ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"PROPUESTA DE UN MÉTODO PARA ELABORAR UN PLAN DE RECUPERACIÓN DE DESASTRES (DRP) EN EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL ECUADOR"

WASHINGTON MESIAS VASQUEZ NARANJO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA-ECUADOR

Junio - 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

El tribunal del PROYECTO DE INVESTIGACIÓN CERTIFICA QUE:

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado "PROPUESTA DE UN MÉTODO PARA ELABORAR UN PLAN DE RECUPERACIÓN DE DESASTRES (DRP) EN EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL ECUADOR", de responsabilidad del Ingeniero Washington Mesias Vásquez Naranjo, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Miguel Duque Vaca, M.Sc. **PRESIDENTE**	**FIRMA**
Ing. Oswaldo Martínez Guashima, M.Sc. **DIRECTOR DE TESIS**	**FIRMA**
Ing. Juan Carlos Díaz, M.Sc. **MIEMBRO DEL TRIBUNAL**	**FIRMA**
Ing. Lady Espinoza Tinoco, M.Sc. **MIEMBRO DEL TRIBUNAL**	**FIRMA**

Riobamba, Junio 2017

DERECHOS INTELECTUALES

Yo, Washington Mesias Vásquez Naranjo, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo y que el patrimonio intelectual generado por la misma pertenecen exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Washington Mesias Vásquez Naranjo
No. Cédula: 0201609401

DECLARACIÓN DE AUTENTICIDAD

Yo, Washington Mesias Vásquez Naranjo, declaro que el presente Proyecto de Investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

_____

Washington Mesias Vásquez Naranjo

No. Cédula: 0201609401

DEDICATORIA

Dedico este trabajo de Investigación a Dios por darme salud y vida para seguir con mis estudios, a mi madre Lucila, a mi esposa Mabell y mis hijas Arianna, Anahi y Mayte por su amor y apoyo incondicional en cada uno de los retos y desafíos en los que me he propuesto.

Washington Mesias

AGRADECIMIENTO

Agradezco a la Escuela Superior Politécnica de Chimborazo, al Instituto de Posgrado, por darme la oportunidad de crecer profesionalmente y permitido alcanzar esta nueva meta.

Reconocimiento y gratitud al personal que labora en la Cooperativa San José Ltda, por brindarme su apoyo en el desarrollo del trabajo investigativo.

Washington Mesias

TABLA DE CONTENIDO

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El objetivo fue definir un método para elaborar un plan de recuperación de desastres (DRP) en el área de tecnología de la información para Cooperativas de Ahorro y Crédito del Ecuador, basado en la normativa resol_JB-2014-3066 emitida por la Junta Bancaria. Su aplicación se la realizó en la Cooperativa de Ahorro y Crédito San José LTDA ubicada en el cantón San José de Chimbo provincia de Bolívar, basándose principalmente en la identificación de procesos, tiempos y recursos críticos que se pueden presentar en las instituciones financieras, posteriormente se procedió a realizar el análisis respectivo para evidenciar cuál sería su impacto financiero en caso de tener interrupciones, el método propuesto se desarrolló tomando como base la normativa del organismo de control fundamentados con la ayuda del estándar internacional ISO 22301 para Sistema de Gestión Continuidad del Negocio y en las experiencia del desarrollador en instituciones financieras. Los planes que constan en este documento han sido elaborados en base al marco teórico definido en el Manual de Administración Integral de Riesgos de la institución, teniendo como punto de partida la Matriz de Identificación de Procesos Críticos, en la cual se han identificado los eventos de riesgos operativos que ameritan planes específicos de acuerdo a la probabilidad de ocurrencia y su impacto en la entidad. La aplicación del método ayudo a cumplir a la institución financiera con el requerimiento del organismo de control, reduciendo el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados. El método desarrollado disminuye el nivel de riesgo en un 95%, por lo que se recomienda realizar actualizaciones al método cuando existan cambios de normativa o de procesos.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INFORMÁTICA>, <SEGURIDAD TELEMÁTICA>, <ANALISIS DE IMPACTO DE NEGOCIOS (BIA)>, <PLAN DE RECUPERACIÓN DE DESASTRES (DRP)>, <ACTIVOS>, <NORMATIVA>

ABSTRACT

The objective was to define a method to develop a disaster recovery plan (DRP) in the technology area of the information to the Savings and Credit Cooperative From Ecuador, based on the regulation resol_JB-2014-3066 issued by the banking board. Its application was made in the Savings and Credit Cooperative San José LTDA located in San José de Chimbo Canton, Bolívar Province, based mainly on the identification of processes, time and critical resources that could appear in the financial institutions. Next, we proceeded to carry out the respective analysis to evidence, which will be its financial impact in case of getting interruptions; the proposed method was developed taking account the control regulations body with the help of the international standard ISO 22301 to the Business Continuity Management System and the experiences of the developer in financial institutions. The plans contained in this document have been prepared based on the theoretical framework defined in the Comprehensive Risk Management Manual from the institution, starting point the identification Matrix of the critical processes, in which the events of operational risks have been identified wich ones deserve specific plans according to the probability of occurrence and their impact on the entity. The application of the method helped to comply with the financial institution with the request of the control body, reducing the risk of affectations to the availability in the critical processes of the business against unexpected informatics incidents. The method developed reduces the level of risk by 95%, so it is recommended to develop updates to the method when there are changes in regulations or processes.

Key words: <TECHNOLOGY AND ENGINEERING SCIENCES>, <INFORMATICS>, <TELEMATICS SECURITY>, <BUSINESS IMPACT ANALYSIS (BIA)>, <DISASTER RECOVERY PLAN (DRP)>, <ASSETS>, <NORMATIVE>

CAPÍTULO I

1. INTRODUCCIÓN

El presente proyecto de investigación se lo realizo de acuerdo a la necesidad de las Cooperativas de Ahorro y Crédito que debe cumplir con las normativas emitidas por los organismos de control en lo relacionado a Riesgo Operativo, las mismas que se orientan a preservar uno de los activos más preciados, como es la información proveniente de las diferentes aplicaciones electrónicas e informáticas que se administran en el área de Tecnología de la Información.

El no disponer de políticas y procedimientos bien definidos y ágiles al momento de restaurar el servicio en las aplicaciones y equipos, produce cuantiosas pérdidas económicas degradando el servicio a sus asociados.

Las Cooperativas de Ahorro y Crédito manejan información muy valiosa de sus asociados en sus operaciones, por lo que se pretende elaborar un plan de recuperación de desastres que permita estar preparados para incidentes que pudieran afectar el normal funcionamiento de la organización y la pérdida de sus datos, software o hardware. Es así que la adopción de los planes de recuperación de desastres se ha convertido en una herramienta indispensable que permite a las empresas su permanencia en el mercado en caso de disrupciones inesperadas.

En nuestro país estos casos se presentan en mayor proporción en el sector privado financiero, que pretende salvaguardar su inversión ante desastres inesperados o incidentes disruptivos que interrumpan las actividades financieras provocando desestabilización y hasta en ocasiones desaparición de las instituciones.

1.1 Problema de la investigación

1.1.1 Planteamiento del Problema

Los cambios de normativa en nuestro país van de la mano del avance tecnológico, solicitando se disponga de herramientas y utilitarios que nos ayuden a una mejor administración y control de los datos que es considerado hoy en día el activo más preciado de toda institución financiera por la importancia de la información que ahí se administra.

Por los antecedentes mencionados el tema de seguridad, confidencialidad y protección de información, es de gran relevancia en la actualidad en las diferentes instituciones financieras, por lo que la información no debe estar expuesta a ningún peligro o amenaza en caso de presentarse una contingencia.

Las Cooperativas de Ahorro y Crédito se rigen a las normativas de Riesgo Operativo emitidas por la Junta Bancaria y la Superintendencia de Bancos y Seguros que son de uso general para las instituciones financieras, en la cual se basan para su control, la misma exige la necesidad de contar con métodos y planes efectivos que sean fácilmente aplicables y del conocimiento del personal ante la presencia de una contingencia o eventualidad mayor.

La principal debilidad que se presenta al momento de brindar el soporte necesario para superar el percance, es la falta de conocimiento personal y uso de un método ágil que nos lleve a superar rápidamente los problemas, además de la falta de recursos y herramientas informáticas.

La mayoría de Cooperativas de Ahorro y Crédito no disponen de un DRP para la Unidad de Tecnología de la Información, por lo que se incumple con la norma de la Junta Bancaria resol_JB-2014-3066 de riesgo operativo, que señala:

Eventos Externos.- *En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, 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. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.(SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 644) **.**

Para el cumplimiento de esta normativa, se consideran las siguientes definiciones:
Incidente de tecnología de la información. - Evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad significativa de comprometer las operaciones del negocio. (Junta Bancaria del Ecuador, 2014, p. 2)

Incidente de seguridad de la información. - Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Junta Bancaria del Ecuador, 2014, p. 2)

Plan de continuidad.- 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. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución. (Junta Bancaria del Ecuador, 2014, p. 2)

1.1.2 Situación Problemática

Las Cooperativas de Ahorro y Crédito en el Ecuador necesitan cumplir con las normativas emitidas por los organismos de control para cubrir los temas relacionados al Riesgo Operativo, para ello es importante tener Planes de Recuperación de Desastres que se verán reflejados en caso de existir percances naturales o humanos, garantizando la continuidad del negocio. El cambio de ente de regulación de la SBS a la SEPS ha ocasionado a que el seguimiento continuo al cumplimiento de la normativa se retrase, se espera que en un mediano plazo esta nueva súper intendencia revise y exija su implementación en todas las cooperativas.

Ante tal situación, como norma interna de cumplimiento de Riesgo Operativo se considera importante realizar la presente investigación con el fin de elaborar un Plan de Recuperación de Desastres (DRP) que contribuya a la solución del problema.

1.2 Formulación del Problema

¿Cuál sería el nivel de mejora en la continuidad del negocio para las Cooperativas de Ahorro y Crédito del Ecuador al implementar un plan de recuperación de desastres (DRP) para el área de tecnología?

1.3 Sistematización del problema

- ¿Cuáles son los requisitos de continuidad para las Cooperativas de Ahorro y Crédito?
- ¿Cómo realizar un análisis de riesgo, una vez identificado los servicios críticos?
- ¿Qué estrategias de recuperación deben implementarse para controlar los riesgos en caso de una interrupción?
- ¿Qué estrategias de continuidad de negocio se pueden generar para los activos críticos y los riesgos de impacto alto?

1.4 Justificación de la Investigación

1.4.1 Justificación Teórica

La información es considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones según lo expresa la Superintendencia de Bancos y seguros en el LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO, TITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO, ARTÍCULO 8.- Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de la información y los eventos externos (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 645).

En este principio se establece la importancia de tener sistemas informáticos integrados, que sustenten las actividades financieras y administrativas que permita que las COOPERATIVAS presten un servicio de calidad mediante un correcto manejo de información y buena gestión de los recursos con los que se cuentan.

El implementar un DRP nos permite proteger la integridad de los equipos informáticos, realizar una adecuada gestión y administración de los recursos tecnológicos en el departamento de Tecnología de la Información de las COOPERATIVAS DE AHORRO Y CREDITO, logrando la continuidad de los servicios que brindan las aplicaciones informáticas de la institución que sustentan las operaciones comerciales y administrativas, evitando la paralización de servicios institucionales que se ofrecen a la ciudadanía.

La ventaja de elaborar un DRP en las COOPERATIVAS DE AHORRO Y CREDITO repercutirá en los siguientes aspectos:

- Reducción de costos por interrupciones imprevistas
- Disminución de tiempos de interrupción del servicio a los clientes
- Facilitar el respaldo y control de información y aplicaciones
- Entrenamiento del personal

1.4.2 Justificación Metodológica

En el sector financiero es imprescindible que se cuente con la capacidad para restablecer las operaciones en el menor tiempo posible. Los riesgos asociados son muy altos y la alta dependencia en las Tecnologías de la Información y Comunicaciones ha motivado la necesidad de contar con las medidas preventivas adecuadas y con un nivel de continuidad que les permita ejecutar sus procesos de negocio sin ningún tipo de pérdida o la mínima posible. Es necesario estar protegido de las múltiples y hasta desconocidas amenazas, garantizando fundamentalmente, la preservación principalmente de tres características establecidas por la arquitectura de seguridad OSI (ISO7498-2), también llamados los pilares de la seguridad, que son (Peña Gerónimo, 2014, p. 19):

- Integridad (Integrity): hace referencia a que se proteja la exactitud y totalidad de los datos y los métodos de procesamiento, es decir, que no pueda ser alterado o destruido el contenido de la información intercambiada entre emisor y receptor.
- Confidencialidad (Confidentiality): se refiere a que la información sea accesible solo a las personas, entidades o procesos que están autorizados.
- Disponibilidad (Availability): hace referencia a que los usuarios autorizados tengan acceso a la información y los recursos en cada momento que los necesiten.

1.4.3 Justificación Práctica

Luego de establecer el nuevo método DRP para recuperación de desastres, la implementación se realizará en la Cooperativa de Ahorro y Crédito San José Ltda, partiendo de la Matriz de Identificación de Procesos Críticos, en la que se han identificado los eventos de riesgos que ameritan planes específicos de acuerdo a la probabilidad de ocurrencia y su impacto en la entidad.

1.5 Objetivos

1.5.1 General

- Definir un método para elaborar un plan recuperación de desastres (DRP) en el área de tecnología de la información para Cooperativas de Ahorro y Crédito del Ecuador.

1.5.2 Específicos

- Seleccionar los modelos y buenas prácticas aplicados a la recuperación de desastres en el Área de Tecnología de la Información de Cooperativas de Ahorro y Crédito del Ecuador.
- Identificar las necesidades de continuidad de las Cooperativas de Ahorro y Crédito del Ecuador.
- Elaborar un método de aplicación general para el desarrollo de un Plan de Recuperación de Desastres, que satisfaga las necesidades de continuidad que establece la normativa vigente.

1.6 Hipótesis

El método propuesto para el Plan de Recuperación de Desastres permitirá reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes del problema

Según la definición de varios autores se define a la continuidad del negocio como:
"Un proyecto estratégico de toda la organización involucrando a todos los departamentos y divisiones para que la información necesaria fluya de forma continuada en la medida de las necesidades de los responsables de llevarlo adelante. Su desarrollo, implementación y mantenimiento, propiciará a la organización beneficios, tales como: minimizar potenciales pérdidas económicas, reducir riesgos, reducir interrupciones, asegurar la estabilidad en la organización, facilitar una recuperación ordenada, entre otras". (Gaspar & Martínez, 2004, p. 1)

"Un instrumento de gestión que contiene las medidas (tecnológicas y humanas y de organización) que garanticen la continuidad del negocio protegiendo al sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto". (López, 2011, p. 23)

"Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la continuidad de las operaciones del negocio". (Gaspar, 2004, p. 205)

"Se cree que algunas empresas gastan hasta el 25 % de su presupuesto en proyectos de recuperación de desastre, sin embargo, esto lo hacen para evitar pérdidas más grandes. De las empresas que tenían una pérdida principal de registros automatizados el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años, y sólo el 6 % sobrevivirá a largo plazo" («Plan de recuperación ante desastres», 2015).
Revisadas y analizadas estas definiciones podemos manifestar que un DRP es parte fundamental de la continuidad del negocio, permitiendo a instituciones estar preparadas

para enfrentar a riesgos inesperados que pudieran afectar la disponibilidad de las operaciones tecnológicas, garantizando la permanencia del negocio en el tiempo.

2.2. Bases Teóricas

Para el desarrollo de este Trabajo de Investigación se utilizaron los siguientes conceptos básicos:

Gobierno de TI, es una metodología de trabajo, no una solución en sí. Está orientado a proveer las estructuras que unen los procesos de TI, recursos de TI e información con las estrategias y los objetivos de la empresa. Además, el Gobierno de TI integra e institucionaliza las mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoriza el rendimiento de TI para asegurar que la información de la empresa y las tecnologías relacionadas soportan los objetivos del negocio («QUE ES GOBIERNO TI? | Gobierno TI», s. f.).

DRP – Plan de Recuperación de Desastres, un DRP (*Disaster Recovery Plan*, o Plan de recuperación de desastres) es la estrategia que se seguirá para restablecer los servicios de TI (Hardware y Software) después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo, el cual atente contra la continuidad del negocio de manera significativa. Cuando las compañías no cuentan con un DRP implementado y se tiene una eventualidad, éstas lo tratan de recuperar a cualquier costo ya que dependen del funcionamiento de sus sistemas de información. («¿Qué es un DRP?», s. f.).

Plan de contingencia, es un instrumento de gestión que contiene las medidas (tecnológicas y humanas y de organización) que garanticen la continuidad del negocio protegiendo al sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.
El plan de contingencia consta de tres subplanes independientes:

- **Plan de respaldo**, ante una amenaza se aplican medidas preventivas para garantizar que se cuenta con la información histórica necesaria para evitar que se produzca un daño importante a la provisión de servicios que brinda la institución.

- **Plan de emergencia**, Contempla qué medidas tomar cuando se está materializando una amenaza o acaba de producirse y se requiere movilizar el personal y las operaciones a otro lugar para recuperar los servicios.
- **Plan de recuperación**, indica las medidas que se aplicarán cuando ha ocurrido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento de la organización y del sistema.

La elaboración del plan de contingencia no puede descuidar al personal de la organización que estará informado del plan y entrenado para actuar en las funciones que le hayan sido encomendadas en caso de producirse una amenaza o un impacto. (López, 2011, p. 23)

Plan de Recuperación de Desastres, es la denominación del proceso que permite de modo planificado, sistemático y organizado resguardar la capacidad de la empresa de proveer un nivel aceptable de servicios en la eventualidad de una falla grave, una emergencia o una contingencia que comprometa de modo significativo la continuidad de las operaciones («Plan de Continuidad del Negocio», s. f.).

Sistemas de información, son un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos, teniendo como elementos: recursos, equipo humano, información y actividades. (López, 2011, p. 8)

Sistema informático, está constituido de un conjunto de elementos físicos (hardware, dispositivos periféricos y conexiones), lógicos (sistemas operativos, aplicaciones) y con frecuencia se incluye también los elementos humanos (personal experto que maneja el software y el hardware) Un sistema informático puede ser un subconjunto del sistema de información, pero en principio un sistema de información no tiene por qué contener elementos informáticos. (López, 2011, p. 8)

Seguridad informática, es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable. (López, 2011, p. 9)

2.3. Estado del Arte

En la actualidad los DRP´s se están desarrollando bajo modelos y buenas prácticas internacionales tales como: ISO 22301:2012 y la Norma Británica BS-25999.

BS 25999-2.- Es una norma británica emitida en 2007 que rápidamente convirtió en la principal norma para gestión de la continuidad del negocio; aunque se trata de una norma nacional británica, se utiliza también en muchos otros países y se convirtió en la norma internacional ISO 22301. Igual que las normas ISO 27001, ISO 9001, ISO 14001 y otras normas que definen los sistemas de gestión, la BS 25999-2 también define un sistema de gestión de la continuidad del negocio que contiene las mismas cuatro fases de gestión: planificación, implementación, revisión y supervisión; y por último, mejora. El objetivo de estas cuatro fases es que el sistema se actualice y mejore permanentemente para que sea útil si se produjera un desastre. («¿Qué es norma BS 25999? | 27001Academy», s. f.)

Según revisiones de la norma se pudo evidenciar que se ha publicado en dos partes.

- BS 25999-1:2006 Parte 1: se trata de un documento orientativo que proporciona las recomendaciones prácticas para el BCM.(Villegas De La Cruz, Marcia Marina, 2013, p. 15)
- BS 25999-2:2007 Parte 2: establece los requisitos para un Sistema de Gestión de la Continuidad (BCM). Esta es la parte de la norma que se certifica a través de una etapa de implementación, de auditoría y posterior certificación. (Villegas De La Cruz, Marcia Marina, 2013, p. 15)

Los siguientes son procedimientos y documentos relevantes requeridos por la BS 25999-2:(«¿Qué es norma BS 25999? | 27001Academy», s. f.)

