# UNIVERSIDAD TÉCNICA DE AMBATO


## FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRONICA E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

**Tema:** "DISEÑO DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL SEGMENTO 1 DEL CANTON AMBATO"

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

**Autora:** Ing. Susana del Pilar Ibarra Canseco
**Director:** Ing. David Omar Guevara Aulestia, Mg.

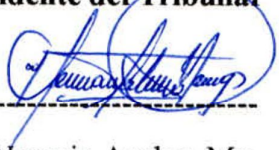
Ambato – Ecuador
2019

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia, Mg., e integrado por los señores Ingeniero Hernán Fabricio Naranjo Avalos, Mg., Ing. Edwin Hernando Buenaño Valencia, Mg. designados por la Unidad Académica de Titulación de Posgrado de la Facultad de Ingeniería en sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "DISEÑO DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL SEGMENTO 1 DEL CANTÓN AMBATO", elaborado y presentado por la señora Ingeniera Susana del Pilar Ibarra Canseco, para optar por el Grado Académico de Magister en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing., Elsa Pilar Urrutia Urrutia, Mg.

**Presidente del Tribunal**



Ing., Hernán Fabricio Naranjo Avalos, Mg.

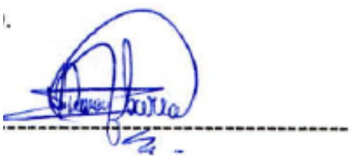
**Miembro del Tribunal**

Ing. Edwin Hernando Buenaño Valencia, Mg

**Miembro del Tribunal**

## AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "Diseño del plan de contingencia y continuidad del negocio para cooperativas de ahorro y crédito del segmento 1 del cantón Ambato", le corresponde exclusivamente a: Ing. Susana del Pilar Ibarra Canseco, Autora bajo la Dirección de Ing. David Omar Guevara Aulestia, Mg., Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



---

Ing. Susana del Pilar Ibarra Canseco

c.c.1803624210

AUTORA

Ing. David Omar Guevara Aulestia, Mg.

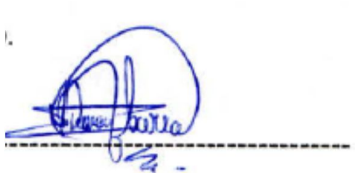
c.c.1802605749

DIRECTOR

## DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.



---

Ing. Susana del Pilar Ibarra Canseco

c.c.1803624210

## INDICE GENERAL DE CONTENIDOS

## ÍNDICE DE FIGURAS

## ÍNDICE DE TABLAS

## AGRADECIMIENTO

Agradezco en primer lugar a Dios y a la Virgen de la Elevación por bridarme su bendición, los siento presentes en cada día de mi vida.

A la Cooperativa Cámara de Comercio de Ambato que me abrió las puertas y me permitió desarrollar este trabajo de investigación.

A mi Director de tesis, por compartir su conocimiento y ser guía para el desarrollo de este trabajo.

## DEDICATORIA

A mi madre que guía cada paso de mi vida y con amor me apoya incondicionalmente.

A mi amado esposo y mis hijos que son la felicidad de mi vida.

**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO**
**MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN**

**TEMA:**

"DISEÑO DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL SEGMENTO 1 DEL CANTON AMBATO"

**AUTOR:** Ing. Susana del Pilar Ibarra Canseco

**DIRECTOR:** Ing. David Omar Guevara Aulestia, Mg.

**FECHA:** Octubre de 2019

## RESUMEN EJECUTIVO

Las instituciones financieras ecuatorianas en la actualidad tienen la obligación de garantizar la disponibilidad de los servicios a sus socios, tanto por disposiciones legales de entes de control como por la necesidad de sobrevivir frente a la abundante competencia del mercado. El departamento de Tecnología de la Información (TI), es esencial en las instituciones financieras para el normal desarrollo de los procesos críticos. Todos los procesos están necesariamente apoyados en los sistemas de información y de comunicación.

Por lo tanto, crece la necesidad de identificar y analizar los riesgos que afectan a los procesos; permitiendo a las instituciones estimar el impacto operacional y financiero de las interrupciones, este análisis provee una base para identificar los procesos críticos de la organización y priorizarlos de acuerdo con su nivel de impacto, identificar cuáles impulsan el negocio, cuáles generan ingresos y cuáles son indispensables para mantenerse operativo. Para garantizar la continuidad del negocio, se debe establecer controles que permitan mitigar los riesgos o tomar el control de los mismos, y finalmente establecer un plan que permita reanudar los servicios inmediatamente luego de una interrupción cumpliendo con los tiempos y puntos objetivos de recuperación aprobados por la alta dirección. Los procesos que permitan guiar las acciones a realizarse en momentos de crisis deben ser claros y precisos de tal manera que reduzcan el nivel de incertidumbre y el uso innecesario de recursos, para ello deben basarse en metodologías y estándares internacionales que aseguren la eficacia de su aplicación. En su mayoría las empresas realizan este proceso de forma empírica, sin estudios previos y sin documentación que certifique su existencia y conocimiento por parte de los interesados. El estándar ISO 22301:2014 que tiene por nombre "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio", propone los lineamientos base para diseñar un completo plan de contingencia y continuidad del negocio.

**Descriptores:** riesgos, servicios financieros, procesos críticos, ISO 22301, metodología, tiempo, recursos, contingencia, continuidad, plan, tecnología.

**UNIVERSIDAD TÉCNICA DE AMBATO**

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO**
**MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN**

**THEME:**

"DISEÑO DEL PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO PARA COOPERATIVAS DE AHORRO Y CRÉDITO DEL SEGMENTO 1 DEL CANTON AMBATO"

**AUTHOR:** Ing. Susana del Pilar Ibarra Canseco

**DIRECTED BY:** Ing. David Omar Guevara Aulestia, Mg.

**DATE:** October 2019

## EXECUTIVE SUMMARY

Ecuadorian financial institutions currently have the obligation to guarantee the availability of services to their partners, both by legal provisions of control entities and by the need to survive in the face of abundant market competition. The Information Technology (IT) department is essential in financial institutions for the normal development of critical processes. All processes are necessarily supported by information and communication systems.

Therefore, the need to identify and analyze the risks that affect the processes grows; allowing institutions to estimate the operational and financial impact of interruptions, this analysis provides a basis for identifying the critical processes of the organization and prioritizing them according to their level of impact, identifying which drives the business, which generate revenue and which are indispensable to stay operational.

To ensure business continuity, controls must be established to mitigate the risks or take control of them, and finally establish a plan that allows services to resume immediately after an interruption, complying with the recovery time and objective points approved by the high direction. The processes that allow guiding the actions to be carried out in times of crisis must be clear and precise in such a way that they reduce the level of uncertainty and the unnecessary use of resources, for this they must be based on international methodologies and standards that ensure the effectiveness of their application. For the most part, companies carry out this process empirically, without previous studies and without documentation that certifies their existence and knowledge by interested parties. The ISO 22301: 2014 standard whose name is "Company Security: Business Continuity Systems", proposes the basic guidelines to design a complete contingency and business continuity plan.

**Keywords:** risks, financial services, critical processes, ISO 22301, methodology, time, resources, contingency, continuity, plan, technology.

# INTRODUCCIÓN

La información en sí es de importancia creciente, se transmite y almacena en sistemas de información soportados por tecnología que está expuesta a sucesos generales que pueden generar su interrupción. Por ello las entidades deben contar con medios que puedan garantizar la continuidad de los sistemas y del negocio o servicio.

La previsión no se debe limitar a entidades con ánimo de lucro sino abarcar entidades de todo tipo, tanto públicas como privadas, y de cualquier sector de actividad. Un Plan de contingencia y continuidad del negocio es conveniente para evitar que en el caso de un problema grave la entidad haya terminado su actividad para siempre o sufrido un daño importante.

Dentro de la seguridad, la continuidad ha sido con frecuencia lo más difícil y lo más caro. No obstante, esto está cambiando y en muchas de las entidades la continuidad ya constituye una preocupación, y a veces el plan un objetivo estratégico, porque si la entidad no llega a implantar las medidas necesarias está poniendo en riesgo su permanencia en el mercado.

El CAPÍTULO I EL PROBLEMA DE INVESTIGACIÓN abarca toda la definición del problema desde el tema de investigación, planteamiento, contextualización, análisis crítico, prognosis, formulación del problema, interrogantes, unidades de observación, justificación y objetivos.

El CAPÍTULO II MARCO TEÓRICO establece la fundamentación de la investigación con antecedentes, base legal, base filosófica, señalización de variables dependiente e independiente y el establecimiento de la hipótesis.

El CAPÍTULO III METODOLOGÍA detalla la forma en la que llevará a cabo la investigación enfoque, modalidad básica, tipo, población y muestra,

operacionalización de variables, recolección, procesamiento y análisis de información.

El CAPÍTULO IV, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS analiza los resultados de la encuesta aplicada, tabulando e interpretando las respuestas.

El CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES resume las principales conclusiones del problema tema de investigación y establece las posibles soluciones.

El CAPÍTULO VI PROPUESTA desarrolla paso a paso la solución para el problema de investigación.

# CAPÍTULO I

## 1. EL PROBLEMA DE INVESTIGACIÓN

### 1.1 Tema de Investigación

Diseño del plan de contingencia y continuidad del negocio para cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

### 1.2 Planteamiento del Problema

#### 1.2.1 Contextualización

La continuidad del negocio se ha convertido en un área de preocupación a nivel mundial cada vez más común, desde el atentado del WorldTrade Center de Nueva York en septiembre de 2011, incidente completamente imprevisto que creó una amenaza grave y repentina para las funciones esenciales de varias empresas. En este sentido, las Normas *ISO 22301:2012 Protección y seguridad de los ciudadanos-Sistema de Gestión de la Continuidad del Negocio-Requisitos* e *ISO 22313:2012 Protección y seguridad de los ciudadanos-Sistema de Gestión de la Continuidad del Negocio-Directrices,* ayudan a las organizaciones a gestionar este aspecto. Desde la publicación de estas normas internacionales ha ido creciendo su importancia en el ámbito mundial tanto en empresas de Tecnologías de la Información y Comunicaciones (TIC) como en todas aquellas que dependen, en mayor o menor medida, de dichas tecnologías; la banca es un buen ejemplo de ellas. (García Mariblanca,2015)

En el Ecuador la Superintendencia de Bancos y Seguros (SBS) y la Superintendencia de Economía Popular y Solidaria (SEPS) han emitido varias Recomendaciones relativas a la contingencia y continuidad del negocio, instando a que ésta debe formar parte de la gestión del riesgo operacional de una entidad financiera.

Las Cooperativas de ahorro y crédito son instituciones cuyo mercado objetivo es el Sector popular y solidario; cuentan con un nivel de activos inferior al de las Instituciones bancarias. Sin embargo, ofrecen la misma gama de servicios.

Actualmente están implementando los canales electrónicos exigidos por las necesidades del consumidor. Entre estos servicios constan la atención en ventanilla compartida, cajeros automáticos, banca en línea y banca móvil.

La SEPS controla la actividad financiera de las cooperativas de ahorro y crédito del Ecuador; establece exigencias, mediante normativas, para que las cooperativas garanticen la continuidad del negocio frente a cualquier incidente (SEPS,2017). La inobservancia o desacato de estas normativas son objeto de sanción a las instituciones, a los directivos y a los responsables de TI.

En el ámbito de esta investigación se considera que la disponibilidad de la información es un factor crítico en el sector financiero. La suspensión de los servicios de una institución financiera puede ser provocada por agentes externos o internos de la institución. Entre los agentes externos se tienen los ataques como suplantación de identidad, denegación de servicio, robo y encriptación de información, penetración en servidores publicados, inyección sql, etc. Los agentes internos están dados por la falta de una cultura preventiva en el departamento de TI (Tecnología de la Información) que no cuenta con adecuados procesos que garanticen la alta disponibilidad de la información. En los dos casos se evidencia la falta de planificación de la gerencia de TI para la contingencia y continuidad del negocio.

Según Villavicencio, el 90% de cooperativas del Ecuador no han podido cumplir con los requisitos que garanticen la alta disponibilidad de los servicios que prestan, debido a diferentes aspectos como:

- Cultura reactiva en lugar de preventiva en el personal de TI.
- Falta de conocimiento y apoyo de la alta gerencia.

- Falta de planificación de la gerencia de TI para la contingencia y continuidad del negocio.
- No se dispone de un presupuesto adecuado para TI que permita implementar soluciones acorde a las necesidades del negocio.(Villavicencio,2016)

En general, en el Ecuador no se maneja una cultura preventiva frente a incidentes informáticos; por esta razón es muy importante iniciar un arduo trabajo para fomentar la planificación que garantice la continuidad del negocio y que permita que el negocio este siempre operativo.

### 1.2.2 Análisis Crítico

Si una cooperativa de ahorro y crédito trabaja sin un plan de contingencia y continuidad del negocio está expuesta a que cualquier evento interrumpa sus servicios. La realidad es que cualquier organización puede ser afectada por un suceso que interrumpa sus servicios pero depende de su capacidad de control y reacción el impacto que cause en el negocio. No sólo están expuestas a catástrofes ambientales, tales como incendios, terremotos o inundaciones, también pueden causar grandes daños los incidentes de seguridad en los sistemas, como delitos cibernéticos, robo de información sensible, daños en las infraestructuras y en los servicios, o fallos en el suministro eléctrico. Los desastres pueden ocurrir en cualquier momento y sus consecuencias sobre las organizaciones que no están preparadas pueden llegar a ocasionar incluso el cierre de las mismas.

Aunque el efecto inmediato parece ser la pérdida económica, hay otros efectos derivados que pueden causar un gran impacto en la institución como el desgaste de su reputación o la pérdida de ventaja competitiva frente a otras cooperativas.

Esperar a que suceda un incidente para buscar una alternativa de solución es crítico y de alto impacto. La cultura actual del departamento de TI de las cooperativas tiene una actitud reactiva en lugar de proactiva. La mayoría de gerentes de TI trabajan para el día a día, no se preocupan por planificar su respuesta ante incidentes o desastres basándose en estándares internacionales.

Otras instituciones realizan el levantamiento de estos planes, pero no les dan el tratamiento respectivo. Los planes deben ser probados, evaluados y actualizados constantemente de acuerdo con el desarrollo institucional, disponibilidad de recursos y cambios de factores externos a la organización.

### 1.2.3 Prognosis

De no instrumentar un plan de contingencia y continuidad del negocio, los principales procesos de la cooperativa sentirán la inoperancia del departamento de TI. La institución estará en riesgo, expuesta a problemas como servicios constantemente interrumpidos y pérdida o alteración de información. Esto generará pérdidas económicas para la institución, deserción de socios y deterioro de la imagen institucional.

### 1.2.4 Formulación del Problema

¿ El diseño del plan de contingencia y continuidad del negocio mejoraría la disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato,?

### 1.2.5 Interrogantes (Subproblemas)

- ¿Cuáles son los instrumentos aplicados actualmente para enfrentar incidentes informáticos que ocasionan la interrupción del servicio de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato?

- ¿Cuáles son las necesidades y requerimientos de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato para garantizar la disponibilidad de los servicios financieros?

- ¿Se puede diseñar un plan de contingencia y continuidad del negocio que mejore la disponibilidad de los servicios financieros de la Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda.?

### 1.2.6 Delimitación del objeto de investigación

**Campo:** Financiero cooperativo.

**Área:** Tecnologías de la Información y de la Comunicación.

**Aspecto:** Diseño del plan de contingencia y continuidad del negocio.

#### 1.2.6.1 Delimitación Espacial:

Cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

#### 1.2.6.2 Delimitación Temporal:

De junio a agosto 2019

#### 1.2.6.3 Unidades de Observación:

Procesos críticos de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

## 1.3 Justificación

Un plan de contingencia y continuidad no es simplemente recuperación ante desastres, gestión de crisis, gestión de riesgos o recuperación tecnológica. Es reconocido como una buena práctica profesional y de gobierno de TI, y es parte integral del buen gobierno de las organizaciones. De esta forma, toma una dimensión estratégica. Es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para construir y reforzar la capacidad de dar una respuesta efectiva que salvaguarde los intereses y la imagen institucional.

Crea el marco estratégico y operativo para revisar, y modificar cuando sea necesario, la forma en que la organización proporciona sus productos y servicios, al mismo tiempo que aumenta su resistencia frente a interrupciones o pérdidas.

Para la Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato el poder contar con un plan de contingencia y continuidad del negocio le permite optimizar el uso de sus recursos, responder de manera oportuna a incidentes, tener su servicio en línea el mayor tiempo posible. Fidelizar a sus clientes por la calidad de sus servicios y fortalecer su imagen institucional.

Por lo antes expuesto, se observa que el presente proyecto de investigación es de interés para la Cooperativa y para el departamento de TI, que buscan mantener sus servicios en línea el mayor tiempo posible, lo cual incide en que el mismo sea factible de realizar al disponer de los recursos necesarios para el cumplimiento de los objetivos.

**Factibilidad Técnica:**

Se puede decir que técnicamente es realizable pues se tiene acceso a la infraestructura, herramientas tecnológicas, sistemas e información necesaria.

**Factibilidad Operativa:**

El proyecto tiene factibilidad operativa porque tiene el consentimiento y aprobación de la administración así como de la dirección de TI, directores departamentales y jefes de agencia, lo cual permite tener la apertura necesaria con el personal de la Cooperativa para obtener información y garantiza que los resultados serán de beneficio y utilidad.

**Factibilidad Económica:**

Se puede mencionar que económicamente el presente proyecto es factible ya que no generará inversión en tecnología o uso de recursos extras de la institución, únicamente implica el tiempo y trabajo del investigador y la colaboración del personal involucrado de la institución que está autorizado por la Cooperativa.

## 1.4 Objetivos

### 1.4.1 Objetivo General

Diseñar el plan de contingencia y continuidad del negocio para mejorar la disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento 1 del cantón Ambato.

### 1.4.2 Objetivos Específicos:

- Identificar los instrumentos aplicados actualmente para enfrentar incidentes informáticos que ocasionan la interrupción del servicio de las cooperativas de ahorro y crédito del segmento 1 del cantón Ambato.

- Determinar las necesidades y requerimientos de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato para garantizar la disponibilidad de los servicios financieros.

- Proponer el diseño del plan de contingencia y continuidad del negocio que mejore la disponibilidad de los servicios financieros de la Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda.

# CAPITULO II

## 2. MARCO TEÓRICO

### 2.1 Antecedentes de Investigativos

Martínez, en el año 2004 en Europa, realizó una investigación acerca de los "*Planes de contingencia: la continuidad del negocio en las organizaciones", en donde textualmente dice:* "El desarrollo e implantación de un Plan de Continuidad de Negocio es 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." Concluye su investigación asegurando que su desarrollo, implementación y mantenimiento propiciará a la organización los beneficios siguientes, en caso de posibles interrupciones" (Martínez, 2004):

- Minimizar las potenciales pérdidas económicas.
- Reducir riesgos potenciales.
- Reducir las probabilidades de que ocurran interrupciones.
- Reducir interrupciones en las operaciones.
- Asegurar la estabilidad de la organización.
- Facilitar una recuperación ordenada.
- Minimizar las primas de seguros.

Al realizar una búsqueda bibliográfica en el repositorio de la Universidad Técnica de Ambato, se encontró que en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial existe un trabajo relacionado, pero desde un enfoque diferente al planteado, el cual se cita a continuación:

Según David Cruz y David Guevara, en el año 2018, en la investigación "Plan de riesgos y contingencias informáticas basado en un acuerdo de nivel de servicio

aplicada a la Empresa Plasticaucho Industrial", en la que analiza la seguridad de las unidades informáticas, mencionan: Las instituciones requieren garantizar la continuidad del servicio en el tiempo, de ahí surge la necesidad de salvaguardar la integridad de su información ante los posibles riesgos. Señala conceptos necesarios para entender la metodología, describe estándares para la gestión de riesgos de seguridad de la información con el objetivo de reducir la probabilidad de ocurrencia de incidentes. Realiza un análisis de riesgos siguiendo la metodología MAGERIT, concluyendo que con una adecuada gestión de riesgos se pueden mitigar los mismos, apoyados en varias metodologías disponibles de acuerdo a la naturaleza de la empresa. (Cruz, Guevara, 2018).

Villavicencio, en el año 2016, realizó un Diagnóstico sobre la Seguridad de la Información en el Sector Cooperativo del Ecuador, aplicado a cooperativas de ahorro y crédito del segmento uno, dos y tres del Ecuador, en el cual concluye que:

- En la gran mayoría de las cooperativas la seguridad de la información no es un tema de relevancia y que se lo haya considerado desde la planificación estratégica En todas las cooperativas en la alta gerencia existe un gran desconocimiento sobre los riesgos y amenazas del ciberdelito en el sector financiero, lo que provoca que no se le preste la atención e importancia necesaria y se lo mire como un gasto y no como una Inversión.
- La mayoría de las cooperativas realizan su gestión por requerimientos urgentes y no por un Proceso de Planificación (Aproximadamente un 60% - URGENTES).
- En la gran mayoría de cooperativas el proceso de seguridad de la información no se encuentra levantado mediante un marco referencial o buenas prácticas.
- Existe un gran desconocimiento de los estándares y la norma de Seguridad de la Información como es la ISO 27001.

- La mayoría de las cooperativas no disponen de un plan de contingencia y continuidad del negocio y no cuentan con un proceso de seguridad de la información separado de TI y mucho menos con un oficial de seguridad de la información.
- En algunas cooperativas la seguridad de la información está dividida en diferentes áreas: TI / RRHH / Riesgo y muy pocas cooperativas realizan un proceso de educación y sensibilización al personal de la cooperativa sobre temas de ciberseguridad (1 vez al año).
- La mayoría de cooperativas no disponen de un Procedimiento para Gestión de Vulnerabilidades e Incidentes (Villavicencio, 2016).

## 2.2 Fundamentación Filosófica

El presente trabajo de investigación se basa en el paradigma Critico Propositivo, es crítico por que realiza un análisis crítico del problema, y es propositivo porque busca proponer una solución factible al problema.

## 2.3 Fundamentación Legal

El presente trabajo de investigación se sustenta en las siguientes leyes:

**La Constitución Sección Octava Sistema Financiero**

**Reglamento General De La Ley De Cooperativas.**

Título VI, Art. 92, Pág. 14, "Cooperativas de ahorro y crédito son las que hacen préstamos a sus socios, que pueden pertenecer a distintas actividades, a fin de solucionar diferentes actividades."

**Normas Generales Para Las Instituciones Del Sistema Financiero, Continuidad del negocio**

Libro I.- Normas generales para las instituciones del sistema financiero, Titulo X.- de la gestión y administración de riesgos Capítulo V.- De la gestión de riesgo operativo Sección IV.- Continuidad del negocio.

