UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACION

CARRERA: MAESTRIA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TEMA:

“PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN UNA COOPERATIVA DE AHORRO Y CRÉDITO EN EL ECUADOR ANTE UN EVENTO DE RIESGO”

AUTOR: **Ec. Byron Iván Solís Bedón**

TUTOR: **Phd. Elfio Pérez Figueiras**

Quito – Ecuador

Septiembre 2014

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Graduación, nombrado por la Comisión Académica de Posgrados de la Universidad Israel certifico:

Que el Trabajo de Investigación "**PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN UNA COOPERATIVA DE AHORRO Y CRÉDITO EN EL ECUADOR ANTE UN EVENTO DE RIESGO**", presentado por el Maestrante Byron Iván Solís Bedón, estudiante del programa de Maestría en Administración y Dirección de Empresas Décima Primera Promoción MBA11, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado que la Comisión Académica de Posgrados designe.

Quito, Septiembre 2014

TUTOR
Phd. Elfio Pérez Figueiras

UNIVERSIDAD TECNOLÓGICA ISRAEL

AUTORÍA DE TESIS

El abajo firmante, en calidad de estudiante de la Maestría en Administración y Dirección de Empresas Décima Primera Promoción MBA11, declaró que los contenidos de este Trabajo de Graduación, requisito previo a la obtención del Grado de Magister en Administración y Dirección de Empresas, son absolutamente originales, auténticos y de exclusiva responsabilidad legal y académica del autor.

Quito, Septiembre 2014

Byron Iván Solís Bedón
CC: 1713387106

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de Grado, designado por la Comisión Académica de Posgrados, aprueban la tesis de graduación de acuerdo con las disposiciones reglamentarias emitidas por la Universidad Tecnológica ISRAEL para títulos de posgrados.

Quito, Septiembre 2014

Para constancia firman:

TRIBUNAL DE GRADO

_____

PRESIDENTE

_____ _____

MIEMBRO 1 MIEMBRO 2

DEDICATORIA

Esta meta alcanzada es una parte de mi vida y comienzo de otras etapas por esto y más, la dedico a Dios que me ha dado la vida, guía y fortaleza para terminar esta disertación, a mis Padres por estar siempre junto a mí y por todos los consejos recibidos; a mi hermano Marcelo, por su apoyo y estímulo; y a mi novia Michelle que con su amor y compañía, me ha dado las fuerzas para culminar este reto.

AGRADECIMIENTO

Quiero manifestar un profundo agradecimiento a mis padres, mi hermano y mi novia por el apoyo incondicional que me dieron para culminar este importante reto.
Además quiero agradecer a mis jefes, por todo el conocimiento, dedicación y apoyo recibido para la realización del presente trabajo; a mis amigos que por medio de las discusiones y preguntas, me hacen crecer en conocimiento.

Y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de esta investigación, hago extensivo mi más sincero agradecimiento.

Byron

ÍNDICE

Índice General

Índice de Ilustraciones

Índice de Tablas

UNIVERSIDAD TECNOLÓGICA ISRAEL

UNIDAD DE POSGRADOS

MAESTRÍA EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

TEMA:

“PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN UNA COOPERATIVA DE AHORRO Y CRÉDITO EN EL ECUADOR ANTE UN EVENTO DE RIESGO”

AUTOR

Byron Iván Solís Bedón

TUTOR

Phd. Elfio Pérez Figueiras

RESUMEN

El presente trabajo de investigación esquematiza un plan de gestión de continuidad del negocio para una Cooperativa de Ahorro y Crédito, como una herramienta preventiva y plan de acción a seguir en el caso que se presente un evento severo de riesgo que pudiera comprometer las actividades, procesos y giro normal del negocio de la Cooperativa.

El resultado estratégico del Plan de Gestión de Continuidad del Negocio es la identificación de procesos críticos en la gestión y giro del negocio, los mismos que deberían ser de recuperación y reanudación prioritaria. De esta forma se dispondrán de elementos imprescindibles para establecer un plan de acción basado en un orden de objetivos a ser alcanzados.

PALABRAS CLAVE: Riesgo Operativo, Gestión de continuidad del negocio.

UNIVERSIDAD TECNOLÓGICA ISRAEL

POSTGRADUATE UNIT

MASTER OF BUSINESS ADMINISTRATION

TOPIC:

"MANAGEMENT PLAN BUSINESS CONTINUITY OF SAVINGS AND CREDIT COOPERATIVE (SACCO) IN ECUADOR TO AN EVENT RISK"

AUTHOR

Byron Iván Solís Bedón

ADVISOR

Phd. Elfio Pérez Figueiras

ABSTRACT

This research outlines a management plan for business continuity of Savings and Credit Cooperative, as a preventive tool and plan of action to follow in this case is a severe risk event that could compromise the activities, processes and ordinary course of business of the Cooperative.

The strategic result of the Business Continuity Management Plan is the identification of critical processes in the management and line of business; they should be recovery and resume priority. This will provide the necessary elements to establish a plan of action based on an order of goals to be achieved.

KEYWORDS: Operational Risk, Business Continuity Management Plan

INTRODUCCIÓN

Debido a que en el ámbito de las instituciones financieras la medición, administración y gestión del riesgo operativo adquiere una importancia abismal por el ingente volumen de recursos que maneja la industria; afectando transversalmente a todos los sectores productivos; el Comité de Supervisión Bancaria de Basilea ha desarrollado varios principios y herramientas encaminadas al manejo y supervisión bancaria, en los últimos tiempos han instaurado un nuevo tipo de supervisión con un enfoque en riesgos.

De esta manera se busca proporcionar a los responsables de riesgos y procesos asignados, un marco útil para definir las tareas esenciales de la gestión de riesgos, y generar un proceso sistemático para crear y mejorar las capacidades de las instituciones financieras; tanto en riesgo operativo, riesgo de mercado, riesgo de liquidez, riesgo de crédito y riesgo legal, con el propósito de encaminarlas a una gestión global de riesgos integrales.

El Plan de Gestión de Continuidad del Negocio, en una Cooperativa de Ahorro y Crédito, es esencial para la no interrupción de las actividades críticas del negocio, en el caso de que se presentara un evento inesperado que pudiera comprometer los procesos y actividades importantes de la operación de la Cooperativa.

Es importante mencionar que un plan adecuado de continuidad de negocio, no se basa únicamente en recuperar los servicios e infraestructuras de Tecnologías de la Información, el objetivo consiste en realizar un análisis profundo de los impactos financieros y operativos generados, evaluar los posibles resultados del proceso, proveer alternativas de solución para evitar que estos eventos se repitan en el futuro y finalmente analizar los beneficios que se obtendrían.

Se debe considerar que la continuidad del negocio es un proceso en donde no existe un retorno de inversión, un costo-beneficio, éste se verá únicamente cuando ocurra el incidente. Dicho plan debe estar alineado a la cultura, estrategia y planificación de la organización, además de contar con objetivos a corto, mediano y largo plazo.

El tener desarrollados los procesos que permitirán administrar la gestión de continuidad del negocio logra proteger las vidas humanas, la información, las operaciones y la infraestructura de la entidad, evitar los posibles escenarios originados por una situación de crisis así como minimizar las consecuencias económicas, reputacionales o de responsabilidad civil derivadas de la misma, y permite reducir los costes asociados a la interrupción o evitar penalizaciones contractuales por incumplimiento de contratos con proveedores de productos o servicios.

Al respecto, el presente trabajo pretende cubrir el análisis y gestión del riesgo operativo, enfocado en el plan de gestión de continuidad del negocio, bajo el marco regulatorio vigente de la Superintendencia de Bancos y Seguros en el Ecuador, riesgos que deben ser identificados, cuantificados, monitoreados y mitigados, con el fin de minimizar las pérdidas potenciales que puedan afectar a las Instituciones Financieras.

EL PROBLEMA

Tema de Investigación

"PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN UNA COOPERATIVA DE AHORRO Y CRÉDITO EN EL ECUADOR ANTE UN EVENTO DE RIESGO".

Planteamiento del Problema

Contextualización

Considerando lo dispuesto en el Libro I, Normas Generales para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X, De la Gestión y Administración de Riesgos, Capítulo V, de la Gestión de Riesgo Operativo (Resolución JB-2005-834), Sección IV Continuidad del Negocio, es necesario:

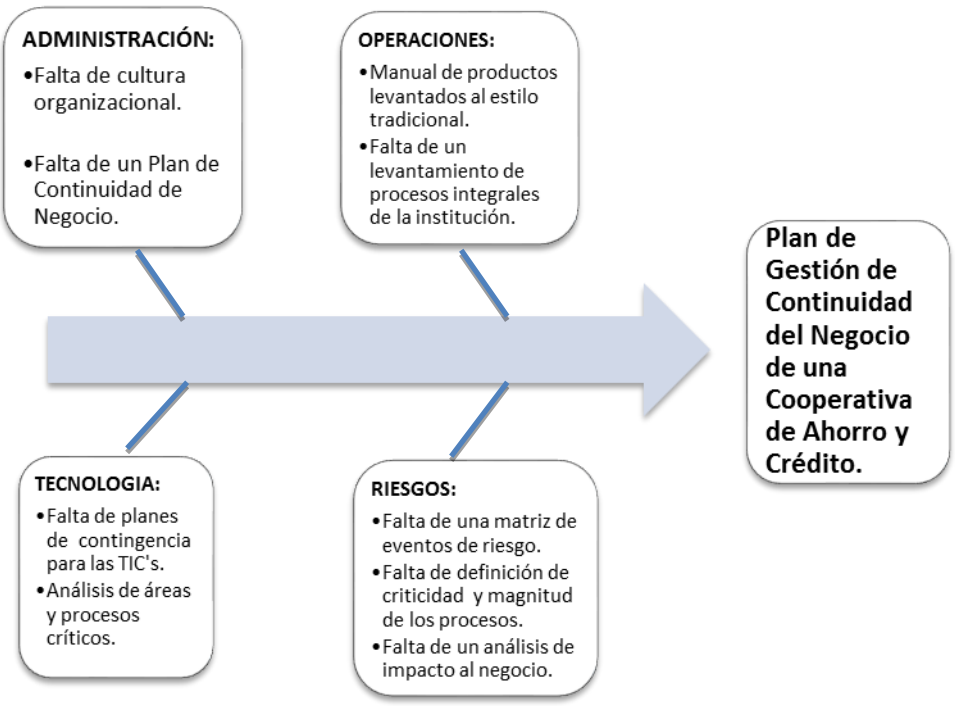
- Definición e implementación de un proceso de administración de la Continuidad del Negocio y su incorporación al proceso de administración Integral de Riesgos.
- Levantamiento de Análisis de Impacto al Negocio.
- Identificación, análisis y evaluación de riesgos que afectan a la continuidad de las operaciones.
- Definición de un Plan de Continuidad del Negocio que incluya estrategias de recuperación de las operaciones, procedimientos para declarar un desastre, procedimientos de respuesta e interrupciones/desastres, procedimientos de evacuación, procedimientos de recuperación, procedimientos alternativos de procesamientos.
- Definición de un Plan de Recuperación de Desastres DRP.
- Implementación de un Centro Alterno de Procesamiento.
- Definición e implementación de políticas y procedimientos para respaldos de información, programas y documentación.
- Definición de políticas y procedimientos para planeación y ejecución de pruebas periódicas al Plan de Continuidad.

- Definición de políticas y procedimientos para ajustes y mantenimiento al PCN.
- Definición de procedimientos de difusión y entrenamiento sobre los procedimientos de recuperación al personal.
- Ejecución de pruebas e implementación de ajustes al PCN.

Análisis Crítico

Para la determinación del problema se aplicó el diagrama de Causa y Efecto según la ilustración N.1, en donde se encontraron las siguientes causas:

Ilustración 1: Árbol de Problema (Diagrama Causa – Efecto)



Elaborado por: Byron Solís.

Prognosis

En el futuro todas las instituciones financieras, incluyendo las cooperativas de ahorro y crédito deberán contar con planes de gestión de continuidad del negocio, que permitan mitigar los impactos negativos frente a severas fallas técnicas, operativas y/o desastres naturales.

En el tiempo actual es cada vez mayor la dependencia en el negocio financiero de las tecnologías de la información, por lo que es necesario precautelar y tener un plan de recuperación de la misma, que esté debidamente documentada y en conocimiento de toda la institución.

