la forma en la cual el ser humano y todo el planeta Tierra vive y se desarrolla.

1.2.2. Acoplamiento de TI en el negocio

La tecnología de la Información (TI) está cambiando la forma tradicional de hacer las cosas, las personas que trabajan en gobierno, en empresas privadas, que dirigen personal o que trabajan como profesional en cualquier campo utilizan la TI cotidianamente mediante el uso de Internet, las tarjetas de crédito, el pago electrónico de la nómina, entre otras funciones; es por eso que la función de la TI en los procesos de la empresa como manufactura y ventas se han expandido grandemente. La primera generación de computadoras estaba destinada a guardar los registros y monitorear el desempeño operativo de la empresa, pero la información no era oportuna ya que el análisis obtenido en un día determinado en realidad describía lo que había pasado una semana antes. Los avances actuales hacen posible capturar y utilizar la información en el momento que se genera, es decir, tener procesos en línea. Este hecho no sólo ha cambiado la forma de hacer el trabajo y el lugar de trabajo sino que también ha tenido un gran impacto en la forma en la que las empresas compiten según lo ha comentado Alter en el año de 1999.

Utilizando eficientemente la tecnología de la información se pueden obtener ventajas competitivas, pero es preciso encontrar procedimientos acertados para mantener tales ventajas como una constante, así como disponer de cursos y recursos alternativos de acción para adaptarlas a las necesidades del momento, pues las ventajas no siempre son permanentes. El sistema de información tiene que modificarse y actualizarse con regularidad si se desea percibir ventajas competitivas continuas. El uso creativo de la tecnología de la

información puede proporcionar a los administradores una nueva herramienta para diferenciar sus recursos humanos, productos y/o servicios respecto de sus competidores (Alter, 1999). Este tipo de preminencia competitiva puede traer consigo otro grupo de estrategias, como es el caso de un sistema flexible y las normas justo a tiempo, que permiten producir una variedad más amplia de productos a un precio más bajo y en menor tiempo que la competencia.

Las tecnologías de la información representan una herramienta cada vez más importante en los negocios, sin embargo el implementar un sistema de información de una empresa no garantiza que ésta obtenga resultados de manera inmediata o a largo plazo.

En la implementación de un sistema de información intervienen muchos factores siendo uno de los principales el factor humano. Es previsible que ante una situación de cambio el personal se muestre renuente a adoptar los nuevos procedimientos o que los desarrolle plenamente y de acuerdo a los lineamientos que se establecieron. De todo lo anterior es necesario hacer una planeación estratégica tomando en cuenta las necesidades presentes y futuras de la empresa. Así como una investigación preliminar y estudio de factibilidad del proyecto que deseamos.

Generalmente la mayoría de empresarias piensa que las Tecnologías de Información solo se usan en la etapa de producción, y vienen a la mente los grandes sistemas de manufactura, o los sistemas automatizados de producción continua, sin embargo, actualmente las Tecnologías de Información deberán estar presentes en todas las actividades de la empresa, en decir, en las etapas de entrada, conversión y salida.

En la etapa de entrada, las tecnologías de información deberán contener todas las habilidades, procedimientos y técnicas que permitan a las organizaciones manejar eficientemente las relaciones existentes con los grupos de interés (Clientes, proveedores, gobierno, sindicatos y público en general) y el entorno en el que se desenvuelven.

En la etapa de conversión, las Tecnologías de Información en combinación con la maquinaria, técnicas y procedimientos, transforman las entradas en salidas. Una mejor tecnología permite a la organización añadir valor a las entradas para disminuir el consumo así como el desperdicio de recursos.

El departamento o equipo que dentro de una organización ejerce las funciones de TI se encarga de estudiar, diseñar, desarrollar, implementar y administrar los sistemas de información utilizados para el manejo de datos e información de toda la organización. Estos sistemas, a su vez, comprenden aplicaciones o software, y equipos o hardware.

Llevar a cabo las tareas de la organización apoyándose en la Tecnología de información, generalmente redunda en un procesamiento más rápido y confiable de su datos. La información resultante tiene mayor movilidad y accesibilidad, y cuenta con mayor integridad, que cuando se procesa en forma manual. Igualmente, las computadoras relevan a los empleados de numerosas actividades repetitivas y aburridas, permitiéndoles aprovechar mejor su tiempo en actividades que agregan más valor.

A medida que los precios de los equipos de computación bajan, su capacidad aumenta, y se hacen más fáciles de usar, la TI se utiliza en nuevas y variadas formas. En las empresas, sus aplicaciones son diversas. Hoy en día, la mayoría de las empresas medianas y grandes (y cada día más pequeñas y micro-empresas) utilizan la TI para gestionar casi todos los aspectos del

negocio, especialmente el manejo de los registros financieros y transaccionales de las organizaciones, registros de empleados, facturación, cobranza, pagos, compras, y mucho más.

La revolución de las Tecnologías de Información ha tenido un profundo efecto en la administración de las organizaciones, mejorando la habilidad de los administradores para coordinar y controlar las actividades de la organización y ayudándolos a tomar decisiones mucho más efectivas. Hoy en día el uso de las Tecnologías de Información se ha convertido en un componente central de toda empresa o negocio que busque un crecimiento sostenido.

El uso de Tecnologías de Información ya no lo es solo para procesos de producción o conversión, sino que deberá estar implícito en todos los ámbitos del negocio, incluyendo en el área administrativa, por ser esta la que controla toda la empresa. Como resultado del uso de estas tecnologías podemos decir que la empresa puede reducir el tamaño de su estructura jerárquica e incrementar el flujo de información horizontal, esto es, a través de todos los departamentos de la empresa, además de proveer de una ventaja competitiva a la empresa. Cabe señalar que los sistemas de información también reducen la necesidad de los administradores de coordinar e integrar las actividades de las subunidades de la empresa, además de que las Tecnologías de Información actualmente pueden coordinar completamente el flujo de producción de una empresa.

1.3. Tecnologías de Información y Administración de Continuidad del Negocio

Tal como se ha mencionado anteriormente, los planes de continuidad del negocio (BCP) son el instrumento más adecuado para ayudar a las empresas a superar situaciones extremas y continuar con su actividad minimizando sus consecuencias más negativas

En el mercado de las Tecnologías de la Información en difícil encontrar un tema sobre el que exista tanta unanimidad como en torno a la necesidad de que todas las empresas y organizaciones cuenten con un Plan de Continuidad de Negocio.

Las razones para poner en marcha un BCP tienen que ver no sólo con ataques terroristas, desastres naturales, actos vandálicos, intrusiones incontroladas, virus informáticos, interrupciones del suministro eléctrico o los inevitables errores humanos, sino también con la gran interdependencia que existe entre los datos, los sistemas informáticos y de comunicación y el funcionamiento y el negocio de las empresas.

1.3.1. Tecnologías de Información y Administración de Continuidad

En TI las fallas no son una opción; es por este motivo que no es de sorprender que las organizaciones tengan como alta prioridad el desarrollo e implementación de planes confiables de continuidad del negocio para asegurar que los servicios TI se encuentren siempre disponibles para los usuarios internos y los clientes externos.

Resulta vital para las empresas que sus operaciones descansen sobre ambientes robustos y seguros, sobre todo, cuando se hace referencia a los llamados sistemas de "misión crítica". Y es que en la actualidad es difícil determinar una operación que, moviéndose en un entorno

altamente influenciado por el artificio tecnológico, no dependa de "estar al aire" para marchar exitosamente.

Las operaciones continuas, la permanente exposición a los clientes, la información administrativa del negocio, las ventas o cualquier otro tipo de transacciones electrónicas son signos del modelo de negocios actual que exigen plataformas TI infalibles, independientemente de la naturaleza de la empresa.

Es por eso que la alta disponibilidad del ambiente de tecnología de información de la operación, la minimización de los tiempos de interrupción de los servicios prestados, el mínimo riesgo de pérdida de información, la capacidad de respuesta a un evento, de tal manera que las funciones críticas de negocio continúen sin cambios esenciales, las herramientas que faciliten el monitoreo y la administración centralizada de los recursos y servicios TI, así como la reducción del costo por caída de los servicios TI o la recuperación automática en caso de fallas o desastres, son aspectos que una plataforma debe garantizar, bajo estándares de rendimiento aceptados globalmente y cumpliendo las mejores prácticas disponibles en el mercado.

Cuando una empresa sufre daños físicos por vandalismo, incendios o desastres naturales, es común que, aunque la información se tenga respaldada, esto no asegure la continuidad inmediata de las operaciones, debido al daño sufrido en el personal, las instalaciones y los equipos de cómputo.

Por esta razón es importante implementar un Plan de Continuidad de Negocios dentro de una unidad de tecnología, que a más de incluir el “back up”, cuente con una estrategia que incluya acciones de los colaboradores de dicho departamento, y una ubicación física alterna equipada

con lo necesario para que el departamento de tecnología pueda empezar a operar prácticamente de inmediato.

Cuando la recuperación tras siniestros se consolidó como disciplina y se convirtió en un negocio en los años 80, el objetivo principal era la protección del centro de datos, el núcleo de la estructura TI extremadamente centralizada de una compañía. A principios de los 90, este modelo empezó verse desplazado por la informática distribuida y la tecnología de cliente/servidor. Y a su vez, la tecnología de la información pasaba a formar parte de prácticamente todos los aspectos empresariales. La informática ya no constituía una actividad en segundo plano, sino que los datos clave llegaban a todos los departamentos de la empresa: en los sistemas PC de sobremesa, las redes de área local de los departamentos y en el centro de datos.

Esta evolución todavía continúa, las iniciativas empresariales más importantes como, por ejemplo, la Planificación de Recursos Empresariales (ERP), la gestión de la cadena de suministros, la gestión de las relaciones con los clientes y e-business han convertido el acceso permanente a la información, desde dondequiera que se encuentren los usuarios, en un aspecto crucial para la empresa. Esta transformación implica que las empresas ya no pueden prescindir de las tecnologías de la información: datos, software, hardware, redes, centros de datos e incluso sistemas portátiles. Una compañía que vende productos o brinda servicios sobre internet, por ejemplo, o da soporte a los clientes mediante un centro de llamadas debe estar operativa las 24 horas al día, todos los días de la semana, o los clientes se buscarán otra compañía. Una empresa que utilice una solución e-business para adquirir y distribuir piezas y productos no sólo depende de su propia tecnología sino también de la de sus proveedores. Por lo tanto, la protección de los procesos empresariales clave, con todas sus complejas interdependencias, es actualmente tan importante como la protección de los datos.

El objetivo de las compañías que no pueden permitirse ni un segundo de inactividad consiste en lograr un estado de continuidad empresarial, en el que los sistemas y redes más importantes estén siempre disponibles, pase lo que pase. Y esto implica pensar de forma activa: incorporar disponibilidad, seguridad y fiabilidad en los procesos empresariales desde el principio, y no elaborar un plan de recuperación tras siniestros a posteriori para hacer frente a los requisitos de la continuidad de negocio.

Muchos ejecutivos senior y directores empresariales consideran que la continuidad empresarial es responsabilidad del departamento de IT. Sin embargo, ya no es suficiente ni práctico que la responsabilidad recaiga en un solo grupo. La informática distribuida y la informática basada en varios niveles han descentralizado los procesos empresariales y los han hecho más complejos. Es más, está en juego la reputación de la empresa, su base de clientes y, por supuesto, sus ingresos y beneficios.

Por lo tanto, todos los ejecutivos, directores y empleados deben participar en el desarrollo, implantación y soporte permanente de la evaluación y planificación de la continuidad. Las mismas tecnologías de la información que impulsan la aparición de nuevas ventajas competitivas han originado nuevas expectativas y puntos débiles.

Haciendo referencia a una entidad financiera, en donde las transacciones y comunicaciones electrónicas se llevan a cabo con tanta rapidez, la cantidad de trabajo y el negocio que se pierde en una hora es mucho mayor que en otras décadas y otros negocios. Según un informe que ha publicado Strategic Research Corporation, una empresa de consultoría y estudios de mercado de Santa Bárbara, California, el impacto financiero de una interrupción grave del sistema puede ser enorme: 6,5 millones de dólares americanos por hora en el caso de una operación de bolsa; 2,6 millones de dólares americanos por hora en el caso de un sistema de

autorización de tarjetas de crédito o la cantidad de 14.500 dólares americanos por hora en gastos de cajeros automáticos (ATM) si el sistema ATM no está activo.

En este entorno, la reputación de los ejecutivos responsables del rendimiento de su compañía está en juego. Las compañías que sufren una interrupción de su negocio online por cualquier motivo son noticia al día siguiente, y la prensa señala a los responsables con nombres y apellidos. Es más, los directores corporativos y los ejecutivos pueden ser demandados por las consecuencias de la interrupción del negocio o la pérdida de información crucial para la empresa. La mayoría de las grandes empresas estipulan en los contratos que los proveedores deben proporcionar servicios o productos bajo cualquier circunstancia.

Asimismo, la protección adecuada de los datos puede estar estipulada por ley, especialmente en el caso de una institución financiera. Todos estos factores hacen que la continuidad de negocio sea responsabilidad compartida de la alta dirección de una organización en su totalidad, desde el director financiero hasta los ejecutivos responsables de los procesos más importantes para la empresa. Aunque TI sigue siendo el principal componente de la fórmula para la continuidad empresarial, la dirección de TI no puede determinar unilateralmente qué procesos son los más importantes para la empresa y cuánto debe invertir para protegerlos.

1.3.2. Apoyo de las TI en tiempo de crisis

Según una encuesta realizada por Freeform Dynamics entre más de 700 directivos TI europeos, explica Josep Micolau, Delivery Director de CA**,** *"la pérdida de datos críticos para el negocio y el tiempo de inactividad de los sistemas clave de TI son dos de los mayores riesgos a los que se enfrentan los responsables de Tecnologías de la Información a la hora de planificar un Plan de Continuidad de Negocio. Este Plan debe permitir minimizar el*

tiempo de recuperación e impacto que supone cualquier incidencia que afecte al nivel de servicio de los procesos críticos de negocio".

De esta manera, el departamento de TI está en la obligación de construir una estrategia de recuperación de desastres que asegure la continuidad de los datos y, por tanto, del negocio y que esta se convierta en un aspecto de vital importancia. No es extraño que, cada vez más, los organismos judiciales, políticos y administrativos se preocupen por regular y legislar todos los aspectos relacionados con esta área. TI como unidad estratégica dentro de la organización debe implementar un Plan de Continuidad de Negocio asumiendo que lo peor ha sucedido. Este tipo de planes provee de una estructura operacional estratégica al departamento de TI gracias a la cual la organización entera pueda continuar ofreciendo los productos y/o servicios, que tengan al menos un componente tecnológico, a sus clientes, proveedores, empleados y socios como lo hace normalmente, al menos en sus procesos críticos, en el menor tiempo posible.

Considerando que una interrupción prolongada en las operaciones de los sistemas de información puede suspender la continuidad de las operaciones de una empresa y, eventualmente, llevarla incluso a la quiebra, es muy importante considerar el Gobierno de TI y las mejores prácticas para asegurar la continuidad de los negocios. Para esto se tienen varios conjuntos de recomendaciones que destacan internacionalmente en lo referente a continuidad de negocios sobre TI; tales como el ISO 17799 y CobIT de la Information Systems Audit and Control Association, ISACA.

Mantener una unidad de tecnología que actúe de manera adecuada ante la acción de recuperarse frente a un desastre puede ser una tarea ardua. Cada departamento de TI en los diferentes tipos de organizaciones podrían tener planes totalmente distintos de acuerdo a los servicios críticos que prestan dentro de las mismas. Algunos planes requieren una revisión

anual, otros una mensual y algunos necesitan ser revisados cada vez que un producto o el entorno sufre algún cambio; sin embargo, estos requieren actualizaciones o revisiones cada vez que se produce un cambio en uno o en varios de los cuatro factores siguientes en el seno de una organización: en el entorno, en el modo en que se ejercita el plan, en cambios en el objetivo de tiempo de recuperación (RTO) y en varios factores externos.

Los factores del entorno hacen referencia a cambios en la organización. Dado que los entornos de las TI varían constantemente, los cambios en el plan de continuidad de TI deberían ir en consonancia, de manera que los códigos y el personal se encuentren al corriente de esos cambios. Algunos ejemplos de cambios más comunes en el entorno de las TI son los cambios en el hardware y las actualizaciones del software, aplicaciones obsoletas o sustituidas, cambios de personal, reducción de la estructura empresarial y nuevas instalaciones y edificios. Cualquiera de estos cambios puede implicar un cambio necesario en el rango y en las funciones del personal. La ausencia de la correlativa actualización del plan de recuperación ante desastres podría dar lugar a complicaciones innecesarias en el seno de una organización.

El modo en que se pone en práctica el plan de continuidad de TI puede desvelar los cambios que es necesario realizar. Si los ejercicios a los que se somete el plan de recuperación ante desastres ponen suficientemente a prueba a sus participantes, TI debería ser capaz de decir si su plan es realista, completo y viable o no lo es. Desafortunadamente, muchos ejercicios de crisis no llegan a reproducir la complejidad de las condiciones del entorno de producción, o bien prescinden de la lista de prioridades en su conjunto. Los ejercicios de crisis bien planeados y ejecutados serán la mejor fuente de información sobre los planes de continuidad de TI, a falta de un evento en vivo de mayor entidad. Un evento en vivo puede incluir

cualquier cosa, desde un incidente que se comunica al servicio técnico hasta una interrupción total de la producción, incluyendo cualquier otra circunstancia entre estos dos extremos.

Además, hay que tener en cuenta que se puede mejorar el plan de continuidad de TI observando los incidentes que hayan ocurrido en el entorno de producción. Muchas organizaciones encuentran posibilidades de mejora incorporando a las actualizaciones del plan las lecciones aprendidas sobre los procesos de producción, especialmente si realizan una revisión anual del plan de continuidad.

Si los factores relacionados con el objetivo de tiempo de recuperación cambian, también deberá cambiar el plan de continuidad. Hay diversas causas que pueden generar un cambio en el RTO. Por ejemplo, las necesidades de recuperación de algunos procesos y funciones pueden ser más o menos urgentes. Los auditores van y vienen, sin olvidarse de dejar su lista de "cosas por hacer". Además, cuando se multiplican las interdependencias, éstas proporcionan una fuente constante de desafíos en la revisión del plan. Por último, las presiones del flujo de caja pueden obligar a una empresa a reconsiderar su estrategia de tiempo de recuperación o de sus necesidades, llegando a reducir la inversión en la recuperación ante desastres. Cualquiera de estos cambios relacionados con el RTO, o todos ellos, debería inducir a la organización a dar un segundo vistazo al plan de continuidad de TI y a realizar los cambios necesarios.

Hay factores externos que también pueden motivar cambios en el plan de continuidad; estos factores hacen referencia a entidades externas a la organización, e incluyen aspectos tanto preceptivos como potestativos. Los aspectos preceptivos comprenden requisitos legales y normativos, regionales y de otro tipo. Hay varios aspectos potestativos, tales como la subcontratación de otro centro de datos, la cual puede generar problemas desde dos puntos de vista: puede disminuir los niveles de alerta entre la organización matriz y la subcontratada; y

puede además aumentar los requerimientos de recuperación en la organización matriz. Por otro lado, la innovación tecnológica externa puede introducir nuevos riesgos en la recuperación ante crisis, aunque también nuevas soluciones.

La frecuencia con la cual se debería actualizar el plan de continuidad de TI depende de todos los factores anteriores. Muchas empresas optan por una frecuencia de revisión anual. Algunas organizaciones ni siquiera contemplen alternativas más frecuentes a ese calendario de revisión. Otras adoptan una actualización semestral o trimestral de los planes en función de elementos tales como el nivel de riesgo o la criticidad. Un enfoque finalista exige que los responsables del plan actualicen los planes cuando la situación lo requiera, independientemente de la fecha de revisión anual. Si bien este método tiene sus ventajas, es prácticamente imposible medir si los responsables del plan están respondiendo con la frecuencia que requieren las circunstancias. La dirección necesita garantizar que el mantenimiento de los planes se realiza con la frecuencia adecuada.