"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. (Artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)
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,…"

"ARTÍCULO 16.- El plan de continuidad del negocio 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,…." (Artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**Resolución No. 128-2015-F de la Junta de Política y Regulación Monetaria y Financiera**:

**Sección VI. Elementos para la administración integral de riesgos**
**Artículo 20.- Sistema de Información**: "Las entidades de los segmentos 1, 2, y cajas centrales deberán disponer de un sistema de información capaz de proveer a la administración y a las áreas involucradas, la información necesaria para identificar, medir, priorizar, controlar, mitigar y monitorear las exposiciones de riesgo, considerando parámetros de metodologías propias de esta gestión. Esta información deberá apoyar la toma de decisiones oportunas y adecuadas. El alcance y nivel de especialización del sistema estará en relación con el volumen de las transacciones de la entidad…"
Con resolución No. JB-2005-834 de 20 de octubre de 2005, la Superintendencia de Bancos y Seguros (SBS) emitió la norma "De la Gestión del Riesgo Operativo". En el Libro I "Normas Generales para las Instituciones del Sistema Financiero", dice:

**CAPÍTULO V.- De La Gestión Del Riesgo Operativo**

Según la República del Ecuador Superintendencia de Bancos (2005) **ARTÍCULO 2.-** Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

**2.15 Tecnología de la información.-** Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**2.18 Responsable de la información.-** Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidade**s**; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**2.29 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; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**2.30 Administración de la continuidad.-** Es un proceso permanente que garantiza la continuidad de las operaciones del negocio de las instituciones del sistema financiero, a través de la efectividad del mantenimiento del plan de continuidad; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**2.43 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; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**2.44 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. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

**ARTÍCULO 3.-** Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de la información y por eventos externos. (Reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014).

**SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO**

Para la República del Ecuador Superintendencia de Bancos (2005) **En el Artículo 4.-** Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

**4.1 Procesos.-** Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

**4.1.1 Procesos gobernantes o estratégicos.-** Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

**4.1.2 Procesos productivos, fundamentales u operativos.-** Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

**4.1.3 Procesos habilitantes, de soporte o apoyo.-** Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

**4.2 Personas.-** Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor "personas", tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

**4.3 Tecnología de la información.-** Las instituciones controladas deben contar con la tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones. (reformado con resolución No. JB- 2014-3066 de 2 de septiembre del 2014)

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir políticas, procesos, procedimientos y metodologías que aseguren una adecuada planificación y administración de la tecnología de la información. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

## 2.4 Categorías Fundamentales

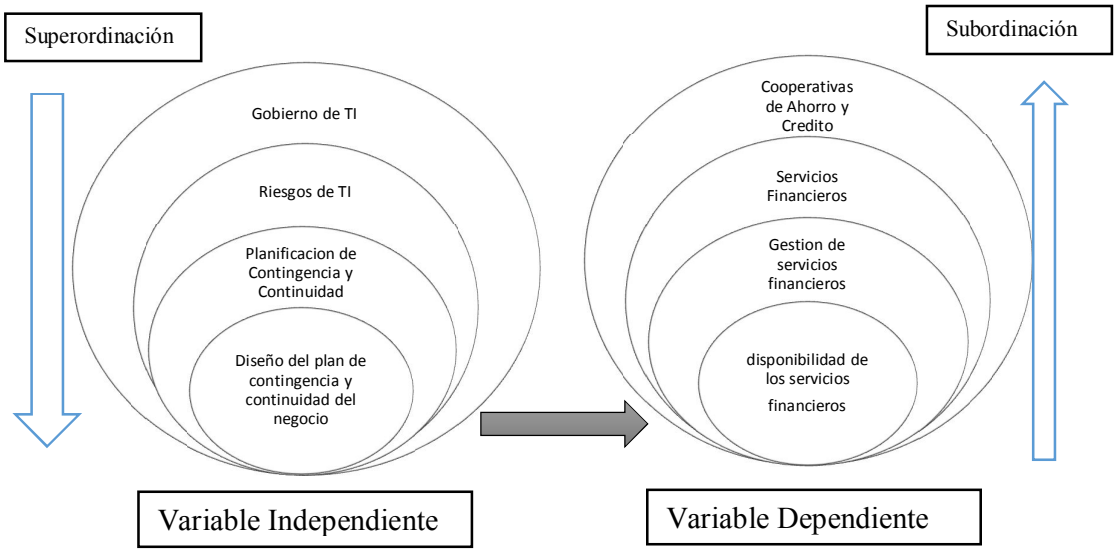



**Figura 1: Inclusiones conceptuales**

Elaborado por: Investigador

## Constelación de ideas variable independiente

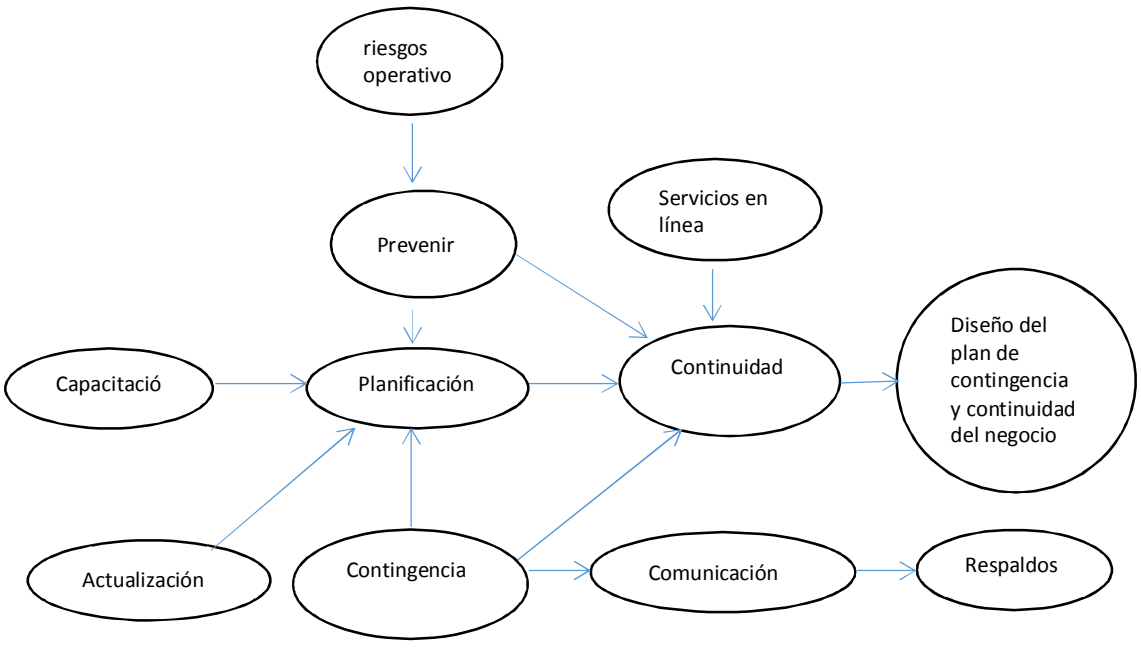



**Figura 2: Constelación de Ideas de la Variable Independiente**

Elaborado por: Investigador

**Constelación de ideas variable dependiente**

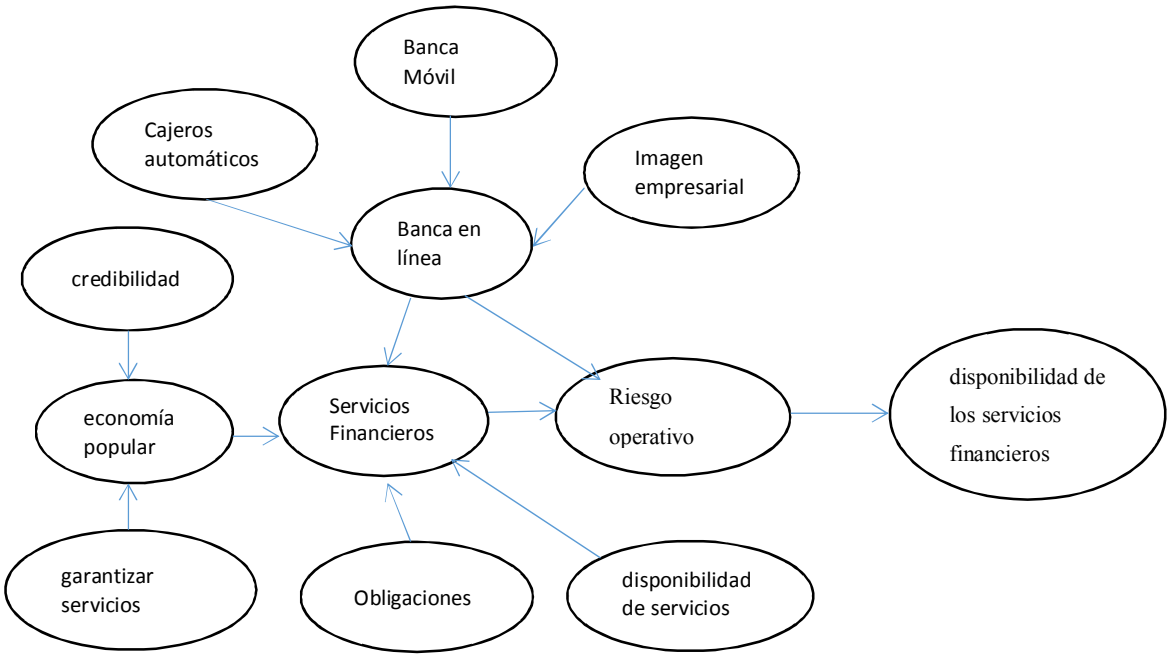



**Figura 3: Constelación de Ideas de la Variable Dependiente**

Elaborado por: Investigador

### 2.4.1 Categorías de la Variable Independiente

**Gobierno de TI**

La principal responsabilidad del gobierno de TI es garantizar la continuidad del negocio, la seguridad es un sistema dentro de sistemas mayores, que más que un producto o un conjunto de ellos, más que una o varias tecnologías, la seguridad es un proceso, que hace intervenir todas las tecnologías, todos los productos y, especialmente, el sentido común de los seres humanos que la gestionan, ese mismo sentido común que es el menos común de los sentidos (Díaz, 2004).

Piense en un buen sistema de seguridad de un banco: debe tener en cuenta la prevención, la detección y la respuesta al problema concreto. Debe tener una cámara acorazada para proteger el dinero, joyas, etc. (prevención), debe tener alarmas para identificar a los posibles ladrones (detección) y debe contactar con

los guardias (o la policía) para que los detenga (respuesta). La seguridad informática de hoy en día suele tener muy en cuenta la prevención (cortafuegos, criptografía, etc. ) pero está evolucionando en cuanto a las otras dos. Empiezan, poco a poco, a verse herramientas de detección (como los sistemas de detección de intrusiones) y herramientas y sistemas (muchas veces humanos) de auditoría de vulnerabilidades (Díaz, 2004).

**Riesgos de TI**

Las empresas actúan en ámbitos donde factores tales como la globalización, la tecnología, las normas, las reestructuras, los mercados cambiantes y la competencia crean incertidumbre. La misma proviene de la dificultad de determinar con precisión la probabilidad de ocurrencia de acontecimientos eventuales y sus consecuencias asociadas. El riesgo es una medida de la incertidumbre, y en ese sentido se lo puede definir como el nivel de exposición a las incertidumbres que una organización debe entender y efectivamente administrar para lograr alcanzar sus objetivos y crear valor para sus interesados. Toda entidad existe para proveer valor a sus grupos de interés. Para cumplir con su misión debe enfrentar la incertidumbre, tanto riesgos como oportunidades.

El desafío para la gerencia es determinar cuanta incertidumbre la entidad está dispuesta a aceptar en su esfuerzo para aumentar el valor a sus grupos de interés. La gerencia debe considerar riegos interrelacionados desde una perspectiva conjunta a nivel de la entidad. Es necesario identificar los riesgos interrelacionados y actuar sobre ellos a efectos de considerar el riesgo en su totalidad dentro del nivel de riesgo aceptado.

El riesgo correspondiente a las unidades operativas de la organización puede estar dentro de las tolerancias de riesgo de la unidad, pero tomado en su conjunto puede exceder el nivel de riesgo aceptado. El nivel global de riesgo aceptado se refleja en una organización a través de las tolerancias al riesgo, establecidas para objetivos específicos (Martínez, 2004).

El nivel de riesgo aceptado, es la cantidad de riesgo que una entidad está dispuesta a aceptar en su búsqueda de valor. Las organizaciones a menudo consideran el nivel de riesgo aceptado en forma cualitativa, con categorías tales como alta,

moderada o baja, o pueden aplicar un enfoque cuantitativo reflejando y buscando un equilibrio entre las metas de crecimiento, rendimiento y riesgo. El nivel de riesgo aceptado por una entidad, orienta la asignación de recursos. La gerencia debe asignar recursos entre las unidades de negocio, tomando en cuenta el nivel de riesgo aceptado y la estrategia de las unidades de negocio individuales, para generar el rendimiento deseado de los recursos asignados. Además debe considerar su nivel de riesgo aceptado, según el mismo sea compatible con su organización, su gente y sus procesos, destinando la infraestructura necesaria para responder y monitorear eficazmente los riesgos.

La gestión del riesgo abarca una amplia gama de actividades para identificar, controlar y mitigar los riesgos de un sistema de TI. Las actividades de gestión de riesgos desde el punto de vista informático de planificación de contingencia tienen dos funciones principales. En primer lugar, la gestión del riesgo debe identificar las amenazas y las vulnerabilidades a fin de que los controles adecuados se puedan poner en cualquier lugar, para evitar incidentes que ocurran o para limitar sus efectos. Estos controles de seguridad protegen al sistema de TI frente a tres categorías de amenazas:

• Naturales - por ejemplo, huracanes, tornados, inundaciones, y el fuego.

• Humanas - por ejemplo, errores del operador, sabotaje, implante de códigos maliciosos y ataques terroristas.

• Ambientales - por ejemplo, fallos de equipos, errores de software, corte de la red de telecomunicaciones, falta de energía eléctrica.

Para determinar efectivamente los riesgos específicos de un sistema de TI durante la interrupción del servicio, una evaluación del riesgo del entorno de TI del sistema es necesaria. Una evaluación exhaustiva de los riesgos debe identificar las vulnerabilidades del sistema, la amenaza, y los controles actuales y tratar de determinar el riesgo sobre la base de la probabilidad y el impacto de las amenazas. Estos riesgos, deben ser evaluados y un nivel de riesgo asignado (por ejemplo, alto, medio o bajo). Debido a que los riesgos pueden variar con el tiempo y los nuevos riesgos pueden reemplazar a los viejos como un sistema que evoluciona, el proceso de gestión del riesgo debe ser continuo y dinámico. La persona

responsable debe ser consciente de los riesgos para el sistema y reconocer si el plan de contingencia actual es capaz de abordar los riesgos residuales por completo y eficazmente (Martínez, 2004).

**Incidente**

Es un problema que afecta la continuidad del negocio es un evento interno o externo, provocado o natural, que interrumpe uno o más de sus procesos. Lo cual, en caso de mantenerse durante un tiempo significativo o si se presenta en reiteradas ocasiones, pondrá en riesgo la continuidad de las operaciones de la empresa, provocando un daño inaceptable (Fernández & Velthuis, 2012).

**Desastre**

Un desastre es un evento súbito e inesperado que causa un gran daño o pérdida (Fernández & Velthuis, 2012).

Los desastres pueden ser catástrofes naturales como terremotos, tornados, erupción de un volcán, o eventos provocados por el hombre como incendios, explosiones de plantas nucleares, ataques terroristas etc.

También existen los desastres que son parte del día a día en negocios de todas partes del mundo como incidentes de seguridad, vandalismo o sabotaje; fallos en el hardware o el software y las pérdidas por corrupción de datos y errores.

**La recuperación de desastres**

Es en realidad la capacidad de mantener la normalidad de las operaciones –o lo más cercano posible a ella– tanto como sea factible y justificable. La planificación para la recuperación ante desastres (DRP) tiene que ver con la preparación y respuesta cuando llegue el desastre; su objetivo directo es la supervivencia de una organización (Fernández & Velthuis, 2012).

**Planificación de contingencia y continuidad**

**Contingencia**

La planificación de contingencia de TI representa una amplia gama de actividades destinadas a mantener y recuperar los servicios críticos después de una

emergencia; ésta se ajusta en un entorno mucho más amplio de preparación para emergencias que incluye la organización, la continuidad de procesos de negocio y la planificación de la recuperación. En última instancia, una organización debería utilizar un conjunto de planes para preparar adecuadamente la respuesta, recuperación y continuidad de los incidentes que afectan a las TI, procesos de negocio, y a las instalaciones. Debido a que existe una relación intrínseca entre un sistema de TI y los procesos de negocio que apoya, debería haber una coordinación entre todos los planes durante el desarrollo y las actualizaciones, para garantizar que las estrategias de recuperación y apoyo a los recursos no se contradicen entre sí ni duplican esfuerzos. En general, las definiciones universalmente aceptadas para la planificación de contingencia y la planificación de estas áreas correspondientes no han estado disponibles. En ocasiones, esta falta de disponibilidad ha dado lugar a confusión sobre el verdadero alcance y el propósito de los distintos tipos de planes. Para proporcionar una base común de entendimiento en relación con la planificación de contingencia de TI, se identifican otros tipos de planes y se describe su finalidad y ámbito de aplicación en relación con la planificación de contingencia (Martínez, 2004).

El plan de continuidad (PC) se centra en el mantenimiento de las funciones comerciales de una empresa durante y después de una interrupción. Un ejemplo de una función de negocio puede ser el proceso de pagos de una organización o el proceso de atención al cliente. Puede estar escrito para un proceso de negocio específico o puede resolver todos los procesos clave de negocio. Los sistemas de TI se consideran en el PC en términos de su apoyo a los procesos de negocio. En algunos casos, el PC no puede tratar la recuperación a largo plazo de los procesos y restablecer el funcionamiento normal, sólo cubre los requisitos de continuidad del negocio de corto plazo. El PC puede incluir además un plan de recuperación de desastres, plan de reanudación de negocios, y el plan de emergencia de los ocupantes. El PC debe coordinarse con el Plan de Continuidad de Operaciones para eliminar los posibles conflictos, siempre siguiendo los lineamientos establecidos en la política de continuidad.

El plan de recuperación se refiere a la restauración de los procesos de negocio después de una emergencia, pero a diferencia del PC, carece de procedimientos

para garantizar la continuidad de los procesos críticos a lo largo de una emergencia o interrupción. Se centra en la restauración de las funciones esenciales en un sitio alternativo. Las organizaciones deben preparar sus procedimientos de comunicaciones internas y externas antes de un desastre. Un plan de comunicación de crisis es a menudo desarrollado por la unidad responsable de la divulgación pública. Los procedimientos de comunicación del plan deberían coordinarse con todos los otros planes para garantizar que sólo las declaraciones aprobadas son liberadas al público (García & Mariblanca, 2015).

**Continuidad**

El objetivo es contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios, de los efectos de fallas significativas o desastres. Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, entre otros, desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas), así como también analizarse las consecuencias ocasionadas. Planes de contingencia deberán desarrollarse para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión (García & Mariblanca, 2015).

La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

**Plan de contingencia y continuidad del negocio**

Es un programa determinado por los requerimientos y necesidades de la organización para responder a las situaciones o incidentes que provoquen

interrupciones con un impacto relevante y, por ende, pretende reducir las consecuencias de las interrupciones a un nivel aceptable por la alta dirección.

Por su parte, la Norma UNE 71599-2:2010, da la siguiente definición de gestión de la continuidad del negocio: "Proceso de gestión holístico que identifica amenazas potenciales para la organización así como el impacto en las operaciones del negocio que dichas amenazas, en caso de materializarse, puedan causar, y que proporciona un marco para aumentar la capacidad de resistencia o resiliencia de la organización para dar una respuesta eficaz que salvaguarde los intereses de sus principales partes interesadas, la reputación, la marca y las actividades de creación de valor"(Fernández & Velthuis, 2012).

**Objetivos:**

- Asegurar la continuidad y la supervivencia de la empresa.
- Proporcionar protección a los activos o, como mínimo, a aquellos críticos para la operación.
- Minimizar el tiempo de recuperación para restaurar las aplicaciones críticas, y los procesos de negocio y funciones.
- Mitigar los riesgos asociados a estos activos críticos.
- Proporcionar o implementar controles que mitiguen dichos riesgos.
- Limitar el número de decisiones que deben tomarse después de una interrupción del servicio.
- Determinar las medidas preventivas.
- De ser inevitable la interrupción, ejecutar las acciones pertinentes para tomar el control.
- Preparar al personal para posibles situaciones de emergencia a través de acciones que se revisan en el control periódico y que se contemplan en la actualización de todos los planes de continuidad del negocio.
- Eliminar la necesidad de desarrollar nuevos procedimientos durante el proceso de recuperación.
- Aumentar la credibilidad de la organización ante los clientes, socios comerciales y partes interesadas mediante la formalización de los procesos

y su documentación, para garantizar la disponibilidad y exactitud de la información para los interesados.

- Apoyar y mejorar el cumplimiento con las disposiciones y leyes, y de las normas y prácticas de negocios a que está sujeta la empresa (Fernández & Velthuis, 2012).

Según Martínez, el proceso que se presenta aquí es común a todos los sistemas de TI. Consta de siete pasos:

1. Desarrollar la declaración de política de planificación de contingencia.
2. Ejecutar el análisis de impacto en el negocio (BIA), por sus siglas en inglés.
3. Señalar los controles preventivos.
4. Establecer estrategias de recuperación de TI.
5. Desplegar un plan de contingencia de TI.
6. Capacitación, difusión y pruebas del plan.
7. Planificar el mantenimiento del plan.

Estos pasos constituyen elementos clave para una amplia capacidad de planificación de contingencia. La responsabilidad por el proceso de planificación general, cae bajo el auspicio del "Coordinador de Planificación de Contingencia" o "Planificador de Contingencia", que normalmente es un funcionario o administrador de recursos dentro de la organización. La coordinación de la estrategia se desarrolla en cooperación con otros empleados y administradores de recursos asociados con el sistema o los procesos de negocios apoyados por el mismo. El Coordinador de Planificación de Contingencia también administra el desarrollo y ejecución del plan de contingencia. Todas las principales aplicaciones y sistemas de apoyo en general deben tener un plan de contingencia (Martínez, 2004).

### 2.4.2 Categorías de la Variable Dependiente

**Cooperativas de ahorro y crédito**

Son instituciones financieras cuyos servicios están orientados a la economía popular y solidaria, trabajan baja la regulación de la SEPS.

Uno de los retos de la institucionalidad ecuatoriana desde que se promulgó la Constitución en el 2008 y en el caso específico de las finanzas y emprendimientos populares, con la promulgación de la Ley de Economía Popular y Solidaria y del Sector Financiero Popular (LOEPS) en el 2011 fue el de conocer y cuantificar al sector de la Economía Popular y Solidaria. Ambos cuerpos legales definieron y delimitaron al sector, pero su conocimiento se ha basado tradicionalmente en las generalidades y el criterio de expertos (SEPS, 2017).

**Servicios financieros**

Son las actividades inherentes al giro del negocio, ejecutadas por las entidades financieras para satisfacer las necesidades de los clientes y/o usuarios (personas naturales o jurídicas), sujetas a regulación y control financiero.