- Alcance del SGCN: área de la organización donde se aplicará la gestión de la continuidad del negocio.
- Política de GCN: definición de objetivos, responsabilidades, etc.
- Gestión de recursos humanos.
- Análisis de impactos en el negocio y evaluación de riesgos.
- Definición de estrategia de continuidad del negocio.
- Planes de continuidad del negocio.

- Mantenimiento de planes y sistemas (mejora continua).

La norma BS 25999-2 requiere los siguientes documentos: («¿Qué es norma BS 25999? | 27001Academy», s. f.)

- El alcance de GCN;
- La política de GCN;
- Responsabilidades específicas para la GCN;
- Procedimientos para gestionar documentos y registros y para medidas correctivas y preventivas;
- Metodología para el análisis de impactos en el negocio y resultados del análisis;
- Metodología de evaluación de riesgos;
- Estrategia de continuidad del negocio;
- Plan de Recuperación de Desastres que incluya planes de respuesta a los incidentes planes de recuperación;
- Registros.

2.3.1 ¿Qué es ISO 22301?

El nombre completo de esta norma es ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio – Requisitos. Esta norma fue redactada por los principales especialistas en el tema y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización. («¿Qué es norma ISO 22301? | 27001Academy», s. f.)

2.3.2 Relación con BS 25999-2

La ISO 22301 ha reemplazado a la 25999-2. Estas dos normas son bastante similares, pero la ISO 22301 puede ser considerada como una actualización de la BS 25999-2.(«Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

2.3.3 Beneficios de la continuidad del negocio

Si se implementa correctamente, la gestión de la continuidad del negocio disminuirá la posibilidad de ocurrencia de un incidente disruptivo y, en caso de producirse, la

organización estará preparada para responder en forma adecuada y, de esa forma, reducir drásticamente el daño potencial de ese incidente.

¿Quién puede implementar esta norma?

La norma está concebida de tal forma que es aplicable a cualquier tamaño o tipo de organización. Un sistema de gestión de la continuidad del negocio (BCMS) alineado con la norma ISO 22301 es adecuado para cualquier organización de cualquier tamaño, grande o pequeña, en todos los sectores, desde públicas a privadas, manufactura y servicios, con o sin fines de lucro. Además, proporciona un lenguaje común para las organizaciones globales.(«Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

¿Cómo encaja la continuidad del negocio en la gestión general?

La continuidad del negocio es parte de la gestión general del riesgo en una compañía y tiene áreas superpuestas con la gestión de seguridad y tecnología de la información.(«Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

Figura 1-2: Gestión del Riesgo
FUENTE: http://advisera.com/27001academy/es/que-es-iso-22301/

ISO 22301 es el nuevo estándar internacional para la Gestión de la Continuidad del Negocio. Ha sido creada en respuesta a un fuerte interés internacional en el estándar británico BS 25999-2 y otros estándares regionales. La ISO 22301 identifica los

fundamentos de un sistema de gestión de la continuidad estableciendo el proceso, los principios y la terminología de la gestión de la continuidad del negocio. Este estándar proporciona una base para entender, desarrollar e implementar la continuidad del negocio dentro de la organización y genera confianza en la relación business-to-business y business-to-customer, asegurando a las partes interesadas que la empresa está totalmente preparada y puede cumplir con los requisitos internos, reglamentarios y del cliente. Esta norma proporciona a las organizaciones un marco para garantizar que puedan seguir operando durante las circunstancias más difíciles e inesperadas protegiendo a su personal, preservando su reputación y ofreciendo la capacidad de seguir operando. Es particularmente relevante para las organizaciones que operan en entornos de alto riesgo donde la capacidad de seguir operando es de suma importancia para los negocios, clientes y partes interesadas, incluyendo servicios públicos, finanzas, telecomunicaciones, transporte y sector público.(«Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

En el caso de las Cooperativas de Ahorro y Crédito, la normativa que les rige exige garantizar la provisión ininterrumpida de los servicios, especialmente los relacionados con el cumplimiento de sus obligaciones, como es la devolución de los ahorros y pago de obligaciones a terceros, por lo que la continuidad juega un papel relevante en la supervivencia de la institución.

Términos básicos utilizados en la norma ISO 22301: («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

- Sistema de gestión de la continuidad del negocio (SGCN): parte del sistema general de gestión que se encarga de planificar, mantener y mejorar continuamente la continuidad del negocio. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Interrupción máxima aceptable (MAO): cantidad máxima de tiempo que puede estar interrumpida una actividad sin incurrir en un daño inaceptable (también Período máximo tolerable de interrupción [MTPD]). («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Objetivo de tiempo de recuperación: tiempo predeterminado que indica cuándo se debe reanudar una actividad o se deben recuperar recursos. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

- Objetivo de punto de recuperación (RPO): pérdida máxima de datos; es decir, la cantidad mínima de datos que necesita ser restablecida. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Objetivo mínimo para la continuidad del negocio (MBCO): nivel mínimo de servicios o productos que necesita suministrar o producir una organización una vez que restablece sus operaciones comerciales. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

2.3.4 Beneficios de la norma ISO 22301:

Los beneficios que la ISO 22301 trae son muchos, e incluyen:(«Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

- Maximizar la calidad y eficiencia: Proporciona un marco común y coherente, basado en las mejores prácticas internacionales que le permite maximizar la calidad y eficiencia de sus procesos. Esto incluye la metodología Planear, Hacer, Verificar, Actuar para la continuidad del negocio. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Resiliencia: Ya sea un desastre internacional o perturbación local, su organización será lo suficientemente fuerte para recuperar su operación rápidamente ó reducir al mínimo la interrupción hasta que el servicio se reanude. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Reputación: Mantenga segura su reputación. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Ventaja competitiva: Abre nuevas oportunidades de mercado y ayuda a ganar nuevos negocios. Obtenga la confianza del cliente a través estándares ISO de aceptación universal que abren oportunidades globales. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Gane más contratos con costos más efectivos: Provee una herramienta de marketing que junto con la certificación le ayuda a reducir el costo de la licitación. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Mejora del negocio: La certificación requiere de un claro entendimiento de su organización lo cual le ayudará a identificar oportunidades de mejora. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

- Mejora continua: El proceso de certificación involucra auditorías continuas que garantizan que su sistema de gestión está siendo actualizado. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Cumplimiento: Demuestra que cumple con los requisitos de leyes y regulaciones aplicables. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Ahorro de Costos: Tendrá la oportunidad de reducir la carga de las auditorías interna y externa de BCM, mejorar el rendimiento financiero y de negocios al reducir las primas de seguros de interrupción. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Entrega: El marco de su BCMS soporta los procesos de gestión que le permiten proporcionar un nivel acordado de los servicios críticos y de los productos en un plazo determinado después de la interrupción. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)
- Gestión: Un BCMS proporciona la capacidad de gestión demostrada durante los tiempos de interrupción. («Norma ISO 22301, Continuidad del Negocio - G4A», s. f.)

Las clausulas principales de la norma ISO 22301 son:

- Clausula 4.- Contexto de la organización
- Clausula 5.- Liderazgo
- Clausula 6.- Planificación
- Clausula 7.- Soporte
- Clausula 8.- Operación
- Clausula 9.- Evaluación del desempeño
- Clausula 10.- Mejora

El BCMS, como cualquier otro sistema de gestión, tiene los siguientes componentes:

- Política
- Responsabilidades definidas
- Procesos de gestión relacionados con la política, planificación, implantación, la operativa, valoración del rendimiento, revisión de la gestión y mejora continua.
- Documentación que suministre evidencias auditables

Tabla 1-2 Estructura de la ISO 22301 (Clausulas)

Introduction	**5 Leadership**	**8 Operation**
0.1 General	5.1 General	8.1 Operational planning and control
0.2 The Plan-Do-Check-Act (PDCA) model	5.2 Management commitment	8.2 Business impact analysis and risk assessment
0.3 Components of PDCA in this International Standard	5.3 Policy	8.3 Business continuity strategy
1 Scope	5.4 Organizational roles, responsibilities and authorities	8.4 Establish and implement business continuity procedures
2 Normative references	**6 Planning**	8.5 Exercising and testing
3 Terms and definitions	6.1 Actions to address risks and opportunities	**9 Performance evaluation**
4 Context of the organization	6.2 Business continuity objectives and plans to achieve them	9.1 Monitoring, measurement, analysis and evaluation
4.1 Understanding of the organization and its context	**7 Support**	9.2 Internal audit
4.2 Understanding the needs and expectations of interested parties	7.1 Resources	9.3 Management review
4.3 Determining the scope of the management system	7.2 Competence	**10 Improvement**
4.4 Business continuity management system	7.3 Awareness	10.1 Nonconformity and corrective action
	7.4 Communication	10.2 Continual improvement
	7.5 Documented information	Bibliography

Realizado por: Washington Vásquez, 2017

2.3.5 El ciclo PLAN-DO-CHECK-ACT (PDCA)

El estándar aplica el ciclo de Plan-Do-Check-Act a la planeación, establecimiento, implementación, operación, monitoreo, revisión, ejercicios, mantenimiento y mejoramiento continuo de la efectividad del SGCN de una organización.

En la siguiente figura se ilustra como un SGCN tomó requerimientos de insumos de "partes interesadas" para la gestión de continuidad y a través de las necesarias acciones y procesos, produce resultados de continuidad que satisfacen los requerimientos.

Figura 2-2: Ciclo PDCA Aplicado al Proceso de Continuidad del negocio

FUENTE: https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

2.4 Normativa

La normativa es todo el cuerpo legal que en el marco de su jurisdicción es aplicable para cada organización de acuerdo a su actividad y lugar donde desarrollan sus actividades. A continuación se cita la normativa relacionada con la Continuidad del Negocio, en su contexto de gestión de riesgos.

Constitución de la República del Ecuador

La Constitución de la República del Ecuador establece en su Título VII Régimen Del Buen Vivir, Capítulo Primero Inclusión y Equidad, Sección Novena, Gestión del Riesgo, que:

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través de organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
2. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.
4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.
5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.
6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidad es y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.
7. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

(Asamblea Nacional Constituyente, 2008)

Así queda evidenciado que por mandato Constitucional las Organizaciones públicas y privadas deben gestionar los riesgos mediante la implementación de planes de continuidad del negocio para la recuperación de sus actividades en caso de interrupciones, que provoquen paralizaciones de los servicios institucionales y que afecte a las personas, las colectividades y la naturaleza.

Marco Regulatorio

La Junta Bancaria ha emitido las siguientes Resoluciones, que norman la Gestión de Riesgos Integrales de las entidades bajo control de la Superintendencia de Bancos y Seguros y posteriormente bajo la Superintendencia de Economía Popular y Solidaria, como marco normativo que rige el presente Plan de titulación.

- Ley General de Instituciones de Sistema Financiero
- Resolución No JB-2002-429 de 22 de enero del 2002
- Resolución No JB-2002-431 de 22 de enero del 2002
- Resolución No JB-2003-602 de 9 de diciembre del 2003
- Resolución No JB-2004-631 de 22 de enero del 2004
- Resolución No JB-2005-834 de 20 de octubre del 2005
- Resolución No JB-2010-1767 de 21 de julio del 2010
- Resolución No JB-2014-3066 de 2 de septiembre del 2014

La normativa citada establece las siguientes responsabilidades sobre la Gestión de Riesgos:

ARTICULO 1.- Las instituciones del sistema financiero controladas por la Superintendencia de Bancos y Seguros, deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme su objeto social, sin perjuicio del cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales y/o particulares. La administración integral de riesgos es parte de la estrategia institucional y del proceso de toma de decisiones. . (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014a, p. 560)

La cooperativa tiene la responsabilidad de administrar sus riesgos, a cuyo efecto debe *contar con procesos formales de administración integral de riesgos que permitan identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgo que está asumiendo*. La institución tiene su propio perfil de riesgo, según sus actividades y circunstancias específicas; por tanto, al no existir un esquema único de administración integral de riesgos, deberá desarrollar el suyo propio. (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014a, p. 562)

La identificación del riesgo es un proceso continuo y se dirige a reconocer y entender los riesgos existentes en cada operación efectuada, y así mismo, a aquellos que pueden surgir de iniciativas de negocios nuevos. Las políticas y estrategias de la Cooperativa deben definir el nivel de riesgo considerado como aceptable; este nivel se manifiesta en límites de riesgo puestos en práctica a través de políticas, normas, procesos y procedimientos que establecen la responsabilidad y la autoridad para fijar esos límites, los cuales pueden ajustarse si cambian las condiciones o las tolerancias de riesgo. Además, deben contar con procedimientos para autorizar excepciones o cambios a los límites de riesgo, cuando sea necesario. (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014a, p. 562)

CAPÍTULO III

3 METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Diseño de la investigación

El diseño de la presente investigación es del tipo Cuasi-Experimental ya que se escoge la metodología que será utilizada como base para la creación del nuevo método DRP, partimos de la descripción del problema, las exigencias de los organismos de control para las Cooperativas de Ahorro y Crédito en el Ecuador y su necesidad que son de aplicación inmediata sin necesidad de someterla a pruebas, además los datos de prueba son generados por el autor de esta investigación.

3.2 Tipo de investigación

Para el presente trabajo de investigación se lo realizo mediante una investigación descriptiva y aplicada, ya que se basa en experiencia y conocimientos existentes para realizar un método que ayude a las instituciones financieras a estar preparados ante incidentes no esperados que puedan provocar la paralización de sus operaciones.

3.3 Métodos

En la investigación se utiliza el método científico ya que se refiere a la serie de etapas que hay que recorrer para obtener un conocimiento válido desde el punto de vista científico, utilizando para esto instrumentos que resulten fiables, el cual consta de las siguientes etapas:

- Planteamiento del problema
- Formulación de la hipótesis
- Levantamiento de la información
- Análisis e interpretación de resultados

- Comprobación de la hipótesis
- Difusión de resultados

3.3.1 Método Inductivo

Partiendo de la teoría explicativa de la problemática, este método nos permite alcanzar los beneficios que constituye para la Cooperativa de Ahorro y Crédito "San José Ltda." el cumplimiento de la normativa a través del Método de Recuperación de Desastres, con un análisis y evaluación de los riesgos.

3.3.2 Método Deductivo

Analizando los riesgos que puede provocar en una institución financiera el paralizar sus actividades por incidentes no esperados, se tratará de encontrar un método adecuado para mitigar y garantizar su continuidad de las operaciones.

3.3.3 Método Analítico

Se explora a fondo los aspectos básicos y las relaciones fundamentales que se manifiestan en el progreso de la investigación, lo que permite comprender, conocer y demostrar las causas y efectos que originan el problema. (Villegas De La Cruz, Marcia Marina, 2013, p. 51)

3.3.4 Método Sintético

Una vez observados los aspectos teóricos, se puede realizar síntesis explicativas de la información recopilada y procesada a través de la redacción de las políticas, estrategias y procedimientos para la continuidad del negocio. (Villegas De La Cruz, Marcia Marina, 2013, p. 51)

3.3.5 Método Empírico

Se analiza las vivencias y experiencias de personas involucradas en esta investigación. (Villegas De La Cruz, Marcia Marina, 2013, p. 52)

3.4 Técnicas

Las técnicas que serán utilizadas son las proporcionadas por la investigación científica para recolección de datos, siendo:

3.4.1 Entrevistas

Se basa en la formulación de preguntas que la aplicamos a funcionarios y empleados de las áreas de Tecnología de la Información y Riesgos de la Cooperativa.

3.4.2 Opinión de Expertos

Es una técnica que obtiene el criterio de una persona reconocida como una fuente confiable de un tema, cuya capacidad para juzgar o decidir en forma correcta, y justa le confiere autoridad por sus pares o por el público en una materia especifica. (Villegas De La Cruz, Marcia Marina, 2013, p. 52)

3.4.3 Bibliografía

La información se obtiene mediante la lectura científica de los textos, documentos, manuales, revistas, acudiendo a las bibliotecas. (Villegas De La Cruz, Marcia Marina, 2013, p. 52)

3.4.4 Observación Directa

La información se la obtiene mediante la observación al desarrollo de ciertos procesos especialmente los relacionados a la cadena de valor, al momento de ocurrir eventos de riesgo. (Villegas De La Cruz, Marcia Marina, 2013, p. 53)

3.5 Fuentes de información

Las principales fuentes que serán utilizadas en el estudio de investigación serán:

3.5.1 Primaria

- Pruebas
- Observación de resultados

3.5.2 Secundaria

- Tesis realizadas internacionales y nacionales de cuarto nivel.
- Trabajos de investigaciones internacionales y nacionales.
- Artículos científicos en base de datos de bibliotecas virtuales.
- Libros especializados en la biblioteca y electrónicos.
- Diccionarios especializados.
- Conferencias académicas, congresos, seminarios.
- Revistas indexadas y no indexadas publicadas de prestigio.
- Revistas electrónicas.

Páginas de internet que brinden información confiable.

3.6 Recursos

3.6.1 Recursos humanos

Dentro la parte humana interviene:

- Ejecutor de tesis
- El Tutor
- Los Miembros
- Proveedores de Equipos
-

3.6.2 Recursos técnicos

Los recursos técnicos que se utilizarán en la investigación son:

3.6.3 Recurso Hardware

Se utilizará el siguiente equipo hardware:

- Modelo: TOS. S55-B5203SL
- Procesador: Intel® Core™ i7-4510U
- Memoria: 8,00 GB DDR3L 1600
- Disco Duro: 1TB (5400 RPM) Serial ATA

3.6.4 Recursos materiales y suministros

Los recursos materiales y suministros que se utilizarán son:

- Resmas de papel
- Empastado de tesis
- Copias
- Flash Memory
- Caja de CD’s
- Carpeta colgante
- Carpetas de cartón
- Botellas de tinta para Epson
- Artículos varios de oficina
- Internet
- Transporte
- Energía eléctrica

3.7 Planteamiento de la hipótesis

El método propuesto para el Plan de Recuperación de Desastres permitirá reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.

3.8 Definición de Variables

Variable Dependiente:

Reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.

Variable Independiente:

Método propuesto para el Plan de Recuperación de Desastres.

3.8.1 Operacionalización conceptual

Tabla 1-3 Operacionalización de variables.

VARIABLES	TIPO	CONCEPTO
Reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.	Variable Dependiente	Garantizar la continuidad de las operaciones mitigando el riego operativo
Método propuesto para el Plan de Recuperación de Desastres.	Variable Independiente	Son los pasos a seguir para restablecer los servicios de TI después de haber un incidente informático no esperado.

Realizado por: Washington Vásquez, 2017

Tabla 2-3 Factores de Riesgo que afectan la continuidad del negocio.

Definición Operativa	Dimensiones	Indicadores	Índices de Medición
	Procesos	➢ Gobernantes ➢ Cadena de Valor ➢ De apoyo	Cuali- cuantitativo Cuali- cuantitativo Cuali- cuantitativo
Factores cuya	Personas	➢ Incorporación	Cuali- cuantitativo

defectuosa aplicación pueden provocar la paralización de las operaciones en el giro normal del negocio		➢ Permanencia ➢ Desvinculación	Cuali- cuantitativo Cuali- cuantitativo
	Tecnología de la Información	➢ Plan de Contingencias ➢ Plan Reanudación ➢ Plan de Recuperación	Cualitativo Cualitativo Cualitativo
	Eventos Externos	➢ Desastres naturales ➢ Daños accidentales ➢ Ataques Intencionados ➢ Ataques Intencionados de origen remoto	Cuali- cuantitativo Cuali- cuantitativo Cuali- cuantitativo Cuali- cuantitativo

Realizado por: Washington Vásquez, 2017

Tabla 3-3 Desarrollar el método para la implementación del DRP.

