UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE LA INFORMACIÓN

DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA.

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULODE INGENIERO DE SISTEMAS DE INFORMACIÓN

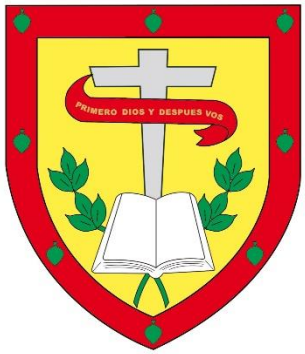
AUTOR: ANGÉLICA MARÍA LOJA MAYANCELA

DIRECTOR: ING. CRISTHIAN FLORES URGILES. MGS

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE LA INFORMACIÓN

DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA.

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULODE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: ANGELICA MARIA LOJA MAYANCELA

DIRECTOR: ING. CRISTHIAN FLORES URGILES. MGS

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Yo Angelica Maria Loja Mayancela portador de la cédula de ciudadanía **Nº 0350164018**. Declaro ser el autor de la obra: **"Diseño De Un Plan De Continuidad De Negocio Para La Cooperativa De Ahorro Y Crédito Achik Inti Ltda"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 8 de agosto de 2023

Angelica Maria Loja Mayancela

C.I: 0350164018

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el/la Est. Angélica María Loja Mayancela bajo mi supervisión.

Ing. Cristhian Flores Urgilés, MSC.

DIRECTOR DELTRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

AGRADECIMIENTO

A Dios por permitir que todas las cosas sean posibles y por las bendiciones recibidas.

A la Universidad Católica de Cuenca Extensión Cañar y en especial a la Facultad de Ingeniería de Sistemas por acogerme y permitir cumplir mis metas.

A todos los catedráticos de la carrera de ingeniería de Sistemas que me guiaron para llegar a la meta deseada que es de ser un profesional y a mi madre que me brindo todo el apoyo necesario en mi vida de estudiante.

DEDICATORIA

A Dios nuestro señor por bendecirme en cada instante de mi vida y con su guía alcanzar una más de mis metas.

A mi madre Angelita Mayancela Mayancela quien fue la que me ayudo a lograr esta meta por su esfuerzo dedicación y apoyo en toda mi vida.

A mis hermanos José, Francisco, Santiago, Luis, Mauricio, Narcisa Loja quienes han sido siempre mi mayor inspiración y el pilar fundamental para lograr esta meta.

RESUMEN

Cada organización, sin importar su campo de acción, está sujeta a enfrentar calamidades o incidentes que pueden perturbar el curso regular de sus operaciones. Para evitar estos problemas es importante establecer planes de continuidad de negocio que permita actuar y reanudar las operaciones empresariales tras incidentes o emergencias. Dentro de este marco, la presente investigación propone la elaboración de un "Plan de Continuidad de Negocio para la Cooperativa de Ahorro y Crédito Achik Inti" con un enfoque técnico y estratégico para asegurar la continuidad operativa y la resiliencia de la organización. El primer y segundo capítulo del estudio se centra en el análisis de la literatura existente sobre la planificación de la continuidad del negocio, las mejores prácticas en la industria de las cooperativas de ahorro y crédito y los estándares internacionales en este campo. En el tercer capítulo se realiza un análisis detallado de la Cooperativa de Ahorro y Crédito Achik Inti Ltda., sus operaciones diarias, su infraestructura, su personal, sus servicios financieros y los riesgos asociados a cada uno. Así como también la selección de la norma ISO 22301 para la elaboración del BCP y la metodología MAGERIT para el análisis y la gestión de riesgos. En el cuarto capítulo de la investigación, se desarrolla el plan de continuidad de negocio propiamente dicho. Esto incluye la identificación de las funciones críticas del negocio, los recursos necesarios para mantenerlas y las estrategias para recuperarlas después de una interrupción.

Palabras clave: Plan de Continuidad de Negocio, Cooperativa de Ahorro y Crédito, Norma ISO 22301 Metodología MAGERIT, BCP.

ABSTRACT

Regardless of its field of operation, every organization is subject to calamities or incidents that could disrupt its normal operations. To avoid these problems, it is crucial to establish business continuity plans that enable it to act and resume business operations after incidents or emergencies. Within this framework, the present investigation proposes an elaboration of a "Business Continuity Plan (BCP) for the Achik Inti Savings and Credit Cooperative" with a technical and strategic approach to ensure the operational continuity and resilience of the organization. The study's first and second chapters analyze the existing literature on business continuity planning, best practices in the credit union industry, and international standards in this field. The third chapter contains a detailed analysis of Savings and Credit Cooperative "Achik Inti Ltda.," its daily operations, infrastructure, staff, financial services, and the risks associated with each aspect. It also includes the selection of the ISO 22301 standard for the preparation of the BCP and the MAGERIT methodology for risk analysis and management. The business continuity plan is developed in the fourth chapter of the investigation. This includes identifying critical business functions, the resources needed to maintain them, and strategies to recover them after an outage.

Keywords: Business Continuity Plan, Savings and Credit Cooperative, ISO 22301 Standard, MAGERIT Methodology, BCP.

Índice

Índice de Tablas

Índice de ilustraciones

Introducción

La cooperativa de Ahorro y Crédito “Achik Inti” se constituye en la ciudad de Cañar en el año 2011, mediante un acuerdo Ministerial Nª 001-DCP-011, está dedicada a brindar servicios a la ciudadanía en el ámbito económico a través de los ahorros y préstamos.

Con el paso de los años la cooperativa ha iniciado un proceso de modernización en sus gestiones, para ello han visto en la necesidad de incrementar nuevos servicios tecnológicos, con el fin de automatizar procesos. El incremento de estas nuevas tecnologías trae consigo un sin número de riesgos, los mismos que pueden afectar los activos más preciados de la institución como lo es la información que administran en la misma.