Las principales características que diferencian a los servicios de los bienes son las siguientes (SEPS, 2017):

- Intangibilidad: Es aquella característica que determina que los servicios no pueden ser vistos, sentidos, probados o tocados, la cual genera incertidumbre a sus usuarios al momento de adquirirlos, ya que no se puede determinar el grado de satisfacción hasta que sean utilizados.
- Inseparabilidad: Es aquella característica que se refiere a que los servicios se producen, venden y consumen al mismo tiempo, lo cual implica que su producción y consumo ocurre de manera simultánea.
- Heterogeneidad: Es aquella característica que se refiere a la variabilidad que presentan los servicios de acuerdo al recurso humano utilizado, al lugar o tiempo en que se efectúa la prestación del mismo. Esta característica dificulta la estandarización de los servicios.
- Caducidad: Es aquella característica que determina que los servicios no se pueden conservar, almacenar o guardar, lo cual hace que sean perecederos. Sinónimo: Imperecedero.
- Propiedad: Es aquella característica que le da el derecho de uso, acceso o alquiler al cliente y/o usuario durante la prestación del servicio, por el pago efectuado por los mismos pero no de propiedad.

**Tipos de servicios financieros:**

SFB Servicio financiero básico

SFM Servicio financiero con cargo máximo

SFD Servicio financiero con cargo diferenciado

De acuerdo a las especificaciones de la SEPS, los servicios financieros son (SEPS, 2017):

- Apertura
- Depósitos
- Retiros
- Administración, mantenimiento
- Consulta de cuentas
- Cierre de cuentas
- Giros nacionales
- Transferencias dentro de la misma entidad
- Transferencias interbancarias
- Activación de cuentas
- Mantenimiento a tarjeta de debito
- Bloqueo, anulación de tarjeta de debito
- Reclamos de socios / clientes
- Emisión de tabla de amortización
- Servicios de reposición de insumos
- Emisión y entrega de estado de cuenta
- Servicio de notificaciones de transacciones
- Servicio de emisión y renovación de tarjetas de debito
- Servicios con cheques
- Servicios de referencias
- Servicio de copias
- Servicio de ventanilla compartida
- Servicios a establecimientos por consumos pagados con tarjeta
- Gestión de cobranza extrajudicial

- Servicio de recaudaciones de pagos a terceros
- Servicios de medios de seguridad adicional
- Alquiler de casilleros de seguridad
- Cuenta de ahorro
- Cuenta básica
- Depósitos a plazo
- Créditos
- Oficina, celular, telefónica, internet, cajero automático.

**Disponibilidad de servicios financieros**

Se refiere a garantizar que el servicio este a disposición del usuario la mayor parte posible del tiempo que se ha ofertado. Esto se lo puede lograr mediante sistemas de respaldo y redundancia.

## 2.5 Hipótesis

El diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento 1 del cantón Ambato.

## 2.6 Señalamiento de Variables

**Variable Independiente**: Diseño del plan de contingencia y continuidad del negocio.

**Variable Dependiente**: Disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

# CAPITULO III

## 3. METODOLOGÍA

### 3.1 Enfoque

La investigación maneja un enfoque cuali-cuantitativo, es cuantitativa debido a que usa parámetros de medición en la variable independiente; es cualitativa debido a que se va a generar juicios de valor respecto a la disponibilidad del servicio en la institución.

### 3.2 Modalidad básica de la investigación

**Investigación Bibliográfica**

El trabajo de investigación es bibliográfico ya que se apoya en textos impresos, libros, documentos técnicos, publicaciones de tecnología, estándares y leyes existentes para la elaboración del marco teórico sobre contingencia y continuidad del negocio y disponibilidad del servicio.

**Investigación de Campo**

El trabajo investigativo es de campo debido a que se busca obtener información de los procesos de contingencia y continuidad del negocio dentro de la institución y con el personal involucrado en el tema.

### 3.3 Nivel o tipo de investigación

**Investigación Exploratoria**

La investigación es de nivel exploratorio porque se acude directamente con las persona encargadas de garantizar la contingencia y continuidad del negocio y se revisaran los resultados con los directores departamentales y jefes de agencia.

**Investigación Descriptiva**

El trabajo de investigación es descriptivo debido a que se realiza un estudio para determinar la incidencia que tiene la instrumentación de un plan de contingencia y

continuidad del negocio para cooperativas de ahorro y crédito en la disponibilidad de los servicios financieros.

**Explicativa**

El trabajo de investigación es explicativo debido a que se puede sustentar el impacto que tiene el diseño de un plan de contingencia y continuidad del negocio para cooperativas de ahorro y crédito en la disponibilidad de los servicios financieros.

**Investigación Correlacional**

La investigación será correlacional por que busca medir el grado de relación entre la instrumentación de un plan de contingencia y continuidad del negocio para cooperativas de ahorro y crédito y la disponibilidad de los servicios financieros.

### 3.4 Población y Muestra

La presente investigación se orienta a las cooperativas de ahorro y crédito del segmento 1, de acuerdo a la "Norma para la segmentación de las entidades del sector financiero popular y solidario", expedida por La Junta de Política y Regulación Monetaria y Financiera en la resolución No. 038-2015-F el 13 de febrero de 2015, en la que establece:

"…En el ejercicio de las atribuciones que le confiere el Código Orgánico Monetario y Financiero resuelve expedir la siguiente:

NORMA PARA LA SEGMENTACIÓN DE LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO

Artículo 1.- Las entidades del sector financiero popular y solidario de acuerdo al tipo y al saldo de sus activos se ubicarán en los siguientes segmentos:

- Segmento 1: Mayor a 80'000.000,00
- Segmento 2: Mayor a 20'000.000,00 hasta 80'000.000,00
- Segmento 3: Mayor a 5'000.000,00 hasta 20'000.000,00
- Segmento 4: Mayor a 1'000.000,00 hasta 5'000.000,00
- Segmento 5: Hasta 1'000.000,00

En base a lo cual, se trabajará con una población formada un grupo de profesionales encargados de garantizar la continuidad del negocio de una cooperativa de ahorro y crédito del segmento 1, Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda. ,que está sujeta a cumplir con el mismo nivel de obligaciones y regulaciones establecidas por los entes de control para todas las cooperativas del mismo segmento, de acuerdo al detalle descrito en la tabla 1.

**Tabla 1: Población de Estudio**

Elaborado por: Investigador

| Población | Número | Porcentaje |
|---|---|---|
| Director de TI | 1 | 6.67% |
| Oficial de Seguridad | 1 | 6.67% |
| Jefe de TI | 1 | 6.67% |
| Oficial de riesgos | 1 | 6.67% |
| Auditor Interno | 1 | 6.67% |
| Director Financiero | 1 | 6.67% |
| Director de Negocios | 1 | 6.67% |
| Jefes de Agencia | 8 | 53.31% |
| **Total** | 15 | 100.00% |

En vista que la población a ser investigada es de 15 personas se trabajará con la totalidad del universo sin que sea necesario sacar muestras representativas.

### 3.5 Operacionalización de Variables

### 3.5.1 Variable Independiente:

**Tabla 2: Diseño del plan de contingencia y continuidad del negocio**

Elaborado por: Investigador

| Conceptualización o Descripción | Dimensiones | Indicadores | Ítems Básicos | Técnicas e Instrumentos |
|---|---|---|---|---|
| El plan de contingencia de TI representa una amplia gama de actividades destinadas a mantener y recuperar los servicios críticos después de una emergencia; ésta se ajusta en un entorno mucho más amplio de preparación para emergencias que incluye la organización y la planificación de la recuperación. Una organización debería utilizar | • Plan de contingencia | Documentación del plan.<br><br>Actividades para recuperarse de la interrupción.<br><br>PMTI Plazo máximo tolerable de interrupción. | ¿La organización posee un documento en donde se indique que hacer frente a una suspensión de servicios de TI?<br>¿Conoce que acciones debe llevar a cabo durante una interrupción de los servicios de TI dentro de la organización?<br>De acuerdo con las disposiciones de los entes de control, ¿conoce el tiempo que la organización puede tolerar la falta de funcionamiento de sus sistemas | - Encuesta con Cuestionario |

| | | | | |
|---|---|---|---|---|
| metodologías para la identificación y gestión de riesgos que afectan a las TI, procesos de negocio y a las instalaciones. | | | informáticos? | |
| | | Respaldo y restauración | ¿Existen en la organización procedimientos de respaldo y restauración de información? | |
| | • Organización | Definición de funciones. | ¿**Existen** funciones definidas formalmente para cada integrante del departamento de TI? | |
| | | Identificación de activos críticos | ¿Se encuentran identificados los activos críticos de TI (Servidores, aplicaciones, equipo de cómputo, equipo de redes y comunicaciones)? | |
| | | Identificación de servicios críticos | Conjuntamente con la alta gerencia, ¿se han identificado los servicios críticos de TI de la organización? | |

| | | | | |
|---|---|---|---|---|
| | • Identificación y gestión de riesgos | Registro de eventos de riesgo<br><br>BIA Análisis de impacto en el negocio<br><br>Mitigación de riesgos<br><br>Gestión de riegos | **En** su organización, ¿se lleva un registro de los sucesos de eventos de riesgo de TI?<br>Cuando suscita un incidente de riesgos de TI, ¿se ejecuta alguna acción para evitar que ocurra nuevamente o para reducir su impacto?<br>¿Existen acuerdos de nivel de servicio con los proveedores de los aplicativos en producción?<br>¿Conoce las debilidades y amenazas que afectan a la infraestructura y servicios de su departamento de TI? | |

### 3.5.2 Variable Dependiente:

**Tabla 3: Disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato**

Elaborado por: Investigador

| Conceptualización o Descripción | Dimensiones | Indicadores | Ítems Básicos | Técnicas e Instrumentos |
|---|---|---|---|---|
| Capacidad de respuesta para garantizar la continuidad de procesos del negocio en relación al tiempo ofertado de prestación de servicios financieros. Tiempo en línea de las actividades inherentes al giro del negocio, ejecutadas por las entidades financieras para satisfacer las necesidades de los clientes y/o usuarios (personas naturales o | • Continuidad del negocio | Inclusión en el plan estratégico.<br><br>Designación de responsabilidades.<br><br>Impacto en el negocio. | ¿Se incluye dentro de la planificación estratégica de la organización la gestión de la continuidad del negocio?<br>¿Existe en la organización una persona o entidad responsable de garantizar la disponibilidad de los servicios de TI?<br>¿Las interrupciones de los servicios de TI ocasionan deterioro de la imagen de | - Encuesta con Cuestionario |

| | | | | |
|---|---|---|---|---|
| jurídicas), sujetas a regulación y control financiero. Con relación a la continuidad del negocio que está en capacidad de ofrecer a los clientes. | | Diseño del plan | la organización, deserción de socios y pérdidas económicas?<br>¿El diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de los servicios financieros de la organización? | |

### 3.6 Recolección de Información

Para recolectar información se usa la técnica de la encuesta dirigida utilizando como instrumento el cuestionario con preguntas de selección múltiple, que permiten identificar claramente los resultados y facilitan la tabulación para interpretar los mismos.

**Tabla 4: Recolección de la Información**

Elaborado por: Investigador

| Preguntas Básicas | Definición |
|---|---|
| ¿Para qué? | Para llegar a cumplir los objetivos del trabajo de investigación. |
| ¿A quién, o a qué? | Director de TI<br>Oficial de Seguridad<br>Jefe de TI<br>Oficial de riesgos<br>Auditor Interno<br>Director Financiero<br>Director de Negocios<br>Jefes de Agencia |
| ¿Sobre qué aspectos? | Acciones cuando se suspende el servicio, tiempo de respuesta, Atención al cliente cuando un riesgo se materializa |
| ¿Quién, Quiénes? | Investigador: Ing. Susana Ibarra |
| ¿Cuándo? | Enero a Junio 2019 |
| ¿Dónde? | Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda. |
| ¿Cuántas veces? | Una |
| ¿Qué técnicas de recolección? | Encuesta<br>Datos Estadísticos |
| ¿Con qué? | Cuestionario |

| | |
|---|---|
| | Inspecciones |
| ¿En qué situación? | En las instalaciones de la empresa, en el área de trabajo de los empleados, dentro de su horario normal, guardando la confidencialidad de la información investigada. |

### 3.7 Procesamiento de datos

- Las respuestas o los datos obtenidos, se transfieren a una matriz de datos y se preparan para su análisis.
- La revisión de la información recolectada se realiza mediante la tabulación de la información para agrupar y estructurar los datos obtenidos en el trabajo de campo, con el objetivo de responder a: problema de investigación, objetivos e hipótesis de estudio.
- Definir las herramientas o programas estadísticos para el procesamiento de los datos.
- Los resultados se presentan con organizadores gráficos mediante tablas y gráficos convirtiéndose en información significativa.

**Análisis de Resultados**

- El análisis e interpretación es traducir la importancia de los datos.
- Reflexión sobre los resultados obtenidos en el trabajo de campo en función de: problema de Investigación, objetivos, hipótesis del estudio y el marco teórico del estudio.
- Describir datos, valores, puntuación y distribución de frecuencia para cada variable.
- Análisis de los resultados estadísticos, recalcando tendencias o relaciones de acuerdo con los objetivos e hipótesis.
- Redactar la interpretación de los resultados apoyados en el marco teórico.
- Verificación estadística de la hipótesis.
- Establecer de conclusiones y recomendaciones.

# CAPITULO IV

## 4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

### 4.1 Análisis de resultados

Por medio de la recopilación de información a través de las técnicas de encuesta, utilizando un formulario para investigar la capacidad de respuesta de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato, frente a eventos de riesgos de TI, se procede a realizar el análisis e interpretación de resultados.

El objetivo es identificar si la institución está preparada para mantener en línea aquellos procesos realmente críticos para la supervivencia de la empresa, así como determinar su dependencia de otras áreas o procesos de negocio críticos o que resultarán indispensables para que los procesos críticos puedan llevarse a cabo o recuperarse.

#### 4.1.1 Formulario de evaluación y medición

El formulario de encuesta, fue aplicado de manera general sobre la disponibilidad de los servicios del departamento de TI de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato, a una muestra de 15 personas entre las que se consideran los cargos de: director de TI, oficial de seguridad de la información, jefe de TI, oficial de riesgos, auditor interno, director financiero, director de negocios y jefe de agencia.

En la encuesta se consideran los siguientes puntos:

- Punto 1. Plan de contingencia
- Punto 2. Organización
- Punto 3. Identificación y gestión de riesgos
- Punto 4. Continuidad del negocio

**Punto 1. Plan de contingencia**

Pregunta 1. ¿La organización posee un documento en donde se indique que hacer frente a una suspensión de servicios de TI?

**Tabla 5: Encuesta - Punto 1 Plan de Contingencia - Pregunta 1**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 3 | 20% | 20% |
| No | 12 | 80% | 100% |
| **Total** | 15 | 100% | |

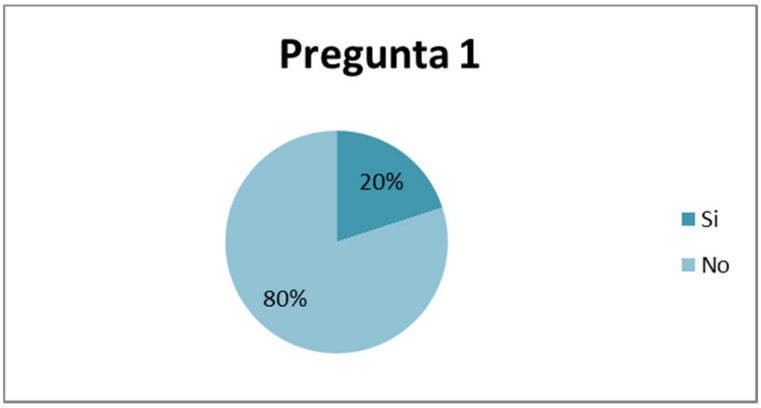



**Figura 4: Encuesta - Punto 1 Plan de Contingencia - Pregunta 1**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 12 personas que representa el 80% indicaron que no poseen un documento en donde se indique que hacer frente a una suspensión de servicios de TI; 3 personas que corresponde al 20% mencionaron que si lo poseen.

Interpretación. - Según las respuestas obtenidas se identifica que las organizaciones no poseen un documento en donde se indique que hacer frente a una suspensión de servicios de TI.

Pregunta 2. ¿Conoce que acciones debe llevar a cabo durante una interrupción de los servicios de TI dentro de la organización?

**Tabla 6: Encuesta - Punto 1 Plan de Contingencia - Pregunta 2**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 4 | 27% | 27% |
| No | 11 | 73% | 100% |
| **Total** | 15 | 100% | |

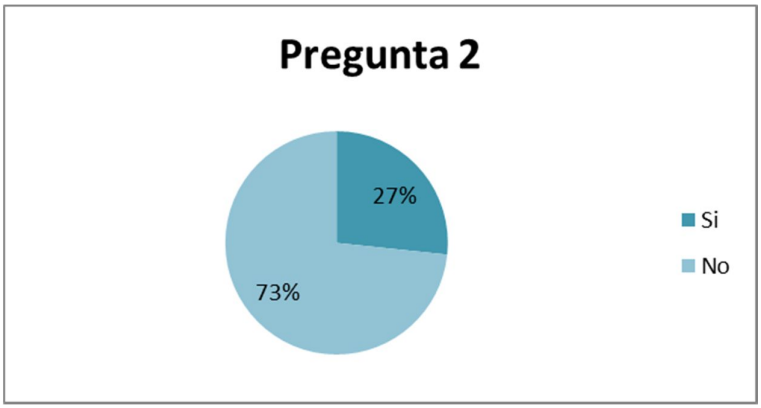



**Figura 5: Encuesta - Punto 1 Plan de Contingencia - Pregunta 2**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 11 personas que representa el 73% indicaron que no conocen que acciones deben llevar a cabo durante una interrupción de los servicios de TI dentro de la organización; 4 personas que corresponde al 27% mencionaron que si conocen.

Interpretación. - Según las respuestas obtenidas se identifica que los colaboradores no conocen que acciones debe llevar a cabo durante una interrupción de los servicios de TI dentro de la organización.

Pregunta 3. De acuerdo con las disposiciones de los entes de control, ¿conoce el tiempo que la organización puede tolerar la falta de funcionamiento de sus sistemas informáticos?

**Tabla 7: Encuesta - Punto 1 Plan de Contingencia - Pregunta 3**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 0 | 0% | 0% |
| No | 15 | 100% | 100% |
| **Total** | 15 | 100% | |

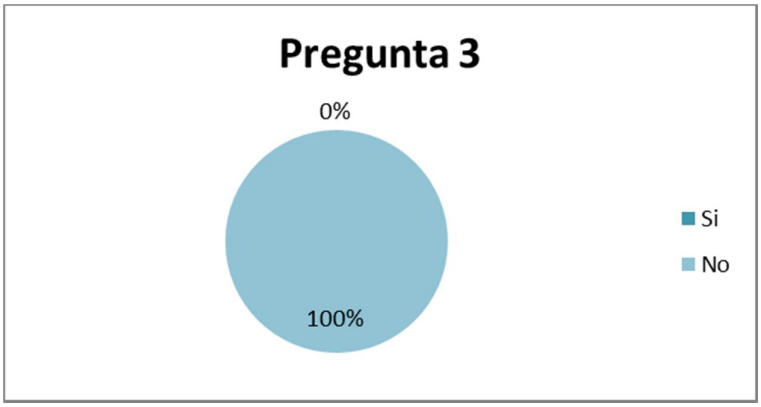



**Figura 6: Encuesta - Punto 1 Plan de Contingencia - Pregunta 3**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 15 personas que representa el 100% indicaron que no conocen el tiempo que la organización puede tolerar la falta de funcionamiento de sus sistemas informáticos de acuerdo a las disposiciones de los entes de control; 0 personas que corresponde al 0% mencionaron que si conocen.

Interpretación. - Según las respuestas obtenidas se identifica que los colaboradores no conocen el tiempo que la organización puede tolerar la falta de funcionamiento de sus sistemas informáticos de acuerdo a las disposiciones de los entes de control.

Pregunta 4. ¿Existen en la organización procedimientos de respaldo y restauración de información?

**Tabla 8: Encuesta - Punto 1 Plan de Contingencia - Pregunta 4**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 5 | 33% | 33% |
| No | 10 | 67% | 100% |
| **Total** | 15 | 100% | |

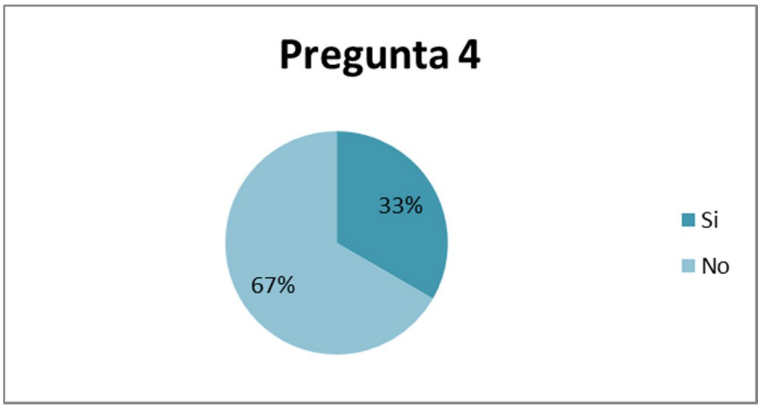



**Figura 7: Encuesta - Punto 1 Plan de Contingencia - Pregunta 4**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 10 personas que representa el 67% indicaron que no existen en la organización procedimientos de respaldo y restauración de información; 5 personas que corresponde al 33% mencionaron que si existen.

Interpretación. - Según las respuestas obtenidas se identifica que no existen en las organizaciones procedimientos de respaldo y restauración de información.

**Punto 2. Organización**

Pregunta 5. ¿Existen funciones definidas formalmente para cada integrante del departamento de TI?

**Tabla 9: Encuesta - Punto 2 Organización - Pregunta 5**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 4 | 27% | 27% |
| No | 11 | 73% | 100% |
| **Total** | 15 | 100% | |

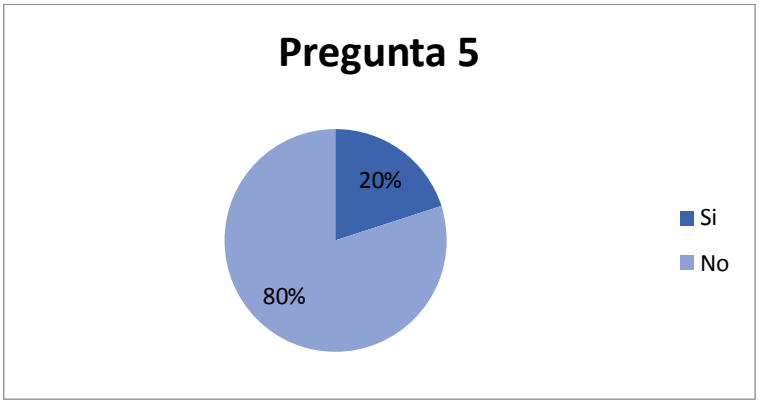



**Figura 8: Encuesta - Punto 2 Organización - Pregunta 5**

Análisis. - En la encuesta realizada a 15 personas, 11 personas que representa el 73% indicaron que no existen funciones definidas formalmente para cada integrante del departamento de TI; 4 personas que corresponde al 27% mencionaron que si existen.

