UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

IMPLEMENTACIÓN DE UN MANUAL DE CONTINUIDAD DE NEGOCIO APLICABLE A INSTITUCIONES FINANCIERAS DEL SEGMENTO 3 REGULADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Gestión de riesgos tecnológicos

LÍNEA DE INVESTIGACIÓN: Normas y estándares

AUTOR: Henry Ricardo Ortega Castro

TUTOR: Ing. Julio Balarezo

Ambato - Ecuador

marzo – 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: IMPLEMENTACIÓN DE UN MANUAL DE CONTINUIDAD DE NEGOCIO APLICABLE A INSTITUCIONES FINANCIERAS DEL SEGMENTO 3 REGULADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, desarrollado bajo la modalidad de proyecto de titulación, por el señor Henry Ricardo Ortega Castro, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, marzo 2023.

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Balarezo

TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: IMPLEMENTACIÓN DE UN MANUAL DE CONTINUIDAD DE NEGOCIO APLICABLE A INSTITUCIONES FINANCIERAS DEL SEGMENTO 3 REGULADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2023.

Henry Ricardo Ortega Castro

C.C. 180449387-0

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2023.

Henry Ricardo Ortega Castro

C.C. 180449387-0

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Henry Ricardo Ortega Castro estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado IMPLEMENTACIÓN DE UN MANUAL DE CONTINUIDAD DE NEGOCIO APLICABLE A INSTITUCIONES FINANCIERAS DEL SEGMENTO 3 REGULADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, marzo 2023.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
EDWIN HERNANDO BUENANO VALENCIA

Ing. Hernando Buenaño
PROFESOR CALIFICADOR

Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

Ing. Dennis Chicaiza
PROFESOR CALIFICADOR

DEDICATORIA

Dedicar este trabajo primero a mis padres por su apoyo incondicional en mi formación, a mi hermana por su esfuerzo y acompañamiento a lo largo de mi trayectoria estudiantil que me permiten seguir adelante y perseverar.

Ambato, marzo 2023.

AGRADECIMIENTO

Agradecer a todas las personas que de una u otra manera contribuyeron en la elaboración de esta investigación, de manera especial a mi Tutor, por su sapiencia y tolerancia. Gracias.

Ambato, marzo 2023.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

TEMA DE INVESTIGACIÓN:

"IMPLEMENTACIÓN DE UN MANUAL DE CONTINUIDAD DE NEGOCIO APLICABLE A INSTITUCIONES FINANCIERAS DEL SEGMENTO 3 REGULADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA"

AUTOR: Henry Ricardo Ortega Castro
TUTOR: Ing. Julio Balarezo Mg.

El objetivo de la investigación es implementar un manual de continuidad de negocio aplicable a instituciones financieras del segmento 3 reguladas por la Superintendencia de Economía Popular y Solidaria, con la finalidad de dar a conocer estrategias a las personas que están al frente de los departamentos informáticos y tecnológicos de las instituciones financieras para de esta manera reducir los tiempos de recuperación de los servicios cuando exista suspensiones cortas o prolongadas que puedan afectar el normal funcionamiento. Dentro de la metodología que se consideró esta la investigación bibliográfica y de campo, así como la exploratoria y la descriptiva que permitió al investigador tener un juicio de las variables y tomar la decisión acertada para plantear la respectiva propuesta. Los resultados obtenidos dan conocer que la mayoría de los empleados desconocen de sistemas y procesos para enfrentar la caída del sistema informático, no existe una inducción sobre estos procedimientos al personal que entra a laborar en la institución. En relación con las conclusiones se refiere a los procedimientos de recuperación ante la interrupción de la operación en servidores y redes de comunicaciones principales donde se elaboran mediante los registros que hayan recolectado en eventos críticos pasados, permitiendo la corrección e implementación de nuevos aspectos que refuercen las estrategias seleccionadas para cada departamento de la institución financiera. El manual de continuidad de negocio permitirá que el personal a cargo de los departamentos maneje de forma adecuada el impacto que la caída de servidores provoque en la institución financiera.

Palabras Claves: Manual de continuidad, servidores informáticos, evento crítico, impacto, instituciones financieras.

ABSTRACT

The objective of the research is to implement a business continuity manual applicable to segment 3 financial institutions regulated by the Superintendency of Popular and Solidarity Economy, in order to make known strategies to the people who are in charge of the IT departments of financial institutions to reduce the recovery times of services when there are short or long suspensions that may affect normal operation. The methodology that was considered is the bibliographic and field research, as well as the exploratory and descriptive one that allowed the researcher to have a judgment of the variables and take the right decision to raise the respective proposal. The results obtained reveal that the majority of the employees are unaware of systems and processes to face the fall of the computer system, there is no induction on these procedures to the personnel who enter to work in the institution. In relation to the conclusions, it refers to the recovery procedures in the event of the interruption of the operation in servers and main communications networks where they are prepared by means of the records that have been collected in past critical events, allowing the correction and implementation of new aspects that reinforce the strategies selected for each department of the financial institution. The business continuity manual will allow the personnel in charge of the departments to adequately manage the impact that the server crash causes on the financial institution.

Keywords: Continuity manual, computer servers, critical event, impact, financial institutions.

CAPÍTULO I

MARCO TEÓRICO

1.1 Tema de Investigación

"IMPLEMENTACIÓN DE UN MANUAL DE CONTINUIDAD DE NEGOCIO APLICABLE A INSTITUCIONES FINANCIERAS DEL SEGMENTO 3 REGULADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA"

1.2 Antecedentes Investigativos

En la actualidad las instituciones financieras son susceptibles a sufrir eventos que afectan a las organizaciones, por lo que contar con una manual de continuidad de negocio permite de una manera eficaz un plan para que puedan recuperarse rápidamente antes que otras organizaciones. A continuación se analizará ciertos conceptos de autores a nivel mundial, regional y nacional para tener un criterio fundamentado del tema que trataremos.

Según la norma internacional ISO 27002 y 22301 manifiesta: "La gestión de continuidad de negocio es un proceso que debe ser aplicado para reducir el impacto y la recuperación por la pérdida de los recursos de la información en la organización combinando los planes que la empresa tenga para prevenir y recuperar recursos humanos y financieros mediante estrategias de repuestas ante riesgos" [1]. La pretensión de la normativa es que las organizaciones tomen en cuenta todos los elementos que los manuales de continuidad poseen para tomar ventaja de otras organizaciones al momento de recuperarse, esto de una forma adecuada y sólida.

Según Martínez en su guía "El plan de Continuidad de Negocios" indica: "Contar con un manual de negocios aumenta las posibilidades de continuar las funciones financieras de las organizaciones cuando ocurra un incidente que interrumpa las operaciones informáticas, de igual forma identifica y proporciona enfoques que permitan realizar actividades de respuesta y recuperación cuando las funciones en el trabajo se vean interrumpidas, generando menos situaciones de caos y tensión" [2].

Desde el punto de vista del autor la gestión de los manuales es de suma importancia para que toda la organización se mantenga estructura y no cause un desorden en cuanto a los procesos informáticos, sugiriendo enfoques direccionados en los debidos puntos que están causando incidentes.

Según la Escuela Superior de Administración Pública de Colombia señala: "El Plan de Continuidad de Negocios (BCP) explora niveles que permitan sostener los procesos críticos del negocio mediante una estructuración definida de los procedimientos e información, los cuales son preparados, desarrollados y aplicados durante y después de un evento que cause interrupción. El plan pretende respaldar los intereses de quienes conforman la organización, a su vez mantener los indicadores de generación de valor como confianza y reputación" [3]. La institución colombiana menciona que además de aplicar un plan de continuidad de negocios, es de suma importancia considerar los niveles de confianza que se genere una vez más en los clientes de las organizaciones.

La Secretaría de Gestión de Riesgos (SGR) reveló: "Las organizaciones necesitan ejecutar planes de continuidad con el fin de garantizar el bienestar de la infraestructura tecnológica y recuperar la operatividad del negocio. Ecuador es un país que presenta alto riesgo ante desastres naturales, por lo que es fundamental la implementación de manuales de continuidad de negocio. A nivel comercial, 88 organizaciones presentaron grandes daños en el terremoto del 16 de abril del 2016" [4]. Lo que pretende la SGR es aportar beneficios relacionados a la evaluación de riesgos dentro del sistema de gestión de la continuidad del negocio, proporcionando a las organizaciones una orientación para su desarrollo, medición y evaluación.

1.2.1 Contextualización del Problema

The Risk Management Soviet (RIMS), analizó la situación de riesgo en Latinoamérica arrojando un 31% de las organizaciones que involucran procesos de riesgo se encuentran en Argentina, Brasil, Chile y Ecuador. Además indica que el 76% de las organizaciones en Latinoamérica creen que la gestión de riesgos da un valor extra a su negocio, mientras que un 54% denotó que dicha gestión esta poco implementada y desarrollada dentro de la empresa.

En el Ecuador el Banco del Pacifico cuenta con un comité específico para la Continuidad del Negocio el cual ha generado un programa de administración de la Continuidad del Negocio donde establecen que: Dentro de su evaluación de riesgos y amenazas, Banco del Pacífico considera aquellas de origen natural, incluidas las relacionadas con el cambio climático, que podrían causar eventos disruptivos que afecten la continuidad de sus operaciones. Estas son gestionadas mediante tratamiento de riesgos, definición de estrategias y elaboración de un plan de continuidad del negocio, el cual permite preparase, responder y recuperar los procedimientos críticos que soportan los principales productos, servicios y canales de la Institución [5].

En las instituciones financieras con menos activos controladas por la SEPS (Superintendencia de Economía Popular y Solidaria) no ha tenido como prioridad esta normativa, en el año 2016 se emitió una circular para poner en alerta la necesidad del cumplimiento de esta: ante el terremoto del sábado 16 de abril de 2016, el Gobierno Nacional declaró la emergencia en las provincias de la costa y emitió el decreto de Estado de Excepción. Las entidades del sector financiero popular y solidario tienen un rol fundamental en la reactivación de la economía de la zona afectada por el terremoto, por lo cual es necesario aunar esfuerzos para que las actividades financieras puedan retomarse y dinamizar los procesos productivos [6].

1.2.2 Fundamentación Teórica

1.2.2.1 Manual de Continuidad de Negocio

Las instituciones financieras deben contar con estrategias para la prevención, protección y reacción ante incidentes con factores de afectación a la seguridad en sus negocios. Es necesario cuidar estos procesos de negocio generando un grupo de tareas que permitan a las instituciones una pronta recuperación después de un evento grave sin comprometer la continuidad de los procesos. Con esto se puede garantizar acciones planificadas cuando la seguridad se vea vulnerable. Estas acciones afectaran positivamente la reputación e imagen de la organización al reducir el impacto financiero y la perdida de información durante estos eventos.

En muchas ocasiones no existe control de los riesgos ya que la organización puede ser afectada de forma substancial, no importa el tamaño ni origen de las entidades, ninguna

está absuelta de sufrir amenazas. Es importante gestionar de una manera adecuada para evaluar si se van a desarrollar consecuencias mayores o menores. El manual de continuidad de negocio no debe relacionarse con el plan de prevención de perdidas, por lo que en este último es necesario registrar actividades a través de sistemas, seguridad y control para identificar la información que se perderá. La continuidad de negocio no es solo de grandes organizaciones, esto va cambiando respecto a las medidas aplicadas para garantizar la continuidad operativa en desastres. Una gran organización cuenta con un centro de respaldo y comunicaciones, sistemas de servidores, mientras que otras pequeñas organizaciones lo óptimo es realizar copias de seguridad en la nube considerando costo rendimiento [7]. Dentro del contexto de Manual de Continuidad de Negocio se distingue tres tipos dependiendo el alcance que tengan:

1.2.2.2 Tipos de manuales de continuidad

1.2.2.2.1. Manual de Continuidad de Negocio (MCN)

Es aquel que abarca la continuidad de una organización desde múltiples aspectos como infraestructura TIC, infraestructura física, sistemas de comunicación, recursos humanos, inmobiliario, etc. Cada área mencionada posee su propio manual de continuidad referenciado desde el MCN principal. Por ejemplo si existe riesgo de inundación en la zona de servidores, se activa el determinado plan para la situación y los otros que no son necesarios permanecen inactivos. Un manual de continuidad de negocio que consta de todos los posibles eventos es considerado uno multidisciplinario en el cual no solo abarca las áreas mencionadas sino también las ubicaciones físicas para el personal. Se considera que estos manuales poseen grandes multinacionales debido a sus niveles de infraestructura [8].

1.2.2.2.2. Manual de Continuidad TIC (MTIC)

Es una estrategia direccionada a los sistemas informáticos ya que se limita al ámbito tecnológico con fases como los recursos de respaldo, organización de emergencia y procedimientos de actuación con el fin de restaurar los sistemas de información que contienen los datos y negocios de una organización. Por ejemplo si existe un incidente que ponga en riesgo la organización, se activa los manuales de continuidad de negocio de la empresa que tengan que ver con los aspectos tecnológicos. Aunque el alcance de

un MCN es por lo general superior al de un MCTIC, ya que hay otros procesos y activos no tecnológicos implicados, las fases de su elaboración son básicamente las mismas [8].

1.2.2.2.3. Manual de Recuperación ante Desastres (MRD)

El ámbito que abarca es más técnico ya que su análisis es menos profundo, de modo que es un manual reactivo ante un posible evento catastrófico. Existen diferentes maneras de abordar el desarrollo de un plan de recuperación, pero éste siempre debe estar alineado con el plan de continuidad, por lo que debe considerar los elementos que definen la razón de ser de una organización. Además, el MRD debe incluir los criterios para determinar cuándo un incidente de seguridad no se puede resolver mediante los procedimientos comunes de atención y se considera como un desastre, es decir, cuando se presenta un evento catastrófico y repentino que nulifica la capacidad de las organizaciones para llevar a cabo los procesos esenciales [8].

1.2.2.3 Fases de un Manual de Continuidad de Negocio

Las estrategias que se implementan en los manuales nos ayudan para:

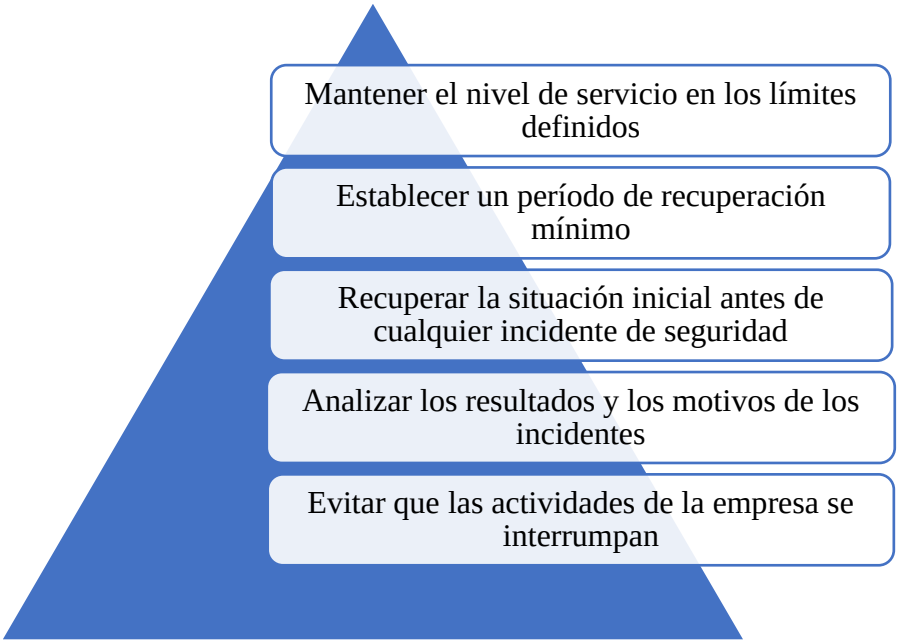

Figura 1. Objetivos del MCN
Fuente: INCIBE, 2019

Partiendo de estos fundamentos, se analiza los factores que garantizan la continuidad del negocio mediante las siguientes fases:

1.2.2.3.1. Fase 1: Determinación del Alcance

Se le identifica como fase cero ya que tiene una corta duración y los recursos que se utilizan son mínimos. Se determina los elementos de la organización que van a ser el foco de su continuidad, el alcance son aquellos procesos críticos que causan un gran impacto sobre la organización. En el alcance mencionado se debe tomar en cuenta además de los recursos tecnológicos y personales informáticos, también se requerirá la colaboración de las demás dependencias de la institución. El enfoque del alcance se aprecia desde el punto de vista del activo (aplicación de la contabilidad) o del proceso (mejorar el proceso contable independientemente de los activos informáticos) [9].

De esta manera el alcance que se pretende para el trabajo es un enfoque por proceso, seleccionar un punto crítico y elaborar un manual para mejorar su continuidad.

1.2.2.3.2. Fase 2: Análisis de la Organización

Permite la obtención, elaboración y compresión de los procedimientos, eventos, tecnologías y recursos que ocurren en la organización para conocer cuáles son claves, de apoyo y a su vez asignar los recursos necesarios para estos. Se requiere una evaluación del impacto del negocio y de los riesgos.

Figura 2. Factores de Análisis
Fuente: A. Cárdenas. Fases del MCN, 2013.