Definición Operativa	Dimensiones	Indicadores	Índices de Medición
	Estrategia de la continuidad del negocio.	➢ Talento Humano ➢ Recurso Tecnológico ➢ Comunicaciones ➢ Infraestructura	Cualitativo Cualitativo Cualitativo Cualitativo
Son un conjunto de tareas orientadas a asegurar la continuidad de las operaciones, la	Análisis de Impacto del Negocio (BIA)	➢ Identificación Procesos Críticos. ➢ Fallas en Tecnología de	Cualitativo Cuali – cuantitativo

satisfacción del cliente y la productividad a pesar de eventos imprevistos.		Información ➢ Escenarios de Contingencia. ➢ Valoración de Riesgos ➢ Escenarios de mayor impacto	Cualitativo Cuantitativo Cuali-cuantitativo
	Desarrollo del Plan de Recuperación de Desastres	➢ Procedimientos del Antes, Durante y Después ➢ Documentación del Plan ➢ Pruebas del Plan	Cualitativo Cualitativo Cualitativo

Realizado por: Washington Vásquez, 2017

3.9 Población y muestra

La población de donde se pudo obtener la información para el desarrollo del proyecto de investigación fue con el personal de Tecnología de la Información 10 personas, Riesgos 5 personas de la Cooperativa de Ahorro y Crédito "San José Ltda.".

3.10 Proceso para construir la propuesta

Desarrollar un método para un Plan de Recuperación de Desastres en la Cooperativa de Ahorro y Crédito "San José Ltda." Es la derivación del estudio a través del manejo de un método científico y se encamina en los siguientes pasos (Villegas De La Cruz, Marcia Marina, 2013, p. 54):

- Análisis de los resultados del diagnóstico realizado a la Cooperativa de Ahorro y Crédito "San José Ltda.", en base a la normativa JB-2014-3066 emitida por la Superintendencia de Bancos para la gestión del riesgo operativo, y consignados a manera de antecedentes en el documento de la propuesta, (Villegas De La Cruz, Marcia Marina, 2013, p. 54)

- Justificación de la propuesta determinando los alcances, directrices y razones, (Villegas De La Cruz, Marcia Marina, 2013, p. 54)
- Identificar a los beneficiarios de la propuesta, (Villegas De La Cruz, Marcia Marina, 2013, p. 54)
- Diseño Técnico de la propuesta que consiste en el desarrollo mismo de la propuesta, (Villegas De La Cruz, Marcia Marina, 2013, p. 54)
- Diseño administrativo de la propuesta: Se define tiempos, recursos, personas, acciones, formas de seguimiento, que se desarrollan una vez que la propuesta técnica haya sido concluida y llevada a la práctica. (Villegas De La Cruz, Marcia Marina, 2013, p. 54)
- Determinación de impactos: precisa los impactos que la propuesta genera en las personas, grupos, instituciones y en la sociedad, además del señalamiento de los impactos en las actividades económicas sociales, (Villegas De La Cruz, Marcia Marina, 2013, p. 54)
- Evaluación: consiste en indicar que momentos, que estrategias de evaluación se utilizan para determinar las bondades o limitaciones de la propuesta. (Villegas De La Cruz, Marcia Marina, 2013, p. 54)

  Se cumple con el objetivo del proyecto de definir un método para elaborar un Plan de Recuperación de Desastres en Cooperativas de Ahorro y Crédito, y se formula una solución integrando los componentes impartidos en las normas técnicas de redacción y los requerimientos de la Escuela Superior Politécnica de Chimborazo y del Instituto de Post Grado. (Villegas De La Cruz, Marcia Marina, 2013, p. 54)

3.11 Valor práctico de la investigación

El presente trabajo de investigación tiene una gran importancia practica debido a que la implementación del Plan de Recuperación de Desastres es imprescindible, porque ayuda a disminuir el impacto negativo que provoca el no estar preparados ante posibles eventos de riesgo que produzcan la paralización de las actividades en la Cooperativa y por consiguiente pérdidas económicas y hasta humanas, además nos permite proteger los intereses de los socios y clientes, generando una confianza y seguridad en la Institución. También estamos asegurando el cumplimiento de normativas vigentes por los organismos de control. (Villegas De La Cruz, Marcia Marina, 2013, p. 55)

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

Definición del DRP para la Unidad de Tecnología de la Información de la Cooperativa de Ahorro y Crédito San Jose Ltda.

Una vez que se cuenta con el método para el desarrollo de un Plan de Recuperación de Desastres que permita a las Cooperativas de Ahorro y Crédito satisfacer sus necesidades de continuidad del negocio y dar cumplimiento a la normativa vigente. Se realizó un plan piloto para demostrar la hipótesis planteada en esta investigación en la Cooperativa de Ahorro y Crédito San José Ltda. A continuación, se presentan los resultados de la aplicación del método desarrollado, partiendo de los antecedentes y necesidades específicas. Para lo cual se realizó un análisis de riesgo, utilizando un método cualitativo con el cual se demuestra que el nivel de riesgo baja luego de aplicado el plan.

4.1 Análisis de la situación actual.

En la presente encuesta se han realizado las siguientes preguntas basadas en la normativa de Riesgo operativo emitida por la Superintendencia de Bancos y Seguros.

Tabla 1-4: Preguntas de la Encuesta.

Preguntas realizadas en base a la Normativa
PLAN DE CONTINUIDAD DEL NEGOCIO.- ¿La entidad ha definido un proceso formal para la administración de la continuidad del negocio que permita mantener activa sus operaciones esenciales en caso de desastres?
Ha establecido un proceso permanente de administración de la continuidad del negocio.
Ha efectuado un análisis de impacto al negocio (BIA)
Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los

procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.
Ha definido un plan de continuidad del negocio, y éste se encuentra formalizado, difundido e implementado.
Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.
PLAN DE RECUPERACIÓN DE DESASTRES. ¿La entidad ha definido un plan de recuperación de desastres (DRP) que permita garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de interrupciones severas del negocio?
El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.
El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.
El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.
El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.
El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.

Realizado por: Washington Vásquez, 2017

Dichas preguntas se las realizo vía encuesta al personal de la Cooperativa San Jose de las áreas de Sistemas y Riesgos ver anexo L donde se obtuvieron los siguientes resultados.

Tabla 2-4: Respuestas de las Encuestas

Número	PREGUNTAS	RESPUESTA	
		SI	NO
1	Ha establecido un proceso permanente de administración de la continuidad del negocio.	6	9
2	Ha efectuado un análisis de impacto al negocio (BIA)	4	11
3	Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.	5	10
4	Ha definido un plan de continuidad del negocio, y éste se encuentra formalizado, difundido e implementado.	5	10
5	Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.	3	12
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	0	15
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	0	15
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	0	15
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	0	15
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que	0	15

	permitan comprobar su aplicabilidad y realizar los ajustes necesarios.		

Realizado por: Washington Vásquez, 2017

La encuesta realizada, establece la probabilidad de ocurrencia de un riesgo, determinado en función del promedio de las respuestas obtenidas de la encuesta, a las preguntas realizadas para la evaluación de cada riesgo, el cálculo de la probabilidad de ocurrencia del riesgo es:

$$\text{Probabilidad} = \frac{\text{Promedio de Respuestas negativas}}{\text{Total de la población encuestada}}$$

Total población encuestada: 15

Donde se obtienen los siguientes resultados de las preguntas, agrupadas por las amenazas:

Tabla 3-4: Probabilidad de ocurrencia de los riesgos.

ITEM	AMENAZAS	PROMEDIOS		PROBABILIDAD
		SI	NO	
1	Ha establecido un proceso permanente de administración de la continuidad del negocio.	6	9	0.60
2	Ha efectuado un análisis de impacto al negocio (BIA)	4	11	0.73
3	Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.	5	10	0.67
4	Ha definido un plan de continuidad del negocio, y éste se encuentra formalizado, difundido e implementado.	5	10	0.67
5	Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su	3	12	0.80

	aplicabilidad y hacer los ajustes necesarios.			
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	0	15	1.00
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	0	15	1.00
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	0	15	1.00
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	0	15	1.00
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	0	15	1.00

Realizado por: Washington Vásquez, 2017

Se procede a obtener la ponderación de ocurrencia, para lo cual evaluamos el impacto de acuerdo a la **tabla 17-4 (escala para materialidad del impacto)** donde se presenta la categorización de impacto definida para los riesgos evaluados de acuerdo a la escala definida anteriormente, donde se obtienen los siguientes resultados.

Tabla 4-4: Ponderación de ocurrencia de los riesgos

ITEM	AMENAZAS	PROBABILIDAD	IMPACTO	PONDERANCIA
1	Ha establecido un proceso permanente de administración de la continuidad del negocio.	0.60	4	2.40
2	Ha efectuado un análisis de impacto al negocio (BIA)	0.73	3	2.20
3	Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.	0.67	4	2.67
4	Ha definido un plan de continuidad del negocio, y éste se encuentra formalizado, difundido e implementado.	0.67	4	2.67
5	Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.	0.80	2	1.60
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	1.00	4	4.00
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	1.00	4	4.00
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del	1.00	4	4.00

	plan de continuidad.			
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	1.00	4	4.00
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	1.00	4	4.00

Realizado por: Washington Vásquez, 2017

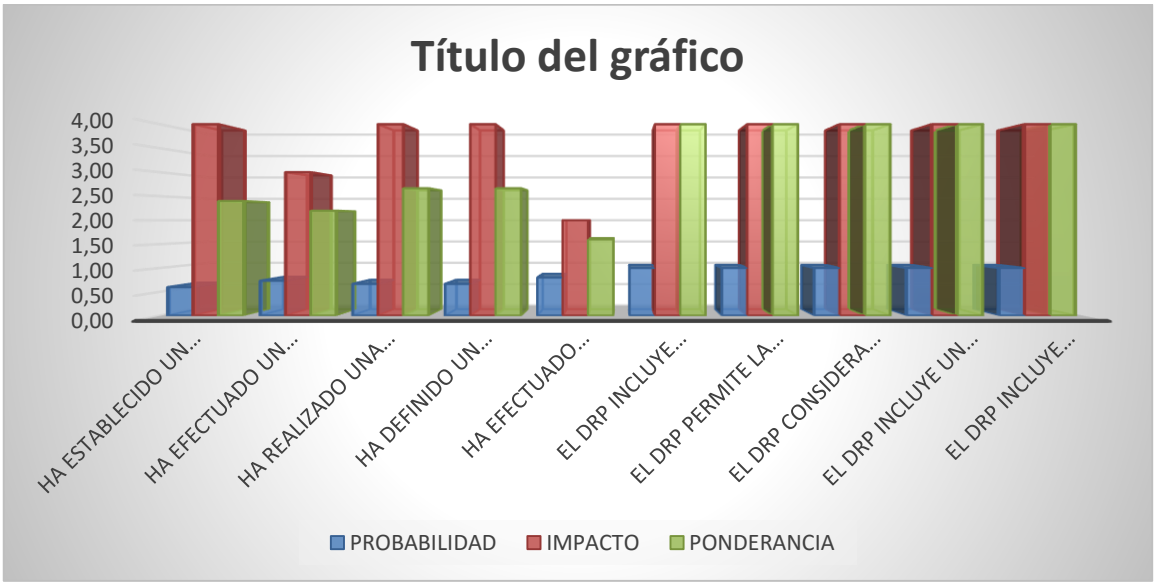

Gráfico 1-4: Ponderación de riesgos
Realizado por: Washington Vasquez, 2017.

Revisando los datos de la tabla anterior en el promedio de la ponderancia es de 3.15 por lo que se debe establecer que los riesgos de ponderación superior a los 3.15 son considerados los más críticos, a los que debemos prestar mayor atención.

Tabla 5-4: Riesgos de mayor ponderación

ITEM	AMENAZAS	PROBABILIDAD	IMPACTO	PONDERANCIA
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	1.0	4	4.00
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	1.0	4	4.00
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	1.0	4	4.00
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	1.0	4	4.00
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	1.0	4	4.00

Realizado por: Washington Vásquez, 2017

Como podemos observar en esta institución no se cuenta con ningún proceso en lo relacionado a DRP, por tal razón con este trabajo de investigación se pretende ayudar a precautelar la información y garantizar la continuidad del negocio.

4.2 Análisis de la situación Post-Implementación.

Una vez implementados los procedimientos obtenidos del método realizado en base a la norma ISO 22301 se aplicó nuevamente la misma encuesta que se hizo el análisis inicial, siguiendo la misma metodología de análisis, de lo cual se obtuvo los siguientes resultados:

Donde se han obtenido los siguientes resultados:

Tabla 6-4: Datos de respuestas Post-Implementación.

Número	PREGUNTAS	RESPUESTA	
		SI	NO
1	Ha establecido un proceso permanente de administración de la continuidad del negocio.	12	3
2	Ha efectuado un análisis de impacto al negocio (BIA)	11	4
3	Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.	10	5
4	Ha definido un plan de continuidad del negocio, y éste se encuentra formalizado, difundido e implementado.	10	5
5	Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.	9	6
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	14	1
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	12	3
8	El DRP considera procedimientos formales de respaldo para los	12	3

	programas, datos y documentación necesarios para la ejecución del plan de continuidad.		
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	13	2
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	15	0

Realizado por: Washington Vásquez, 2017

Tabla 7-4: Probabilidad de ocurrencia de los riesgos Post-Implementación.

ITEM	AMENAZAS	PROMEDIO		PROBABILIDAD
		SI	NO	
1	Ha establecido un proceso permanente de administración de la continuidad del negocio.	12	3	0.20
2	Ha efectuado un análisis de impacto al negocio (BIA)	11	4	0.27
3	Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.	10	5	0.33
4	Ha definido un plan de continuidad del negocio, y éste se encuentra formalizado, difundido e implementado.	10	5	0.33
5	Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.	9	6	0.40
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	14	1	0.07

7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	12	3	0.20
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	12	3	0.20
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	13	2	0.13
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	15	0	0.00

Realizado por: Washington Vásquez, 2017

Se procede a obtener la ponderación de ocurrencia.

Tabla 8-4: Ponderación de ocurrencia de los riesgos Post- Implementación

ITEM	AMENAZAS	PROBABILIDAD	IMPACTO	PONDERACION
1	Ha establecido un proceso permanente de administración de la continuidad del negocio.	0.20	4	0.80
2	Ha efectuado un análisis de impacto al negocio (BIA)	0.27	3	0.80
3	Ha realizado una identificación, análisis y evaluación de los riesgos a los que se encuentra expuesta la entidad en el desarrollo de sus negocios y operaciones por los procesos, personas, tecnología de información y los eventos externos, tomando en cuenta el impacto y la probabilidad de que sucedan.	0.33	4	1.33
4	Ha definido un plan de continuidad del	0.33	4	1.33

	negocio, y éste se encuentra formalizado, difundido e implementado.			
5	Ha efectuado pruebas periódicas del plan y de los procesos implantados para verificar su aplicabilidad y hacer los ajustes necesarios.	0.40	2	0.80
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	0.07	4	0.27
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	0.20	4	0.80
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	0.20	4	0.80
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	0.13	4	0.53
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	0.00	4	0.00

Realizado por: Washington Vásquez, 2017

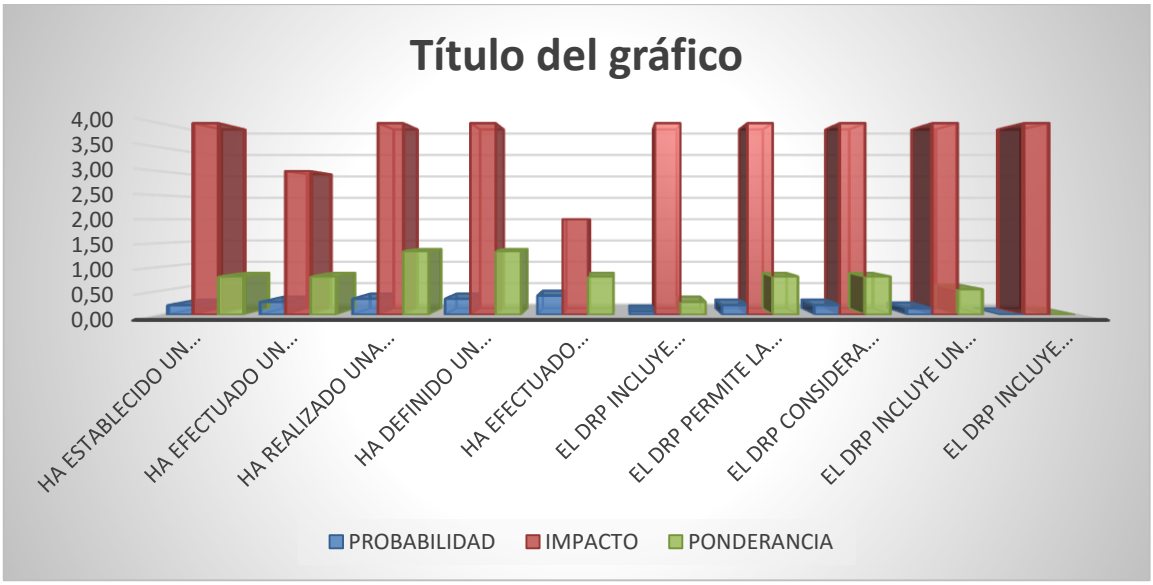

Gráfico 2-4: Ponderación de riesgos Post-Implementación
Realizado por: Washington Vásquez, 2017

Como podemos observar se puede establecer que los riesgos de ponderación superior a los 3.15 que se establecieron en la situación inicial han disminuido notablemente:

Tabla 9-4: Riesgos de Ponderación Inicial - Post-Implementación

ITEM	AMENAZAS	PONDERACION INICIAL	PONDERACION POST-IMPLEMENTACION
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	4.00	0.27
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	4.00	0.80
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del	4.00	0.80

	plan de continuidad.		
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	4.00	0.53
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	4.00	0.00

Realizado por: Washington Vásquez, 2017

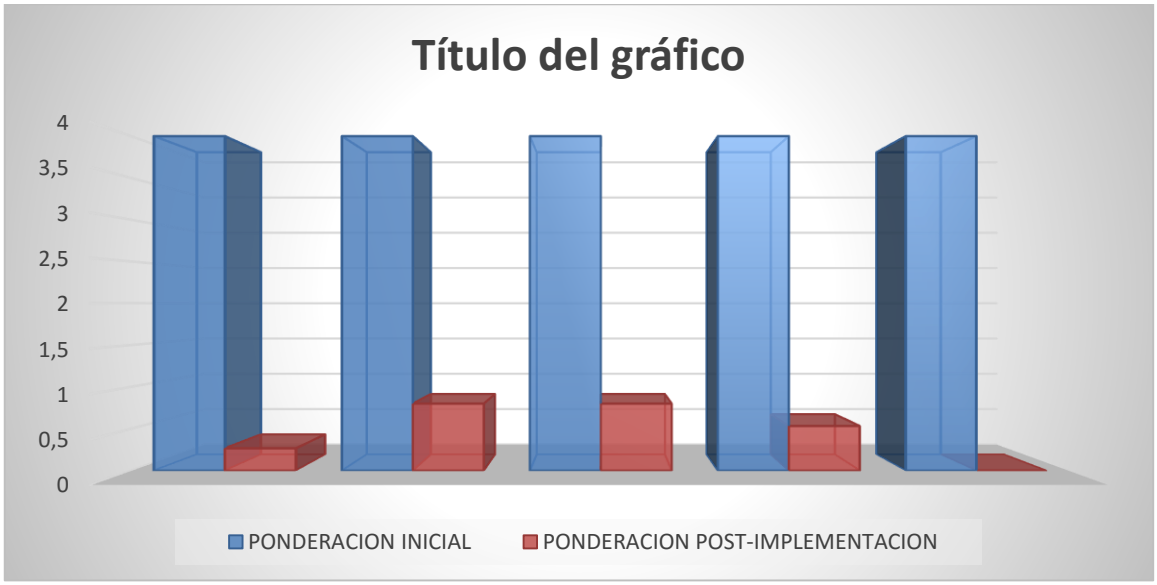

Gráfico 3-4: Ponderación de riesgos Inicial y Post-Implementación
Realizado por: Washington Vásquez, 2017

Expresamos la tabla en función de porcentaje.