Formulación del Problema

A continuación se detalla la pregunta a ser investigada:

¿Cómo el plan de gestión de continuidad del negocio en una Cooperativa puede contribuir a mitigar los posibles impactos negativos frente a severas fallas técnicas, operativas y/o desastres naturales?

Delimitación del Objeto de Investigación

Límite de contenido

Campo:	Administración y Dirección de Empresas
Área:	Riesgo Operativo
Área secundaria 1:	Gestión por Procesos
Área secundaria 2:	Planificación Estratégica

Límite Espacial

Cooperativa de Ahorro y Crédito en el Ecuador.

Límite Temporal

Periodo, Enero 2013 – Diciembre 2015.

JUSTIFICACIÓN

El Plan de Continuidad de Negocio está elaborado sobre la base de las propias necesidades de una Cooperativa de Ahorro y Crédito, pero también basado en las limitaciones que pudiese encontrar en la implementación del mismo, y que serán conocidas y aceptadas por el Comité de Administración. Por lo indicado, el presente desarrollo de la metodología del plan de gestión de continuidad del negocio proporciona una respuesta inmediata a los escenarios previstos y alineados en las consideraciones que a continuación se detallan:

- Áreas Funcionales
- Aplicativos Críticos
- Tipos de Eventos de riesgo
- Premisas de partida

Si bien se identifican las áreas de riesgo como tal, se les agrupa por áreas de impacto, porque cada área está relacionada con un mismo tipo de recurso y esto hace factible realizar procedimientos de recuperación y prevención para cada componente.

La realización de este trabajo de investigación, conlleva a tener un Plan de Continuidad del Negocio para una Cooperativa de Ahorro y Crédito con un enfoque integral de riesgos y alineados con la normativa expedida por la Superintendencia de Bancos y Seguros del Ecuador.

Para realizar la presente investigación se realizarán reuniones y talleres in situ con las jefaturas de todas las áreas, miembros del Consejo de Administración y demás personal involucrado en la administración de una Cooperativa, con el fin de analizar los posibles impactos negativos frente a severas fallas técnicas, operativas y/o desastres naturales, y la viabilización y tiempos de ejecución del Plan.

OBJETIVOS PROPUESTOS

Objetivo General

Proponer un plan de gestión de continuidad de negocio en una cooperativa de ahorro y crédito en el Ecuador, que permita responder y mitigar de manera inmediata y efectiva ante un evento de interrupción.

Objetivos Específicos

1. Identificar los procesos críticos del negocio de manera oportuna ante un incidente que haya afectado el sistema informático en los que se apoyan.

2. Desarrollar los planes de contingencia realizados para cada proceso crítico del negocio por parte de los responsables definidos.

3. Cuantificar el tiempo de recuperación y como consecuencia las pérdidas económicas, directas o inducidas, como resultado de un desastre ocasionado por un evento severo de interrupción.

4. Elaborar un plan organizado y consolidado para dirigir actividades de respuesta, atención al cliente y recuperación ante cualquier incidente de interrupción, evitando la confusión, duplicación de esfuerzos y reduciendo el riesgo de cometer errores cuando se activen los planes.

CAPÍTULO 1: MARCO TEÓRICO Y METODOLÓGICO

El presente capitulo detalla, con definiciones claras y explicativas, los términos y palabras que se encuentran en todo el proyecto de investigación, sustentadas científicamente para la mejor comprensión del lector.

1.1 Marco Conceptual

- **Amenaza:**
  Evento probable que afectaría negativamente las operaciones del negocio.

- **Business Continuity Management (BCM), Gestión de la Continuidad del Negocio:**
  Proceso de gestión global que identifica impactos potenciales que pueden afectar la organización y provee la estructura para dar flexibilidad y respuestas efectivas para salvaguardar los intereses y la consecución del objetivo final de la organización ante condiciones adversas.

- **Business Continuity Plan (PCN), Plan de Continuidad del Negocio**
  Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación.

- **Business Impact Analysis (BIA) / Análisis de Impacto del Negocio**
  Permite identificar las funciones críticas del negocio, conocer sus vulnerabilidades, evaluar los controles existentes y el impacto que puede producir cuando estas funciones interrumpan en función del tiempo, por tanto se identifica la urgencia de recuperación de cada función del negocio mediante una estrategia.

- **Eventos Externos**

Son aquellos ajenos al control de las instituciones, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades.

- **Impacto**

Es la magnitud de la consecuencia negativa si se materializa el riesgo.

- **Incidente**

Cualquier evento o suceso no planificado que potencialmente puede interrumpir uno o varios procesos críticos en el entorno operacional normal, con consecuencias inaceptables para la organización.

- **Plan de Contingencia**

Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado especifico. El plan de contingencia se ejecuta el momento en que se produce el evento.

- **Plan de Reanudación**

Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema.

- **Plan de Recuperación**

Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución. Dentro de este plan se considera la recuperación y restauración de los datos, servicios informáticos e infraestructura tecnológica que se lo denomina Plan de Recuperación Tecnológica ante Desastres (DRP) de la organización sobre los cuales se apoya el negocio.

- **Probabilidad**

Es la frecuencia con que se puede presentar el riesgo.

- **Proceso Crítico**

  Es el indispensable para la continuidad del negocio y las operaciones de la institución, y cuya identificación o aplicación puede generarle un impacto financiero negativo.

- **Recovery Point Objective (RPO), Punto Objetivo de Recuperación**

  Identifica la fecha, momento o punto de corte para la recuperación de los procesos críticos que se hayan visto afectados. Se necesita disponer de los respaldos de información antes que sucediera el incidente, que puede ser justo el momento del mismo, de hace una hora, inicio del día, hace un día, una semana, etc.

- **Recovery Time Objective (RTO), Tiempo Objetivo de Recuperación**

  Umbral de tiempo optimo dentro del cual deben ser recuperados los procesos críticos de la organización después de una interrupción.

- **Riesgo**

  Es la probabilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones.

- **Vulnerabilidad**

  Es todo desfase, debilidad, inconsistencia o posibilidad de falta dentro del proceso y/o actividad.

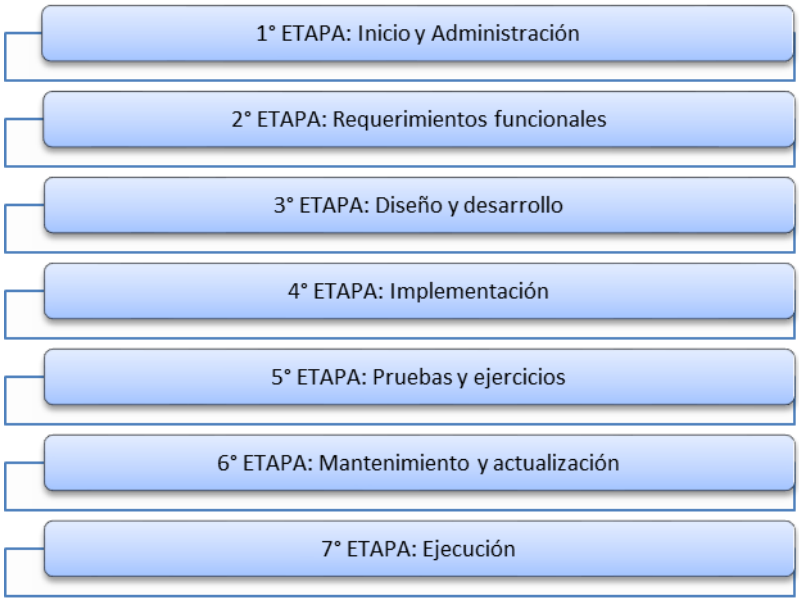
1.2 Marco Referencial

El marco de referencia para el desarrollo del plan de gestión de Continuidad de Negocio de una Cooperativa de Ahorro y Crédito; está basado en los requerimientos estándar del Instituto Internacional de Recuperación de Desastres (DRII – Disaster Recovery Institute International).

1.2.1 Metodología del DRII

El DRII es reconocido y aprobado internacionalmente por proponer lineamientos en la recuperación de negocios, permitiendo una adecuada Administración de la Continuidad del Negocio. El estándar del DRII propone su propia metodología para desarrollar los planes de continuidad del negocio aplicando prácticas profesionales, y para esto la metodología consolida el desarrollo de dichas prácticas en 7 fases. La metodología permite en cualquier momento devolverse para efectuar cambios en una fase previa o retroalimentar a otras fases. En la siguiente ilustración se enuncian las mismas y el detalle de cada una de las fases:

Ilustración 2: Metodología del DRII



Fuente: www.drii.org
Elaborado por: Byron Solis

1.2.1.1 PRIMERA ETAPA: Inicio y Administración

Establece los objetivos de continuidad de la organización y del proyecto, las políticas de continuidad dadas por la alta gerencia (Consejo de Administración) que son generales para todos los planes que se elaboren para la organización, así como los supuestos y el esquema de administración para el plan que se desarrolla, determinando la necesidad de la Gestión de Continuidad del Negocio de los procesos o funciones que tendrán el apoyo de la Gerencia y Consejo de Administración. En esta etapa se desarrollan cinco tareas:

a. Conformación del equipo inicial de trabajo

Para la constitución del plan de continuidad de la Cooperativa y el desarrollo de los planes de contingencia de cada área, se conforma un equipo que consta del personal responsable de la coordinación del proyecto y otro equipo interdisciplinario con los líderes designados de cada unidad, los cuales son apoyados por el Consejo de Administración.

b. Familiarización de la metodología por parte del equipo de trabajo

Tanto el equipo responsable de la coordinación del proyecto como el equipo interdisciplinario, son capacitados de acuerdo con los niveles de responsabilidad de cada uno de ellos, conociendo la metodología de trabajo empleada para este proyecto.

c. Definición de objetivos, alcance y escenarios del problema

El equipo inicial define los objetivos, el alcance y los escenarios que se abarca con el plan de continuidad.

d. Estructurar la administración del proyecto

Siguiendo el modelo de metodología del DRII, se establece una buena administración del proyecto, la cual incluye, creación (definir tareas y duración, establecer relaciones entre las tareas, asignar recursos), administración (es un proceso que nunca termina, se debe hacer seguimiento y ajustes al proyecto que reflejen los cambios efectuados) y reportes de progreso (se deben realizar presentaciones a Consejo de Administración (CAD) y Gerencia General y proponer ajustes para su aprobación).

e. Aprobación por parte de Consejo de Administración

Una vez terminadas estas tareas, el equipo responsable del PCN presenta un informe a CAD del proyecto de implementación del PCN para su aprobación.

1.2.1.2 SEGUNDA ETAPA: Requerimientos Funcionales

Es el estudio de amenazas, vulnerabilidades, valoración de datos, análisis de riesgo e impacto al negocio, al igual que los tiempos de recuperación que ayudan a determinar las estrategias para minimizar el riesgo de interrupción de los procesos del área que se consideren críticos para el negocio. En esta fase se desarrollan seis tareas:

a. Identificación de las áreas y proceso críticos de la Cooperativa

En este punto se establecen todas las áreas y sus procesos críticos, identificando sus prioridades de recuperación y sus dependencias internas y externas, para que puedan ser definidos los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO).

b. Identificación de recursos críticos

Determinar, para cada área y proceso, en qué recursos (computacionales o logísticos) se apoya y de esta manera establecer la criticidad de los recursos. Adicionalmente, identificar la información o registros vitales para la operación de dichos procesos.

c. Recopilación de Información

Recolectar los datos de los colaboradores, que se involucran en los procesos y servicios del área.

d. Análisis de riesgos y controles

Determinar los eventos y agentes externos que pueden afectar en forma adversa con una interrupción o con un desastre tanto la Cooperativa como sus instalaciones, el daño que dichos eventos pueden ocasionar y los controles necesarios para prevenir o minimizar los efectos de una pérdida potencial.

e. Análisis de impacto

Una vez determinados los riesgos sobre los recursos, se identifica los daños resultantes de escenarios de interrupciones y desastres que pueden afectar a la Cooperativa y técnicas que se pueden usar para cualificarlos y en lo posible cuantificarlos.

f. Aprobación por parte de Consejo de Administración

Después de terminadas estas tareas, el equipo responsable del PCN presenta un informe a CAD de los resultados del BIA para su revisión y aprobación y de esta manera dar conformidad para que el proyecto siga adelante o, en caso contrario, solicitan revisión de alguno de los puntos expuestos.