Mantener Reuniones

Se toma en cuenta el personal seleccionado en la revisión del alcance para recolectar información de proveedores, usuarios implicados y las aplicaciones que se necesitan. Se procede a obtener la información de las aplicaciones del proceso anterior para determinar su proveedor y funcionamiento. Se opta por realizar una entrevista al personal a cargo o simplemente revisando los datos que se tenga para saber si poseen copias de seguridad y cada qué período recibe soporte considerando el tiempo de respuesta del proveedor.

a. Análisis de Impacto sobre el Negocio

Es uno de los principales análisis del plan de continuidad TIC que contiene las necesidades de los procesos definidos como alcance. En esta parte contiene los requisitos temporales y de recursos de los procesos dentro de su alcance y, con el Análisis de Riegos permite definir las iniciativas que se implantaran para la recuperación de procesos en situación de contingencia. Permite determina el impacto en caso de interrupción de los procesos y seleccionar la estrategia adecuada que se va a aplicar. En pocas palabras el análisis respondería cuanto perdería la organización si un proceso se ve interrumpido. Las actividades que posee el análisis son las siguientes [7]:

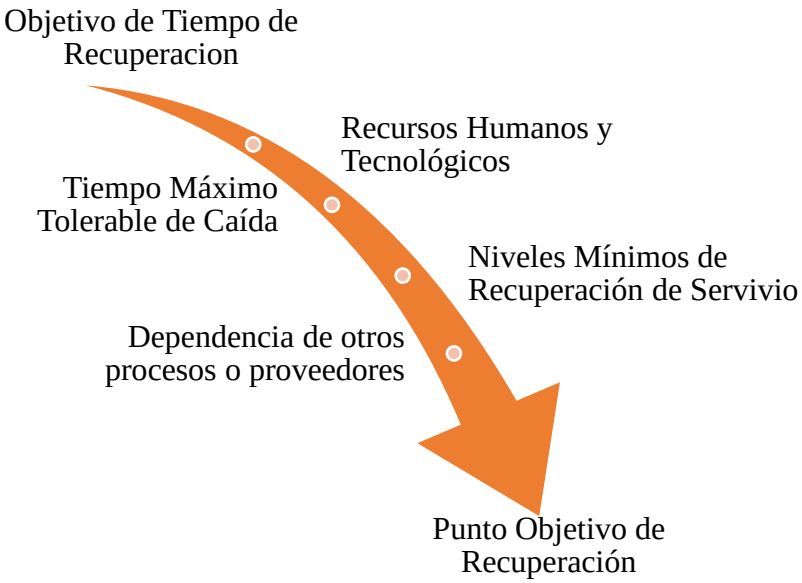

Figura 3. Procesos de la organización

Fuente: D. Mora. PCN como base del éxito organizacional, 2018.

Objetivo de Tiempo de Recuperación (RTO)

Es el tiempo que el proceso estará suspendido antes que vuelva a entrar en funcionamiento. Pueden existir procesos en los que el tiempo de recuperación es muy pequeño (horas), por ejemplo, el servicio de banca electrónica de un banco, y otros procesos como la facturación a clientes en una empresa de servicios, pueden tener un periodo de recuperación mayor (días o semanas).

Recursos Humanos y Tecnológicos

Consiste en determinar las aplicaciones, sistemas y equipamientos que cada proceso necesite para los eventos de contingencia, de igual forma como los tiempos de recuperación de cada uno. En la parte tecnológica, se debe considerar la infraestructura tecnológica, mientras que en los recursos humanos se debe identificar el personal critico sin reemplazo.

Tiempo Máximo Tolerable de Caída (MTD)

Es el tiempo que permanece interrumpido la actividad antes que se produzcan grandes pérdidas en la organización. Se debe tomar en cuenta que la valoración de este factor es subjetiva ya que se puede medir cualitativamente el impacto durante la contingencia, identificar en qué momento la contingencia pone en riesgo definitivamente la continuidad de la organización. El MTD se encuentra relacionado con el negocio, mientras que el RTO es determinado porAunque el alcance de 5 un MCN el personal técnico, De todas formas, el RTO debe ser inferior al MTD, caso contrario el daño de la empresa será irreversible.

Niveles Mínimos de Recuperación de Servicio (ROL)

Es el nivel mínimo de recuperación que se espera de alguna actividad sin considerar la calidad de servicio que se ofrezca durante este infortunio. Se considera el público objetivo que es destinatario de la actividad de servicio, se considera que el proceso ha sido recuperado cuando alcanza un 70% con las expectativas de completarlo al 100%.

Dependencias de otros Procesos Internos o Proveedores Externos

El proceso mencionado dependerá de la disponibilidad de un plan de recuperación de desastres por parte del proveedor y los tiempos que maneje al aplicarlo. Se comprueba que las contingencias de los proveedores no afecten a la organización.

Punto Objetivo de Recuperación (RPO)

Hace referencia al impacto sobre la pérdida de datos, siendo fundamental al momento de establecer las políticas de copias de seguridad sin tener relación con el RTO. Debemos tomar en cuenta: cuanto mayor sean las exigencias de conservación de los datos, los recursos a utilizar son directamente proporcionales, debido que esta información es proporcionada por cada departamento que se encuentre en el alcance, se recomienda realizar un ejercicio de evaluación adicional con el fin de identificar exigencias demasiado elevadas para no aceptar requisitos que no posean una valoración previa.

b. Análisis de Riesgo

En esta sección se revisará las amenazas que al materializarse afectarán los procesos del alcance, analizando las probabilidades, el impacto y los activos que recaen sobre los procesos de negocios críticos. Se resalta tres pasos para realizar un análisis de riesgo de la manera adecuada [10]:

Determinar Amenazas	• Robo de información, afectación eléctrica , caída de servidores, etc. • Que implican indisponibilidad de los procesos de alcance.
Probabilidad e Impacto	• Usar escalas cualitativas como de uno a cinco; o muy baja o muy alta. • Identificar riesgos que pongan en peligro la información o la continuidad de la organización.
Producto de la Probabilidad por el Impacto de Amenza	• Seleccionar riesgos con mayor prioridad. • Recolectar lista de riesgos de la organización.

Figura 4. Pasos Análisis de Riesgos
Fuente: H. Ortega, 2021.

Estos pasos nos ayudan a encontrar el grupo de amenazas que la organización está expuesta, además de los pasos mencionados existen otros métodos que obtiene resultados más fiables ya que consideran el valor de los activos y sus vulnerabilidades. Se espera que los rangos de impacto sean temporales con el fin de no relacionar el MTD/RTO con los tiempos del impacto de las amenazas.

1.2.2.3.3. Fase 3: Determinación de la Estrategia de Continuidad

En esta fase se determinan estrategias para la recuperación de elementos identificados como críticos o los que se ven afectados en una contingencia. Se identifica el sistema a recuperar para evitar que el evento de riesgo lo dañe de una manera irreversible para la organización. Para diferenciar las necesidades del proceso de negocio y las capacidades de los recursos que utilizan, se indica la siguiente información:

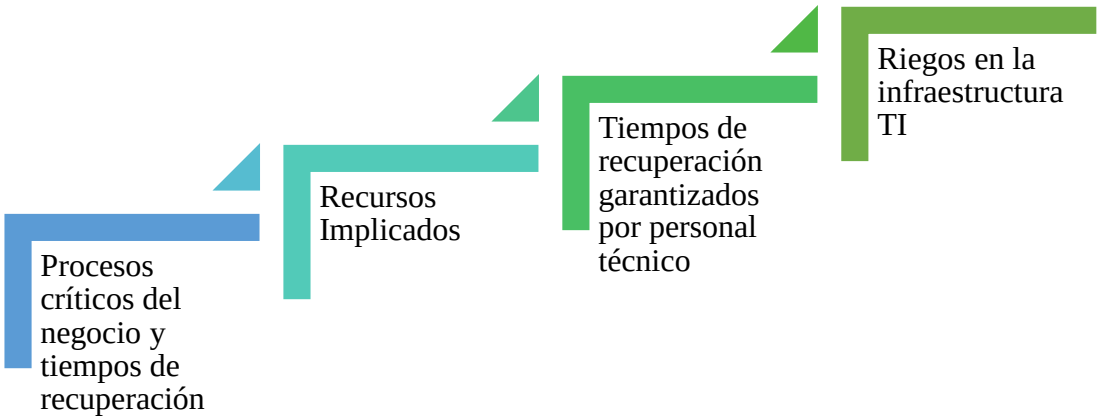

Figura 5. Información para Estrategia de Continuidad
Fuente: H. Ortega, 2021.

Los elementos que se ven afectados en las contingencias son:

- ✓ Personal. - Identificar el personal crítico para revisar las diferentes opciones y contrarrestar su ausencia.
- ✓ Locales. - Analizar situaciones que no dispongan sitios para trabajar.
- ✓ Tecnología. – Evaluar las tecnologías que formen parte en los activos para valorar posibles alternativas de funcionamiento adicional.
- ✓ Información. – Cuidar la información que relacione los procesos críticos.
- ✓ Proveedores. – Asegurarse que los tiempos de respuesta de los proveedores sean acordes a los de la empresa y que sus contingencias no afecten a la organización.

Las estrategias de la organización se deben aplicar en una fase posterior evaluando el valor del coste, mantenimiento, recursos necesarios, etc., con el fin de elaborar iniciativas a tener en cuenta para mejorar la continuidad del proceso.

1.2.2.3.4. Fase 4: Respuesta a la Contingencia

En esta fase se efectúa la estrategia y las iniciativas consideradas en la fase anterior donde se ordenará las medidas en función de prioridad y criticidad. La documentación que responde a las contingencias relacionadas con la parte tecnológica se trabajará mediante un árbol de jerarquía, ordenando el momento crítico después de la crisis en la parte superior, las bases para la recuperación de la infraestructura en la parte media y en los ítems inferiores se emplean los procedimientos técnicos necesarios para la recuperación de la organización. Dentro de la respuesta a la contingencia se considera ciertos elementos que se detallarán a continuación [11].

a. Plan de Crisis

El objetivo de este plan es evitar que se tomen decisiones improvisadas que causen más daños a la crisis o en lo posible no tomar las peores decisiones. Se considera que todo comienza analizando la situación límite en la que se declara una situación de crisis, revisando los MTDs de los procesos críticos. De esta forma se tomará las decisiones respectivas para cada proceso y se contará con los medios para anunciar la situación de crisis. El personal responsable tiene la obligación de activar el Plan de Crisis y gestionarlo de una manera óptima para la organización. Se tomará contacto con el personal implicado en la gestión de la crisis lo que permitirá generar los datos que se necesiten. A su vez, se requiere que los niveles de priorización estén establecidos en la recuperación de la infraestructura de la organización.

b. Plan Operativo de Recuperación de Entornos

Se necesita evaluar el alcance de la crisis para identificar que Planes Operativos de Recuperación se activan dependiendo los entornos que contienen información de estos o de forma independiente. Con lo mencionado cada infraestructura empezará el proceso de recuperación iniciando del último elemento que ejecutará la estrategia de continuidad: los procedimientos técnicos de trabajo.

c. Procedimientos Técnicos de Trabajo

Se refiere a la documentación que respalda las acciones que se han desarrollado con las tareas indispensables para la recuperación de una aplicación, sistema o infraestructura determinado. En si no forma parte de la continuidad de negocio pues se considera un procedimiento diario en la organización, pero en situación de crisis toma un papel fundamental. La documentación contiene información valiosa para la organización como direcciones IP, comandos, tablas, versiones de programas y copias de bases de datos.

1.2.2.3.5. Fase 5: Prueba, Mantenimiento y Revisión

El manual de continuidad TIC controla de la mejor manera la crisis que presente la organización reduciendo los tiempos de recuperación, por lo que necesita estar actualizado constantemente y comprobar su vigencia. Se requiere efectuar pruebas sobre el alcance y entorno estimado anualmente para las amenazas que se han calificado como catastróficas. Dentro de la planificación de las pruebas que se van a realizar se considera:

- Personal técnico
- Usuario implicado
- Clientes y proveedores
- Descripción de la prueba
- Descripción del resultado
- Horario de la prueba

Luego de aplicar la prueba se necesita un informe que indique los resultados descritos de los incidentes encontrados durante el proceso. Adicionalmente se menciona los resultados no esperados, tiempos estimados, mala comunicación e indisponibilidad de proveedores. A continuación se revisará las posibles pruebas que se puedan ejecutar dentro de la organización. El objetivo del plan es mantener actualizado la documentación cuando se realice cambios en el personal, infraestructuras TIC o algún

proceso que se considere crítico. Esto da confianza en que la documentación que se utilice en alguna situación de contingencia, es totalmente segura y real [12].

Figura 6. Pruebas para aplicarse
Fuente: H. Ortega, 2021.

1.2.2.3.6. Fase 6: Concienciación

La última fase de la implementación del Manual de Continuidad de Negocio TIC consiste en concientizar al personal implicado en todos los procesos de la organización incluyendo el personal TI de la empresa. Se debe planificar un proceso completo de concienciación exponiendo elementos como análisis de impacto, plan de crisis y estrategias a aplicar. Con independencia del sector o del tamaño, cualquier organización debe estar preparada para afrontar con garantías un incidente de seguridad que pueda afectar al desarrollo de sus actividades. Establecer una serie de medidas dirigidas a minimizar el impacto que pueda tener cualquier tipo de contingencia sobre el negocio proporcionará mayor seguridad y capacidad de respuesta ante cualquier eventualidad.

1.2.2.4. Instituciones Financieras

El sistema financiero se considera uno de los factores fundamentales de la economía en cada país, difundiendo el ahorro y la inversión para poder generar riqueza por lo que los entes económicos han delegado a diversas instituciones financieras para conseguir capital de trabajo, infraestructura y expansión productiva. Se establece que el sistema financiero es el conjunto de bancos, sociedades financieras, mutualistas y cooperativas que trabajan en la intermediación financiera con el público. Las empresas financieras, de inversión y desarrollo se identifican como principales intermediarios en el mercado financiero que se encargan de captar recursos públicos para recolectar fondos mediante depósitos con la finalidad de utilizar los recursos obtenidos para gestionar créditos e inversiones [13].

Según el diccionario de José Heras manifiesta que "Las instituciones financieras sirven para contactar a las personas que quieren ahorrar con quienes necesitan créditos". Se plantea la idea que las instituciones financieras no son solo un medio para atender la emergencia, sino que además contribuyan a generar nuevas estructuras socioeconómicas, en esta definición, se puede valorar la idea de que las finanzas para otra economía deben buscar el fomento de organizaciones que forman parte de la Economía Social y Solidaria (formas Asociativas, cooperativistas de diferente naturaleza) [14].

Según el Banco de México indica que "Las instituciones financieras son aquellas entidades de crédito que ofertan y demandan dinero al público partiendo de la captación de depósitos y la concesión de créditos como actores del sistema se tiene a bancos, cooperativas, sociedades, gestoras de fondos" [15]. Dichas instituciones se caracterizan por ser los principales intermediarios en el mercado financiero. De esta manera se puede decir que el sistema financiero es un ente que permite captar unidades excedentarias de liquidez y por otra parte unidades económicas deficitarias de liquidez para canalizar el ahorro hacia la inversión.

Se define a una institución financiera como una empresa con fin de lucro que tiene como propósito la prestación de servicios financieros a los agentes económicos de la sociedad. Debido al pasar de los años y el avance que han tenido los grupos financieros es difícil delimitar sus actividades, iniciando desde los servicios clásicos de la banca

como depositario y préstamo hasta productos actuales como la banca de inversión o el factoring. Las entidades financieras se mantienen reinventando sus servicios a sus clientes relacionados con dinero, aunque de igual forma han surgido otras empresas que desarrollan estas tareas como las empresas Fintech (tecnología financiera) [16].

1.2.2.4.1 Tipos de Instituciones Financieras

Las instituciones financieras se encuentran normadas o reguladas por un conjunto de principios y normas jurídicas que se fundamentan en instrumentos y documentaciones especiales que permiten direccionar el ahorro y la inversión de los diferentes sectores hacia las necesidades que se presenten para apoyar y desarrollar la economía. En la actualidad las instituciones financieras del país se clasifican en dos tipos:

a. Instituciones Bancarias

Es la entidad que se capta fondos del público en forma de dinero o de distintos tipos de recursos financieros. Su fin es captar fondos de agentes con excedentes de capital para prestarlo a agentes con déficit. De igual forma, se presta garantías y avales, dinero electrónico y transferencias bancarias.

b. Instituciones No Bancarias

Se diferencia de las anteriores debido a que la captación no proviene de depósitos públicos, pero en si son habilitados a realizar las mismas actividades ya conocidas.

1.2.2.4.2. Instituciones Financieras en Ecuador

Todas las instituciones financieras están controladas por entes reguladores de todas las actividades que brinden al público. Los órganos rectores nacionales que rigen los procederes son Banco Central del Ecuador, el cual tiene como función constitucional establecer, controlar y aplicar la política crediticia del Estado, de igual forma concede, aprueba y evalúa la ejecución de los presupuestos de las instituciones financieras públicas. La Superintendencia de Bancos,como entidad autónoma, se encarga de controlar y supervisar las funciones de las instituciones financieras. Dentro de estos entes reguladores, la Junta Bancaria se encuentra controlada por la Superintendencia de Bancos y es responsable de establecer leyes, resoluciones y regulaciones que permiten el funcionamiento de los sistemas fundamentales en la economía [17].

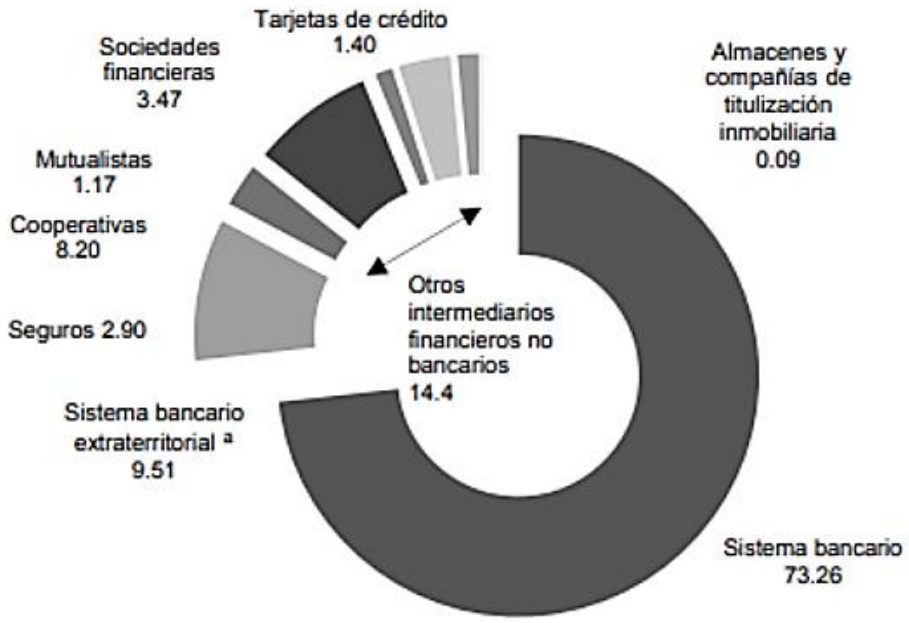

Figura 7. Estructura Sistema Financiero Ecuatoriano
Fuente: Superintendencia de Bancos, 2018.

La Constitución del Ecuador manifiesta en el Art.275 que "el régimen de desarrollo es el conjunto organizado, sostenible y dinámico de los sistemas económicos, político, socioculturales y ambientales, que garantiza la realización del buen vivir (sumakkawsay)", mientras que el Art. 283 señala que "el sistema económico se considera social y solidario ya que permite reconocer al ser humano como sujeto y fin, además propone una relación dinámica y equilibrada entre sociedad, estado y mercado. Estos tienen por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir para que el sistema económico se integre con las formas de organización económica pública, privada, mixta popular y solidaria, y las de más que la constitución determine" [18]. La economía popular y solidaria se regulará de acuerdo con la ley e incluirá a los sectores cooperativistas, asociativos y comunitarios.