En última instancia, se deberá actualizar el plan de continuidad de TI cada vez que se produzca un cambio en un factor importante de la organización, al margen de que dicha variable sea interna o externa. Y el marco temporal en que se producen esos cambios es impredecible. Actualizar frecuentemente los planes de continuidad hace que éstos sean más completos y fiables, lo cual genera un entorno de trabajo más seguro en caso de una crisis.

CAPÍTULO II: SITUACIÓN ACTUAL

Una vez descritos los conceptos necesarios para el entendimiento general de la problemática a ser tratada en el presente trabajo, en este capítulo se dará un enfoque a la situación actual de Continuidad de Negocio tanto a nivel mundial como a nivel nacional y su estrecha relación con los departamentos de tecnología de las organizaciones.

2.1. Entorno Macro

Dentro de este entorno se analizarán las tendencias actuales y futuras del manejo de continuidad del negocio a nivel internacional así como el enfoque de los departamentos de TI sobre estos procesos; y aunque en teoría no guardan una relación causa-efecto con la administración interna de una organización en el Ecuador, tienen un efecto de condición sobre sus actividades.

2.1.1. Continuidad del Negocio a nivel mundial

Los sucesivos acontecimientos que han marcado los últimos tiempos en Estados Unidos, Europa, Asia y Latinoamérica; comenzando con la tragedia del 11-S[5] ocurrido el 11 de Septiembre del 2001, el apagón en el norte de Estados Unidos en Agosto del 2003, el incendio en el Hotel Windosor en Madrid-España en Febrero del 2005, otro incendio ocurrido en las bodegas de Almacenar en Cali-Bogotá en Mayo del 2005, el tsunami provocado por un terremoto en Japón en Marzo del 2011, han proporcionado un protagonismo significativo al concepto de continuidad de negocio.

[5] Atentado terrorista perpetrado en Estados Unidos en donde varios aviones comerciales fueron utilizados como armas empleadas a destruir blancos estratégicos-comerciales

Todos estos eventos no programados han ocasionado graves pérdidas de información, recursos y activos que son críticos para las empresas, que paralelamente se han traducido en importantes pérdidas económicas. A esto, se unen las apariciones de nuevas normativas y regulaciones, como Basilea II, Sarbanes-Oxley o MiFiD, las cuales obligan a salvaguardar y almacenar la información y sus activos. Efectivamente, para hacer frente a esta realidad, las empresas consideran la continuidad de negocio como un factor primordial que juega un rol decisivo en el desarrollo y crecimiento de su negocio; pero, anecdóticamente, todavía las organizaciones trabajan sin planes específicos de este tipo debido al elevado coste que supone invertir en infraestructuras propias o por desconfianza hacia el proveedor y los servicios que ofertan. Muestra de esta falta de inversión es el estudio desarrollado por Veritas (Ver figura 2.1) en el año 2012, en donde se muestra claramente que la mayoría de empresas a nivel mundial, aún cuando han concientizado sobre la importancia de contar con un adecuado manejo de la continuidad de negocio, todavía sus implementaciones carecen de validez y soporte frente a eventos catastróficos.

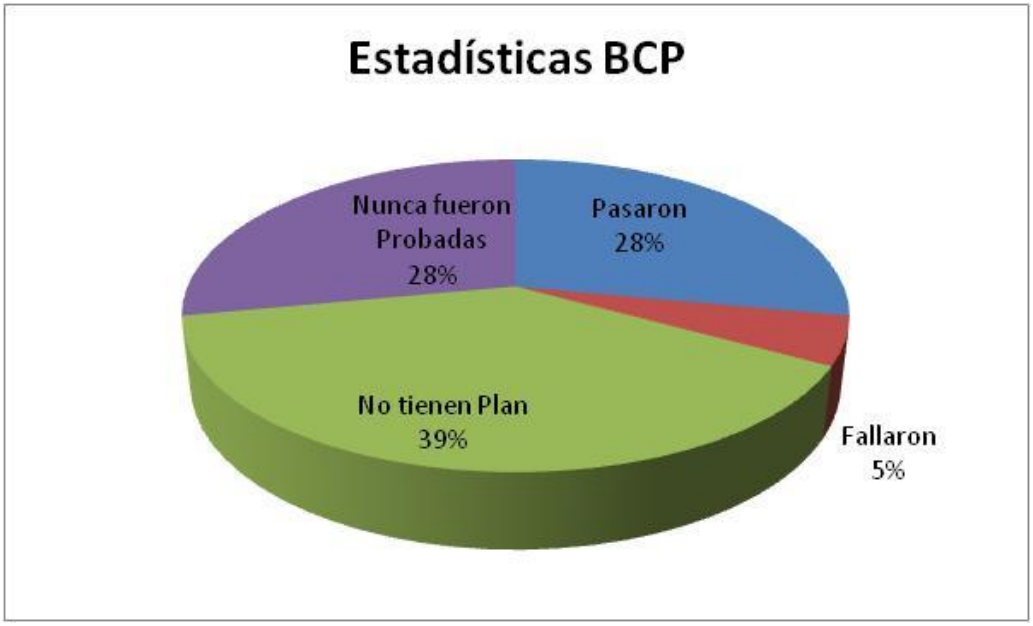

Ilustración 2. Estadísticas de Implementación de BCP. Fuente: Veritas Survey 2011

Sin embargo, y antes estas estadísticas, la continuidad de negocio es un concepto y una necesidad constante en toda actividad empresarial. Y es que, el hecho de que una parte significativa de las necesidades incluidas en dicho concepto se refieran al cumplimiento de normativa de diversa naturaleza, convierte la necesidad en una obligación la cual no se debe esperar a "activar" por una u otra causa. No hay que olvidar que la consecución de una adecuada continuidad de negocio responde, en algunos de sus objetivos, a la necesidad de cumplimiento de determinadas normas aplicables.

2.2. Entorno Micro

La necesidad de incrementar la seguridad ha crecido y se ha convertido en una prioridad para las empresas y sus profesionales del ámbito TI, que se plantean si sus organizaciones están preparadas para afrontar catástrofes y otras situaciones de crisis más frecuentes. En el Ecuador existen ya algunas iniciativas que intentan abarcar esta problemática tal como lo describiremos en los siguientes puntos.

2.2.1. Continuidad del Negocio en Ecuador

La continuidad empresarial en el Ecuador es vital para el éxito de la empresa: actualmente las empresas de nuestro país trabaja de manera interconectada con todas sus cadenas de producciones, ya sean estos proveedores, clientes, distribuidores entre otros: convirtiendo a sus operaciones vulnerables a interrupciones. De esta manera el empresario ecuatoriano ha comenzado a preocuparse por dichas interrupciones que se extienden mucho más allá de TI. Debido a la creciente cantidad de amenazas tanto locales como extranjeras hacia las organizaciones, el enfoque de "política de seguridad" ya no es suficiente.

Sin embargo, podemos notar que en el entorno empresarial del Ecuador no existen inciativas definidas para crear una responsabilidad de continuidad de negocios en las operaciones de dichas empresas. La Superintendencia de Compañías del Ecuador no tiene potestad sobre la forma de garantizar las operaciones de las empresas y por lo tanto brindar tranquilidad a sus clientes. Está claro que nuestros empresarios tardarán algún tiempo en adoptar como norma o política de seguridad la implementación de una Administración de Continuidad del Negocio, ya que usualmente el factor que mayor peso tiene en estas decisiones es el económico la hora de decidirse por una solución a un potencial problema. Es obvio entonces, que se espera a que un hecho grave ocurra en nuestra organización para tomar los correctivos, cuando la prevención puede salir mucho más adecuada y menos costosa.

En la teoría de administración de proyectos, al momento de efectuar el control de calidad de los entregables, siempre se hace énfasis en que al inicio pareciera que los costos de prevención son extremadamente altos y que quizás "nunca se los vaya a utilizar" la evidencia demuestra que si un riesgo se hace tangible esa inversión es recuperada hasta en tres veces su valor. Muchos empresarios ecuatorianos aún mantienen ciertas ideologías que les impide implementar políticas de continuidad de negocios, esos pensamientos se basan en frases tales como "Somos demasiado grandes para caer..", "A nosotros nunca nos ha sucedido eso…", "No somos un blanco terrorista", sin embargo cuando estos eventos se presentan en una compañía pueden inclusive acabar con la existencia de las mismas.

Ante estos escenarios, la única actividad económica que se encuentra regulada en el Ecuador y que obliga a sus operantes contar con una adecuada Administración de Continuidad de Negocios son la Banca y Finanzas, pues las consecuencias de afectar las operaciones financieras en estas instituciones impactaría directamente en la economía y estabilidad del país entero.

Bajo este escenario, la Superintendencia de Bancos y Seguros del Ecuador, bajo resolución No. JB-2005-834 del 20 de Octubre del 2005, generó una normativa de la gestión y administración de riesgos aplicable a la ley general de instituciones del sistema financiera. Esta resolución ha sido mejorada y actualizada con el pasar de los años generando en su última revisión varios artículos referentes a este tema:

"*4.3 Tecnología de información: Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones*"[6].

"*Artículo 15.- Las instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. (artículo renumerado con resolución No. JB-2008-1202 de 23 de Octubre del 2008)*"[7].

Bajo esta regulación, todas las entidades financieras controladas por la Superintendencia de Bancos y Seguros del Ecuador están en la obligación de implementar una administración de continuidad del negocio soportada en los procesos de TI que sean necesarios: y tal como se mencionó anteriormente, son las únicas "obligadas" a cumplirlo.

[6] Normativa de Riesgo Operativo, Sección II.- Factores del Riesgo Operativo, Artículo 4
[7] Normativa de Riesgo Operativo, Sección IV.- Continuidad del Negocio

2.2.2. Administración de Continuidad del Negocio en los departamentos de TI de la Banca Privada en Ecuador

Tal como se mencionó en el punto anterior, la Superintendencia de Bancos normó la implementación de un plan de continuidad que permita mantener las operaciones activas de un banco en caso de una crisis. Actualmente cualquier proceso de negocio de un Banco se encuentra apalancado en una o varias plataformas tecnológicas y operativas; por lo tanto para brindar una continuidad de negocio a los procesos críticos definidos dentro de la institución, es imprescindible contar con un plan tecnológico que aumente la disponibilidad de dichos elementos a fin de dar cumplimiento con el tiempo de operación inactivo soportado por las instituciones financieras.

Dentro de la administración de continuidad del negocio, existen varios planes que deben ser implementados, dentro de los cuales podemos mencionar los siguientes:

- Plan de Manejo de Crisis, Area: Directorio del Banco
- Plan de Unidad de Negocios, Area: Vicepresidencias de cada unidad
- Plan de Recuperación de Desastres, Area: Vicepresidencia de TI
- Plan de Respuestas de Emergencia, Area: Seguridad física
- Plan de Continuidad del Negocio, Area: Todas las Vicepresidencias

Tal como se indica, la Vicepresidencia de TI de un Banco es la encargada de implementar el Plan de Recuperación de Desastres (DRP: Disaster Recovery Plan) el cual hace referencia a la disponibilidad de todos los elementos tecnológicos que la entidad requiera para continuar con su operación luego de una crisis. En una institución financiera, todo gira alrededor de sistemas de información, no solo los procesos que involucran el dinero de los clientes, sino todos los elementos que son posibles mantener la operación en línea: consultas,

transacciones, registros, eliminaciones, etc. Es tan importante la operación de los sistemas de información que una interrupción prolongada de los mismos puede hacer que se detenga la operación de la compañía y presentar pérdidas económicas. Inclusive puede generar pánico de mercado, lo que provocaría que todos los cuenta ahorristas y corrientes retiren sus fondos de manera inmediata provocando la iliquidez inmediata de la institución.

Según una encuesta realizada por Freeform Dynamics entre más de 700 directivos TI europeos, explica Josep Micolau, Delivery Director de CA, "*la pérdida de datos críticos para el negocio de una entidad financiera y el tiempo de inactividad de los sistemas clave de TI son dos de los mayores riesgos a los que se enfrentan los responsables de Tecnologías de la Información a la hora de planificar un Plan de Continuidad de Negocio. Este Plan debe permitir minimizar el tiempo de recuperación e impacto que supone cualquier incidencia que afecte al nivel de servicio de los procesos críticos de negocio*".

Para Ángel Fernández, director general de Hitachi Data Systems en España y Portugal, "*una estrategia de recuperación de desastres que asegure la continuidad de los datos y, por tanto, del negocio se convierte en un aspecto de vital importancia. No es extraño que, cada vez más, los organismos judiciales, políticos y administrativos se preocupen por regular y legislar todos los aspectos relacionados con esta área".*

Desde la perspectiva de Fernando Martínez, country presales Manager de Symantec para Latinoamérica, *"el valor de la información se ha multiplicado en la actualidad. Por ello, la Continuidad del Negocio ha sido una de las prioridades para las empresas y las organizaciones, convirtiéndose así en uno de los pilares fundamentales en materia de gestión de seguridad, almacenamiento de datos y recuperación ante desastres".*

En el sector financiero y de servicios es imprescindible se cuente con la capacidad para restablecer las operaciones de TI. Los riesgos asociados son muy altos y la alta dependencia en las tecnologías de información y de telecomunicaciones ha motivado la necesidad de contar con las medidas preventivas adecuadas y con un nivel de continuidad que les permita ejecutar sus procesos de negocio sin ningún tipo de pérdida o la mínima.

Es necesario estar protegido de las múltiples (y hasta desconocidas) amenazas, garantizando

fundamentalmente, la preservación de tres características:

- **Integridad:** que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento.
- **Confidencialidad:** que la información sea accesible solo a las personas autorizadas.
- **Disponibilidad:** que los usuarios autorizados tengan acceso a la información y los recursos cuando lo necesiten.

La norma IRAM/ISO/IEC17799 sostiene que "la seguridad de la información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al negocio y maximizar el retorno sobre las inversiones y las oportunidades", también agrega "la seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software".

Para lograr ello, se debe identificar los procesos y recursos críticos, entender los riesgos e impactos por interrupciones, definir estrategias y planes de recuperación, entrenar a las personas involucradas, realizar ejercicios de prueba y mantener actualizados los planes y procedimientos.

Esto les permite proteger a su personal, sus recursos, su reputación y sus relaciones con clientes y proveedores, además de la ventaja competitiva que representa el contar con una habilidad de mantener la continuidad de sus operaciones y cumplir con sus compromisos.

El plan de recuperación ante desastres es un elemento más que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operativa mínima luego de una contingencia, en la que se vean afectados los procesos y recursos informáticos que sostienen el negocio.

De esta manera, el Plan de Recuperación de Desastres (DRP) a ser implementado en el departamento de TI responde a cómo los sistemas de información podrán funcionar nuevamente una vez que un siniestro se haya tornado realidad; el DRP apoyado en el Plan de continuidad del negocio (BCP) permitirá conocer al departamento de TI cuáles de esos sistemas son más críticos de recuperar, su orden de recuperación y su tiempo máximo de inactividad tanto en datos como en transacciones.

2.2.3. Banco Privado como caso de Estudio

Según un informe generado por la Superintendencia de Bancos y Seguros emitido a inicios del año 2009, en donde se analizó la situación actual de los Bancos Privados en esa fecha, se identifica que únicamente dos de los diez bancos analizados tienen un Plan de Continuidad generado, sin embargo ninguno de ellos han completado el proceso de pruebas y difusión del mismo dentro de sus organizaciones.

Muestra de ello es el evento generado en Banco de Guayaquil a inicios del año 2012, que al ser uno de los bancos con un BCP generado, tuvieron que ponerlo en marcha debido a la indisponibilidad de varios de sus servidores de datos. Dicho plan falló por la falta de pruebas

programadas, lo cual generó miles de pérdidas a la institución y varios llamados de atención por parte de los entes reguladores.

En el informe antes especificado, se indica como conclusión del ente regulador que: "*El grupo de bancos más grandes del país todavía no ha definido la metodología para la administración de la continuidad del negocio, responsables de su ejecución, cronogramas de cumplimiento, no cuentan con un Plan de Continuidad del Negocio ni tampoco con un sitio alterno de procesamiento, lo cual podría afectar de manera significativa las operaciones de las entidades e incluso del sistema financiero.*"[8]

Aún cuando se han generado varias iniciativas de uno de esos bancos a partir del año 2009 para eliminar esta observación, la metodología y aplicación del Plan de Continuidad dentro de TI no ha sido definida ni implementada al momento, es por este motivo que se ha decidido seleccionar al "*Banco Nacional Financiero*"[9] para la implementación del presente proyecto.

[8] Informe de evaluación de la Banca Privada de la Supertendencia De Bancos y Seguros del Ecuador, año 2009
[9] Banco Nacional Financiero es el nombre seleccionado para proteger la identidad de la organización seleccionada

CAPÍTULO III: DEFINICIÓN DE METODOLOGÍA

De acuerdo a lo especificado en el Capítulo 1, literal 1.1.3 Metodologías Disponibles del presente documento, se ha generado un análisis de cuáles de esas metodologías puede ser aplicable al Banco Nacional Financiero para la implementación de su Administración de Continuidad del Negocio. Tomando en cuenta la madurez y aplicabilidad de esas metodologías en el entorno actual de esta organización, se ha decidido seleccionar como un marco de referencia a la metodología "BS 25999-1 BS 25999-2"; sin embargo, los procesos y procedimientos definidos en dicha norma deberán ser adaptados a la realidad de la empresa, tal como se detalla en los siguientes literales del presente capítulo.

3.1. Metodología de Administración de Continuidad de Negocios en TI

Tomando como marco de referencia la norma BS 25999-1/2, debido a su grado de madurez dentro de la Administración de Continuidad de Negocios, y además por brindar conceptos claros de procesos y procedimientos a implementar, se ha decidido definir la siguiente metodología para Banco Nacional Financiero descrita a continuación:

3.1.1 Fase I: Análisis de Procesos del Banco

Cada vez que la organización ha identificado un nuevo producto o servicio a entregar, ya sea a clientes internos o externos; dichos entregables se convierten en un proceso que la misma organización debe ejecutar. Para cada nuevo proceso generado dentro de la organización es necesario seguir los siguientes pasos descritos a continuación:

- La Unidad de Riesgos Operativos, en conjunto con el Departamento de TI, evalúa los riesgos asociados a ese nuevo componente y se generan los planes y acciones de mitigación.
- El Negocio es consultado en base a su criterio si este nuevo componente es crítico para el Banco o no.
- Si el Negocio considera que es un proceso crítico se procede a agendar sesiones de evaluación entre el oficial de continuidad y el referente o responsable del nuevo componente.
- En el primer paso de las sesiones se hace un análisis del impacto operacional (no financiero), evaluando la categoría para cada punto operacional así como el valor (entre 1 y 5) con su respectiva justificación
- Se procede con el análisis del impacto financiero, evaluando la categoría a nivel económico por pérdida de ingresos y aumento de costos así como el valor (entre 1 y 5) con su respectiva justificación.
- Una vez concluidas las evaluaciones a nivel financiero y no financiero (operacional) se procede a hacer la conversión de los valores asignados obteniendo únicamente tres rangos para cada proceso (1,2 y 3). Si el componente en cualquier categoría se ubica en 3, es considerado como crítico para el Banco.
- Si el componente ha sido identificado como crítico, se procede con el cuestionario BIA (Bussiness Impact Analysis). Fase II

3.1.2 Fase II: Análisis de Impacto de Negocios (BIA)

Esta Fase es la de mayor importancia en el plan debido a que de ella surge el informe que permitirá a Banco Nacional Financiero evaluar el riesgo que existe en cada proceso o aplicación de negocio y su impacto en la entidad.