1.2.1.3 TERCERA Y CUARTA ETAPA: Diseño, Desarrollo e Implementación

Se detallan las estrategias que se han considerado implementar y que corresponde a un riesgo específico. Se describen también los escenarios definidos de acuerdo al resultado del BIA, los equipos de trabajo, los esquemas de comunicación, los procedimientos de activación y retorno, registros vitales, interdependencias, entre otros. En esta fase se desarrollan cinco tareas:

a. Diseño de estrategias y controles

Una vez identificados los riesgos, se deben diseñar estrategias y controles para mitigarlos. Para cada uno de estos componentes se identifican claramente los recursos necesarios y la forma de consecución de los mismos (desarrollo, compra de recursos, convenios, contrataciones, políticas y procedimientos).

b. Identificar equipos para operación y contingencia

Para implementar las estrategias y controles que entrarán a operar durante una contingencia, se identifica las personas necesarias para llevar a cabo la recuperación, las cuales se agruparán de acuerdo con las tareas que se establezca realizar. Así mismo se registrará la información de contacto del personal que forma parte de los equipos de trabajo.

c. Diseñar el esquema de comunicación

Con el propósito de mantener el orden y respetar los conductos regulares durante los momentos de crisis, se conforma un esquema de comunicación que permita que las personas adecuadas tomen las decisiones del momento, evitando confusiones y tropiezos. Todos los

colaboradores deben tener claro como notificar y a quien los sucesos que se presenten durante las etapas de una emergencia.

d. Contenido tentativo del plan

Se elabora un bosquejo de lo que contendrá el plan de contingencia para el área específica que se está trabajando, para que de esta manera sea comprensible para los responsables del PCN y los líderes del grupo interdisciplinario que desarrollaran el mismo, permitiendo así evaluar que sea consistente con los procedimientos actuales de la Cooperativa. Se elabora en este punto una matriz de decisión para de acuerdo al escenario conocer cual plan debe ser activado.

e. Aprobación por parte de CAD

Después de analizadas estas tareas, el equipo responsable del PCN presentará un informe de los resultados obtenidos en el diseño e implementación, quienes después de revisarlo deciden su aprobación o, en caso contrario, solicitan revisión de alguno de los puntos expuestos.

En esta fase se implantan las estrategias y controles diseñados y aprobados por el CAD, se realiza la compra y adquisición de los recursos necesarios para la recuperación, se firman contratos, se escriben los procedimientos y responsabilidades para cada integrante de los equipos de recuperación en cada momento de ésta y se preparan los sitios de recuperación.

1.2.1.4 QUINTA ETAPA: Pruebas y Ejercicios

Desarrollar programas de capacitación y entrenamiento que permita llegar a todos los niveles de la Cooperativa para poder enfrentar eventos adversos, utilizando los planes documentados, las herramientas desarrolladas para que apoyen la contingencia e instructivos elaborados para estos fines. Se complementa con la realización de pruebas, las cuales consisten en simulacros de las situaciones que se contemplan en el plan, con escenarios lo más reales posible, así como calcular los tiempos de respuestas del personal, probar los controles definidos, reanudar las operaciones con elementos reducidos y determinar el conocimiento

que tienen los colaboradores de su función en dichos procedimientos. Cada prueba se evalúa para detectar fallas y aplicar correctivos que retroalimenten el plan.

1.2.1.5 SEXTA Y SÉPTIMA ETAPA: Mantenimiento y Actualización

Un plan de contingencia no es un proyecto con inicio y fin, sino que es un proceso que nunca termina; por tanto luego de efectuarse todas las fases hasta su aprobación, debe diseñarse un plan de mantenimiento continuo para que este permanezca vigente y funcional en el tiempo.

Se desarrollarán procedimientos y mecanismos de mantenimiento y actualización de los planes definidos, para garantizar que estos se podrán utilizar efectivamente en una emergencia, velando porque su información se encuentre actualizada, completa y precisa. Se definirá mecanismos de divulgación y distribución de los planes cuando se hagan modificaciones, en donde residirán los documentos de los planes y copias de seguridad.
Y por último, se ejecutará el plan.

1.3 Hipótesis de Trabajo

La elaboración del plan de gestión de continuidad del negocio para una Cooperativa de Ahorro y Crédito permitirá que la institución financiera cuente con un plan de acción a seguir, en el caso de presentarse severos eventos de riesgo que interrumpan el giro normal del negocio, las actividades, procesos y operaciones. La ejecución del plan busca mitigar y cuantificar los impactos económicos y no económicos de dichos eventos.

1.3.1 Señalamiento de variables

Variable independiente:

- Plan de gestión de la continuidad del negocio de una Cooperativa de Ahorro y Crédito.

Variables dependientes:

- Identificación de procesos críticos en la gestión del negocio que deberían ser de recuperación y reanudación prioritaria.
- Evaluación de la probabilidad de ocurrencia e impacto en el negocio

1.3.2 Enfoque de la modalidad

Es una investigación cualitativa ya que el plan de gestión de continuidad de negocio implica la identificación de procesos críticos y la creación de un plan de acción, en el caso de presentarse un severo evento de riesgo interruptor del negocio. Proporciona orientación a los planes de corto, mediano y largo plazo, integra los planes funcionales y de contingencia en su esquema general. Es realista y se halla orientado a la acción.

La investigación cualitativa busca identificar las razones y causas profundas de las realidades, sus relaciones y correlaciones y la estructura dinámica en un contexto específico.

1.3.3 Modalidad de la Investigación

El presente trabajo de investigación utilizará dos tipos de modalidades, la primera es la investigación de campo; la cual permite recolectar información de primera mano en una forma directa; mientras que la segunda es la investigación bibliográfica; la cual utilizará la modalidad documentada, ya que es necesaria la consulta técnica para el mejor entendimiento.

1.3.3.1 Tipo de Investigación

Para la realización de la presente tesis se utilizarán los siguientes tipos de investigación:

- **Investigación Exploratoria:** La finalidad es explorar, analizar y buscar todo lo relacionado con el problema objeto de estudio, para tener una idea clara del mismo.

- **Investigación Descriptiva:** Permite conocer detalladamente las características del problema en estudio y describir su contexto tanto interno como externo en determinadas circunstancias de espacio y tiempo.

- **Investigación Correlacional:** Permite medir el impacto e incidencia entre las variables que se manipulan en el problema en un contexto específico, de tal manera que podamos relacionar la variable independiente “gestión de continuidad del negocio” con las variables dependientes, “identificación de procesos críticos” y “actividades de respuesta y recuperación”.

CAPÍTULO 2: PLAN DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

A continuación se describe paso a paso el plan de gestión de continuidad del negocio para una cooperativa de ahorro y crédito, el cual se enfoca en las Tecnologías de la Información y el Front office / cajas, ya que son las áreas más críticas al momento de una eventualidad.

2.1 Alcance

La presente tesis proporciona una respuesta inmediata a los escenarios previstos en este documento y únicamente alineados en las consideraciones que a continuación se detallan:

- Áreas Funcionales
- Aplicativos Críticos
- Tipos de Eventos
- Premisas de partida

Si bien se identifican las áreas de riesgo como tal, se les agrupa por áreas de impacto, porque cada área de impacto está relacionada con un mismo tipo de recurso y esto hace factible realizar procedimientos de recuperación y prevención para cada componente.

2.1.1 Áreas Funcionales

Se consideran áreas funcionales aquellas donde se ejecutan los procesos críticos del negocio, éstas de acuerdo a los resultados obtenidos en el Análisis de Impacto de Negocio realizado:

- Tecnología
- Cajas

2.1.2 Aplicativos Críticos

En la Cooperativa de Ahorro y Crédito de estudio, se considera al core bancario y operativo “COBISCORP”, como el aplicativo crítico, ya que el mismo centraliza las operaciones de las áreas funcionales por su modalidad de servicio ASP.

2.1.3 Tipos de eventos considerados

Para establecer el nivel del plan a seguir o activar y a su vez escalar al equipo de trabajo adecuado, se tomará en cuenta la gravedad del incidente en función del período de interrupción, las áreas afectadas y si se dispone o no de respuestas a los escenarios presentados. Las categorías son las siguientes:

- **Evento Menor:** Riesgo que causa un daño menor en el desarrollo del proceso y que no afecta mayormente el cumplimiento de sus objetivos estratégicos. Esto es, aquel que provoca una interrupción localizada en una oficina o agencia, o que de ser general **no sobrepase de las 24 horas** de paralización en el negocio. En el plan se contempla cortes de energía, telecomunicaciones o fallas menores en el hardware o software aplicacional.

- **Evento Moderado:** Riesgo cuya materialización causaría un deterioro en el desarrollo del proceso, dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que este se desarrolle de forma adecuada. Esto es, aquel que provoca una interrupción que afecta a las áreas funcionales y **que sobrepase las 24 hasta las 36 horas de paralización**. En el plan se considera: la no disponibilidad del sistema COBIS por cualquier fuente de interrupción, desastres naturales que puedan impedir la movilización o acceso normal al personal encargado de las operaciones, y que las instalaciones (principal o alterna), sean recuperables, tales como: inundaciones moderadas, terremotos moderados, caída de ceniza y que sobre las mismas se tiene un plan de respuesta desarrollado.

- **Evento Mayor:** Riesgo cuya materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de sus objetivos, impidiendo

finalmente que este se desarrolle de forma normal. Esto es, aquel que provoca una interrupción que afecta a las áreas funcionales y **que sobrepase las 36 horas de paralización**. En el plan se considera: la no disponibilidad del sistema COBIS por cualquier fuente de interrupción, desastres naturales que puedan impedir la movilización o acceso normal al personal encargado de las operaciones, y que las instalaciones (principal o alterna), sean recuperables, tales como: inundaciones, terremotos, erupciones volcánicas, caída de ceniza y que sobre las mismas se tiene un plan de respuesta desarrollado.

- **Evento Catastrófico:** Riesgo cuya materialización influye gravemente en el desarrollo del proceso y el cumplimiento de sus objetivos impidiendo finalmente que este se desarrolle. Esto es, aquel que provoca una interrupción generalizada que afecta a todas las áreas funcionales y **que sobrepase las 72 horas de paralización,** que comprometen la integridad de las personas, que cause graves daños físicos a las instalaciones o equipos tecnológicos. Sobre este impacto no existe una respuesta total pero si acciones preventivas que aporten en la solución según la contingencia.

2.2 Comités de Trabajo y Responsabilidades

Los comités de trabajo se conforman de acuerdo al tipo de incidente o evento de interrupción que se presente. Estos equipos son formados por personal clave que se encargarán de una serie de actividades para conseguir en el mínimo de tiempo un proceso eficiente de análisis y decisión de plan de contingencia a activarse, notificación al personal y establecer los procesos de recuperación. Cada equipo tiene funciones y procedimientos que tendrán que desarrollar antes, durante y posterior a la interrupción.

Los comités definidos son:

- Mesa de Ayuda o Help-desk
- Comité de Recuperación Tecnológica
- Comité de Manejo de Incidentes
- Comité de Manejo de Crisis

Para su ubicabilidad el coordinador del Plan establecerá formatos específicos para registrar la información de contacto de los miembros que conforman los comités definidos en el presente plan, y serán comunicados al personal de comité cuando se registre una actualización.

2.2.1 Mesa de Ayuda o Help-desk

Help-desk es quien receptará de parte de los usuarios finales todas las novedades que tengan que ver con la normal atención a los clientes y procederán a determinar el tipo de incidente para canalizarlo con el personal adecuado y dar una solución. Help-desk estará conformada por:

- Supervisor de producción
- Soporte de productos

Las principales funciones y responsabilidades de este equipo son:

- Receptar las novedades emitidas por los usuarios, recabar información de apoyo, analizar y determinar el tipo de incidente para canalizar al personal adecuado para que dé una solución.
- Coordinar la solución de los eventos menores definidos en el presente plan.
- Ser el nexo con el resto de comités de continuidad para notificar a todo el personal las acciones que se tomarán o se están activando antes, durante y posterior a un contingente, por los medios de comunicación que se encuentren habilitados en el momento del incidente.

2.2.2 Comité de Recuperación Tecnológica

El objetivo del Comité de Recuperación Tecnológica, es el responsable de restablecer la infraestructura y servicios tecnológicos afectados, que son necesarios para operar en condiciones normales en cualquiera de los tipos de eventos presentados.