Dichos activos pueden verse afectados ante fallas en los sistemas de tecnología de la información o eventos naturales y la falta de políticas, normas y procedimiento en la restauración de servicios puede provocar pérdidas de información, pérdidas económicas, y por último pueden perder la credibilidad de los socios.

Ante lo expuesto, es importante que las entidades financieras cuenten con un plan de continuidad de negocio, debido a que permite identificar y mitigar los riesgos que podrían afectar la continuidad del negocio de la cooperativa, así como proporcionar un marco para la recuperación y la gestión de crisis, garantizando de esta manera la seguridad financiera de los miembros y manteniendo la finanza del público en la institución.

La implementación de un BCP sólido ayudará a garantizar que la cooperativa de ahorro y crédito Achik Inti, pueda continuar operando de manera segura y eficiente en cualquier circunstancia adversa.

CAPITULO I

MARCO REFERENCIAL

1.1. PLANTEAMIENTO DEL PROBLEMA

La Cooperativa de Ahorro y Crédito Achik Inti, se constituye en la Ciudad de Cañar, Provincia de Cañar, mediante el acuerdo Ministerial Nº 0001 – DPC – COOP – 011, desde su creación no se ha podido desarrollar un modelo de plan de continuidad de negocio, como herramienta necesaria para la que entidad financiera logre recuperarse en el menor tiempo posible y de forma más eficaz ante un incidente mayor o un evento de indisponibilidad.

En el tiempo que la cooperativa brinda sus servicios a la ciudadanía, ha presentado fallos en los equipos, perdida de servicios, entre otras cuestiones técnicas que ha conllevado a que se termine perdiendo la credibilidad de los socios.

Razón por la cual y con el fin de evitar daños a futuro, el presente proyecto plantea el diseño un modelo de plan de continuidad de negocio que se basa en un manual para mitigar el riesgo en caso de que no exista disponibilidad de los servicios y recursos para el normal funcionamiento de las operaciones. La continuidad de negocio es un punto clave preventivo que contribuye al buen desarrollo y al cumplimiento de las estrategias de la entidad financiera y cualquier otra organización.

1.1.1. FORMULACIÓN DEL PROBLEMA

- ¿Cuál sería el estándar de continuidad de negocio más adecuado para aplicar a la cooperativa?

- ¿El diseño de un plan de continuidad de negocio, en qué medida mejorara la recuperación de los procesos de TI?
- ¿Cómo mejorara la continuidad de negocio de la Cooperativa de Ahorro y Crédito Achik Inti Ltda, al implementar un plan de recuperación en el área de TIC?

1.2. ANTECEDENTES DE LA INVESTIGACIÓN

Las instituciones financieras además de tener la mejor tecnología deben garantizar la seguridad de los datos ante desastres que pudiera paralizar su actividad. Como se puede observar hoy en día la información que manejan las organizaciones es un activo esencial y van de la mano con las tecnologías modernas que también están expuestas a amenazas.

Por todo ello, es conveniente tener elaborado una propuesta de PLAN DE CONTINUIDAD DE NEGOCIO que indique y visualice las pautas de lo que se debe realizar en caso de que haya una falla y se pierda la información. Actualmente la mayoría de las empresas han utilizado un plan de contingencia con el fin de mejorar la calidad del servicio.

Con respecto al tema planteado se han encontrado estudios realizados en distintos lugares algunos de ellos se describen a continuación.

Un estudio realizado por el Ing. Jairo Rojas, titulado PROPUESTA DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA UNA INSTITUCIÓN FINANCIERA DEL SECTOR PRIVADO BANCARIO DEL ECUADOR en donde propone un plan de continuidad de negocios en el cual se identifican las amenazas y riesgos tecnológicos así también la evaluación de los mismos. También se realiza un análisis de los diferentes estándares internacionales como las

normas de calidad. Esta tesis servirá como guía para la estructura de un plan de continuidad de negocio. (Rojas Bustamante, 2017)

El estudio realizado por la Lic. Alba Muñoz, Lic. Eduardo Llanes, titulado ANÁLISIS Y EVALUACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO (BCP) DE LA EMPRESA "IMPULSADORA DE CRÉDITOS, S.A" DURANTE EL PERIODO 2015-2016. En donde se realiza el análisis y evaluación de un plan de continuidad de negocio de la empresa "Impulsadora de créditos, S.A", que tiene como objetivo la determinación de si el BCP de la empresa se ajusta a las mejores prácticas internacionales. (Muñoz & Llanes, 2017)

Por otra parte el estudio de Carolina Malaver (2020), titulado "DISEÑO E IMPLEMETACION DEL PLAN DE CONTINUIDAD DEL NEGOCIO EN BANCOMPARTIR". Establecen estrategias de continuidad del negocio basado en los procesos críticos y en los recursos como personal, aplicativos, costos y tecnologías, todo enfocado a mantener el servicio en caso de un evento de indisponibilidad. (Duarte, 2020)

Luego de haber realizado un análisis de las investigaciones de un BCP es recomendable la utilización de la norma ISO 22301 la cual especifica los requisitos de planificar, establecer, implantar, operar, monitorear y revisar un sistema de gestión de la empresa, así saber cómo actuar en reanudar sus actividades diarias en el caso de que ocurra alguna interrupción.

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

El propósito de esta investigación es dar a conocer las pautas necesarias de lo que se debe realizar ante desastres ya sean estos ocasionados por el hombre, la naturaleza etc. Para ello la

utilización de un Plan de continuidad de negocio ayudara a estar preparados frente a la contingencia con el único propósito de minimizar las pérdidas de la organización.