Interpretación. - Según las respuestas obtenidas se identifica que no existen funciones definidas formalmente para cada integrante del departamento de TI.

Pregunta 6. ¿Se encuentran identificados los activos críticos de TI (Servidores, aplicaciones, equipo de cómputo, equipo de redes y comunicaciones)?

**Tabla 10: Encuesta - Punto 2 Organización - Pregunta 6**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 2 | 13% | 13% |
| No | 13 | 87% | 100% |
| **Total** | 15 | 100% | |

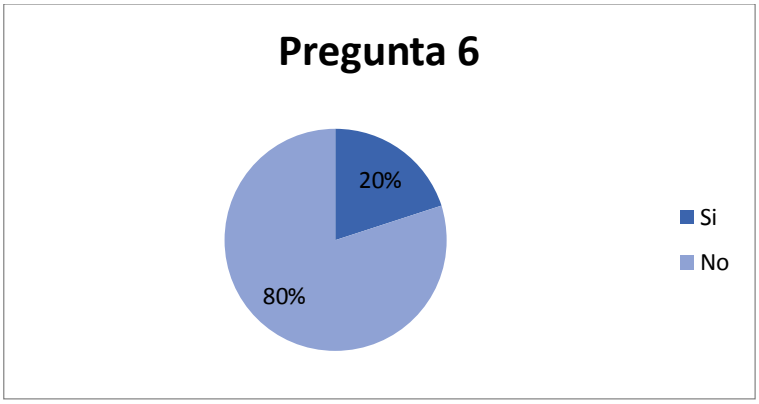



**Figura 9: Encuesta - Punto 2 Organización - Pregunta 6**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 13 personas que representa el 87% indicaron que no se encuentran identificados los activos críticos de TI; 2 personas que corresponde al 13% mencionaron que si.

Interpretación. - Según las respuestas obtenidas se identifica que no se encuentran identificados los activos críticos de TI en las organizaciones.

Pregunta 7. Conjuntamente con la alta gerencia, ¿se han identificado los servicios críticos de TI de la organización?

**Tabla 11: Encuesta - Punto 2 Organización - Pregunta 7**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 3 | 20% | 20% |
| No | 12 | 80% | 100% |
| **Total** | 15 | 100% | |

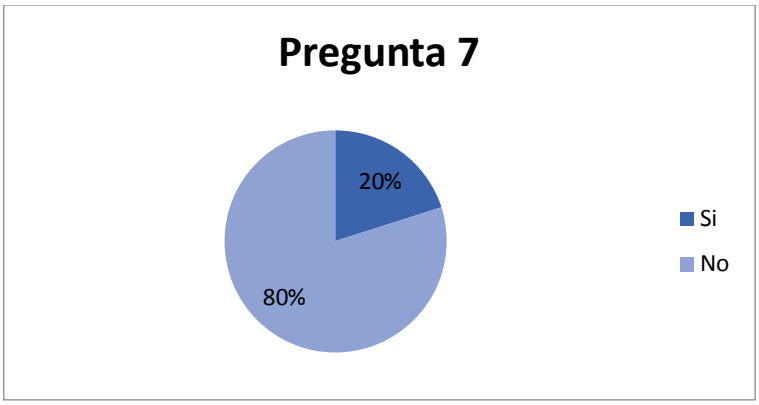



**Figura 10: Encuesta - Punto 2 Organización - Pregunta 7**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 12 personas que representan el 80% indicaron que no se han identificado los servicios críticos de TI de la organización conjuntamente con la alta gerencia; 3 personas que corresponde al 20% mencionaron que si se ha identificado.

Interpretación. - Según las respuestas obtenidas se observa que no se han identificado los servicios críticos de TI de la organización conjuntamente con la alta gerencia.

**Punto 3. Identificación y gestión de riesgos**

Pregunta 8. En su organización, ¿se lleva un registro de los sucesos de eventos de riesgo de TI?

**Tabla 12: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 8**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 4 | 27% | 27% |
| No | 11 | 73% | 100% |
| **Total** | 15 | 100% | |

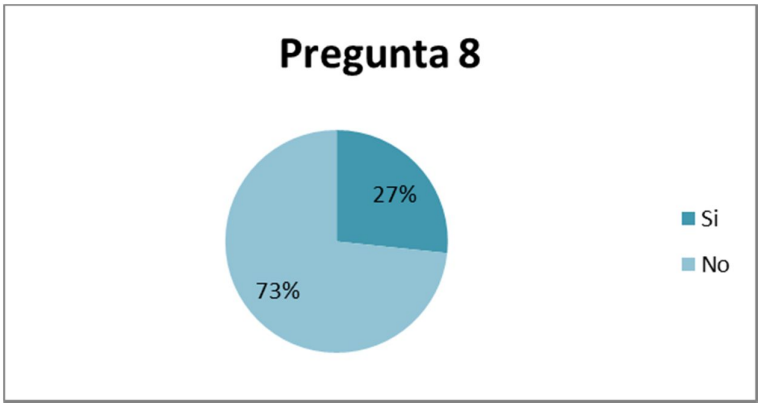



**Figura 11: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 8**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 11 personas que representa el 73% indicaron que no se lleva un registro de los sucesos de eventos de riesgo de TI en la organización; 4 personas que corresponde al 27% mencionaron que si se lleva un registro.

Interpretación. - Según las respuestas obtenidas se identifica que no se lleva un registro de los sucesos de eventos de riesgo de TI en la organización.

Pregunta 9. Cuando suscita un incidente de riesgos de TI, ¿se ejecuta alguna acción para evitar que ocurra nuevamente o para reducir su impacto?

**Tabla 13: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 9**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 7 | 47% | 47% |
| No | 8 | 53% | 100% |
| **Total** | 15 | 100% | |

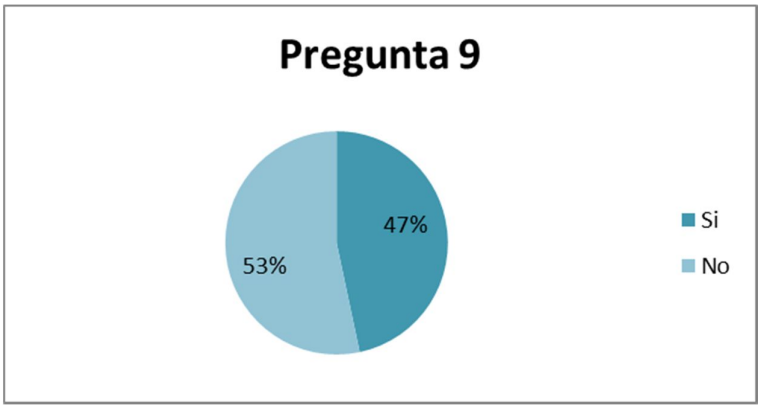



**Figura 12: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 9**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 8 personas que representa el 53% indicaron que cuando suscita un incidente de riesgos de TI no se ejecuta ninguna acción para evitar que ocurra nuevamente o para reducir su impacto; 7 personas que corresponde al 47% mencionaron que si se ejecutan acciones.

Interpretación. - Según las respuestas obtenidas se identifica que cuando suscita un incidente de riesgos de TI no se ejecuta ninguna acción para evitar que ocurra nuevamente o para reducir su impacto.

Pregunta 10. ¿Existen acuerdos de nivel de servicio con los proveedores de los aplicativos en producción?

**Tabla 14: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 10**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 7 | 47% | 47% |
| No | 8 | 53% | 100% |
| **Total** | 15 | 100% | |

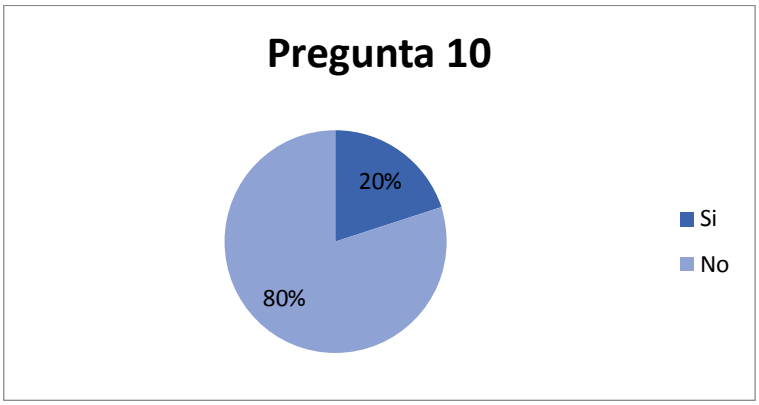



**Figura 13: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 10**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 8 personas que representa el 53% indicaron que no existen acuerdos de nivel de servicio con los proveedores de los aplicativos en producción; 7 personas que corresponde al 47% mencionaron que si existen.

Interpretación. - Según las respuestas obtenidas se identifica que no existen acuerdos de nivel de servicio con los proveedores de los aplicativos en producción.

Pregunta 11. ¿Conoce las debilidades y amenazas que afectan a la infraestructura y servicios de su departamento de TI?

**Tabla 15: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 11**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 3 | 20% | 20% |
| No | 12 | 80% | 100% |
| **Total** | 15 | 100% | |

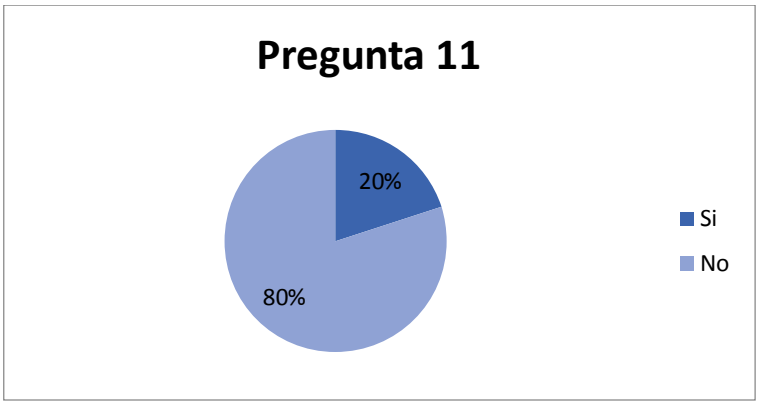



**Figura 14: Encuesta - Punto 3 Identificación y gestión de riesgos - Pregunta 11**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 12 personas que representa el 80% indicaron que no conocen las debilidades y amenazas que afectan a la infraestructura y servicios de su departamento de TI; 3 personas que corresponde al 20% mencionaron que si conocen.

Interpretación. - Según las respuestas obtenidas se identifica que los colaboradores no conocen las debilidades y amenazas que afectan a la infraestructura y servicios de su departamento de TI.

**Punto 4. Continuidad del negocio**

Pregunta 12. ¿Se incluye dentro de la planificación estratégica de la organización la gestión de la continuidad del negocio?

**Tabla 16: Encuesta - Punto 4 Continuidad del negocio - Pregunta 12**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 3 | 20% | 20% |
| No | 12 | 80% | 100% |
| **Total** | 15 | 100% | |

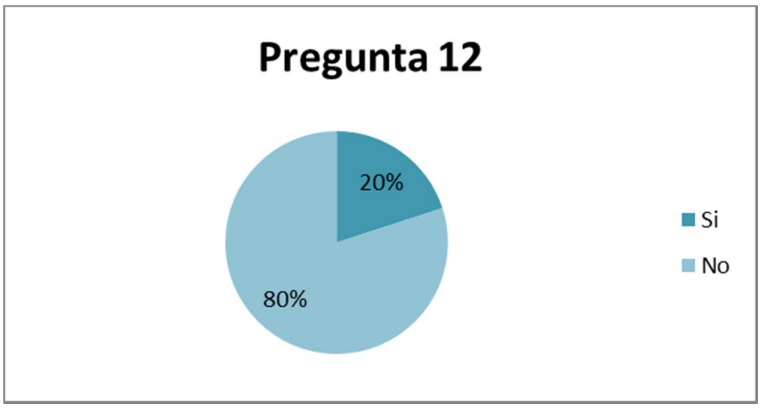



**Figura 15: Encuesta - Punto 4 Continuidad del negocio - Pregunta 12**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 12 personas que representa el 80% indicaron que no se considera dentro de la planificación estratégica de la organización la gestión de la continuidad del negocio; 3 personas que corresponde al 20% mencionaron que si se considera.

Interpretación. - Según las respuestas obtenidas se identifica que no se considera dentro de la planificación estratégica de la organización la gestión de la continuidad del negocio.

Pregunta 13. ¿Existe en la organización una persona o entidad responsable de garantizar la disponibilidad de los servicios de TI?

**Tabla 17: Encuesta - Punto 4 Continuidad del negocio - Pregunta 13**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 12 | 80% | 80% |
| No | 3 | 20% | 100% |
| **Total** | 15 | 100% | |

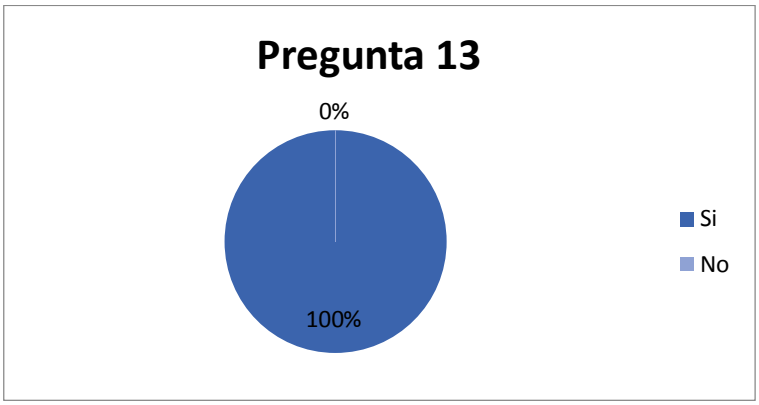



**Figura 16: Encuesta - Punto 4 Continuidad del negocio - Pregunta 13**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 3 personas que representa el 20% indicaron que no existe en la organización una persona o entidad responsable de garantizar la disponibilidad de los servicios de TI; 12 personas que corresponde al 80% mencionaron que si existe.

Interpretación. - Según las respuestas obtenidas se identifica que si existe en la organización una persona o entidad responsable de garantizar la disponibilidad de los servicios de TI.

Pregunta 14. ¿Las interrupciones de los servicios de TI ocasionan deterioro de la imagen de la organización, deserción de socios y pérdidas económicas?

**Tabla 18: Encuesta - Punto 4 Continuidad del negocio - Pregunta 14**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 15 | 100% | 100% |
| No | 0 | 0% | 100% |
| **Total** | 15 | 100% | |

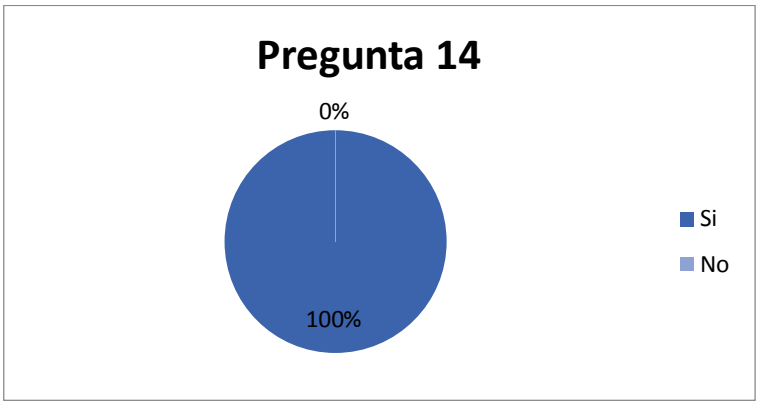



**Figura 17: Encuesta - Punto 4 Continuidad del negocio - Pregunta 14**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 15 personas que representa el 100% indicaron que consideran que las interrupciones de los servicios de TI ocasionan deterioro de la imagen de la organización, deserción de socios y pérdidas económicas; 0 personas que corresponde al 0% mencionaron que no consideran que se deteriore la imagen.

Interpretación. - Según las respuestas obtenidas se identifica que los colaboradores consideran que las interrupciones de los servicios de TI ocasionan deterioro de la imagen de la organización, deserción de socios y pérdidas económicas.

Pregunta 15. ¿El diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de los servicios financieros de la organización?

**Tabla 19: Encuesta - Punto 4 Continuidad del negocio - Pregunta 15**

Elaborado por: Investigador

| Categoría | Frecuencia | Porcentaje | Porcentaje Acumulado |
|---|---|---|---|
| Si | 15 | 100% | 100% |
| No | 0 | 0% | 100% |
| **Total** | 15 | 100% | |

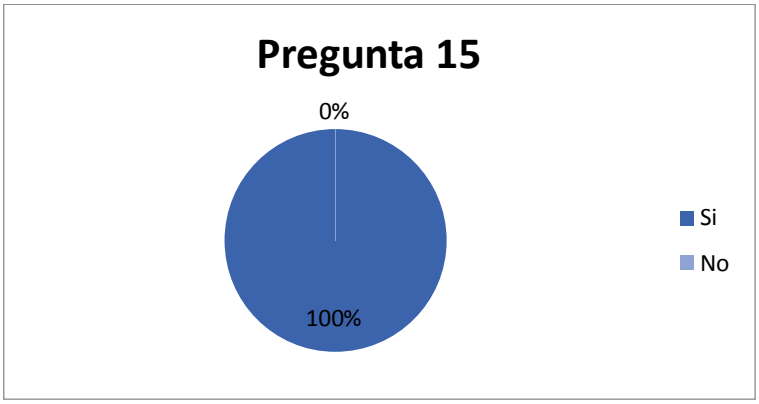



**Figura 18: Encuesta - Punto 4 Continuidad del negocio - Pregunta 15**

Elaborado por: Investigador

Análisis. - En la encuesta realizada a 15 personas, 15 personas que representa el 100% indicaron que consideran que el diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de los servicios financieros de la organización; 0 personas que corresponde al 0% mencionaron que no.

Interpretación. - Según las respuestas obtenidas se identifica que los colaboradores consideran que el diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de los servicios financieros de la organización.

### 4.1.2 Validación de las respuestas obtenidas

Para la validación de las respuestas obtenidas en la encuesta se utilizará una prueba de chi-cuadrado, es una prueba estadística de hipótesis que compara la distribución observada de los datos con una distribución esperada de los datos.

$H_0$ indica que ambas variables son independientes, mientras que $H_i$ indica que las variables tienen algún grado de asociación. Se usa la siguiente fórmula:

$$\chi_c^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$$

Dónde:

O representa la frecuencia observada
E representa la frecuencia esperada

Para la comprobación de la hipótesis , se plantea la hipótesis de trabajo ($H_i$) y la hipótesis nula ($H_o$):

**$H_o$** = El diseño del plan de contingencia y continuidad del negocio no mejorará la disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

**$H_i$** = El diseño del plan de contingencia y continuidad del negocio si mejorará la disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

Para cada variable dependiente e independiente se procede a seleccionar una pregunta, con esto se crea una primera tabla cruzada de frecuencia observada:

**Frecuencia Observada**

Variable independiente: Pregunta 15

Variable dependiente: Pregunta 1

**Tabla 20: Frecuencia Observada**

Elaborado por: Investigador

| Categoría /Pregunta | Pregunta 1 | Pregunta 15 |
|---|---|---|
| Si | 3 | 15 |
| No | 12 | 0 |

Basándose en los valores registrados en la tabla de frecuencia observada, se calcula la tabla de frecuencia esperada:

**Frecuencia Esperada**

**Tabla 21: Frecuencia Esperada**

Elaborado por: Investigador

| Categoría /Pregunta | Pregunta 1 | Pregunta 15 |
|---|---|---|
| Si | 9 | 9 |
| No | 6 | 6 |

Con los valores de las tablas de frecuencia observada y esperada se procede a calcular la matriz de Chi cuadrado calculado:

**Tabla 22: Chi cuadrado calculado**

Elaborado por: Investigador

| Frecuencia Observada O | Frecuencia Esperada E | O-E | (O-E)2 | (O-E)2/E |
|---|---|---|---|---|
| 3 | 9 | -6 | 36 | 4 |
| 12 | 6 | 6 | 36 | 6 |
| 15 | 9 | 6 | 36 | 4 |
| 0 | 6 | -6 | 36 | 6 |
| | Chi cuadrado calculado $X^2$ | | | 20 |

Para tomar una decisión se debe relacionar con el chi cuadrado tabular para lo cual se establece el grado de libertad y el alfa que será de 0,95, ya que se busca una probabilidad de ocurrencia del 95%, para los grados de libertad se toma el orden de la matriz de la frecuencia observada y se aplica la siguiente fórmula:

Cálculo de chi cuadrado crítico:

$\alpha = 0.01$
*Grados de libertad gl* = (#filas-1)(#columnas-1)
*Grados de libertad gl* = (2-1) (2-1)
*Grados de libertad gl = 1*

Obtenido el alfa y los grados de libertad se selecciona el valor de chi cuadrado tabular en la figura 19: **3,841**

| n | 0,995 | 0,99 | 0,975 | 0,95 | 0,9 | 0,75 |
|---|---|---|---|---|---|---|
| 1 | 7,879 | 6,635 | 5,024 | 3,841 | 2,706 | 1,323 |
| 2 | 10,597 | 9,210 | 7,378 | 5,991 | 4,605 | 2,773 |
| 3 | 12,838 | 11,345 | 9,348 | 7,815 | 6,251 | 4,108 |
| 4 | 14,860 | 13,277 | 11,143 | 9,488 | 7,779 | 5,385 |
| 5 | 16,750 | 15,086 | 12,833 | 11,070 | 9,236 | 6,626 |
| 6 | 18,548 | 16,812 | 14,449 | 12,592 | 10,645 | 7,841 |
| 7 | 20,278 | 18,475 | 16,013 | 14,067 | 12,017 | 9,037 |
| 8 | 21,955 | 20,090 | 17,535 | 15,507 | 13,362 | 10,219 |
| 9 | 23,589 | 21,666 | 19,023 | 16,919 | 14,684 | 11,389 |
| 10 | 25,188 | 23,209 | 20,483 | 18,307 | 15,987 | 12,549 |
| 11 | 26,757 | 24,725 | 21,920 | 19,675 | 17,275 | 13,701 |
| 12 | 28,300 | 26,217 | 23,337 | 21,026 | 18,549 | 14,845 |

**Figura 19: Valor chi cuadrado tabular**

Fuente: Fórmula Chi cuadrado

**Decisión**

Chi cuadrado calculado (20,00) es mayor que chi cuadrado tabular (3,841), en consecuencia se valida la hipótesis $H_i$ y se rechaza la nula $H_o$ es decir:

El diseño del plan de contingencia y continuidad del negocio mejorará la disponibilidad de los servicios financieros de las cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

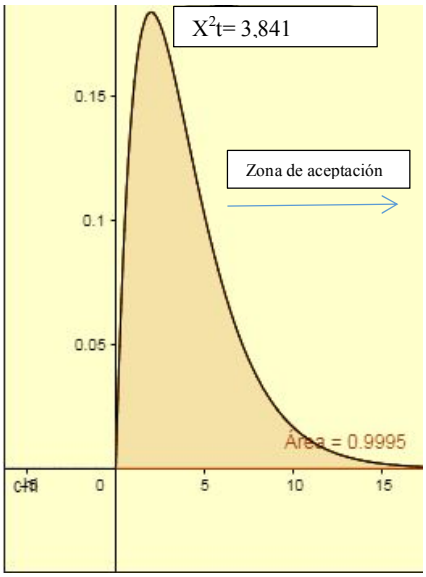



**Figura 20: Distribución de chi cuadrado**

# CAPITULO V

## 5. CONCLUSIONES Y RECOMENDACIONES

### 5.1 Conclusiones

No existe un plan documentado en donde se indique que hacer frente a una suspensión de servicios de TI, por lo tanto los colaboradores no conocen que acciones deben llevar a cabo durante y después de un incidente.