El Comité de Recuperación Tecnológica estará conformado por los siguientes miembros:

- Jefe de Sistemas
- Supervisor de producción
- Soporte de productos

Las principales funciones y responsabilidades de este comité son:

- Restaurar servidores, computadores, comunicaciones de datos y voz y cualquier otro elemento necesario para la restauración de un servicio crítico de acuerdo a su plan de recuperación tecnológica.
- Coordinar con las empresas proveedoras de servicio para restablecer o activar procedimientos alternos o de back-up.
- Comprobar el correcto accionamiento de generadores eléctricos y UPS que soportan los equipos del centro de cómputo, verificando constantemente los parámetros de carga y habilitación.
- Recuperar las copias de seguridad de bases de datos e información de sistemas, si estos están custodiadas en un almacenamiento externo.
- Instalar y configurar el sistema operativo y aplicacional en los equipos alternos, verificando el correcto funcionamiento de las aplicaciones.
- Restablecer los equipos afectados por el incidente y una vez operativos coordinar con los equipos adecuados la vuelta a la normalidad y las instrucciones que deban notificarse a los usuarios.
- Respaldar la información (Bases de Datos, Tablas, Reportes) que registrarán las transacciones procesadas en el sistema de contingencia activado durante el evento de interrupción, información que será almacenada en el mismo medio en el cual se respaldan las bases de datos del sistema, registrando esta inclusión en el inventario de control de Tapes, con el fin de realizar futuros controles y revisiones de ser el caso.

2.2.3 Comité de Manejo de Incidentes

El objetivo del Comité de Manejo de Incidentes, es quien accionará los planes de contingencia definidos en el presente plan ante un evento moderado, de acuerdo a los escenarios planteados.

El Comité de Manejo de Incidentes está conformado por los siguientes miembros:

- Gerente General
- Jefe de Riesgos
- Jefe de Sistemas
- Jefe de Negocios
- Jefe de Operaciones
- Auditor Interno

Las principales funciones y responsabilidades de este Comité son:

- Analizar la situación o incidente presentado que interrumpe la continuidad de los procesos críticos del negocio y que fue reportado por el personal de Help-desk (HD).
- Notificar una vez conocido el incidente a los responsables de las áreas del negocio afectadas, anticipando que el personal este preparado ante una posible activación de planes de contingencia por los medios de comunicación habilitados y pueden mitigar la interrupción con el cliente.
- Determinar el escenario y si este está contemplado en la Matriz de Decisión de Planes, notificar al Comité de Recuperación Tecnológica y a los usuarios a través de Help-desk para activar el Plan definido por esta instancia y las instrucciones del caso, de lo contrario, si el escenario no está previsto, solicitar la activación del Comité de Manejo de Crisis para escalar el incidente.
- Coordinar y controlar las actividades el tiempo que dura la contingencia, notificando a través de Help-desk la situación del evento

mientras este dure y cuando se retome la normalidad para activar los procesos de reanudación.

- Emitir un informe luego de aplicado el Plan de Continuidad del Negocio, evaluando el impacto y la efectividad de las acciones tomadas.

2.2.4 Comité de Manejo de Crisis

El objetivo del Comité de Manejo de Crisis, es quien tomará decisiones claves durante los eventos mayores o catastróficos que interrumpan los procesos críticos del negocio, sobre los cuales el presente Plan de Continuidad no está preparado para garantizar continuidad en caso de desastres "GENERALIZADOS", calificados como muy improbables.

El Comité de Manejo de Crisis estará conformado por los siguientes miembros:

- Consejo de Administración
- Gerente General
- Asesor Legal
- Jefes Departamentales
- Auditor Interno

Las principales funciones y responsabilidades de este comité son:

- Analizar la situación o incidente presentado que interrumpa la continuidad de los procesos críticos del negocio y cuyo escenario en el presente plan no está preparado para garantizar continuidad en caso de desastres "GENERALIZADOS".
- Determinar las acciones a ejecutarse para controlar y mitigar el evento de interrupción, reduciendo al máximo aceptable el riesgo.
- Informar de la situación a los responsables de las distintas áreas y de terceros para que den instrucción a su personal y a los clientes para mitigar la interrupción, y el momento de activarse un plan de contingencia, dar las instrucciones del caso a través de Help-desk a

todo el personal por los medios de comunicación que se encuentren habilitados.

- Coordinar y controlar las actividades el tiempo que dure la contingencia, dando seguimiento del proceso de reanudación o restauración y vuelta a la normalidad, con relación a los tiempos estimados de recuperación.

2.3 Políticas

2.3.1 Políticas Generales

Para el manejo eficiente de las actividades que deben cumplirse en el desarrollo de los planes, su mantenimiento y actualización en el tiempo y la participación en el momento en que se requiera activar un plan de contingencia, se ha definido a más de los Comités antes descritos, las siguientes funciones:

➢ Responsable del PCN	Jefe de Riesgos
➢ Coordinador del PCN	Jefe de Sistemas
➢ Líderes del PCN	Colaboradores asignados en cada área

- El coordinador del Plan de Continuidad del Negocio (PCN), es el responsable de analizar, coordinar y sugerir el plan más adecuado de activarse cuando se presente un evento.
- Los Jefes Departamentales o Responsables de Área deberán comunicarse con el coordinador del PCN quien es el único filtro de información y coordinación durante la contingencia.
- Cuando exista un incidente o novedad el Jefe Operativo, Jefe de Negocios o Responsable de Área deberán reportar por cualquier medio a la mesa de servicio el inconveniente presentado.
- Si se presentan eventos moderados o mayores, Help-desk comunicará vía email al grupo PLANES DE CONTINGENCIA, que está conformado por: Gerente General, Jefes Departamentales, Auditor Interno y Comité de Recuperación de Tecnología.

- Cada responsable de área designará el o los delegados a quienes se los denominará Líderes del PCN, con quien el Coordinador trabajará en desarrollo, actualización y pruebas de los planes.
- Los planes de contingencia establecidos serán activados ya sea por el Comité de Recuperación Tecnológica o por el Comité de Manejo de Incidentes, de acuerdo con la matriz de decisión para activación de planes que se ha elaborado en el presente documento.
- Todo escenario no previsto en el presente documento escalará al Comité de Manejo de Crisis y esta instancia será la que tome las decisiones claves durante los incidentes adversos que interrumpan los procesos críticos del negocio.
- La comunicación entre los miembros de los diferentes Comités así como con los usuarios finales se realizará por los medios que estén disponibles en el momento de la contingencia, esto es correo electrónico, celular, teléfono o fax; siempre respetando el árbol jerárquico de comunicación.
- Si el evento de interrupción afecta la disponibilidad del aplicativo COBIS, el área de Sistemas a través del responsable de Help-desk, comunicará inmediatamente a los miembros del Comité de Recuperación Tecnológica y Comité de Manejo de Crisis, quienes analizarán la situación y determinarán previamente el Plan de Contingencia a aplicarse, quedando establecido que la activación de los Planes de Contingencia se realizarán en un tiempo aproximado de 30 minutos, tiempo referencial que dependerá de la temporada de demanda transaccional.

2.3.2 Políticas Específicas

- Los planes de contingencia en una Cooperativa son el resultado del análisis de impacto al negocio (BIA) que fue desarrollado en las matrices del Plan de continuidad del negocio, donde se identificó los escenarios de interrupción. Estas matrices del BIA deben ser revisadas por el Coordinador del PCN y si es el caso actualizarlas al menos una vez por año.

- Si bien se identifican las áreas de riesgo como tal, se les agrupa por áreas de impacto, porque cada área de impacto está relacionada con un mismo tipo de recurso y esto hace factible realizar procedimientos de recuperación y prevención para cada área en los diferentes escenarios.
- Fallas en la infraestructura o Aplicativos del Negocio por interrupciones técnicas y del medio ambiente.
    - Fallas o Cortes de Energía Eléctrica o de Telecomunicaciones
    - Fallas en los Sistemas Informáticos por Intervención Humana
    - Eventos Naturales
- Dentro de los aplicativos el no disponer del sistema COBIS se considera el más crítico y se puede presentar por los siguientes eventos:
    - Fallas en los equipos principales del Centro de Computo
    - Fallas en los enlaces de comunicación
    - Fallas en la red de fluido eléctrico
    - Desastres Naturales

2.4 Plan de Continuidad de las Tecnologías de Información

2.4.1 Identificación de las áreas de impacto y procesos críticos

En esta etapa vamos a identificar la infraestructura actual de la institución en la que se puede evidenciar los componentes que son susceptibles a sufrir daños en caso de que se suscite un evento no previsto en la operativa normal y deban ser sustituidos o reemplazados.

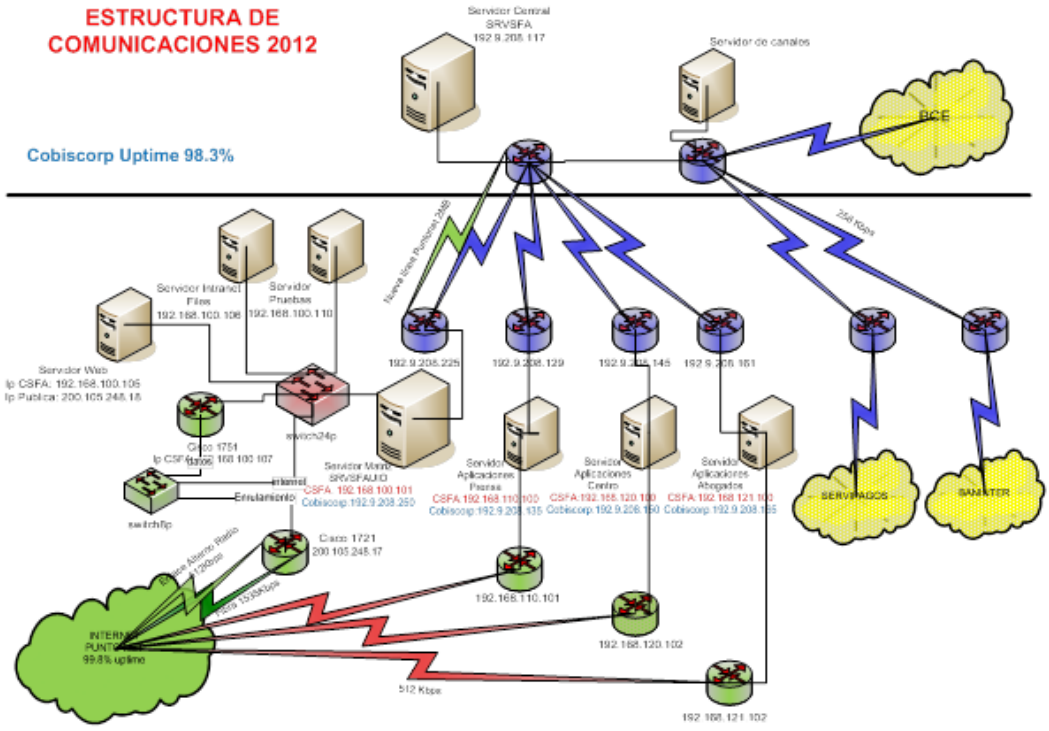
En la ilustración N°2 se muestra la red completa que presta servicio a una cooperativa y lo que pertenece a cada institución que interviene.

Cada proveedor tiene su propio plan de contingencia y la institución tiene que revisar los planes de contingencia de manera especial con su proveedor principal, para este estudio, COBISCORP, en todas las áreas de riesgos.

2.4.1.1 Estructura de Comunicaciones

- La red azul es la red de Cobiscorp con Uptime por contrato de 99.6%.
- La red verde es la red de la Cooperativa para funcionamiento de mail e internet y de respaldo de la red de Cobiscorp proporcionada por Punto-net, con Uptime por contrato de 99.6%.
- Para aplicaciones Cobiscorp la red primaria -de funcionamiento es la que está con color azul, en caso de problemas en esa red se realiza las definiciones para trabajar con la red de la cooperativa en color verde re direccionando normalmente desde el centro de cómputo en matriz, la puerta de enlace del servidor que dispone de dos interfaces de salida.

Ilustración 2: Estructura de Comunicaciones



Fuente: COBISCORP

Elaborado: COBISCORP

- La comunicación de punto-net en forma primaria se utiliza para internet e intranet de todas las agencias, en caso de caída de la comunicación de Matriz con la red de punto-net existe un respaldo

automático del enlace físico con un enlace de radio de la misma velocidad.