Tabla 10-4: Porcentaje de la reducción de riesgo

ITEM	AMENAZAS	PONDERACION INICIAL	PONDERACION POST-IMPLEMENTACION	PORCENTAJE DE REDUCCION DE RIESGO
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	100.00 %	0.27%	99.73%
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	100.00 %	0.80%	99.20%
8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	100.00 %	0.80%	99.20%
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	100.00 %	0.53%	99.47%
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	100.00 %	0.00%	100.00%

Realizado por: Washington Vásquez, 2017

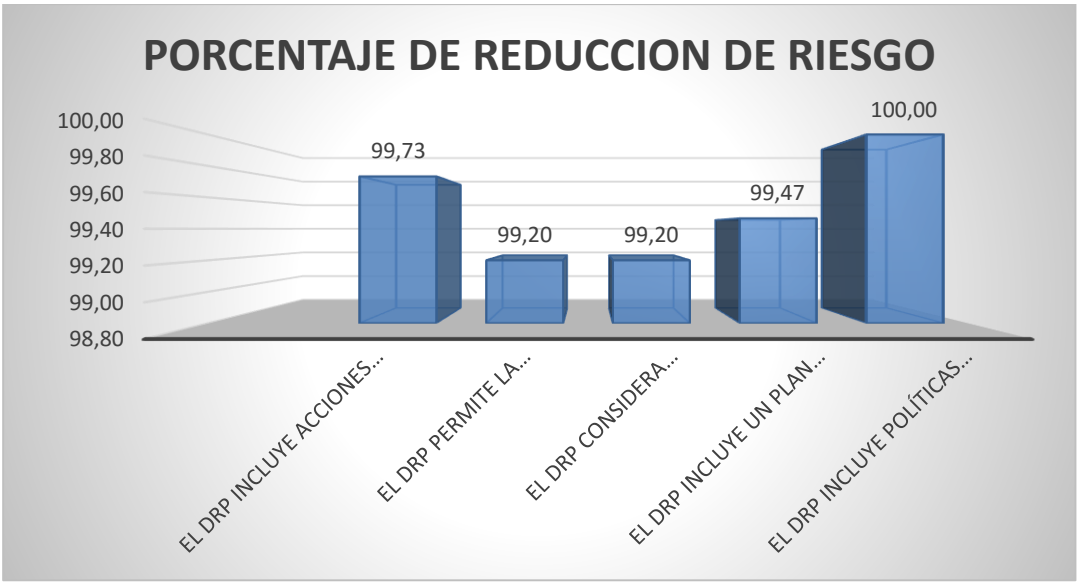

Gráfico 4-4: Porcentaje de reducción de riesgo
Realizado por: Washington Vásquez, 2017

Como se puede evidenciar en la ilustración, luego de haber aplicado el método, se ha reducido sustancialmente la ponderación de la probabilidad de que los riesgos frente a la situación inicial.

4.3 Comprobación de Hipótesis.

Una de las pruebas estadísticas es la prueba T de Student, que es cualquier prueba en la que el estadístico utilizado tiene una distribución T de Student si la hipótesis nula es cierta.

Se aplica cuando la población estudiada sigue una distribución normal pero el tamaño de la muestra es demasiado pequeño como para que el estadístico en el que está basada la inferencia esté normalmente distribuido, utilizándose una estimación de la desviación típica en lugar del valor real.

4.3.1 Planteamiento de la Hipótesis.

Hipótesis de investigación Hi: El método propuesto para el Plan de Recuperación de Desastres permitirá reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.

Hipótesis de Nula H_0: El método propuesto para el Plan de Recuperación de Desastres no permitirá reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.

$$H_o: \mu_{\bar{d}} = 0$$

Hipótesis Alternativa H_1: El método propuesto para el Plan de Recuperación de Desastres .
permitirá reducir el riesgo de afectaciones a la disponibilidad en los procesos críticos del negocio frente a incidentes informáticos no esperados.

$$H1: \mu_{\bar{d}} \neq 0$$

Donde$\mu_{\bar{d}}$ es la media de las medidas.

4.3.2 Nivel de significancia

Se debe elegir un nivel de significancia para la prueba que permite juzgar si los resultados de la prueba son estadísticamente significativos y también determina la probabilidad de error que es inherente a la prueba.
Para nuestra investigación se establece un nivel de significancia (denotado como α o alfa) de 0.05. Un nivel de significancia de 0.05 indica un riesgo de 5% de concluir que existe una diferencia cuando no hay una diferencia real.

$$\alpha = 0.05$$

4.3.3 Estadístico de prueba

En función de los datos obtenidos utilizamos la distribución T de Student, donde se establece que:

$$t_c = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}$$

$$S_d = \sqrt{\frac{\sum_{i=1}^{n}(d - \bar{d})^2}{n-1}}$$

Donde:

t_c = valor estadístico del procedimiento calculado.

$\bar{d}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después.

S_d = desviación estándar de las diferencias entre los momentos antes y después.

n = tamaño de la muestra.

4.3.4 Regla de decisión

Caso 1.

$$t_c > t_\alpha, rechaza\ la\ hipotesis\ nula\ H_0$$

Caso 2.

$$Valor\ p < \alpha, se\ rechaza\ la\ hipotesis\ nula\ H_0$$

4.3.5 Conclusiones

La data fue evaluada en la herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras empararejadas, de Microsoft Excel.

Normalidad

Para la prueba de Normalidad en la que se debe aceptar la hipótesis nula y se consideran todas las categorías de riesgos ponderadas según la siguiente tabla:

Tabla 11-4: Datos Iniciales y de Post-Implantación

ITEM	AMENAZAS	PONDERACION INICIAL	PONDERACION POST-IMPLEMENTACION
6	El DRP incluye acciones a ejecutar antes, durante y después de ocurrido el incidente, recursos necesarios así como los responsables de ejecutar cada actividad, procedimientos de capacitación y difusión al personal involucrado.	4.00	0.27
7	El DRP permite la reubicación de las operaciones en un nuevo lugar, es decir cuenta con una alternativa de recuperación en un sitio distinto a la ubicación física primaria.	4.00	0.80

8	El DRP considera procedimientos formales de respaldo para los programas, datos y documentación necesarios para la ejecución del plan de continuidad.	4.00	0.80
9	El DRP incluye un plan de restauración que permita regresar las operaciones a la normalidad en la instalación original recuperada o en una nueva.	4.00	0.53
10	El DRP incluye políticas y procedimientos para la realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios.	4.00	0.00

Realizado por: Washington Vásquez, 2017

Tabla 12-4: Resultados de la prueba t Student

	Variable 1	*Variable 2*
Media	4.0000	0.4800
Varianza	0.0000	0.12045
Observaciones	5.0000	5
Coeficiente de correlación de Pearson	#¡DIV/0!	
Diferencia hipotética de las medias	0.0000	
Grados de libertad	4.0000	
Estadístico t	22.6790	
P(T<=t) una cola	0.0000	
Valor crítico de t (una cola)	2.1318	
P(T<=t) dos colas	0.000022	
Valor crítico de t (dos colas)	2.7764	

Fuente: Herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras emparejadas.

Realizado por: Washington Vásquez, 2017

En promedio de los riesgos de amenazas inicial es 4,0000 mayor que los riesgos de amenaza post implementación igual 0,4800, hay una diferencia significativa. El valor de P, que es el nivel de significancia cuya valor es 0,000022, es menor que el valor

determinado para α = 0,05 por lo que nos lleva a rechazar la hipótesis nula H0 y aceptar la alternativa H1.

Con esto concluimos que la diferencia de las medias de los riesgos obtenidos con amenaza inicial y post-Implementación, son significativamente diferentes con un nivel de confianza del 95%.

4.4 Descripción de la Unidad de Tecnología de la Información de la COOPERATIVA DE AHORRO Y CREDITO SAN JOSE LTDA

La Unidad de Tecnología de la Información de la Cooperativa de Ahorro y Crédito San José Ltda., es un área de planificación y asesoría tecnológica diseñada para elaborar, evaluar y efectuar el seguimiento permanente del uso de los sistemas e ilustrar o recomendar a los usuarios su mejor aplicación y la administración de la Infraestructura Tecnológica.

4.4.1 Estructura orgánica de la Cooperativa de Ahorro y Crédito San José Ltda.

La estructura Orgánica funcional está elaborada en forma vertical, presentando las unidades divididas de arriba abajo a partir del titular, en la parte superior, y desagregan los diferentes niveles jerárquicos en forma escalonada, VER FIGURA 4.5.

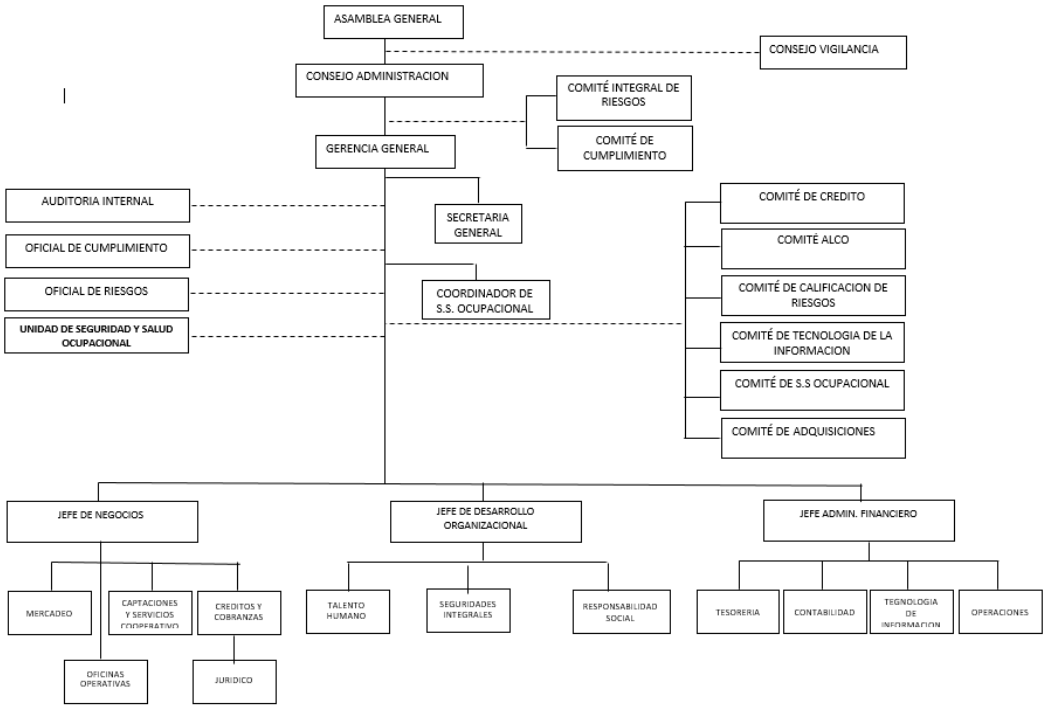

Figura 1-4 Organigrama Institucional
FUENTE: Cooperativa de Ahorro y Crédito San José Ltda.

4.4.2 Servicios Informáticos – Unidad de Tecnología

Este departamento se encuentra posicionado dentro del Orgánico funcional, como un área de asesoría al jefe administrativo financiero y Gerencia General, brindando la asesoría tecnológica alineada siempre a los objetivos institucionales.

4.4.5.1 Misión

Proveer a los departamentos, oficinas y usuarios en general las herramientas basadas en la tecnología para incrementar la productividad, agilizar los procedimientos y reducir los costos operacionales. A su vez debemos proveerles a los administradores la información actualizada y rápida para la toma de decisiones.

4.4.2.2. Productos

- Asesorar a los usuarios en el buen uso del equipo tecnológico y de los sistemas informáticos utilizados. (enviar periódicamente políticas de TI, y de buen uso de Hardware y Software)
- Instalar, configurar y dar mantenimiento a las computadoras asignadas a las oficinas operativas y corporativas.
- Colaborar con todas las áreas de la institución, en base a sus requerimientos y necesidades.
- Respaldar periódicamente la información de los sistemas utilizados de la cooperativa.
- Implementar proyectos de automatización en base a las necesidades de la institución.
- Proteger la confidencialidad y privacidad de la información de la institución almacenada en los sistemas utilizados.
- Establecer mecanismos de seguridad para salvaguardar la información almacenada en los sistemas.
- Tener personal de tecnología capacitado para ofrecer un mejor servicio.
- Desarrollar proyectos y aplicaciones para mejorar los procesos de la Cooperativa.
- Servir de apoyo y asesoramiento técnico a los departamentos, oficinas y usuarios en general.
- Automatizar los procesos dentro de la cooperativa, con la finalidad de proporcionar un soporte eficiente a los asociados y entes involucrados con los procesos (Clientes Internos).
- Involucrar a la Cooperativa en un ambiente competitivo dentro del contexto financiero presentando alternativas de seguridad y fiabilidad en las transacciones y créditos requeridos.
- Mejorar la integración de Sistemas y Subsistemas, etc.
- Posibilidad de agregar datos de distintas formas que sean útiles para la planificación y la toma de decisiones.
- Mejorar las posibilidades de mantener una continua monitorización de los procesos y los recursos disponibles.
- Mantenimiento de registros completos y sistemáticos.
- Beneficios de las contribuciones a la posibilidad de reestructuración del sistema.

- Reducción de la necesidad de trabajo forzado en el control de procesos y de recursos.
- Mejora en la seguridad en el almacenamiento y portabilidad de registros.

4.4.2.3 Estructura Orgánica de la Unidad de Tecnología de la Información de la Cooperativa de Ahorro y Crédito San José Ltda.

La Unidad de tecnología consta de una pequeña estructura jerárquica de 3 departamentos básicos (Analista de tecnología mantenimiento/desarrollo, Analista de tecnología proyectos/desarrollo y Analista de tecnología Help Desk), los cuales son responsables del cumplimiento de las políticas y procedimientos vigentes, y de proceder con la ejecución de proyectos a corto y largo plazo, de acuerdo a las disposiciones de la Gerencia General y del Comité de Tecnología en pro del avance tecnológico de la cooperativa, dependen de un Administrador de Tecnología quien es la cabeza principal de esta unidad, ver Figura 4.2, su estructura funcional esta detallada en el Anexo K.

Departamento de Tecnología de la Información

Figura 2-4: Estructura Unidad de TI Cooperativa San José LTDA.
FUENTE: Cooperativa de Ahorro y Crédito San José Ltda.

4.4.3 Sistemas informáticos relacionados a los servicios organizacionales

La Cooperativa de Ahorro y Crédito San José Ltda. Cuenta con sistemas informáticos que dan servicio a sus clientes ya sea a través de sistemas propios o de terceros, los cuales se detallan en los siguientes Numerales.

4.4.3.1 Sistema informático financiero – FITBANK

FIT-BANK es un core bancario integrado para automatización de la gestión bancaria, orientado especialmente a controlar y mejorar la rentabilidad del negocio Financiero, elevar el nivel de servicio al cliente, facilitar el lanzamiento de nuevos productos y dinamizar el negocio. A través de un análisis detallado de la información tanto financiera como no financiera, FIT-BANK permite determinar cuáles clientes, productos, sucursales y ejecutivos son rentables y cuáles no, permitiendo al mismo tiempo analizar las causas por las cuales no son rentables de modo que, con este análisis, la institución pueda corregir deficiencias, diseñar y crear nuevos productos y servicios ajustados a las necesidades particulares de los clientes con el propósito de volverlos rentables. La correcta administración de la información de los clientes y una total orientación al servicio, permitirán a los ejecutivos comerciales manejar eficientemente la relación con los clientes consiguiendo de esta manera clientes satisfechos y por lo tanto fieles a la institución, dispuestos a seguir confiando en su Institución para adquirir nuevos productos y servicios.
FIT-BANK, ha sido diseñado y construido en un esquema de capas:

La capa más exterior, Universal Channel Interface (UCI), es un Middleware independiente de Core, orientado al manejo de canales de acceso, se encarga de la interacción con el mundo externo (usuarios, clientes, prospectos, otras aplicaciones, etc.) esta capa además de manejar la seguridad y normalizar el acceso al Core, maneja canales como ATMs, Internet, Banca por teléfono, Kioscos, SMSs con Celulares, PDAs etc.

La capa inmediata inferior corresponde a los diferentes módulos los mismos que son accedidos mediante transacciones ingresadas por cualquiera de los canales soportados por UCI, estas a su vez interactúan con la base de datos de clientes y alimentan también

la contabilidad. Esta concepción permite, de forma muy fácil, la incorporación de nuevos subsistemas los mismos que solo necesitan concentrarse en sus funciones especificas ya que todos los aspectos de seguridad, la interacción con los clientes y la contabilidad es proporcionada automáticamente por el sistema.

La siguiente capa hacia adentro corresponde a la información sobre los clientes y la contabilidad, estos dos subsistemas son los pilares de toda la estructura del sistema. La información de los clientes está organizada por niveles que pueden ser parametrizados para ser requeridos o no, dependiendo del producto, su propósito fundamental es proporcionar la información necesaria para que conociendo al cliente se puedan crear productos y servicios acordes a sus posibilidades y necesidades y de esta forma gerenciar la relación con el cliente para obtener el mayor beneficio posible del Cliente (CRM Analítico).

El subsistema contable ha sido diseñado independientemente de cualquier plan preestablecido de cuentas y principalmente como un sistema gerencial orientado a proporcionar información financiera oportuna para el manejo del negocio financiero, complementariamente de forma muy sencilla se pueden obtener los reportes legales exigidos por los diferentes organismos de control.

Finalmente en el centro mismo del sistema se encuentra el módulo de información gerencial (MIS), todos los subsistemas han sido diseñados para alimentar y almacenar información relevante para que la gerencia del Banco cuente con toda la información para realizar análisis (desde los más básicos hasta los más sofisticados) de Rentabilidad por Cliente, Producto, Ejecutivos de cuenta, Sucursal y Canal, también permite análisis de Activos y Pasivos, Análisis de Gap y Cash Flow. Utiliza el gestor de base de datos Oracle standart One y sus interfaces de usuario se encuentran desarrolladas en java.

4.4.3.2 Sistema informático de talento humano – COMPERS

Software que facilita la implantación de un Sistema de Administración de Recursos Humanos basado en Competencias, mediante la automatización de su gestión. ADMINISTRACION DE RECURSOS HUMANOS BASADA EN COMPETENCIAS que es una nueva tendencia administrativa que están aplicando las organizaciones de

vanguardia. Utiliza el gestor de base de datos Sql Server 2008 y sus interfaces de usuario se encuentran desarrolladas en visual Basic.

4.4.3.3 Sistema informático para manejo de Cajeros Automáticos – ENTURA

Es una aplicación desarrollada para una red transaccional que unifica a las cooperativas de ahorro y crédito, logrando su objetivo estratégico de dar acceso a sus socios para que realicen operaciones financieras a nivel nacional, generando la inclusión financiera en los lugares más alejados de la geografía Ecuatoriana. ENTURA ofrece una red de cajeros automáticos, situándolos en localizaciones públicas estratégicas fuera de las oficinas sucursales, tomando en cuenta que uno de los factores más importantes para los depositantes es el acceso a su dinero.

4.4.3.3 Sistema informático para manejo de lavado de Activos

Una herramienta de control que tiene como objetivo minimizar el riesgo de establecer vínculos con posibles involucrados o señalados en actividades ilícitas como lavado de activos, narcotráfico o terrorismo, así como su identificación en la cartera actual de una entidad, de forma que se salvaguarde a su Institución de riesgos significativos en su reputación y actividad comercial. RCS es un software basado en el sistema Bridger Insight que utiliza una tecnología muy sofisticada y los algoritmos de búsquedas inteligentes, especializados y tecnológicamente más avanzados, los cuales son producto de investigaciones y análisis de empresas y organismos entendidos en el tema de Cumplimiento y Control de Lavado de Activos a nivel mundial como GAFI, la Reserva Federal, etc. RCS cuenta con muchas listas de impedidos provistas por ChoicePoint Bridger System, empresa certificada por la Reserva Federal y por el Departamento de Tesoro Americano. Cabe recalcar que dichas listas son emitidas y certificadas por estos organismos internacionales de control, legalmente autorizados y, por lo tanto, son fuentes confiables y fidedignas.