Al implementar un plan de contingencia la organización tendrá mayor ventaja competitiva frente a otras organizaciones, ya que el hecho de mostrar que se toman las diferentes medidas para garantizar la continuidad del negocio mejora la imagen pública, consigue mayor confianza de los clientes y proveedores. Por otra parte, ayuda también a la gestión preventiva de los riesgos que puede impactar en sus operaciones, así podrá prevenir y minimizar las pérdidas de la organización en caso de que se presente un desastre.

Así también asegura la resiliencia de las actividades de negocio ante interrupciones, mejorando la disponibilidad de los servicios dispuestos al cliente, implementar un plan de continuidad de negocio en una empresa ayuda a estar preparados ante cualquier incidente o problema que afecte los procesos y servicios.

1.4. OBJETIVOS

1.4.1. Objetivo General

Diseñar un Plan de Continuidad de Negocio para la Cooperativa de Ahorro y Crédito Achik Inti Ltda. Utilizando los estándares existentes para garantizar la provisión de los servicios que brinda a sus clientes.

1.4.2. Objetivos Específicos

- Realizar un estudio teórico de las normativas del plan de continuidad de negocio.
- Identificar los riesgos internos que presenta la cooperativa de Ahorro y Crédito Achik Inti Ltda. y que generen interrupciones en el servicio, mediante el análisis del entorno.

- Elaborar el plan de continuidad de negocio para la cooperativa de ahorro y crédito Achik Inti Ltda. Como herramienta preventiva que garantice la continuidad del proceso ante un incidente existente.

1.5. LIMITACIONES

- El tiempo estimado para la culminación del proyecto de investigación será corto y resultará complicado cumplir a tiempo con los objetivos definidos

1.6. DELIMITACIONES

- El presente trabajo se llevará a cabo en el área de TI de la "Cooperativa de Ahorro y Crédito Achik Inti Ltda." Ubicada en el Cantón Cañar.

CAPITULO II

2. MARCO TEÓRICO

2.1. Plan de Continuidad de Negocio

Es un conjunto de prácticas, normas, reglas de conducta y herramientas organizativas que ante eventos imprevistos que interrumpen algunas o todas las áreas del negocio de la organización, le permite restaurar su funcionalidad en el menor tiempo posible para que las pérdidas económicas resultantes sean pequeñas, así como cuidar su reputación y posicionamiento en la región. (Zapata Vásquez, 2020)

El objetivo principal de un BCP es minimizar el impacto de la interrupción en la organización, sus clientes, empleados y otras partes interesadas, y permitir una recuperación rápida y efectiva. El plan incluye una serie de medidas preventivas y de mitigación, así como un conjunto de pautas y procedimientos para garantizar la continuidad de las operaciones críticas y la recuperación de los servicios y sistemas clave.

En sí, un BCP es un plan integral que permite a las organizaciones continuar operando en situaciones de interrupción y minimizar el impacto en el negocio y sus operaciones críticas. El plan se actualiza regularmente para garantizar que sea efectivo y refleje los cambios en el entorno operativo de la organización.

2.1.1. Fases de un Plan de Continuidad de Negocio

Según el estándar ISO 22301:2012 y las guías prácticas de implementación de un plan de continuidad, se define las siguientes fases.

Fase 0: Determinar el alcance, dependiendo de la complejidad organizativa de la empresa, determinar las áreas de interés y definir el alcance de plan de continuidad.

Fase 1: Análisis de la Organización, recopilar información necesaria, para determinar procesos y activos que dan soporte a dichos procesos.

Fase 2: Determinar las estrategias de continuidad, análisis de riesgo para determinar si la empresa es capaz de recuperar activos, en caso de ocurrir algún desastre.

Fase 3: Respuesta a la contingencia, establecer acciones necesarias con base a estrategias de recuperación.

Fase 4: Prueba, mantenimiento y revisión.

Fase 5: Concienciación, Fomentar la mejora continua del BCP.

2.1.2. Beneficios del Plan de Continuidad de negocio

- Competitividad: Fomenta a crear una nueva imagen de la empresa, suministrando seguridad y confianza a sus clientes.
- Fallos o interrupciones: Permite restaurar y proteger los procesos de la empresa, para que sigan funcionando en cualquier situación.
- Prevenir perdidas: identificar los posibles impactos de riesgo de las interrupciones del proceso.
- Estrategia: Plan de recuperación de activos, en caso de pérdida en el tiempo necesario.
- Tiempo de recuperación: Recurso necesarios para garantizar la continuidad. (Pincay Ronquillo, 2021, pág. 8)

2.2. Análisis de impacto del negocio (BIA)

Según Bautista (2014) citado por Pincay (2021), afirma que el BIA permite diseñar la estrategia para la empresa y su recuperación en un tiempo estimado, reiniciar sus operaciones, identificar las fallas, las causas y los procesos críticos. De la misma manera indica que el análisis BIA es un paso critico en el desarrollo de una estrategia de recuperación de desastres, el cual consiste en evaluar los procesos de la organización, determinar plazos, prioridades, recursos e interdependencias como resultados de la paralización de actividades que pongan en riesgo la continuidad de la empresa (Pincay Ronquillo, 2021).

El BIA se utiliza para determinar la cantidad de tiempo que una organización puede permitirse estar sin sus servicios y recursos críticos, así como las posibles pérdidas financieras y operativas asociadas con una interrupción. Esto ayuda a priorizar la recuperación de los servicios críticos y a establecer objetivos realistas de recuperación.

2.3. Plan de Recuperación de Desastre (DRP)

Según Arévalo (2022) menciona que "un plan de recuperación de desastres (DRP) está diseñado como lista de comprobación o instructivo de trabajo en caso de la materialización de un escenario de desastre a nivel de infraestructura" (pág. 23).