En base a los informes que se entregarán, la entidad deberá proceder a su revisión y aprobación para poder continuar con la siguiente fase de identificación y determinación de la estrategia de recuperación de los procesos de negocio críticos.

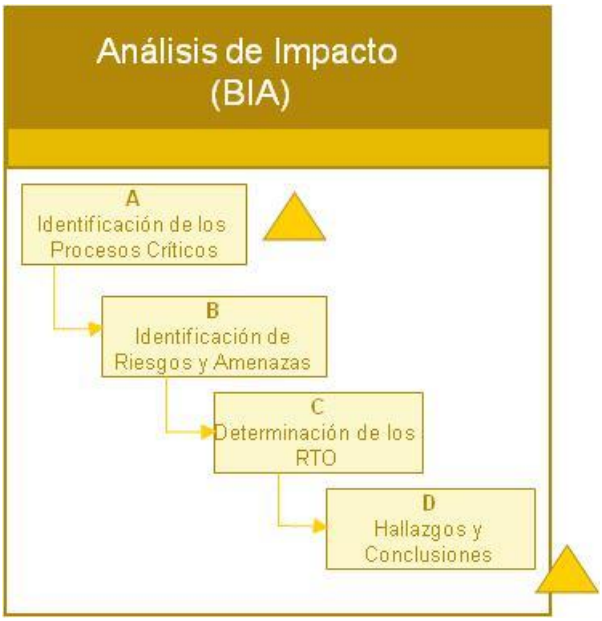

Ilustración 3. Proceso de Análisis de Impacto (BIA). Elaborado por: Wilson Jácome

Pasos:

- Identificar y evaluar riesgos y amenazas
- Revisar las prácticas administrativas y controles físicos
- Utilizando la información disponible, a través de entrevistas y workshops con el personal clave de negocios de Banco Nacional Financiero se identificarán los procesos de negocios críticos
- En conjunto con el personal de la compañía, determinar los objetivos de tiempo de recuperación para cada proceso clave
- Identificar las interdependencias entre procesos

Herramientas:

- Checklist de Análisis de Riesgo
- Bases de conocimiento
- Cuestionarios de relevamiento de recursos

Productos:

- Listado de procesos críticos
- Ranking de los procesos de negocios de misión crítica
- Objetivos de Tiempo de Recuperación (RTO)

- Identificación de Riesgos y Amenazas
- Recomendaciones para la mitigación de riesgos
- Informe de Análisis de Impacto en el Negocio

Para detalle de información BIA a ser entregada, ver Anexo D

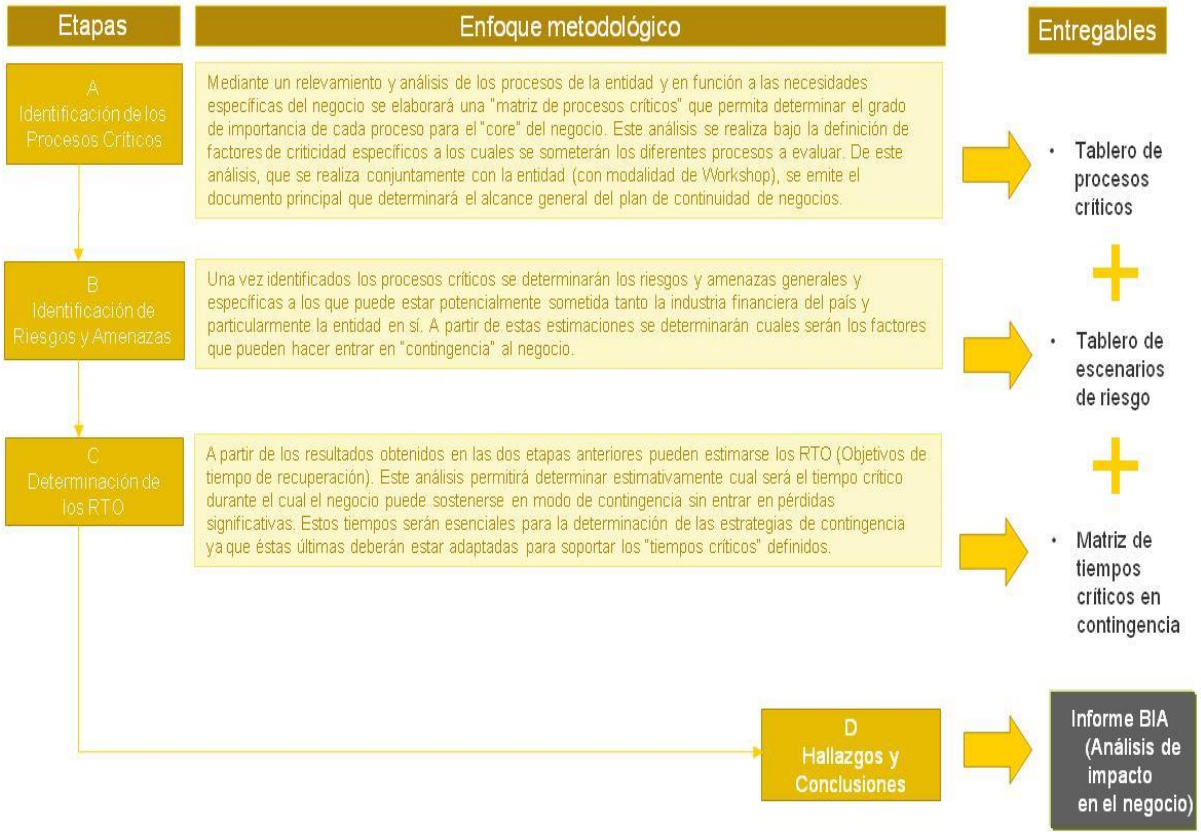

Ilustración 4. Enfoque Metodológico de BIA. Elaborado por: Wilson Jácome

3.1.3 Fase III: Selección de Estrategia

La ejecución de esta Fase se limita a los siguientes pasos:

- Definición del DRP (Disaster Recovery Plan)
- Efectuar workshops o reuniones de trabajo con el personal clave responsable de los procesos críticos a los efectos de seleccionar la estrategia.
- En caso de ser necesario contratar proveedores de bienes y/o servicios sus respuestas o información requerida sean recibidas en un plazo no mayor a dos semanas.

Ilustración 5. Proceso de Selección de Estrategia. Elaborado por: Wilson Jácome

Pasos:

- Identificar todas las alternativas de recuperación viables y diseñar el DRP
- Realizar un análisis de costo beneficio para cada alternativa, si corresponde
- Identificar los recursos mínimos necesarios para la recuperación

Herramientas:

- Estándares de la industria e información de las mejores prácticas del mercado
- Cuestionarios de relevamiento de recursos

Productos:

- Diseño del DRP
- Listado de recursos mínimos requeridos para la recuperación
- Listado de alternativas de recuperación viables
- Informe de selección de estrategias

Ilustración 6. Enfoque de Metodología de Selección de Estrategias. Elaborado por: Wilson Jácome

Dentro de esta metodología se cuenta con la fase de definición de estrategia cuyo objetivo es identificar la estrategia que mejor se adecua a las necesidades de recuperación de Banco Nacional Financiero y a partir de ella identificar los recursos mínimos necesarios para su implementación y eventual ejecución.

Antes de arrancar con la selección de estrategias es necesario y mandatorio haber definido un DRP (Disaster Recovery Plan) el cual está orientado únicamente al plan de Recupero de IT de Banco Nacional Financiero, en esta etapa además de definirlo, posteriormente se validará que éste plan establezca las aplicaciones y servicios informáticos que dan soporte a los procesos de negocio críticos, se analizará su alineación con el BCP y se debe entregar un informe de diagnóstico.

Para esta fase del proyecto se debe verificar con personal de la organización que los procesos críticos que surgieron en la etapa anterior y que fueron aprobados, pueden ser recuperados.

Asimismo, se debe identificar las posibles estrategias de recuperación para aquellos procesos operativos críticos no relacionados con aspectos informáticos.

Por lo tanto en esta etapa los productos que se deben entregar serán los siguientes:

- Procesos de negocio críticos
- Plan de Recuperación de Desastres TI (DRP)
- Identificación de estrategias de recuperación posibles.
- Informe de selección de estrategias

3.1.4 Fase IV: Desarrollo del Plan de Continuidad de TI

Un Plan de Continuidad es un mecanismo de respuesta que asegura orden y control durante una interrupción operacional. Estos planes incluyen la Identificación del Incidente, Evaluación, Escalamiento, Declaración, Activación del Plan, Desactivación del Plan y procedimientos de Restauración. Este plan está compuesto por el Plan de Continuidad del Negocio (BCP), el cual ayuda a continuar y mantener los procesos críticos del negocio, y el Plan de Recupero de Sistemas (DRP), mediante el cual se restauran los sistemas e infraestructura que soportan a los procesos críticos antes identificados. El resultado final del Plan de Continuidad de Negocios de TI corresponde al mapeo de los procesos críticos del negocio con el Plan de Recuperación de Desastres o Plan de Recupero de Sistemas.

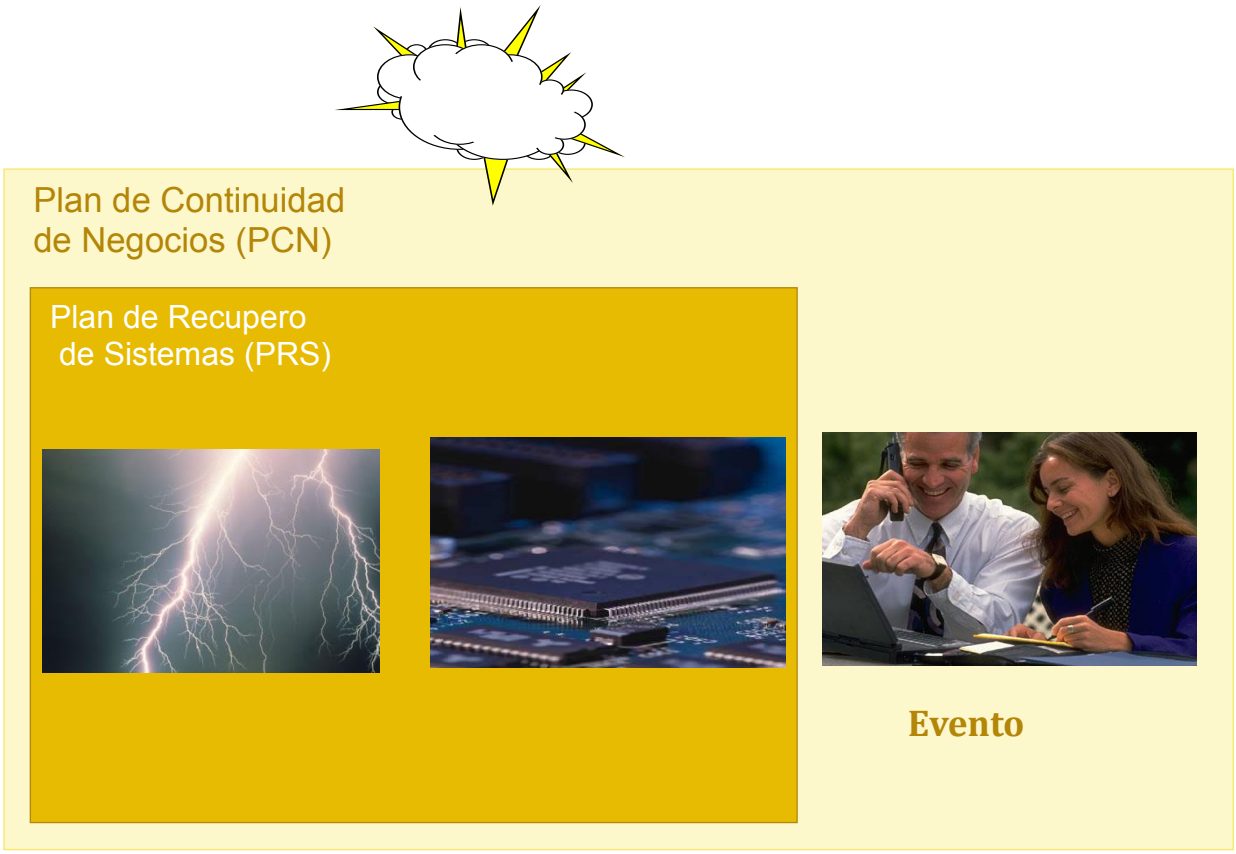

Ilustración 7. Enfoque del Plan de Continuidad del Negocio. Elaborado por: Wilson Jácome

Comprenden las siguientes tareas:

- Desarrollo de los procedimientos técnicos de contingencias
- Desarrollo del Plan de Recuperación de Sistemas o Plan de Recuperación de Desastres (PRS – DRP)
- Definición de los escenarios para retornar a la operación normal y preparación del plan de trabajo para recuperar la normalidad en las operaciones tecnológicas afectadas por la contingencia

Prerequisitos de información:

- Inventario de procesos, aplicaciones, hardware y enlaces de comunicaciones
- Análisis de impacto de las aplicaciones y/o procesos actualizado (BIA elaborado en la Fase I)

- Site/Sites de contingencias definidos
- Estrategia de recuperación definida (alineada a la del BCP TI)
- Requerimientos actualizados de hardware, software y conectividad para la estrategia de contingencias adoptada.

Procedimientos de contingencias:

En base a los documentos de análisis de criticidad de los procesos y aplicaciones actualizado más la estrategia de contingencias, se desarrollaran documentos de:

- Procedimientos de DRP
- Procedimientos generales de administración del plan
- Equipo de contingencias
- Procedimientos a realizar para cada aplicación crítica

Productos a entregar:

- DRP preliminar
- BCP preliminar

Confección del Plan de Continuidad de TI y del Plan de Recuperación de Desastres:

La documentación del Plan de Continuidad de Negocios de TI (BCP) y del Plan de Recuperación de Desastres (DRP) se realizará una vez que se cuente con la aprobación formal de las estrategias de recuperación de la fase anterior de forma tal de contar con la base para el diseño de los procedimientos de recuperación. Los componentes de esta fase son los siguientes:

- Documentar los procedimientos del BCP de TI y del DRP en base a la información que proveerán los involucrados en cada proceso de negocio y procesos técnicos.
- Distribuir los planes en su versión borrador para su revisión y aprobación por los usuarios que ejecutarán el plan.

Luego de la confección de los planes, y una vez cumplida las aprobaciones formales del mismo, se inicia la fase de Comunicación, cuyo objetivo es preparar la documentación de comunicación interna de la metodología e instruir al personal acerca de cómo actuar ante la necesidad de aplicación del Plan de Continuidad de Negocio de TI.

Asimismo, se debe incluir una sesión de capacitación final a todos los responsables del proceso de mantenimiento futuro del plan de manera de transmitir la metodología de mantenimiento documentada, el uso de las herramientas que se utilizarán, los mecanismos de control, checklists, formularios de aprobación y demás documentación mencionada en la estrategia de mantenimiento y acordados en el proyecto.

Ilustración 8. Proceso de Desarrollo del Plan. Elaborado por: Wilson Jácome

Pasos

- Desarrollar los procedimientos de recuperación e identificar a los miembros de los equipos
- Desarrollar y documentar el borrador del BCP y del DRP

Herramientas

- Template de recursos
- Formatos standard de Planes

Productos

- Borrador del BCP y del DRP
- Elaboración del material a utilizar durante la capacitación.

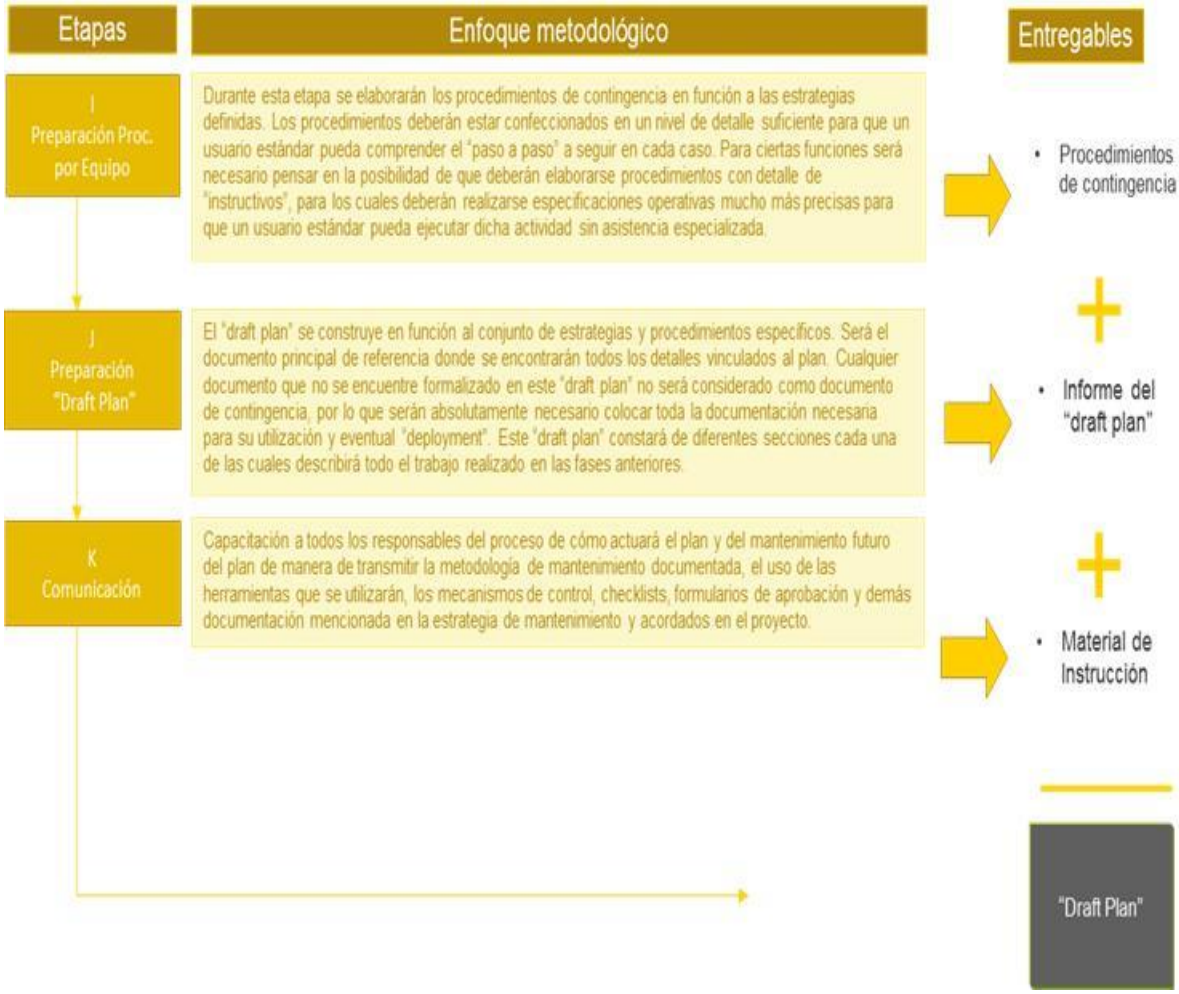

Ilustración 9. Enfoque de Metodología de Desarrollo de los planes. Elaborado por: Wilson Jácome

3.1.5 Fase V: Prueba y Mantenimiento

Prueba del Plan

Esta fase se inicia con la definición del tipo de pruebas que se realizarán y la documentación de un plan de pruebas. Se debe realizar una simulación total y una prueba parcial de los BCP y DRP desarrollados.

Esta etapa debe arrancar con la prueba parcial y prueba del DRP y luego continuar con la simulación total, de manera de que la prueba parcial sirva como elemento corrector del plan en su primer versión.