Existe desconocimiento en cuanto a normativa y regulaciones de continuidad del negocio, los colaboradores no conocen el tiempo que la organización puede tolerar la falta de funcionamiento de sus sistemas informáticos de acuerdo a las disposiciones de los entes de control.

No existen procedimientos documentados de respaldo y restauración de información, tampoco se han definido formalmente funciones para cada integrante del departamento de TI en caso de una interrupción de servicios, generando riesgo operativo.

No se ha identificado las debilidades y amenazas que afectan a la infraestructura y servicios del departamento de TI, tampoco se han identificado los activos y servicios críticos, imposibilitando realizar una efectiva gestión de riesgos.

La gestión de riesgos es inadecuada, no se lleva un registro de los sucesos de eventos de riesgo de TI, no se ejecuta ninguna acción para evitar que ocurra nuevamente o para reducir su impacto, ni existen acuerdos de nivel de servicio con los proveedores de los aplicativos en producción.

Dentro de la planificación estratégica de la organización no se incluye la gestión de la continuidad del negocio, pero si se ha designado una persona responsable de garantizar la disponibilidad de los servicios de TI.

Las interrupciones de los servicios de TI ocasionan deterioro de la imagen de la organización, deserción de socios y pérdidas económicas.

La falta de un plan de contingencia y continuidad del negocio perjudica la disponibilidad de los servicios financieros de la organización.

## 5.2 Recomendaciones

El director del departamento de TI debe levantar y documentar procedimientos de respaldo y restauración de información con responsables, cuyas funciones estén claramente identificadas, reduciendo riesgo operativo.

El director del departamento de TI conjuntamente con el oficial de riesgos de la institución deben identificar las debilidades y amenazas que afectan a la infraestructura y servicios del departamento de TI, especificando los activos y servicios críticos, con el objetivo de realizar una efectiva gestión de riesgos. Es necesario llevar un registro de los sucesos de eventos de riesgo de TI, e implementar acciones para evitar que ocurran nuevamente o para reducir su impacto.

El director de TI conjuntamente con el tesorero de la cooperativa debe levantar acuerdos de nivel de servicio con los proveedores de los aplicativos en producción, garantizando un aceptable tiempo objetivo de respuesta y recuperación.

Ante la inminente probabilidad de incidentes de tecnología de la información a los que las empresas están expuestas, se recomienda realizar una evaluación y análisis de riesgos basado en metodologías y estándares internacionales.

La alta dirección debe incluir dentro de la planificación estratégica de la organización la gestión de la continuidad del negocio, designando las personas responsables de gestionar la disponibilidad de los servicios.

El director del departamento de TI debe diseñar un plan de contingencia y continuidad del negocio basado en estándares internacionales, cumpliendo con las normativas de los entes de control para mejorar la disponibilidad de los servicios financieros de la Cooperativa.

# CAPITULO VI

## 6. PROPUESTA

### 6.1 Datos informativos

#### 6.1.1 Título

Diseño del plan de contingencia y continuidad del negocio para cooperativas de ahorro y crédito del segmento uno del cantón Ambato.

#### 6.1.2 Institución ejecutora

Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda.

#### 6.1.3 Beneficiarios

- Alta gerencia
- Departamento de TI
- Directores de área
- Oficial de riesgos
- Jefes de agencia
- Usuarios del sistema
- Socios

#### 6.1.4 Ubicación

Ambato-Tungurahua

#### 6.1.5 Responsable

Ing. Susana del Pilar Ibarra Canseco

#### 6.1.6 Director

Ing. David Omar Guevara Aulestia, MSc.

### 6.2 Antecedentes de la propuesta

El departamento de Tecnología de la Información (TI), de la Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda., es esencial para el normal desarrollo de los procesos críticos de la institución. Todos los procesos están necesariamente apoyados en sistemas de información y de comunicación. De acuerdo a la investigación desarrollada se ha podido concluir que:

La gestión de riesgos es inadecuada, no se lleva un registro de los sucesos de eventos de riesgo de TI, no se ejecuta ninguna acción para evitar que ocurra nuevamente o para reducir su impacto, ni existen acuerdos de nivel de servicio con los proveedores de los aplicativos en producción.

Dentro de la planificación estratégica de la organización no se incluye la gestión de la continuidad del negocio, pero si se ha designado una persona responsable de garantizar la disponibilidad de los servicios de TI.

Las interrupciones de los servicios de TI ocasionan deterioro de la imagen de la organización, deserción de socios y pérdidas económicas.

La falta de un plan de contingencia y continuidad del negocio perjudica la disponibilidad de los servicios financieros de la organización.

### 6.3 Justificación

Como resultado del análisis realizado a la criticidad de los servicios de TI, se identifica la necesidad de implementar un plan de contingencia y continuidad del negocio que garantice la disponibilidad de los servicios financieros de la Cooperativa. El mismo que de acuerdo a la Constitución del Estado Ecuatoriano - Normas Generales para las Instituciones Del Sistema Financiero debe tomar como referencia el estándar ISO 22301, que tiene por nombre "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio".

### 6.4 Objetivos

#### General

Definir las acciones, procedimientos y recursos necesarios para garantizar la restauración de los servicios de la dirección de tecnología de la información que soportan los procesos críticos del negocio, ante la inminente probabilidad de un

incidente, cumpliendo con los tiempos y puntos objetivos de recuperación aprobados por la alta dirección.

**Específicos**

- Determinar la probabilidad de ocurrencia y el impacto de los riesgos que afectan a los servicios de tecnología de la información.
- Documentar de forma clara y precisa las acciones a ejecutar en una contingencia.
- Establecer la estrategia, tiempo y puntos objetivos de recuperación de los servicios de tecnología de la información acorde con los objetivos estratégicos de la organización.

## 6.5 Análisis de factibilidad

### 6.5.1 Factibilidad operativa

Se cuenta con la aprobación y el interés de la alta dirección de la Cooperativa, que facilita el acceso a la información, infraestructura y recursos para diseñar el plan de contingencia y continuidad del negocio.

### 6.5.2 Factibilidad económica

La propuesta no representa un costo adicional para la Cooperativa, debido a que el investigador será responsable de todo el diseño del plan y utilizará sus propios recursos.

### 6.5.3 Factibilidad técnica

Se cuenta con autorización para que el personal de la Cooperativa proporcione acceso al investigador a su plataforma tecnológica, para el diseño del presente plan.

### 6.5.4 Factibilidad legal

La propuesta aporta al cumplimiento de leyes y normativas emitidas por entes de control que regulan las actividades de la Cooperativa, así como al cumplimiento del reglamento, manuales y procedimientos internos.

## 6.6 Fundamentación

### 6.6.1 Como implementar un plan de contingencia y continuidad del negocio

Según Fernández y Velthuis (Fernández & Velthuis, 2012), para el éxito del plan es necesario integrar las siguientes tareas claves:

- Documentar y evidenciar la necesidad de contar con un plan de contingencia y continuidad del negocio ante la alta dirección.
- Determinar el alcance del plan.
- Evaluar y reducir los riesgos asociados.
- Realizar el análisis de impacto en el negocio.
- Priorizar las funciones críticas.
- Desarrollar estrategias y pasos para recuperarse de un incidente.
- Definir responsables y tareas.
- Escribir los planes.
- Capacitar al personal.
- Ejecutar pruebas del plan.
- Actualizar el plan permanentemente.

### 6.6.2 Análisis de impacto en el negocio

Análisis de impacto en el negocio (***Business Impact Analysis*** BIA, por sus siglas en inglés), permite a las instituciones estimar el impacto operacional y financiero de las interrupciones, provee una base para identificar los procesos críticos para la organización y priorizarlos de acuerdo con su nivel de impacto, identificar cuáles impulsan el negocio, cuáles generan ingresos y cuáles son indispensables para mantenerse operativo. Contiene un detalle de procesos, software, activos, personas y proveedores que están asociados con las actividades críticas de una empresa. Sus objetivos principales son:

- Identificar los procesos críticos relacionados con la misión y objetivos de la organización, que necesitan ser restablecidos a su estado operativo tan pronto como sea posible después de una interrupción.
- Determinar el tiempo máximo tolerable y prioridad con que deben ser restablecidos estos procesos antes de que la organización deje de operar.
- Determinar los recursos necesarios para restablecer los procesos críticos después de la materialización de un riesgo.

#### 6.6.2.1 Determinar el nivel de impacto

El BIA debe contener además la clasificación de la criticidad de cada proceso. De acuerdo, a la resolución de la SEPS especificada en el manual de auditoría interna, como se puede ver en la tabla 23, se considera una escala de 5 niveles de impacto:

**Tabla 23: Niveles de impacto**
Fuente: SEPS

| NIVEL DE IMPACTO | |
|---|---|
| Catastrófico | 10 |
| Crítico | 8 |
| Moderado | 6 |
| Menor | 4 |
| Insignificante | 2 |

De esta forma se podrá obtener una hoja de cálculo con todos los procesos ordenados por su nivel de impacto, definiendo los procesos críticos de la Cooperativa. Dichos resultados deben ser sometidos a consideración de la alta dirección para que sean aprobados y se puedan utilizar en el plan de contingencia y continuidad.

#### 6.6.2.2 Plazo máximo tolerable de interrupción

Para cada proceso documentado en el BIA, es necesario determinar el plazo máximo tolerable de interrupción (MTPD por sus siglas en inglés). El tiempo máximo de tolerancia es el tiempo tras el cual, si el proceso no está disponible, provoca consecuencias irreversibles para la empresa, desde un daño grave en las posibilidades de producción hasta el fracaso material del negocio. El MTPD, dependiendo del negocio y del proceso se puede expresar en horas, días o periodos superiores. Para establecer un MTPD razonable para un proceso se puede usar datos históricos de la organización o incluso de otras organizaciones similares. Estos datos deberán ser validados y aprobados por la alta dirección (Fernández &Velthuis, 2012).

#### 6.6.2.3 Objetivo de tiempo de recuperación

El objetivo de tiempo de recuperación (RTO por sus siglas en inglés), es el periodo óptimo de tiempo en el cual la organización pretende tener nuevamente en operación los procesos interrumpidos. Por definición, el RTO debe ser menor que el MTPD de un proceso; de otra forma no será útil (Fernández &Velthuis, 2012).

El RTO de un proceso es la base para planificar la recuperación del mismo. Por ejemplo, si se requiere un RTO de horas o minutos, se debe considerar una inversión mayor para tener los datos replicados y un data center alterno; en caso de tener un RTO de días, se tiene tiempo para configurar servidores, instalar el software y recuperar los respaldos para volver a tener el producto o servicio operativo.

#### 6.6.2.4 Objetivo de punto de recuperación

El objetivo de punto de recuperación (RPO, por sus siglas en inglés) es la cantidad máxima de datos que la organización puede permitirse perder si un proceso se interrumpe y se recupera más tarde. Si una organización financiera no puede permitirse perder más de 5 minutos de información, debe implementar un data center alterno con réplica de datos temporizada para transmitir archivos cada 5 minutos, en el caso crítico

de empresas como la bolsa de valores o empresas de producción robotizadas no pueden permitirse perder ni un solo minuto, por lo tanto su inversión para tener servidores redundantes y en línea será mucho mayor. Como se observa en la figura 20, los procedimientos de recuperación están dados tanto por el RTO como por el RPO que las necesidades del negocio determinan.

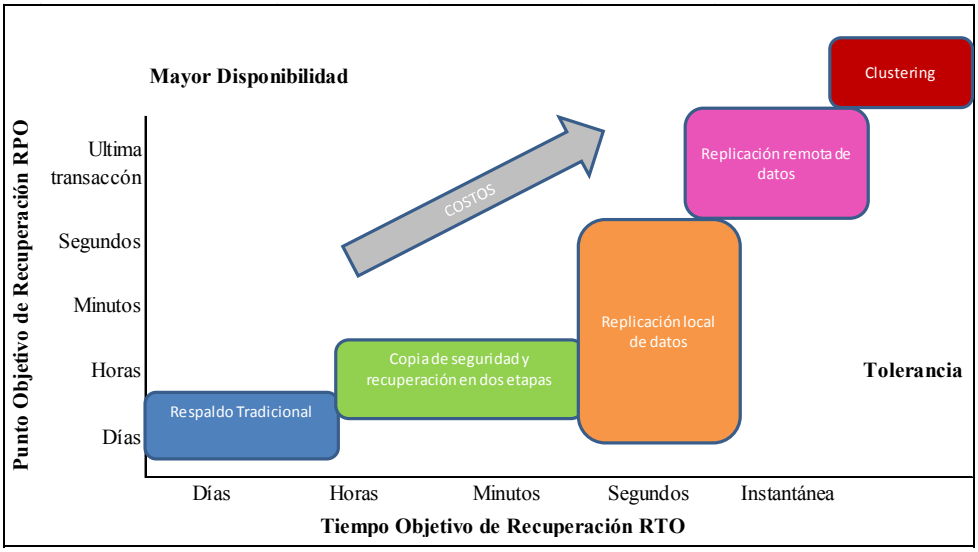



**Figura 21: Tiempo objetivo de recuperación - Punto objetivo de recuperación**

Fuente: Internet, recuperado de https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo

### 6.6.3 Análisis de riesgos

Según Fernández & Velthuis, el proceso de análisis de riesgos permitirá a la organización entender las amenazas y vulnerabilidades que afectan a los procesos críticos que fueron determinados en el BIA y los recursos que estos procesos necesitan para operar (Fernández & Velthuis, 2012).

**Principales factores de riesgo operativo**

Según (ISOtools, 2015) y la normativa de riesgos de la SEPS, los riesgos operativos se dan, sobre todo, en 4 ámbitos:

**1. Recursos humanos**

- Pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude o robo.
- Apropiación indebida de información sensible.
- Lavado de dinero.
- Ambiente laboral desfavorable.
- Errores o falta de las especificaciones necesarias en los términos de contratación del personal, entre otros factores.
- Inadecuada selección de personal por no identificar claramente el perfil que necesita la empresa en cada momento o selección de personas con competencias insuficientes o capacitación inadecuada.
- Formación de personal errónea o insuficiente.

2. **Procesos Internos**

- Diseño inapropiado de los procesos críticos de la organización.
- Políticas y procedimientos inadecuados o inexistentes.
- Desarrollo deficiente de las operaciones.
- Fallos de infraestructura o logísticos o que lleva a la suspensión (temporal o permanente) de la producción o la ejecución de servicios.
- Riesgos asociados a fallos en los modelos utilizados.
- Errores en las transacciones.
- Evaluación inadecuada de contratos.
- Errores de contabilidad.
- Fallos en los cálculos de los recursos necesarios para determinadas operaciones
- Incumplimiento de plazos.
- Presupuestos mal calculados o diseñados.

- Deficiencias en los procesos de gestión de documentación.

**3. Tecnología de Información**

- Ataques informáticos que provoquen el robo de datos de la propia empresa o de terceros.
- Fallos de hardware o software.
- Mal funcionamiento o selección incorrecta de las herramientas informáticas de la empresa.
- Pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías.
- Anormal desarrollo de operaciones y servicios que realiza la compañía por fallos informáticos.
- Pérdida de información o de material informático (hardware y software) por contingencias como: incendios, inundaciones o averías graves.
- Riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas informáticos.
- Errores en el desarrollo e implementación de dichos sistemas y/o su compatibilidad e integración.
- Problemas de calidad de información.
- Inadecuada inversión en tecnología.
- Falla o interrupción de los sistemas.
- Recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

**4. Eventos externos**

- Contingencias legales.
- Fallas en los servicios públicos.
- Desastres naturales, atentados y actos delictivos.
- Cambios en las leyes y normativos.
- Riesgo político del país.

- Revueltas sociales

El análisis de riesgo para un plan de continuidad se realiza con los siguientes pasos:

- Recolección inicial de información.
- Identificación de vulnerabilidades y categorización de amenazas.
- Documentación de eventos de riesgo y acciones para controlar los mismos.
- Definición del impacto.
- Elaboración de la matriz de evaluación de riesgos de continuidad del negocio.
- Revisión y aprobación de la matriz por la alta dirección.

La matriz de análisis de riesgos deberá contener la siguiente información:

- Levantamiento del riesgo
- Análisis de riesgo
- Evaluación del riesgo
- Riesgo residual

De acuerdo al manual de auditoría interna definido por la SEPS, los valores de las diferentes categorías de análisis de riesgos se detallan en la tabla 24.

En la cual, se asignan cifras cuantitativas a las propiedades de la probabilidad (P) y nivel de impacto (I), con valores pares del 2 al 10, siendo 2 el más bajo o insignificante y 10 el más alto o catastrófico.

El producto de estas categorías dan como resultado el nivel de riesgo: (R)= (P)*(I), con valores pares que van del 4 al 100, siendo 4 el nivel de riesgo más bajo y 100 en nivel de riesgo extremo.

**Tabla 24: Categorías de análisis de riesgos**

Fuente: SEPS

| PROBABILIDAD (P) | | NIVEL DE IMPACTO (I) | | RIESGO (P * I) | |
|---|---|---|---|---|---|
| Muy Alta | 10 | Catastrófico | 10 | Riesgo Extremo | 100 |
| Muy Alta | 10 | Crítico | 8 | Riesgo Extremo | 80 |
| Muy Alta | 10 | Moderado | 6 | Riesgo Extremo | 60 |
| Muy Alta | 10 | Menor | 4 | Riesgo alto | 40 |
| Muy Alta | 10 | Insignificante | 2 | Riesgo medio | 20 |
| Alta | 8 | Catastrófico | 10 | Riesgo Extremo | 80 |
| Alta | 8 | Crítico | 8 | Riesgo Extremo | 64 |
| Alta | 8 | Moderado | 6 | Riesgo Extremo | 48 |
| Alta | 8 | Menor | 4 | Riesgo alto | 32 |
| Alta | 8 | Insignificante | 2 | Riesgo medio | 16 |
| Media | 6 | Catastrófico | 10 | Riesgo Extremo | 60 |
| Media | 6 | Crítico | 8 | Riesgo Extremo | 48 |
| Media | 6 | Moderado | 6 | Riesgo alto | 36 |
| Media | 6 | Menor | 4 | Riesgo alto | 24 |
| Media | 6 | Insignificante | 2 | Riesgo medio | 12 |
| Baja | 4 | Catastrófico | 10 | Riesgo alto | 40 |
| Baja | 4 | Crítico | 8 | Riesgo alto | 32 |
| Baja | 4 | Moderado | 6 | Riesgo alto | 24 |
| Baja | 4 | Menor | 4 | Riesgo medio | 16 |
| Baja | 4 | Insignificante | 2 | Riesgo bajo | 8 |
| Muy baja | 2 | Catastrófico | 10 | Riesgo medio | 20 |
| Muy baja | 2 | Crítico | 8 | Riesgo medio | 16 |
| Muy baja | 2 | Moderado | 6 | Riesgo medio | 12 |
| Muy baja | 2 | Menor | 4 | Riesgo bajo | 8 |
| Muy baja | 2 | Insignificante | 2 | Riesgo bajo | 4 |

Una vez identificados y medidos los riesgos la empresa debe documentar los controles que le permitirán reducir la probabilidad de una interrupción y evitar en lo posible que, en caso de materializarse un incidente, se interrumpan las operaciones, en las tablas 25,26,27 se detalla las categorías para evaluar el nivel del control del riesgo.

**Tabla 25: Tipo de control**

Fuente: Basilea

| Tipo | Descripción |
|---|---|
| Preventivo | Es un control orientado a prevenir el origen del riesgo antes de que se genere. |
| Correctivo | Es un control que se ejecuta durante el proceso, cuando el incidente se ha materializado y se debe corregir. |
| Evaluativo | Es un control clave que únicamente actúa cuando el proceso ha terminado. |

**Tabla 26: Período de control**

Fuente: Basilea

| Tipo | Descripción |
|---|---|
| Permanente | Controles aplicados durante todo el proceso diaria o semanalmente. |
| Periódico | Controles aplicados en forma programada, mensual, trimestral, semestral,anual. |
| Ocasional | Controles aplicados cuando un evento del proceso lo requiere. |

**Tabla 27: Nivel de automatización del control**

Fuente: Basilea

| Tipo | Descripción |
|---|---|
| Automatizado | Controles realizados por un conjunto de elementos tecnológicos. |
| Semi-automátizado | Controles realizados con la ayuda de elementos tecnológicos. |
| Manual | Controles realizados con la intervención humana. |

En base a la evaluación de estos parámetros se determina el grado de eficiencia del control del riesgo, en la tabla 28:

**Tabla 28: Grado de eficiencia del control**

Fuente: Basilea

| Periodicidad (P) | Automatización (A) | Oportunidad (O) | Eficacia | Valor |
|---|---|---|---|---|
| Permanente | Automatizado | Preventivo | Optimo | 10 |
| Permanente | Semi-automatizado | Preventivo | Optimo | 10 |
| Permanente | Manual | Preventivo | Optimo | 10 |
| Permanente | Automatizado | Correctivo | Optimo | 10 |
| Permanente | Semi-automatizado | Correctivo | Optimo | 10 |
| Permanente | Manual | Correctivo | Optimo | 10 |
| Permanente | Automatizado | Evaluativo | Muy bueno | 8 |
| Permanente | Semi-automatizado | Evaluativo | Muy bueno | 8 |
| Permanente | Manual | Evaluativo | Muy bueno | 8 |
| Periódico | Automatizado | Preventivo | Muy bueno | 8 |
| Periódico | Semi-automatizado | Preventivo | Muy bueno | 8 |
| Periódico | Manual | Preventivo | Muy bueno | 8 |
| Periódico | Automatizado | Correctivo | Bueno | 6 |
| Periódico | Semi-automatizado | Correctivo | Bueno | 6 |
| Periódico | Manual | Correctivo | Bueno | 6 |
| Periódico | Automatizado | Evaluativo | Bueno | 6 |
| Periódico | Semi-automatizado | Evaluativo | Bueno | 6 |
| Periódico | Manual | Evaluativo | Bueno | 6 |
| Ocasional | Automatizado | Preventivo | Regular | 4 |
| Ocasional | Semi-automatizado | Preventivo | Regular | 4 |
| Ocasional | Manual | Preventivo | Regular | 4 |
| Ocasional | Automatizado | Correctivo | Regular | 4 |
| Ocasional | Semi-automatizado | Correctivo | Regular | 4 |
| Ocasional | Manual | Correctivo | Regular | 4 |
| Ocasional | Automatizado | Evaluativo | Insuficiente | 2 |
| Ocasional | Semi-automatizado | Evaluativo | Insuficiente | 2 |
| Ocasional | Manual | Evaluativo | Insuficiente | 2 |

### 6.6.4 Desarrollo de la estrategia

En base al listado de los procesos críticos que se obtienen en el BIA, a continuación se listan algunos de los campos que se deben incluir para el desarrollo de la estrategia de recuperación:

- Nombre del proceso.
- Descripción del proceso.
- Activos que requiere cada proceso.
- Personal esencial sin el cual el proceso no puede llevarse a cabo.
- Proveedores requeridos para el proceso.
- Declaración de impacto si el proceso falla o se interrumpe.
- Plazo máximo tolerable de interrupción (PMTI).
- Objetivo de tiempo de recuperación (RTO).
- Objetivo de punto de recuperación (RPO).
- Criticidad.