El objetivo principal de un DRP es minimizar el impacto negativo de un desastre en el negocio y permitir una rápida recuperación de los servicios críticos de la empresa. El plan incluye una serie de procesos, protocolos y herramientas para garantizar la continuidad del negocio, la protección de los datos y la recuperación de los sistemas y aplicaciones en caso de un desastre.

En sí, un DRP es un plan integral que ayuda a las organizaciones a recuperarse de manera rápida y efectiva de desastres, minimizando el impacto negativo en el negocio y sus operaciones críticas.

2.4. Amenazas, Vulnerabilidades y Riesgos Informáticos

Son términos relacionados con la seguridad de la información y la tecnología en general. A continuación, te explico brevemente en qué consisten:

2.4.1. Amenazas informáticas

Son situaciones, eventos o acciones que pueden causar daño a los sistemas informáticos o a la información que se encuentra en ellos. Las amenazas pueden ser de origen interno o externo, intencionales o no intencionales. Algunos ejemplos de amenazas informáticas incluyen virus, malware, phishing, ataques de hackers, robo de identidad, entre otros. (Bedoya, 2014)

2.4.2. Vulnerabilidades Informáticas

Son debilidades o fallas en los sistemas informáticos que pueden ser aprovechadas por un atacante para comprometer la seguridad de la información. Estas vulnerabilidades pueden ser causadas por errores de programación, configuraciones inseguras, sistemas operativos obsoletos, entre otros factores. Las vulnerabilidades son explotadas por los atacantes para llevar a cabo sus acciones maliciosas. (Castro, y otros, 2018)

2.4.3. Riesgos informáticos

Son la posibilidad de que una amenaza explote una vulnerabilidad y cause un daño. Los riesgos informáticos son el resultado de la combinación de amenazas y vulnerabilidades. Cuanto mayor es la cantidad de amenazas y vulnerabilidades en un sistema informático, mayor es el riesgo de que se produzca un incidente de seguridad. Los riesgos informáticos pueden tener un impacto significativo en las empresas, organizaciones y usuarios individuales. (Bedoya, 2014)

Para protegerse contra las amenazas informáticas, es importante implementar medidas de seguridad informática adecuadas, como el uso de software antivirus, el cifrado de datos sensibles, la autenticación de usuarios y la realización de copias de seguridad regulares. También es importante mantenerse actualizado sobre las amenazas informáticas y las mejores prácticas de seguridad informática para estar preparado para enfrentar los riesgos que pueden surgir.

2.5. Riesgos en tecnología de información

Son aquellos eventos que pueden afectar la confidencialidad, integridad o disponibilidad de los datos y sistemas de información de una organización.

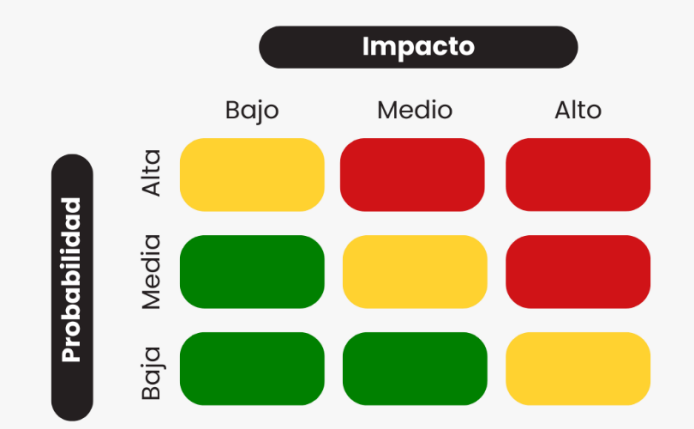
2.5.1. Valoración del riesgo

La valoración de riesgo consta de 4 etapas: la identificación, el análisis, evaluación y mitigación del riesgo. La valoración de riesgos es una herramienta importante para cualquier organización que busque identificar y controlar los riesgos asociados con sus actividades, proyectos o procesos. (Cruz Mendoza, Jalpilla Jiménez, & Ramírez, 2016)

2.5.2. Identificación del Riesgo

Este paso implica la identificación de los riesgos potenciales que podrían afectar la actividad, proyecto o proceso a través de la elaboración de un mapa de riesgos. Los riesgos pueden provenir de una amplia variedad de fuentes, incluyendo factores internos y externos. (Cruz Mendoza, Jalpilla Jiménez, & Ramírez, 2016)

Ilustración 1: Mapa de Riesgos



Nota: Tomado de https://blog.centrodeelearning.com/2022/09/13/como-realizar-un-mapa-de-riesgos-en-planta-de-forma-correcta/

2.5.3. Evaluación del riesgo

Este paso implica evaluar la importancia de cada riesgo y determinar su nivel de prioridad en función de su probabilidad e impacto. Esta evaluación puede ayudar a decidir cómo se deben asignar los recursos para controlar o mitigar los riesgos.

Ilustración 2: Matriz de Riesgo

Impacto

¿Qué tan severos serían los resultados si ocurriera el riesgo?

Probabilidad

¿Cuál es la probabilidad de que ocurra el riesgo?