En base a los resultados de las pruebas se modificará el borrador del plan y se generará la versión final.

Para cada una de las pruebas previstas se generará un informe con el resultado de las mismas que el Banco debe presentar ante organismos de regulación como elemento que demuestra la existencia del Plan y la realización de pruebas.

En esta etapa también se documenta la estrategia futura de pruebas y actualizaciones del plan.

Ilustración 10. Proceso de Prueba y Mantenimiento. Elaborado por: Wilson Jácome

Pasos

- Entregar la versión final del Plan de Continuidad de Negocios de TI
- Desarrollar procedimientos de prueba y mantenimiento en base a las mejores prácticas del mercado

Herramientas

- Bases de conocimiento

- Templates de Planes de prueba
- Checklist de rutinas de mantenimiento
- Templates formularios

Productos

- Procedimientos de Prueba y Mantenimiento
- Versión final del Plan de Continuidad de Negocios de TI

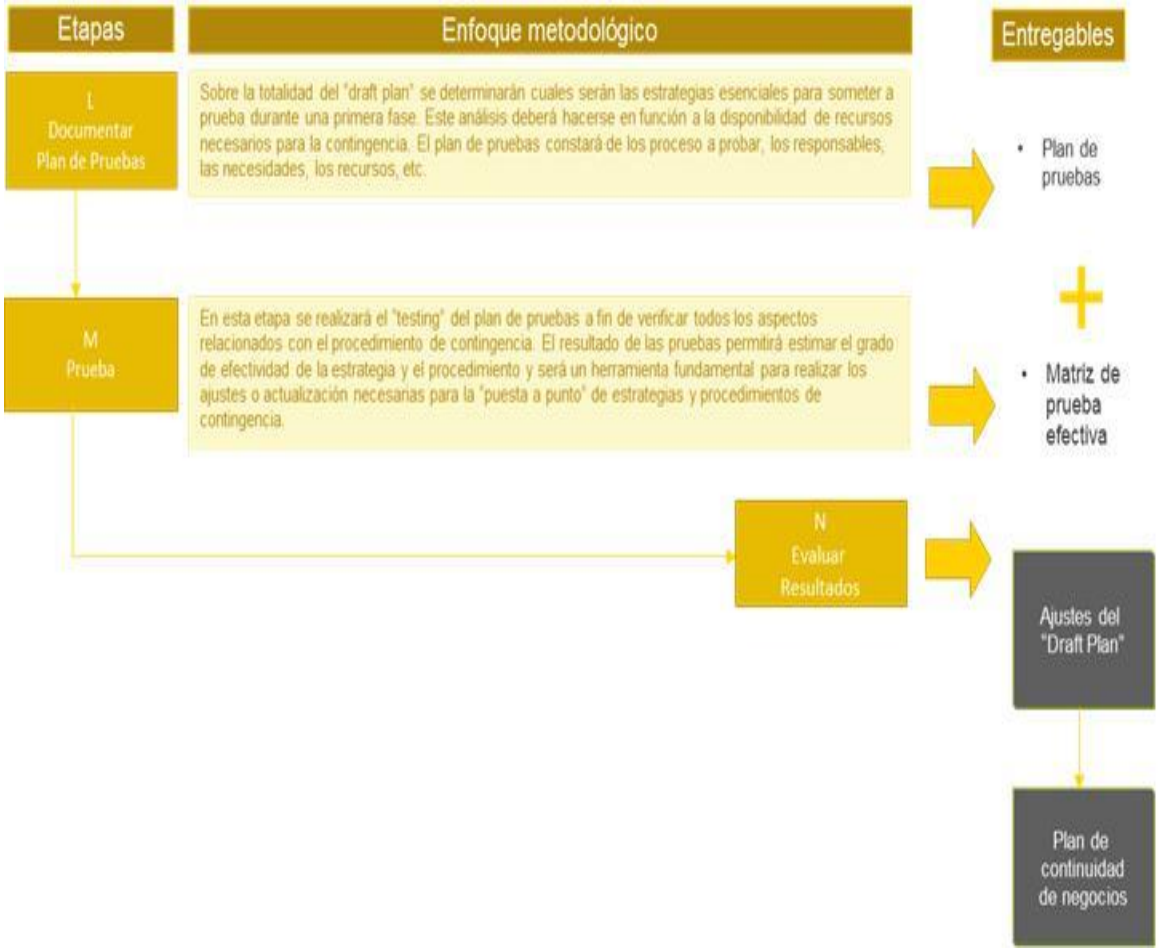

Ilustración 11. Enfoque de Metodología de Prueba y Mantenimiento. Elaborado por: Wilson Jácome

Un plan de continuidad de negocios de TI debe contar con un plan de mantenimiento activo para capturar la naturaleza dinámica del negocio. El plan debe ser revisado a intervalos regulares de tiempo para confirmar que los componentes más importantes se mantienen

actualizados, así como también para identificar e incorporar en forma inmediata aquellos cambios importantes que puedan comprometer su efectividad.

Se debe definir una estrategia para el mantenimiento de los planes de continuidad de negocio de ti en base a las mejores prácticas del mercado. Los principales aspectos que incluye esta estrategia se detallan a continuación:

- Revisiones Cuatrimestrales y Checklists de mantenimiento de PCN
- Revisiones Anuales y Checklists de mantenimiento anual
- Proceso de aprobación del Plan y sus formularios
- Revisiones de eventos estipulados

La guía estratégica de mantenimiento debe contar con todos los elementos, procedimientos, formularios, circuito de aprobación (workflow) para que el Banco pueda realizar el mantenimiento de todo el Modelo Operativo del Plan de Continuidad de Negocio de TI.

3.2. Entregables de la Metodología

Generando un resumen de todos los procesos propuestos en el punto anterior, sobre la definición de la metodología de continuidad de negocios de TI, es necesario hacer referencia a los entregables finales que presentará el presente trabajo, así como su orden de implementación:

1. BIA’s de Negocio
2. BIA’s de TI
3. Estrategias Tecnológicas para soportar a los procesos críticos de negocio y de TI

4. Implementación de estrategias
5. Pruebas de estrategias

La siguiente figura muestra de manera general la metodología definida para este proyecto y sus fases en la ejecución de un desastre:

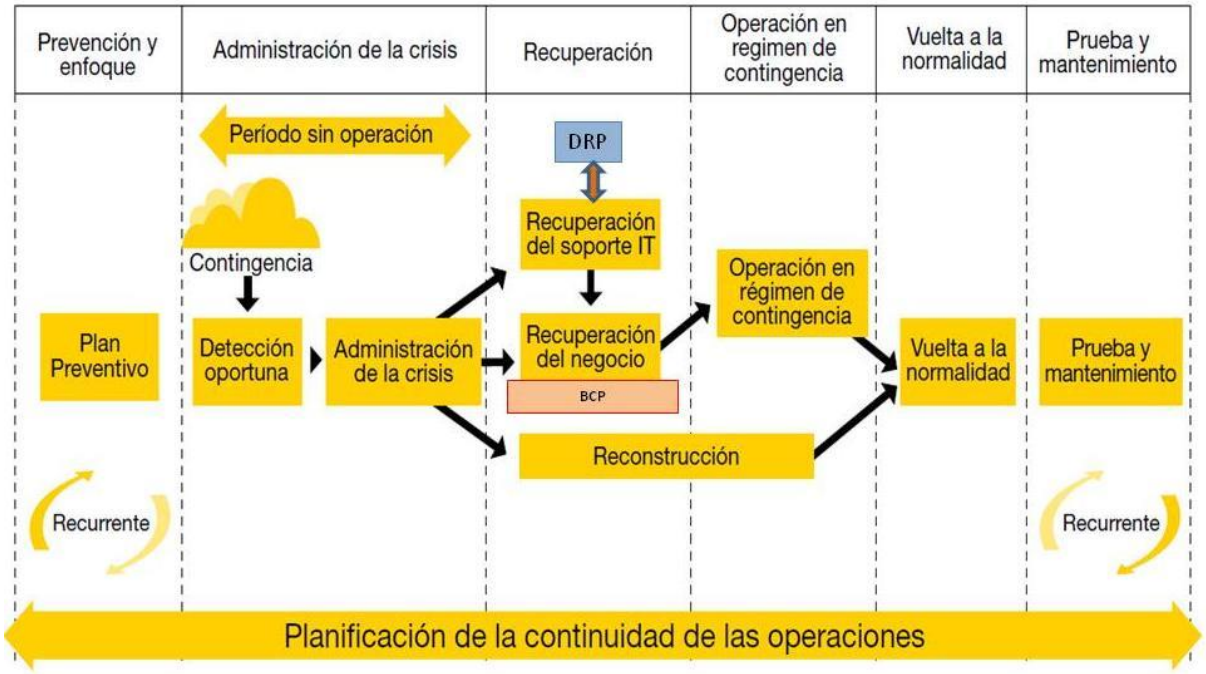

Ilustración 12. Metodología definida. Elaborado por: Wilson Jácome

Se debe definir una estrategia para el mantenimiento de los planes de continuidad de negocio de ti en base a las mejores prácticas del mercado. Los principales aspectos que incluye esta estrategia se detallan a continuación:

CAPÍTULO IV: IMPLEMENTACIÓN DE METODOLOGÍA

Históricamente, el plan de continuidad de negocios ha residido en el departamento de tecnología en la gran mayoría de las organizaciones. Por esta razón, muchas compañías tienen alternativas de recuperación de desastres en lugares geográficamente dispersos del principal para sus servicios de TI. La continuidad de negocios de TI debe soportar los procesos de negocio, ya que busca asegurar que dichos procesos se encuentran protegidos de desastres, y que la organización es capaz de responder positiva y efectivamente cuando estos hechos se presenten.

A continuación se describirán los procesos que han sido implementados en Banco Nacional Financiero para blindar de resilencia tecnológica a la organización sobre la ocurrencia de eventos que pueden afectar al negocio en caso de un desastre.

4.1. Análisis de Procesos Críticos del Negocio

Para el análisis de los procesos críticos del negocio se tomó como base de referencia el documento denominado “Base Técnica de PCN” desarrollado y provisto por la unidad de riesgos operativos de Banco Nacional Financiero. En dicho documento se especificaban alrededor de 68 procesos de criticidad alta para el negocio. Para cada uno de esos procesos, y aplicando lo descrito en la metodología, se realizó un análisis de impacto operacional y financiero en el negocio en el caso de que cada uno de esos procesos sufra una para en su operación.

El resultado de estos análisis financieros y operativos generó como resultado la tabla final de procesos críticos a ser analizados en detalle, incluyendo cada uno de los referentes a quienes

fue necesario ejecutar las entrevistas para poder generar como salida el BIA de cada uno de esos procesos:

Macroproceso	Proceso del negocio	Referente	Usuario clave
Gestión de Tarjetas y Consumo	Activación de tarjetas canales	Subgerente de Tarjetas	Ejecutivo de Tarjetas A
	Autorizaciones – Aprobadas	Subgerente de Tarjetas	Ejecutivo de Tarjetas A
	Monitoreo y Fraude	Subgerente de Tarjetas	Ejecutivo de Tarjetas A
	Gestión de tarjetas de crédito Boletín 21	Subgerente de Tarjetas	Ejecutivo de Tarjetas A
Servicio al Cliente	Atención cajas	Subgerente de Sucursales	Ejecutivo de agencia
	Atención canales electrónicos (ATMs)	Subgerente de Canales	Subgerente de Canales
	Call Center	Subgerente de Canales	Subgerente de Canales
	Banca Electrónica	Subgerente de Canales	Ejecutivo de Banca Móvil
Administración de Servicios Financieros (Cash Management)	Afiliación empresas	Subgerente empresas	Subgerente empresas
	Liquidación y contabilización	Subgerente empresas	Subgerente empresas
Canje y compensación	Canje y compensación	Subgerente de Sucursales	Subgerente de Sucursales
Gestión de Compras, Pagos y Distribución	Logística y distribución de documentos	Subgerente de Seguridad	Ejecutivo de logística
	Logística y distribución del efectivo	Subgerente de Seguridad	Ejecutivo de logística
Administración de Servicios Institucionales	Administración de seguridad física	Subgerente de Seguridad	Ejecutivo de seguridad

Macroproceso	Proceso del negocio	Referente	Usuario clave
Gestión de Tesorería	Administración de liquidez y posición	Subgerente de Negocios Internacionales	Ejecutivo de Banca
	Administración de portafolios institucional	Subgerente de Negocios	Ejecutivo de Banca

		Internacionales	
	Administración de Portafolio Internacional	Subgerente de Negocios Internacionales	Ejecutivo de Banca
	Análisis y gestión de la información	Subgerente de BI	Ejecutivo de Análisis de Datos
	Administración de captaciones	Subgerente de Negocios Internacionales	Ejecutivo de Banca
Manejo de Captaciones	Prohibiciones (cheques y certificados de inversión) Seg. Personas	Subgerente de Negocios Internacionales	Ejecutivo de Banca
	Prohibiciones (cheques y certificados de inversión) Seg. Empresas	Subgerente de Canje	Ejecutivo de Cámara
	Consideraciones de Cámara (Seg. Empresas)	Subgerente de Canje	Ejecutivo de Cámara
	Consideraciones de Cámara (Seg. Personas)	Subgerente de Canje	Ejecutivo de Cámara
Originación de Crédito	Instrumentación Desembolso (Segmento Personas)	Subgerente de Crédito	Ejecutivo de Crédito
	Instrumentación Desembolso (Segmento Empresas)	Subgerente de Crédito	Ejecutivo de Crédito
	Instrumentación Desembolso (Segmento Consumo)	Subgerente de Crédito	Ejecutivo de Crédito
	Confirmación Rechazo de Negocio Emisión de Instrumentos Comex	Subgerente de Crédito	Ejecutivo de Crédito

Tabla 1. MacroProcesos Críticos. Elaborado por: Wilson Jácome

Para cada uno de los procesos ya identificados como críticos se procedió mediante talleres a completar el formulario BIA (análisis de impacto), los cuales fueron formalmente aprobados

por cada referente del proceso. El propósito de completar los Formularios de Análisis de Impacto del Negocio (BIA) fue:

- Determinar el grado de criticidad de cada proceso de negocio evaluado.
- Identificar los servicios tecnológicos que soportan al proceso crítico identificado.
- Determinar el impacto operacional y financiero de la pérdida o interrupción del proceso crítico.
- Identificar los objetivos de recuperación (tiempos, información de negocio) y recursos necesarios para concretar dicha recuperación.

A fin de relevar las particularidades de cada proceso crítico, incluyendo sus riesgos y amenazas, el formulario del BIA comprendió los siguientes aspectos:

- Descripción del proceso en contingencia.
- Análisis de riesgos y amenazas.
- Entradas y salidas de información.
- Proveedores y terceros.
- Requerimientos de información de entidades reguladoras.
- Recursos de soporte.
- Dependencia en las telecomunicaciones y de los aplicativos.
- Equipamiento específico.
- Impacto financiero: Pérdida de ingresos y Aumento de Costo.
- Impacto no financiero de una interrupción: Necesidades de clientes / Servicio al cliente / Requerimientos legales / Incremento en las responsabilidades legales /Imagen en el medio/Confianza de los accionistas/Suspensión de las operaciones.
- Alternativas de contingencia.

La información registrada en los formularios fue compilada, lo que permitió identificar:

- Ordenamiento de procesos críticos, por combinación de impactos
- Riesgos y amenazas de los procesos

Una vez evaluados los BIAs, se realizó un resumen de los RTO (Objetivos de Tiempo de Recuperación) para establecer las prioridades respecto a los planes de acción sobre cada proceso crítico. Se determinó el mapa de RTO, clasificando cada uno de los procesos dentro del mapa que se muestra a continuación:

1 h	6 h	24 h	48 h
Call Center (por información de contingencia)	Logística y distribución del efectivo	Cash Management Liquidación y Contabilización Afiliación empresas	Administración de captaciones (empresas)
Administración de seguridad física	Comex Confirmación Rechazo de Negocio Emisión de Instrumentos	Logística y distribución de documentos	Consideraciones de Cámara Personas
Atención cajas	Call Center (prohibiciones y cancelaciones: personas y empresas)	Canje y compensación	Tarjetas de Crédito Autorización/Aprobación Monitoreo/Fraude Boletín
		Administración de liquidez y posición	Instrumentación Desembolso Segmentos Personas, Empresas, Consumo
		Administración de Portafolio Internacional/Institucional	Atención canales electrónicos (ATMs)
		Análisis y gestión de la información	Atención canales electrónicos (Banca Electrónica)

Tabla 2. RTO de Procesos Críticos. Elaborado por: Wilson Jácome

4.1.1 Clasificación de Amenazas

Para la planificación adecuada de las estrategias del plan de continuidad de negocios, es necesario hacer una clasificación de las diferentes tipos de amenazas que pueden afectar a dichos procesos. De esta manera se debe definir una estrategia diferente dependiendo del tipo de amenazas que haya afectado al proceso. Es necesario hacer esta agrupación pues los recursos requeridos para soportar un evento responden al tipo de amenaza que se haya cristalizado.

Amenazas	Descripción	Proceso afectados
Tecnológicas Infraestructura	• ***Caída de sistemas, redes, telecomunicaciones, bases de datos, servidores.*** • Falta de energía eléctrica, gas, agua, AA, telefonía, problemas de accesos físicos.	Afecta a todos los procesos cuya operación se soporta en un aplicativo. Afecta a todos los procesos críticos identificados.
Ambientales	• Tornados, huracanes, inundaciones, incendios.	Afecta a todos los procesos cuya operación se ejecute en el radio de acción de la catástrofe.
Humanas **(Sociales y Salud Pública)**	• Paros sorpresivos, cortes de ruta, amenazas de bomba, atentados. Epidemias, enfermedades, intoxicaciones.	Afecta a todos los procesos cuya operación es realizada por recursos humanos afectados, inclusive los tercerizados.
Servicios Tercerizados	• Incumplimiento de contratos totales y parciales, ausencia de personal tercerizado, falta de contingencia por parte de los terceros.	La operación de todos los procesos críticos relevados depende de al menos un proveedor externo, a saber: a)Proveedores de Infraestructura Tecnológica y operaciones b)Proveedores de tarjetas de crédito c)Proveedores de transporte d)Proveedores de

		Telecomunicaciones e)Proveedores de Cajeros automáticos f) Otros proveedores

Tabla 3. Clasificación de Amenazas. Elaborado por: Wilson Jácome

4.2. Correlación de los Procesos Críticos del Negocio con el Catálogo de Servicios de TI

Después de un análisis profundo de cada uno de los procesos críticos definidos por el negocio se ha encontrado la siguiente correlación con cada uno de los servicios que brinda el área de TI al Banco, según se describe en la siguiente tabla:

PROCESO CRITICO	DESCRIPCION	SERVICIO DE TI
Call Center	Servicio de Call Center hacia los clientes externos del Banco, definido exclusivamente para habilitar emergencias bancarias (bloqueo de cuentas, cheques, autorizaciones de transacciones) en caso de una crisis. Igualmente servirá como canal de comunicaciones hacia los clientes	• Enlaces Digitales • Infraestructura • Aplicaciones
Administración de Seguridad Física	Apertura y cierre de agencias; monitoreo de operación de agencias	• Enlaces Digitales • Infraestructura • Aplicaciones
Atención de Cajas	Depósitos y retiros en ventanillas solo para clientes del Banco	• Enlaces Digitales • Infraestructura • Aplicaciones
Logística y distribución del efectivo	Distribución de efectivo entre agencias, y conciliación en centro de acopio	• Enlaces Digitales • Infraestructura • Aplicaciones
Comex	Operaciones de comercio exterior del Banco con entidades internacionales	• Enlaces Digitales
Cash Management	Servicio de administración de efectivo para empresas (Unicamente bloqueos y autorizaciones de usuarios(	• Enlaces Digitales • Infraestructura • Aplicaciones
Logística y distribución	Distribución de documentos legales	• NA

de documentos	entre agencias del Banco	
Canje y Compensación	Canje y compensación de cheques con el banco central	• Enlaces Digitales • Infraestructura • Aplicaciones
Administración de liquidez	Operaciones de liquidez y reportes del Banco hacia entidades regulatorias	• Enlaces Digitales • Infraestructura • Aplicaciones
Administración de Portafolio	Operaciones de inversiones locales e internacionales del banco	• Enlaces Digitales • Infraestructura • Aplicaciones
Análisis y Gestión de la Información	Datawarehouse de Banco para toma de decisiones	• Enlaces Digitales • Infraestructura • Aplicaciones
Administración de captaciones (Empresas)	Generación de nuevos negocios con empresas locales e internacionales	• Enlaces Digitales
Consideraciones de Cámara	Pagos de cheques hacia otras entidades financieras	• Enlaces Digitales • Aplicaciones
Tarjetas de Crédito	Autorizaciones de consumo, bloqueo de tarjetas	• Enlaces Digitales • Infraestructura • Aplicaciones
Instrumentación de Desembolso	Desembolso de créditos para aquellos que han sido aprobados	• Enlaces Digitales • Infraestructura • Aplicaciones
Atención Canales Electrónicos (ATM)	Retiro de efectivo por ATMS, transferencias entre cuentas propias	• Enlaces Digitales • Infraestructura • Aplicaciones
Atención Canales Electrónicos (Banca Electrónica)	Servicio de Banca Electrónica para consulta de saldos	• Enlaces Digitales • Infraestructura • Aplicaciones

Tabla 4. Correlaciones de Procesos Críticos con Estrategías de TI. Elaborado por: Wilson Jácome

En base a la tabla anterior, en el siguiente punto se definen las estrategias de TI para poder brindar los servicios antes expuestos en caso de una crisis.