### 6.6.5 Desarrollo del plan

Es necesario que los involucrados estén de acuerdo con el contenido del plan y con las actividades que cada responsable debe ejecutar. El plan debe ser aprobado por la alta dirección.

Según ISO 22301, algunos de los elementos que deberá contener el plan son:

- Una estrategia a seguir en caso de desastre.
- Un procedimiento para la declaración de desastre.
- Listas de contactos de emergencia.
- Selección del equipo que tomará las decisiones.
- Selección del personal que formará el equipo de recuperación.
- Procedimientos para la evaluación de daños.
- Procedimientos para la recuperación y reinicio de los sistemas.
- Procedimientos para el regreso a las operaciones normales.

Cada empresa debe determinar su propia estrategia en función de sus necesidades, prioridades, tipos de activos, legislaciones y regulaciones, RTO y RPO.

El propósito de la estrategia de continuidad de negocio es identificar las medidas que permitan a la organización restablecer sus actividades críticas dentro de los tiempos establecidos como objetivos de recuperación.

Fernández y Velthuis proponen una estrategia de activación del plan de recuperación ante desastres que comprende cinco fases (Fernández & Velthuis, 2012):

**Fase I: respuesta inicial:**

- Salvaguardar al personal y a las instalaciones.
- Evaluar la activación del plan de continuidad de negocio o plan de recuperación ante desastres.
- Activar la notificación del desastre a los involucrados.
- Notificar al centro alternativo (en caso de contar con estas instalaciones).

**Fase II: medidas intermedias de contingencia:**

- Establecer líneas alternas de comunicación con empleados, usuarios, autoridades, proveedores, clientes y medios de comunicación.
- Establecer un centro de control fuera del centro primario.
- Revisar y aprobar la prioridad de la lista de productos y servicios para reiniciar operaciones en el centro alternativo.

**Fase III: aprovisionamiento de recursos:**

- Habilitar el centro alternativo: sistemas propios del negocio y comunicaciones.
- Verificar la operación de servicios y productos a habilitar en el centro alternativo.
- Disponer de recursos monetarios para la operación en el centro alternativo.

**Fase IV: reanudación de negocio en centro alternativo:**

- Habilitar al personal en el centro alternativo de acuerdo con las posiciones asignadas.
- Coordinar las actividades del personal de acuerdo con roles, asignaciones y prioridades.
- Iniciar de forma coordinada las actividades mínimas requeridas del negocio.
- Validar la infraestructura y la operación de los sistemas iniciados.
- Dar aviso del inicio de operaciones a usuarios, autoridades, proveedores, clientes y medios (o solo a quien corresponda, conforme a la estrategia planteada).
- Monitorizar la operación para validar los niveles de servicio ofrecidos.

**Fase V: restablecer centro primario:**

- Activar tareas de recuperación y restablecimiento del centro primario.
- Restablecer (comprar o reparar) la infraestructura afectada del centro primario.
- Habilitar la operación normal.
- Dar aviso del reinicio de operaciones normales a usuarios críticos, autoridades, proveedores, clientes, empleados y medios (o solo a quien corresponda, conforme a la estrategia planteada).
- Monitorizar la operación.

Para el diseño del plan se debe considerar que los procedimientos a definir y documentar deberán ser completos, sencillos y fáciles de seguir y ejecutar, considerando que se llevarán a cabo en situaciones de estrés con poco tiempo y recursos mínimos.

Los procedimientos deben seguir el mismo formato que la institución tenga definido para sus otros procesos, con el cual el personal está familiarizado. Debe existir un registro de las actividades y decisiones tomadas durante la interrupción con el objetivo de mejorar los procesos.

### 6.6.6 Difusión y capacitación

El plan de contingencia y continuidad del negocio debe ser difundido, explicado, practicado entre los empleados de la organización, de forma que se asegure su inclusión en la cultura organizacional. Se puede incluir en las charlas de inducción del personal nuevo, en las capacitaciones programadas de seguridad de la información y garantizar que este siempre disponible para los usuarios.

El objetivo es que el empleado conozca y esté consciente de la importancia del plan para la consecución de los objetivos estratégicos de la institución.

### 6.6.7 Pruebas y ejercicios

El objetivo de las pruebas es garantizar que el plan funciona acorde a lo planificado, que los tiempos de recuperación son los calculados y que los riesgos son controlados. La alta dirección de la organización querrá tener la confianza de que las cosas salen según lo planeado en caso de que se presente el desastre, que el esfuerzo e inversiones realizadas son eficientes y eficaces.

Según Fernández y Velthuis las pruebas se establecen bajo las siguientes condiciones:

- Pruebas en papel o pruebas de escritorio.
- Pruebas paso a paso, por procedimiento o por área.
- Simulaciones.
- Pruebas en paralelo.
- Pruebas integrales.

Toda prueba debe ser planificada, debe ser periódica, se debe validar por cada escenario y por cada proceso. No debe afectar la operación de la empresa ni los procesos críticos. Debe contar con el personal que la llevará a cabo. Requiere la

aprobación de la alta dirección para ejecutarse ya que implica el esfuerzo, recursos y tiempo considerables.

En las pruebas individuales pueden identificarse errores y oportunidades de mejora que permitirán corregir el plan, que ahorraran tiempo e incertidumbre en un incidente real.

Toda prueba debe ser registrada y sus resultados evaluados y documentados para tomar acciones correctivas sobre el plan, de ser el caso.

### 6.6.8 Mantenimiento y actualización

Las organizaciones evolucionan, cambian en su estructura, personal, la forma de hacer negocios, agregan y eliminan productos y servicios, cambian de proveedores, etc. Todos estos cambios afectan el plan de continuidad del negocio y deben ser considerados para garantizar que sigue vigente y será efectivo en el momento de ser requerido.

Las principales afectaciones se encuentran en:

- Cambios de tecnología. Mejoras o cambios en el software, hardware y otras tecnologías.
- Cambios en los negocios. Los cambios en los procesos por fusiones y adquisiciones, cambios geográficos.
- Cambios de personal. Los cambios en el organigrama: reestructuraciones, despidos, rotación del personal, cambios en las responsabilidades de departamentos o individuales.
- Cambios del mercado. Cambios en la forma de hacer negocios, en los precios, modificaciones de los productos o servicios, incluso cambios en los consumidores y en la forma de entregar los productos o servicios.

- Cambios externos. Cambios políticos, clima, regulaciones, etc (Fernández & Velthuis, 2012).

## 6.7 Elaboración de la propuesta

Diseño del plan de contingencia y continuidad del negocio para cooperativas de ahorro y crédito del segmento 1 del cantón Ambato"

### 6.7.1 Antecedentes

La Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda., en una entidad financiera con más de 30 años al servicio de la comunidad ecuatoriana, regulada por la Superintendencia de Economía Popular y Solidaria (SEPS). La Cooperativa no cuenta con un plan de contingencia y continuidad del negocio que cumpla con metodologías y estándares internacionales que garanticen la eficacia de la estrategia de recuperación de los servicios críticos ante la materialización de incidentes de riesgo.

**Misión**

Brindar productos y servicios financieros con la más alta calidad que promuevan el desarrollo socioeconómico de los socios, contando con el recurso humano capaz y motivado para construir una organización más sólida, rentable y segura, siendo una entidad que profundiza el proceso de constitución de un sistema económico, social y solidario, en el que los seres humanos son el fin.

**Visión**

Ser una Cooperativa innovadora y líder en productos y servicios financieros, sustentados en la prevalencia de las personas por sobre el capital, en el alto desempeño del recurso humano y el uso de tecnología de vanguardia.

**Servicios**

- Ahorros
- Inversiones
- Préstamos
- Canales electrónicos

**Agencias**

- Ambato
- Baños
- Pelileo
- Píllaro
- Guayaquil
- Guaranda
- San Rafael
- Latacunga
- Quito Norte
- Puyo

**Estructura del departamento de TI**

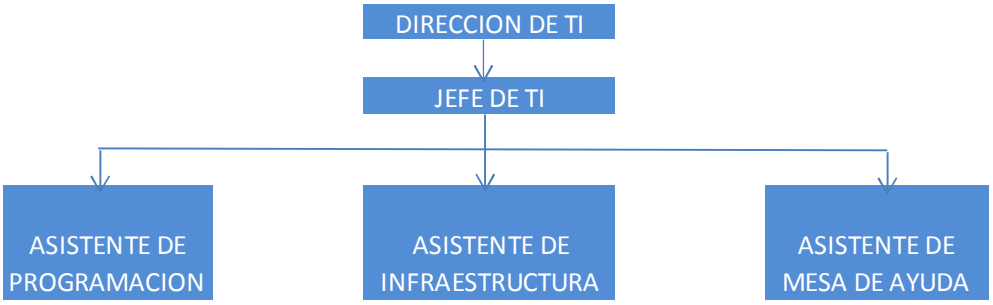



**Figura 22: Estructura departamento de TI**

### 6.7.2 Descripción de plataforma tecnológica

**Tabla 29: Inventario de Servidores**

Elaborado por: Investigador

| Servidor | Objetivo | Ubicación |
|---|---|---|
| SRVCOREPROD | Core financiero producción | Datacenter principal |
| SRVCORECONTIN | Core financiero contingencia | Datacenter alterno |
| SRVBASEPROD | Base de datos, core financiero producción | Datacenter principal |
| SRVBASECONTIN | Base de datos, core financiero contingencia | Datacenter alterno |
| SRVDESARROLLO | Desarrollo core financiero | Datacenter principal |
| SRVDIRECTORIO | Directorio active | Datacenter principal |
| SRVRML | Sistema RML | Datacenter principal |
| SRVTELEFONIA | Telefonia IP | Datacenter principal |
| SRVCORREO | Correo electrónico | Datacenter principal |
| SRVCAJEROS | Cajeros automáticos | Datacenter principal |

**Tabla 30: Inventario de sistemas**

Elaborado por: Investigador

| Sistema | Objetivo | Proveedor | Responsable |
|---|---|---|---|
| Core financiero | Plataforma de servicios financieros | Softwarehouse | Director de TI |
| RML | Control y gestión de riesgos | | Jefe de TI |
| Vip | Prevención de lavado de activos | VIP S.A. | Jefe de TI |
| Zimbra | Correo electrónico | | Asistente de infraestructura |
| Active directory | Administración de usuarios del directorio activo | | Jefe de TI |
| Elastix | Sistema de telefonía ip | Sistemtronic | Asistente de infraestructura |
| Filelym | Sistema para almacenar bóvedas de documentos escaneados | | Jefe de TI |

**Diagrama de red**

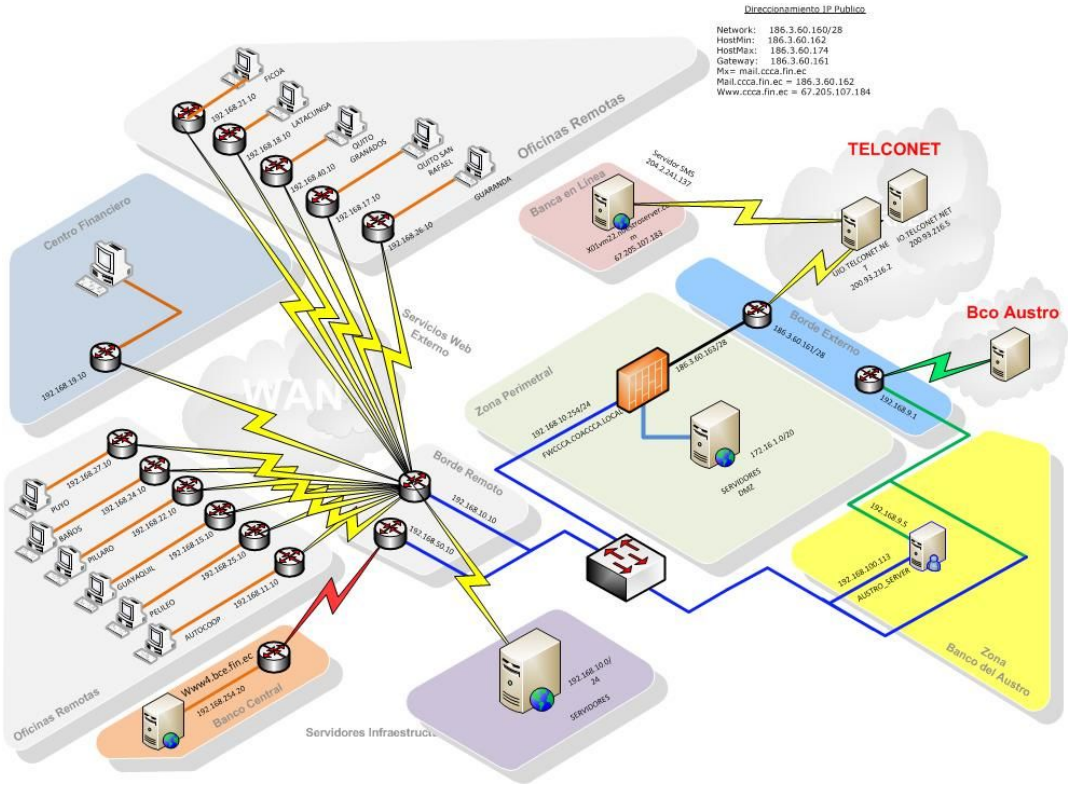



Figura 23: Diagrama de red Fuente: CCCA

### 6.7.3 Procesos de TI

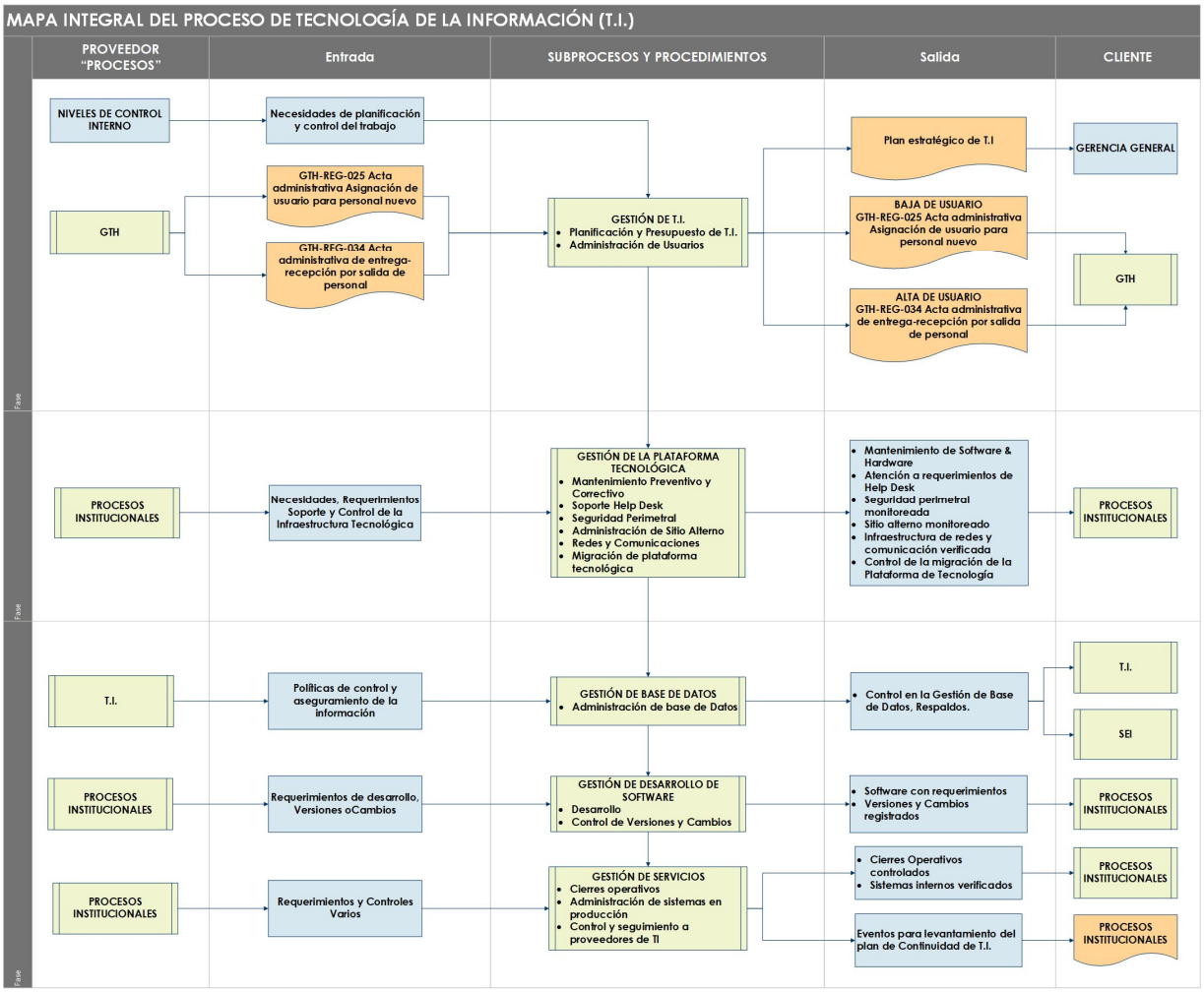



**Figura 24: Procesos de TI**

Fuente: CCCA

### 6.7.4 Alcance

El presente plan esta desarrollado en base al estándar internacional ISO 22301 y la metodología de gestión de riesgos Basilea, tomando en consideración las disposiciones de los entes de control para cooperativas de ahorro y crédito; contempla el planear, establecer, implementar, operar, monitorear, revisar y continuamente mejorar un sistema de gestión de continuidad documentada, preparando a la cooperativa para, responder y recuperarse de interrupciones. Protege la disponibilidad de los servicios de

la dirección de tecnología de la información para toda la organización, priorizando la recuperación de los servicios críticos del negocio en todas las agencias de la institución, cumpliendo con los tiempos y puntos objetivos de recuperación aprobados por la alta dirección.

### 6.7.5 Políticas

El oficial de riesgos y el director de TI son los responsables de la administración y gestión del plan de contingencia y continuidad del negocio desde el diseño hasta la ejecución y mantenimiento permanente.

Los dueños de procesos críticos, deben intervenir activamente y desarrollar conjuntamente con el oficial de riesgos el plan de contingencia y continuidad del negocio.

La alta dirección es la encargada de aprobar el plan, autorizar su ejecución y controlar que las direcciones de los procesos críticos ejecuten las acciones preventivas y de control descritas en el plan.

La organización debe contar con infraestructura para garantizar la recuperación de las operaciones y no podrá ser usada para otro fin.

Las pruebas controladas del plan de contingencia y continuidad del negocio, se realizarán de forma periódica y planificada y sus resultados serán registrados y documentados.

Todos los colaboradores y proveedores que tengan asignadas tareas en la ejecución del plan deberán ser capacitados y evaluados además de participar en los ejercicios del mismo.

El plan debe ser difundido, precautelando el acceso según la confidencialidad de la información, a los colaboradores, directivos y proveedores afectados.

En una contingencia, la alta dirección de la Cooperativa será la encargada de establecer los lineamientos y dar la autorización para emitir comunicados a los interesados, medios, socios y entes de control.

El Plan de contingencia y continuidad del negocio, deberá revisarse porlo menos una vez al año, o cada vez que exista un cambio en procesos, recursos, tecnología o en el negocio que lo amerite.

Todo evento de riesgo materializado debe ser debidamente registrado y documentado.

En el presupuesto anual de la Cooperativa debe contemplarse un rubro para la implementación, ejecución y control del plan de contingencia y continuidad del negocio.

### 6.7.6 Análisis de riesgo

#### 6.7.6.1 Metodología

**Basilea**

La metodología de control de riesgos de la Cooperativa está basada en los principios de buenas prácticas para la gestión y supervisión del riesgo operativo de Basilea.

Los Acuerdos de Basilea son los acuerdos de supervisión bancaria o recomendaciones sobre regulación bancaria emitidos por el Comité de Basilea de Supervisión Bancaria. Están formados por los acuerdos Basilea I, Basilea II y Basilea III. Reciben su nombre a partir de la ciudad de Basilea, Suiza, donde el CBSB mantiene su secretariado en la sede del Banco de Pagos Internacionales(Comité de Supervisión Bancaria de Basilea, 2003).

#### 6.7.6.2 Mapa de calor

| | | | | Probabilidad de ocurrencia | | |
|---|---|---|---|---|---|---|
| | | | | Bajo | Medio | Alto |
| | | | Frecuencia | 0.9 | 5 | 12 |
| | | | Probabilidaddias/año | 5 | 8 | 12 |
| | | | | 1 | 2 | 3 |
| Categoria de impacto | Alto | $4,800.00 | 3 | $4,320.00 | $24,000.00 | $57,600.00 |
| | Medio | $3,200.00 | 2 | $2,880.00 | $16,000.00 | $38,400.00 |
| | Bajo | $1,600.00 | 1 | $1,440.00 | $8,000.00 | $19,200.00 |

**Figura 25: Mapa de calor**

Fuente: CCCA

| | Categoria | Valor | Descripción |
|---|---|---|---|
| Probabilidad de ocurrencia | Alto | 3 | Riesgo con alta probabilidad de ocurrencia, 10 veces al año. |
| | Medio | 2 | Riesgo con probabilidad de ocurrencia media, 5 veces al año. |
| | Bajo | 1 | Riesgo con baja probabilidad de ocurrencia, 2 veces al año. |

**Figura 26: Probabilidad de ocurrencia**

Fuente: CCCA

| | Categoria | Valor | Descripción |
|---|---|---|---|
| Categoria de impacto | Alto | 3 | Riesgo que impide la ejecución del proceso y la consecución de sus objetivos. |
| | Medio | 2 | Riesgo que perjudica la ejecución del proceso, dificultando la consecución de sus objetivos. |
| | Bajo | 1 | Riesgo con leve efecto sobre la ejecución del proceso, no perjudica al cumplimiento de objetivos. |

**Figura 27: Categoría de impacto**

Fuente: CCCA

### 6.7.6.3 Análisis de amenazas y vulnerabilidades

El Business Impact Analysis (BIA), es un proceso dedicado a identificar y evaluar los efectos potenciales ya sean financieros, de seguridad, legales, regulatorios o de reputación que los incidentes de riesgo que puedan causar en las operaciones del negocio.

Sus objetivos son proveer una base para identificar los procesos críticos en la marcha de la organización y priorizarlos, considerando que a mayor impacto, mayor será la prioridad.

Es necesario definir el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés), es el período de tiempo permitido para la recuperación de una actividad, y el Punto Objetivo de Recuperación (RPO por sus siglas en inglés) que es la cantidad máxima de datos que se permite perder para su restauración, es decir, la tolerancia que el negocio admitir para trabajar con datos de respaldo, en consecuencia el RPO está dado en base a la naturaleza y actividades críticas del negocio, como se describe en la tabla 31.