	Insignificante 1	Menor 2	Significativo 3	Mayor 4	Severo 5
5 Casi seguro	Medio 5	Alto 10	Muy alto 15	Extremo 20	Extremo 25
4 Probable	Medio 4	Medio 8	Alto 12	Muy alto 16	Extremo 20
3 Moderado	Bajo 3	Medio 6	Medio 9	Alto 12	Muy alto 15
2 Poco probable	Muy bajo 2	Bajo 4	Medio 6	Medio 8	Alto 10
1 Raro	Muy bajo 1	Muy bajo 2	Bajo3	Medio 4	Medio 5

Notas: Obtenido de https://safetyculture.com/es/temas/evaluacion-de-riesgos/matriz-de-riesgo/

2.5.4. Mitigación del Riesgo

La mitigación del riesgo se enfoca en minimizar el impacto de los riesgos. Una vez que se haya evaluado el riesgo, se debe identificar medidas de mitigación para reducir el riesgo a un nivel aceptable para la organización. Esto puede implicar la implementación de controles de seguridad, la modificación de procesos y procedimientos, o la transferencia del riesgo a través del seguro.

2.6. Análisis y Gestión de Riesgo

El análisis y gestión de riesgos es una práctica importante en la gestión de proyectos y en la toma de decisiones empresariales, ya que ayuda a identificar y mitigar los riesgos asociados a las actividades empresariales, lo que puede reducir el impacto negativo de los riesgos potenciales y aumentar las oportunidades de éxito.

2.6.1. Metodología para análisis de Riesgo

La identificación de riesgos es una actividad esencial al momento de construir un Sistema de Gestión de Seguridad (SGSI), debido a que como primer punto es necesario la identificación de los factores que puedan amenazar a la empresa y comprender las vulnerabilidades que pueden ser explotadas por las amenazas. (Molina & Sánchez, 2015)

Existen diferentes metodologías para análisis de riesgo informático como: OCTAVE, CRAMM, ISO 27005, MAGERIT, etc.

Según la investigación realizada por Bermúdez & Bailón (2015), Determina que MAGERIT es una metodología que abarca de forma completa, las pautas a seguir para el análisis de riesgos, a la vez que se encuentran alineadas a los estándares de gestión de riesgos ISO 27005 e ISO 31000. A más de ellos una tabla comparativa realizada por los

mismo establece que la metodología MAGERIT es la adecuada para la correcta gention de riesgos.

Tabla 1: Matriz Comparativa de las metodologías de Análisis de Riesgo.

		MAGERIT	OCTAVE	CRAMM	EBIOS
Alcance Considerado	Análisis de Riesgos	Si	Si	Si	Si
	Gestión de Riesgos	Si	Si	Si	Si
Tipo de Análisis	Cuantitativo	Si	Limitada	Si	Si
	Cualitativo	Si	Limitada	Si	Si
	Mixto	Si	Limitada	Si	No
Objetivos de Seguridad	Confidencialidad	Si	Si	Si	Si
	Integridad	Si	Si	Si	Si
	Disponibilidad	Si	Si	Si	Si
	Autenticidad	Si	No	No	No
	Trazabilidad	Si	No	No	No
Ayudas a la Implantación	Herramienta	Si	No	Limitada	Si
	Plan de Proyecto	Si	Si	Limitada	No
	Técnicas	Si	Si	No	No
	Roles	Si	Si	Si	No
	Comparativas	Si	No	Si	No

Nota: Obtenida de

2.6.1.1. Fases de ejecución del análisis de riesgo de MAGERIT

Ilustración 3: Proceso de MAGERIT

NOTA: Obtenido de; Fuente: *(Guagalango Vega & Moscoso Montalvo, 2014, pág. 11)*

- **Identificación de Activos**

Se identifican los activos de información crítica de la organización, en los que el impacto por la ausencia, deterioro o pérdida del activo se traduce en problemas para afrontar la continuidad del negocio.

- **Determinar la Amenaza**

Identificar las posibles amenazas que pueden afectar a los activos de información crítica con el fin de poder evaluar la magnitud del deterioro ejercido sobre el activo y la probabilidad de ocurrencia en la que puede darse.

- **Determinar Salvaguardas**

Las salvaguardas se vuelven punto importante en el análisis de riesgo, son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo (Carolina, 2013). Dichas salvaguardas entran en el cálculo del riesgo cumpliendo dos paradigmas importantes como es la *reducción de la probabilidad de las amenazas* y *limitando el daño causado.*

- **Estimación de Impacto ejercido por las amenazas**

La estimación de impacto es un ítem también de gran importancia debido a que permite evaluar el posible impacto que puedan tener los activos de información ante la materialización de una amenaza.

- **Estimación de riesgo**

"La estimación trata de evaluar la probabilidad, el impacto y la proximidad de cada amenaza u oportunidad" (Tayo, 2017, pág. 38). En si la estimación de riesgo tiene como finalidad minimizar la probabilidad de que ocurra u evento negativo y maximizar los beneficios de las oportunidades positivas.

2.7. Metodología Y Estándares Para La Construcción Del Plan De Continuidad De Negocio.

Ilustración 4: Plan de Continuidad de Negocio

NOTA: Obtenido de https://occidentesp.com.co/plan-de-continuidad-del-negocio/

El PCN se centra en la identificación de los procesos y sistemas críticos de la organización y en la planificación de cómo mantenerlos en funcionamiento durante y después de una interrupción. Esto incluye la implementación de medidas preventivas y de contingencia, la asignación de roles y responsabilidades, la identificación de los recursos necesarios para la recuperación y la realización de pruebas y simulaciones.

La construcción del Plan de Continuidad de Negocio (PCN) se basa en una metodología específica y en estándares establecidos por organizaciones como ISO (Organización Internacional de Normalización) y NIST (Instituto Nacional de Estándares y Tecnología).

Las normas y estándares son un conjunto de reglas, requisitos o especificaciones que se utilizan para establecer y mantener la calidad, seguridad, eficiencia y compatibilidad en diferentes áreas.