4.3. Definición de Estrategias de TI

En base al análisis de impacto de negocio de los diferentes procesos críticos del Banco, se desarrolló un conjunto de estrategias agrupadas por las amenazas descritas en el punto 4.1.1 del presente documento.

Cono resultado de este análisis se obtuvieron los siguientes resultados:

Proceso: Administración de Seguridad Física		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Implementar un servicio de monitoreo de contingencia en un Data Center Alterno
	Humanas **Sociales y Salud Pública)**	La ausencia del personal del banco en una agencia para su apertura no puede considerarse una contingencia que afecte la continuidad del negocio sin embargo se documentarán los procedimientos que se llevan a cabo en estas situaciones.
	Servicios Tercerizados	Companías de Seguridad.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Atención Cajas		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Implementar un nodo alterno de comunicaciones y contar con un Centro de Cómputo secundario donde se pueda levantar el aplicativo de atención a cajas para dar el servicio limitado a depósitos y retiros. Adicionalmente documentar los procedimientos que aplica el área de cajas cuando falla el sistema, este procedimiento de contingencia les permite brindar el servicio en un período de hasta 4 horas.
	Humanas **Sociales y Salud Pública)**	La ausencia del personal del banco en una agencia no puede considerarse una contingencia que afecte la continuidad del negocio sin embargo se documentarán los procedimientos que se llevan a cabo en estas situaciones.
	Servicios Tercerizados	No dependen de proveedores de servicios adicionales a los de infraestructura y comunicaciones para la operatividad de los aplicativos críticos y telecomunicaciones respectivamente.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Logística y Distribución del Efectivo		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	En el caso de no contar con el sistema de logística de efectivo las agencias deberán estimar los requerimientos de efectivo a ser solicitados. Sin embargo considerando que el proceso depende de los aplicativos de atención en cajas y monitoreo de efectivo, la estrategia óptima es la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	El proceso de monitoreo del efectivo es efectuado por personal del área ubicado en la ciudad de Quito, se considera factible con la adecuada capacitación que este proceso pueda ser efectuado por personal ubicado en Guayaquil.
	Servicios Tercerizados	El proceso es realizado por personal de los proveedores de seguridad, se incluirá en el contrato los acuerdos de contingencia y adicionalmente se definirán procedimientos en donde con la ayuda de otras empresas calificadas pueda brindarse el servicio en el caso de que una de las empresas proveedoras no puede brindarlo.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Comex (Confirmación Rechazo de Negocio Emisión de Instrumentos)		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente de los aplicativos de COMEX por lo tanto la estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	El proceso de confirmación rechazo de negocio emisión de Instrumentos, cuenta con 9 especialistas en total distribuidos en las ciudades de Quito, Guayaquil, Cuenca y Manta; en caso de presentarse problemas en alguna de las localidades los clientes pueden ser atendidos por el recurso humano restante sin ningún inconveniente. Documentar el procedimiento a aplicarse en caso de contingencia considerando los recursos existentes y la logística del ruteo de llamadas.
	Servicios Tercerizados	Depende del proveedor que ejecuta el proceso de recepción y envío de mensajes swift de comercio exterior. El proveedor posee un plan de contingencias que cubre el escenario humano excepto catástrofes mayores. Para el caso de catástrofes mayores: Desarrollar procedimientos con la colaboración de otros bancos.

		Enviar el servidor espejo de swift a la ciudad de Guayaquil y establecer procedimientos de contingencia con el proveedor.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Call Center (prohibiciones y cancelaciones: personas y empresas)		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente de los aplicativos usados para consultas de información de clientes. La estrategia debe implementar un call center alterno.
	Humanas **Sociales y Salud Pública)**	El personal pertenece al proveedor de Call Center, actualmente esta compañía se encuentra elaborando un plan de contingencias que contempla este escenario.
	Servicios Tercerizados	1. Rutear las llamadas del call center a cualquiera de los call center de campañas que se ubican físicamente en lugares distintos, para esto se deberá capacitar al personal o llevar gente del call center actual que conozca el proceso. Además se deberían habilitar los sistemas informáticos necesarios para el soporte y los accesos correspondientes. 2. Rutear las llamadas al call center del banco que está constituido por agentes de servicio que tienen acceso a los sistemas del banco y el conocimiento apropiado para brindar soporte. 3. Implementar un call center en la ciudad de Guayaquil.
	Ambientales	Instalar un call center para atender emergencias bancarias y servicios de Tarjeta de Crédito en la ciudad de Guayaquil

Proceso: Cash Management Liquidación y Contabilización		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Al depender principalmente de los aplicativos de manejo de empresas. La estrategia depende de la implementación del data center alterno. Para el caso de que el cliente no pueda generar las transacciones en el sistema, el área de cash management cuenta con un plan de contingencia descrito y publicado en la intranet, para que se procesen las operaciones de forma manual a través de operaciones y balcones. Operaciones recibe la información en un medio magnético.
	Humanas	En caso de presentarse inconvenientes con el personal de las agencias, El cliente puede enviar las transacciones en un dispositivo de

	Sociales y Salud Pública)	almacenamiento o vía correo electrónico (manera encriptada) para que los pagos sean procesados por el personal de operaciones. Es necesario que está información tenga adjunta una carta de autorización del cliente para poder procesar las transacciones.
	Servicios Tercerizados	No se depende de proveedores de servicios adicionales a los de operaciones y comunicaciones para la operatividad de los aplicativos críticos y telecomunicaciones.
	Ambientales	La estrategia depende de la implementación del data center alterno.

Proceso: Cash Management Afiliación empresas		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente de los aplicativos de manejo de empresas. La estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	El proceso de Afiliación Empresas necesita un número de 3 personas de operaciones ubicadas en Quito, Guayaquil y Cuenca, en caso de presentarse problemas con el personal se irían soportando en las personas disponibles, por ejemplo si la persona de Quito presenta problemas se contaría con el soporte de Guayaquil y Cuenca.
	Servicios Tercerizados	No dependen de proveedores de servicios adicionales a los de operaciones y comunicaciones para la operatividad de los aplicativos críticos y telecomunicaciones.
	Ambientales	La estrategia depende de la implementación del data center alterno.

Proceso: Logística y Distribución de Documentos		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	El proceso manual de entrega y recepción de documentación solventaría cualquier crisis sobre este proceso.
	Humanas **Sociales y Salud Pública)**	Este proceso requiere de al menos 4 personas, encargadas de llevar el control manual de los documentos entregados.
	Servicios Tercerizados	Proveedor de transporte de documentación
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Canje y compensación		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Implementación de un centro de Canje y Compensación alterno, en la ciudad de Guayaquil.
	Humanas **Sociales y Salud Pública)**	
	Servicios Tercerizados	
	Ambientales	

Proceso: Administración de liquidez y posición		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente de los aplicativos de liquidez, por lo tanto la estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	Si bien el proceso requiere de tres personas, en caso de contingencia para mantener la continuidad del proceso sería necesaria solamente una; es necesario tomar en cuenta factores como son el expertise y claves necesarias para el ingresos a los aplicativos involucrados por lo que es complejo que otra persona pueda realizar esta operación. Sin embargo es necesario capacitar a una persona que se encuentre en una zona de riesgo distinta para que lleve a cabo el proceso en caso de contingencia y actualizar el manual de Administración de Liquidez y Posición.
	Servicios Tercerizados	Depende del proveedor de operaciones para el proceso de recepción y envío de mensajes swift. El proveedor se encuentra elaborado un plan de contingencias que cubre el escenario humano excepto catástrofes mayores. Para el caso de catástrofes mayores: Desarrollar procedimientos con la colaboración de otros bancos. Enviar el servidor espejo de swift a la ciudad de Guayaquil y establecer procedimientos de contingencia con el proveedor.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Administración de Portafolio Institucional		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente de los aplicativos de banca de portafolio, por lo tanto la estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	El proceso requiere de dos personas, en caso de contingencia se podría mantener la continuidad con una. Cada persona puede reemplazarse mutuamente. Las dos personas se encuentran en la misma zona de riesgo por lo tanto es necesario capacitar a un persona que se encuentre en una zona de riesgo distinta para que lleve a cabo el proceso en caso de contingencia es necesario contar con documentación soporte del Instructivo para la administración de las RML y con un token de un usuario alterno para el ingreso en las páginas del BCE.
	Servicios Tercerizados	Depende del proveedor de operaciones para el proceso de recepción y envío de mensajes swift. El proveedor se encuentra elaborando un plan de contingencias que cubre el escenario humano excepto catástrofes mayores. Para el caso de catástrofes mayores: Desarrollar procedimientos con la colaboración de otros bancos. Enviar el servidor espejo de swift a la ciudad de Guayaquil y establecer procedimientos de contingencia con el proveedor.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Análisis y gestión de la información		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente del datawarehouse, por lo tanto la estrategia depende de la implementación del data center alterno que incluya los aplicativos de reportes desarrollados en SQL.
	Humanas **Sociales y Salud Pública)**	En contingencia debe existir una persona en un área de riesgo distinta que, soportada en los manuales y capacitación que pueda llevar a cabo el proceso.
	Servicios Tercerizados	No dependen de proveedores de servicios adicionales al del proveedor de operaciones y comunicaciones para la operatividad de los aplicativos críticos y telecomunicaciones.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Administración de Portafolio Internacional		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	El principal aplicativo informático que se requiere para la administración de este proceso es Bloomberg (página web informática en donde se exponen las situaciones del mercado, notificaciones y transacciones). Por lo tanto dado que este aplicativo no depende del Banco, puede ser accedido en cualquier lugar que tenga internet; concluyendo que la no accesibilidad a la matriz no presenta problemas siendo lo necesariamente requerido para la continuidad del proceso es el acceso a internet, línea telefónica y el correo electrónico.
	Humanas **Sociales y Salud Pública)**	El proceso de Administración de Portafolio Internacional es realizado principalmente por una persona. En el caso de contingencia debe existir una persona en un área de riesgo distinta que soportada en los manuales y capacitación que pueda llevar a cabo el proceso.
	Servicios Tercerizados	Adicionalmente a la operatividad de los aplicativos y telecomunicaciones también dependen del proveedor de operaciones para la liquidación de negociaciones, formas de pago - SWIFT, creación de instrumentos en caso de tratarse de papeles nuevos, valoración del portafolio, conciliaciones de los estados de cuenta. El proveedor se encuentra elaborando un plan de contingencias que cubre el escenario humano excepto catástrofes mayores. Para el caso de catástrofes mayores: Desarrollar procedimientos con la colaboración de otros bancos. Enviar el servidor espejo de swift a la ciudad de Guayaquil y establecer procedimientos de contingencia con el proveedor. Para el resto de procesos se desarrollarán procedimientos por parte del Banco.
	Ambientales	Se deberá activar el comité de Crisis.

Proceso: Instrumentación Desembolso Segmentos Personas, Empresas, Consumo		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente de los aplicativos Crédito, por lo tanto la estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	El proveedor de operaciones se encuentra elaborando un plan de contingencias que cubre el escenario humano que no cubre catástrofes, mayores en cuyo caso el proceso deberá ser asumido por personal del

	Servicios Tercerizados	banco ubicado en un sitio geográfico fuera del área de riesgo.
	Ambientales	La estrategia depende de la implementación del nuevo data center.

Proceso: Administración de captaciones (empresas)		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente del aplicativo de captaciones, por lo tanto la estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	Si bien el proceso requiere de tres personas, en caso de contingencia se podría mantener la continuidad con una sola persona. En el caso que esta persona falte, otra puede realizar las operaciones; sin embargo las tareas de autorización en la mesa de dinero caerían en Administración de portafolio internacional ya que cuenta con las opciones apropiadas dentro del aplicativo. Para casos de una contingencia mayor debe existir una persona capacitada en un área de riesgo distinta.
	Servicios Tercerizados	No dependen de proveedores de servicios adicionales al de los proveedores de operaciones y comunicaciones para la operatividad de los aplicativos críticos y telecomunicaciones.
	Ambientales	La estrategia depende de la implementación del data center alterno.

Proceso: Manejo de Tarjetas de Crédito		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Tercerización del servicio de tarjetas de crédito con el proveedor de tarjetas de crédito.
	Humanas **Sociales y Salud Pública)**	
	Servicios Tercerizados	
	Ambientales	

Proceso: Atención canales electrónicos (ATMs)		
AT EG IA	**Tecnológicas**	Depende principalmente del aplicativos de ATM. La estrategia depende

	Infraestructura	de un proyecto de ATM de alta disponibilidad
	Humanas **Sociales y Salud Pública)**	Para la recarga de dinero depende de los procesos de caja y logística de efectivo.
	Servicios Tercerizados	Identificar con el proveedor de servicios de ATM y de comunicaciones la existencia de planes de contingencia
	Ambientales	La estrategia depende de la implementación del data center alterno.

Proceso: Consideraciones de Cámara Empresa/Personas		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Si bien para el proceso de Consideraciones de Cámara - Empresas se requiere principalmente del aplicativo de cámara; en el caso de que el aplicativo o el nodo de comunicación falle, el proceso de consideración de cámara se lo puede realizar mediante un listado de los cheques emitidos sin fondos enviado mediante cualquier medio de comunicación.
	Humanas **Sociales y Salud Pública)**	El proceso de Consideraciones de Cámara – Empresas lleva a cabo sus actividades en las oficinas principales; en el caso que las instalaciones tengan algún tipo de inconveniente de accesibilidad tal como inundaciones, incendios, entre otros. El personal puede acceder al aplicativo desde cualquier agencia de banco, siempre y cuando se habilite una máquina con este fin. En el caso de una contingencia mayor debe existir una persona en un área de riesgo que pueda llevar a cabo el proceso.
	Servicios Tercerizados	No dependen de proveedores de servicios adicionales a los de operaciones y comunicaciones para la operatividad de los aplicativos críticos y telecomunicaciones.
	Ambientales	Dependen de la implementación del data center alterno

Proceso: Atención canales electrónicos (Banca Electrónica)		
ESTRATEGIAS	**Tecnológicas** **Infraestructura**	Depende principalmente del aplicativo de banca electrónica, por lo tanto la estrategia depende de la implementación del data center alterno.
	Humanas **Sociales y Salud Pública)**	No depende de personas
	Servicios Tercerizados	No dependen de proveedores de servicios adicionales a los de operaciones y comunicaciones para la operatividad de los aplicativos

		críticos y telecomunicaciones.
	Ambientales	Dependen de la implementación del data center alterno

4.4. Implementación de Estrategias de TI

Una vez definidas y aprobadas las estrategias a aplicar en cada uno de los procesos críticos, como departamento de Tecnología es importante centrarse en aquellas amenazas que afectan a los servicios tecnológicos, ya sean causadas por daños ambientales, catástrofes o paralizaciones.

Agrupando las diferentes estrategias de TI definidas dentro del Plan de Continuidad de Negocios, es posible identificar los siguientes grupos de planes que deben ser implementados (Ver Figura 4.1):

- Implementación de un servicio de Call Center Alterno
- Implementación de un Data Center Alterno con un Nodo Alterno de Comunicaciones
- Implementación de un centro de Canje y Compensación Alterno
- Implementación de un servicio de ATM de alta disponibilidad

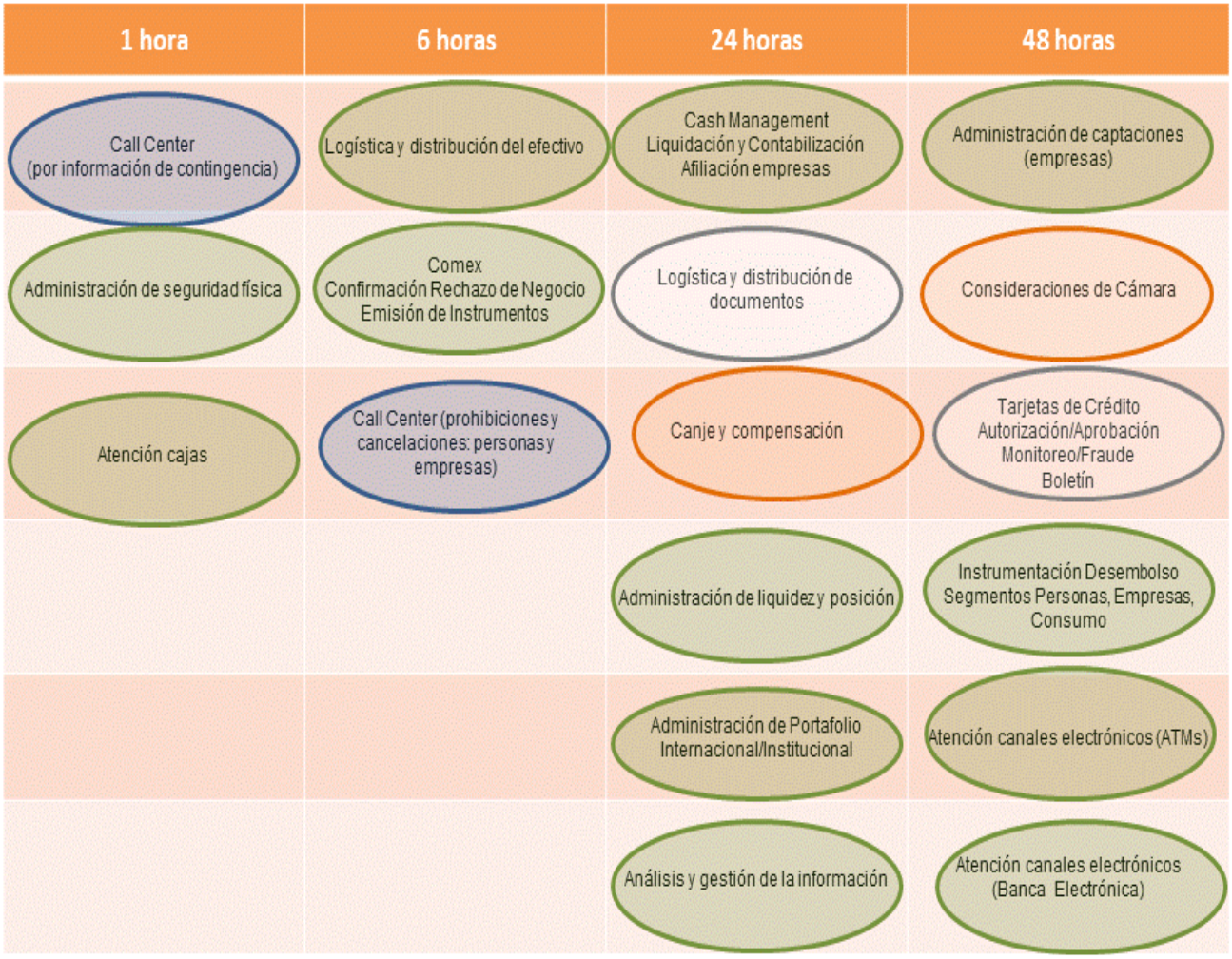

Ilustración 13. Estrategias de TI para el BCP. Elaborado por: Wilson Jácome

4.4.1 Call Center Alterno

Objetivo General:

Implementar un servicio de Call Center Alterno para Banco Nacional Financiero ubicado en la ciudad de Guayaquil.