4.4.3.4 Sistema informático para pago de servicios FACILITO

Es un sistema para pago de servicios básicos o masivos, que integra entidades financieras, comerciales y de servicios en productos que generan valor agregado las instituciones financieras.

4.4.3.5 Sistema informático para pago de servicios SERVIPAGOS

Es un canal de distribución de servicios de pagos del Ecuador.

4.4.4 Diagrama de red Organizacional

En la Figura 4.3 y 4.4, se puede apreciar los diagramas de red con los que cuenta la COOPERATIVA, actualmente tienen enlace de datos con 2 empresas las conexiones con Claro y CNT, la matriz de tecnología está ubicada en la ciudad de Guaranda, con sus agencias en San José de Chimbo, San Miguel, Chillanes, Montalvo, Ventanas y Quito.

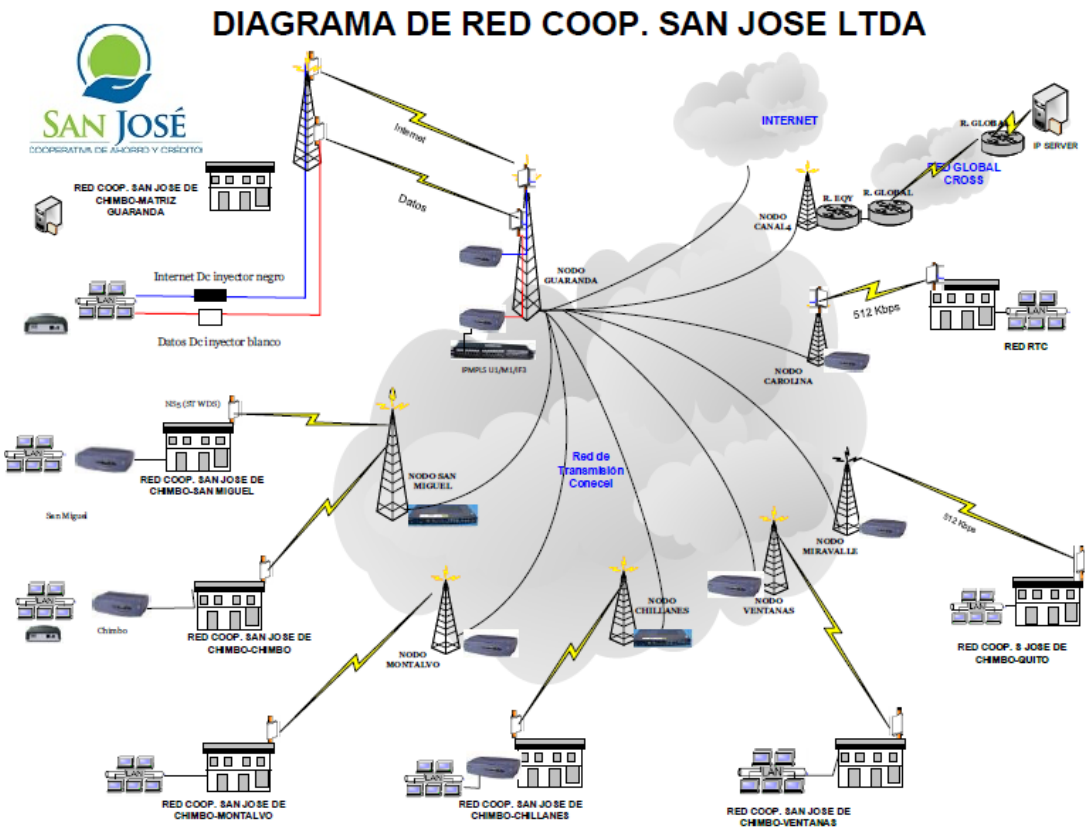

Figura 3-4: Diagrama de Red Organizacional Proveedor EQUYSUM
FUENTE: Cooperativa de Ahorro y Crédito San José Ltda.

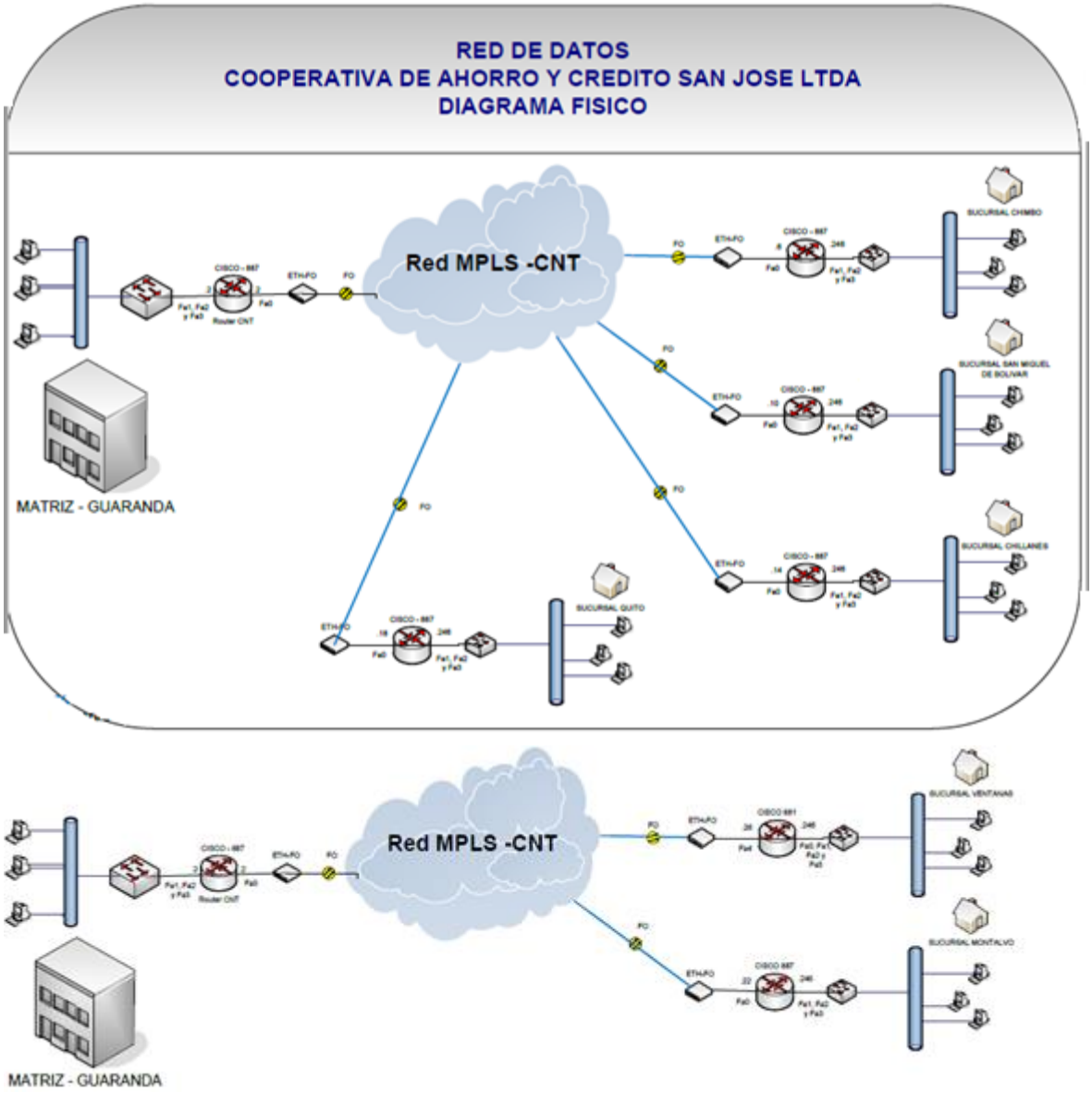

Figura 4-4: Diagrama de Red Organizacional Fibra Óptica Proveedor CNT
FUENTE: Cooperativa de Ahorro y Crédito San José Ltda.

4.4.5 Servidores con servicios críticos

- Servidor Mail
- Servidor Directorio Activo
- Servidor E-Learning
- Servidor Aplicación Móvil
- Servidor Ventanillas Compartidas
- Servidor ATM
- Servidor Pandora
- Servidor ServiceTonic

- Servidor Desarrollo

4.5 Desarrollo del DRP

La norma ISO 22301:2012, abarca un campo muy amplio como es la continuidad del negocio que comprende la recuperación de todo el engranaje de procesos de las Operaciones que se llevan a cabo en la organización; lo cual para la aplicabilidad de esta tesis se tomó lo más importante y complementario para el desarrollo del DRP, enfocándose en la recuperación de las actividades tecnológicas de mayor relevancia que mantienen los procesos financieros de la Cooperativa de Ahorro y Crédito San José.

El DRP se basa en la continuidad de las operaciones de los sistemas informáticos y procesos tecnológicos que mantiene la Unidad de Tecnología de la Cooperativa de Ahorro y Crédito San José LTDA, para sustentar las principales actividades que se desarrollan en la organización; estos servicios que ofrece la Unidad de tecnología a las áreas usuarias, deben estar siempre disponibles para poder asegurar la estabilidad económica y financiera de la institución y su permanencia en el mercado, sin caer en violaciones de las leyes y de observancias de los organismos de control que así lo exigen.

El DRP para la Unidad de Tecnología de la Cooperativa de Ahorro y Crédito San José LTDA se desarrolla un método basado en las recomendaciones de la normativa ISO 22301, los requerimientos de la norma sobre Riesgo Operativo y apoyada en la experiencia de casos prácticos realizados en nuestro país.

4.5.1 Planificación

4.5.1.1 Objetivo

Dotar a la institución de herramientas necesarias para incrementar la posibilidad de supervivencia del negocio ante la presencia de factores de riesgo operativos generadores de pérdidas y eventos catastróficos.

4.5.1.2 Alcance

El DRP se ha diseñado para minimizar pérdidas económicas y riesgos ante la interrupción inesperada de procesos de criticidad muy alta de la institución, de acuerdo a lo determinado en la Resolución de Riesgo Operativo de la Superintendencia de Bancos.
El general el alcance del DRP, garantiza a la Cooperativa de Ahorro y Crédito "San José" Ltda., la continuidad de sus operaciones en los procesos de la cadena de valor del negocio definido como críticos, a continuación se describen los cuatro factores fundamentales para la operación.

Humano: Certificar que el personal cuente con las habilidades, conocimientos, y destrezas necesarias para que todos los procesos considerados como críticos estén disponibles durante la recuperación o contingencia.

- Comité de Continuidad del Negocio.
- Equipo de Contingencias.
- Talento Humano necesario para operar en Contingencia.
- Logística de movimiento personal.
- Lista de contactos.

Infraestructura Física: Dotar de la infraestructura necesaria alterna para habilitar los procesos críticos. Suponiendo que la infraestructura física considerada como principal este inhabilitada o afectada debido a un desastre o evento presentado.

- Facilidades de instalaciones.

- Provisión de servicios básicos.
- Provisión de suministros.
- Seguridad física.

Comunicacional: Debemos manejar 2 escenarios de comunicación durante la contingencia.

- **Interna**.- Son los colaboradores de la institución.
- **Externa.-** Canal de comunicación entre los clientes, proveedores y la organización.

Tecnológico: Infraestructura tecnológica que este configurada como espejo de la principal con el objetivo de habilitar los procesos críticos del negocio. Suponiendo que la infraestructura considerada como principal este inhabilitada o afectada por causa de un desastre.

- Centro de cómputo alternativo.
- Equipamiento y software necesario.
- Redes de comunicaciones.
- Recuperación de datos.
- Soporte técnico.

4.5.1.3 Responsables

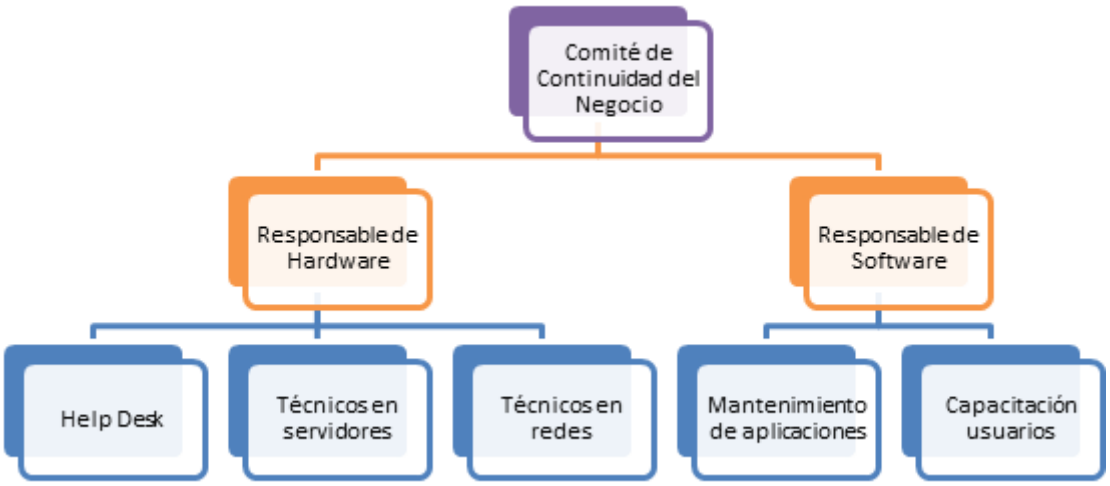

Figura 5-4: Roles y Responsabilidades
FUENTE: TECSERVIN

Comité de Continuidad del Negocio.

Para gestionar y supervisar el proceso de elaboración e implantación del plan de continuidad de negocio y cumpliendo con la normativa vigente se consideró necesario implementar la tarea clave de designar a un comité de continuidad del negocio conformado por: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648).

El comité de continuidad del negocio debe tener al menos las siguientes responsabilidades: (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648)

- Monitorear la implementación del plan y asegurar el alineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente. (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648)
- Proponer cambios, actualizaciones y mejoras al plan. (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648)
- Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos. (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648)
- Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y, (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648)
- Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones. (SUPERINTENDENCIA DE BANCOS Y SEGUROS, 2014b, p. 648)

Presidente del Comité de Continuidad del Negocio (Oficial de Riesgos).

Presidente del Comité de Continuidad es el encargado (a) de liderar la implementación y cumplimiento del proceso y demás las actividades relacionadas al Plan de

Continuidad. En caso de contingencia ante el escenario de interrupción en lugar de trabajo, se encarga de comunicar las decisiones tomadas por el Comité de Continuidad del Negocio en circunstancias en donde merezca realizar su activación. («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013, p. 11)

Dentro de las funciones del presidente de continuidad se encuentran las siguientes:

Responsabilidades:

- Determinar el alcance y los objetivos que persigue el plan conjuntamente con la dirección.
- Monitorear la ejecución del Plan de Recuperación de Desastres a través de los diferentes responsables.
- Identificar las actividades de negocio que son críticas en la institución conjuntamente con la alta dirección.
- Dirigir las acciones durante la contingencia y recuperación.
- Análisis de la situación de contingencia.
- Decisión de activar o no el Plan de Continuidad.
- Iniciar el proceso de notificación a los medios de comunicación, directivos, empleados y asociados, a través de los diferentes responsables.
- Tomar decisiones claves durante los incidentes, con la finalidad de reducir al máximo el riesgo y la incertidumbre ante la ocurrencia de eventos de riesgo en coordinación con el Gerente General.
- Evaluar daños, en el caso de sucedido el evento conjuntamente con los diferentes responsables.
- Ser el enlace, con la dirección de la institución, manteniéndoles informados de la situación de contingencia frecuentemente.
- Dirigir, monitorear y evaluar las acciones durante la contingencia y recuperación con los diferentes responsables.
- Dar seguimiento al proceso de recuperación, con relación a los tiempos estimados de recuperación.
- Delegar de manera expresa en el Comité, la responsabilidad de actualizar, mantener y probar el plan de continuidad.
- Liderar las reuniones del Comité.

- Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del plan de continuidad.
- Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia.
- Velar por la seguridad del personal que actúa en el área del evento.
- Establecer los objetivos de recuperación y activar el plan de continuidad ante el escenario de interrupción de lugar teniendo en cuenta el resultado de la evaluación
- Velar por la ejecución del debido análisis causa raíz del evento que ocasionó la contingencia.
- Llevar a cabo las decisiones tomadas por el Comité de Continuidad del Negocio.
- Documentar el manual de continuidad de la institución.
- Establecer las pruebas requeridas para la implementación adecuada del Plan de Recuperación de Desastres, en coordinación con los diferentes responsables.
- Llevar un control adecuado de la actualización de: procesos, recursos humanos, recursos tecnológicos, etc.
- Activación del personal de soporte y equipos responsables de los departamentos.

Administrador de Continuidad del Negocio.

El administrador de Continuidad, es el representante de Negocios, el avance de la tecnología y la administración genera también la ocurrencia de nuevas amenazas que deben ser determinadas con anticipación para la incorporación de planes que minimicen sus efectos. Para ello, representante de Negocios, perteneciente al comité planteado deberá cumplir las siguientes responsabilidades.

- Asumir el rol y cumplir con las responsabilidades del Presidente del Comité de Continuidad del Negocio, cuando éste no se encuentre disponible o presente.
- Declarar el estado de contingencia cundo exista algún inconveniente tecnológico de uno o varios aplicativos..
- Verificar la existencia de riesgos tanto internos como externos que puedan afectar al normal desempeño de las actividades.
- Incorporar el plan de continuidad necesario en función de los riesgos detectados.
- Coordinar la capacitación del plan de continuidad al personal de la institución.
- Llevar a cabo el desarrollo de las diferentes etapas del PCN.

Líder de Recuperación Tecnológica.

Es la persona encargada de liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas. Es el contacto directo entre el departamento de Tecnología de la Información y el Comité de Continuidad del Negocio; además, apoya las decisiones tomadas por el Presidente del Comité de Continuidad, durante la declaración y activación de la contingencia. («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013, p. 12)

Responsabilidades.

Consideramos las responsabilidades de acuerdo («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013, p. 12)

- Liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas.
- Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad.
- Mantener comunicación constante entre Coordinadores de Recuperación del Negocio durante el estado de contingencia.
- Colaborar en la comunicación a los proveedores de los temas o servicios de su competencia, sobre el estado de contingencia en que se encuentra la Entidad, esto previa decisión y autorización del Presidente de Continuidad.
- Entregar los reportes correspondientes al Comité de Continuidad del Negocio sobre el estado de la recuperación.
- Velar por la actualización de la Estrategia Tecnológica en los casos que se presenten situaciones como: cambios en los aplicativos, cambio en la infraestructura, roles y responsabilidades, disponibilidad de los recursos, entre otros.
- Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en las mismas, en lo concerniente a la parte tecnológica.
- Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.

Coordinadores de Recuperación.

Son personas encargadas de liderar la recuperación de procesos de negocio críticos, basados en las estrategias de contingencia. Son el contacto directo entre los procesos de negocio y el Comité de Continuidad del Negocio; además, colaboran con las decisiones tomadas por el Presidente del Comité de Continuidad de Negocio y el Comité durante la declaración y activación de la contingencia. («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013, p. 13)

Responsabilidades.

Consideramos las responsabilidades de acuerdo («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013, p. 13)

- Liderar las reuniones del equipo de recuperación, para diagnosticar y evaluar las interrupciones que están afectando la prestación del servicio.
- Colaborar en la ejecución de los planes de contingencia ante el o los incidentes presentados.
- Identificar los posibles riesgos que afectan la continuidad de la operación normal de la Entidad y que ponen al descubierto debilidades del plan de continuidad.
- Mantener comunicación constante durante el estado de contingencia con los principales actores.
- Colaborar en la comunicación a los proveedores sobre el estado de contingencia en que se encuentra la Entidad, esto previa decisión y autorización del Presidente del Comité de Continuidad del Negocio.
- Entregar los reportes correspondientes al Comité de Continuidad del Negocio, sobre el estado de la recuperación de sus áreas.
- Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos en la misma.
- Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.