A continuación, se describe algunas normas de continuidad del negocio:

2.7.1. Norma ISO 22301

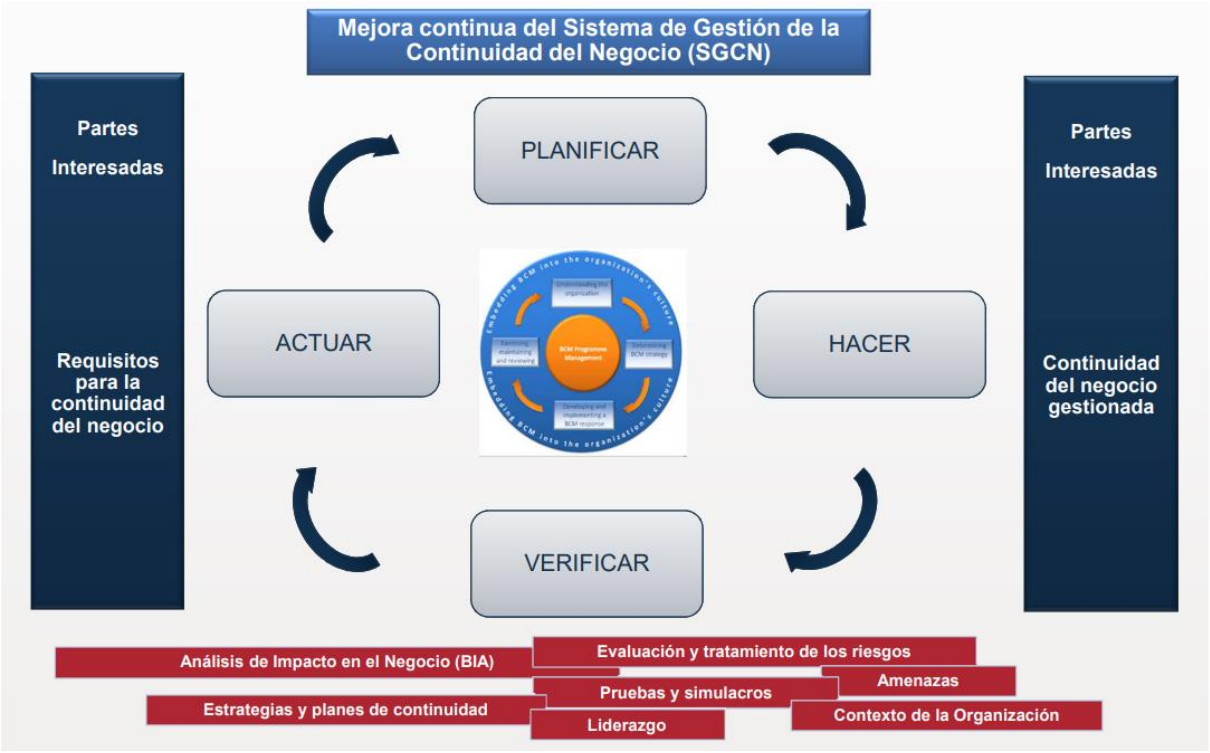
La norma ISO 22301 es reconocida internacionalmente como una referencia para la gestión de la continuidad del negocio y puede ayudar a las organizaciones a demostrar su compromiso con la gestión efectiva de los riesgos relacionados con la continuidad del negocio. “El estándar permite proteger los activos de amenazas hacia la empresa y las interrupciones que generan pérdidas y seguir con la continuidad de las actividades ejecutadas independientemente de la complejidad que presente en su activo de incidentes que provoque interrupciones” (Pincay Ronquillo, 2021, pág. 12).

“La norma ISO 22301 está alineada con ISO 27001, ISO 9001 e ISO 20000 con el objeto de facilitar la consistencia necesaria y permitir la sinergia en la implantación y operación del sistema de gestión” (Cruz, 2012, pág. 13).

El propósito de esta norma es permitir que las organizaciones sincronicen e incorporen su Sistema de Gestión de Continuidad del Negocio (BCMS, por sus siglas en inglés) con los requerimientos de los sistemas de gestión relacionados.

Esta norma adopta el ciclo de Plan – Do – Check – Act (PDCA) como marco de referencia para el sistema de gestión de continuidad de negocio en todas sus etapas, lo cual hace ideal y ajustable a cualquier tipo y tamaño de empresa.

Ilustración 5: Ciclo PDCA



Nota: Fases para la mejora continua del SGSI

Plan: En esta etapa, se identifica el problema y se desarrolla un plan para resolverlo. Esto incluye definir el problema, identificar la causa raíz, establecer objetivos y crear un plan de acción para lograr esos objetivos.

Do: Esta etapa consiste en implementar el plan. Se llevan a cabo las acciones descritas en el plan y se recopilan datos para monitorear el progreso.

Check: Los datos recopilados durante la etapa "Do" se analizan para determinar si el problema se ha resuelto y se han logrado los objetivos. Si no, el proceso se repite hasta lograr el resultado deseado.

Act: Consiste en tomar medidas en función de los resultados de la etapa "Check". Si el problema se ha resuelto y se han logrado los objetivos, se implementa el nuevo proceso. Si no, el proceso se repite hasta lograr el resultado deseado.

2.7.1.1. Fase de la ISO 22301

Ilustración 6: Fase para el desarrollo de un Plan de continuidad de negocio.

Nota: Obtenido de https://es.linkedin.com/pulse/fases-para-un-plan-la-continuidad-del-negocio-enrique-chicalote

Fase 1: E Elaboración del programa de BCM

"En esta fase se diseña el programa de gestión de un BCP, considerando el tamaño y la propia complejidad de la empresa. Se define el equipo básico encargado del BCM, incluyendo funciones y responsabilidades" (ISOTools Excellence, 2018).