- Se debe trabajar en la contratación e instalación de una línea de conexión entre la Matriz y el servidor central con dos propósitos:

    a. Poder obtener en línea el respaldo diario de la información de las bases de datos que se encuentran en el Servidor operado por Cobiscorp.

    b. Como línea alterna en caso de fallas en línea de Cobiscorp que da servicio a la Matriz por considerarlo critico en el sentido de que por esta línea se requiere de mayor capacidad por fallas en cualquiera de las agencias o por que se activa el servidor principal de contingencia ubicado en Matriz.

2.4.1.2 Hardware, Software e Información

Los elementos primarios de funcionamiento de Hardware, Software y aplicaciones se encuentran en color gris y están identificados por letreros de 2 caracteres en rojo. (Ver Ilustración 3)

Cada elemento de funcionamiento primario en HW dispone de un letrero en letras azules que indica cuál es su respaldo en caso de problemas en la funcionalidad.

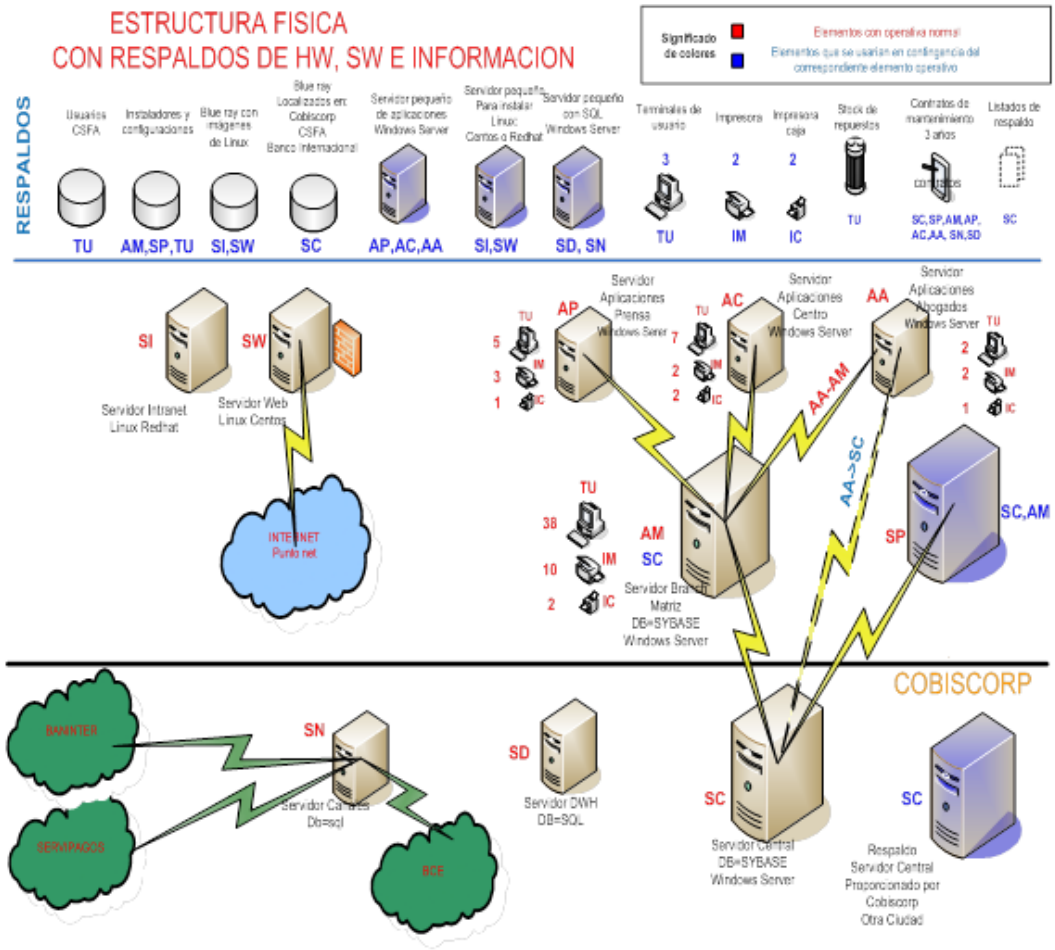
En la parte superior se encuentran todos los elementos que son exclusivamente de respaldo con letreros en color azul que indican a que elementos funcionales primarios respaldan.

Los elementos de HW de funcionamiento primario que se encuentran etiquetas con letreros de color Azul son aquellos que teniendo una función primaria pueden actuar como respaldos de otros elementos que se identifican en color azul. Ejemplo. El servidor de pruebas “SP” puede ser también utilizado en caso de contingencia como respaldo de “SC” servidor central o como respaldo de servidor de matriz “AM”.

No es factible identificar los respaldos físicos (de HW, SW, Comunicaciones) con los escenarios de eventos, se identifican con elementos funcionales a quienes respaldan.

De esta manera estableciendo ampliamente los respaldos de diferente naturaleza es factible enfrentar variados escenarios de contingencia, haciendo más eficiente la respuesta ante eventos de contingencia.

Ilustración 3: Estructura Física con Respaldos



Fuente: COBISCORP

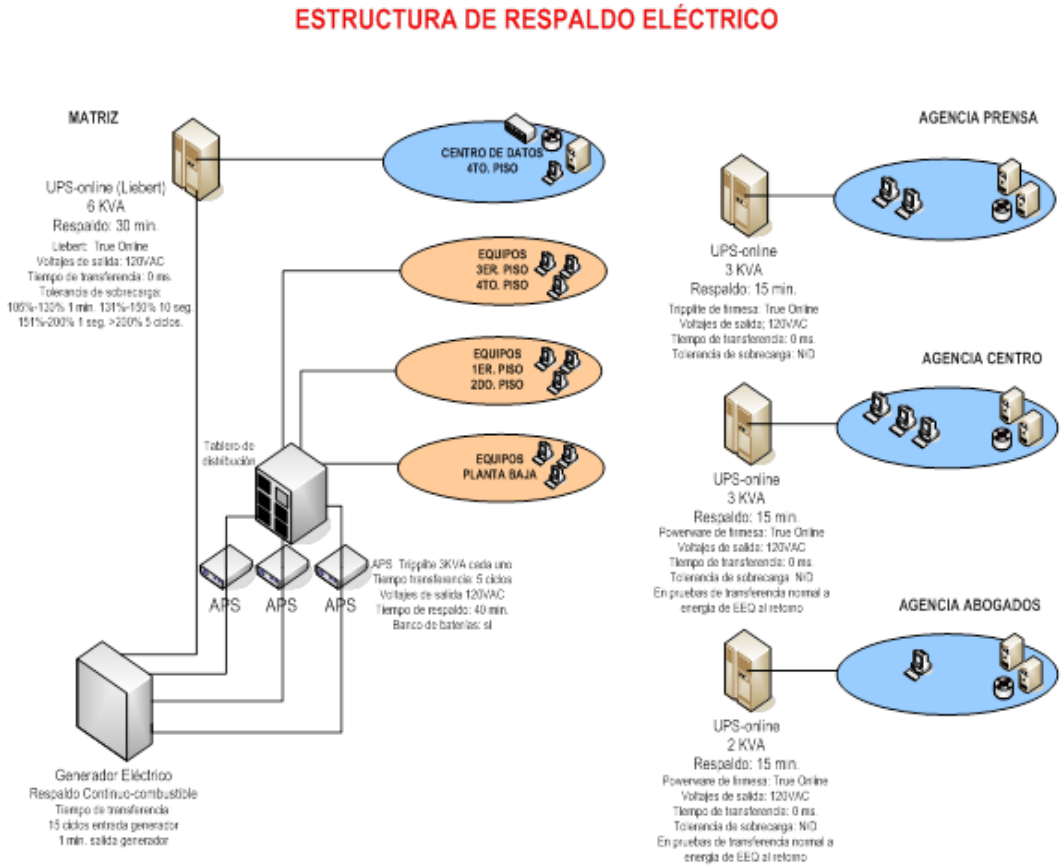
Elaborado: COBISCORP

2.4.1.3 Red de Respaldo Eléctrico

En la ilustración N° 4 se encuentra todos los respaldos eléctricos existentes.

La oficina Matriz es la mejor cubierta en energía eléctrica pues tiene centralizado la mayoría de elementos de respaldo tanto en comunicaciones como hardware, software e información.

Ilustración 4: Estructura de Respaldo Eléctrico



Fuente: COBISCORP

Elaborado: COBISCORP

- Existe el nivel de respaldo de ups para el centro de cómputo y de APS para las demás áreas.
- El generador provee un tiempo no limitado de respaldo y funciona sincronizado con los UPS y APS.

- En agencias se dispone normalmente solo de un nivel de respaldo y limitado al tiempo de UPS.

2.4.2 Evaluación del riesgo-Áreas de Impacto

Para la evaluación de riesgos se ha considerado como metodología cualitativa la escala que es utilizada en la metodología de Riesgo Operativo[1], para identificar los eventos de riesgo tanto real como potencial en los diferentes escenarios, que deben tomarse en cuenta para su tratamiento y aplicación de controles y planes de contingencia.

El plan de contingencia se aplicará a los escenarios con eventos de severidad de riesgo considerado desde moderado, que en este caso son todas las áreas de impacto. De acuerdo a los elementos que se consideran vitales en un ambiente de TIC´s, se establecen las siguientes áreas de impacto:

Múltiples áreas de impacto por Desastres Naturales

- Erupciones Volcánicas
- Inundaciones
- Incendios
- Terremotos
- Errores o Acciones Humanas

Infraestructura: Componentes Físicos

- Fallas Eléctricas
- Daño de software base (ambiental) en configuración
- Daño de equipos y de comunicación

Aplicaciones: Automáticas o Manuales

- Daños o no disponibilidad en software aplicacional
- Procesos
- No disponibilidad de documentación de operativa de aplicaciones

[1] Metodología de Riesgo Operativo, Superintendencia de Bancos y Seguros del Ecuador.

Información: Datos Procesados

- Corrupción o pérdida datos
- Falta de respaldos

Personas: Internas, outsorcing o externas a contrato (naturales o jurídicas)

- No disponibilidad de funcionarios de sistemas
- Contratos de Servicios Externos

2.4.3 Análisis de Impacto al Negocio

Los eventos de riesgo en las áreas de impacto definidas anteriormente en la evaluación de riesgos se clasifican de acuerdo a su probabilidad e impacto en el negocio. (Ver tabla 1).

Tabla 1: Impacto al Negocio

Área de impacto	Evento	Descripción	Probabilidad	Impacto	Severidad del Riesgo
Múltiples áreas de impacto por desastres naturales	Erupciones Volcánicas	En este escenario se produciría daños a toda la red de la cooperativa, dependiendo de su magnitud podría afectar múltiples sectores y áreas de impacto.	Muy Improbable	Catastrófico	Alto
	Inundaciones	Las inundaciones producirían daños a los equipos de la red de la oficina y equipos en la cual se produzca el daño, en la ciudad de Quito existen sectores en los cuales es poco probable que suceda este evento.	Improbable	Moderado	Moderado

	Incendios	Este escenario puede suscitarse en cualquiera de las sucursales al ser un desastre natural y de afectación a múltiples áreas.	Improbable	Mayor	Alto
	Terremotos	Este escenario puede suscitarse en cualquiera de las sucursales al ser un desastre natural.	Improbable	Mayor	Alto
	Errores o acciones Humanas	Los errores o acciones humanas son considerados como desastres debido a que pueden afectar en la misma magnitud que cualquier otro desastre y tienen relación con varias áreas de impacto. Aquí se considera también Sabotaje o terrorismo.	Probable	Moderados	Alto
Infraestructura	Fallas Eléctricas	Problemas en el sistema eléctrico puede ocasionar para en los equipos por faltas de provisión de energía o daños en los mismos por deficiencias en la calidad del suministro.	Probable	Menor	Alto
	Daño de software base (ambiental) en configuración	El daño de software de igual forma puede afectar al correcto funcionamiento de los equipos de la red.	Probable	Menor	Alto
	Indisponibilidad de equipos y de comunicación	Por Robo, daños mayores o por cualquier otra causa que involucre indisponibilidad de los equipos en general y de comunicación.	Improbable	Moderadas	Moderado

Área de impacto	Evento	Descripción	Probabilidad	Impacto	Severidad del Riesgo
Aplicaciones	Daños o no disponibilidad en software aplicacional	Incluye todo software, propio o de terceros. Incluye adicionalmente configuración que pueden ocasionar problemas operativos.	Probable	Insignificante	Moderado
	Procesos	Si la ejecución de los procesos planificados de TI tuviese alguna dificultad y no estaría la institución en capacidad de levantar su operativa normal. Revisar la prioridad de las aplicaciones existentes para su levantamiento.	Probable	Menor	Alto
	No disponibilidad de Documentación de operativa de aplicaciones	Los manuales de usuario y los instructivos operativos pueden no estar disponibles cuando se los necesita o pueden sufrir daños de forma premeditada o por desconocimiento.	Probable	Menor	Alto
Información	Corrupción o perdida Datos	Por fallas de software, por falta de administración, por errores operativos, por falta de seguridad y auditoria.	Improbable	Moderada	Moderado
	Falta de respaldos	Por fallas en procedimiento o incumplimientos de los mismos.	Muy Improbable	Moderado	Moderado

Área de impacto	Evento	Descripción	Probabilidad	Impacto	Severidad del Riesgo
Personas	No disponibilidad de funcionarios de sistemas	Por cualquier razón personal o porque existe una mejor oportunidad laboral.	Improbable	Mayor	Alto
	Contratos de Servicios Externos	Este escenario es afectado si no se elige bien el tipo y calidad de servicio que se necesita, o cuando el servicio prestado por el proveedor no cumple los niveles acordados. También están considerados problemas de cualquier proveedor para mantener el servicio y con la calidad contratada.	Improbable	Mayor	Alto

Fuente: Cooperativa de estudio
Elaborado: Byron Solís

2.4.4 Análisis de Prioridades

El análisis en el Plan de Continuidad de Negocio se determina a través de la asignación de prioridades. La prioridad de las aplicaciones está dada por la criticidad del riesgo en base a la actividad central de la cooperativa que es mantener las operaciones al público en un uptime del 98.3% que es el nivel de servicio garantizado teniendo las siguientes prioridades en las aplicaciones a ser restauradas.