Con lo indicado en los artículos anteriores, se analiza el Art.311 donde determina que "el sector financiero popular y solidario se compondrá de Cooperativas de Ahorro y Crédito, Entidades Asociativas o Solidarias, Cajas y 22 Bancos Comunales, Cajas de Ahorros las que recibirán un tratamiento diferenciado y preferencial del estado, en la medida de que impulsen el desarrollo de la economía popular y solidaria" [19]. Dentro de la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular

y Solidario expresa en el art.88 que" las inversiones las cooperativas de ahorro y crédito, preferentemente deberán invertir en el sector financiero popular y solidario. De manera complementaria podrán invertir en el sistema financiero nacional y en el mercado secundario de valores y de manera excepcional, en el sistema financiero internacional, en este caso, previa la autorización y límites que determine el ente regulador" [19].

1.2.2.4.3. Economía Popular y Solidaria en Ecuador

La estabilidad laboral se ha visto apoyada por los diferentes sectores del país mediante la aplicación de medidas económicas para cumplir con el buen vivir solidario y justo. El conjunto de las leyes, normativas, instituciones y sectores comunitarios encargados de dar el apoyo necesario, permiten desarrollar la gobernanza en los sectores de producción [20]. Según el Ministerio de Inclusión Economía y Social sugiere que la propuesta de la Economía Popular y Solidaria desempeña un rol fundamental en el Buen Vivir o Sumak Kawsay como plan o proyecto para que las personas puedan superar las desigualdades que el país presenta [21].

En el Ecuador, la Economía Popular y Solidaria, refiere a los sectores comunitarios como las organizaciones con relación de territorio, cuidado de la naturaleza, familiares, comunidades, pueblos y nacionalidades, tanto urbanas como rurales, que tienen como objetivo la producción, comercialización, distribución y consumo de bienes lícitos y necesarios. Los sectores asociativos, constituidos por personas naturales, las cuales se abastecen de materias primas, insumos, herramientas, tecnologías, equipos u otros bienes y a su vez comercializan su producción. El sector cooperativo, integrado por cooperativas, las cuales se han unido de manera voluntaria para así satisfacer sus necesidades y las unidades económicas populares integradas por las familias, domésticos comerciantes minoristas, talleres artesanales, con actividades económicas de producción y comercialización [20].

El Plan Nacional del Buen Vivir, en su objetivo 8 establece: "Consolidar el sistema económico social y solidario de forma sostenible" plantea las relaciones de poder, la redistribución de riquezas y al ser humano sobre el crecimiento económico y el capital, como la nueva concepción de inclusión económica y transformación del modo de producción, con regulaciones y estabilidad en las condiciones laborales (Secretaría Nacional de Planificación y Desarrollo. Durante los últimos seis años el incremento

de las organizaciones, en el sector financiero y sector no financiero, se registró entre 6.016 a 9.139, teniendo un incremento del 52%, lo que significó un gran avance y desafío de la EPS en el Ecuador. El Buen Vivir es el desarrollo alternativo, como una oportunidad para construir otra sociedad sustentada en la convivencia del ser humano y principios fundamentales de la humanidad. El premio Nobel de Economía 2001 y ex vicepresidente del Banco Mundial Joseph Siglitz, propuso la definición de una nueva política de intervención del Estado con impulso al desarrollo económico con la participación de las pequeñas y medianas empresas [22].

La economía social y solidaria se identifica por la centralidad del trabajador como factor de la producción con respeto al capital y el papel que asumen los trabajadores asociados. En las organizaciones de la EPS se identifica al socio/ asociado y cliente de una organización; el ser cliente permite acceder a los servicios que ofrece cualquier organización; el ser socio/ asociado es tener acceso a los bienes y servicios que genera la organización, además de ejercer actividades y eventos planificados, asesoría y la facultad para ser parte de la dirigencia. El control externo conlleva a la consolidación y correcto funcionamiento de las organizaciones en concordancia con los principios de cooperación, democracia y reciprocidad.

1.2.2.4.4. Superintendencia de Economía Popular y Solidaria (SEPS)

Es el ente regulador que supervisa a las organizaciones no gubernamentales (ONG), cooperativas, bancos comunales, etc., que proveen servicios financieros en la economía solidaria, con personalidad jurídica de derecho público y autonomía administrativa y financiera buscando la estabilidad, desarrollo, solidez y el correcto funcionamiento del sector económico popular y solidario. El objetivo de la entidad es fiscalizar, formalizar y regular a los nuevos organismos que no están siendo regulados. La Ley Orgánica de la Economía Popular y Solidaria (LOEPS) concede atribuciones a la Superintendencia como otorgar personalidad jurídica a las organizaciones del sistema financiero popular y solidario, fijar tarifarios de servicios y autorizar actividades financieras para que levanten estadísticas, impongan sanciones y consignen normas [23].

Es así como la Ley protege la economía popular y solidaria a las cooperativas, asociaciones, comunidades y a las unidades económicas populares, todas aquellas que tengan como finalidad social y solidarias al no buscar acumulación y priorizando al

trabajo antes que al dinero [24]. De esta forma se establece las funciones de la SEPS, las cuales son:

a. Supervisar con las más amplias facultades y sin restricción alguna, a las organizaciones económicas de los sectores asociativos y cooperativistas, para lo cual podrá inspeccionar, vigilar, controlar, auditar, aplicar sanciones, intervenir y liquidar a dichas organizaciones, en caso de que, sus acciones violen la normativa aplicable.
b. Velar por la preservación de la naturaleza jurídica y doctrinaria de las organizaciones sujetas a su supervisión y la vigencia de sus características, así como el correcto uso de los beneficios otorgados por el Estado.
c. Cumplir y hacer cumplir las normas regulatorias del sector y las resoluciones del Consejo Nacional.
d. Efectuar, de oficio o por denuncia de legítimo interesado, inspecciones a las organizaciones sometidas a supervisión, examinar sus archivos, su contabilidad y ordenar que se tomen las medidas tendientes a subsanar las irregularidades que pudieran existir.
e. Imponer sanciones administrativas o pecuniarias a los socios, directivos o administradores, determinando sus responsabilidades mediante resolución motivada.
f. Determinar, mediante resolución debidamente motivada y luego del debido proceso, responsabilidades civiles o indicios de responsabilidad penal, en contra de socios, dirigentes, administradores, interventores o liquidadores de las organizaciones sujetas a su control.
g. Emitir informe previo sobre la conveniencia y legalidad de la constitución de nuevas cooperativas y de apertura de sucursales, agencias u oficinas.

1.3 Objetivos

1.3.1 Objetivo General

Implementar un manual de continuidad de negocio aplicable a instituciones financieras del segmento 3 reguladas por la superintendencia de economía popular y solidaria.

1.3.2 Objetivos Específicos

- Analizar las posibles interrupciones de operación en los principales servidores y redes de comunicación.
- Definir los procedimientos de recuperación ante la interrupción de la operación en servidores y redes de comunicaciones principales
- Asegurar la continuidad de negocio mediante la priorización de la viabilidad del servicio y restablecimiento de operaciones informáticas.

CAPÍTULO II

METODOLOGÍA

2.1. Materiales

2.1.1. Humanos

- Investigador
- Docente tutor de la investigación de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos.
- Personal Administrativo de la Cooperativa de Ahorro y Crédito "Crecer Wiñari" Ltda.

2.1.2. Institucionales

- Cooperativa de Ahorro y Crédito "Crecer Wiñari" Ltda.
- Bibliotecas y repositorios virtuales de la Universidad Técnica de Ambato.
- Accedo a internet que brinda la Universidad Técnica de Ambato.

2.1.3. Recursos

Tabla 1. Recursos Económicos

Recurso	**Costo (usd.)**
Impresiones	50.00
Copias	10.00
Servicio Eléctrico	75.00
Internet	150.00
Materiales de Oficina	30.00
Laptop	800.00
Transporte	200.00
Total:	**1315.00**

Elaborado por: H. Ortega, 2021.

2.2. Métodos

2.2.1. Modalidad de la Investigación

Investigación Bibliográfica

La presente investigación se considera bibliográfica por la necesidad de respaldar los conceptos señalados en el Capítulo I mediante textos impresos, libros, artículos científicos, tesis de grado y posgrado, revistas tecnológicas, documentos de internet, reglamentos y leyes que se indagaron para elaborar la fundamentación teórica sobre la continuidad de negocio en las instituciones financieras.

Investigación de Campo

La investigación se considera de campo ya que se pretende recolectar información sobre las estrategias de continuidad de negocio ante la ocurrencia de eventos críticos, mediante la colaboración del personal involucrado de la Cooperativa de Ahorro y Crédito "Crecer Wiñari" Ltda. con el fin de tener documentación que respalde los datos dados por los involucrados.

Investigación Descriptiva

Se considera que la investigación es descriptiva por los datos que se obtienen del problema que permitirán definir y analizar las causas y consecuencias que se generan para identificar los riesgos que se den en las contingencias que la empresa presente.

Investigación Exploratoria

La investigación presenta aspectos de nivel exploratorio ya que se realizará un análisis sobre el problema planteado al inicio con el fin de encontrar soluciones o posibles acciones que se implementen en la seguridad de los sistemas informáticos con los procedimientos adecuados.

2.2.2. Población y Muestra

La presente investigación se direcciona a las instituciones financieras del segmento 3 reguladas por la superintendencia de economía popular y solidaria. De acuerdo con la Norma para la Segmentación de las Entidades del Sector Financiero Popular y

Solidario, en el artículo 1 establece que las entidades del sector financiero popular y solidario con respecto a el saldo de sus activos se ubicarán en los siguientes segmentos:

Tabla 2. Activos de Entidades Financieras

Segmento	Activos (USD)
1	Mayor a 80´000.000,00
2	Mayor a 20´000.000,00 y hasta 80´000.000,00
3	Mayor a 5´000.000,00 y hasta 20´000.000,00
4	Mayor a 1´000.000,00 y hasta 5´000.000,00
5	Hasta 1´000.000,00
	Cajas de ahorro, bancos y cajas comunales

Fuente: SEPS, 2015.
Elaborado por: H. Ortega, 2021.

Con los datos proporcionados se trabajará con una población de un grupo de empleados encargados de garantizar la continuidad del negocio de una cooperativa de ahorro y crédito en el segmento 3, la Cooperativa de Ahorro y Crédito "Crecer Wiñari" Ltda., que está regularizada y sujeta a cumplir con el mismo nivel de obligaciones y regulaciones establecidas por los entes de control para todas las cooperativas del mismo segmento.

Tabla 3. Población de estudio

Población	Cantidad	Porcentaje
Jefes de Agencia	3	7%
Jefe de Sistemas	1	2%
Jefe de Inversiones	1	2%
Jefe de Cajas	1	2%
Área Contable	2	5%
Área de Riesgos	1	2%
Área de Cumplimiento	1	2%
Asesores de Crédito	9	21%
Asistentes de Crédito	4	9%
Atención al Cliente	5	12%
Recaudadores	7	16%
Cajeros	8	19%
Total	43	100%

Fuente: C.A.C. "Crecer Wiñari" Ltda.
Elaborado por: H. Ortega, 2021.

2.2.3. Recolección de Información

El instrumento que se utilizará para recolectar información es el cuestionario con preguntas de selección múltiple, con el fin de procesar e identificar los resultados obtenidos y posteriormente tabular las preguntas con su respectiva interpretación.

2.2.4. Procesamiento y Análisis de Datos

Tabla 4. Plan de recolección de datos

PREGUNTAS BÁSICAS	**EXPLICACIÓN**
¿Para qué?	Para tener procedimientos en un manual de continuidad de negocio que permita dar a conocer a los diferentes departamentos o áreas de las instituciones financieras.
¿A quiénes?	Al personal administrativo de cooperativas de ahorro y crédito del segmento 3.
¿Sobre qué aspectos?	Procedimientos de un manual de continuidad de negocio ante un evento crítico que comprometa las actividades de la cooperativa.
¿Quien?	Henry Ricardo Ortega Castro
¿Cuándo?	Recopilación bibliográfica del 10 de junio al 20 de julio. Aplicación de encuestas del 27 de julio al 10 de agosto. Procesamiento y análisis de información desde agosto a septiembre.
¿Donde?	Cooperativa de Ahorro y Crédito “Crecer Wiñari” Ltda.
¿Técnicas de recolección?	Se utilizará instrumentos para entrevista y encuesta para poder tabular la información recolectada y poder elaborar un manual de continuidad de negocio que respalde los resultados obtenidos en la investigación.

Elaborado por: H. Ortega, 2021.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

El desarrollo de la presente investigación se fundamenta en la situación que se encuentra el departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito “Crecer Wiñari” Ltda., con respecto al manual de continuidad de negocio que respalden la información y la reactivación de procesos y servicios.

El procesamiento y análisis de la información se la realizó con la colaboración del personal administrativo de la cooperativa mediante una encuesta a cada persona que labora en los distintos departamentos de la institución financiera. El propósito es identificar los conocimientos y procedimientos que se realizan ante un evento crítico que comprometa las actividades y servicios en la Cooperativa de Ahorro y Crédito “Crecer Wiñari” Ltda.

Una vez recolectada la información se analizará los datos de cada interrogante de la encuesta para procesar y obtener antecedentes reales que permitan elaborar un manual de continuidad de negocio aplicable a la cooperativa. Se considerará las preguntas que den resultados negativos para considerarlas con cierta preferencia en las gestiones institucionales.

3.1.1. Encuesta dirigida al personal de la Cooperativa de Ahorro y Crédito "Crecer Wiñari" Ltda.

Pregunta 1. ¿Está de acuerdo con las estrategias vigentes de recuperación de los servicios frente a una caída de los sistemas de información y comunicación en la institución financiera?

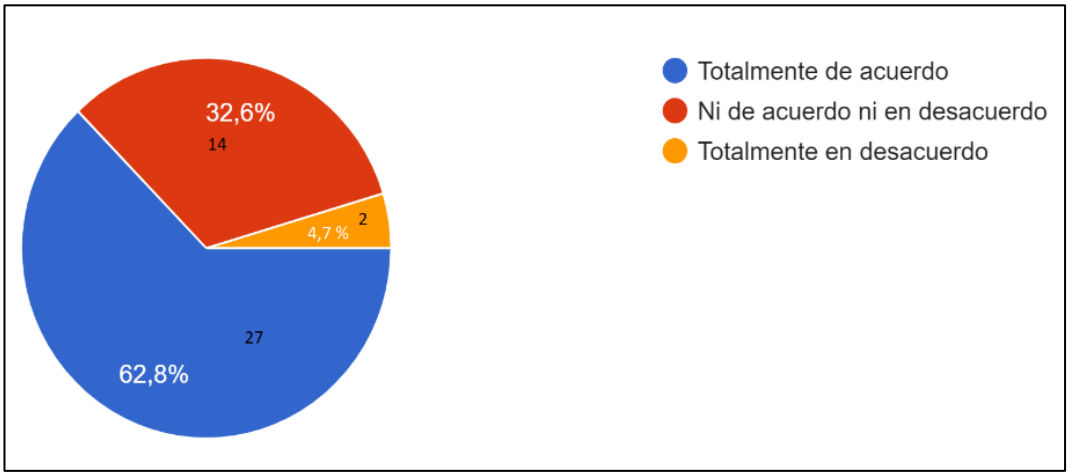

Figura 8. Estrategias de recuperación
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

Del total de los encuestados, el 62,8% indicó que está totalmente de acuerdo con las estrategias vigentes de recuperación de los servicios, el 32,6% señaló que está ni de acuerdo ni en desacuerdo y apenas el 4,7% manifestó que está totalmente en desacuerdo.

La mayoría del personal de la cooperativa no está conforme con las estrategias de recuperación frente a las caídas de los sistemas informáticos que se aplican actualmente en la institución, lo que denota una actualización inmediata de los procedimientos a seguir ante los eventos que se presenten.

Pregunta 2. ¿La cooperativa posee un instructivo vigente que haga referencia a los procedimientos a seguir frente eventos críticos de Coordinación de Tecnología e Innovación de la Cooperativa?

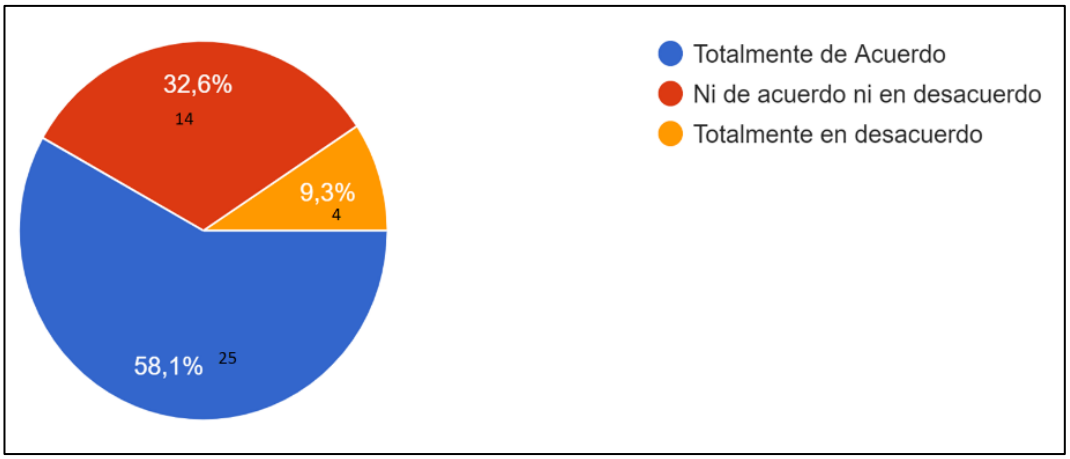

Figura 9. Instructivo de procedimientos
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

El 58,1% del personal encuestado reveló que está totalmente en acuerdo que la cooperativa posee un instructivo vigente de procedimientos ante eventos críticos, el 32,6% señaló que está ni de acuerdo ni en desacuerdo y el 9,3% de los encuestado tachó que está totalmente en desacuerdo.

Con los datos recolectados se evidencia que la mitad del personal cooperativo está totalmente de acuerdo que debe existir un instructivo vigente de procedimientos ante eventos críticos tecnológicos y de innovación, ya que al tener dichas estrategias actualizas se podrá dar un mejor servicio a los clientes que utilizan los servicios financieros de la institución.