Objetivos Específicos:

- ✓ Cumplir con la estrategia de Continuidad de Negocios definida para el Proceso de Call Center (Atención Canales Electrónicos)
- ✓ Contratar un servicio de call center alterno que permita entregar los procesos críticos definidos en caso de contingencia referentes a la atención en canales electrónicos
- ✓ Mantener un canal de comunicaciones alterno con los clientes del Banco Nacional Financiero

Descripción General De La Solución Requerida:

La implementación de un servicio alterno de Call Center permitirá al banco proveer de los siguientes servicios (Emergencias Bancarias) en una ubicación física diferente a la del Call Center Principal :

- ✓ Bloqueos temporales y cancelaciones definitivas de tarjetas de débito
- ✓ Prohibición de Cheques
- ✓ Bloqueos Libretas de ahorro
- ✓ Cancelación de TC por medio de Call Center
- ✓ Cancelación de tarjeta clave electrónica
- ✓ Eliminación de usuarios Cash
- ✓ Medio de Comunicación a Clientes en caso de contingencia o manejo de crisis

La solución debe incluir, además de brindar el servicio de los procesos antes mencionados, las siguientes funcionalidades:

- ✓ Software, hardware y aplicativos que permitan brindar los servicios antes mencionados
- ✓ Comunicación entre el proveedor de Call Center Alterno hacia los aplicativos del Banco usados para dicho servicio

El servicio debe incluir todo el software y hardware necesario, así como el recurso humano para poder brindar el servicio de call center antes definido; es decir, desde un IVR hasta las estaciones de los telefonistas.

Diagrama de la solución:

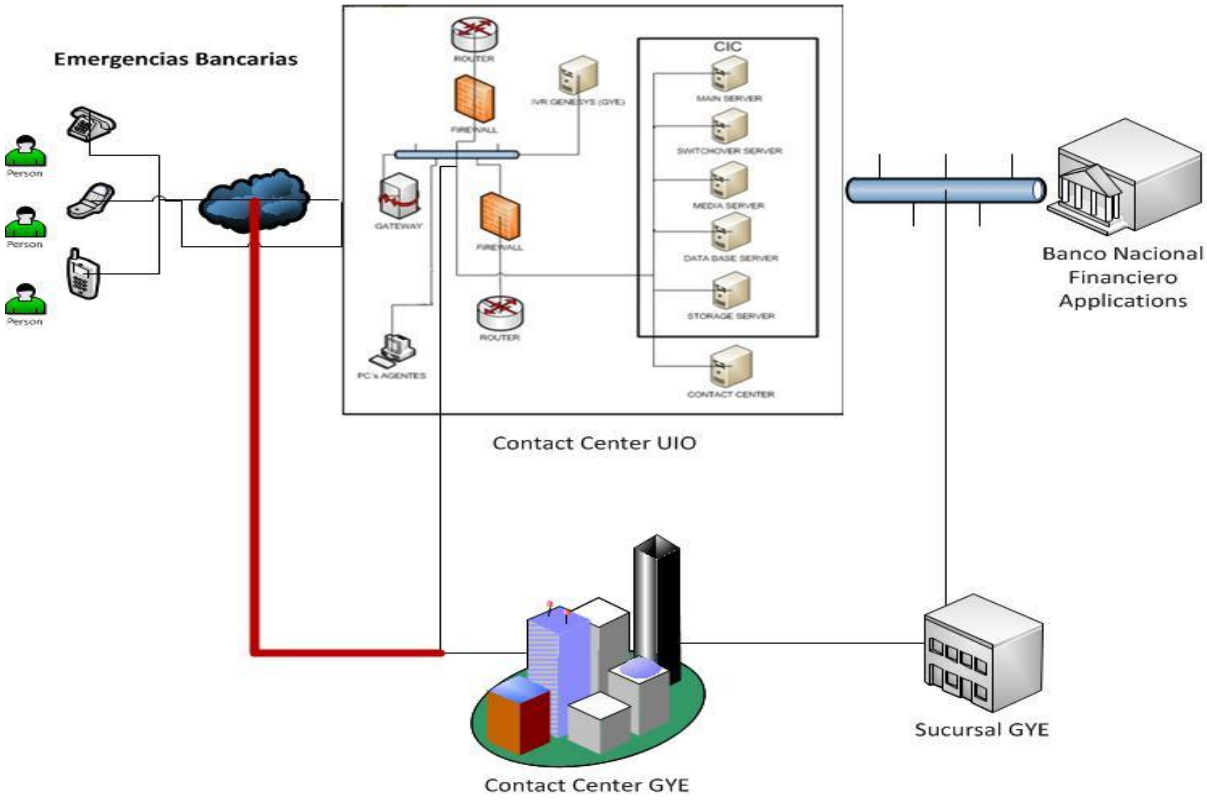

Ilustración 14. Servicio de Call Center Alterno (GYE). Elaborado por: Wilson Jácome

4.4.2 Data Center Alterno / Nodo Alterno de Comunicaciones

Objetivo General:

Implementar un Data Center Alterno por medio del servicio de aprovisionamiento de infraestructura para entregar los servicios de aplicaciones identificadas en los procesos críticos a los clientes en caso de una crisis.

Objetivos Específicos:

- ✓ Cumplir con la estrategia de Continuidad de Negocios definida para todos los procesos críticos que requieren servicios de aplicaciones de software
- ✓ Implementar un Nodo Alterno de Comunicaciones que permita habilitar las comunicaciones entre las diferentes agencias y el Data Center Alterno en caso de una crisis
- ✓ Aprovisionar todo el hardware y software requerido por los procesos críticos para mantener el servicio en caso de una contingencia

Descripción General De La Solución Requerida:

La implementación de un Data Center Alterno permitirá al banco proveer la mayoría de los procesos críticos definidos en el análisis del plan de continuidad de negocios bajo las siguientes premisas:

- ✓ Mitigar las amenazas y los riesgos normativos y de mercado minimizando el costo
- ✓ Evitar inversiones en construcción de bienes no asociados directamente a la misión
- ✓ Aprovechar las oportunidades de nuevas tecnologías, i.e., virtualización y cloud computing, teniendo en cuenta el estado de madurez de la tecnología

El aprovisionamiento del Data Center Alterno debe ser ejecutado por intermedio de:

- Aprovisionamiento de infraestructura similar a la del Site Principal
- Aprovisionamiento de información proveniente del Site Principal mediante configuraciones de réplica de las diferentes plataformas del Banco
- Aprovisionamiento del software base y aplicaciones en el hardware instalado en el Site Alterno mediante réplica de sistemas operativos, instalaciones manuales y restauración de información mediante cintas o archivos.

Para activar los puntos antes descritos la solución incluye la implementación de un NAC (Nodo Alterno de Comunicaciones) que permita ejecutar las siguientes actividades:

- Habilitar la réplica de información entre el Site Principal y el Site Alterno
- Habilitar las comunicaciones entre las agencias locales hacia el Data Center Alterno cuando sea activado en caso de una crisis

Diagrama de la solución:

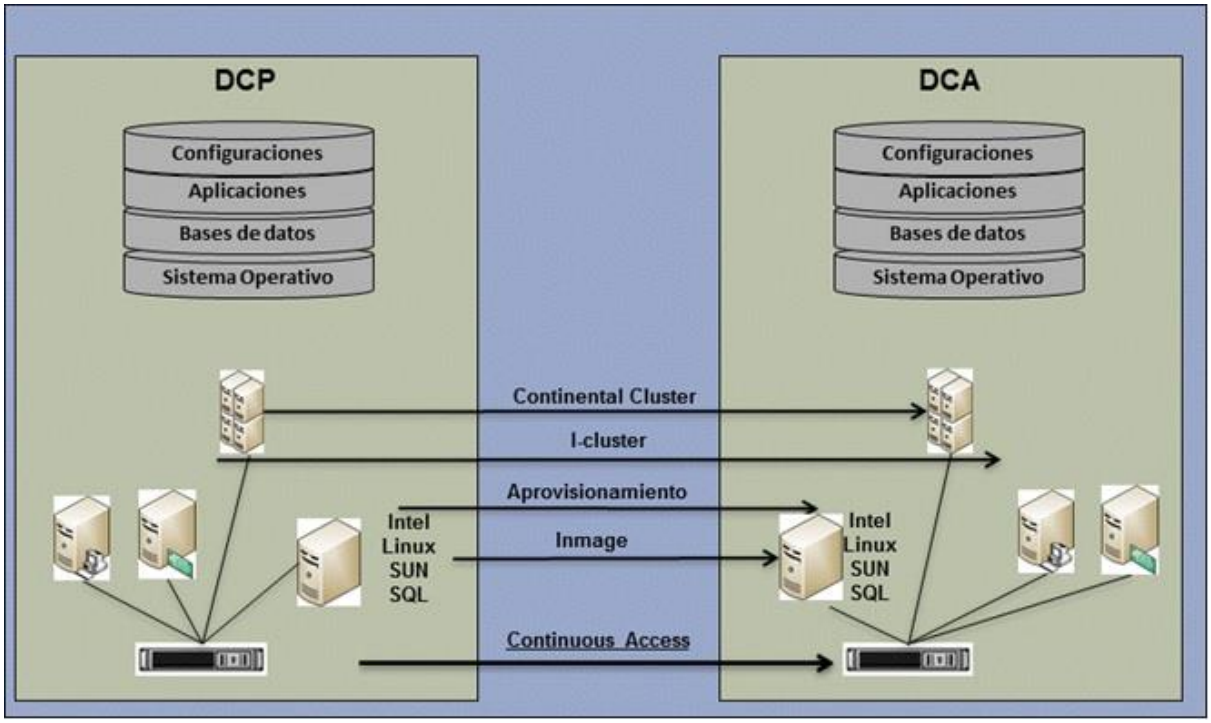

Ilustración 15. Proceso de réplica de información. Elaborado por: Wilson Jácome

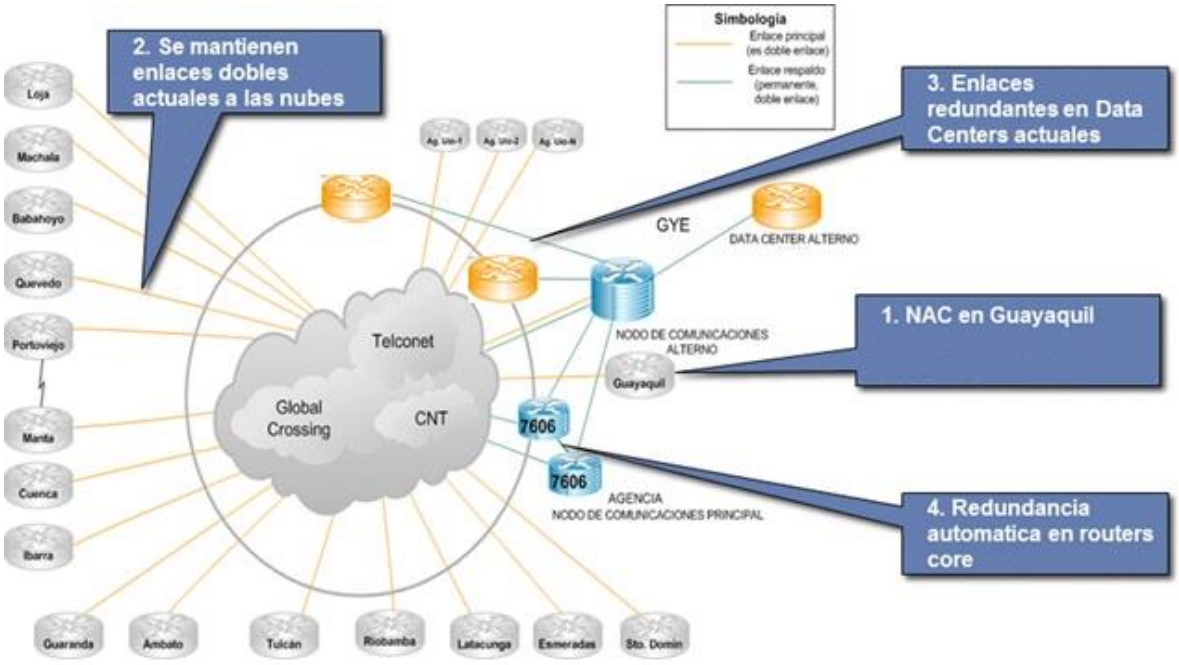

Ilustración 16. Servicio de Data Center Alterno. Elaborado por: Wilson Jácome

4.4.3 Centro de Canje y Compensación Alterno

Objetivo General:

Implementar un servicio Alterno de Canje y Compensación para Banco Nacional Financiero.

Objetivos Específicos:

- ✓ Cumplir con la estrategia de Continuidad de Negocios definida para el Proceso de Canje y Compensación.
- ✓ Contratar un servicio de canje y compensación alterno que permita entregar los procesos críticos definidos en caso de contingencia referentes al mismo.

Descripción General De La Solución Requerida:

La implementación de un centro alterno de Canje y Compensación permitirá al banco proveer de los siguientes procesos en caso de contingencia del mismo desde el ingreso de un cheque (operaciones) hasta su pago o protesto:

- ✓ Recepción de Lotes, captura y transmisión de imágenes por corte de lote, depuración y organización de la información, completación, prueba cero o de cuadratura.
- ✓ Entrega parcial de planillas, elaboración de datos de cheques a entregar a otros bancos y envío de remesas.
- ✓ Asistencia a cámara preliminar.
- ✓ Proceso y transmisión de cheques de la cámara preliminar entrante, revisión firma y forma.
- ✓ Reporte de cheques devueltos.
- ✓ Impresión de notas de débito.
- ✓ Envío reparto.

- ✓ Consideraciones de cámara definitiva.
- ✓ Generación de Reportes.

El servicio debe incluir todo el software, hardware y personal necesario para poder brindar el servicio de canje y compensación.

Diagrama de la solución:

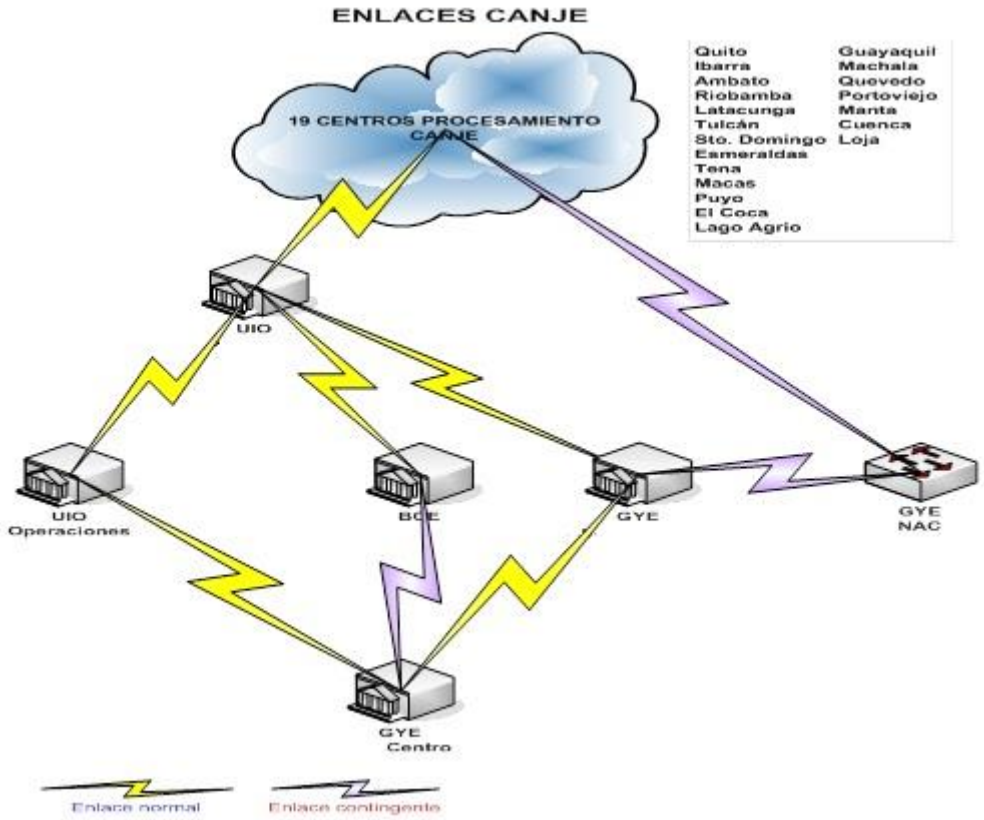

Ilustración 17. Servicio de Centro Alterno de Canje y Compensación. Elaborado por: Wilson Jácome

4.4.4 Servicio de ATM en Alta Disponibilidad

Objetivo General:

Implementar un servicio alterno de prestación de servicios a través de la red de cajeros automáticos

Objetivos Específicos:

- ✓ Cumplir con la estrategia de Continuidad de Negocios definida para el Proceso de Atención Canales Electrónicos ATM
- ✓ Contratar un servicio de atención de cajeros automáticos alterno que permita entregar los procesos críticos definidos en caso de contingencia referentes al mismo

Descripción General De La Solución Requerida:

La implementación de un servicio alterno de atención por medio de cajeros automáticos permitirá al banco proveer de los siguientes procesos en caso de contingencia del mismo:

- ✓ Ingreso de los datos de autentificación y autorización, para ejecutar transacciones
- ✓ Extracción de dinero

El alcance de este proyecto implica el diseño y planificación por parte del proveedor del servicio de contingencia para operar en caso de una crisis que permita brindar el servicio de ATM, debe llegar inclusive hasta la implementación de los sistemas y procedimientos necesarios por el lado del proveedor, incluyendo los cambios necesarios que deben ser ejecutados en el autorizador del Banco.