De tal forma que los procedimientos de restauración estarán enfocados en restablecer las aplicaciones de acuerdo a su prioridad, según la siguiente tabla:

Tabla 2: Análisis de Prioridades

SISTEMA	PRIORIDAD
ADMINISTRACION Y CONTROL	Alta
ADMINISTRADOR DE TARJETAS PARA CAJEROS	Alta
ATX (CAJA)	Alta
CARTERA	Alta
CLIENTES	Alta
CREDITO	Alta
CUENTAS DE AHORROS	Alta
DEPOSITOS A PLAZO FIJO	Alta
FIRMAS ELECTRONICAS	Alta
GARANTIAS	Alta
INTERFASE CAJEROS	Alta
TESORERIA	Alta
INFORMATION FACTORY (BI Y ALM)	Media
CONTABILIDAD	Media
GESTION LEGAL	Media
NOMINA	Media
RIESGO OPERATIVO	Media
SCORING DE SOLICITUDES DE CREDITO	Media
INTRANET	Media
SIDAC, CUENTAS POR COBRAR	Baja
SIDAC, CUENTAS POR PAGAR	Baja
SIDAC, ACTIVOS FIJOS	Baja
MAIL	Baja

Fuente: Cooperativa de estudio
Elaborado: Byron Solís

2.4.4.1 Tiempos de recuperación según evento (RTO)

El tiempo de recuperación depende de las áreas de impacto y la magnitud de la contingencia, por esta razón se define a todos los casos en un rango, como muestra la siguiente tabla:

Tabla 3: Tiempos de Recuperación

		Evento	Aplicaciones prioridad alta	Aplicaciones prioridad media	Aplicaciones prioridad baja
Áreas de impacto	Múltiples áreas de impacto por desastres naturales	Erupciones Volcánicas	Depende magnitud	Depende magnitud	Depende magnitud
		Inundaciones	1 a 10 días	1-20 días	1 – 30 días
		Incendios	1 a 10 días	1-20 días	1 – 30 días
		Terremotos	Depende magnitud	Depende magnitud	Depende magnitud
		Errores o acciones Humanas	1 a 10 días	1-20 días	1 – 30 días
	Infraestructura	Sabotaje o terrorismo	1 a 10 días	1-20 días	1 – 30 días
		Fallas Eléctricas	1 a 12 horas	1 a 24 horas	1 a 36 horas
		Daño de software en configuración	1 a 12 horas	1 a 24 horas	1 a 36 horas
		Daño de equipos de comunicación	1 a 3 horas	1 a 3 horas	1 a 3 horas
	Aplicaciones	Daños en software ambiental o aplicacional	1-24 horas	1-24 horas	1 a 36 horas
		Procesos de aplicaciones	1- 8 horas	1-16 horas	1-24 horas
		No disponibilidad de Documentación de operativa de aplicaciones	Un mes a 12 meses	1 mes a 18 meses	1 mes a 24 meses
	Información	Corrupción o perdida Datos	1-24 horas	1-24 horas	1 a 36 horas
		Falta de respaldos	1-6 horas	1-12 horas	1 a 24 horas
	Personas	Renuncia de funcionarios de sistemas	1 día a 6 meses	1 día a 6meses	1 día a 6meses
		Contratos de Servicios Externos	6 meses a 12 meses.	6 meses a 18 meses.	6 meses a 36 meses

Fuente: Cooperativa de estudio
Elaborado: Byron Solís

2.4.4.2 Relación de los elementos de Recuperación y Áreas de impacto

En la siguiente tabla se ilustra todos los elementos de recuperación que deben ser construidos en forma previa, algunos de ellos están relacionados a varias áreas de impacto y en alguna forma definen la prioridad intrínseca para su construcción y disponibilidad. Se constituye en un CHECKLIST para los responsables de su disponibilidad y preparación y de esta forma se da mayor

posibilidad al hecho que debamos estar lo mejor preparados para las contingencias.

Tabla 4: Relación de elementos de Respaldo y áreas de impacto

		ÁREAS DE IMPACTO					
ELEMENTOS DE RESPALDO QUE DEBEN ESTAR DISPONIBLES PARA SUPERAR CONTINGENCIAS	**Responsable**	**Múltiples áreas de impacto**	**Infraestructura**	**Aplicaciones**	**Información**	**Personas**	**Total (prioridad para la preparación)**
Análisis de alternativas de proveedores y de servicios.	Jefe de sistemas			1		1	**2**
Análisis de alternativas de software bancario incluido costos de: migración, capacitación, software ambiental	Jefe de sistemas					1	**1**
Análisis de costos y funcionalidad de otras cooperativas Con Cobiscorp y con administración propia.	Soporte de sistemas			1		1	**2**
Auditoria de servicios que proporcionan los proveedores	Jefe de sistemas			1			**1**
Carpetas con hojas de vida de proceso de selección, organizados	Jefe de sistemas					1	**1**
Centro alterno de Servidor principal (servidor de contingencia) en matriz que dispone todos los programas ejecutables.	Soporte de sistemas	1	1	1	1		**4**
Comunicación alterna con Punto net	Producción de sistemas	1	1				**2**
Conocimientos de respaldo mutuo entre funcionarios de sistemas.	Jefe de sistemas					1	**1**
Contar con antivirus efectivo y de administración centralizada.	Producción de sistemas			1	1		**2**
Contratos de mantenimiento disponibles	Producción de sistemas	1	1	1			**3**
Documentación de configuración de toda la infraestructura	Producción de sistemas	1	1	1			**3**
Equipos de calidad y con garantía	Producción de sistemas		1				**1**
Equipos de respaldo para caso de daño	Producción de sistemas	1	1				**2**
Garantías de proveedores y niéveles de servicio	Producción de sistemas		1	1			**2**
Impresora de caja	Producción de sistemas	1	1				**2**
Impresoras de respaldo para caso de daño	Producción de sistemas	1	1				**2**

Información de Listados histórico, respaldados en servidor Windows usado en desarrollo	Producción de sistemas	1					**1**
Información de respaldo más importante en archivos texto	Soporte de sistemas	1			1		**2**
Infraestructura de respaldo eléctrico funcional y con tiempo de respuesta menor a un ciclo. Por APS. En los lugares que haya UPS el tiempo de respuesta debe ser TRUE ON LINE (o segundos)	Producción de sistemas	1	1				**2**
Inventario de software en el que indique el tipo de licencia y que dispone en cada máquina, en este inventario debe estar solo software autorizado.	Producción de sistemas			1			**1**
Línea de comunicación aérea, de respaldo entre oficina Matriz y Punto net.	Producción de sistemas	1					**1**
Línea de comunicación entre Matriz y Servidor principal para obtener los respaldos diarios	Producción de sistemas	1	1		1		**3**
Líneas de comunicación de proveedor	Producción de sistemas	1	1				**2**
Mantenimiento de firewalls	Producción de sistemas			1	1		**2**
Plan de capacitación actualizado	Jefe de sistemas		1	1		1	**3**
Plan de contingencia Cobiscorp actualizado	Jefe de sistemas	1	1	1	1	1	**5**
Preparar a personal de la institución en mantenimientos de equipos elementales.	Producción de sistemas		1				**1**
Procedimiento para activar comunicación alterna.	Producción de sistemas	1	1				**2**
Procedimientos de limpieza de archivos	Producción de sistemas			1	1		**2**
Procesos para contingencia en forma coordinada con áreas operativas y procesos.	Sistemas y procesos	1		1			**2**
Renovación oportuna de todos los contratos de mantenimiento, antivirus y comunicaciones	Jefe de sistemas y producción		1	1			**2**
Respaldo de servidor de canales	Producción de sistemas	1	1				**2**
Respaldos con imágenes de servidor Web y servidor de Internet	Producción de sistemas	1	1				**2**
Respaldos de aplicaciones propias de la institución	Producción de sistemas			1			**1**
Respaldos de documentación: Manual de usuario e instructivos operativos actualizados y completos	Producción de sistemas Soporte	1		1			**2**
Respaldos de ejecutables de aplicaciones de proveedores-	Soporte de sistemas			1			**1**
Respaldos de instaladores y configuraciones	Producción de sistemas	1	1				**2**
Respaldos de información de usuarios	Producción de sistemas	1					**1**

Respaldos diarios de base de datos, disponibles en caja fuerte de Banco Internacional.	Producción de sistemas	1			1		**2**
Respaldos diarios de base de datos, disponibles en Matriz.	Producción de sistemas	1			1		**2**
Revisión de contrato y sustentación para disponibilidad de fuentes del sistema Cobiscorp	Jefe de sistemas			1		1	**2**
Servidor de contingencia para servidores de aplicaciones: Prensa, Centro y abogados.	Producción de sistemas	1	1				**2**
Servidor de contingencia para servidores de Web e Internet.	Producción de sistemas	1	1				**2**
Stock de repuestos	Producción de sistemas	1	1				**2**
Todos los equipos con contrato de mantenimiento	Producción de sistemas		1				**1**
Para respaldo de Información a ser utilizada en casos de desastres mayores o extremos.-Buscar acuerdos con Instituciones, de preferencia cooperativas, en otra ciudad del Ecuador, que dispongan de infraestructura Cobiscorp, para respaldo mutuo de información y procesos.	Jefe de Sistemas	1			1		**2**
TOTAL DE EVENTOS SEGÚN ÁREA DE IMPACTO		**27**	**24**	**19**	**10**	**8**	**88**

Fuente: Cooperativa de estudio
Elaborado: Byron Solís

2.4.5 Planes de Continuidad para las Áreas de Impacto de las TIC's

A continuación, se presentan todas las áreas que podrían ser afectadas o impactadas por los eventos antes analizados.

2.4.5.1 Área de Impacto: Desastres Naturales

Escenario de Contingencia

Para todos estos escenarios se ha considerado como contingencias disponer de varios elementos que se preparan con anticipación y se utilizan de acuerdo a la magnitud del desastre.

Premisas de recuperación

Los escenarios dentro de esta categoría pueden presentase solos o acompañados, son considerados como riesgo alto debido a que la magnitud de

su impacto puede llevar a la destrucción total de los centros de almacenamiento, procesamiento, recurso humano, infraestructura de oficinas etc., para ello definiremos las acciones generales que deben ser tomadas.

Elementos principales de recuperación

1. Servidor principal
2. Comunicación alterna con Punto net
3. Respaldos diarios de nuestras bases de datos

Para una concepción global, en este plan se encuentra la relación de elementos de respaldo y eventos.