Pregunta 3. ¿Las políticas para la gestión de continuidad de negocios son relevantes en la cooperativa?

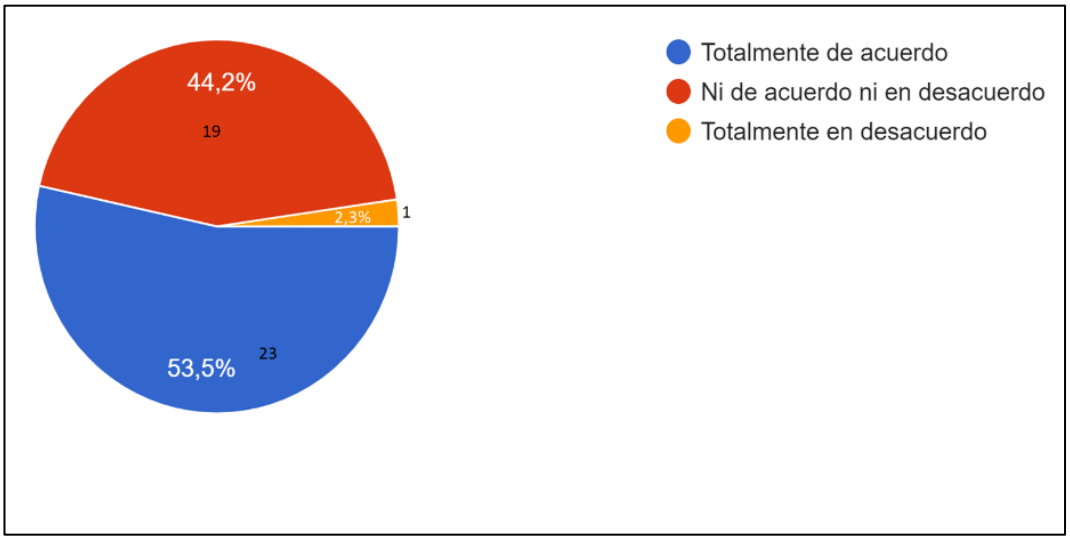

Figura 10. Políticas de Gestión
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

El 53,5% de los encuestados respondieron que están totalmente de acuerdo en que las políticas para la gestión de continuidad de negocios son relevantes, el 44,2% indicó que está ni de acuerdo ni en desacuerdo y el 2,3% añadió que se encuentra totalmente en desacuerdo.

Los trabajadores de la cooperativa afirman que las políticas para la gestión de continuidad de negocios son relevantes para el correcto funcionamiento de los distintos departamentos que trabajan en la institución financiera.

Pregunta 4. ¿Los tiempos empleados en las estrategias de recuperación de los servicios críticos son los adecuados frente a una caída de los sistemas de información y comunicación en la cooperativa?

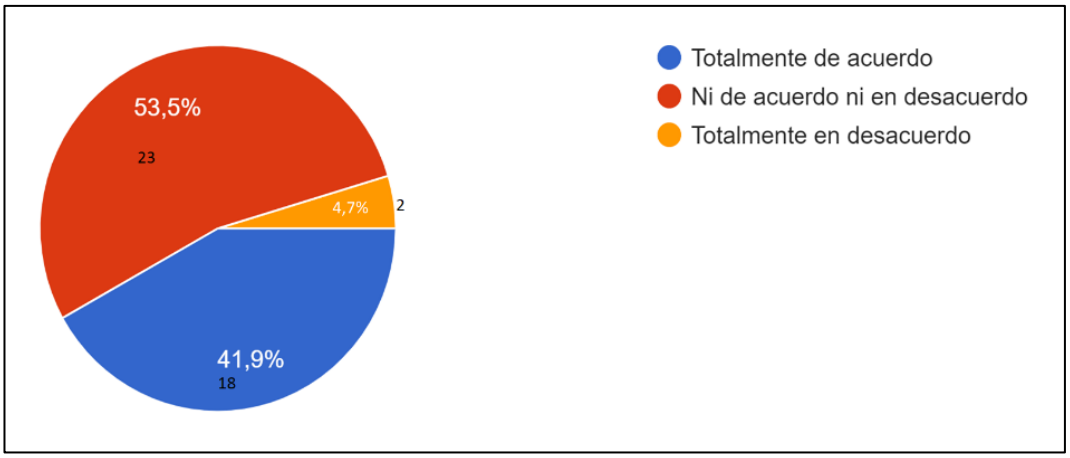

Figura 11. Tiempos de Estrategias
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

De total de los encuestados, el 41,9% respondió que está ni de acuerdo ni en desacuerdo que los tiempos empleados en las estrategias de recuperación son adecuados frente a las caídas de los sistemas, el 53,5% del personal señaló que está totalmente de acuerdo, mientras que el 4,6% restante manifestó que se encuentra totalmente en desacuerdo.

Los tiempos que la cooperativa destina a las estrategias de recuperación no satisfacen a gran parte del personal administrativo de la institución, probablemente frente a las caídas de los servidores han sido tiempos insuficientes para procesar y dar solución inmediata a estos.

Pregunta 5. ¿Está de acuerdo con que se deben realizar 2 simulacros al año en caso de interrupción de los sistemas de información y comunicación en la cooperativa?

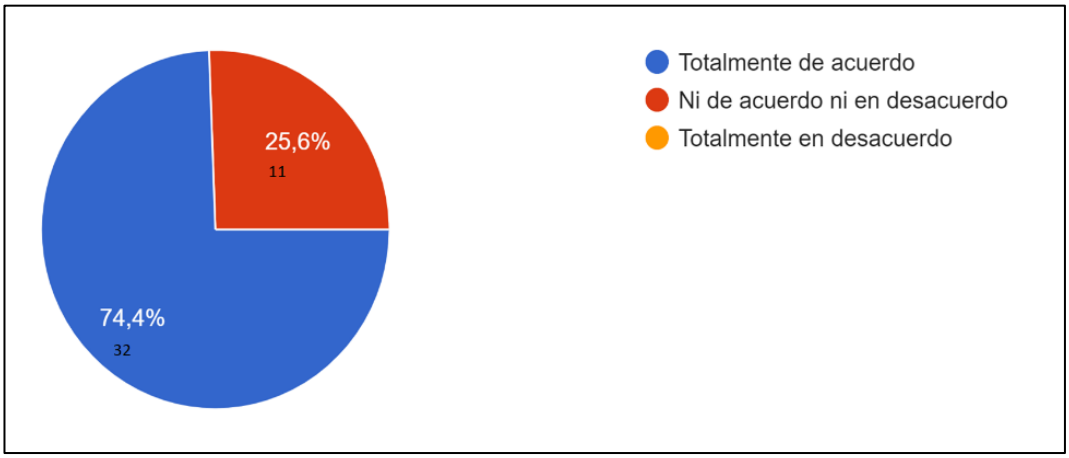

Figura 12. Simulacros
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

El 74,4% de las personas encuestadas indicaron que están totalmente de acuerdo en realizar dos simulacros cada año en caso de interrupción de los sistemas de información, tanto que el 25,6% reveló que está ni de acuerdo ni en desacuerdo con el enunciado.

Según la información proporcionada las tres cuartas partes del personal involucrado en la cooperativa necesitan de un par de simulacros anuales para estar preparados ante los eventos críticos que se presenten en la institución. Con las respuestas obtenidas se evidencia un gran interés en participar en los procedimientos previos para la continuidad de negocio.

Pregunta 6. ¿Se debe actualizar el manual de Continuidad de Negocio después de cada simulacro o acontecimiento de emergencia con resultados satisfactorios?

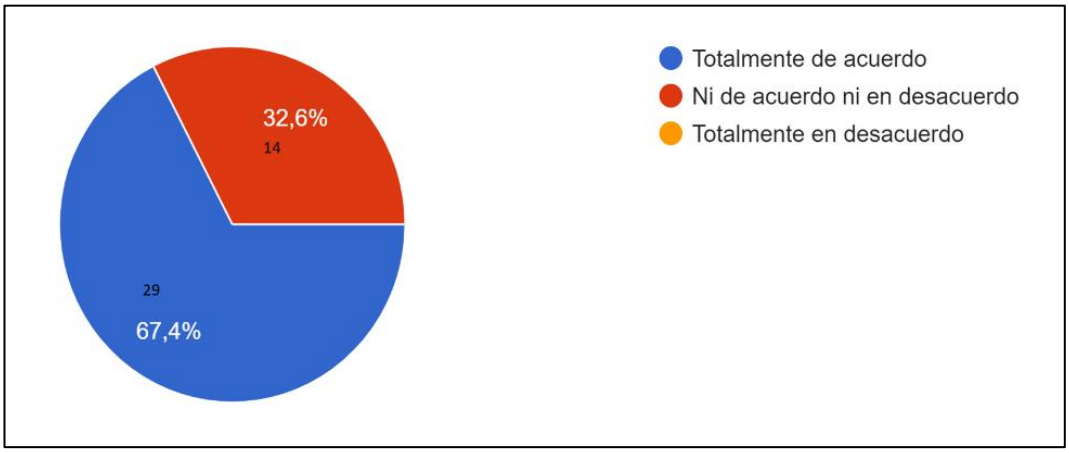

Figura 13. Actualización del Manual
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

De la totalidad de las respuestas obtenidas, el 67,4% tachó que está totalmente de acuerdo en que se debe actualizar el manual de continuidad de negocio después de cada simulacro y a su vez el 32,6% respondió que está ni de acuerdo ni en desacuerdo.

Acorde a los datos tabulados, la actualización del manual de continuidad de negocio de la cooperativa debe realizarse después de algún simulacro o evento critico donde se pueda identificar los fallos y deficiencias que afectaron los procedimientos para el correcto funcionamiento de los servicios informáticos y de comunicación.

Pregunta 7. ¿En la cooperativa se debe realizar tareas de monitoreo y mantenimiento a los sistemas de información y comunicación para evitar riesgos?

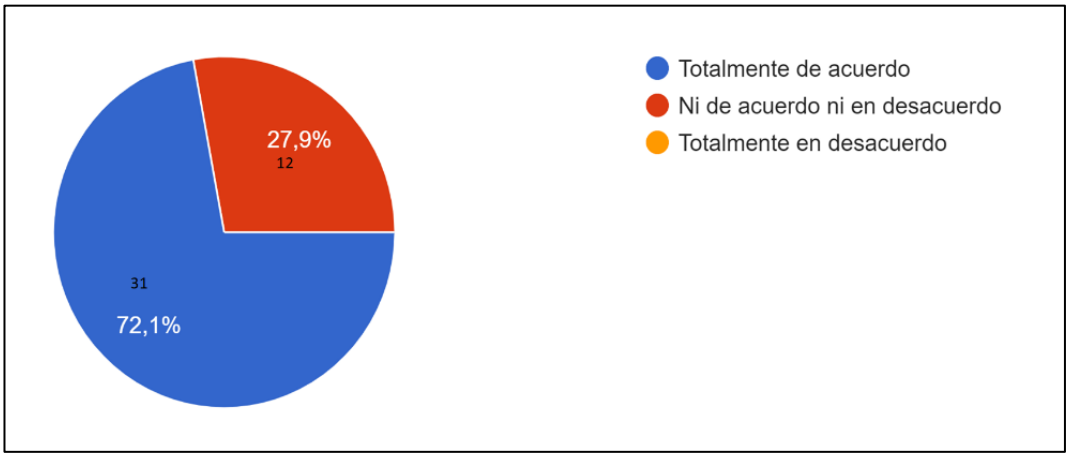

Figura 14. Monitoreo y Mantenimiento
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

El 72,1% de los trabajadores encuestados indicó que está totalmente de acuerdo con que la cooperativa debe realizar tareas de monitoreo y mantenimiento a los sistemas de información, mientras que el 27,9% manifestó que se encuentra ni de acuerdo ni en desacuerdo con la interrogante.

Según las respuestas recolectadas se enuncia que las tareas de monitoreo y mantenimiento de los sistemas de información y comunicación son primordiales para prevenir riesgos que comprometan el funcionamiento de los servicios financieros. Además que el departamento de informática y comunicación debe ser evaluado para encontrar problemas físicos o digitales y posteriormente puedan recibir un óptimo mantenimiento.

Pregunta 8. ¿Conoce qué acciones se debe aplicar para evaluar y reducir el impacto de un incidente crítico de los sistemas de información y comunicación en la cooperativa?

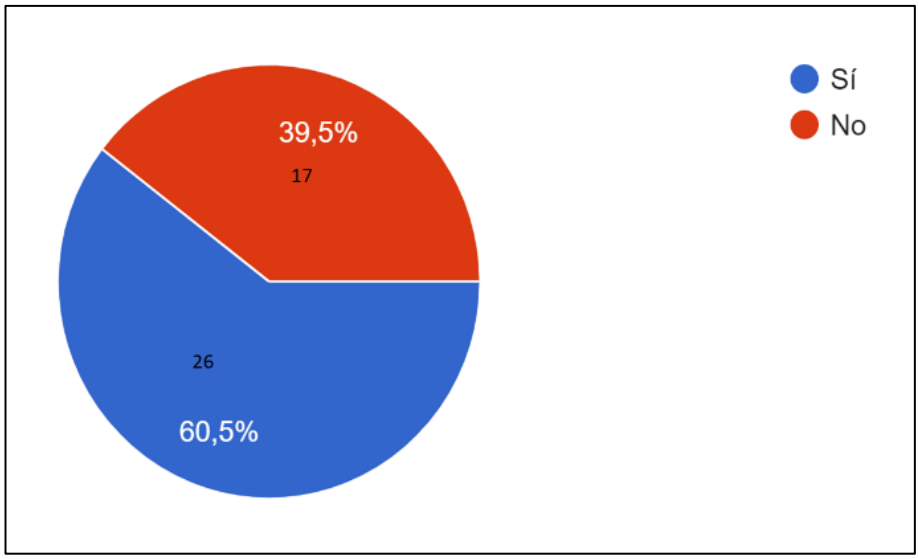

Figura 15. Acciones de Impacto
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

De acuerdo con la información encuestada, el 60,5% de las personas revelaron que si conocen las acciones que se deben aplicar para evaluar y reducir el impacto de un incidente crítico, mientras que el 39,5% señaló que no conocen nada relevante al tema.

El personal que labora en la cooperativa no conoce las acciones que se deben seguir para evaluar y reducir el impacto que cause algún evento crítico sobre los sistemas de informática y comunicación de la institución financiera. El conflicto se origina que al desconocer los procedimientos, el tiempo de recuperación se va a extender y por ende los servicios no van a estar disponibles de forma inmediata.

Pregunta 9. ¿Conoce las debilidades y amenazas que afectan a los servicios e infraestructura del departamento TIC de la institución?

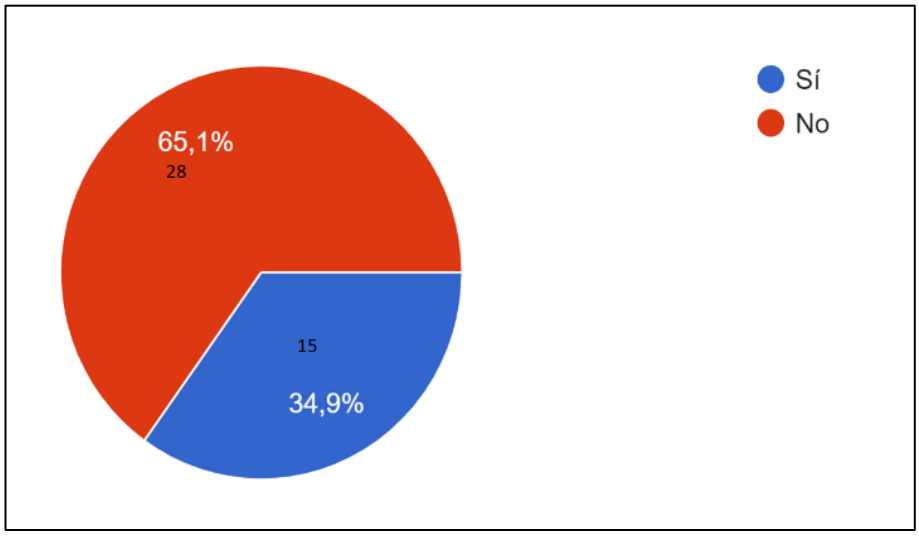

Figura 16. Debilidades y Amenazas
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

Del total de los encuestados el 34,9% respondió que si conoce las debilidades y amenazas que afectan a los servicios e infraestructura del departamento TIC, y a su vez el 65,1% de las personas manifestó que no.

Según los datos obtenidos en la encuesta, el personal desconoce las debilidades y amenazas que influyen completamente en el departamento TIC de la institución. Identificar las falencias de cada departamento permite una oportuna intervención para prevenir ante cualquier evento critico que se presente.

Pregunta 10. ¿Se debe capacitar al personal nuevo y vigente sobre los procedimientos actualizados frente a un evento crítico?

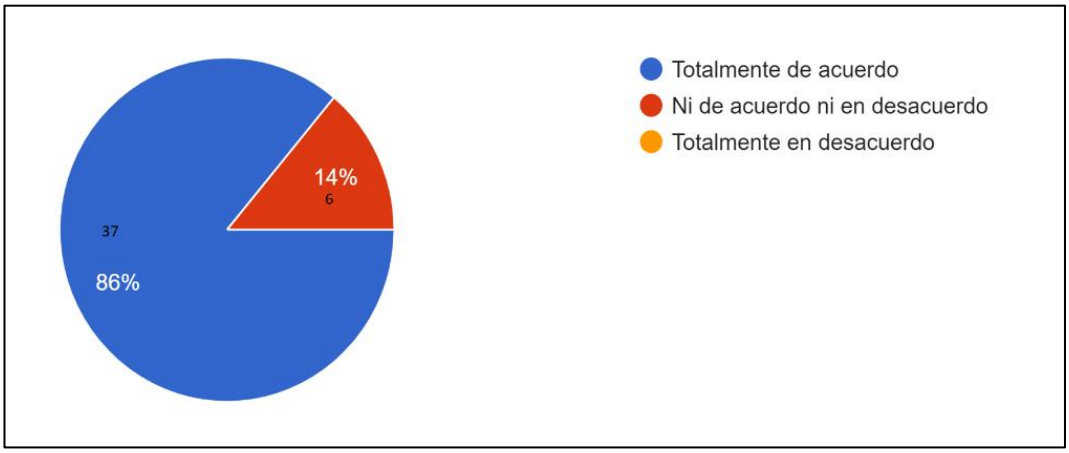

Figura 17. Capacitación al Personal
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

La gran mayoría de los encuestados con el 86% reveló que están totalmente de acuerdo en capacitar al personal nuevo y vigente sobre los procedimientos ante un evento crítico, a su vez el 14% indicó que está ni de acuerdo ni en desacuerdo con lo enunciado.