Para un mejor entendimiento las funciones que debe cumplir:

Coordinadora de Talento Humano:

Responsabilidades:

- Atender todas las necesidades extraordinarias de índole laboral que puedan aparecer como consecuencia de las características especiales de los trabajos que hay que realizar, (contacto con el comité, establecimiento de turnos, horas extraordinarias, transporte de personal, etc.).
- Atender el estado físico y psicológico del personal afectado por el incidente con la asistencia de expertos en la materia.
- Atender e informar a familiares de posibles heridos, etc.

Responsables de Hardware y Software:

Responsabilidades:

Consideramos las responsabilidades de acuerdo («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013, p. 13)

- Realizar las actividades que le sean asignadas durante la declaración de contingencia.
- Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan.
- Establecer la infraestructura necesaria para la recuperación, esto incluye servidores, comunicaciones de voz y datos, y otros elementos necesarios para la restauración de un servicio.
- Realizar pruebas que verifiquen la recuperación de los sistemas críticos.
- Informar al CCN las estrategias implementadas antes, durante y después de la contingencia.
- Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos.

4.5.2 Análisis de Impacto en el Negocio (BIA).

El Análisis BIA, constituye la actividad de la gestión en la Continuidad del Negocio que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir Proveedores, personas, otros Procesos de Negocio, Servicios de Tecnología de la Información (TI), etc. Este análisis define los requerimientos de recuperación para los servicios de TI, los que incluyen objetivos de tiempos de recuperación, objetivos del punto de recuperación y los objetivos de nivel de servicio mínimos para cada Servicio de TI, («GLOSARIO | SpanishPMO», s. f.).

Los fracasos en sistemas de información y procesos internos pueden conducir a errores tanto en la dirección automatizada como en recursos humanos, una situación que causa pérdidas financieras y suspensiones del servicio, comprometiendo el desarrollo de organización.

Para inferir se determina que la identificación de los procesos críticos parte de la matriz de valoración de riesgos de todos los procesos existentes en la institución, se determinarán en base a los siguientes criterio según Villegas : (Villegas De La Cruz, Marcia Marina, 2013, p. 94)

- Costo de horas de trabajo perdidas, al no poder usar las aplicaciones que no tengan alternativa manual o cuyo tratamiento manual suponga una pérdida de eficiencia importante.
- Ingresos dejados de percibir por paralización de actividades.
- Penalizaciones por incumplimientos de contratos con clientes.
- Sanciones administrativas por incumplimiento de leyes debido a la falta de control en situación de desastre.
- Gastos financieros.
- Identificación de los procesos relacionados directamente con clientes y el mercado financiero.
- Definición del personal, los equipos, sistemas, ubicaciones físicas, comunicaciones necesarias para reanudar el servicio.
- Establecimiento del cumplimiento de disposiciones legales y regulatorias.

Tabla 13-4 Cálculo de pérdidas por hora.

Estado de resultados al 31 de diciembre de 2016			**Cálculo promedio de horas trabajadas en un año.**	
Cuenta	Saldo (USD$) (n)	Pérdida por hora (USD$) m=(n/e)	Días trabajados en el mes. (a)	26
Intereses en cartera de crédito.	13873669.97	5558.36	Meses del año (b)	12
Otros Ingresos	54177.86	21.71	Días trabajados en el año ©=a*b	312
Gastos de Operación	5119417.72	2051.05	Horas laborables en un día (d)	8
Utilidad Operacional.	1064274.12	426.39	Total horas trabajadas en el año (e) =c*d	2496
TOTAL GENERAL	20111539.67	8057.51		

Realizado por: Washington Vásquez, 2017

Con estas consideraciones se identifica que los procedimientos críticos de la Institución se concentran en los procesos productivos de captaciones, colocaciones y en los procesos de apoyo: Tecnología de Información, para lo cual debemos considerar lo siguiente:

- Identificar los procesos críticos existentes en la institución, considerando los factores críticos de éxito, además del impacto y la probabilidad de ocurrencia de los procesos sobre la continuidad del negocio.
- Determinar los tiempos de recuperación de los procesos críticos.

- Determinar los requerimientos de recursos Tecnológicos y no Tecnológicos de cada uno de los procesos críticos.
- Determinar los procedimientos alternos y el desarrollo de las estrategias de los procesos críticos.

4.5.2.1 Identificar los procesos críticos para el negocio.

Consiste en calcular las ponderaciones que serán utilizadas para calificar a todos los procesos de la Cooperativa. Entre los factores que se han tomado para el efecto, se detallan a continuación:

- Cumplimiento de normativas.
- Capacidad de enfrentar la Competencia.
- Contar con información del endeudamiento en entidades es no controladas y casas comerciales
- Satisfacción (Fidelidad) de socios y clientes.
- Adaptación al entorno económico, político y social.
- Control Morosidad.
- Gobernabilidad (estrategias y políticas).
- Recurso Humano Satisfecho, Capacitado y Profesional.
- Imagen Corporativa.
- Solvencia.
- Mantener adecuada Calificación de Riesgos.
- Diversidad de Productos (Innovación).
- Trabajo en Equipo y Planificado.
- Apropiada Plataforma Informática.
- Clima Organizacional.
- Liderazgo.
- Cultura de Riesgos

Al calificar, se considerará al “0” como de menor importancia, mientras que el “1” será el de mayor importancia, es decir si los factores de las columnas son más importantes que los factores de las filas se obtendrá “1”, caso contrario será “0”. Cuando los factores tanto de la fila como de la columna coinciden, no tendrán calificación. Las

ponderaciones se obtienen al dividir la suma de las calificaciones de cada fila para la sumatoria total de las calificaciones. (Ver anexo A).

Una variante de esta matriz consiste en usar las ponderaciones de cada FCE como un factor de cada celda.

4.5.2.2 Determinar el impacto de la interrupción de cada proceso crítico y el tiempo máximo tolerable de interrupción para cada uno

Matriz de Cruce entre Factores Críticos de Éxito vs. Procesos.

Durante esta fase se procede a llenar una matriz de puntajes que cruza Factores Críticos de Éxito vs. Mapa de Procesos de la Cooperativa San José Ltda., para colocar en puntaje en cada celda de cruce entre un proceso y un FCE se deberá realizar la siguiente pregunta:

“ Si se logra ejecutar el proceso extremadamente bien se obtendría el Factor Crítico de Éxito?”

La respuesta puede tener tres posibles puntajes:

Tabla 14-4 Calificación de procesos

Respuesta	Puntaje
Si existe relación marcada entre ejecutar el proceso extremadamente bien y lograr el FCE	1
Existe una mediana relación entre ejecutar el proceso extremadamente bien y lograr el FCE.	0.5
No existe ninguna relación entre ejecutar el proceso extremadamente bien y lograr el FCE.	0

Realizado por: Washington Vásquez, 2017

Los resultados obtenidos de la relación entre los FCE, se muestran en la matriz de cruce. Luego de llenar la matriz de cruce se procede a sumar cada fila (puntaje de cada proceso). (Ver anexo B).

Tabulación de los procesos (Nivel de Satisfacción de los procesos)

Se deberá además otorgar un puntaje que representa el nivel de satisfacción que tiene la institución con cada uno de los procesos, subprocesos o procedimientos, depende de la profundidad con la que se haya realizado el inventario de procesos y con el cual se realizará la matriz de cruce.

Para otorgar el puntaje de nivel de satisfacción se podrá tomar en cuenta entre otras las siguientes características:

- Nivel de documentación del proceso.
- Nivel de automatización del proceso.
- Número de quejas sobre el proceso.
- Cantidad y calidad de los controles existentes sobre el proceso.

(Ver anexo C. NIVEL DE SATISFACCIÓN DE LOS PROCESOS).

TABULACIÓN DE LOS PROCESOS.

Para un mejor entendimiento la tabulación consiste en la multiplicación de las ponderaciones de los FCE por cada una de las calificaciones de los procesos tomados de la Matriz de Cruce. Estos valores se suman luego horizontalmente y se multiplican con el Nivel de Satisfacción de los procesos, para su efecto se ha utilizado la siguiente tabla:

Tabla 15-4 Nivel de satisfacción de los procesos

NIVEL DE SATISFACCIÓN	
1	Muy Alta
2	Alta
3	Media
4	Baja
5	Nula

Realizado por: Washington Vásquez, 2017

El resultado de este producto, se multiplica por el impacto y la probabilidad de ocurrencia de los procesos sobre la continuidad del negocio. (Ver anexo D)

Tabla 16-4 Escala para probabilidad de ocurrencia

Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene plena seguridad que éste se presente, tiende al 100%
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 75% a 95% de seguridad que éste se presente.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 51% 74% de seguridad que éste se presente.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 26% a 50% de seguridad que éste se presente.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 25% de seguridad que éste se presente.

Fuente: (https://www.coursehero.com/file/p6o37nt/Organizacionales-06-01-Objetivos-de-costos-tiempo-y-alcance-inconsistentes-06/)

Realizado por: Washington Vásquez, 2017

Tabla 17-4 Escala para materialidad del impacto

Categoría	Valor	Descripción
Catastróficas	5	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, pérdida patrimonial o deterioro de la imagen, dejando además sin funcionar totalmente o por un período importante de tiempo, los programas o servicios que entrega la institución.
Mayores	4	Riesgo cuya materialización dañaría significativamente el patrimonio, imagen o logro de objetivos sociales. Además, se requeriría una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños
Moderadas	3	Riesgo cuya materialización causaría ya sea una pérdida importante en el patrimonio o un deterioro significativo de la imagen. Además, se requeriría una cantidad de tiempo importante de la alta dirección en investigar y corregir los daños.

Menores	2	Riesgo que causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo y que no afecta el cumplimiento de los objetivos estratégicos
Insignificantes	1	Riesgo que puede tener un pequeño o nulo efecto en la institución.

Fuente:https://www.coursehero.com/file/p6o37nt/Organizacionales-06-01-Objetivos-de-costos-tiempo-y-alcance-inconsistentes-06/Realizado por: Washington Vásquez, 2017

Tabla 18-4 Procesos

PROCESOS						
PROBABILIDAD	Casi con certeza	5					
	Probable	4					
	Posible	3				R	
	Poco probable	2					
	Raro	1					
			1	2	3	4	5
			Insignificante	Menor	Moderada	Mayor	Catastrófica
IMPACTO							

Fuente:https://www.coursehero.com/file/p6o37nt/Organizacionales-06-01-Objetivos-de-costos-tiempo-y-alcance-inconsistentes-06/Realizado por: Washington Vásquez, 2017

¿Qué puede hacer la organización ante los riesgos que ha identificado?

Existen diferentes opciones para hacer frente a los mismos:(Intelco, s. f., p. 40)

Aceptar el riesgo: la organización conoce el riesgo y decide asumirlo sin tomar ninguna acción al respecto, bien porque no tiene capacidad o bien porque el coste para mitigar el riesgo es desproporcionado para los beneficios que aporta.

Transferir el riesgo: como por ejemplo a través de la subcontratación de servicios o mediante la contratación de un seguro de cobertura, de forma que si el riesgo se materializa exista una compensación externa que lo mitigue.

Reducir el riesgo a niveles aceptables por la organización: mediante el diseño y la implantación de controles o medidas preventivas o que atenúen los impactos y las consecuencias del mismo.

Evitar el riesgo: mediante la eliminación del mismo (por ejemplo a través de la reingeniería de procesos o incluso suspendiendo la actividad que origina el riesgo sin penalizar los objetivos de negocio de la organización).

Las distintas opciones para hacer frente a los riesgos pueden ser utilizadas conjuntamente, si bien es destacable que no todos los riesgos pueden ser reducidos o prevenidos a un nivel aceptable. La continuidad de negocio constituye por sí misma una estrategia o una opción de respuesta para hacer frente a aquellos riesgos que pueden interrumpir las operaciones de la organización.

Procesos Críticos.

Para determinar si un proceso es crítico o no, se utilizó la ponderación de los datos del producto total tomado de la Tabulación de los Procesos. De estos porcentajes se calcula el promedio. Aquellos procesos que superan este porcentaje se consideran críticos. (Ver Anexo. E)

4.5.2.3 Determinar el RTO, RPO y MTD de cada sistema crítico.

Consiste en determinar el tiempo máximo que se puede tolerar cuando el proceso se ha detenido, basado en su impacto financiero y su impacto operacional (Ver anexo F). Estos tiempos se describen a continuación:

MTD (Tiempo de inactividad máximo tolerable).- Período máximo de tiempo de interrupción tolerable por la organización, sin entrar en colapso (desde la ocurrencia del evento hasta el reinicio de las operaciones).

Las siguientes son algunas estimaciones de tiempos máximos permitidos de interrupción que pueden ser empleados por la institución para conocer la criticidad de sus actividades y/o de sus recursos: no prioritario (30 días); normal (7 días); importante (72 horas); urgente (24 horas) y crítico (minutos u horas).

En este punto es necesario destacar que el impacto total asociado a la paralización de alguna actividad de la organización depende de varios factores:

Tabla 19-4 Factores

Tipos de Impacto	Descripción del Impacto
Operativos.	Actividades de negocio que dejan de estar en funcionamiento o el coste de las horas de trabajo perdidas por los empleados
Económicos.	Costes directos o indirectos como por ejemplo el lucro cesante.
Regulatorios o contractuales.	Sanciones por incumplimiento legal o penalizaciones por incumplimiento del contrato con clientes
Imagen.	Relación de aspectos más intangibles y por tanto más difíciles de valorar como la imagen, la fiabilidad y la reputación de la organización frente a clientes, proveedores y accionistas

Fuente: Cooperativa de Ahorro y Crédito San José Ltda.

Realizado por: Washington Vásquez, 2017

RTO (Tiempo recuperación objetivo).- Expectativa de tiempo de recuperación de los servicios de tecnología de información.

RPO (Objetivo de punto de recuperación).- Período de tiempo que un proceso puede tolerar. Pérdida de datos.

WRT (Tiempo de recuperación de trabajo).- Tiempo disponible para recuperar los datos perdidos, una vez que los servicios de tecnología de información han sido restablecidos. (Recuperación manual de datos).

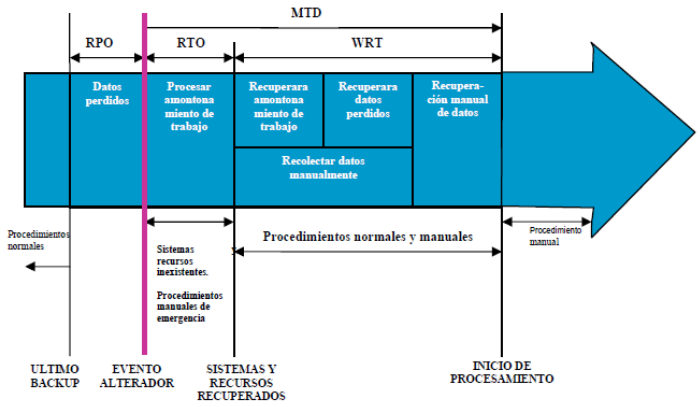

Figura 6-4 Tiempos para la recuperación ante desastre
Fuente: Cooperativa de Ahorro y Crédito San José Ltda.

Determinación de los recursos críticos.

Consiste en identificar los requerimientos de recursos de los procesos críticos. Estos recursos pueden ser de sistemas de tecnología de información y los que no pertenecen a tecnología de información. (Ver anexo G)

Recursos organizacionales sobre los cuales se diseñan las estrategias de recuperación.

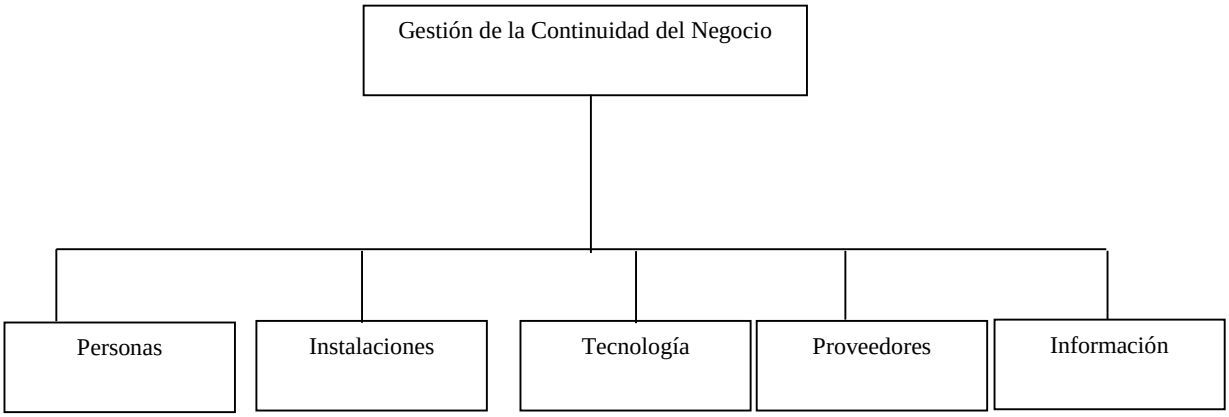

FIGURA 7-4: Recursos organizacionales sobre los cuales se diseñan las estrategias de recuperación.

Fuente: Cooperativa de Ahorro y Crédito San José Ltda.

Determinación de los procedimientos alternos

La identificación de procedimientos alternos, permiten que los procesos de negocio puedan continuar si se presenta una interrupción, mediante operaciones manuales temporales para todos los procesos críticos.

4.5.3 Análisis del Riesgo

Consiste en evaluar las amenazas, pormenorizar las vulnerabilidades existentes, identificar, implementar los controles necesarios para prevenir o reducir los riesgos en los procesos identificados en el análisis BIA.

Este procedimiento se demuestra en el siguiente gráfico:

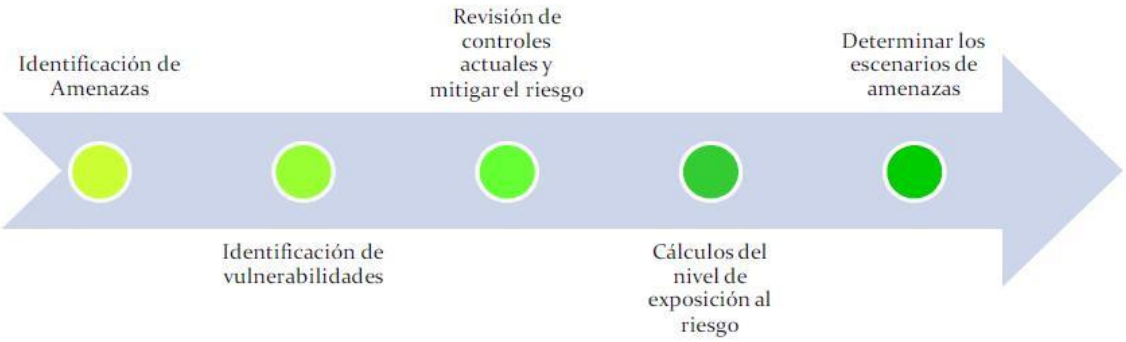

Figura 8-4: Análisis BIA
Fuente: Cooperativa de Ahorro y Crédito San José Ltda.