Diagrama de la solución:

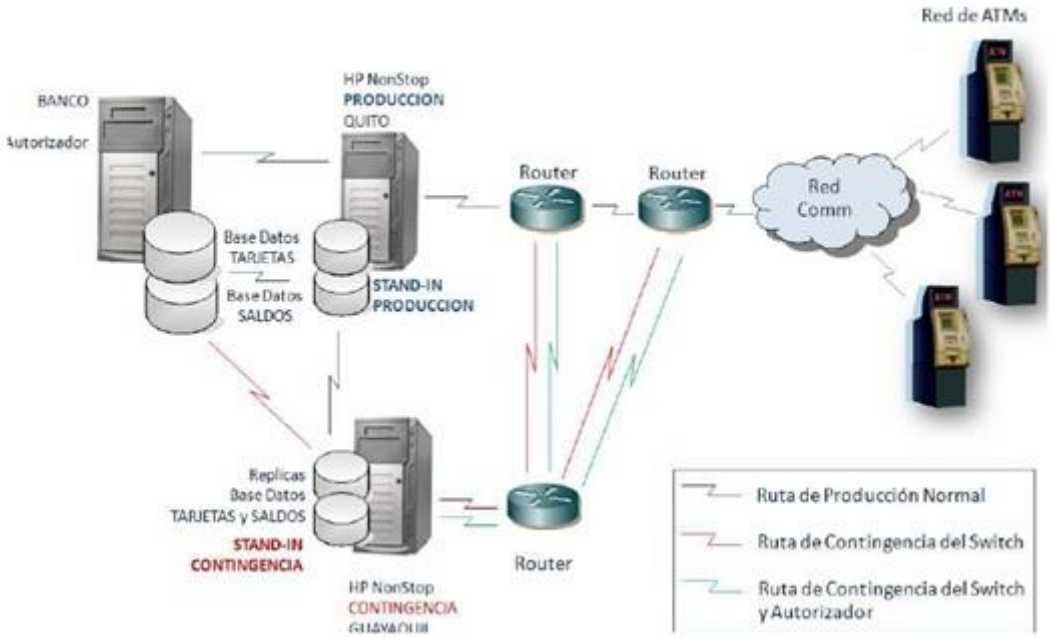

Ilustración 18. Servicio de ATM en alta disponibilidad. Elaborado por: Wilson Jácome

4.5. Difusión de la Administración de Continuidad de Negocios de TI en la Organización y Mejora Continua

4.5.1 Continuidad de Negocios de TI en la Organización

El departamento de TI tiene muchas responsabilidades dentro de una organización, sin embargo, el objetivo principal siempre será ofrecer los servicios tecnológicos de la mejor manera posible. Sin embargo, el servicio de continuidad de negocios tecnológicos no es visionado dentro de una empresa mientras no haya existido una amenaza que afecte tanto a clientes internos como externos. Es por este motivo que la gerencia general y el directorio debe entender la necesidad de asegurar los servicios informáticos en caso de una crisis.

La criticidad de la información dentro de la organización y la complejidad de los sistemas de información hacen que las organizaciones sean más sensibles ante las amenazas de la

integridad de la información. Los incidentes de pérdida de información que con cierta frecuencia se presentan y son dados a conocer por los medios de comunicación, provocan alarma en las Organizaciones ya que afectan a la totalidad de las actividades de las mismas. Sin embargo, incidentes menos relevantes como el fallo de una línea de comunicación puede tener un efecto devastador en los procesos de la organización.

En la actualidad la regulación de la Superintendencia de Bancos y Compañías no hace una referencia específica a la continuidad de negocio de TI. En general, los administradores suelen poner énfasis en la integridad y disponibilidad de la información más que en la disponibilidad de los sistemas como base a la continuidad del negocio de la empresa.

Este es uno de los principales motivos por los cuales la mayoría de los empleados dentro de la organización no conocen el concepto de "continuidad de negocios" y menos aún que la resilencia frente a desastres depende en gran parte de como respondan los servicios tecnológicos de cara a estos imprevistos. Para ello es primordial que el Plan de Continuidad de Negocios de TI sea socializado dentro de la organización de manera adecuada enfocando los aspectos más importantes del mismo.

Al menos dos copias completas del Plan de Continuidad de TI deben ser mantenidas fuera del sitio principal de operaciones del Banco

Directriz de distribución del plan: El Plan de Continuidad de TI debe ser distribuido a todo el personal autorizado, ya que sólo el personal activo puede tener acceso al plan. Si un individuo deja de laborar para el negocio o una de sus unidades específicas, es su responsabilidad retornar las copias y todos los duplicados o partes duplicadas de este plan a su superior respectivo. A nadie fuera de la organización le será permitido a leer, revisar, copiar o auditar el Plan sin la autorización formal y escrita por parte del Directorio del Banco.

Distribución de los documentos: Debido a la confidencialidad de este documento únicamente el Coordinador de la Continuidad de Negocios de TI mantendrá una copia completa del mismo. Subconjuntos del Plan serán distribuidos tomando como base la premisa "need-to-know". Adicionalmente, es necesario desarrollar el mecanismo de control para asegurar que todas las copias de las hojas que han sido modificadas sean colocadas fuera de circulación. Para controlar la actualización de los documentos se ejecutarán las siguientes acciones:

- Enviar secciones completas para reemplazar aquellas con cambios, en lugar de enviar sólo las hojas que han cambiado.
- Asegurar que los responsables de cada unidad provean algún tipo de recibo para verificar que recibieron las nuevas versiones del plan. El retornar las hojas reemplazadas podría ser considerado como un recibo.
- Mantener el control de los planes de recuperación para propósitos de seguridad.

El desarrollo e implementación de un Plan de Continuidad del Negocio de TI debe ser visto como uno de los temas más importantes dentro de la organización y dentro de la Vicepresidencia de Tecnología; pues requiere del esfuerzo y compromiso de muchas personas, el uso de muchos recursos y una cantidad importante de tiempo.

4.5.2 Proceso de Mejora Continua

Una de las actividades principales en la gestión de la continuidad del negocio dentro del departamento de tecnología es la medición del rendimiento de dicho programa. Una buena gestión implica el análisis de los procesos del negocio apalancados en servicios tecnológicos en curso para asegurarse de que se están cumpliendo los objetivos de la empresa. En la

mayoría de las actividades de gestión de la continuidad del negocio de TI se realiza (o se debería realizar) una revisión de la gestión y un proceso de evaluación; con el fin de encontrar fallas en dichos procesos y estrategias, para posteriormente corregirlas.

La administración de continuidad del Negocio dentro de TI es un proceso dinámico, el cual debe ser actualizado periódicamente para que se reflejen en él los cambios operativos relacionados con el manejo y control de la información, así como los cambios tecnológicos y de negocio que surgen a través del tiempo y ocasionan variaciones dentro de las prioridades establecidas en las estrategias de mitigación.

Dentro de dicho proceso, y como marco de trabajo dentro del presente proyecto se han definido las siguientes acciones a ejecutar, las cuales no obedecen a un orden específico:

Gestión de la Continuidad de TI:

- Revisión del proceso macro de gestión de continuidad de negocios
- Revisión de los procesos de gestión de continuidad de negocios de TI, incluyendo la metodología aplicada
- Análisis del equipo de trabajo cualificado que gestiona la continuidad de negocios de TI
- Políticas y procedimientos de gestión de continuidad de negocios de TI, aprobados por el directorio y dados a conocer a la organización.

Gestión de los Riesgos de TI:

- Revisión del proceso de gestión de riesgos tecnológicos
- Análisis periódico de los riesgos tecnológicos
- Revisión de los procesos de tratamiento de riesgos tecnológicos identificados

Análisis de Impacto de Negocios (BIAS)

- Identificación de las principales relaciones y dependencias con las organizaciones internas y externas (proveedores de tecnología)
- Revisión de las consecuencias financieras y no financieras de un incidente disruptivo de la tecnología
- Revisión de los objetivos de tiempos de recuperación (RTO) y de punto de recuperación (RPO) de las funciones críticas
- Revisión de nuevos procesos dentro de la organización que sean considerados como críticos y que tengan componentes tecnológicos para su ejecución.

Revisión de las Estrategias de Continuidad de TI:

- Revisión de las estrategias tecnológicas definidas para los procesos críticos
- Proceso para determinar la eficacia de las estrategias (pruebas periódicas de las estrategias definidas)
- Análisis de nuevas tecnologías que puedan suplantar a las estrategias actuales ya sean generando una reducción del costo, reducción de los RPO u optimización de recursos

Práctica de las Estrategias de la Continuidad de TI:

- Calendario de de ejercicios conocido y popularizado en toda la organización
- Evaluación de los ejercicios y recomendaciones
- Lista de contactos de proveedores tecnológicos críticos y con los organismos de control y emergencia

La Administración de Continuidad de Negocios dentro de TI se define como un proceso de gerenciamiento continuo, para asegurarse. que regularmente se revisen los escenarios de

posibles emergencias ,accidentes , desastres y amenazas. Lo que también involucra; evaluación de los impactos de dichos eventos; elaboración de estrategias de recuperación y planes de mantenimiento, documentación y entrenamiento al personal; la realización de pruebas o simulacros. Componente importante de esta administración es la documentación, las actividades y recomendaciones para usar en los momentos de emergencia de continuidad de negocios, incidentes y/o crisis. Típicamente esta mejora continua cubre todo el personal clave, recursos , servicios y acciones que se requieren en el proceso de continuidad del negocio.

CAPÍTULO V: ADMINISTRACIÓN DE CRISIS EN TI

La crisis se la puede definir como una emergencia de cualquier evento no planificado que puede causar desde muerte de los empleados, clientes o público en general hasta cortar la operatividad del negocio, hacer que el mismo cierre, causar daños materiales o hacer perder la imagen corporativa.

Dentro del departamento de tecnología, es primordial contar con un plan formal para identificar y definir acciones y opciones que deben ser tomadas cuando la organización esté en crisis. Dicho plan incluye la creación de un comité de crisis dentro de la organización, el cual sea capaz de administrar estos eventos inesperados y activar los planes definidos dentro de la continuidad de negocio.

5.1. Comité de Crisis

Dentro de Banco Nacional Financiero, es necesario definir cada uno de los siguientes roles y responsabilidades para la administración de la crisis dentro del departamento de tecnología:

Banco Nacional Financiero:

- Deberá designar un Oficial de Continuidad de Negocio de Tecnología, el cual debe formar parte de la Vicepresidencia de Tecnología del Banco cuyo rol principal sea el de integrar todas las áreas del negocio con las plataformas tecnológicas que soportan dichos servicios con el fin de implementar un proceso de Administración de Continuidad de Negocios de TI para crear una respuesta consistente y disponer de una planificación ordenada que permita al Banco minimizar el impacto y consecuencias

de un suceso inesperado, a la vez que le asista durante las etapas de recuperación de su normal operación.

- El Directorio del Banco Nacional Financiero, establecerá un Comité de Crisis con su respectivo delegado, los cuales administren y ejecuten los planes de contingencia y los planes de continuidad de negocios a fin de cumplir con las responsabilidades establecidas en la ResoluciónNo. JB-2005-834 Sección V Artículo 1 Numeral 1.5. Este Comité estará formado por los Líderes de Auditoría, Riesgos y Recuperación, Administrativo y Recursos Humanos, Personas, Empresas, Tesorería, Legal, Control Financiero, Marketing y Tecnología; a nivel de delegado del comité el Responsable de Riesgo Operativo y por parte de los Proveedores de Servicios de Seguridad Informática, Tecnología y Operaciones. Este Comité deberá ser el responsable de aprobar y analizar los procesos definidos en la Administración de Continuidad de Negocios de TI así como la toma de decisiones estratégicas que permitan ejecutar en el Banco Nacional Financiero el proceso de Administración de la Continuidad de Negocios de TI.

La administración de Continuidad de Negocios de TI deberá incluir controles destinados a:

- Identificar y reducir riesgos que afecten a los procesos críticos de la organización que tengan un componente tecnológico para su supervivencia.
- Atenuar las consecuencias de los incidentes perjudiciales, y
- Asegurar la reanudación oportuna de los servicios tecnológicos que apalancan los Procesos Críticos

Oficial de Continuidad de Negocios de TI:

- Implementar un proceso controlado para el desarrollo y mantenimiento de la Administración de la Continuidad de Negocios de TI del Banco. Este proceso deberá al menos contemplar lo siguiente:
    - Análisis de Riesgo tecnológicos, identificación de los riesgos en términos de probabilidad de ocurrencia e impacto de los procesos críticos.
    - Análisis de Impacto de Negocios (BIA- Business Impact Analisys)
    - Estrategias de Continuidad de TI
    - Elaboración y documentación del BCP para sus componentes tecnológicos de conformidad con la estrategia de continuidad acordada.
    - Pruebas Periódicas
    - Política de Comunicación

5.1.1. Estructura

Es importante que el equipo de personas este compuesto por pocos miembros, dado que de esta manera se asegurará una gestión ágil de los problemas presentados. Sobre dicho comité recaerá el trabajo y la responsabilidad de prevenir y solventar cualquier situación crítica.

El Comité de Crisis estará conformado por personas que pertenezcan a la dirección de Banco Nacional Financiero con capacidad técnica y experiencia profesional para formar parte del comité que vaya a gestionar la crisis. Los miembros del comité podrán designar un representante ó miembro alterno que pueda representar a su principal dentro del comité en caso de no estar disponible para el efecto, teniendo su miembro alterno las mismas responsabilidades y capacidad de decisión.

Los miembros del Comité de Crisis son por lo tanto, los mismos miembros del Comité de Tecnología a los que han sido agregados representantes de otras áreas del banco, de acuerdo al siguiente organigrama:

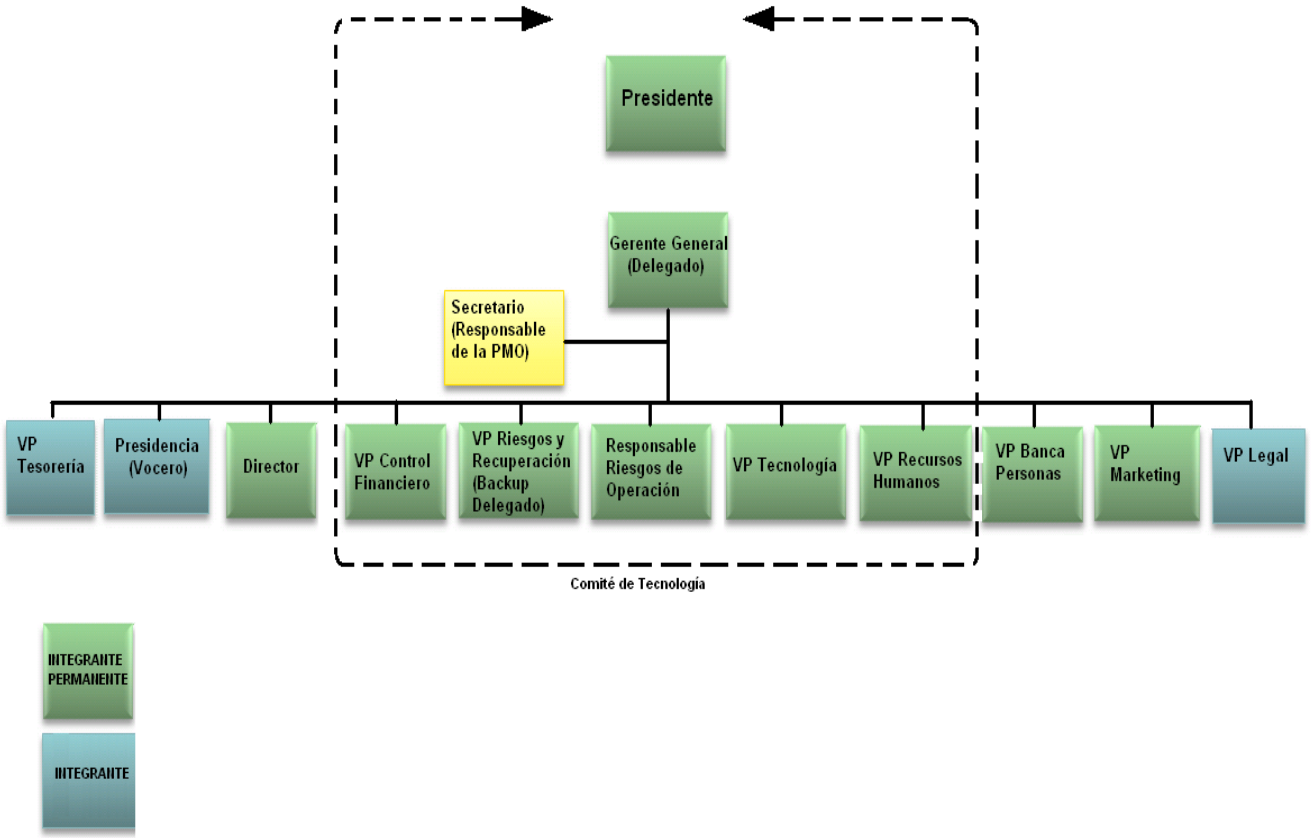

Ilustración 19. Estructura de Comité de Crisis. Elaborado por: Wilson Jácome

5.1.2. Roles

- **Presidente:** Es la persona moral responsable de la institución, por lo cual es el árbitro de las decisiones graves. Deberá asistir en la toma de decisiones y autorización de acciones así como aprobar las comunicaciones al resto del personal y externos en conjunto con el Gerente General.
- **Gerente General:** es la persona jurídicamente responsable de la institución, por lo cual es el centro mismo de la crisis. Deberá asistir en la toma de decisiones y autorización de acciones así como aprobar las comunicaciones al resto del personal y

externos en conjunto con el Presidente. Adicionalmente cumple las funciones de Delegado de Comité de Crisis ejecutando en primera instancia el plan de crisis, constituyéndose en el primer punto de contacto dentro de la organización en caso de generarse una crisis, y es el encargado de llamar a funciones al comité de ser necesario.

- **Secretario (Responsable de la PMO):** Apoya y asiste al Presidente y Gerente General: tomar actas, coordina agendas, coordina mensajería, archivo.
- **Responsable de Riesgos de Operación:** posee la información de las políticas, procedimientos y planes de acción respecto a la Administración de la Continuidad del Negocio y la Recuperación de Desastres.
- **Vicepresidente Tesorería:** poseen la información de la gestión de flujos monetarios dentro de la organización.
- **Presidencia Adjunta:** posee la capacidad de reacción dado que conoce internamente a la empresa y posee la credibilidad ante las personas a comunicar. Canaliza y coordina todas las comunicaciones formales con terceros, actúa en calidad de Vocero del comité y se encarga de organizar conferencias de prensa y aconsejar sobre como efectuar declaraciones.
- **Director:** Deberá asistir en la toma de decisiones y autorización de acciones así como aprobar las comunicaciones al resto del personal y externos en conjunto con el Presidente y Gerente General.
- **Vicepresidente Control Financiero:** Provee en forma oportuna y controlada acceso a los fondos necesarios para ejecutar las operaciones de recuperación, Presupuestar/estimar gastos, mantener contacto con aseguradores y presentar registros contables primarios.

- **Vicepresidente Riesgos y Recuperación:** posee los conocimientos de definición, monitoreo y seguimiento de todos los riesgos asociados a la generación y administración de crisis dentro de la organización. Provee la definición de identificación, clasificación y ponderación de riesgos así como sus planes de mitigación y contingencia.
- **Vicepresidente Tecnología:** Asegura el soporte informático y de telecomunicaciones para la Administración de la Crisis, la Recuperación del Negocio, y la operativa en régimen de contingencia. Deberá asistir en la determinación del impacto del incidente para el Negocio, desde el punto de vista tecnológico, establecer prioridades y estrategia de recuperación tecnológica alineadas a las necesidades del negocio.
- **Vicepresidente de Recursos Humanos:** Maneja todos los aspectos relacionados con el personal, brinda información sobre el personal a servicios de emergencia autorizado, asiste en la identificación de víctimas y realiza tareas de contención. Además centraliza las alertas e información proveniente de las distintas instalaciones al tiempo, realiza una evaluación preliminar, notifica a los servicios de emergencia y asegura el acceso a los sitios alternativos.
- **Vicepresidente Legal:** poseen los conocimientos legales y jurídicos a fin de asesorar correctamente al resto de los integrantes del comité; y por otro lado poseen la información de la gestión de flujos monetarios dentro de la organización. Estos representantes participan del Comité de Crisis como "invitados" con el fin de brindar información necesaria para la toma de decisiones.
- **Vicepresidente Banca:** es aquella persona que tiene el conocimiento técnico de los temas y es capaz de transmitir información pertinente a ser procesada por la institución. Sirve de nexo entre el comité y las unidades del negocio, prioriza

aspectos de la recuperación del negocio, proveer una visión macro de las operaciones del Negocio, asegura los niveles de servicio.