El personal de la cooperativa está convencido que la capacitación inicial al personal entrante es necesaria para que se familiaricen con los procedimientos que se manejan ante eventos críticos en la institución financiera. De igual forma, se debe capacitar periódicamente al personal que labora con anterioridad en la cooperativa para que los simulacros puedan ser aplicados de manera ordenada y eficaz.

Pregunta 11. ¿Conoce donde puede encontrar el manual de procesos en un momento de emergencia?

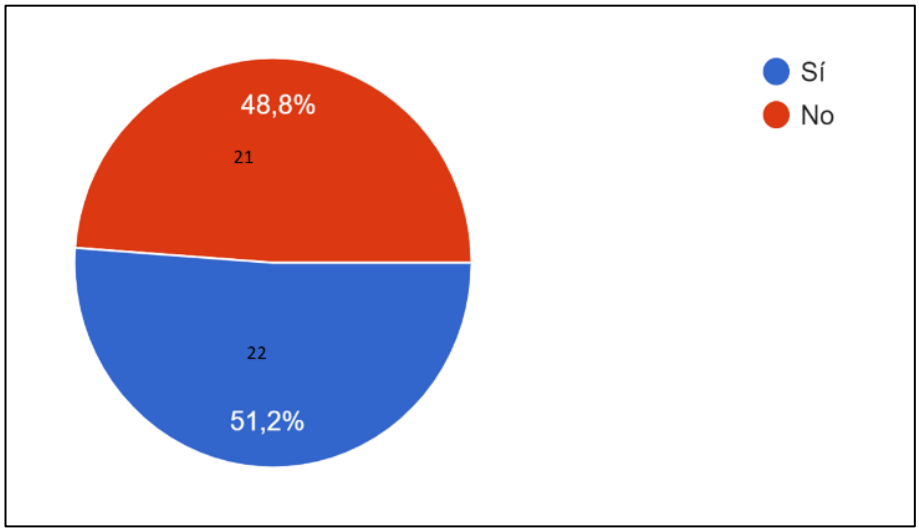

Figura 18. Manual de Procesos
Fuente: Henry Ricardo Ortega Castro

Análisis e Interpretación

Del total de los encuestados, el 51,2% respondió que si conoce donde se encuentra el manual de procesos, mientras que el 48,8% indicó que no.

Según los datos proporcionados por el personal encuestado, existe un desconocimiento del lugar donde pueden encontrar las herramientas necesarias para enfrentar y solventar ante eventos críticos que comprometan la continuidad de los servicios y operaciones financieras.

3.2. Desarrollo de la Propuesta

MANUAL DE CONTINUIDAD DE NEGOCIO DE LA COAC "CRECER WIÑARI" LTDA.

En este manual se presenta el planteamiento de los planes de acción a tomar en caso de presentarse un evento el cual comprometa el correcto flujo de los procesos de la COAC "Crecer Wiñari" ltda. para esto se emplean los siguientes procedimientos: comunicación y gestión de incidentes necesarios para la activación y ejecución del plan de continuidad de negocio. En tal sentido en este manual se mencionará los siguientes ítems:

- Plan de Comunicación - Crisis
- Estrategias de Continuidad de negocio
- Procesos de Continuidad y Reanudación
- Plan de Pruebas

Plan de Comunicación - Crisis

Se detallan los procesos de comunicación necesarios en el caso de aparecer un incidente de tipo crisis, así como la forma de ejecución y asignación de responsables, mismos que servirán como base en la activación del plan de continuidad de Negocio en este manual.

En la COAC "CRECER WIÑARI" LTDA. es importancia la creación, validación y ejecución de los planes de comunicación los cuales incluyan a todos los responsables de la ejecución de las actividades incluidas en el plan de continuidad, por lo cual se han definidociertas actividades que aportarán al correcto flujo de la comunicación:

a) Identificar y establecer un equipo de trabajo que gestione la comunicación de los eventos de crisis.
b) Establecer las vías de comunicación más favorables que permitan la correcta comunicación entre entes internos y externos de la institución con el fin de notificar correctamente.

c) Considerar dentro de los planes de comunicación todo personal que se pueda ver afectado por un evento de crisis dentro de las instalaciones de la institución.

Objetivo

Establecer vías de comunicación efectivas que permitan el mayor porcentaje de alcance del personal que pudiera verse afectado, en caso de presentarse un evento que obligue a la COAC "CRECER WIÑARI" LTDA. a detener sus actividades y operaciones de manera normal.

Alcance

El plan de comunicación incorporará todas las áreas de negocio que pertenezcan a la Administración Central de la COAC "CRECER WIÑARI" LTDA. De igual aquellos proveedores externos claves para la ejecución del plan de continuidad

Escenarios considerados para comunicación:

- Denegación de servicio
- Acceso no autorizado
- Caída del sistema (agotamiento de recursos)
- Degradación de los soportes de almacenamiento de información
- Fallos de servicio en canales de Comunicación
- Corte de Suministros Eléctricos
- Erupción Volcánica
- Terremoto
- Fuego

Equipo de Comunicación

El personal de Comunicación - Crisis consta de:

- Coordinador: Gestiona recursos de comunicación para la notificación de eventos de crisis de una forma organizada y oportuna.

- Asesor Legal: Ejecuta e informar sobre las normativas legales y los

requerimientos que emiten los entes de control en caso de presentarse un evento de crisis.

- Staff de Comunicación: Comunican a la parte operativa de la institución.
- Voceros internos y externos: transmiten la información necesaria al público relacionado.

Estrategias de comunicación durante un evento de Crisis. - Las estrategias a tomar se dividen en:

Antes. - Actividades de prevención y preparación.

Se debe informar y dimensionar los posibles eventos de crisis que tengan afectación en el flujo de las operaciones en la Administración Central de la COAC "Crecer Wiñari" Ltda.

Mantener actualizada la base del personal, así como también asegurarse que los mecanismos de comunicación habilitados en caso de un incidente operen de una forma adecuada.

Durante. - Actividades de control y operación alterna

- **Análisis de la situación.**

Ejecutar un análisis objetivo del incidente presentado para identificar el origen del problema, las consecuencias internas y externas de la institución dimensionando el impacto final que tendrá sobre la operación del negocio

- **Planteamiento de estrategias de comunicación.**

Una vez realizado el análisis de la situación y tomando en cuenta el posible impacto sobre la institución, se deberá evaluar cuales son los recursos necesarios y la forma más adecuada de comunicar el incidente.

Para identificar las estrategias de comunicación, se debe considerar ciertas observaciones tales como:

- Todo incidente tiene una consecuencia sobre la imagen de la institución por lo cual el canal de comunicación debe generar un mensaje acorde a la magnitud del incidente con capacidad de alcanzar a la mayor cantidad de personas.

- El coordinador de comunicación de crisis entregará el mensaje a todos los involucrados, mismo que deberán comprender a la versión oficial de lo ocurrido.

- El alcance del mensaje depende de la magnitud del incidente, por lo cual únicamente deberá llegar a los puntos o personal afectado de manera prudente y cautelosa teniendo presente los vacíos pueden dar lugar a la tergiversación de la información.

- La retroalimentación de comentarios por parte de socios y clientes son fundamentales, por lo que se deberán estabilizar los procesos.

- **Prioridades a la hora de informar**

Una vez iniciado el plan de comunicación el mensaje debe llegue a todos nuestros grupos de interés, esta tiene que ser la primera versión que conozcan dando preferencia a los entes de control, socorro, autoridades y funcionarios clave de la organización.

Después. - Actividades de estabilización

Fin del evento de crisis, evaluación y retroalimentación

Una vez que se ha estabilizado los procesos de negocio, se necesita iniciar un proceso de evaluación el mismo que permita identificar fortalezas y deficiencias durante cada fase del proceso de comunicación, establecer cambios que nos permita mejorar la capacidad de respuesta por parte del personal involucrado.

Además, se debe monitorear el impacto de la crisis sobre la confianza de nuestro

grupo de interés con el fin de implementar procedimientos de mejora y optimización.

Organización de Comunicación de Crisis

Tabla 5. Grupos de recuperación

Posición / Rol	Prioridad	Critico (S/N)
Coordinador de Comunicación en el evento de Crisis	1	S
Staff de Comunicación	2	S
Asesor legal	1	S
Voceros	3	S

Elaborado por: H. Ortega, 2021.

Leyenda.

Posición: Posición o rol al que pertenece el grupo de Comunicación en Crisis

Prioridad: Es el orden de importancia de las posiciones donde 1 es el primero que se ejecutará, 2 el segundo y así sucesivamente.

Criticidad: Permite determinar si es crítica/indispensable dentro del Grupo. S=Sí, N=No es Crítico.

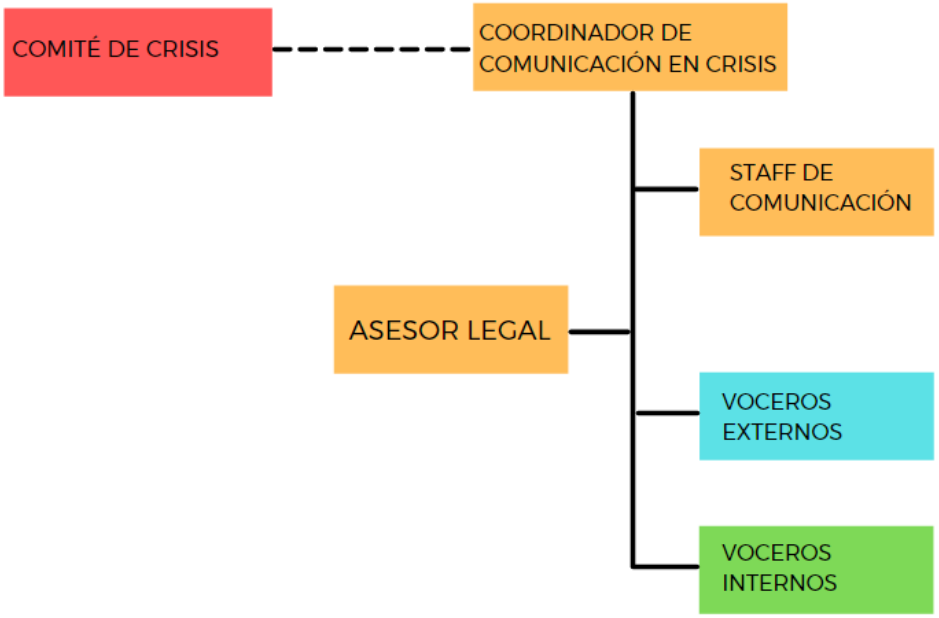

Figura 19. Organización de comunicación de crisis
Fuente: Henry Ricardo Ortega Castro

Para este caso y tomando en cuenta que se analizará únicamente los eventos de crisis que afecten la provisión de servicios por parte del departamento de Tecnología los roles representados en el organigrama serán ocupados por el siguiente personal:

- Coordinador de Comunicación en Crisis: Jefatura de Tecnología
- Staff de Comunicación en Crisis: personal del Comité de Crisis
- Asesor Legal: Representante de la Dirección Jurídica

Fase Antes: Actividades de Preparación

Tabla 6. Actividades de Preparación

Tarea-Descripción	Frec.	R 1	R 2	R 3	R 4
Establecer sitios alternativos que serán utilizadas durante los eventos de crisis	Anual	X			
Asegurar el listado de sitios externos actualizados y de conocimiento del personal de comunicación de crisis.	Anual	X			
Asegurar la existencia y disponibilidad de recursos necesarios para la recopilación de toda la información posible del evento de crisis.	Anual	X			
Identificar y asegurarse el conocimiento sobre las responsabilidades del personal que conforman los organismos de acción.	Anual	X			X
Mantener actualizado y disponible el listado de participantes con sus respectivos contactos del equipo de comunicación en crisis.	Trimestral	X			
Validar y actualizar el directorio interno del personal clave de cada área.	Anual	X			
Asegurar la distribución, entendimiento y actualización del Plan de Comunicación en Crisis.	Semestral	X			
Programar simulacros periódicos que activen el plan de comunicación en crisis.	Semestral	X			

Elaborado por: Henry Ricardo Ortega Castro

Leyenda.

Nro.: Número de la tarea.

Tarea Descripción: Descripción de la actividad o tarea.

Duración: Tiempo de ejecución de la tarea.

R1, R2, R3, R4: Roles responsables.

Fase Durante: Actividades de Respuesta y Operación Alterna

Coordinador de Comunicación en Crisis

Tabla 7. Actividades de Respuesta y Operación Alterna

Rol: Coordinador de Comunicación en Crisis		
Nro.	**Tarea-Descripción**	**Duración**
Actividades de Respuesta (DURANTE)		
1	Activado el Comité de Crisis se debe esperar la notificación para la activación del Plan junto con la información detallada del evento de crisis mismo que fue analizado por el comité	Dentro de una hora
2	Convocar al Asesor Legal para la elaboración de los mensajes que serán transmitidos a las audiencias afectadas.	Dentro de las primeras 2 horas.
3	Implementar un cronograma de comunicación que incluya el orden de difusión hacia las áreas afectadas de negocio.	Dentro de las primeras 6 horas.
4	Solicitar la definición de los canales de comunicación para los mensajes previamente aprobados al Comité de Crisis.	Dentro de la primera hora.
5	Al recibir la aprobación del comité de crisis, se debe comunicar a los voceros que harán llegar a cada una de las audiencias los mensajes específicos.	Dentro de la primera hora.
6	Dar seguimiento a la respuesta del público con el fin de valorar el impacto que ha sufrido el negocio.	Desde el envío del comunicado hasta que concluya la crisis.
7	En función de las respuestas entregadas por los involucrados se procede a identificar y ejecutar acciones correctivas.	Desde el envío del comunicado hasta que concluya la crisis.
8	Desactivar el estado de comunicación de crisis	Inmediato

Elaborado por: Henry Ricardo Ortega Castro

Leyenda:

Rol: Nombre del grupo de Comunicación en Crisis

Nro.: Número de tarea.

Tarea: Descripción de la actividad o tarea.

Frecuencia: Frecuencia de ejecución de tareas

Duración: Tiempo de aplicación de la tarea.

En cada fase el coordinador de comunicación deberá interactuar con los miembros responsables de la ejecución del plan de comunicación por que estas tareas serán compartidas variando únicamente el grado de responsabilidad de cada participante

Fase Después: Restauración y Retorno

Tabla 8. Restauración y Retorno

N°	Tarea	Duración	R	R	R	R
			1	2	3	4
A	REPARACIÓN: Establece actividades que minimicen los daños ocasionados por el evento de crisis y también ser utilizado como línea base para el retorno a la normalidad.					
Estado de la situación: Desastres Controlados						
1	El comité de crisis notificará que la crisis ha sido controlada	Dentro de la primera hora.	X	X	X	X
B	VUELTA A LA NORMALIDAD: Generar actividades que reestablezcan el correcto funcionamiento de la institución, desactivando los ambientes alternos y activando el entorno de producción normal.					
Estado de la situación: Fin del Desastre						
2	Documentar cada proceso de comunicación ejecutados durante el evento de crisis	Dentro de las 48 horas.	X	X		
3	Dimensionar el impacto generado por la crisis en la imagen de la institución.	Dentro de las 48 horas.	X	X		

4	Presentar ante el comité de crisis el informe del evento	Dentro de las 48 horas.	X			
5	Generar y aplicar planes para solventar los daños, producto de la crisis	Dentro de las 72 horas.	X			
6	Esperar que el Comité Crisis la notificación de finalización de la crisis por parte del Comité de Crisis	Dentro de las 72 horas.	X	X	X	X
7	Reestructurar en caso de ser necesario el plan de comunicación de crisis basado al conocimiento adquirido por el evento sucedido.	Dentro de las 72 horas.	X	X	X	X
8	Actualizar toda documentación que sustente el plan de continuidad.	Dentro de las 72 horas.	X			

Elaborado por: Henry Ricardo Ortega Castro

Leyenda:

- **Nro.**: Número de la tarea.
- **Tarea:** Descripción de la actividad o tarea.
- **Duración:** Tiempo de aplicación de la tarea
- **R1, R2, R3, R4:** Roles responsables

Rol Descripción del Rol

- ✓ R1 Coordinador de Comunicación en Crisis
- ✓ R2 Staff de Comunicación
- ✓ R3 Asesor Legal
- ✓ R4 Voceros

1. Estrategias de Continuidad de Negocio

Se presenta planteamiento del BCP (Business Continuity Plan) para la COAC "Crecer Wiñari Ltda." en base a análisis recolectados anteriormente con el fin de asegurar la continuidad de los procesos de Tecnología.

1.1. Establecer Estrategias de Recuperación de Continuidad de Negocio

Se explicará los procedimientos y estrategias más viables para la ejecución de los análisis de impacto y factibilidad. Dichos procedimientos y estrategias tienen como finalidad determinar el camino más optimo el cual asegure la continuidad de los procesos, la recuperación ante incidentes que generen un impacto alto.

Adicionalmente se señalan puntos específicos de la norma ISO/IEC 22301:2012 en la cual se basa este trabajo para identificar las Estrategias de Recuperación, los procedimientos y acciones que se implementaran en la COAC "Crecer Wiñari Ltda.".

1.1.1. Síntesis

Este plan tiene como propósito la definición, diseño y selección de estrategias fundamentales que aseguren la continuidad de negocio de la institución estableciendo Tiempos Estimados de Recuperación (RTO) y tiempos máximos Tolerables de Interrupción (MTD), los cuales que deben alinearse a los objetivos de la institución.

1.1.2. ISO/IEC 22301:2012 – Procesos y Actividades Fundamentales

La norma ISO/IEC 22301:2012 establece que la institución debe señalar sus procesos fundamentales y actividades críticas de cada uno para poder enfocar sus esfuerzos en la implementación de controles y estrategias de mitigación de riesgo que ayuden a la generación de un estado de continuidad para el negocio.

En ese sentido es importante que la institución logre:

1.1.2.1. Determinar los Tiempos Objetivos de Recuperación (RTO), así las estrategias, planes y recursos disponibles que permitan cumplir estos tiempos, para lo cual el personal asignado debe tener en cuenta que los RTO no puede superar los Plazos Máximos Tolerables de interrupción (MTPD) de los servicios ofrecidos por el área de Tecnología, estos soportar los procesos y actividades de cada ciclo de negocio.