Responsables

- Jefe de Sistemas
- COBISCORP
- Supervisor en Producción
- Jefe de Soporte

Procedimiento Recuperación Desastres Naturales

Respaldos diarios

- Los respaldos la cooperativa los obtiene del centro del hosting en forma diaria.
- El Blue-ray está ubicado en la caja fuerte de la cooperativa y el responsable de guardar es el Supervisor de Producción.
- Este respaldo debe estar disponible todos los días en el primer estante de la caja fuerte ubicado en el departamento de Sistemas.
- Una copia del Blue-ray debe enviarse a la caja fuerte de un Banco de la localidad.
- Cobiscorp en calidad de dueño y operador del core bancario respalda cada semana bajo sus políticas y necesidades y envía a un sitio distante al menos de 50Km. de distancia.

Comunicar del inicio del plan por desastre natural

- Se debe comunicar al área de sistemas.
- Se debe dar la alerta de inicio del plan por desastre natural de esto será responsable el Jefe de Sistemas.
- Se debe comunicar al responsable de COBISCORP de acuerdo a la hoja de notificación, el responsable es el Jefe de Sistemas.
- Esta actividad se la debe realizar en el plazo más reducido que podría ser entre 2 y 15 minutos.

Apagar los equipos

- Se deben apagar los equipos de toda la Cooperativa que este comprometido con el desastre, el Supervisor de Sistemas y help-desk darán las instrucciones a los usuarios. Tiempo 5 minutos.
- Se apagarán los servidores de la oficina Matriz, responsable help-desk y Supervisor de Sistemas. Tiempo entre 2 minutos y máximo 15 minutos.

Evacuar

- Tomar el Blue-ray del último respaldo ubicada en el primer estante de la caja fuerte ubicada en el Departamento de Sistemas. Tiempo 1 minuto. Responsable help-desk.
- Tomar para rescatar el servidor Branch o de Aplicaciones o Principal de cada oficina. Responsable Supervisor de Sistemas en la Matriz y Asistente Operativo en las oficinas. Tiempo 5 minutos.
- Salir por los sitios destinados para la evacuación.

Centro Alterno

- En un tiempo máximo de 2 horas entregar el Blue ray a COBISCORP para subir los datos. Cobiscorp puede utilizar este respaldo u otro más reciente que disponga.
- En caso de problemas del servidor principal, utilizar el centro alterno definido para esta actividad, que es la oficina Matriz de la Institución.

Evaluación general

- El Jefe de Sistemas y de ser necesario de acuerdo a la magnitud del desastre con el Comité de Manejo de Incidentes, evaluaran todos los elementos que se requieran y se priorizará en base a la circunstancia especial.
- Realizar plan completo estableciendo tiempos y responsables.

Nota: No se considera Desastres Extremos.

El presente plan de continuidad y contingencia no está preparado para garantizar continuidad en caso de desastres "GENERALIZADOS", calificados como muy improbables. Sobre "la información" sistematizada o digitalizada de la Cooperativa, se debe indicar que la misma en el presente plan está protegida en diferentes lugares y en diferentes circunstancias, que permitan que luego de un desastre generalizado la Cooperativa de Ahorro y Crédito este en capacidad de reiniciar las actividades cuando se pueda rearmar la infraestructura de equipos, comunicaciones y RRHH, con soportes de otros centros de cómputo factibles, con los cuales se puede realizar un convenio tanto del mismo proveedor que dispone de servicios en otras ciudades y países o con otro software.

2.4.5.2 Área de Impacto: Infraestructura

Escenario de Contingencia

Para este escenario vamos a tomar en cuenta varios eventos por los cuales los equipos principales pueden quedar fuera de servicio.

Premisas de Recuperación

Con el fin de responder eficientemente con los elementos de respaldo requerido en esta área de impacto se realizará y mantendrá en forma previa las mejores condiciones para enfrentar una contingencia:

- Los equipos servidores contaran con garantía del fabricante 7X24 y garantía de partes y piezas.
- Los equipos de usuario (terminales) contaran con la garantía básica, 1 año.
- Los equipos de comunicación estarán respaldados de un nivel de servicio de uptime mayor al 99.5%.
- Los computadores de la institución serán de calidad y conforme se vaya terminando la vida útil de los clones se remplazarán.
- La Cooperativa dispondrá de las partes y piezas más usadas y realizará mantenimientos anuales en todos los equipos, para ello capacitará al personal interno en las tares elementales de mantenimiento de equipos y/o a su vez contratará los servicios de una empresa especializada que complemente este trabajo.
- Mantener en el centro de cómputo todas las normas de seguridad y estándares de energía. En la Cooperativa se cuenta con ups y aps que garantizan la continuidad hasta que la planta eléctrica tome el control de energía alterna.
- En caso de falla total de equipos se dispondrá en la bodega del centro de cómputo de respaldos de acuerdo a su índice y frecuencia de daño.
- Para el caso de los equipos que están bajo la administración de COBISCORP se trabajará de acuerdo a los recursos y a la contingencia que se establezca en el plan enviado por ellos.
- Todos los equipos cuentan con software legal en la Cooperativa de tal manera de contar con el soporte inmediato del proveedor. Se mantendrá en forma permanente un inventario de software que usa cada usuario o elemento de la red. Adicionalmente se debe disponer de instaladores de cada software ambiental.
- Se dispondrá de instructivos operativos de configuración.

Elementos principales de recuperación

Normalmente se presenta un equipo a la vez. Los equipos más importantes son:

1. Equipos de comunicación
2. Servidor central y los servidores Branch de impresión
3. Aplicaciones servidores web y de Internet.

Responsables

- Jefe de Sistemas
- COBISCORP
- Supervisor en Producción
- Jefe de Soporte

Procedimiento de Recuperación de Infraestructura

Para cualquier evento en este escenario se deberá reemplazar equipos mediante el siguiente procedimiento:

- El Supervisor de Producción será el encargado de evaluar el daño en un tiempo no mayor a 30 minutos.
- Se tomará el equipo de back-up y se reemplaza en tiempo de 5 minutos a 1 hora, este equipo está ubicado en el cuarto de máquinas en un lugar específico de equipos de respaldo.
- Con instructivos de configuración se configura los equipos cambiados.

Procedimiento para subir comunicación alterna

- Notificar a la persona responsable en Cobiscorp que está en la lista de contactos para que realice la configuración del Server central según sus procedimientos. Tiempo 10 minutos.
- El Supervisor de Sistemas cambia el getway del Server Branch de la oficina que tiene el problema con la dirección que sea de la comunicación alterna. Tiempo 10 minutos.
- Cambiar el servidor de conexión de la oficina, ejemplo: SREVSFAUIO A SRVSFA, es decir los usuarios se conectaran de forma directa al central.
- Esta comunicación estará arriba el tiempo que la comunicación principal este fuera de línea y se restablezca de forma normal.

2.4.5.3 Área de Impacto: Aplicaciones

Escenario de Contingencia

Para este escenario se tomarán en cuenta varios eventos para los cuales las aplicaciones financieras y administrativas pueden haber sufrido un deterioro.

El software ejecutable de las aplicaciones financieras y administrativas se encuentra en el Servidor de Contingencia ubicado en la Matriz y está listo para entrar en producción solamente restaurando el último respaldo.

Premisas de Recuperación

Con el fin de responder eficientemente con los elementos de respaldo requerido en esta área de impacto se realizará y mantendrá en forma previa las mejores condiciones para enfrentar una contingencia:

- En caso del software administrado por proveedor de outsorcing se trabajará bajo las contingencias que estén bajo su plan, exigiendo como normas mínimas las que se establecen para el software de la Cooperativa. Esto es factible cuando se disponga cada año de una auditoria del servicio ASP, considerando todos los procesos Cobiscorp.
- En caso de aplicaciones propias de la institución, se deberá:
  - Disponer de todos los programas fuente y ejecutables.
  - Disponer de un control de cambios y versiones de software.
  - Disponer de un respaldo de los puntos anteriores en un área diferente a la institución.
  - Se debe disponer de respaldos ejecutables de la última versión estable de software aplicacional de proveedores.
- Está instalado un antivirus con administración centralizada para proteger el software base contra intrusos o virus que puedan dañar las configuraciones diseñadas.
- Está configurado e instalado firewalls en los servidores de Linux para proteger la intromisión a la red y posibles instalaciones de rootkit.

- Como parte del mantenimiento de hardware también se hace una limpieza de software de archivos innecesarios, y de herramientas de reparación como scandisk.
- En el caso de los servidores de correo se realizará una actualización de los servicios y nuevos correos una vez a la semana
- Se mantendrán respaldos de documentación, de manual de usuario e instructivos operativos. Las aplicaciones de proveedores deben disponer de manuales actualizados.
- Se debe analizar y disponer de alternativas de proveedores en caso de que por alguna causa de fuerza mayor no se pueda continuar con un proveedor.

Responsables

- Jefe de Sistemas
- Supervisor de Sistemas (Soporte)
- Proveedores de aplicaciones

Procedimientos de Recuperación de Aplicaciones

Para los escenarios descritos dentro del área de impacto de aplicaciones de equipos, se resume un solo evento que uno o más equipos de la red LAN o WAN no puedan prestar el servicio adecuado interrumpiendo las actividades normales del negocio de la institución.

Para cualquier evento en este escenario se deberá actualizar la última versión de software mediante el siguiente procedimiento:

- El Supervisor de sistemas (soporte) será el encargado de evaluar el daño en un tiempo entre 15 minutos y 60 minutos.
- Con los respaldos de aplicaciones se actualizara los equipos en que sea necesario. Se actualizará en el equipo correspondiente en tiempo de 5 minutos a 2 horas. El respaldo de aplicaciones está ubicado en la caja fuerte de sistemas.
- Se configura en base a instructivos.
- Se verifica la confiabilidad.

2.4.5.4 Área de Impacto: Información

Este área de impacto en cualquiera de los dos eventos podrían tener un impacto alto y determinantes para la operación del negocio, pero con la obtención de respaldos continuos y una verificación que realiza la institución diariamente sobre la validez, la severidad del riesgo es moderado y menor.

Es necesario tener presente que la administración la está realizando como parte del sistema de tercerización.

Escenario de Contingencia

Para estos eventos tenemos respaldos diarios de la base de datos, estos respaldos son generados como parte del proceso Batch y son guardados en Blue-rays, estas son guardadas y custodiadas por la Cooperativa en una caja fuerte y las de fin de mes en una caja de seguridad en una institución financiera.

Responsables

- Help-desk
- Cobiscorp
- Jefe de Sistemas

Procedimientos de Recuperación

El jefe de sistemas determinara el evento de riesgos, y notificará a la persona responsable descrita en la lista de contactos.

De forma inmediata se pondrá en aplicación el plan y procedimientos descritos en el plan de contingencia que posee COBISCORP. De acuerdo a la determinación de los tiempos.

2.4.5.5 Área de Impacto: Personas

Se considera como personas al personal técnico de sistemas tanto interno como externo, contratos de provisión de servicios con personas naturales

o jurídicas. La severidad del riesgo es alta y por ello se revisaran cada uno de los eventos.

Escenario de Contingencia

No disponibilidad de funcionarios de Sistemas por renuncia, enfermedad u otras razones que incluyen mejores oportunidades laborales.

Para poder responder a este evento de contingencia se realizará en forma previa:

Procedimientos de Recuperación

- Sobre la base de la estructura existente de funciones, se definirá conocimientos de respaldo mutuo entre los funcionarios de sistemas.
- Se buscará una política para mantenerse competitivo en esta área laboral.
- Se estimulará al Recurso Humano con capacitación.
- Se dispondrá de carpetas de procesos de selección anterior con hoja de vida y conocimientos disponibles para las necesidades de la institución.
- Se mantendrá al tanto de las disponibilidades en el medio de recurso humano necesario para cumplir funciones en sistemas de la institución

2.5 Plan de Continuidad del Front Office – Cajas

A continuación se detallan las áreas de impacto relacionadas a Front Office.

2.5.1 Identificación de las áreas de impacto

2.5.1.1 Áreas de Impacto: Desastres naturales e infraestructura

Escenario del riesgo

Los escenarios dentro de esta categoría pueden presentase solos o acompañados, son considerados como riesgo moderado o alto debido a que la magnitud de su impacto puede llevar hasta el deterioro/daño de las instalaciones físicas e interrupción en el sistema de telecomunicaciones, en estas circunstancias no estarán autorizados los retiros en ninguna agencia o canales externos, habilitando únicamente los depósitos (con doble papeleta).