Fase 2: Comprensión de la empresa

Durante esta fase, se recolecta la información necesaria para identificar las actividades clave y de apoyo, así como los recursos que se requieren para llevarlas a cabo. También se evalúa el impacto que estas actividades tienen en el negocio y se analizan los riesgos asociados a su implementación. (ISOTools Excellence, 2018)

Fase 3: Definir las estrategias para la gestión de la continuidad del negocio

Esta fase tiene como objetivo identificar todas las actividades empresariales clave que permitirán a la empresa recuperar sus servicios en un plazo determinado después de una interrupción.

Fase 4: Elaboración y ejecución de una respuesta BCM

En esta etapa, se elaboran todas las soluciones necesarias para hacer frente a las situaciones de emergencia. Se detallan los planes con los pasos a seguir antes, durante y después de la interrupción, con el objetivo de reorganizar los procesos de negocio en orden de prioridad. (ISOTools Excellence, 2018)

Fase 5: Poner en práctica, cumpliendo los acuerdos definidos del BCM

Este paso permite determinar si las estrategias y planes son adecuados para lograr el propósito previsto. Se logra mediante la planificación de ejercicios regulares para revisar la continuidad del negocio y detectar posibles oportunidades de mejora. Estos ejercicios se programan en intervalos específicos y permiten una evaluación sistemática de la efectividad de las estrategias y planes establecidos. (ISOTools Excellence, 2018)

2.7.2. NIST SP 800-34

Esta es una guía del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos para la gestión de la continuidad de negocio. La guía describe un proceso paso a paso para la elaboración de un PCN, desde la identificación de los servicios críticos hasta la elaboración de planes de recuperación y pruebas de continuidad.

La finalidad de los planes de contingencia es minimizar el riesgo de posibles interrupciones, ya sean de gravedad leve o alta, y se enfocan en la implementación de soluciones efectivas y eficientes para mejorar la disponibilidad del sistema. Aunque se proporcionan conocimientos, recomendaciones y consideraciones para estos planes, es importante tener en cuenta que no se pueden eliminar por completo todos los riesgos posibles. (Yarlequé Gutiérrez, 2019)

2.7.2.1. Fases de la IST SP 800-34

La norma NIST SP 800-34 establece un proceso de seis fases para la elaboración de un plan de continuidad de negocio (BCP). Tales como:

Fase 1: Iniciación del proyecto

Esta fase implica el establecimiento de un equipo de proyecto, la definición del alcance del BCP y la obtención del compromiso y apoyo de la dirección de la organización.

Fase 2: Análisis de impacto en el negocio

En esta fase se identifican los procesos críticos del negocio, los sistemas y recursos que los respaldan, y se evalúa el impacto de su interrupción en la organización.

Fase 3: Estrategias de continuidad de negocio

En esta fase se desarrolla una estrategia para garantizar la continuidad de las operaciones críticas del negocio, y se identifican las soluciones de recuperación ante desastres necesarias para lograrlo.

Fase 4: Desarrollo del Plan

En esta fase se crea un plan de continuidad de negocio que incluye los procedimientos de respuesta a emergencias, la asignación de roles y responsabilidades, y los requisitos de comunicación y coordinación.

Fase 5: Implementación del Plan

En esta fase se implementan los procedimientos y soluciones de recuperación ante desastres identificados en el plan de continuidad de negocio, y se establecen mecanismos de seguimiento y control.

2.7.3. Matriz Comparativa entre la norma ISO 22301 y la norma NIST SP 800-34

Tabla 2: ISO 22301 VS NIST SP 800 - 34

Aspecto	ISO 22301	NIST SP 800-34
Ámbito de aplicación	Se aplica a todos los tipos de organizaciones y sectores	Se aplica a organizaciones gubernamentales y no gubernamentales
Objetivo	Establecer, implementar y mantener un Sistema de Gestión de Continuidad de Negocio (SGCN)	Proporcionar una guía para la elaboración y mantenimiento de planes de contingencia
Enfoque	Basado en procesos y en la mejora continua	Basado en fases y en el ciclo de vida del plan de contingencia
Estructura	Requisitos y directrices	Guía detallada y exhaustiva
Enfoque de riesgos	Evaluación de riesgos y evaluación de impacto en el negocio (BIA)	Identificación y evaluación de riesgos
Comunicación y gestión de crisis	Requiere un plan de comunicación y un plan de gestión de crisis	Requiere la identificación de las responsabilidades y autoridades durante una crisis
Continuidad del negocio	Requiere la implementación de estrategias y planes de continuidad de negocio	Proporciona una guía para la elaboración de planes de contingencia para mitigar interrupciones en los procesos de negocio
Mejora continua	Requiere la monitorización y la revisión del SGCN para la mejora continua	Proporciona una guía para el mantenimiento y la actualización del plan de contingencia

De acuerdo a la matriz comparativa realizada entre las dos normas descritas anteriormente, se determina que, ambas normas se enfocan en la gestión de la continuidad del negocio y la mitigación de riesgos, pero difieren en su alcance y enfoque. Es decir que, la norma ISO 22301 es más amplia en su alcance y se enfoca en el establecimiento de un Sistema de Gestión de Continuidad de Negocio, mientras que la norma NIST SP 800-34 se enfoca en la elaboración y mantenimiento de planes de contingencia.

CAPITULO III

3. ENFOQUE DE LA INVESTIGACIÓN

3.1. ENFOQUE DE LA INVESTIGACIÓN.

En el presente trabajo investigativo se considera un enfoque Cuali-Cuantitativo: El enfoque Cualitativo será utilizado para obtener información detallada sobre los riesgos que enfrentan la Cooperativa y como estas podrían afectar a la continuidad de sus operaciones, mientras que el enfoque cuantitativo se utiliza analizar los datos y medir la probabilidad y el impacto de los riesgos identificados.