1.1.2.2. Identificar al personal primordial asignado a las tareas de recuperación ya sea interno o externo (proveedores).

1.1.2.3. Documentar el organigrama del comité de recuperación, la estructura del grupo de trabajo en la ejecución, las tareas operativas necesarias, la reanudación de los servicios, tomando en cuenta las pérdidas económicas y de información que la institución esté dispuesta a asumir.

1.1.3 Aplicación en la COAC "Crecer Wiñari" Ltda.

- Identificar las estrategias y necesidades de continuidad para el proceso critico ofrecido por el área de Tecnología:
    - Validar mecanismos disponibles que aseguren la continuidad de negocio sobre las comunicaciones del personal.
    - Establecer parámetros que aseguren la continuidad de los recursos, la infraestructura y el personal de Tecnología que soporten al negocio.
    - Identificar los procedimientos alternativos que abastezcan la continuidad de los procesos que mantienen los servicios de Tecnología del negocio

Para esto se puede contar con diferentes estrategias preventivas y de recuperación, proporcionales a las capacidades del personal, operacionales y económicas de la institución considerando lo siguiente:

- **Diversificación:** Es adecuando si se dispone de recursos económicos y técnicos, cuando el RTO está definido en minutos o un par de horas es adecuado.

- **Replicación:** se encuentra sujeta a la capacidad económica de la institución, infraestructura, comunicaciones y recursos que soporten la replicación de datos ofrecidos por Tecnología, se debe contemplar espacios físicos para alojar la infraestructura esto es factible cuando el RTO es menor de un día.

- **Stand By:** Es la más adoptada por los especialistas de TIC's, ofrece continuidad a costos más accesibles, permite implementar sitios alternos capaces de soportar los principales aplicativos de la institución mediante equipos con capacidades dedicadas, mientras que la automatización de dichos servicios puede ser tercerizados como el arrendamiento de equipos e infraestructura para contingencia. Esta estrategia es viable cuando el RTO está definido en un par de días.

- **Adquisición Post Incidente:** En caso de adoptar esta estrategia, es necesario realizar evaluaciones a proveedores calificando su criticidad y se evalúe las capacidades de respuesta ante los requerimientos de la institución, Esto es viable cuando los RTO están definidos para varios días o semanas.

- Definir una estrategia de continuidad la cual se encuentre alineada con el BIA (Bussiness Impact Analysis) y sus resultados, con el fin de enfocar los esfuerzos en los servicios críticos del área de TI los cuales soportan el giro del negocio.

- Analizar los factores necesarios para la elaboración de una estrategia de continuidad alineada, eficaz y fiable las macro estrategias y objetivos de

la organización, proveyendo a la Alta Gerencia los fundamentos para la toma de decisión óptima.

- Definir cuál será la estructura de respuesta necesaria para una adecuada ejecución de las estrategias establecidas.

- Analizar los acuerdos contractuales con los proveedores, para identificar requerimientos incluidos y no incluidos en los estándares sugeridos.

ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO

Objetivo

Validar y definir las estrategias capaces de adaptarse con los tiempos objetivos para la recuperación definidos por parte de la BIA, los cuales deben ser capaces de ofrecer continuidad en los servicios de TI para los entornos y procesos de negocio que estos soportan

Componentes

Los principales componentes necesarios para una correcta definición de una estrategia de continuidad de negocio viable, tenemos: Infraestructura, Recursos, Personal, Información sensitiva y Proveedores Críticos. Además, hay que considerar ciertos puntos clave como: La seguridad de la Información, sitios alternos donde se levantaran los servicios críticos y la seguridad del personal encargado de ejecutar las distintas tareas de recuperación y continuidad.

Tipos de Sitios Alternos

Warm Site: Es el levantamiento de respaldos de información, genera menos costos de implementación dado que no se requiere de recursos para la replicación en línea, solo se debe disponer de conectividad base con enlaces a los organismos externos y equipos básicos que soporte los servicios críticos de TIC’s. Se estima un tiempo de 24 a 48 horas de recuperación con esta estrategia.

Hot Site: Ofrece una recuperación casi inmediata de los servicios, sin embargo, maneja una inversión económica bastante alta debido a que ya que es necesario

canales de replicación de datos en caliente para alimentar la base de datos del sitio alterno. Se estima un tiempo de 0 a 4 horas.

Cold Site: Es la solución más económica genera un ahorro notable durante la implementación de recursos de contingencia para el sitio alterno, da interés a comunicaciones estrictamente críticas y equipos necesarios para el levantamiento de los servicios fundamentales, se encuentra basada en el levantamiento de copias de respaldo con tiempos de recuperación son de aproximadamente una a dos semanas.

Tabla 9. Estrategias Propuestas a Nivel de Infraestructura

	Estrategia	Tipo	Responsable
Espacio Físico			
1	Determinar los sitios alternos que levantaran los servicios críticos de TI fundamentales para los procesos de negocio.	Táctico	Jefe de Operaciones y Tecnología
2	Seleccionar una adecuada localidad para el Sitio Alterno, éste debe contar con recursos mínimos para levantar los servicios críticos de TI capaz de soportar el giro del negocio.	Táctico	Jefe de Operaciones y Tecnología
Ordenamiento de aplicaciones/servidores			
3	Identificar las aplicaciones críticas que las automatizan basado en las necesidades específicas en el ciclo de negocio, así como servidores o recursos de infraestructuras necesarios para su correcto funcionamiento con el fin de agilizar los procesos de continuidad.	Táctico	Dirección de Informática y comunicaciones
4	Evaluar los procedimientos de la institución para la adquisición e implementación de aplicaciones y procedimientos de evaluación que determinen la criticidad de los RTO y MTDs.	Táctico	Dirección de Informática y comunicaciones

Elaborado por: Henry Ricardo Ortega Castro

Tabla 10. Estrategias Propuestas a Nivel de Personal

	Estrategia	Tipo	Responsable
Identificación de roles primarios y alternos			
1	Establecer jerarquías adecuadas para el comité de continuidad de negocio, establecer la estructura de TI (personal) necesario para la ejecutar procesos de levantamiento de servicios, conocimientos técnicos y las responsabilidades para cada actividad. Además, se debe identificar al personal fundamental de cada área de negocio que se encarguen de las operaciones del sistema.	Estratégico	Comité de Continuidad
2	Identificar personal alterno para asegurar la continuidad de las operaciones de la COAC "Crecer Wiñari Ltda." en caso de que el personal primario no se encuentre disponible por causa de un evento de desastre, se recomienda nombrar más de un alterno con capacidades para cumplir las funciones del personal primario. De igual manera se debe considerar el trabajo remoto en caso de no poder contar con un ambiente de trabajo.	Estratégico	Comité de Continuidad
3	Identificar características similares entre el personal de la institución para definir los distintos roles alternos en los procesos que demanden mayor cantidad de personal, este personal no necesita ser necesariamente de la misma área o ubicación geográfica.	Estratégico	Jefatura de Riesgos
4	Asignar un responsable para el BCP, dicha persona debe tener dedicación exclusiva de ello, gestionará el BCP, los elementos tecnológicos necesarios por el negocio además de contar con conocimientos avanzados para el manejo de Continuidad de Negocios.	Estratégico	Jefatura de Riesgos
Capacitación de Personal			
5	Promover mediante una agenda de fechas las capacitación para que cada dirección y jefatura gestione la inducción tanto a personal primario como alterno y disminuir brechas de conocimiento.	Estratégico	Jefatura de Riesgos

6	Crear programas de capacitación virtual para todo el personal, se debe incluir protección a la familia, prevenciones de emergencias, reportes de incidentes en casos de desastres, entre otros.	Estratégico	Talento Humano
7	Implementar talleres sobre el manejo de situaciones de crisis por parte del personal, con el fin de asegurar una respuesta adecuada durante un desastre. Invitar al ejercicio autoridades tales como policía nacional, defensa civil, bomberos, para que participen en estos talleres.	Estratégico	Talento Humano
8	Implementar un Plan de Capacitación Anual por parte del área de tecnología para los responsables primarios y alternos, considerar temas técnicos y de procesos, la recuperación en sí de los componentes tecnológicos y poder reducir las brechas de conocimiento que puedan existir entre personal primario y alterno.	Estratégico	Jefatura de Operaciones y Tecnología
Comunicación entre el personal			
9	Asegurar que las distintas áreas que definan un árbol de llamadas internas y poder garantizar una comunicación efectiva entre el personal en caso de desastre.	Estratégico	Cada Área del Negocio
10	Incluir dentro de la política de vacaciones, cláusulas que prevengan que el personal primario y alterno tomen vacaciones en las fechas de capacitaciones, de modo que siempre estén disponibles para estas eventualidades.	Estratégico	Talento Humano
11	Identificar los canales de comunicación posibles entre la COAC "Crecer Wiñari Ltda." y el personal, definir un responsable que administre y comparta cada canal (mensajes de texto, usando un software o tercerizando, canales virtuales)	Estratégico	Jefatura de Tecnología y Comunicaciones

12	Identificar los canales de comunicación que permitan la coordinación entre los integrantes del equipo de recuperación de los sistemas involucrados. Definir un responsable que administre y comparta estos canales: a. Utilizar Celulares y/o radios. b. Crear una evaluación sobre el uso de mensajes telefónicos masivos. c. Crear grupos de mensajería instantánea y/o grupos de correo para informar los roles de recuperación del área y utilizarlos como herramienta de comunicación en caso de desastre.	Estratégico	Jefatura de Tecnología y Comunicaciones
Políticas			
13	Implementar equipos que permita disponer de dinero (efectivo) y poder apoyar de manera económica a los colaboradores afectados por un desastre.	Operativo	Talento Humano
14	Evaluar la distribución de dispositivos móvil de los líderes de recuperación en cada plan y sus respectivos colaboradores.	Operativo	Talento Humano
15	Proporcionar a todo el personal primario y alterno acceso al correo electrónico	Operativo	Jefatura de Tecnología y Comunicaciones
16	Establecer indicadores de continuidad de negocio para medir el desempeño del personal participante en las actividades de recuperación	Operativo	Jefatura de Riesgos
Brigada de Emergencia			
17	Mantener un listado de brigadistas actualizado y organizado de acuerdo con las funciones y sedes para Evacuación, Seguridad, Incendios y Primeros Auxilios.	Operativo	Talento Humano
18	Replicar el esquema de brigadistas en otras instalaciones donde no esté implementado	Operativo	Talento Humano

19	Realizar un plan de responsabilidad social incluyendo los siguientes puntos: a. Definir un kit básico para la asistencia a la comunidad, compuesta por: Alimentos no perecibles, carpas, abrigos, botiquín con medicinas básicas de primeros auxilios. b. Identificar los distintos almacenes para el kit básico de asistencia c. Identificar las alternativas de reutilización para el kit básico d. Presentar un presupuesto total para dichas actividades a implementar	Operativo	Talento Humano
20	Establecer líderes de responsabilidad social (independientemente de los brigadistas del apoyo interno de la COAC "Crecer Wiñari Ltda.") con el objetivo de gestionar las actividades orientadas a velar por el bienestar de la familia y la comunidad en general	Operativo	Talento Humano

Elaborado por: Henry Ricardo Ortega Castro

Tabla 11. Estrategias Propuestas a Nivel de Recursos

	Estrategia	Tipo	Responsable
Relación con autoridades y organismos públicos			
1	Tener un acercamiento con las autoridades.	Operativo	Talento Humano
2	Identificar protocolos vigentes que utiliza el estado para el control de los recursos y servicios necesarios contra desastres.	Operativo	Talento Humano
Acuerdos y/o cláusulas en los contratos			
3	Anexar en los contratos, mantenimiento del edificio, acuerdos que den compromiso de los proveedores y prioridad a la formalización, para realizar una primera evaluación de los daños y establecer las posibilidades de continuar con las operaciones en la instalación afectada.	Operativo	Talento Humano

4	Seleccionar proveedores para la reparación/reconstrucción de las instalaciones y establecer contratos con acuerdos acorde la necesidad.	Operativo	Talento Humano
5	Revisar la existencia de acuerdos a nivel de servicio (SLA) en los contratos vigentes con proveedores mismos que incluyan sanciones por incumplimiento, así aseguramos la continuidad de dichos servicios en casos de desastre.	Operativo	Talento Humano
Políticas			
6	Revisar las políticas vigentes y coordinar con proveedores permitiendo contratos con base que incluyan cláusulas de Riesgo estableciendo requisitos mínimos los cuales deben cumplir un proveedor considerando la auditoria de esquemas de continuidad de negocio para proveedores críticos.	Operativo	Dirección Jurídica
7	Establecer una política que permita realizar gastos adicionales en eventos de desastre. Se debe valorar los siguientes aspectos como: definir esquemas locales o por área y coordinar con entes públicos como ONPE y SUNARP sobre dichas políticas y procedimientos que se implementarán en la COAC "Crecer Wiñari Ltda."	Operativo	Asistente Contable
Evaluación de esquemas de continuidad			
8	Investigar esquemas de contingencia que manejen los proveedores críticos, calificar si estos pueden asegurar el servicio, además, seleccionar un mínimo de dos opciones de comunicación a los contactos clave En caso de que los proveedores no posean un Plan de Continuidad, se solicitará de manera urgente la implementación de contingencia que se pueda utilizar en eventos de desastre.	Operativo	Talento Humano
9	Establecer un plan de citas periódicas de los proveedores con el fin de revisar los esquemas de continuidad ofrecidos.	Operativo	Talento Humano
Pruebas de contratos y acuerdos de niveles de servicio			

10	Definir un Plan Anual de testeo a los servicios y/o aplicaciones que se relacionados con los procesos que involucren a los proveedores más críticos, definiendo pruebas que evalúen los diferentes escenarios y niveles de estrés, considerando como insumo un formato de Esquema de testeo proporcionado por la Continuidad de Negocio	Operativo	Jefatura de Operaciones y tecnología

Elaborado por: Henry Ricardo Ortega Castro

1.2. Procesos de Reanudación y Continuidad

1.2.1. Procedimiento de Continuidad de Negocio COAC "Crecer Wiñari" Ltda.

Descripción: En el caso de aparecer un evento de indisponibilidad, los responsables de las áreas afectadas participarán de la siguiente manera e informarán al responsable de Riesgos:

1) Identificar las causas del incidente, indicando los sistemas informáticos, servicios y procesos afectados.

2) Esclarecer el nivel de afectación, teniendo en cuenta lo establecido en este documento.

3) Comunicar al personal responsable los procedimientos de activación del plan de continuidad por medios disponibles y en orden de ejecución de los procedimientos.

4) El personal responsable ejecutará los procesos de continuidad de negocio y restablecerá los servicios afectados por el evento de desastre.

5) Se solicitará a los proveedores que restablezcan los servicios afectados en caso de ser necesario y según sus procedimientos de continuidad de negocio acordado.

6) En caso de ser necesaria la movilización del personal critico de La Cooperativa y/o proveedores se utilizarán los recursos de la institución o personales del personal.

7) Gerencia General determinará según sea necesario los términos de comunicación a los clientes perjudicados por la indisponibilidad del servicio, incluyendo tiempos estimados en que se restablecerán.

8) El Comité supervisará en todo momento esta activación, en caso de presentarse inconvenientes deberán tomar acciones necesarias para la reanudación del servicio.

9) El personal responsable de la ejecución de los procedimientos deberá informar al Comité de Continuidad de Negocio la aplicación de los procedimientos o cualquier novedad referente a su cumplimiento.

10) Una vez restaurados los servicios con los procedimientos de continuidad de negocio, se realizará un monitoreo del servicio en periodos máximos de 1 hora identificando los inconvenientes que puedan surgir en la prestación del servicio y aplicar los correctivos en caso de presentarse.

11) Una vez restablecidos los servicios con los procedimientos de continuidad de negocio se realizará el monitoreo del servicio en períodos de máximo 1 hora, buscando identificar posibles inconvenientes en la prestación del servicio y tomar los correctivos del caso.

12) Una vez los servicios se han restablecido, se determinarán acciones necesarias para habilitar toda infraestructura afectada por el incidente inicializando toda acción para la recuperación correspondiente.

1.2.2. Consideraciones Generales

1.2.2.1. Cada miembro del Comité de Continuidad de negocio debe tener una copia vigente impresa de los documentos referentes al Plan de Continuidad.

1.2.2.2. Una vez distribuida la información de los procedimientos de continuidad de negocio aprobado, el jefe de Tecnología, deberá custodiar los procedimientos de manera física y socializarlos con el personal de la dirección.

1.2.2.3. Los responsables principales y alternos de la aplicación de procedimientos deben tener todos los documentos vigentes y los procedimientos a su cargo para ejercer sus actividades dentro del Plan de Continuidad.

1.2.2.4. Todo documento correspondiente al Plan de Continuidad de Negocio que se encuentre bajo custodia del personal de la Institución debe mantenerse bajo los respectivos niveles de confidencialidad, sin limitar el fácil acceso al personal responsable aplicación y actualización.

1.2.2.5. La Dirección de Desarrollo Organizacional y Procesos tiene la responsabilidad de velar por la distribución, actualización y garantía acerca del acceso a los documentos del Plan.

1.2.2.6. La jefatura de Tecnología pondrá a disposición el Plan de Continuidad de Negocio en formato digital, medios tales como: computadores y/o servidores documentales, garantizando el acceso solo al personal pertinente y con autorización.

1.2.3. EJECUTAR PROCEDIMIENTOS DE RECUPERACIÓN Y RESTAURACIÓN DE LA COAC "CRECER WIÑARI" LTDA.

Descripción: Una vez el servicio se encuentre restablecido bajo los procedimientos de continuidad de negocio, los integrantes del Comité de acuerdo con el tipo de evento y los daños ocurridos a la infraestructura principal, se iniciarán las acciones en coordinación con el personal responsable de las áreas afectadas para restaurar y/o recuperar las instalaciones, sistemas informáticos y procesos principales hasta lograr la operatividad normal.

Los responsables de la ejecución los procedimientos informarán al Comité cuando se realicen las actividades previstas en los documentos para que los servicios se encuentren restaurados.

Una vez los servicios se encuentren reestablecidos con procesos y sistemas informáticos principales, el Comité confirmará y declarará el fin de la Continuidad de Negocio a todos los responsables de la ejecución del Plan.

Consideraciones Generales:

- El Comité de Continuidad de Negocio conjunto con el área de Riesgos y por los medios disponibles informará la activación de los procedimientos de restauración y recuperación en orden de aplicación y con sus respectivos responsables para ponerlo en ejecución.