- **Vicepresidente de Marketing:** es aquella persona que tiene el conocimiento técnico de los principales servicios en agencias que se ofrecen a los clientes de la organización, proveer una visión macro de las operaciones de cara al cliente del Negocio, asegura los niveles de servicio.

5.1.3. Responsabilidades

En el Comité de Crisis es indispensable que cada uno de los integrantes que la conforman, cumplan con determinadas obligaciones principales, tanto antes como durante y tras la situación de crisis.

Cada uno de los integrantes permanentes del comité de Crisis, deberá designar a un representante ó backup que pueda suplirlo en el caso de que por cualquier motivo, un integrante permanente no pudiera estar presente.

El delegado designado del integrante permanente podrá actuar en el Comité de Crisis, con todas las atribuciones de la persona a la que reemplaza y estará habilitado a tomar las decisiones que sean requeridas en su calidad de representante. La asistencia de los integrantes permanentes es obligatoria mientras que los demás integrantes del Comité, serán convocados de acuerdo a las necesidades y requerimientos propios del Comité y de la Crisis. Cada integrante deberá designar un representante que actúe en caso de ausencia del integrante principal.

El Comité de Crisis tiene responsabilidades a cumplir incluso en aquellos momentos en los que no hay crisis presentes.

En operación normal:

- ✓ Aprobación, incorporación y eliminación de procesos del inventario de procesos críticos.
- ✓ Realizar seguimiento de la actualización del BCP y la realización de pruebas anuales de las estrategias implementadas para los procesos críticos
- ✓ Tomar decisiones relativas a necesidades de recursos

En Crisis:

- ✓ Evaluar la contingencia detectada y tomar, en consecuencia, la decisión final de activar o no un determinado procedimiento de contingencia o una serie de ellos.
- ✓ Evaluar el curso de la contingencia a fin de establecer nuevas necesidades de activación.
- ✓ Evaluar el curso de la contingencia a fin de establecer la desactivación de un determinado procedimiento o un conjunto de ellos.
- ✓ Evaluar el curso de la contingencia y tomar la decisión sobre la finalización de la misma con la posterior notificación sobre la vuelta a la "normalidad".
- ✓ Mantener una fluida comunicación con los coordinadores de contingencia (responsables de los procedimientos de contingencia) a fin de que puedan mantener informado al comité y que puedan recibir las instrucciones para cada caso.

5.1.4. Sitio de Operación (Centro de Comando)

El Sitio de operación del comité de crisis o centro de comando debe ser una sala de juntas acondicionada tecnológicamente para trabajar durante varias horas. En caso de que el acceso al sitio predefinido de operación quede inhabilitado, se deberá identificar un sitio ubicado en

una zona de riesgo distinta que pueda ser rápidamente acondicionado para albergar al comité en situaciones de catástrofes naturales que hayan afectado a dicho sitio.

El sitio de operación queda especificado en la siguiente ubicación:

En etapa normal y/o acceso habilitado a Matriz del Banco (Centro de Comando 1)

En etapa de crisis con acceso inhabilitado a Matriz del Banco:

Agencia Los Valles

En etapa de crisis sin acceso habilitado a Matriz del Banco (Centro de Comando 2) y ciudad de Quito:

Agencia Norte GYE

En caso de no estar habilitado el Centro de Comando 2 (Centro de Comando 3):

Agencia Centro GYE

5.2. Rol de TI en Comité de Crisis

Como departamento de tecnología, al momento de una administración de crisis a continuación se describen sus principales roles y funciones:

5.2.1. Procedimiento de TI en Etapa de Crisis

Ante un incidente o contingencia la Vicepresidencia de Tecnología deberá ejecutar las siguientes tareas macros:

a) Registrar el Evento: cada crisis/contingencia sobre los componentes tecnológicos producida deberá registrarse a fin de tener un listado de eventos ocurridos.

b) Ejecutar Contingencia: Si existe previamente un plan de contingencia aplicado para la crisis identificada sobre ese o esos componentes tecnológicos se ejecuta automáticamente dicho procedimiento.

c) Tipificar y Diagnosticar: la Vicepresidencia de Tecnología es quien tipifica y diagnostica la situación tecnológica. Esto deberá realizarse de forma inmediata a fin de tomar las medidas correspondientes para el caso en cuestión. La información de base disponible al producirse el evento es la que se fundamentará la toma de decisiones.

d) Comunicar el evento: es necesario comunicar la ocurrencia de la contingencia. Dicha comunicación deberá hacerse al Comité de Crisis a fin de tratarlos formalmente si es que la crisis así lo amerita. Una vez recibida esta información, el receptor deberá convocar al resto del comité a fin de realizar un diagnóstico preliminar de la situación.

e) Plan de Continuidad de TI (BCP): Si la crisis tecnológica afecta a uno o más de los procesos críticos definidos en el Plan de Continuidad de Negocios (BCP) es necesario ejecutar las estrategias tecnológicas definidas y probadas previamente para dichos procesos.

f) Resolución de la contingencia: se procede a la ejecución de las acciones pertinentes a fin de conseguir la solución del evento.

g) Seguimiento: es necesario realizar un seguimiento del evento/contingencia a fin de determinar si la solución implementada fue satisfactoria o deberán tomarse otras medidas al respecto.

h) Registrar e informar resolución: deberá registrarse los pasos ejecutados para la resolución de la contingencia e informar con posterioridad a las personas que correspondan.

i) Cerrar crisis: dar por concluida la crisis en lo referente a los aspectos tecnológicos, registrar las soluciones para manejo de lecciones aprendidas.

5.2.2. Procedimiento de TI en Etapa Normal

a) Revisar Inventarios Tecnológicos: analizar el inventario de procesos críticos que tengan una o varias estrategias tecnológicas definidas en el BCP de Banco Nacional Financiero con el fin de verificar su RTO con su respectivo nivel de criticidad. De igual manera chequear las estrategias de continuidad atadas a dichos procesos para ajustes o mejoras de ser el caso.
b) Revisar Planes de Contingencia Tecnológicos: analizar el inventario de planes de contingencia tecnológicos para eventos previamente identificados y ponderados (Amenazas de bomba, asaltos, etc.) para los respectivos ajustes o mejoras de ser el caso.
c) Aprobar pruebas tecnológicas: Calendarizar y aprobar la ejecución de pruebas en cuanto a presupuesto, equipos a participar y fechas
d) Ejecutar Lecciones aprendidas: llevar a cabo la revisión de lecciones aprendidas en las crisis ocurridas desde la última reunión del comité con el fin de ajustar los procesos indicados en los puntos anteriores.

5.2.3. Responsabilidades

Es responsabilidad de la persona que ha sido designada como oficial de continuidad de TI colaborar en las tareas de mantenimiento del plan de continuidad de TI.

La responsabilidad sobre los contenidos de los procedimientos técnicos y/o operativos incluidos, así como requerimientos técnicos, tipo y cantidad de recursos especificados, es responsabilidad exclusiva del líder del equipo tecnológico.

5.2.4. Plan de Comunicación

- ✓ Ante un evento de crisis, cualquier empleado del banco está en la obligación de comunicar el evento a su línea de supervisión en un plazo no mayor a una hora de presentado el mismo.
- ✓ Es obligación de la Línea de Supervisión, informar a su Vicepresidencia sobre el evento de crisis tan pronto tome conocimiento del mismo, señalando temas importantes que deban ser considerados.
- ✓ Una vez que el Vicepresidente del área ha tomado conocimiento del evento de crisis presentado, deberá comunicar al Vocero del Comité que existe una Crisis que debe ser analizada.
- ✓ El Vocero del Comité definirá si es necesario convocar al Comité de Administración de Crisis para tomar decisiones, dentro del cual la Vicepresidencia de Tecnología es miembro permanente.
- ✓ Si se considera necesaria la convocatoria, el Vocero del Comité solicitará la presencia de todos los Miembros Permanentes, indicando la situación de crisis a analizar.
- ✓ Por su parte cada Miembro Permanente del Comité convocado y dependiendo de la crisis, puede solicitar la presencia de personal especializado para apoyar con información relevante al Comité. En este momento la Vicepresidencia de Tecnología verificará si es necesario ejecutar las estrategias tecnológicas definidas para el proceso o procesos críticos afectados por la crisis

- ✓ El Comité de Crisis, también podrá ser convocado de forma ordinaria para revisar el inventario de procesos críticos, las estrategias, cambios a las estrategias y procesos que requieran algún tipo de aprobación.

Ilustración 20. Flujo de Comunicaciones. Elaborado por: Wilson Jácome

CAPÍTULO VI: CONCLUSIONES, RECOMENDACIONES Y LINEAS DE INVESTIGACIÓN

6.1. Conclusiones

El manejo constante de la continuidad de negocios dentro de TI involucra un conjunto de procesos y estrategias creados para identificar impactos potenciales sobre los sistemas tecnológicos que pueden ser vividos en una organización, con el fin de proveer resilencia y la capacidad de dar una respuesta tecnológica efectiva para resguardar los intereses de los accionistas, clientes, reputación, marca y valores creando actividades de prevención. La diferente entre tener y no tener un Plan de Continuidad de Negocios de TI puede suponer que la compañía pueda desaparecer en caso de un incidente grave que perjudique sus principales procesos tecnológicos; de esta manera cuando se tiene en consideración los costos reales del tiempo de inactividad imprevisto, las estrategias tecnológicas de continuidad son rentables para la protección de las empresas frente a problemas graves.

Todas las estrategias tecnológicas pensadas para brindar continuidad de negocios deben tener su justificación adecuada, pues no tendría sentido invertir tiempo y recursos en procesos que no necesariamente deben ser automatizados para generar una solución al respecto. Para este tipo de análisis se concluye que se debería utilizar un esquema de continuidad de negocios de TI basado en el modelo PHVA (Planear, Hacer, Verificar y Actuar) de la siguiente manera:

Planear: A partir del "Análisis de impacto al negocio" de la organización, se definen los requerimientos de continuidad de TI, la política, el entendimiento de los servicios críticos de tecnología y los requerimientos para la preparación, identificando las "brechas" actuales de preparación con que cuenta TIC.

A partir de estas, se formulan las estrategias, definiendo las habilidades y conocimientos necesarios, los recursos, la tecnología, los datos, los proveedores y los requerimientos de capacidad y desempeño "resiliente" requeridos.

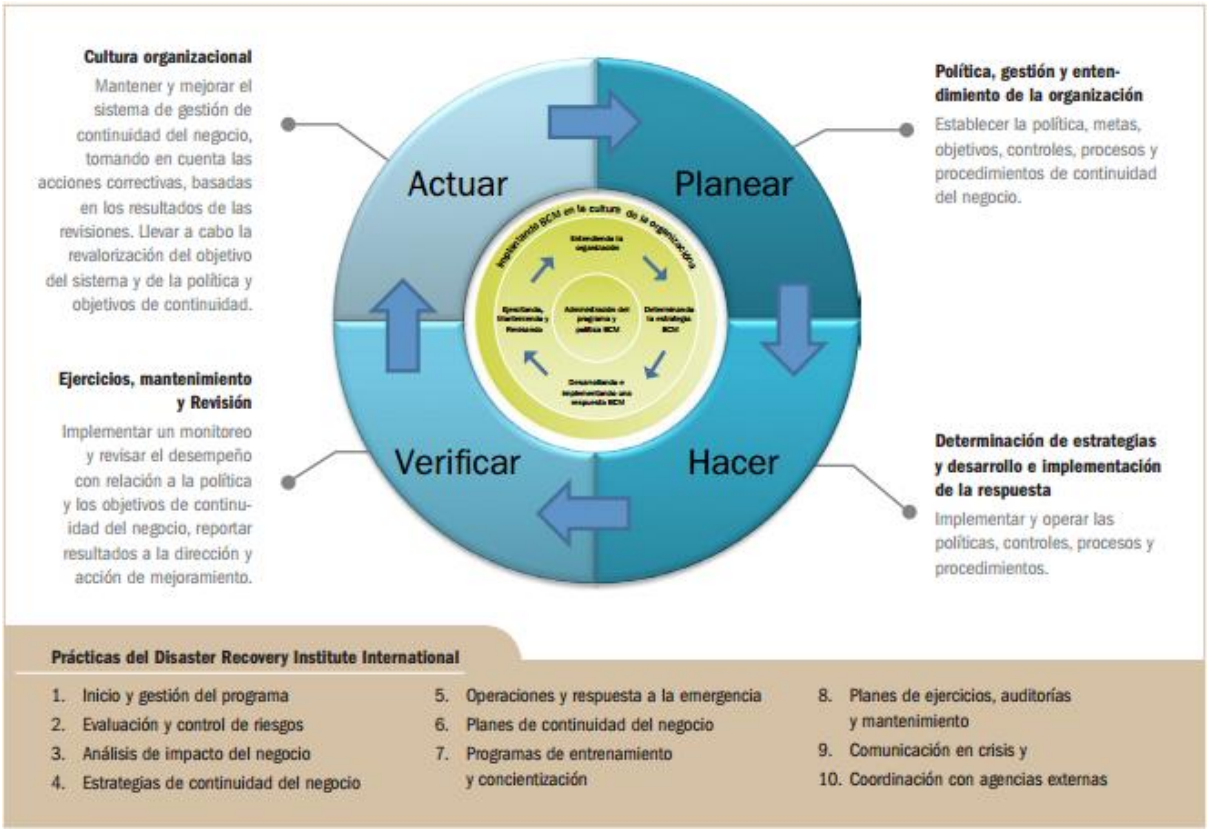

Ilustración 21. Diagrama PHAV. Fuente: Sandra Camacho, Banco Central Colombia, 2011

Hacer: Recopilación, mantenimiento e implementación del plan de preparación de TI, dentro de lo cual se encuentran: los procesos, las estrategias, los planes de respuesta y recuperación, los programas de concientización, competencia y entrenamiento así como el control de documentos relacionados.

Verificar: Monitoreo y revisión continuos, para los cuales se consideran el análisis de amenazas, la medición del desempeño de preparación de TI, las revisiones anuales, tanto de pruebas y ejercicios como de las auditorías internas y externas.

Actuar: Revisión por la dirección y el mejora- miento del plan de preparación de TI.

En conclusión, es importante contar con estándares y esquemas de medición que nos permitan identificar la posición en que se encuentra la organización, pero el gran riesgo es confiar en que solo la teoría y la documentación nos brinda protección y confiabilidad sin mantener el control en un evento de catástrofe, es en este sentido importante, resaltar que para contar con una exitosa preparación ante desastres, las pruebas y ejercicios se convierten en un elemento fundamental de las estrategias y arquitecturas tanto de TIC como operativas; las cuales deben ser realizadas de manera programada y constante, ya que nos permiten desarrollar confianza en nuestras capacidades de reacción, así como fortalecer las habilidades y experiencia de los equipos de encargados de la continuidad. Estas pruebas y ejercicios se deben hacer tanto de "escritorio" como "simuladas", con escenarios de fallas totales o parciales de todos y cada uno de los recursos críticos para el negocio.

Es importante superar el temor que nos representa "simular" una falla o crisis, mediante la preparación de todas las áreas, no solo de tecnología, sino también de las áreas operativas, ante la posibilidad de una falla severa a nivel de la provisión de recursos (personal clave, infraestructura, potencia, ambiente, tecnología, etc.), todo esto orientado al final, a minimizar la "incertidumbre" y conocer las propias vulnerabilidades, trabajar en ellas y aumentar la capacidad de "resiliencia" para la organización como un todo y así garantizar una real "continuidad del negocio".

6.2. Recomendaciones

- Por los resultados obtenidos en la aplicación de la continuidad de negocios dentro de TI , es conveniente considerar un seguimiento de los demás procesos en el que la institución financiera se desempeña como son aquellos que no son apalancados por tecnología, pero sin embargo al existir una falla pueden tener impactos trascendentales en la marca e imagen de la institución, siempre considerando salvaguardar la vida humana.
- Poner en práctica evaluaciones periódicas de los diferentes factores tecnológicos, climáticos, humanos, políticos y económicos que afectarían el normal desenvolvimiento de la entidad, para analizar si las medidas consideradas en el plan de continuidad de TI son aún vigentes o necesariamente deben ser actualizadas.
- Con respecto a cambios económicos y/o políticos que puedan presentarse debe efectuarse seguimiento a los eventos posibles que fueron considerados en el presente trabajo, ya que puede existir en un futuro algún cambio crucial provocando reformas de la estabilidad económica y legislación de nuestro país para lo cual se debe considerar la cuantificación en caso que aquellos eventos descritos en los descritos aquí de riesgo se llegue a concretar. El planteo de escenarios de desastre servirá de base al momento de determinar las alternativas viables para la recuperación.
- El plan de continuidad de negocios de TI deberá ser desarrollado para cubrir el peor escenario, de manera que escenarios menores queden cubiertos también, desde una simple motivación del personal de crédito como la adquisición de nuevos equipos para garantizar la seguridad de la documentación.
- La alta dirección debe estar disponible para decidir la activación del plan y tomar las decisiones no previstas en un tiempo oportuno y con la seriedad que el caso amerita,

pues alguna desconsideración de algún análisis y estimaciones de costos puede provocar un caos a la entidad en el momento que llegue a materializarse el desastre.

- Debe existir el compromiso de la alta gerencia para establecer un equipo directivo encargado del cumplimiento de las políticas de continuidad de negocios de TI, con el fin de lograr la participación de las distintas áreas de la empresa y entendiendo los riesgos y el impacto que puedan tener.
- Se debe implementar como política la renovación del estudio del plan de continuidad de TI y estructurarlo para proyectarlo y mantenerlo a un tiempo ilimitado considerando los cambios en la magnitud del riesgo y del evento que puedan presentarse en las diferentes áreas que integran la entidad.
- Ejecutar planes de cumplimiento de las acciones preventivas para conocer si se está cumpliendo y/o llevando a cabo y medir los resultados mediante evaluaciones según sea el caso.
- Establecer mecanismos de auditoría que permitan evaluar si se cumplen las políticas definidas en la organización así como sistemas que detectan cuando se ha realizado una intrusión y permitan evaluar que vulnerabilidades tanto al sistema como a los procesos.

6.3. Líneas de Investigación

David Lacobcci. 2010. Global Crossing Conference, Quito 2010

SaiGlobal. 2010. AS/NZS 5050:2010 Business continuity – Managing disruption-related risk

Ministerio de Comunicaciones República de Colombia. 2008. Gobierno en línea Colombia, Gestión de Crisis. 2008

International Standard ISO/DIS 22313. 2012. Social Security – Business continuity management systems – Guidence

Business Continuity Institute. 2010. BCM Legislation, Regulation & Standards

Price Waterhouse Coopers. 2013. Explore the data. [En línea] 2013.

http://www.pwc.com/gx/en/information-security-survey/giss.jhtml

Gartner Blog. 2013. BCM Actually. [En línea] 2013.

http://blogs.gartner.com/business-continuity/

Tecnología al instante. 2007. TI: Tecnologías de Información. [En línea] 2007.

http://www.tecnologiahechapalabra.com/tecnologia/glosario_tecnico/articulo.asp?i=875

DeGerencia.com. 2013. Qué es Tecnología de Información. [En línea] 2013.

http://www.degerencia.com/area.php?areaid=2001

Price Waterhouse Coopers. 2013. Explore the data. [En línea] 2013.

http://www.pwc.com/gx/en/information-security-survey/giss.jhtml

Business Continuity Institute. 2008. Good Practice Guidelines, A management Guide to Implementing Global Good Practice in Business Continuity Management

Veritas Software Corporation. 2009. Disaster Recovery Solutions Guide

Disaster Recovery Institute. 2013. BCLS 2000, Administración de continuidad de negocios