Identificación de amenazas.- Consiste en Identificar las amenazas que afecten a los activos de las funciones organizacionales, principalmente originadas por:

Tabla 20-4 Amenazas

AMENAZAS	POSIBLE
DESASTRES NATURALES.	
Inundaciones	**NO**, en las oficinas de Chimbo, Guaranda, Chillanes, San Miguel, Quito pero **SI,** en Montalvo, Ventanas.
Incendios	SI
Huracanes	NO
Fenómeno sísmico o volcánico.	SI
Rayos.	SI
Avalanchas.	NO
Derrumbes.	**NO**, en las oficinas de Guaranda, Chillanes, San Miguel, Quito, Montalvo, Ventanas pero **SI,** en la oficina de Chimbo.
Terremotos/Sismos.	SI

DAÑOS ACCIDENTALES	
Fuego fortuito	SI
Inundaciones.	NO
Fallo del aire acondicionado.	SI
Exceso de humedad.	NO
Humo, Gases tóxico.	NO
Subida de tensión.	NO
Fallo de suministro eléctrico.	SI
Accidentes del personal.	SI
Capacidad inadecuada de las comunicaciones.	SI
Fallo/degradación del hardware.	SI
Fallo/degradación de las comunicaciones.	SI
Errores de operación.	SI
Fallos en las copias de seguridad.	SI
Fallos en los sistemas de autenticación/autorización.	SI
Pérdida de confidencialidad.	SI
Incumplimientos legales.	SI
ATAQUES INTENCIONADOS.	
Explosivos.	NO
Fuego intencionado.	SI
Accesos no autorizados al edificio.	SI
Actos de vandalismo.	SI
Bombas	SI
Violencia laboral	SI
Terrorismo	SI
Radiaciones electromagnéticas.	NO
Robos intencionados.	SI
Manipulación de datos/software.	SI
Manipulación de hardware.	SI
Uso de software por personal no autorizado.	SI
Acceso no autorizado a datos de la institución.	SI
Software malicioso.	SI
Robo de equipos.	SI
Robo de documentos.	SI
Robo de software.	SI
Descarga de software no controlada.	SI
Interceptación de las líneas de comunicación.	SI
Manipulación de las líneas de comunicación.	SI
Abuso de privilegios de acceso.	SI
Introducción de virus en los sistemas.	SI
Ataques por ingeniería social.	SI
Bombas lógicas.	NO

Ataques de denegación de servicio.	SI
Errores intencionados (de uso, de diseño o entrega de información).	SI
Acceso físico NO autorizado.	SI
Acceso lógico NO autorizado.	SI
Indisponibilidad de recursos (abandonos, rotación).	SI
Sabotaje interno.	SI
Copias incontroladas de documentos/software/datos.	SI
Errores en el mantenimiento.	SI
Corrupción de datos.	SI
Incumplimientos legales intencionados.	SI
ATAQUES INTENCIONADOS DE ORIGEN REMOTO.	
Acceso lógico NO autorizado.	SI
Virus.	SI
Cyber Attack.	SI

Fuente: Cooperativa de Ahorro y Crédito San José Ltda.

Realizado por: Washington Vásquez, 2017

Como comprobamos existen una serie de amenazas que pueden darse y otras que no, incluso en función de la ubicación de las oficinas pueden darse unas en una de las oficinas y otras en otras, por tanto es misión de los involucrados, es saber discernir qué amenazas y en qué lugares pueden darse.

Identificación de vulnerabilidades.- Es el momento en que se listan las potenciales vulnerabilidades por cada amenaza.

Revisión de Controles actuales.- Consiste en generar un listado de todos los controles.

Cálculo del nivel de exposición al riesgo.- Permite identificar el grado de severidad de las amenazas y la cobertura de los controles.

Para el cálculo de la severidad se utilizó las siguientes categorías:

Tabla 21-4 Calculo de severidad

N/A: No aplica	**0**
B: Baja	10
M: Moderada	50
A: Alta	100
Exposición al riesgo = (Severidad * (100% - % de Cobertura))/100.	

Realizado por: Washington Vásquez, 2017

Descripción de amenazas, control, vulnerabilidad, riesgos, severidad, cobertura y exposición.

De acuerdo a nuestros procesos críticos y enfocando los recursos de tecnología de información, se procede a analizar las amenazas, los controles existentes y sus vulnerabilidades, para luego estimar la severidad y la cobertura. (Ver anexo H).

4.5.4 Selección de la Estrategia (Estrategia)

En la selección de la estrategia de los procesos críticos, se toma en cuenta los tipos de plan en base a lo establecido en la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros, puesto que aún la Superintendencia de Economía Popular y Solidaria no se pronuncia con respecto al tema de riesgos, con lo que se asegura que la misma sea aplicable a la materialización de un evento de riesgo.

Tabla 22-4 Estrategia

Recursos de TI/Otros	Estrategias	Tipo de Plan
Estación de Trabajo	➢ Reemplazar equipos de cómputo dañados. ➢ Mantener una estación de trabajo de respaldo en cada una de las oficinas. ➢ Disponer de respaldos de información de estación de trabajo. ➢ Proveer equipos funcionales a cada puesto de trabajo.	Recuperación
	➢ Almacenamiento de respaldo de	Recuperación/Reanudación

Red WAN	configuraciones. ➢ Redundancia de enlaces y equipos de comunicación. ➢ Habilitar el enlace de back up en caso de fallas de antenas. ➢ Reemplazar equipos en caso de fallas en router y switch de matriz y oficinas operativas de la WAN.	
Red LAN	➢ Redundancia de equipos de comunicación. ➢ Respaldo de configuraciones. ➢ Realizar un nuevo cableado en caso de falla en el cableado estructural. ➢ Reemplazar equipos en caso de falla de switch.	Reanudación
Servidor de Producción de Switch Transaccional	➢ Redundancia de equipos. ➢ Habilitar el servidor de back up.	Reanudación
Servidor de Producción de Base De Datos	➢ Mantener un servidor de stand by de base de datos. ➢ Respaldo de datos diario. ➢ Habilitar el servidor de stand by de la base de datos.	Recuperación
Servidor de producción de Firewall	➢ Mantener un equipo de back up para firewall. ➢ Habilitar el servidor de back up de ➢ Firewall.	Reanudación
Servidor de producción de Aplicaciones	➢ Redundancia de equipos. ➢ Habilitar el servidor de back up de aplicaciones.	Reanudación
Servidor de Producción Correo Electrónico, Intranet, Help Desk y Proxy	➢ Almacenar respaldo de configuraciones. ➢ Recuperar configuraciones en un nuevo servidor.	Reanudación
Centro de cómputo	➢ Mantener centro de cómputo alterno con los equipos necesarios para que pueda operar un sistema informático. ➢ Habilitar un centro de cómputo alterno.	Reanudación
Cajeros Automáticos	➢ Mantener vigente el soporte especializado. ➢ Solicitar soporte especializado.	Recuperación
Valores en efectivo y cheques	➢ Disponer de financiamiento externo. ➢ Racionalizar el ritmo de colocaciones.	Contingencia
	➢ Mantener una adecuada estructura financiera.	Contingencia
	➢ Intensificar la recuperación de la cartera.	Contingencia
Instalaciones	➢ Asegurar la integridad física del recurso humano.	Contingencia

	➢ Contar con pólizas de seguros de los activos físicos de la institución. ➢ Garantizar la atención al público.	
Personas que participan en las actividades de negocio	➢ Documentar actividades críticas. ➢ Formación. ➢ Conocimiento compartido y multidisciplinar. ➢ Separación de tareas clave	Contingencia
Proveedores	➢ Contacto con proveedores alternativos. ➢ Acuerdos con terceros. ➢ Envío y almacenamiento de recursos críticos en ubicaciones alternativas	Contingencia
Servicios civiles de emergencia (tráfico, bomberos)	➢ Recomendaciones de rutas de evacuación y puntos de reunión. ➢ Participación en simulacros.	Contingencia
Información y documentación	➢ Copias de seguridad. ➢ Procedimientos de recuperación. ➢ Documentación de activación del plan de continuidad.	

FUENTE: Cooperativa de Ahorro y Crédito San José Ltda.

Realizado por: Washington Vásquez, 2017

4.5.5 Implementación (desarrollo de la estrategia).

Sabiendo que los eventos de riesgo podrían afectar en corto tiempo (horas o días) significativamente a la operatividad de la institución, en el Anexo J se detalla el desarrollo de las estrategias que permiten la contingencia, recuperación o reanudación de la operaciones del negocio, considerando cada una de las instancias de ocurrencia del evento de riesgo: antes, durante y después de la materialización del evento.

4.5.6 Operación, Monitoreo y Mejora

El monitoreo del DRP permitirá obtener:

- Pruebas definidas y documentadas de las pruebas del DRP.
- Detalle de los cambios realizados en el DRP.
- La Verificación y Validación del cumplimiento de las políticas y estrategias establecidas para el DRP.
- La identificación y seguimiento de los cambios en los sistemas y proceso críticos de la entidad.

- La identificación de los cambios en la legislación aplicable a la Entidad.
- La revisión periódica del análisis de impacto BIA y de la evaluación de riesgos.
- Retroalimentación acerca del entendimiento que tiene el personal involucrado en la gestión del DRP con respecto a sus funciones y responsabilidades.
- Seguimiento a las acciones preventivas y correctivas.

a) AUDITORÍA DEL PLAN.

El propósito es detectar desviaciones en el DRP, con el fin de emitir recomendaciones de acuerdo a los estándares y mejores prácticas definidas.
La auditoría para el DRP debe contener métodos y técnicas que optimicen éste proceso. Algunas de ésta técnicas pueden ser la auto evaluación y la auditoría.

b) PRUEBA ESPECÍFICA.

Consiste en probar en una sola unidad o agencia un evento específico, entrenando al personal involucrado y basándose en los procedimientos definidos en la institución. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

c) PRUEBA DE ESCRITORIO.

Implica el desarrollo de un cuestionario de preguntas con el fin de averiguar el grado de conocimiento del personal involucrado en el mismo, el cuestionario deberá considerar lo siguiente:

- El banco de preguntas se basará en un formato específico preestablecido.
- Estará dirigido a todos los involucrados en el evento.
- Permitirá probar los conocimientos de los involucrados con respecto a su responsabilidad en el Plan.

Los ejercicios de escritorio serán ejecutados por el encargado de la prueba y el personal responsable de poner el Plan en Ejecución.

d) SIMULACIÓN EN TIEMPO REAL.

Las pruebas de simulación en tiempo real están dirigidas a una situación de contingencia por un período de tiempo definido, para lo cual se considerará:

- Las pruebas se harán en tiempo real.
- Se usará para probar partes específicas del Plan.
- Permitirá probar las habilidades coordinativas y de trabajo en equipo del personal asignado para afrontar contingencias.

ACTIVIDADES A REALIZAR EN LAS PRUEBAS.

Previo a realizar las pruebas se considerarán los siguientes aspectos:

- Verificar que el Plan de Recuperación de Desastres este aprobado por la alta dirección de la Institución.
- Revisar los planes de contingencia seleccionados para probar.
- Definir los eventos que serán sometidos a las pruebas.
- Verificar si se han asignado las respectivas responsabilidades.
- Establecer la fecha y la hora para la ejecución de la prueba.
- Definir el ambiente en donde se realizarán las reuniones del equipo de recuperación de contingencias.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
- Concientizar al personal que la meta es aprender y descubrir las vulnerabilidades, evitando generar fracaso y frustración.

4.5.6.1 ACTUALIZACIÓN (CICLO DE MEJORA CONTINUA).

El plan de continuidad de negocio debe ser mantenido a través de un ciclo de mejora continua, cualquier cambio a nivel organizativo (estratégico), operacional o técnico puede impactar en el negocio y por tanto en el plan de continuidad. Consecuentemente, la cooperativa debe emprender un proceso para mantener al día la capacidad, eficacia e idoneidad del plan de continuidad de negocio. Algunas propuestas en ese sentido son:

- Revisión periódica en busca de cambios en la estructura de la organización, en los productos/servicios que desarrolla, en la plantilla, etc., los cuales pueden tener consecuencias en el plan de continuidad de negocio (política, BIA, procedimientos de recuperación, etc.).
- Confirmación de que el plan de continuidad de negocio es acorde y contempla los citados cambios en los diversos componentes de la organización.
- Adecuación de los planes de continuidad de negocio a requerimientos de socios, clientes, u otro tipo de requerimientos regulatorios.
- Revisión de los resultados de las pruebas realizadas y de que las mejoras identificadas en las mismas han sido aplicadas.
- Incluso auditorías internas o externas de todos y cada uno de los componentes del plan de continuidad de negocio.

El objetivo fundamental del ciclo de mejora es asegurar que el Plan de Recuperación de Desastres se mantenga actualizado, completo, preciso y listo para sea ejecutado.

4.5.6.2 PRUEBAS DEL PLAN DE RECUPERACIÓN DE DESASTRES

Introducción

El Plan de Recuperación de Desastres, debe ser probado para demostrar su habilidad para mantener la continuidad de los procesos críticos de la Institución. Las pruebas se efectuarán anualmente a través de múltiples departamentos incluyendo las oficinas operativas.

Realizadas las pruebas se descubrirán elementos operacionales que requieren ajustes para asegurar el éxito en la ejecución del plan, de tal forma que dichos ajustes perfeccionen los planes establecidos.

Objetivo

Determinar si los procedimientos alternos de los procesos críticos considerados en el Plan de Recuperación de Desastres, proporciona la capacidad de respuesta de la Cooperativa frente a posibles eventos negativos que afecten su continuidad, en el antes, en el momento y después de concluido el hecho negativo

Procedimientos para las pruebas del Plan de Recuperación de Desastres

Se realizará dos niveles de pruebas:

- Pruebas en unidades departamentales en oficina Matriz.
- Pruebas en oficinas Operativas.

Métodos para realizar pruebas al Plan de Recuperación de Desastres

La Cooperativa ha definido tres métodos para realizar las pruebas al Plan de Recuperación de Desastres, las mismas que se detallan a continuación:

a) Prueba específica

Consiste en probar en un solo departamento y/o oficina operativa un evento específico, entrenando al personal involucrado y basándose en los procedimientos definidos en la institución. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

b) Prueba de escritorio

Implica el desarrollo de un cuestionario de preguntas con el fin de averiguar el grado de conocimiento del personal involucrado en el mismo, el cuestionario deberá considerar lo siguiente:

- El banco de preguntas se basará en un formato específico preestablecido.
- Estará dirigido a todos los involucrados en el evento.
- Permitirá probar los conocimientos de líderes y sublíderes que tiene mayor responsabilidad en el Plan.
- Los ejercicios de escritorio serán ejecutados por el encargado de la prueba y el personal responsable de poner el Plan en ejecución.

c) Simulación en Tiempo Real

Las pruebas de simulación en tiempo real están dirigidas a una situación de

contingencia por un período de tiempo definido, se evidencia un ejemplo en el Anexo I, para lo cual se considerará:

- Las pruebas se harán en tiempo real.
- Se usará para probar partes específicas del Plan.
- Permitirá probar las habilidades coordinativas y de trabajo en equipo del personal asignado para afrontar contingencias.

Actividades a realizar en las pruebas

Previo a realizar las pruebas se considerarán los siguientes aspectos:

- Verificar que el Plan de Recuperación de Desastres este aprobado por la alta dirección de la Institución.
- Revisar los planes de contingencia seleccionados para probar.
- Definir los eventos que serán sometidos a las pruebas.
- Verificar si se han asignado las respectivas responsabilidades.
- Establecer la fecha y la hora para la ejecución de la prueba.
- Definir el ambiente en donde se realizarán las reuniones del equipo de recuperación de contingencias.
- Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
- Concientizar al personal que la meta es aprender y descubrir las vulnerabilidades, evitando generar fracaso y frustración.

4.5.6.3 Mantenimiento del Plan de Recuperación de Desastres y revisiones

Las limitaciones y problemas observados durante las pruebas deben analizarse planteando alternativas y soluciones, las cuales luego de la presentación del informe respectivo serán actualizadas en el Plan de Recuperación de Desastres.

4.5.6.4 ACTUALIZACIÓN (CICLO DE MEJORA CONTINUA).

El plan de continuidad de negocio debe ser mantenido a través de un ciclo de mejora continua, cualquier cambio a nivel organizativo (estratégico), operacional o técnico

puede impactar en el negocio y por tanto en el plan de continuidad. Consecuentemente, la cooperativa debe emprender un proceso para mantener al día la capacidad, eficacia e idoneidad del plan de continuidad de negocio. Algunas propuestas en ese sentido son:

- Revisión periódica en busca de cambios en la estructura de la organización, en los productos/servicios que desarrolla, en la plantilla, etc., los cuales pueden tener consecuencias en el plan de continuidad de negocio (política, BIA, procedimientos de recuperación, etc.).
- Confirmación de que el plan de continuidad de negocio es acorde y contempla los citados cambios en los diversos componentes de la organización.
- Adecuación de los planes de continuidad de negocio a requerimientos de socios, clientes, u otro tipo de requerimientos regulatorios.
- Revisión de los resultados de las pruebas realizadas y de que las mejoras identificadas en las mismas han sido aplicadas.
- Incluso auditorías internas o externas de todos y cada uno de los componentes del plan de continuidad de negocio.

El objetivo fundamental del ciclo de mejora es asegurar que el Plan de Recuperación de Desastres se mantenga actualizado, completo, preciso y listo para sea ejecutado.

CAPÍTULO V

5. PROPUESTA

5.1 Identificación de Necesidades

Para identificar las necesidades de continuidad que tienen las Cooperativas de Ahorro y Crédito, se ha tomado como referencia la normativa de la Superintendencia de Bancos que consta en el libro I, título X, capítulo V de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria cuyos numerales se citan a continuación de acuerdo a la normativa (Junta Bancaria del Ecuador, 2014):

Tabla 1-5 Normativa

BASE LEGAL	REQUERIMIENTO	DRP
4.3.2.4 Procedimientos de respaldo de información periódicos, acorde a los requerimientos de continuidad del negocio que incluyan la frecuencia de verificación, las condiciones de preservación y eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesto a los mismos riesgos del sitio principal.	Procedimientos de respaldo de información	
4.3.4.3 Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio.	Procedimientos de continuidad para casos de migración de la plataforma tecnológica	
ARTÍCULO 6.- Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 4 del presente capítulo y adicionalmente, deberán contar […]; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de la información adecuada.	Pruebas de planes de contingencias y de continuidad del negocio	X
ARTÍCULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio.	Procedimientos actualizados para continuidad del negocio	X
Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya.	Proceso de administración de la continuidad basado en el estándar ISO 22301	X
15.1 La definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad.	Objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto	X

15.2 Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad.	Comité de continuidad del negocio	
15.3 Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.	Análisis de impacto en el negocio	X
15.4 Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos.	Análisis de riesgos	X
15.5 Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso.	Selección de estrategias de continuidad por proceso	
15.6 Realización de pruebas del Plan de Recuperación de Desastres que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una (1) vez al año.	Actualización periódica del Plan de Recuperación de Desastres	X
15.7 Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento.	Difusión del plan Entrenamiento Concienciación	X
15.8 Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continúa del Plan de Recuperación de Desastres.	Proceso de administración de la continuidad integrado al de administración integral de riesgos	
ARTÍCULO 16.- El Plan de Recuperación de Desastres debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente:	Inclusión de procedimientos operativos, tecnológicos, de emergencias y comunicaciones en el BCP	X
16.1 Escenarios de riesgos y procesos críticos cubiertos y alertas de los	Procesos críticos cubiertos y no	X

escenarios y procesos críticos no cubiertos por el plan	cubiertos por el plan	
16.2 Roles y responsabilidades de las personas encargadas de ejecutar cada actividad	Roles y responsabilidades	X
16.3 Criterios de invocación y activación del plan	Criterios de invocación y activación del plan	X
16.4 Responsable de su actualización	Responsable de su actualización	X
16.5 Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal	Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente	X
16.6 Tiempos máximos de interrupción y de recuperación de cada proceso	Tiempos máximos de interrupción y de recuperación de cada proceso	X
16.7 Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas o para el restablecimiento de los procesos críticos de manera urgente	Procedimientos de traslado de las operaciones a un sitio alterno	X
16.8 Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros)	Información vital y cómo acceder a ella	X
16.9 Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros)	Contactos de emergencia	X
16.10 Interacción con los medios de comunicación	Interacción con los medios de comunicación	
16.11 Comunicación con los grupos de interés	Comunicación con los grupos de interés	
16.12 Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno)	Establecimiento de un centro de comando	X
16.13 Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.	Procedimientos de restauración en un sitio alterno	X

Realizado por: Washington Vásquez, 2017

Como se puede observar en el cuadro anterior, existen algunos requisitos de continuidad establecidos por la normativa vigente que son aplicables total o parcialmente al DRP, y otros que son únicamente administrativos y por lo tanto deben encontrarse en el Plan de Recuperación de Desastres o en otros procedimientos de tecnología de la información.