- El comité mantendrá una reunión para calificar los resultados, en un plazo menor a 4 días laborables una vez declarado el fin de la continuidad de negocio.

PROCEDIMIENTOS DIRECCIÓN DE INFORMÁTICA Y COMUNICACIONES

Tabla 12. Incendio

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento de Incendio dentro DATA CENTER

En caso de presentarse una alarma de Incendio dentro del Data Center se considera que debido a la estructura de éste el incendio no puede extender fuera del Data Center y por tal motivo se debe seguir el procedimiento siguiente:

a) Poner en aviso al jefe de Tecnología y/o jefe de Seguridades.

b) Dar seguimiento a la activación automática del sistema de extinción de incendios, mediante los sistemas de monitoreo, en caso de no ser activados automáticamente se lo debe realizar de forma manual utilizando mecanismos manuales en los puntos estratégicos.

c) Verificar que el incendio se encuentre extinguido completamente mediante los sistemas de monitoreo.

d) Ejecutar los procedimientos de Apagado de Servidores con posible afectación.

e) Cortar el suministro de energía.

Procedimiento de Reanudación de Incendio dentro DATA CENTER

a) Solicitar al proveedor del o los enlaces de contingencia, enrute todo el tráfico de datos hacia el Sitio Alterno.

b) Levantar el Sitio Alterno como producción.

c) Analizar y desarrollar un diagnóstico del sistema eléctrico del Data Center (Cableado, fuentes de energía, conexiones) para poder detectar las causas del incendio.

d) Generar un diagnóstico del sistema eléctrico del Data Center (Cableado, fuentes de energía, conexiones) para detectar la causa del incendio.

e) Realizar el cambio de las partes o equipos afectadas.

f) Diagnosticar todos los equipos y determinar si el incendio causo alguna afectación a los mismos para restablecer el suministro de energía.

g) Si algún equipo necesita ser parcial o totalmente cambiado, contactar con los proveedores para solicitar el soporte respectivo.

h) Gestionar los procesos de cobro del seguro para solventar costos relacionados con el evento sucedido.

Tabla 13. Erupción Volcánica

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento en caso de alarma por falla de aire acondicionado principal

a) Verificarla funcionalidad de encendido automático del Aire Acondicionado de Contingencia.

b) Activar manualmente el Aire Acondicionado en caso de falla en el encendido automático.

c) Si el encendido manual presenta fallas, se procederá a encender el aire secundario.

d) Verificar que las ranuras de ventilación no posean rastros de cenizas obstruyéndolos.

e) Solicitar soporte técnico con el proveedor a cargo en caso de ser necesario.

Procedimiento en caso de alarma por falla de aire acondicionado principal y secundario

a) Solicitar soporte técnico inmediato y en sitio con el proveedor que se encuentre a cargo.

b) Comunicarse con el proveedor responsable y solicitar soporte técnico en sitio.

c) Solicitar el diagnóstico y solución al problema del Aire acondicionado.

d) Si el proceso de apagado tarda más de 20 minutos, cambiar al aire acondicionado de emergencia y realizar el apagado de los equipos no críticos.

e) Si la temperatura del Data Center supera los 30° C proceder con el apagado de los servidores, para evitar el daño de estos.

Procedimiento de reactivación en caso de apagado de equipos por falla de aire acondicionado

a) Solicitar al proveedor de los enlaces de contingencia que enrute el tráfico hacia el sitio alterno.

b) Activar el sitio alterno.

c) Cuando el proveedor haya reparado al menos un aire acondicionado, proceder a encenderlo.

d) Esperar que la temperatura disminuya y se obtenga la temperatura adecuada.

e) Encender todos los equipos.

f) Una vez verificado que los sistemas funcionen correctamente se procederá a activar el Data Center Principal.

g) Devolver a estado pasivo el aire acondicionado de contingencia.

Tabla 14. Terremoto

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento de Terremoto

a) Dar aviso al jefe de Tecnología y/o jefe de Seguridades.

b) Si el personal responsable no corre ningún tipo de peligro, comenzar el procedimiento de apagado de Servidores en sitio.

c) Cortar el suministro de energía.

Procedimiento de Reanudación de Terremoto

a) Solicitar al proveedor de los enlaces de contingencia que enrute el tráfico hacia el sitio alterno.

b) Activar el sitio alterno.

c) Identificar la oficina más cercana a la matriz y solicitar la autorización a gerencia del traslado del personal operativo y reanudar las actividades de los procesos en eventos críticos.

d) En caso de ser seguro el ingreso, verificar las instalaciones eléctricas que alimentan al Data Center.

e) Diagnosticar todos los equipos y verificar si el evento causo algún daño a los mismos.

f) En caso de que algún equipo necesite ser parcial o totalmente cambiado, contactar con los proveedores responsables para solicitar este soporte.

g) Una vez verificado que los sistemas funcionen correctamente, proceder con la activación del Data Center Principal.

h) Gestionar los procesos de cobro del seguro para solventar costos relacionados con el evento sucedido.

Tabla 15. Corte de Suministro Eléctrico

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento falla de energía de la red Pública

a) Dar aviso al jefe de Tecnología y/o jefe de Seguridades.

b) Verificar la automatización de encendido del generador de energía del edificio, en caso de no encenderse, realizarlo de manera manual.

c) Validad la transferencia de energía automática, de no iniciarse, iniciar la transferencia manual ubicado en la parte superior del edificio.

d) Verificar el nivel de combustible cuando el corte supere las 3 horas de duración, si es necesario cargar combustible, iniciar el proceso de carga de combustible.

Procedimiento por Falla de energía de Red Pública y Generador

a) Dar aviso al jefe de Tecnología y/o jefe Seguridades Físicas, proceder al apagado de los equipos y servidores no críticos.

b) En caso de no restaurar el suministro de energía en 20 minutos iniciar el procedimiento de apagado de los servidores.

Procedimiento de Reanudación de falla de energía de la red Pública y Generador

a) Solicitar al proveedor de los enlaces de contingencia que enrute el tráfico hacia el sitio alterno.

b) Activar el Sitio Alterno.

c) Al restaurarse el suministro de energía de la red pública, realizar el encendido de los UPS.

d) Proceder con el encendido de servidores y equipos.

e) Verificar que todos los servicios se levanten correctamente.

f) En caso de que algún equipo necesite ser parcial o totalmente cambiado, contactar con los proveedores responsables para solicitar este soporte.

g) Una vez verificado el funcionamiento adecuado activar el Data Center Principal.

h) Gestionar los procesos de cobro del seguro para solventar costos relacionados con el evento sucedido.

Tabla 16. Falla Servicio de Comunicación

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento en caso de falla de Firewall

a) Dar aviso al jefe de Tecnología y/o jefe de Seguridades

b) Solicitar al proveedor de los enlaces de contingencia que enrute el tráfico hacia el sitio alterno.

c) Activar el sitio alterno.

d) Solicitar soporte de manera inmediata al proveedor responsable.

Procedimiento de Reanudación en caso de falla de Firewall

a) Una vez instalado el nuevo equipo, cargar las configuraciones y reglas respaldadas.
b) Verificar con pruebas la conectividad correspondiente con las redes de los proveedores.
c) Solicitar al proveedor de los enlaces, que se enrute nuevamente el tráfico al sitio Matriz.

Procedimiento en caso de falla de enlace de comunicación principal en agencias

a) Contactar al proveedor de enlaces de Datos solicitando un informe de los eventos y tiempos de solución.

b) Validar que se ejecute correctamente la conmutación automática al enlace alterno, en caso de no realizarse, contactarse con la oficina y darles guía para proceder con desconexión física del enlace principal.

c) Informar y solicitar al departamento de Seguridades físicas se apague todo monitoreo de cámaras y utilice el enlace de contingencia evitando consumo innecesario y utilizar netamente en transaccionalidad.

Procedimiento en caso de falla del enlace de comunicación con el edificio Matriz

a) Contactar al proveedor de enlaces de Datos solicitando un informe de los eventos y tiempos de solución.

b) Solicitar al proveedor de los enlaces de contingencia que enrute el tráfico de datos hacia el Sitio Alterno.

c) Activar el Sitio alterno

DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACION

Tabla 17. Procedimientos en caso de falla de Base de Datos de Producción

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento en caso de falla total del servidor de Base de Datos

a) Dar aviso al jefe de Tecnología y/o jefe de Seguridades físicas.

b) Contactarse con el proveedor responsable para habilitar del servidor de contingencia ubicado en el Sitio Alterno.

c) Enrutar la comunicación de la base de datos principal hacia el servidor de contingencia.

d) Contactar al proveedor en caso de necesitar soporte técnico.

Procedimiento en caso de falla de la data de la base de datos Producción

a) Dar aviso al jefe de Tecnología y/o jefe de Seguridades físicas.

b) Recuperar la información almacenada en los discos externos o en la base de contingencia de acuerdo con las políticas de respaldo del Departamento de Sistemas, proceder con la toma de los respaldos de la bóveda de matriz.

c) En caso de no poder recuperar la información de la Base de Datos, habilitar el servidor de contingencia del Sitio Alterno.

d) Enrutar la comunicación de la base de datos principal hacia el servidor de contingencia.

e) Contactar al proveedor para obtener soporte técnico en caso de ser necesario.

Tabla 18. Procedimiento en caso de falla de la Base de Datos de Desarrollo

Responsable Directo:	**Otros responsables:**
Jefe de Seguridades	Administrador de Sistemas - Operador de turno.

Elaborado por: Henry Ricardo Ortega Castro

a) Dar aviso al jefe de Tecnología.
f) Recuperar la información almacenada en los discos o en la base de contingencia de acuerdo con las políticas de respaldo del Departamento de Sistemas, proceder con la toma de los respaldos de la bóveda de matriz.

b) En caso de no poder recuperar la información de la Base de Datos, solicitar al proveedor del servidor de base de datos el activar un servidor temporal y proceder a migrar y actualizar la base de pruebas o desarrollo.
c) Notificar al personal operativos de la institución la indisponibilidad/disponibilidad de la base de datos actual.

Tabla 19. Procedimiento de Reanudación en caso de falla de Base de Datos

Responsable Directo:	**Otros responsables:**
Jefe de Tecnología	Administrador de Base de Datos Técnicos de SoftwareHouse

Elaborado por: Henry Ricardo Ortega Castro

Procedimiento de Reanudación en caso de falla total del servidor

a) Verificar que la conectividad de la base de datos funcione de forma adecuada.
b) Solventado el problema iniciar el levantamiento de la base de datos principal.

Procedimiento de Reanudación en caso de falla de la data de la base de datos desarrollo o producción.

a) Generar el respaldo de la Base de Datos de Contingencia.
b) Cargar la data en la base de Datos de Producción o Desarrollo.
c) Activar el funcionamiento de la base de Datos principal.

1.3. PLAN DE PRUEBAS COAC CRECER WIÑARI LTDA.

1.3.1. Planificar Pruebas

Descripción: Para desarrollar el plan de pruebas, previamente analizado por la responsable de Riesgo Operativo acerca de las fases descritas en el mismo para realizar el levantamiento de información, se procede a evaluar la situación actual y analizar el impacto al negocio (B.I.A) para el Plan de Continuidad de Negocio con los responsables de las áreas que intervienen.

El Análisis de Riesgo Operativo, la planificación de pruebas acorde a los servicios críticos analizados en el BIA, generan el Plan de Pruebas, mismo que permite la ejecución de procesos de forma organizada y controlada, para poder identificar los mejores procedimientos, necesidades de capacitación, fechas y tiempos de ejecución, mismos que serán presentados en el primer Comité de Continuidad de Negocio del año.

Las distintas pruebas previstas para ejecución se detallan a continuación:

1.3.1.1. **Pruebas de los Procedimientos de Continuidad de Negocio:** La planificación de estas pruebas son responsabilidad del Área de Riesgos y deben considerar la activación de los procesos y validar la efectividad para la recuperación de los servicios afectados.

1.3.1.2. **Pruebas de los Procedimientos de Continuidad y Restauración:** La planificación de estas pruebas está a cargo del Área de Operaciones y Tecnología, se debe verificar la efectividad de los procesos, la integridad de los sistemas, la infraestructura tecnológica que se encuentra asignada para los eventos de contingencia.

1.3.1.3. **Pruebas de los procedimientos de apoyo:** La planificación de estas pruebas está a cargo de uno varios delegados del Comité de Continuidad de Negocio, estos son designados en el último Comité del año, los procesos pueden validarse de forma conceptual o practica según sea el caso.

Consideraciones Generales:

1.3.1.4 . La planificación de las pruebas se realiza a inicios de cada año.

1.3.1.5. Se debe considerar los proveedores, procesos, personal crítico y aplicaciones tecnológicas relacionadas con los servicios resultantes del análisis BIA.

1.3.1.6. Las pruebas de los procesos de continuidad y recuperación, procesos de continuidad y restauración deben realizarse con un mínimo de 3 veces al año, mientras las pruebas de procesos de apoyo deben realizarse al menos 1 vez al año.

1.3.1.7. Anualmente se deberá realizar al menos 1 prueba total y 2 pruebas parciales.

1.3.1.8. En caso de existir modificaciones a los procesos principales o a la infraestructura tecnológica la cual afecte a un servicio crítico, estos deben ser actualizados en los procesos del Plan de Continuidad de Negocio y generar al menos una prueba parcial y una total anual.

1.3.2. Revisar y Aprobar Plan de Pruebas

Descripción: El comité de Continuidad de Negocio debe revisar y aprobar o solicitar modificaciones según las sugerencias de sus integrantes, el Plan de pruebas explica las actividades con sus responsables, fechas y horarios estimados para la aplicación de las pruebas y en caso de eventualidades se realizará en tiempos adicionales.

Consideraciones Generales:

1.3.2.1. El responsable de ejecutar las pruebas debe evaluar el impacto que puede generar a las normas de operaciones de la Cooperativa y se procederá en horarios

donde la afectación sea en lo mínimo posible y permita el total restablecimiento de gestión normal de la Cooperativa

1.3.2.2. El responsable de la ejecución de las pruebas, previa la ejecución de las pruebas evaluará el impacto que podrá ocasionar a las normales operaciones de la Cooperativa y se procederá en horarios que la afectación sea la menor posible y que garantice el total restablecimiento de la gestión normal de la Cooperativa.

1.3.2.3. El responsable de la ejecución de las pruebas debe notificar al personal involucrado con al menos 5 días de anticipación

1.3.2.4. El responsable de la ejecución de las pruebas, para la aplicación de las pruebas se notificará al personal involucrado con un mínimo de 5 días de anticipación.

1.3.3 Ejecutar y evaluar pruebas

Descripción: El área de Riesgo debe convocar al personal involucrado (interno o externo) identificando fecha y una nómina del personal convocado para la ejecución de pruebas con el fin de validar la asistencia y participación. Durante la ejecución de estas pruebas se aplican las actividades descritas en los procedimientos del Plan de Continuidad de Negocio, al finalizar las pruebas, el personal involucrado debe registrar los resultados y entregárselos al área de Riesgo.

El jefe de Riesgo debe generar un informe y presentarlo en el Comité de Continuidad de Negocio para su revisión, cualquier observación por el comité a las pruebas realizadas serán registradas para el respectivo seguimiento y solución. El Comité de Continuidad de Negocio al concluir las pruebas si estas son o no satisfactorias generaran una evaluación y análisis el mismo que se registrara en un acta del comité para poner en conocimiento al Consejo de Administración.

En caso de que las pruebas no cumplan con las expectativas, el jefe de Riesgo realizará los ajustes necesarios a los procesos o planificaciones para repetir las pruebas hasta lograr el objetivo deseado, considerando como prioridad los tiempos de ejecución para el restablecimiento del servicio.

Consideraciones Generales:

- El Comité de Continuidad de Negocio tendrá la protestad de solicitar la realización de pruebas adicionales pertinentes a las detalladas en el Plan de Pruebas ya sean totales y/o parciales.

- El Comité de Continuidad de Negocio debe ser comunicado con al menos 15 días de anticipación que se realizarán las pruebas, con la finalidad de poder aplazar las mismas en caso de surgir alguna eventualidad imprevista o actividad interna de la Cooperativa la cual pueda afectar el normal desarrollo de las pruebas o del negocio, en caso de ser solicitado, este aplazamiento no podrá ser mayor a 15 días.

- La presentación de informes de resultados correspondientes a las pruebas será presentada en un máximo de 20 días tras culminar las mismas, donde ya se incluirán las mejoras identificadas y los plazos de implementación.

- En caso de ser pruebas insatisfactorias, estas deben repetirse una vez identificadas las mejoras a los procesos para garantizar el éxito de la prueba.

1.3.4. Análisis de resultados de pruebas

El análisis de la inesperada incidencia de una amenaza se realiza de acuerdo con la severidad y afectación de la continuidad de negocio en la COAC "Crecer Wiñari" Ltda., los cuales son:

- Terremoto
- Incendio
- Acceso no autorizado
- Denegación de servicio
- Degradación de los soportes de almacenamiento de la información
- Fallos de servicio de Comunicación

- Corte de Suministro Eléctrico
- Caída del sistema por agotamiento de recursos

Se escogieron escenarios fijos de desarrollo para la evaluación de pruebas de Continuidad de Negocio, con el objetivo de medir su impacto en la institución. Al ejecutar el análisis en la COAC "Crecer Wiñari" Ltda., se identificó los escenarios con mayor probabilidad de ocurrencia e impacto en el negocio, siendo los siguientes: Fallo de servicio de comunicaciones y Caída del sistema por agotamiento de recursos. Los escenarios mencionados anteriormente provocan la interrupción de los servicios y la continuidad de negocio ofrecidos por la COAC "Crecer Wiñari" Ltda., los mismos que se encuentran detallados de acuerdo con su importancia.

Para estos casos se establece el **MTPD** (Periodo Máximo Tolerable de Interrupción), definidos por el análisis BIA en donde se concretan los tiempos en el cual la institución puede permanecer sin ofrecer los servicios que maneje al Área de Tecnología de la COAC "Crecer Wiñari Ltda." sin verse amenazado financieramente o perder su reputación, es de 3 horas para la recuperación de los enlaces de comunicación, por lo que se debe realizar los procedimientos de continuidad y reanudación descritos anteriormente en el **RTO** (Tiempo objetivo de recuperación).

1.3.4.1. Análisis del primer caso de prueba: Fallos de servicio de comunicación

Hipótesis: COAC "Crecer Wiñari Ltda." se queda sin enlaces de comunicación en el edificio matriz.