Premisas de Recuperación

Los planes para afrontar todos estos escenarios deberán ser preparados y revisados periódicamente, deberán tener asignados los recursos necesarios de acuerdo a la magnitud del desastre que se prevé. Deberá salvaguardarse la documentación de las transacciones realizadas, guardar la información procesada, poner en buen recaudo el efectivo en mano.

Elementos principales de recuperación

1. Bóvedas;
2. Papelería.

Responsables

- Jefe de Operaciones;
- Supervisor de Operaciones;
- Auxiliar de Cajas / Asistente de Operaciones.

Procedimiento de Recuperación Desastres Naturales

Consideraciones previas al inicio del evento

- El Auxiliar de Cajas / Asistente Operativo comunicará al Comité de manejo de incidentes sobre el evento que ocurre;
- El Auxiliar de Cajas deberá grabar (opción “transmitir” del sistema Cobiscorp) la información de las transacciones realizadas de forma permanente;
- El Asistente Operativo deberá grabar (opción “transmitir” del sistema Cobiscorp) la información de las transacciones realizadas;
- El Auxiliar de Cajas deberá recopilar toda la documentación generada desde y previa la apertura de caja (atención al público) y el efectivo para poner a buen recaudo (bóveda);
- El Asistente Operativo deberá cerciorarse de Cerrar las bóvedas.

Actividades al reinicio y posteriores

- El Asistente Operativo/ Auxiliar de Cajas deberá comunicarse con el Comité de manejo de incidentes, quienes le brindarán indicaciones para el reinicio de las actividades;
- El Asistente Operativo/ Auxiliar de Cajas deberá cerciorarse de que las condiciones físicas del sitio asignado para la atención sea la más adecuada;
- La atención al público, será solo para transacciones de depósitos y se lo realizará con doble papeleta; a continuación se describe la forma de proceder:
    - El depositante deberá llenar la papeleta de depósito por duplicado;
    - El Auxiliar de Cajas verificará que las papeletas estén debidamente llenas y sin enmendaduras;
    - El Auxiliar de Cajas contará el efectivo y verificará que no existan billetes falsificados;
    - El Auxiliar de Cajas sumillará y sellará ambas papeletas; una entregará al depositante y la otra archivará el Auxiliar de Cajas;
    - Una vez que se restablezcan las telecomunicaciones y que help-desk confirme el reinicio de las actividades en el sistema, se ingresará toda la información de las transacciones realizadas en esta etapa.

Nota: En el caso de no poder reiniciar actividades, una vez que el evento no presente réplicas y con el consentimiento del Comité de manejo de incidente, el Auxiliar de Cajas / Asistente Operativo deberá direccionar al canal externo habilitado en la contingencia.

2.5.1.2 Área de Impacto: Aplicaciones

Escenario del riesgo

Para este escenario se considera la interrupción en el flujo de las actividades ocasionado por daños o deficiencias en el software institucional o por inexistencia de documentación que describan los procedimientos a seguir.

Premisas de Recuperación

Deberá contarse con el apoyo de la mesa de ayuda (help-desk), knowhow de personas de apoyo (back up).

Elementos principales de recuperación

1. Software;
2. Personal back up.

Responsables

- Help-desk
- Jefe de Operaciones
- Supervisor de Operaciones
- Personal back up.

Procedimiento de Recuperación de Aplicaciones

Una vez presentado el evento (inexistencia documentos)

- El Jefe de Operaciones y/o Supervisor de Operaciones identificarán al personal que conoce el procedimiento (back up);

- El Jefe de Operaciones gestionará para que back up asista al punto de contingencia;
- La persona seleccionada brindará apoyo mientras se supera la contingencia;
- El Supervisor de Operaciones registrará las acciones realizadas.

Posterior al evento

- El Jefe de Operaciones y/o Supervisor de Operaciones generarán o actualizarán la documentación correspondiente con el apoyo del Supervisor de Procesos y Calidad.

Una vez presentado el evento (daño o deficiencia en software)

- El Auxiliar de Cajas deberá revisar los procedimientos e instrucciones impartidas en los manuales respectivos (de usuario o de procesos);
- El Auxiliar de Cajas deberá ejecutar las actividades descritas;
- El Auxiliar de Cajas / Asistente Operativo deberá comunicar a help-desk, en el caso de que no se solucione el problema.

Si el reinicio de las actividades sobrepasan los 15 minutos

- El Auxiliar de Cajas / Asistente Operativo deberá direccionar hacia canales externos para que realice la transacción, para lo cual deberá señalar la ubicación de los mismos.

2.5.1.3 Área de Impacto: Información

Escenario del riesgo

El evento podrían tener un impacto alto y determinante para la operación del negocio, pero con la obtención de respaldos continuos y la verificación, la severidad del riesgo es moderado.

Premisas de Recuperación

Deberá contarse con la documentación debidamente verificada, así como acceso a los archivos magnéticos generados.

Elementos principales de recuperación

1. Documentación de respaldo de las transacciones debidamente llenadas y selladas;
2. Respaldos en microfilm.

Responsables

- Auxiliar de Cajas
- Asistente Operativo
- Supervisor de Operaciones

Procedimiento de Recuperación de Información

Acciones previas al evento

- El Asistente Operativo es el encargado de la revisión y certificación de la documentación diaria generada en cajas;
- El Asistente Operativo es el responsable del archivo cronológico y custodio de la documentación de las transacciones realizadas en cajas.

Acciones durante y posterior al evento

- El Auxiliar de Cajas es el responsable en la recopilación de la documentación e información pertinente a cada transacción;
- El Asistente Operativo es el responsable de validar las transacciones realizadas;
- El Auxiliar de Cajas / Asistente Operativo es el encargado de determinar el error;
- El Auxiliar de Cajas / Asistente Operativo es el encargado de determinar las acciones a seguir para corregir error;
- El Supervisor de Operaciones es el encargado de determinar alternativas a seguir en el caso de que no surtan efecto las acciones tomadas;
- El Asistente Operativo será el encargado en aplicar los correctivos;
- El Supervisor de Operaciones es el responsable de actualizar o mejorar el procedimiento actual;

- El Jefe de Operaciones es el responsable de documentar cambios;
- El Jefe de Operaciones es el responsable de implementar en toda la institución;
- En el caso de no poder reiniciar las actividades pasados los 15 minutos, el Auxiliar de Cajas deberá direccionar hacia los canales externos, para lo cual proporcionará información sobre la ubicación.

2.5.1.4 Área de Impacto: Personas

Escenario del riesgo

No disponibilidad del funcionario encargado de la apertura de cajas por renuncia, enfermedad u otras razones que incluyen mejores oportunidades laborales.

Premisas de Recuperación

Deberá contarse con personal capacitado como back up.

Responsables

- Asistente operativo
- Supervisor de operaciones
- Jefe de operaciones

Procedimiento de Recuperación de Personas

Una vez presentado el evento

- El Jefe de Operaciones y/o Supervisor de Operaciones identificarán al personal que conoce el procedimiento (back up);
- El Jefe de Operaciones gestionará para que back up asista al punto de contingencia;
- La persona seleccionada brindará apoyo mientras se supera la contingencia;
- El Supervisor de Operaciones registrará las acciones realizadas.

Posterior al evento

- En el proceso de selección de personal operativo el supervisor de recursos humanos deberá incluir el criterio de un postulante que tenga experiencia de cajas;
- Recursos humanos periódicamente deberá evaluar el clima laboral en el área operativa;
- Recursos humanos deberá elaborar la matriz de reemplazo;
- Recursos humanos deberá programar la capacitación del personal con el perfil adecuado para el reemplazo.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El plan desarrollado de Gestión de Continuidad del Negocio permite a una Cooperativa tener un plan para la no interrupción de las actividades críticas del negocio, en el caso de que se presentara un evento severo de riesgo que pudiera comprometer los procesos y actividades importantes de la operación de la institución.

- Un resultado estratégico del Plan de Gestión de Continuidad del Negocio es la identificación de procesos críticos en la gestión de los negocios que se supone deberían ser de recuperación y reanudación prioritaria. De esta forma se dispondrán de elementos imprescindibles para establecer un plan de acción basado en un orden de objetivos a ser alcanzados.

- El principal evento de riesgo identificado como crítico es el asociado a las Tecnologías de la Información, puesto que en este se sustenta más del 95% de la operatividad de una Cooperativa.

- El Plan de Gestión de Continuidad del Negocio debe estar alineado a la cultura, planificación estratégica y procesos de la institución y contar con objetivos a corto, mediano y largo plazo.

- La investigación planteada en este trabajo es netamente teórica y metodológica puesto que la puesta en práctica se dará solo en el momento en que se presenten los severos eventos de riesgo descritos.

Recomendaciones

- Un aspecto clave y requerido por las mejores prácticas, es que aquellas sean implementadas con la participación de los responsables de los diferentes procesos que definen los negocios de una organización, tanto a nivel operacional-administrativo como a nivel tecnológico.

- Cuantificar las probables pérdidas esperadas cuando ocurra un evento severo interruptor del negocio para disponer de un marco de toma de decisiones, con la finalidad de estimar la ecuación “costo-beneficio” de implementar en el presente medidas tendentes a reducir pérdidas eventuales en el futuro.

- Realizar actualizaciones periódicas al Plan de Gestión de Continuidad del Negocio y que la Alta Dirección realice el seguimiento del plan operativo anual.

BIBLIOGRAFÍA

- Aragonés, J. R. (2000). *Valor en Riesgo: aplicación de la gestión empresarial.* España: Ediciones Pirámide.
- Auditoria Sistemas. (2013). *Auditoria Sistemas.* Recuperado el 2013, de http://auditoriasistemas.com/plan-de-continuidad-de-negocio/
- Ballester, M. (2005). *Continuidad del Negocio.* México: Mc Graw Hill.
- Banco Central del Ecuador. (2014). *Banco Central del Ecuador.* Recuperado el 2014, de www.bce.fin.ec
- BIS. (2014). *BIS.* Recuperado el 2014, de www.bis.org
- Business Continuity Institute. (2007). *Manual de buenas prácticas globales en gestión de Continuidad de Negocio.* España: EmelartGrafic S.L.
- Comité de Supervisión Bancaria de Basilea. (2003). *El nuevo acuerdo de capital de Basilea.*
- DRII. (2014). *DRII.* Recuperado el 2014, de www.drii.org
- Graham, J., & Kaye, D. (2006). *Enfoque de gestión de riesgos de la continuidad del negocio.* Bogotá-Colombia: Paperback.
- Herrera García, B. (2004). La Supervisión de los bancos y el rol del Comité de Basilea para la supervisión bancaria. *Contaduría y Administración N.212* .
- Instituto de Estudios Socioeconómicos de Cajamar. *El riesgo en la industria Bancaria: una aproximación a BasileaII.* España: Escobar Impresores.
- Isaca. (2014). *Isaca*. Recuperado el 2014, de www.isaca.org
- Mora, R. (2002). *El Nuevo enfoque de la Supervsión Bancaria.* Ecuador.
- Newbold, P. (2008). *Estadística para dministración y economía.*

- Norma BS-25999-1. (2006). *Gestión de la Continuidad del negocio.* España: EmelartGrafic S.L.
- OGC. (2013). *OGC.* Recuperado el 2014, de www.ogc.gov.uk
- Ramirez, G. (2011). *Informe de Auditoria Interna.*
- Romero, Y. (2007). *La Investigación.*
- Sachse, M. (2003). *Administración un enfoque basado en competencias.*
- Salazar, F. (2004). *Gestión Estratégica de Negocios.*
- Simons, K. (1996). VAR- New Approaches to Risk MAnagement . *New England Economic Review* .
- Soler Ramos, J. (1999). *Gestión de Riesgos Financieros: un enfoque práctico para países latinoamericanos, Banco Interamericano de Desarrollo.* Washingtong D.C.
- Standards. (2014). *Standards*. Recuperado el 2014, de www.standards.com.au
- Superintendencia de Bancos y Seguros. (2014). *Codificación de Resoluciones de la SBS y de la junta Bancaria.* Ecuador.
- Superintendencia de Bancos y Seguros. (2014). *Ley General de Instituciones del sistema Financiero.* Ecuador.
- Superintendencia de Bancos y Seguros. (2014). *Nota técnica sobre riesgo Operativo.* Ecuador.
- Superintendencia de Bancos y Seguros. (2014). *Superintendencia de Bancos y Seguros*. Recuperado el 2014, de www.sbs.gob.ec
- worldbank. (2014). *worldbank*. Recuperado el 2014, de www.worldbank.org