**Tabla 31: Nivel de criticidad**

Fuente: CCCA

| Tolerancia | | Impacto | | Criticidad | |
|---|---|---|---|---|---|
| Menos de 3 horas | 3 | Mayor | 6 | Alta | 9 |
| Menos de 3 horas | 3 | Importante | 4 | Alta | 7 |
| Menos de 3 horas | 3 | Menor | 2 | Media | 5 |
| Menos de 8 horas | 2 | Mayor | 6 | Alta | 8 |
| Menos de 8 horas | 2 | Importante | 4 | Alta | 6 |
| Menos de 8 horas | 2 | Menor | 2 | Media | 4 |
| Mas de 24 horas | 1 | Mayor | 6 | Alta | 7 |
| Mas de 24 horas | 1 | Importante | 4 | Media | 5 |
| Mas de 24 horas | 1 | Menor | 2 | Baja | 3 |

| Nivel de criticidad | |
|---|---|
| Alta | <10 |
| Media | <6 |
| Baja | <3 |

### 6.7.6.4 Matriz de riesgo

| LEVANTAMIENTO DEL EVENTO DE RIESGO | | | | | |
|---|---|---|---|---|---|
| **PROCESO** | **FACTOR** | **RIESGO** | **DESCRIPCIÓN** | **CAUSAS** | **CONSECUENCIAS** |
| Administración de base de datos | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento. | Daño de discos.<br>Daño de partes como fuente de poder, procesador, memoria.<br>Error en el sistema operativo.<br>Error en archivos del sistema.<br>Saturación de rendimiento de recursos:procesador,memoria. | Tiempo de uso de recursos.<br>Falta de mantenimiento preventivo.<br>Fluctuaciones de corriente eléctrica.<br>Sobrecarga de procesos asignados al equipo. | Interrupción de servicios.<br>Pérdida de información.<br>Pérdidas económicas.<br>Deterioro de calidad de servicios de TI. |
| | Externo | Desastres naturales, Desastres industriales. | Pérdida total del servidor por terremoto, incendio, erupción volcánica. | Destrucción total o parcial del datacenter por terremoto.<br>Destrucción total o parcial del datacenter por incendio.<br>Destrucción total o parcial del datacenter por erupción volcánica. | Interrupción de servicios.<br>Pérdida de información.<br>Pérdidas económicas.<br>Deterioro de calidad de servicios de TI.<br>Pérdida de recursos de TI.<br>Afectación importante a los procesos críticos de la Cooperativa. |
| | Humano | Daño no intencional de hardware o software.<br>Acceso malintencionado.<br>Daño intencional de hardware o software. | Error en configuración o actualización del servidor: hardware/software.<br>Empleado o tercero que intencionalmente genera pérdida de información o daño de hardware.<br>Negligencia en la ejecución de actividades que genera interrupción de los servicios. | Contratación de personal sin el perfil adecuado para el área.<br>Negligencia o falta de conocimiento técnico.<br>Incumplimiento de procesos.<br>Sabotage interno.<br>Ataques externos. | Interrupción de servicios.<br>Pérdida de información.<br>Alteración al presupuesto programado de TI.<br>Deterioro de calidad de servicios de TI. |
| | Proceso | Acciones fraudulentas o no autorizadas de empleados.<br>Robo de información.<br>Errores en la generación de respaldos de bases de datos. | | Usuarios muy privilegiados.<br>Inadecuada definición de funciones por cargo.<br>Falta de definición y asignación de roles de usuarios.<br>Falta de controles de seguridad en el acceso a la información.<br>Incumplimiento de procesos. | Fuga de información.<br>Divulgación no autorizada de información.<br>No disponibilidad de respaldos de bases de datos. |

**Figura 28: Matriz de riesgo 1** Elaborado por: Investigador

| LEVANTAMIENTO DEL EVENTO DE RIESGO | | | | | |
|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | DESCRIPCIÓN | CAUSAS | CONSECUENCIAS |
| Redes y comunicaciones | Tecnológico | Daño o desconfiguración de equipos de comunicación.<br>Saturación de la red.<br>Pérdida de paquetes. | Pérdida de canal de datos entre agencias. | Vida útil de los equipos transcurrida.<br>Falta de mantenimiento preventivo.<br>Fluctuaciones de corriente eléctrica.<br>Sobrecarga de procesos asignados al equipo.<br>Cables de red mal elaborados o en mal estado.<br>Error de configuración de los equipos. | Red lenta.<br>Telefonía ip robotizada.<br>Video conferencia inestable.<br>No disponibilidad del core financiero.<br>Interrupción del servicio al cliente.<br>Retraso en el trabajo de los empleados.<br>Insatisfación del cliente.<br>Incumplimiento de responsabilidades con terceros.1 |
| | Externo | Caida del servicio del proveedor. | Pérdida del canal de comunicación de datos entre agencias, del servicio de internet o comunicación con servicios de terceros, debido a: problemas del proveedor, deslaves, erupción volcánica, terremoto, inundaciones, incendio, accidentes. | Rotura de fibra óptica<br>Error en configuración de equipos<br>Daño de equipos de comunicación<br>Saturación del canal<br>Inhibición de equipos.<br>Sabotaje | Interrupción del servicio al cliente<br>Deterioro de calidad de servicios de TI<br>Deterioro de imagen institucional<br>Pérdidas económicas<br>Retraso en el trabajo de los colaboradores<br>Incumplimiento de responsabilidades con terceros. |
| | Humano | Error de configuración de los equipos.<br>Sabotaje | Pérdida del canal de comunicación de datos entre agencias o del servicio de internet.<br>Pérdida del canal de comunicación con servicios de terceros. | Contratación de personal sin el perfil adecuado para el área.<br>Negligencia o falta de conocimiento técnico.<br>Incumplimiento de procesos. | No disponibilidad del core financiero.<br>Interrupción del servicio al cliente.<br>Retraso en el trabajo de los empleados.<br>Insatisfación del cliente.<br>Incumplimiento de responsabilidades con terceros. |
| | Proceso | Contratación inadecuada de servicios | Se contrata un servicio que no cumple con las necesidades del negocio | No se define al alcance y objetivos del proyecto.<br>Desconocimiento de tecnologías de redes y comunicación | Red lenta.<br>Interrupción del servicio.<br>Telefonía ip robotizada.<br>Video conferencia inestable.<br>No disponibilidad del core financiero. |

**Figura 29: Matriz de riesgo 2** Elaborado por: Investigador

| LEVANTAMIENTO DEL EVENTO DE RIESGO | | | | | |
|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | DESCRIPCIÓN | CAUSAS | CONSECUENCIAS |
| Servicios de producción | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento.<br>La funcionalidad del sistema no cumple con las necesidades del negocio.<br>Inadecuada parametrización de software. | Daño de servidor o sus partes.<br>Daño o deterioro de dispositivos de almacenamiento.<br>Error en el sistema operativo.<br>Error en archivos del sistema.<br><br>Errores de parametrización en los sistemas.<br>Saturación de rendimiento de recursos:procesador,memoria.<br>No se dispone de las herramientas tecnológicas necesarias para cumplir con los requerimientos del negocio o de normas reguladoras de entes de control. | Vida útil de los equipos transcurrida<br>Falta de mantenimiento preventivo.<br>Fluctuaciones de corriente eléctrica.<br>Sobrecarga de procesos asignados al equipo.<br>Falta de capacitación a los usuarios.<br>Adquisición de software sin un estudio profundo de cumplimiento de objetivos y factibilidades.<br>Sistemas adquiridos no se ajustan a las necesidades del negocio y requerimientos del usuario.<br>Falta de personal o de presupuesto para administrar herramientas tecnológicas que cumplan con requerimientos del negocio y de leyes vigentes.<br>1.Falta y/o inadecuado mantenimiento de los recursos tecnologicos<br>2.Baja calidad de los recursos tecnologicos<br>3.Inadecuado uso de los recursos tecnologicos | Interrupción de servicios.<br>Pérdida de información.<br>Pérdidas económicas.<br>Deterioro de calidad de servicios de TI.<br>Incumplimiento de normativas.<br>Insatisfacción del usuario y del cliente.<br>Desempeño o resultados de sistemas no esperados. |
| | Externo | Caida del servicio del proveedor. | Denegación de servicio.<br>Terremoto, erupción volcánica, inundaciones,incendios. | Problemas de continuidad del negocio de los proveedores.<br>Daños en equipos. | Interrupción de servicios.<br>Pérdida de información.<br>Pérdidas económicas.<br>Deterioro de calidad de servicios de TI.<br>Incumplimiento de normativas.<br>Insatisfacción del usuario y del cliente.<br>Desempeño o resultados de sistemas no esperados. |
| | Externo | Hackeo, ataques que suspendan los servicios. | Denegación de servicio.<br>Robo de información.<br>Posibilidad de que se acceda, manipule y/o divulgue sin autorización la información privilegiada o de reserva que se origine, suministre o custodie en los sistemas informáticos | Error en la configuración de seguridad de la información. | Interrupción de servicios.<br>Pérdida de información.<br>Pérdidas económicas.<br>Deterioro de calidad de servicios de TI.<br>Incumplimiento de normativas.<br>Insatisfacción del usuario y del cliente.<br>Desempeño o resultados de sistemas no esperados. |
| | Externo | Desastres naturales e industriales. | Terremoto, erupción volcánica, inundaciones,incendios. | Error en la configuración de seguridad de la información.<br>Problemas de continuidad del negocio de los proveedores.<br>Daños en equipos. | Interrupción de servicios.<br>Pérdida de información.<br>Pérdidas económicas.<br>Deterioro de calidad de servicios de TI.<br>Incumplimiento de normativas.<br>Insatisfacción del usuario y del cliente.<br>Desempeño o resultados de sistemas no esperados. |

**Figura 30: Matriz de riesgo 3** Elaborado por: Investigador

| LEVANTAMIENTO DEL EVENTO DE RIESGO | | | | | |
|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | DESCRIPCIÓN | CAUSAS | CONSECUENCIAS |
| Servicios de producción | Humano | Error de configuración de los equipos o sistemas.<br>Error de desarrollo.<br>Error de paso a producción. | Caida del servicio de proveedores. | Negligencia o falta de conocimiento técnico.<br>Incumplimiento de procesos.<br>Falta de personal técnico. | Interrupción de los servicios.<br>Retraso en el trabajo de los empleados.<br>Insatisfación del cliente.<br>Incumplimiento de responsabilidades con terceros.<br>Problemas contractuales. |
| | Proceso | Inadecuada seguridad en los sistemas y canales electrónicos.<br>Vulnerabilidad del sistema de información | Posibilidad que terceros entre de forma indebida o fraudulenta a los sistema de información de la cooperativa, para alterar, hurtar o dañar la información.<br>1. Adquirir un software que no cumpla los requerimientos y las necesidades de la Institución | Ausencia de procedimientos y políticas de seguridad.<br>Deficiente definición de funciones.<br>Bajo nivel de seguridad para el acceso a la información.<br>cortafuegos inadecuados.<br>Bugs en los sistemas informáticos.<br>Desconocimiento en estándares para la implementación de niveles de seguridad en los sistemas informáticos. | Interrupción de servicios.<br>Pérdida de información.<br>Ataques de seguridad. |
| | | Inadecuada adquisicion de software y hardware | Adquirir software o equipos que no cumplan los requerimientos y las necesidades de la Institución | Análisis inadecuado de los requerimientos y/o necesidades del software y hardware<br>Desconocimiento técnicos. | Pérdidas económicas<br>Inestabilidad de los procesos de TI |

**Figura 31: Matriz de riesgo 4 Elaborado por: Investigador**

### 6.7.7 Análisis de impacto en el negocio

| ANALISIS DE RIESGOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | PROBABILIDAD | VALOR P | IMPACTO | VALOR I | P*I | RIESGO INHERENTE |
| Administración de base de datos | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento. | Media | 6 | Crítico | 8 | 48 | Riesgo extremo |
| | Externo | Desastres naturales, Desastres industriales. | Baja | 4 | Moderado | 6 | 24 | Riesgo alto |
| | Humano | Daño no intencional de hardware o software.<br>Acceso malintencionado.<br>Daño intencional de hardware o software. | Alta | 8 | Moderado | 6 | 48 | Riesgo extremo |
| | Proceso | Acciones fraudulentas o no autorizadas de empleados.<br>Robo de información.<br>Errores en la generación de respaldos de bases de datos. | Media | 6 | Crítico | 8 | 48 | Riesgo extremo |
| Redes y comunicaciones | Tecnológico | Daño o desconfiguración de equipos de comunicación.<br>Saturación de la red.<br>Pérdida de paquetes. | Alta | 8 | Crítico | 8 | 64 | Riesgo extremo |
| | Externo | Caida del servicio del proveedor. | Alta | 8 | Crítico | 8 | 64 | Riesgo extremo |
| | Humano | Error de configuración de los equipos.<br>Sabotaje | Alta | 8 | Crítico | 8 | 64 | Riesgo extremo |
| | Proceso | Contratación inadecuada de servicios | Baja | 4 | Moderado | 6 | 24 | Riesgo alto |

**Figura 32: Análisis de riesgos 1** **Elaborado por: Investigador**

| ANALISIS DE RIESGOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | PROBABILIDAD | VALOR P | IMPACTO | VALOR I | P*I | RIESGO INHERENTE |
| Servicios de producción | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento.<br>La funcionalidad del sistema no cumple con las necesidades del negocio.<br>Inadecuada parametrización de software. | Alta | 8 | Crítico | 8 | 64 | Riesgo extremo |
| | Externo | Caida del servicio del proveedor. | Alta | 8 | Moderado | 6 | 48 | Riesgo extremo |
| | Externo | Hackeo, ataques que suspendan los servicios. | Media | 6 | Crítico | 8 | 48 | Riesgo extremo |
| | Externo | Desastres naturales e industriales. | Baja | 4 | Moderado | 6 | 24 | Riesgo alto |
| | Humano | Error de configuración de los equipos o sistemas.<br>Error de desarrollo.<br>Error de paso a producción. | Alta | 8 | Moderado | 6 | 48 | Riesgo extremo |
| | Proceso | Inadecuada seguridad en los sistemas y canales electrónicos.<br>Vulnerabilidad del sistema de información | Alta | 8 | Crítico | 8 | 64 | Riesgo extremo |
| | | Inadecuada adquisicion de software y hardware | MEDIA | 6 | Moderado | 6 | 36 | Riesgo alto |

**Figura 33: Análisis de riesgos 2** **Elaborado por: Investigador**

| EVALUACIÓN DE RIESGOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | CONTROL | DESCRIPCIÓN DEL CONTROL | PERIODICIDAD | OPORTUNIDAD | AUTOMATIZACION | EFICACIA DEL CONTROL |
| Administración de base de datos | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento. | Se revisa y se registra el rendimiento de los recursos del servidor.<br>Se verifica fisicamente las alertas emitidas por los servidores del datacenter principal y alterno.<br>Ejecutar procedimiento de respaldo de base de datos diario en el cierre del sistema.<br>Enviar los respaldos diarios de la base de datos a la bóveda en el Banco.<br>Mantener un servidor de réplica de base de datos en el data center alterno.<br>Replicar al servidor alterno la base de datos cada 5 minutos, mediante archivelogs.<br>Control permanente y emisión de alertas sobre el funcionamiento del sistema de réplica.<br>Pruebas de funcionamiento del servidor de réplica. | | Permanente | Preventivo | Automatizado | 10 |
| | Externo | Desastres naturales, Desastres industriales. | Mantener servidores de respaldo en el datacenter alterno, especialmente de los servicios críticos de TI. | Monitoreo de los servidores del data center alterno.<br>Pruebas de funcionamiento de los servidores. | Permanente | Preventivo | Automatizado | 10 |
| | Humano | Daño no intencional de hardware o software.<br>Acceso malintencionado.<br>Daño intencional de hardware o software. | Control de acceso físico a los recursos de TI.<br>Control de roles y perfiles de usuarios.<br>Procedimiento de mantenimiento de preventivo y correctivo.<br>Difusión de procedimientos de TI. | | Permanente | Preventivo | Automatizado | 10 |
| | Proceso | Acciones fraudulentas o no autorizadas de empleados.<br>Robo de información.<br>Errores en la generación de respaldos de bases de datos. | Logs de auditoria.<br>Definición contractual de prohibición de divulgación de información no autorizada.<br>Verificación de bitácoras de respaldo de base de datos.<br>Procedimiento de respaldo de base de datos.<br>Definición de roles y permisos de acceso a la información. | | Permanente | Correctivo | Automatizado | 10 |

**Figura 34: Evaluación de riesgos 1** **Elaborado por: Investigador**

| EVALUACIÓN DE RIESGOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | CONTROL | DESCRIPCIÓN DEL CONTROL | PERIODICIDAD | OPORTUNIDAD | AUTOMATIZACION | EFICACIA DEL CONTROL |
| Redes y comunicaciones | Tecnológico | Daño o desconfiguración de equipos de comunicación.<br>Saturación de la red.<br>Pérdida de paquetes. | Monitoreo de pérdida de paquetes entre agencias.<br>Monitoreo y control de consumo de ancho de banda frente al ancho de banda contratado.<br>Filtro de uso de recursos de red por perfiles de usuario.<br>Control de actualizaciones de software automáticas. | | Permanente | Correctivo | Automatizado | 10 |
| | Externo | Caida del servicio del proveedor. | Acuerdo de nivel de servicio con proveedor.<br>Monitoreo de pérdida de paquetes entre agencias.<br>Monitoreo y control de consumo de ancho de banda frente al ancho de banda contratado. | | Permanente | Correctivo | Automatizado | 10 |
| | Humano | Error de configuración de los equipos.<br>Sabotaje | Control de acceso físico a los recursos de TI. | | Permanente | Correctivo | Automatizado | 10 |
| | Proceso | Contratación inadecuada de servicios | Estudio del alcance, necesidades y objetivos del proyecto.<br>Asesoramiento y cotización con 3 proveedores de servicios. | | Permanente | Correctivo | Automatizado | 10 |

**Figura 35: Evaluación de riesgos 2** Elaborado por: Investigador

| EVALUACIÓN DE RIESGOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | CONTROL | DESCRIPCIÓN DEL CONTROL | PERIODICIDAD | OPORTUNIDAD | AUTOMATIZACION | EFICACIA DEL CONTROL |
| Servicios de producción | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento.<br>La funcionalidad del sistema no cumple con las necesidades del negocio.<br>Inadecuada parametrización de software. | Control y registro del rendimiento de los recursos del servidor.<br>Revisión de alertas emitidas por los servidores del datacenter principal y alterno.<br>Ejecución de procedimiento de respaldo de datos.<br>Pruebas de funcionamiento del servidor de réplica.<br>Mantener servidores de respaldo en el datacenter alterno.<br>Mantenimiento preventivo de servidores. | | Permanente | Correctivo | Automatizado | 10 |
| | Externo | Caida del servicio del proveedor. | Implementación de controles de seguridad de la información.<br>Control de seguridad perimetral.<br>Acuerdos de nivel de servicio con proveedores.<br>Datacenter alterno. | | Permanente | Correctivo | Automatizado | 10 |
| | Externo | Hackeo, ataques que suspendan los servicios. | Implementación de controles de seguridad de la información.<br>Control de seguridad perimetral.<br>Acuerdos de nivel de servicio con proveedores.<br>Datacenter alterno. | | Permanente | Correctivo | Automatizado | 10 |
| | Externo | Desastres naturales e industriales. | Implementación de controles de seguridad de la información.<br>Control de seguridad perimetral.<br>Acuerdos de nivel de servicio con proveedores.<br>Datacenter alterno. | | Permanente | Correctivo | Automatizado | 10 |
| | Humano | Error de configuración de los equipos o sistemas.<br>Error de desarrollo.<br>Error de paso a producción. | Control de acceso físico a los recursos de TI.<br>Control de roles y perfiles de usuarios.<br>Procedimiento de mantenimiento preventivo y correctivo.<br>Cumplimiento de procedimientos de TI.<br>Acuerdos de nivel de servicio. | | Permanente | Correctivo | Automatizado | 10 |
| | Proceso | Inadecuada seguridad en los sistemas y canales electrónicos.<br>Vulnerabilidad del sistema de información | Definición de procedimientos de seguridad de acuerdo a la normativa vigente.<br>Implementación de seguridad en canales electrónicos. | | Permanente | Correctivo | Automatizado | 10 |
| | | Inadecuada adquisicion de software y hardware | Evalución de experto | Diagnostico sobre ventajas y desventajas del software | Permanente | Correctivo | Automatizado | 10 |

**Figura 36: Evaluación de riesgos 3** Elaborado por: Investigador

| RIESGO RESIDUAL | | | | |
|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | VALOR | NIVEL DE RIESGO |
| Administración de base de datos | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento. | 38 | Riesgo alto |
| | Externo | Desastres naturales, Desastres industriales. | 14 | Riesgo medio |
| | Humano | Daño no intencional de hardware o software.<br>Acceso malintencionado.<br>Daño intencional de hardware o software. | 38 | Riesgo alto |
| | Proceso | Acciones fraudulentas o no autorizadas de empleados.<br>Robo de información.<br>Errores en la generación de respaldos de bases de datos. | 38 | Riesgo alto |
| Redes y comunicaciones | Tecnológico | Daño o desconfiguración de equipos de comunicación.<br>Saturación de la red.<br>Pérdida de paquetes. | 54 | Riesgo extremo |
| | Externo | Caida del servicio del proveedor. | 54 | Riesgo extremo |
| | Humano | Error de configuración de los equipos.<br>Sabotaje | 54 | Riesgo extremo |
| | Proceso | Contratación inadecuada de servicios | 14 | Riesgo medio |

**Figura 37: Riesgo residual 1** Elaborado por: Investigador

| RIESGO RESIDUAL | | | | |
|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | VALOR | NIVEL DE RIESGO |
| Servicios de producción | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento.<br>La funcionalidad del sistema no cumple con las necesidades del negocio.<br>Inadecuada parametrización de software. | 54 | Riesgo extremo |
| | Externo | Caida del servicio del proveedor. | 38 | Riesgo alto |
| | Externo | Hackeo, ataques que suspendan los servicios. | 38 | Riesgo alto |
| | Externo | Desastres naturales e industriales. | 14 | Riesgo medio |
| | Humano | Error de configuración de los equipos o sistemas.<br>Error de desarrollo.<br>Error de paso a producción. | 38 | Riesgo alto |
| | Proceso | Inadecuada seguridad en los sistemas y canales electrónicos.<br>Vulnerabilidad del sistema de información | 54 | Riesgo extremo |
| | | Inadecuada adquisicion de software y hardware | 26 | Riesgo alto |