Como se había mencionado anteriormente, el ciclo Plan-Do-Check-Act que sigue la norma ISO 22301 incluye las fases de planeación, establecimiento, implementación,

operación, monitoreo, revisión, ejercicios, mantenimiento y mejoramiento continuo del BCP. A continuación, se analizará el alcance de aplicación de cada requerimiento normativo relacionado con el DRP, indicando la fase de la norma ISO 22301 en la que deberá considerarse cada requerimiento normativo, de acuerdo a (Junta Bancaria del Ecuador, 2014):

Tabla 2-5 Fase de la norma ISO 22301

REQUERIMIENTO NORMATIVO	ALCANCE DE APLICACIÓN EN EL DRP	FASE DE LA ISO 22301
Pruebas de planes de contingencias y de continuidad del negocio	Pruebas periódicas del DRP	Ejercicios
Procedimientos actualizados para continuidad del negocio	Actualización periódica del DRP	Monitoreo, revisión
Proceso de administración de la continuidad basado en el estándar ISO 22301	DRP basado en ISO 22301	Planeación
Objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto	Procedimientos, metodología y presupuesto para implementar el DRP	Planeación
Análisis de impacto en el negocio	El DRP aplica a los procesos con mayor impacto en el negocio	Establecimiento
Análisis de riesgos	Análisis de riesgos del DRP	Establecimiento
Actualización periódica del Plan de Recuperación de Desastres	Actualización periódica del DRP	Revisión
Difusión del plan, entrenamiento, concienciación	Difusión y entrenamiento al personal que debe ejecutar el DRP	Revisión, ejercicios
Inclusión de procedimientos operativos, tecnológicos, de emergencias y comunicaciones en el BCP	Procedimientos operativos y tecnológicos para la recuperación de desastres	Implementación
Procesos críticos cubiertos y no cubiertos por el plan	Procesos críticos cubiertos y no cubiertos por el DRP	Establecimiento
Roles y responsabilidades	Roles y responsabilidades del DRP	Establecimiento
Criterios de invocación y activación del plan	Criterios de invocación y activación del DRP	Planeación
Responsable de su actualización	Responsable de la actualización del DRP	Planeación
Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente	Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el desastre	Implementación
Tiempos máximos de interrupción y de recuperación de cada proceso	El DRP debe atender los RPO y RTO de los procesos críticos	Establecimiento
Procedimientos de traslado de las operaciones a un sitio alterno	Procedimientos para recuperar los servicios de TI en un sitio alterno	Establecimiento
Información vital y cómo acceder a ella	Información de la infraestructura crítica y proveedores	Planeación
Contactos de emergencia	Contactos de emergencia del DRP	Establecimiento
Establecimiento de un centro de comando	Equipo de respuesta a incidentes	Operación
Procedimientos de recuperación en un sitio alterno	Procedimientos de recuperación de servicios	Planeación

	críticos en un sitio alterno	

Realizado por: Washington Vásquez, 2017

Los requerimientos normativos con el alcance antes indicado deberán estar contenidos en el DRP a fin de satisfacer las necesidades de continuidad del negocio, lo que permitirá a su vez dar cumplimiento a la normativa vigente.

5.2 Selección de la Metodología

Para el desarrollo de este proyecto investigativo se ha decidido trabajar con la siguiente metodología para realizar el DRP para los sistemas de información críticos de TI, proponiendo desde el inicio del proyecto hasta la realización de pruebas los análisis de riesgos, estrategias de recuperación, roles y responsabilidades, La figura 3.1, presenta las fases de esta metodología, basada en las recomendaciones de la normativa ISO 22301, los requerimientos de la norma sobre Riesgo Operativo y apoyada en la experiencia de casos prácticos realizados en nuestro país:

Figura 1-5: Esquema General del Proceso
FUENTE: Ing. KATALINA CORONEL HOYOS

Las fases antes indicadas, así como las actividades a realizar en cada una de ellas, se detallan a continuación, considerando para este efecto la equivalencia de términos entre la metodología indicada y la norma ISO 22301:

Tabla 3-5 Metodología a utilizar

NORMA ISO 22301	METODOLOGÍA
Planeación	Planificación
Establecimiento	BIA Análisis de Riesgo Estrategia
Implementación	Implementación
Operación	Operación
Monitoreo	Monitoreo y Mejora
Revisión	Monitoreo y Mejora
Ejercicios	Operación
Mantenimiento	Monitoreo y Mejora
Mejoramiento Continuo	Monitoreo y Mejora

Realizado por: Washington Vásquez, 2017

5.2.1 Planificación

Considerar los objetivos, políticas y estrategias de continuidad establecidos en el Plan de Recuperación de Desastres institucional

- Objetivo
- Alcance
- Responsables
- Metodología

5.2.2 Análisis de Impacto en el Negocio (BIA)

- Procesos Críticos (Cadena de Valor).
- Impacto (Económico, Operacional, Reputacional, Legal).
- Identificación del MTD (Ventana máxima de interrupción).
- Determinación de RTO y RPO (Tiempo objetivo de recuperación y Punto objetivo de recuperación).

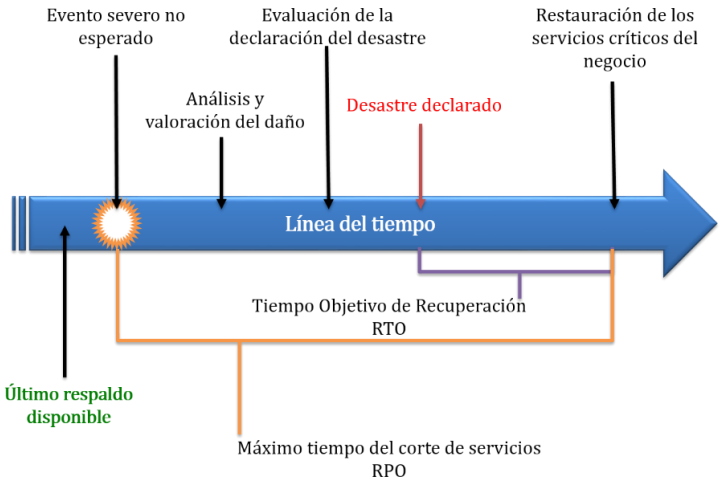

Figura 2-5: Análisis de líneas de Tiempo
FUENTE: TECSERVIN

5.2.3 Análisis del Riesgo

- Identificación de Activos (procesos, información, equipos, personal).
- Valoración de Activos (dependencia, uso, seguridad).
- Riesgo Inherente (Amenazas, vulnerabilidades, controles existentes)
- Riesgo Residual (Probabilidad, Impacto, Nivel de riesgo, respuesta reputacional).

5.2.4 Estrategia

- Dueño del Riesgo.
- Análisis de la estrategia de respuesta.
- Aprobación (DRP).

5.2.5 Implementación

- Diseño (Procedimientos, Responsables, Configuración).
- Presupuesto (Adquisiciones).
- Pruebas (Comités, Seguimiento)

5.2.6 Operación

- Concientización (Campañas, Entrenamiento).
- Respuesta (Recuperación, Resultados, Lecciones aprendidas).

- Gestión de Cambios (Adecuación, Actualización).

5.2.7 Monitoreo y Mejora

- Concientización (Campañas, Entrenamiento, Personal Nuevo).
- Pruebas (Cambios en procesos de negocio, Nuevas Oficinas y productos, Pruebas Anuales, Auditoría).
- Gestión de Cambios (Adecuación y Ajustes, Alineamiento estratégico).

CONCLUSIONES

Finalizado el trabajo de investigación se concluye lo siguiente:

- Se realizó revisiones de varios estándares, modelos y buenas prácticas que se aplican a la recuperación de desastres, determinado que la normativa a utilizar se base en el estándar internacional ISO 22301:2012, el cual nos ayudó a minimizar el riesgo ante incidentes informáticos no esperados.
- El estándar internacional ISO 22301:2012 se acopla a las necesidades de una Institución Financiera como lo es la Cooperativa de Ahorro y Crédito San José Ltda., su flexibilidad y adaptación fue muy importante ya que no importa el tamaño o la actividad económica que realiza para su implementación, lo cual permitió la culminación del Plan de Recuperación de Desastres.
- El diseño y desarrollo del método DRP basado en el estándar internacional ISO 22301:2012, facilito a que se pueda implementar en la Cooperativa de Ahorro y Crédito San José Ltda., sin ningún inconveniente para garantizar la continuidad de sus operaciones críticas.
- Se identificó que las Cooperativas de Ahorro y Crédito del Ecuador necesitaban la implementación de un DRP para continuidad de sus operaciones, para cumplir con normativas vigentes de los entes de control como es la Superintendencia de Bancos y Seguros.
- Se determina que la implementación de un método de aplicación general para el desarrollo de un Plan de Recuperación de Desastres, se puede implementar en cualquier institución financiera a la cual regule el mismo ente de control y utilice la misma normativa, para este caso de investigación se implementó en la Cooperativa de Ahorro y Crédito San José Ltda., para satisfacer las necesidades de continuidad que la misma tenía.
- Este trabajo de investigación se realiza en conjunto con el personal de TI de la COOPERATIVA DE AHORRO Y CRÉDITO SAN JOSÉ LTDA, y se ha concluido exitosamente. Por lo que se implementó y se encuentra trabajando teniendo el aval del Gerente General de la misma institución.

RECOMENDACIONES

- Socializar el plan de recuperación de desastres a todos los departamentos de la institución para que sepan qué medidas correctivas que se puedan tomar antes de ejecutar el plan, dándoles una idea más clara y de prevención ante incidentes o desastres que puedan presentarse.
- Realizar un programa de capacitación para el personal encargado de cada área para que adquieran las habilidades y conocimientos básicos sobre la recuperación de desastres y su continuidad, garantizando estar preparados en una situación de emergencia.
- Realizar convenios de alianzas estratégicas entre Cooperativas o a través de las redes con las cuales ya trabajan a fin de que puedan compartir infraestructura tecnológica por temas de economía de escala, lo cual ayudará a tener tecnología de punta disponible ante cualquier incidente no esperado.
- Realizar por lo menos una prueba anual del Plan de Recuperación de Desastres y actualizarlo cuando existan cambios de normativa o de procesos, a fin de corregir posibles errores que se puedan presentar.
- Implementar servidores virtualizados de los servicios críticos con el objetivo de poder tener disponibles sus imágenes cuando se presente algún evento de riesgo, garantizando la continuidad de las operaciones.

GLOSARIO.

Se define algunos conceptos que es necesario conocerlos de acuerdo («MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO», 2013)

Activo.- Algo a lo que la institución directamente le asigna valor, y por lo tanto se debe proteger. Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de la institución y son generadores de renta, o fuente de beneficios como: bienes, inversiones, cuentas por cobrar, inmuebles, instalaciones, maquinarias, etc.

Administración de Riesgos.- Actividades coordinadas para guiar y controlar una organización con respecto al riesgo. Incluye valoración, tratamiento, aceptación y comunicación de riesgos.

Administración del Plan de Continuidad de Negocios: Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio.

Amenaza.- Es la causa potencial de un incidente no deseado, podría ser perjudicial para una organización.

Amenaza: Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.

Análisis de Impacto del Negocio (BIA): Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.

Análisis de Riesgo.- Sistemático uso de información para identificar fuentes y estimar el riesgo, busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo, abarca las personas, procesos de negocios, tecnología e infraestructura.

Confidencialidad.- Definida como lo que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas, con reserva e intimidad; garantizando que sea accesible sólo aquellas personas autorizadas a tener acceso a ella.

Contingencia: evento que interrumpe la continuidad de los sistemas, con consecuencias catastróficas para el negocio; sólo puede reducirse por medios extraordinarios y en general muy costosos, organizativa y técnicamente.

Continuidad: se refiere al negocio (a sus funciones); requiere la disponibilidad de la información y por tanto de los sistemas que la tratan y su entorno (suministros, etc.)

Control de Riesgo.- Proceso que busca asegurar que las políticas, límites, y procedimientos para el tratamiento de riesgos sean apropiadamente tomados y/o ejecutados, buscan la eficacia y eficiencia de las operaciones de la cooperativa, la confiabilidad de la información financiera u operativa, interna y externa, así como el cumplimiento de las disposiciones legales que le sean aplicables.

Control: Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.

Disponibilidad.- La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso explotadas por una o más amenazas.

Factores Críticos de Éxito (FCE).- Son factores que describen aquellas actividades que son necesarias de ejecutar o de realizar exitosamente para que la Misión se cumpla.

Frecuencia: Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.

Gestión de Riesgo.- Conjunto de procesos efectuados por el Consejo de Administración, la gerencia, los funcionarios y los trabajadores de la cooperativa, destinados a proveer una seguridad razonable sobre el logro de los objetivos de la institución, está diseñada para desarrollar una adecuada determinación de objetivos, implementar una oportuna identificación, evaluación, tratamiento y control de riesgos, elaborar los reportes pertinentes y efectuar un adecuado monitoreo.

Identificación de Riesgo.- Proceso por el que se determinan los eventos internos y externos, que puedan tener un impacto negativo sobre los objetivos de la institución.

Impacto: Es el efecto que causa la ocurrencia de un incidente o siniestro, la implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación

Incidencia/Interrupción: evento que interrumpe la continuidad de los sistemas, con consecuencias limitadas para el negocio; puede reducirse por medios razonables y disponibles.

Incidente de la Seguridad de la Información.- Un incidente de la seguridad de la información, en un o una serie de eventos inesperado relacionado con la integridad, disponibilidad y confiabilidad de la información, que tienen probabilidad significativa de comprometer operaciones comerciales y amenazar la seguridad de la información.

Incidente de Trabajo: Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.

Información.- Cualquier forma de registro electrónico, óptico, magnético, o en otros medios, susceptible de ser procesada, distribuida y almacenada.

Integridad.- Es la garantía que una información sea y permanezca confiable, completa y exacta, dado que la misma no ha sido alterada borrada o reorganizada.

Monitoreo de Riesgo.- Proceso que consiste en la evaluación de la existencia y el adecuado funcionamiento del sistema de gestión integral de riesgos.

Objetivo de Control.- Una declaración del propósito o resultado deseado, mediante la implementación de controles apropiados.

Plan de Continuidad de Negocio (BCP).- Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción1.

Plan de Recuperación de Desastres (DRP).- Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

Planes de contingencia.- Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Política.- Toda intención y dirección formalmente expresada por la institución.

Proceso Crítico.- Proceso considerado indispensable para la continuidad de las operaciones y servicios de la entidad.

Proceso.- Conjunto de actividades, tareas, procedimientos organizados y repetibles.

Riesgo de Operación.- Entiéndase por riesgo de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencia o fallas en los procesos internos, la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

Riesgo de Tecnología de Información.- Los riesgos de operación asociados a los sistemas informáticos y a la tecnología relacionada a dichos sistemas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la entidad al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Riesgo inherente.- Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles.

Riesgo residual.- Riesgo remanente tras la aplicación de controles.

Riesgo.- Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad.

Riesgo: Es la probabilidad de que se produzca un impacto determinado en un activo. El análisis del riesgo permite, en conjunto con la vulnerabilidad y el impacto ambos derivados a su vez de las relación del activo y la amenaza, calcular si dicho riesgo es asumible o aceptable.

Tratamiento de Riesgo.- Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de Riesgos.- Todo proceso de análisis de riesgos y evaluación de riesgos.

Vulnerabilidad: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.

CCN.- Comité de Continuidad del Negocio

DRP.- Plan De Recuperación De Desastres

SBS.- Super Intendencia De Bancos Y Seguros

SEPS.- Super Intendencia De La Economía Popular Y Solidaria

FCE.- Factores Críticos Del Éxito

CORE.- Programa Financiero Principal De La Cooperativa

DRP (Disaster Recovery Plan, Plan de Recuperación de Desastre).

BCP (Bussiness Continuity Planning, Plan de Continuidad de Negocios).

BIA (Business Impact Analysis, Análisis del Impacto al Negocio).

AR (Risk Analysis, Análisis de Riesgo).

RPO (Recovery Point Objective, Objetivos de Punto de Recuperación).

PIN (Probabilidad de Impacto al Negocio).

ERA (Environment Risk Analisys, Análisis de Riesgos Ambientales).

RAS (Alternative and Solutions, alternativas y soluciones).

RTO(Recovery Time Objetive, Tiempo Objetivo de Recuperación)

BIBLIOGRAFIA

GASPAR, J., & MARTÍNEZ, J. G. (2004). *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones*. Ediciones Díaz de Santos.

GLOSARIO | SPANISHPMO. (s. f.). Recuperado 23 de febrero de 2017, a partir de http://spanishpmo.com/index.php/glosario/?l=a

INTELCO. (s. f.). *Plan de continuidad*. Recuperado a partir de http://es.calameo.com/read/001441005dcf633ec43ac

ECUADOR. JUNTA BANCARIA DEL ECUADOR. (2014, septiembre 2). Resolución jb-2014-3066, junta bancaria. Recuperado a partir de http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/2014/resol_JB-2014-3066.pdf

LÓPEZ, P. A. (2011). *Introducción a la seguridad informática (Seguridad informática)*. Editex. Recuperado a partir de http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO. (2013). Recuperado a partir de http://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf

NORMA ISO 22301, Continuidad del Negocio - G4A. (s. f.). Recuperado 29 de marzo de 2016, a partir de https://www.g4a.mx/norma-iso-22301-continuidad-del-negocio/

ORGANIZACIONALES 06 01 OBJETIVOS DE COSTOS TIEMPO Y ALCANCE - BI - 01. (s. f.). Recuperado 8 de febrero de 2017, a partir de https://www.coursehero.com/file/p6o37nt/Organizacionales-06-01-Objetivos-de-costos-tiempo-y-alcance-inconsistentes-06/

PEÑA GERÓNIMO. (2014). revista ingeniería en redes y telecomunicaciones, *1*. Recuperado a partir de http://revistas.ipl.edu.do/index.php/RedesTelecomunicaciones/article/view/Art%203

PLAN DE CONTINUIDAD DEL NEGOCIO. (s. f.). Recuperado 23 de febrero de 2017, a partir de http://www.bconsultores.com/index.php?option=com_content&view=article&id=31&Itemid=80

QUE ES GOBIERNO TI? | Gobierno TI. (s. f.). Recuperado 28 de marzo de 2016, a partir de https://gobiernoti.wordpress.com/2011/06/19/gobierno-ti/

¿QUÉ ES NORMA BS 25999? | 27001ACADEMY. (s. f.). Recuperado 28 de marzo de 2016, a partir de http://advisera.com/27001academy/es/what-is-bs-25999/

¿QUÉ ES NORMA ISO 22301? | 27001ACADEMY. (s. f.). Recuperado 31 de octubre de 2016, a partir de http://advisera.com/27001academy/es/que-es-iso-22301/

¿QUÉ ES UN DRP? (s. f.). Recuperado 28 de marzo de 2016, a partir de http://www.inbest.me/comunidad/que-es-un-drp

ECUADOR. SUPERINTENDENCIA DE BANCOS Y SEGUROS. (2014a, septiembre 2). Normas generales para las instituciones d el sistema financiero, capitulo i.- de la gestión integral y control de ri esgos. Recuperado a partir de http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_I.pdf

ECUADOR. SUPERINTENDENCIA DE BANCOS Y SEGUROS. (2014b, septiembre 2). NOrmas generales para las instituciones del sistema financiero, capítulo v.- de la gestión del riesgo operativo. Recuperado a partir de http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

VILLEGAS DE LA CRUZ, MARCIA MARINA. (2013, julio 2). *Sistema de gestión para la continuidad del negocio que garantice a la Cooperativa de Ahorro y Crédito Atuntaqui Ltda. La capacidad de operar en forma continua y minimizar las pérdidas ante la ocurrencia de eventos de riesgo.* (Postgrado). Universidad Tecnica del Norte. Recuperado a partir de

http://repositorio.utn.edu.ec/bitstream/123456789/1260/1/PG%20337_PLAN%20DE%20CONTINUIDAD%20DE%20NEGOCIO.pdf