El tiempo estimado de recuperación objetivo para estas actividades de reanudación de los encales de comunicación es de 30 minutos a 3 horas, al revisar los valores obtenidos del ejercicio de prueba se invirtieron los siguientes tiempos:

Tabla 20. Caso de Prueba 1

ÁREA DEL NEGOCIO	ACTIVIDADES	SERVICIOS O APLICACIONES CRITICAS	TIEMPO INVERTIDO
Gestión de Tecnología de la Información	Comunicación	Internet	10 minutos
	Procesos de continuidad y reanudación		25 minutos
	Vuelta a la normalidad		15 minutos

Elaborado por: Henry Ricardo Ortega Castro

Se ha invertido un tiempo de 10 minutos asignado para la etapa de Comunicación al Comité de Continuidad, 20 minutos para ejecutar los procedimientos de continuidad de negocio y reactivación, se detalla la revisión y el contacto con a proveedor para dar la solución del problema y 15 minutos estabilizando los enlaces dando un total de 50 minutos.

Los tiempos demuestran que los procedimientos de continuidad y reactivación se alinean a los tiempos definidos por la COAC "Crecer Wiñari Ltda." demostrando una correcta practica de las actividades para la solución del caso propuesto como incidente.

1.3.5. Análisis del segundo caso de prueba: Caída del sistema por agotamiento de recursos

Hipótesis: COAC "Crecer Wiñari Ltda." queda sin Core Financiero en el edificio Matriz.

El tiempo de recuperación objetivo para realizar las actividades de reanudación del sistema es de 30 minutos a 2 horas, al revisar los valores obtenidos de la prueba, se invirtieron los tiempos siguientes:

Tabla 21. Caso de Prueba 2

AREA DEL NEGOCIO	ACTIVIDADES	SERVICIOS O APLICACIONES CRITICAS	TIEMPO INVERTIDO
Gestión de Tecnología de la Información	Comunicación	Core Financiero	10 minutos
	Procesos de continuidad y reanudación		50 minutos
	Vuelta a la normalidad		15 minutos

Elaborado por: Henry Ricardo Ortega Castro

Se invirtió 10 minutos en la etapa de Comunicación al Comité de Continuidad, para ejecutar los procedimientos de continuidad de negocio y reactivación se invirtió 50 minutos en el cual se detalla la revisión y contacto con el proveedor para la solución del problema y 15 minutos estabilizando los enlaces, lo que da un total de 1 hora 15 minutos.

Los tiempos demuestran que los procedimientos de continuidad y reactivación se alinean en los tiempos definidos por COAC “Crecer Wiñari Ltda.” lo que refleja una correcta practica de las actividades de continuidad para la solución del caso propuesto como incidente.

Conclusiones y Recomendaciones del Manual de Continuidad de Negocio

Al terminar el análisis de la situación actual, el análisis de Riesgo y la elaboración del Plan de Continuidad de Negocio, la definición de procesos, continuidad y reactivación, la ejecución de pruebas de los principales escenarios de riesgo de la COAC "Crecer Wiñari Ltda.", se ha concluido lo siguiente:

Conclusiones

1. La metodología utilizada para el análisis de riesgo ha sido ajustada para la realidad económica de la institución, orientada a la perdida financiera soportable por la misma y alineada a las necesidades normativas e institucionales que proporcionan beneficios para la protección de información e infraestructura.

2. El impacto en el Negocio BIA es la base principal para el desarrollo de estos estudios por lo que su realización es de suma importancia para su correcta implementación en el Plan de Continuidad de Negocio.

3. El éxito del Plan de Continuidad de Negocio depende del compromiso de la Alta Gerencia y la colaboración de los funcionarios involucrados directamente con la continuidad.

4. Las instituciones financieras deben garantizar la continuidad de los servicios críticos que ofrecen a sus clientes, los servicios inactivos proporcionan impacto y pérdidas económicas, legales y de imagen que sufren al no poder realizar sus actividades normalmente.

5. La evaluación y mejora continua es de suma importancia con el fin de obtener un nivel de madurez para satisfacer las necesidades normativas e institucionales de la Cooperativa.

Recomendaciones

1. El área de riesgos debe definir una metodología de análisis, alineada principalmente a la pérdida económica soportable por la Cooperativa con sus riesgos particulares con la finalidad de no mal gastar esfuerzos en una

nueva personalización.

2. Se necesita actualizar permanentemente el Análisis de impacto en el Negocio BIA, basado en los cambios organizacionales respecto a amenazas y vulnerabilidades que puedan suceder.

3. Sostener el interés y compromiso de la Alta Gerencia con la Continuidad del Negocio a fin de tener facilidades para simulacros, análisis y capacitaciones que involucren al personal de la Institución y así poder generar una cultura de Riesgo y continuidad.

4. Los sucesos no controlados que involucren a los servicios que no sean administrados por la COAC “Crecer Wiñari” Ltda., deben ser comunicados directamente con los proveedores y buscar la estrategia que mejor se adapte a dar una solución garantizada y en el menor tiempo posible.

5. El área de tecnología debe realizar revisiones del plan de continuidad de negocio al menos 2 veces al año y evaluar la vigencia de los simulacros y pruebas con el personal responsable con la finalidad de reforzar y retroalimentar los conocimientos aprendidos.

3.3. Verificación de hipótesis

La validación de las respuestas recolectadas en la encuesta aplicada a la COAC "Crecer Wiñari" Ltda., se llevará a cabo mediante el uso del análisis estadístico denominado Chi-cuadrado (X^2), la cual consiste en una prueba a la hipótesis para comparar la distribución observada con los datos de la distribución que se espera.

Hipótesis Nula (Ho): La implementación de un manual de continuidad de negocio no mejora los servicios de las instituciones financieras del segmento 3 reguladas por la superintendencia de economía popular y solidaria

Hipótesis Alternativa (Hi): La implementación de un manual de continuidad de negocio si mejora los servicios de las instituciones financieras del segmento 3 reguladas por la superintendencia de economía popular y solidaria.

Se pretende identificar y establecer los resultados en la hipótesis, por lo cual se procederá a tomar las dos variables del problema y seleccionar una pregunta por cada una para establecer una tabla de datos observados.

Distribución Observada

- Variable Independiente:

Manual de Continuidad de Negocios en la pregunta 10

¿Se debe capacitar al personal nuevo y vigente sobre los procedimientos actualizados frente a un evento crítico?

- Variable Dependiente:

Instituciones Financieras en la pregunta 2

¿La cooperativa posee un instructivo vigente que haga referencia a los procedimientos a seguir frente eventos críticos de Coordinación de Tecnología e Innovación de la Cooperativa?

Tabla 22. Frecuencias Observadas

Alternativas	Preguntas		TOTAL
	2	10	
Totalmente de acuerdo	25	37	62
Ni de acuerdo ni en desacuerdo	14	6	20
Totalmente en desacuerdo	4	0	4
TOTAL	43	43	**86**

Elaborado por: Henry Ricardo Ortega Castro

Los valores presentados en la tabla #22 permiten calcular la distribución esperada.

Tabla 23. Frecuencias Esperadas

Alternativas	Preguntas		TOTAL
	2	10	
Totalmente de acuerdo	31	31	62
Ni de acuerdo ni en desacuerdo	10	10	20
Totalmente en desacuerdo	2	2	4
TOTAL	43	43	**86**

Elaborado por: Henry Ricardo Ortega Castro

Con los datos de las tablas de distribución observada y esperada se calcula la matriz para hallar el valor de Chi-Cuadrado.

Tabla 24. Cálculo del Chi Cuadrado

DISTRIBUCIÓN		O - E	$(O - E)^2$	$(O - E)^2/E$
Observada (O)	Esperada (E)			
25	31	-6	36	1,16
14	10	4	16	1,60
4	2	2	4	2,00
37	31	6	36	1,16
6	10	-4	16	1,60
0	2	-2	4	2,00
CHI-CUADRADO X^2				**9,52**

Elaborado por: Henry Ricardo Ortega Castro

Se establece un grado de libertad (v) que se relacionará con el chi cuadrado y el valor de la región de rechazo de la hipótesis donde se asumirá $\alpha=0,05$.

v = (#filas-1) (#columnas-1)

v = (3-1) (2-1)

v = 2

Con los datos calculados y encontrados se procede a seleccionar el valor de chi cuadrado tabular en la siguiente tabla:

g.d.l	0,001	0,005	0,01	0,02	0,025	0,03	0,04	0,05
1	10,828	7,879	6,635	5,412	5,024	4,709	4,218	3,841
2	13,816	10,597	9,210	7,824	7,378	7,013	6,438	5,991
3	16,266	12,838	11,345	9,837	9,348	8,947	8,311	7,815
4	18,467	14,860	13,277	11,668	11,143	10,712	10,026	9,488
5	20,515	16,750	15,086	13,388	12,833	12,375	11,644	11,070
6	22,458	18,548	16,812	15,033	14,449	13,968	13,198	12,592
7	24,322	20,278	18,475	16,622	16,013	15,509	14,703	14,067
8	26,124	21,955	20,090	18,168	17,535	17,010	16,171	15,507
9	27,877	23,589	21,666	19,679	19,023	18,480	17,608	16,919
10	29,588	25,188	23,209	21,161	20,483	19,922	19,021	18,307
11	31,264	26,757	24,725	22,618	21,920	21,342	20,412	19,675
12	32,909	28,300	26,217	24,054	23,337	22,742	21,785	21,026
13	34,528	29,819	27,688	25,472	24,736	24,125	23,142	22,362
14	36,123	31,319	29,141	26,873	26,119	25,493	24,485	23,685
15	37,697	32,801	30,578	28,259	27,488	26,848	25,816	24,996

Figura 20. Tabla de Distribución Chi Cuadrado
Fuente: Martínez Ciro, 2012

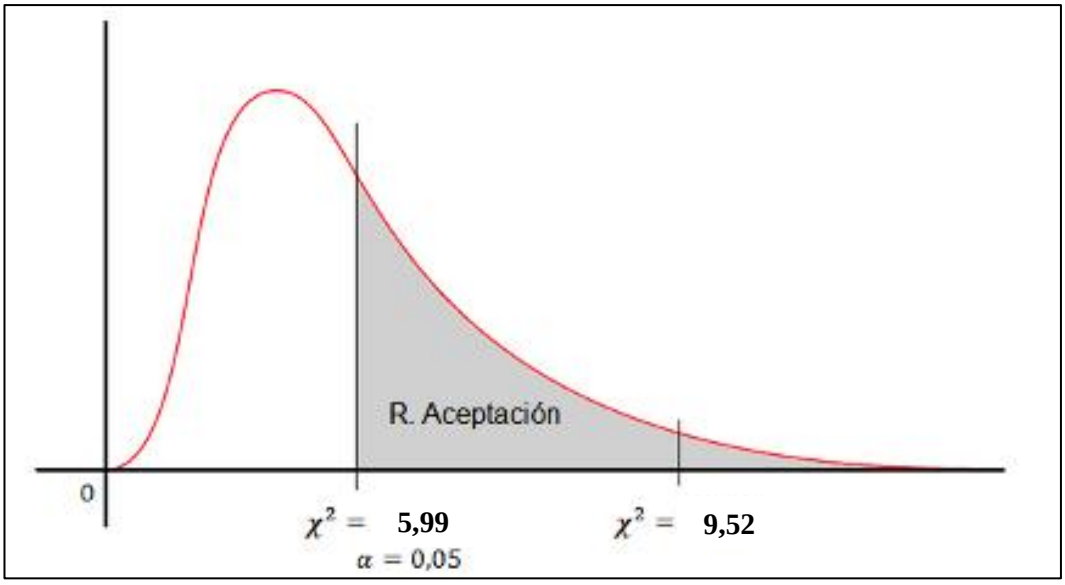

Figura 21. Distribución Chi Cuadrado
Fuente: Martínez Ciro, 2012

$$Chi\ Cuadrado\ Calculado > Chi\ Cuadrado\ Tabulado$$

$$9{,}52 > 5{,}99 \qquad OK$$

Decisión

Se comprueba que el Chi Cuadrado Calculado no es menor que el Tabulado, por lo que se rechaza la Hipótesis Nula **(Ho)** y se acepta la Hipótesis Alternativa **(Hi)**. La implementación de un manual de continuidad de negocio si mejora los servicios de las instituciones financieras del segmento 3 reguladas por la superintendencia de economía popular y solidaria.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Las interrupciones de operación de los principales servidores y redes de comunicación en las instituciones financieras se ocasionan por la falta de un manual de continuidad de negocio que permita evaluar y seleccionar la estrategia adecuada para enfrentar los eventos críticos que se presenten, y de esa forma habilitar los servicios afectados en un corto tiempo.

Los procedimientos de recuperación ante la interrupción de la operación en servidores y redes de comunicaciones principales se elaboran mediante los registros que hayan recolectado en eventos críticos pasados, permitiendo la corrección e implementación de nuevos aspectos que refuercen las estrategias seleccionadas para cada departamento de la institución financiera.

La continuidad de negocio se llevará acabo con las estrategias establecidas para priorizar la viabilidad del servicio y restablecimiento de operaciones informáticas. El departamento TIC de la institución tiene la responsabilidad de coordinar con los demás departamentos adecuado manejo de los tiempos de caída de sus servidores para garantizar un óptimo servicio a sus clientes y de igual manera reducir el impacto y las pérdidas que estos eventos provoquen a cada dependencia.

Los distintos departamentos de las instituciones financieras requieren planificar y ejecutar simulacros periódicamente para recolectar información frente a una posible caída de los principales sistemas informáticos y financieros que administra cada departamento.

El personal de la institución financiera no desarrolla de manera eficiente el monitoreo del comportamiento adecuado de los sistemas de información y de la infraestructura tecnológica prevenir y localizar de manera temprana una posible interrupción o caída de los sistemas de información.

4.2. Recomendaciones

Es necesario la implementación de un manual de continuidad de negocio donde se establezcan medidas a seguir frente a la caída de servidores informáticos, para que sus colaboradores tengan la información necesaria de las acciones requeridas durante y después del incidente.

Los directores de cada departamento deben ordenar y archivar los documentos necesarios que respalden la información en caso de que los servidores se vean altamente afectados y en el peor de los casos sufran una pérdida total de información.

El manual de continuidad de negocio de la institución debe seguir los lineamientos que dictan las normativas nacionales e internacionales sobre el manejo de los servicios informáticos y financieros de las instituciones del segmento 3.

El personal cooperativo debe identificar y elaborar un documento sobre las debilidades y amenazas que comprometan los servicios y la infraestructura del departamento TIC, con el fin de gestionar los recursos necesarios para un correcto manejo de las acciones que reduzcan impactos negativos en la institución.

REFERENCIAS BIBLIOGRÁFICAS

[1] A. López, «ISO27000,» 01 Octubre 2005. [En línea]. Available: https://www.iso27000.es/iso27002.html. [Último acceso: 15 Junio 2021].

[2] J. Martínez, «El Plan de Continuidad de Negocio,» Díaz Santos, España, 2006.

[3] Oficina de Sistemas e Informática-OSI, «Escuela Superior de Administración Pública,» 01 Junio 2018. [En línea]. Available: http://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf. [Último acceso: 15 Junio 2021].

[4] Secretaria de Gestión de Riesgos, *C.O.E. Nacional*, vol. 2, pp. 1-17, 2016.

[5] Mango, «Memorias de sostenibilidad,» 2016.

[6] SEPS, «CIRCULAR SEPS IR DNSES 2016 06791 PLANES DE CONTINGENCIA,» Quito, 2016.

[7] Instituto Nacional de Ciberseguridad, «Plan de Contigencia y Continuidad de Negocio,» Protege tu Empresa, España, 2019.

[8] A. Cárdenas, Desarrollo del plan de continuidad del negocio para la empresa EQUIVIDA S.A para el período 2012-2015, Sangolquí, 2013.

[9] N. Angulo, J. Cárdenas y F. Bolaños, «La continuidad de negocio en las instituciones de educación superior del Ecuador. Caso de estudio,» *Revista Científica Multidisciplinaria Arbitrada YACHASUN*, vol. 4, nº 7, p. 36, 2020.

[10] M. Gallardo y P. Jácome, «Análisis de riesgos informáticos y elaboración de un plan de contingencia T.I. para la empresa eléctrica Quito S.A.,» Escuela Politécnica Nacional, Quito, 2011.

[11] F. Motta y R. Gineth, Importancia de la planeación de la continuidad del negocio en las empresas radicadas en la ciudad de Bogotá, Bogotá, 2012.

[12] J. De León, Introducción al análisis de riesgos, Limusa, 2007.

[13] D. Aguirre y S. Andrago, «Preferencias en el uso de productos y servicios financieros que ofrecen las instituciones del Sistema Financiero Regulado ecuatoriano,» Quito, 2011.

[14] J. Heras, Diccionario de mercados financieros, Madrid: Deusto, 2000.

[15] Banco de México, «Instituciones Financieras,» 2010. [En línea]. Available: http://www.banxico.org.mx/sistema-financiero/materialeducativo/basico/fichas/estructura-del-sistema-financiero/%7BA7DF9134-AA14-. [Último acceso: 06 Julio 2021].

[16] S. Ayala, Análisis Financiero, 2005.

[17] Superintendencia de Bancos, «Comportamiento del cédito de consumo del sistema financiero nacional,» 2019. [En línea]. Available: http://estadisticas.superbancos.gob.ec/portalestadistico/portalestudios/wpcontent/uploads/sites/4/downloads/2020/01/comportamiento_credito_consumo_sept_19.pdf/. [Último acceso: 07 Julio 2021].

[18] Constitución de la República del Ecuador, «Economía,» de *Sistema Financiero*, Montecristi, Asamblea Nacional, 2008.

[19] Superintendencia de Economía Popular y Solidaria, «Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario,» Ecuador, 2017.

[20] E. Coba y J. Díaz, «El crédito de desarrollo humano asociativo en la economía social y solidaria de la provincia de TungurahuaEcuador,» *Analítica*, pp. 33-47, 2014.

[21] Ministerio de Inclusión Económica y Social, « Hacia una caracterización de la Economía Popular y Solidaria en el Ecuador,» Quito, 2014.

[22] Secretaría Nacional de Planificación y Desarrollo, «SENPLADES,» 2013. [En línea]. Available:

http://documentos.senplades.gob.ec/Plan%20Nacional%20Buen%20Vivir%202013-2017.pdf. [Último acceso: 09 Julio 2021].

[23] La Hora Loja, «El rol de la Superintendencia de Economía Popular y Solidaria,» *La Hora,* 07 Julio 2019.

[24] A. Castro, Economía popular y solidaria ¿realidad o utopía?, Quito: Universitaria Abya-Yala, 2018.