**Figura 38: Riesgo residual 2** Elaborado por: Investigador

| ACCIONES CORRECTIVAS | | | | | | |
|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | ACCIÓN A EJECUTAR | PMTI - Plazo máximo tolerable de interrupción | RTO - Objetivo de tiempo de recuperación | RPO - Objetivo de punto de recuperación |
| Administración de base de datos | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento. | Mantener stock de repuestos de servidores por modelo de servidor.<br>Realizar mantenimientos preventivos de los servidores, por lo menos una vez al año. | 60 minutos | 30 minutos | 5 minutos |
| | Externo | Desastres naturales, Desastres industriales. | Mantener servidores de respaldo en el data center alterno, especialmente de los servicio críticos de TI. | 24 horas | 18 horas | 8 horas |
| | Humano | Daño no intencional de hardware o software.<br>Acceso malintencionado.<br>Daño intencional de hardware o software. | Respaldos de configuración de servidores.<br>Mantener un stock de repuestos de servidores.<br>Capacitación al personal.<br>Contratación de personal técnico especializado. | 60 minutos | 30 minutos | 5 minutos |
| | Proceso | Acciones fraudulentas o no autorizadas de empleados.<br>Robo de información.<br>Errores en la generación de respaldos de bases de datos. | Adecuada segregación de funciones. | 60 minutos | 30 minutos | 5 minutos |
| Redes y comunicaciones | Tecnológico | Daño o desconfiguración de equipos de comunicación.<br>Saturación de la red.<br>Pérdida de paquetes. | Contratación de canal alterno de comunicación.<br>Mantenimiento preventivo de equipos de redes y comunicación.<br>Configuración y administración de equipos de comunicación.<br>Respaldo de configuración de equipos.<br>Mantener en stock equipos de respaldo configurados.<br>Aplicar QoS o calidad de servicio de la red para dar prioridad al tráfico de datos | 30 minutos | 20 minutos | 5 minutos |
| | Externo | Caida del servicio del proveedor. | Contratación de canal alterno de comunicación.<br>Aplicar QoS o calidad de servicio de la red para dar prioridad al tráfico de datos | 20 minutos | 10 minutos | 5 minutos |

**Figura 39: Acciones correctivas 1** Elaborado por: Investigador

| ACCIONES CORRECTIVAS | | | | | | |
|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | ACCIÓN A EJECUTAR | PMTI - Plazo máximo tolerable de interrupción | RTO - Objetivo de tiempo de recuperación | RPO - Objetivo de punto de recuperación |
| Redes y comunicaciones | Humano | Error de configuración de los equipos.<br>Sabotaje | Capacitación permanente al personal en administración y control de nueva tecnología de redes y comunicación.<br>Adecuada definición y asignación de funciones al personal.<br>Contratación de soporte técnico con especialistas. | 30 minutos | 20 minutos | 5 minutos |
| | Proceso | Contratación inadecuada de servicios | Capacitación permanente al personal en administración y control de nueva tecnología de redes y comunicación.<br>Adecuada definición y asignación de funciones al personal.<br>Contratación de soporte técnico con especialistas. | 30 minutos | 20 minutos | 5 minutos |
| Servicios de producción | Tecnológico | Daño o deterioro de servidores, medios de almacenamiento.<br>La funcionalidad del sistema no cumple con las necesidades del negocio.<br>Inadecuada parametrización de software. | Mantener stock de repuestos de servidores por modelo de servidor.<br>Realizar mantenimientos preventivos de los servidores, por lo menos una vez al año.<br>Guardar respaldos de la configuración de los servidores.<br>Replicar en el datacenter alterno los servidores de los principales servicios de TI.<br>Capacitación permanente al usuario de los diferentes sistemas. | 60 minutos Servidor core financiero<br>5 horas Servidores servicios de canales electrónicos.<br>36 horas servidores otras aplicaciones | 30 minutos Servidor core financiero<br>4 horas Servidores servicios de canales electrónicos.<br>24 horas servidores otras aplicaciones | 5 minutos Servidor core financiero<br>4 horas Servidores servicios de canales electrónicos.<br>24 horas servidores otras aplicaciones |
| | Externo | Caida del servicio del proveedor. | Mantener servidores de respaldo en el data center alterno, especialmente de los servicio críticos de TI.<br>Guardar respaldos de la configuración de los servidores. | 5 horas Servidores servicios de canales electrónicos.<br>36 horas servidores otras | 4 horas Servidores servicios de canales electrónicos.<br>24 horas servidores | 4 horas Servidores servicios de canales electrónicos. |
| | Externo | Hackeo, ataques que suspendan los servicios. | Control permanente de la seguridad de la información.<br>Capacitación en seguridad de la información.<br>Actualización permanente de tecnología y metodología de seguridad de la información. | 5 horas | 4 horas | 5 minutos |

**Figura 40: Acciones correctivas 2** Elaborado por: Investigador

| ACCIONES CORRECTIVAS | | | | | | |
|---|---|---|---|---|---|---|
| PROCESO | FACTOR | RIESGO | ACCIÓN A EJECUTAR | PMTI - Plazo máximo tolerable de interrupción | RTO - Objetivo de tiempo de recuperación | RPO - Objetivo de punto de recuperación |
| Servicios de producción | Externo | Desastres naturales e industriales. | Mantener servidores de respaldo en el data center alterno, especialmente de los servicio críticos de TI. | 24 horas | 18 horas | 8 horas |
| | Humano | Error de configuración de los equipos o sistemas.<br>Error de desarrollo.<br>Error de paso a producción. | Capacitación permanente en administración y control de nueva tecnología.<br>Adecuada definición y asignación de funciones al personal.<br>Contratación de soporte técnico con especialistas.<br>Monitoreo y control de calidad de los servicios de TI. | 60 minutos Servidor core financiero<br>5 horas Servidores servicios de canales electrónicos.<br>36 horas servidores otras aplicaciones | 30 minutos Servidor core financiero<br>4 horas Servidores servicios de canales electrónicos.<br>24 horas servidores otras aplicaciones | 5 minutos Servidor core financiero<br>4 horas Servidores servicios de canales electrónicos.<br>24 horas servidores otras aplicaciones |
| | Proceso | Inadecuada seguridad en los sistemas y canales electrónicos.<br>Vulnerabilidad del sistema de información | Monitoreo y control de sucesos de seguridad.<br>Contratación de servicios especializados de control antiphishing, suplantación de identidad,etc. | 24 horas | 18 horas | 8 horas |
| | | Inadecuada adquisicion de software y hardware | Considerar la participación de las personas expertas.Elaborar un procedimiento de adquisición de software, para garantizar que cumpla conlos requerimientos del negocio, del usuario y de normativas vigentes.<br>Plan de adquisiciones de TI y asignación de presupuesto de acuerdo a necesidades del negocio, actualización tecnologica, nuevos productos y servicios y normativas vigentes. | | | |

**Figura 41: Acciones correctivas 3** **Elaborado por: Investigador**

### 6.7.8 Estrategia

El plan de contingencia de los procesos críticos se ha estructurado con el detalle de las actividades a desarrollarse antes, durante y después de que ocurra un evento de riesgo en cualquiera de los procesos críticos. Para esto se utilizan como escenarios los posibles eventos de riesgo, frente a los cuales se describen los procedimientos que deben ser ejecutados por los usuarios de los procesos.

Los puntos clave descritos en esta estrategia son: contactos, responsables de tomar decisiones, responsables de ejecución de tareas de contingencia y recuperación, procedimientos para recuperación, evaluación de daños, reinicio de sistemas y de regreso a operaciones normales.

Los escenarios de eventos de riesgos para los cuales se han delineado procedimientos son:

- Pérdida parcial del sistema
- Pérdida total de sistema
- Suspensión temporal del servicio de redes y telecomunicaciones

**Escenario: Pérdida parcial del sistema**

| | |
|---|---|
| **Escenario** | **Pérdida parcial del sistema**<br>Corresponde cuando el Core Financiero de la Cooperativa se encuentra fuera de servicio y su tiempo de reanudación es menor a dos horas. |
| **Subprocesos Críticos:** | • Atención al cliente en ventanillas: depósitos, retiros, pago de préstamos.<br>• Atención al cliente en canales electrónicos |
| **Estrategia:** | Brindar continuidad en la atención en ventanillas, en lo concerniente a servicios propios que brinda la Cooperativa, y suspender las transacciones con entidades externas como: Facilito, Puntomático y remesadoras. |
| **Contactos:** | Softwarehouse: franklin.ortega@finantech.com.ec, 0984265990<br>Data center alterno: ftoalombo@ccca.fin.ec |
| **Procedimiento:** | **Activación de data center alterno** |
| **Instancias:** | **Acciones a implementarse** |

| | |
|---|---|
| **Antes** | **Asistente de TI** Revisar diariamente la conectividad con servidores de data center alterno y registrar en la bitácora.<br>**Asistente de TI**Publicar diariamente en la unidad compartida "Información pública/Contingencia", el archivo en Excel con los saldos de ahorros, préstamos y plazo fijo.<br>**Jefe de TI** Revisar diariamente la répllica de base de datos del core financiero y registrar en la bitácora.<br>**Jefe de TI** Actualizar la configuración de los servidores del datacenter alterno con los respaldos de los servidores principales, cuando exista algún cambio y registrar en la bitácora.<br>**Director de Tesoreria y Director de TI**Mantener actualizado el inventario de equipos de cómputo asegurados y equipos con garantía.<br>**Oficial de riegos**Capacitar al personal de la Cooperativa en el uso del plan de contingencia y continuidad del negocio. |
| **Durante** | **Director de TI** Comunica a Gerencia General la no disponibilidad de la base de datos del core financiero en el data center principal.<br>**Gerente General** autoriza la activación del servidor de base de datos en el sitio alterno.<br>**Director de TI** Establece la metodología a aplicar SWITCHOVERycomunica al personal responsable.<br>**Jefe de TI**, Realiza el cambio al data center alterno según la metodología aprobada.<br>**SWITCHOVER**.- No hay pérdida de información.<br>Paso 1 Detener los servicios del servidor principal de base de datos.<br>Paso 2 Aplicar los archives pendientes y sincronizar las bases.<br>Paso3Iniciar el proceso de cambio de roles del servidor principal al servidor alterno (tiempo estimado 15 minutos)<br>Paso4 Cambiar la configuración de los servidores de aplicación (core financiero, canales electrónicos), apuntando al servidor de base de datos alterno.<br>Paso 5 Auditor Interno, Oficial de Seguridad y Oficial de Riesgos<br>Realizan pruebas de diagnóstico (ingreso al sistema, consulta de saldos.)<br>Paso 6 Difundir por whatsapp la nueva instancia del aplicativo al personal de la Cooperativa: (SERVIDOR_ALTERNO/CORE_FINANCIERO)<br><br>**Supervisores y/o Jefes de Agencia.-** Revisar los últimos movimientos registrados de todos los procesos.<br>Disponer al personal a su cargo el ingreso de los movimientos pendientes.<br>Disponer al personal a su cargo la atención al público con el sistema.<br>Cuadre de transacciones. |

| | |
|---|---|
| **Después** | **Supervisores y/o Jefes de Agencia.-** Emitir informe con los incidentes suscitados durante la contingencia a Auditoría Interna y Oficial de riesgos.<br><br>**Oficial de Seguridad, Jefe Financiero y Auditoría Interna**.- Deben emitir en el transcurso de 24 horas el informe de diagnóstico e impacto de la operatividad del sitio alterno con sus respectivas conclusiones y recomendaciones<br>**Gerente General**.- tomar las acciones correctivas en base al informe de diagnóstico.<br>**Director de TI**.- Evaluar los daños de los recursos de TI y planificar la restauración de actividades en el servidor de base de datos principal.<br>**Director de Tesorería**.- Tramitar garantías y seguros de equipos. |

## Escenario: Pérdida Total del Sistema

| | |
|---|---|
| **Escenario** | **Pérdida Total del Sistema**<br>Se considera pérdida total del Core Financiero cuando se estima un tiempo de reanudación mayor a dos horas. |
| **Subprocesos Críticos:** | • Atención al cliente en ventanillas: depósitos, retiros, pago de préstamos.<br>• Atención al cliente en canales electrónicos |
| **Estrategia:** | Brindar continuidad en la atención de ventanillas, en lo concerniente a servicios propios que brinda la Cooperativa, y suspender las transacciones con entidades externas como: Facilito, Puntomático y remesadoras. |
| **Contactos:** | Softwarehouse: franklin.ortega@finantech.com.ec, 0984265990<br>Data center alterno: ftoalombo@ccca.fin.ec |
| **Procedimiento:** | **Activación de data center alterno** |
| **Instancias:** | **Acciones a implementarse** |
| **Antes** | **Asistente de TI** Revisar diariamente la conectividad con servidores de data center alterno y registrar en la bitácora.<br>**Asistente de TI**Publicar diariamente en la unidad compartida "Información pública/Contingencia", el archivo en Excel con los saldos de ahorros, préstamos y plazo fijo.<br>**Jefe de TI** Revisar diariamente la répllica de base de datos del core financiero y registrar en la bitácora.<br>**Jefe de TI**Actualizar la configuración de los servidores del datacenter alterno con los respaldos de los servidores principales, cuando exista algún cambio y registrar en la bitácora.<br>**Director de Tesoreria y Director de TI**Mantener actualizado el inventario de equipos de cómputo asegurados y equipos con garantía.<br>**Oficial de riegos**Capacitar al personal de la Cooperativa en el uso del plan de contingencia y continuidad del negocio. |

| | |
|---|---|
| **Durante** | **Director de TI** Comunica a Gerencia General la no disponibilidad de los principales servicios en el data center principal.<br>**Gerente General** autoriza la activación del sitio alterno.<br>**Director de TI** Establece la metodología a aplicar (FAILOVERoSWITCHOVER)ycomunica al personal responsable.<br>**Jefe de TI**, Realiza el cambio al data center alterno según la metodología aprobada:<br>**FAILOVER**.- Posible pérdida de información.<br>Paso 1 En el servidor de base de datos alterno suspender el modo archive y activar modo escritura.<br>Paso 2 Aplicar archives pendientes.<br>Paso 3 Levantar servicios del core financiero en el servidor alterno.<br>Paso 4 Auditor Interno, Oficial de Seguridad y Oficial de Riesgos<br>Realizan pruebas de diagnóstico (ingreso al sistema, consulta de saldos)<br>Paso 5 Difundir por whatsappla nueva instancia del aplicativo al personal de la Cooperativa: (SERVIDOR_ALTERNO/CORE_FINANCIERO)<br>**SWITCHOVER**.- No hay pérdida de información.<br>Paso 1 Detener los servicios en el datacenter principal.<br>Paso 2 Aplicar los archives pendientes y sincronizar las bases.<br>Paso3Iniciar el proceso de cambio de roles del servidor principal al servidor alterno (tiempo estimado 15 minutos)<br>Paso3 Levantar servicios del core financiero en el sitio alterno.<br>Paso 5 Auditor Interno, Oficial de Seguridad y Oficial de Riesgos<br>Realizan pruebas de diagnóstico (ingreso al sistema, consulta de saldos.)<br>Paso 6 Difundir por whatsapp la nueva instancia del aplicativo al personal de la Cooperativa: (SERVIDOR_ALTERNO/CORE_FINANCIERO)<br><br>**Supervisores y/o Jefes de Agencia.-** Revisar los últimos movimientos registrados de todos los procesos.<br>Disponer al personal a su cargo el ingreso de los movimientos pendientes.<br>Disponer al personal a su cargo la atención al público con el sistema.<br>Cuadre de transacciones. |
| **Después** | **Supervisores y/o Jefes de Agencia.-**Emitir informe con los incidentes suscitados durante la contingencia a Auditoría Interna y Oficial de riesgos.<br><br>**Oficial de Seguridad, Jefe Financiero y Auditoría Interna**.- Deben emitir en el transcurso de 24 horas el informe de diagnóstico e impacto de la operatividad del sitio alterno con sus respectivas conclusiones y recomendaciones<br>**Gerente General**.- tomar las acciones correctivas en base al informe de diagnóstico.<br>**Director de TI**.- Evaluar los daños de los recursos de TI y planificar la restauración de actividades en el data center principal.<br>**Director de Tesorería**.- Tramitar garantías y seguros de equipos. |

## Escenario: Suspensión temporal del servicio de redes y telecomunicaciones

| | |
|---|---|
| **Escenario** | **Suspensión temporal del servicio de redes y telecomunicaciones**<br>Suspensión temporal de la red de comunicación de datos que afectalos servicios de tecnología que realizan intercambio de datos. |
| **Subprocesos Críticos:** | • Atención al cliente en ventanillas: depósitos, retiros, pago de préstamos.<br>• Atención al cliente en canales electrónicos |
| **Estrategia:** | En caso de suspensión del servicio del proveedor principal de comunicación de datos TELCONET, debe subir automáticamente el proveedor alterno Telefónica. |
| **Contactos:** | **Telconet:** soporte@telconet.ec>, (593)-2-3963100 ext. 8000<br>**Telefónica:** soporte.datos@telefonica.com,(593) 2 2227700 |
| **Procedimiento:** | **Activación de sistema de comunicación de datos alterno** |
| **Instancias:** | **Acciones a implementarse** |
| **Antes** | **Asistente de TI**Publicar diariamente en la unidad compartida "Información pública/Contingencia", el archivo en Excel con los saldos de ahorros, préstamos y plazo fijo.<br>**Jefe de TI**Realizar un control diario de disponibilidad de los enlaces de comunicación entre agencias y con externos(BCE, canales electrónicos), evaluar el consumo de ancho de banda, registrar en la bitácora.<br>Realizar pruebas programadas de subida automática del canal alterno de comunicación, con los proveedores.<br>**Director de TI** Planificar mantenimiento periódico de equipos de red y comunicación propios de la Cooperativa y gestionar el mantenimiento de equipos de proveedores.<br>Mantener acuerdos de nivel de servicio actualizados con los proveedores.<br>Mantener stock de respaldo de equipos de redes y comunicaciones, debidamente configurados.<br>**Oficial de riegos**Capacitar al personal de la Cooperativa en el uso del plan de contingencia y continuidad del negocio.<br>**Director de Tesoreria y Director de TI**Mantener actualizado el inventario de equipos de cómputo asegurados y equipos con garantía. |

| | |
|---|---|
| **Durante** | **Usuarios del sistema** Comunican a Jefe de TI la no disponibilidad de la red de comunicación de datos y trabajan con el archivo de contingencia publicado en "Información pública/Contingencia", mientras se restaura el servicio.<br>**Jefe de TI**Realiza pruebas de conectividad para determinar la causa y el alcance del incidente. Puede ser problema de red LAN o WAN.<br>**Red LAN**<br>**Asistente de TI**De acuerdo al incidente detectado aplica las correcciones necesarias: Cambio de cable de red, verificación de punto de red en el switch, configuración de adaptador de red, verificación de permisos de acceso en directorio activo, etc.<br>**Red WAN con agencias de la Cooperativa**<br>**Jefe de TI** En las agencias que mantienen un canal alterno de comunicación se verifica con los proveedores la situación por la cual no se subió automáticamente el canal alterno, y lo sube manualmente.<br>Si es falla de un equipo de red, se procede con el cambio inmediato, usando los equipos de respaldo.<br>En las agencias que no mantienen canal alterno de comunicación se verifica inmediatamente con el proveedor la causa y se obtiene un tiempo de respuesta, que no puede ser mayor al establecido en el acuerdo de nivel de servicio.<br>**Red WAN con proveedores de servicios o instituciones de convenios(BCE, canales electrónicos)**<br>**Jefe de TI** Si se mantiene un canal alterno de comunicación se verifica con los proveedores la situación por la cual no se subió automáticamente el canal alterno, y lo sube manualmente.<br>Si es falla de un equipo de red, se procede con el cambio inmediato, usando los equipos de respaldo.<br>En las agencias que no mantienen canal alterno de comunicación se verifica inmediatamente con el proveedor la causa y se obtiene un tiempo de respuesta, que no puede ser mayor al establecido en el acuerdo de nivel de servicio.<br>Se comunica por correo electrónico al proveedor de servicios o institución de convenio del incidente y se trabaja por FTP o correo electrónico para la transmisión de archivos. |
| **Después** | **Supervisores y/o Jefes de Agencia.-**Emitir informe con los incidentes suscitados durante la contingencia a Auditoría Interna y Oficial de riesgos.<br><br>**Oficial de Seguridad, Jefe Financiero y Auditoría Interna**.- Deben emitir en el transcurso de 24 horas el informe de diagnóstico e impacto de la operatividad del sitio alterno con sus respectivas conclusiones y recomendaciones<br>**Gerente General**.- tomar las acciones correctivas en base al informe de diagnóstico.<br>**Director de TI**.- Evaluar los daños de los recursos de TI y controlar la restauración del canal principal de comunicación.<br>**Director de Tesorería**.- Tramitar garantías y seguros de equipos. |

**Bibliografía**

(Díaz, 2004) Díaz, G., Mur, F., and Sancristóbal, E., (2004). *Seguridad en las comunicaciones y en la información*. Madrid, España: UNED - Universidad Nacional de Educación a Distancia. ProQuestebrary. Web. 5 August 2017.

(Cruz & Guevara, 2018) Cruz, D., Guevara, D., (2018). *Plan de riesgos y contingencias informáticas basado en un acuerdo de nivel de servicio aplicada a la Empresa Plasticaucho Industrial.* Ambato, Ecuador. Recuperado de: http://repositorio.uta.edu.ec/jspui/handle/123456789/28103

(Cabezas, 2016) Cabezas, V., (2016). *Estudio cualitativo del impacto de aplicación de buenas prácticas para la administración de proyectos de software en 11 organizaciones del sector público*. Quito, Ecuador: Pontificia Universidad Católica del Ecuador.

(SEPS, 2017) SEPS, (2017). *Planes de contingencia y continuidad del negocio, oficio circular N° SEPS-IRDNSES-2016-06791*. Quito, Ecuador. Recuperado de: http://www.seps.gob.ec/tramites?manuales-para-la-gestion-de-envio-de-informacion

(Fernández &Velthuis, 2012)Fernández, C. M., Velthuis M. P.,(2012).*Modelo para el gobierno de las TIC basado en las normas ISO.* Madrid, España: AENOR.

(Martínez, 2004)Martínez, J. G., (2004).*Planes de contingencia: la continuidad del negocio en las organizaciones*. Madrid, España: Ediciones Díaz de Santos. ProQuestebrary. Web. 19 August 2017.

(Superintendencia de Bancos, 2015) Superintendencia de Bancos, (2015). *Normas generales para las instituciones del sistema financiero, Titulo X, CapítuloV, Sección IV.- Continuidad del negocio*. Quito, Ecuador

(Villavicencio,2016) Villavicencio, A., *Diagnóstico seguridad de la información*. Quito, Ecuador: ICORED.

(García & Mariblanca, 2015) García, P., Mariblanca, A.M., (2015). *Planes de Continuidad.* Recuperado de: https://www.aenor.com/Certificacion_Documentos/Folletos/articulo-ISO22301-REVISTAAENOR.pdf

(ISOtools, 2015) *¿Qué se entiende por riesgo operativo en una organización?*. *Recuperado* de: https://www.isotools.org/2015/11/16/que-se-entiendepor-riesgo-operativo-en-una-organizacion/

(Comité de Supervisión Bancaria de Basilea, 2003) Comité de Supervisión Bancaria de Basilea, (2003). *S Buenas prácticas para la gestión y supervisión del riesgo operativo*. Basilea, Suiza: Secretaría del Comité de Supervisión Bancaria de Basilea.