3.2. Nivel de investigación

El nivel de investigación será descriptivo, puesto que se realizará un levantamiento de información del departamento de sistemas de la cooperativa de Ahorro y Crédito "ACHIK INTI", también se realiza la identificación y descripción de los riesgos que enfrentan la cooperativa a través de entrevistas, encuestas y otros métodos para obtener información relevante para el desarrollo de proyecto investigativo.

3.3. Población y Muestra

La población considera para el desarrollo de la investigación es la totalidad de la Cooperativa de Ahorro y Crédito ACHIK INTI. Es decir, todas las personas que laboran en la organización.

La muestra se centra en las personas claves de la organización, en este caso la gerencia y el personal de TI quienes tienen un conocimiento relevante sobre el riesgo que enfrenta la cooperativa en términos de continuidad de negocio.

3.4. Técnicas e instrumento de recolección

Para recopilar la información necesaria, se llevarán a cabo entrevistas con los directivos del proyecto de TI.

3.5. Tratamiento de la Información

La información recopilada de las entrevistas con los directivos y el responsable del área de TI será procesada y organizada de manera adecuada a través de la creación de matrices estructuradas y sistematizadas.

3.6. Resultados

Después de haber elaborado las preguntas para la entrevista, se procede a su aplicación. Es importante destacar que la entrevista se llevó a cabo únicamente con el gerente de la cooperativa y el director del área de TI, quienes serán los responsables del proyecto.

3.7. Análisis e interpretación de los datos

Se realizó una entrevista en la Cooperativa de Ahorro y Crédito “ACHIK INTI” con el objetivo de recopilar información relacionado a los procesos, riesgos, activos, etc., necesarios para el desarrollo del modelo de un BCP. La entrevista se llevó a cabo con el director de tecnología y el gerente de la Cooperativa, la misma fue grabada para su posterior análisis.

A continuación, se presenta los resultados de los datos recopilados y su interpretación.

3.7.1. Matriz de resultados obtenidos mediante la entrevista

Entrevista realizada al gerente de la Cooperativa de Ahorro y Crédito “ACHIK INTI”		
Pregunta	**Respuesta**	**Interpretación**
¿Dentro de su organización que tipos de información maneja?	La cooperativa maneja la información de credenciales, financieras, servicios no financieros, datos personales de los socios, empleados.	La cooperativa maneja información confidencial y crítica que incluye credenciales de acceso, información financiera, servicios no financieros y datos personales de socios y empleados. Esta información debe ser protegida adecuadamente para garantizar la privacidad y seguridad de los socios y empleados, así como la continuidad y reputación de la cooperativa.
¿De los tipos de información manejada dentro de la cooperativa a cuál de ella considera importante?	La información de credenciales y los datos financieros de los socios son consideradas de gran importancia para la cooperativa.	La información de credenciales y los datos financieros de los socios son críticos para la cooperativa, ya que contienen información confidencial sobre las transacciones financieras y la situación económica de los socios. La divulgación o pérdida de esta información puede tener un impacto significativo en la operación y reputación de la cooperativa.
¿La cooperativa cuenta con un plan de continuidad de negocio?	La cooperativa no cuenta con un plan de continuidad de negocio.	La falta de un plan de continuidad de negocio puede dejar a la cooperativa vulnerable a interrupciones significativas en sus

		operaciones y pérdida de datos críticos en caso de un evento de interrupción o desastre.
¿La cooperativa cuenta con procesos bien definidos y con sus respectivos responsables?	Si se cuenta con procesos definidos en cada área.	De acuerdo a la respuesta se determina que la cooperativa tiene una estructura organizacional clara, en la que se establecen roles y responsabilidades para cada proceso en la organización. Esto puede ayudar a mejorar la eficiencia de la cooperativa, ya que cada miembro del equipo sabe exactamente cuáles son sus responsabilidades.
¿La cooperativa realiza la gestión de riesgos de seguridad de la información?	la cooperativa no cuenta con un programa para identificar, evaluar y abordar los riesgos de seguridad de la información.	Se determina que la cooperativa no tiene un programa estructurado para identificar, evaluar y mitigar los riesgos de seguridad de la información que puedan afectar su operación y a sus clientes. Lo que provoca que la cooperativa puede estar en riesgo de sufrir incidentes de seguridad informática que podrían tener un impacto negativo en la operación de la cooperativa y en la confianza de sus clientes.

¿Cuándo se produce problemas con los equipos o suspensión de servicio, estos son atendidos con el fin de disminuir el impacto que puede ocasionar a la cooperativa?	En efecto, se atiende inmediatamente por el área de TI, a fin minimizar el tiempo de inactividad del sistema.	La cooperativa cuenta con el personal de TI que está disponible para atender y resolver problemas técnicos que puedan surgir en los equipos o servicios que se utilizan en la cooperativa.
¿Cuál es el tiempo que emplea para realizar el análisis de gestión de riesgos dentro de la cooperativa?	No se realiza un análisis de riesgo	La respuesta indica que la cooperativa no realiza ningún análisis para identificar y evaluar los riesgos que pueden afectar su operación y a sus clientes. Esto puede exponer a la cooperativa y a sus clientes a una variedad de riesgos, como seguridad informática, fraude y errores operativos, entre otros.
¿Cuáles son los principales riesgos que enfrenta la Cooperativa de Ahorro y Crédito Achik Inti en términos de interrupciones de sus operaciones?	Desastre natural, filtrado de red, Errores y fallos no intencionados en los equipos.	La cooperativa determina estos riesgos como los más importantes en términos de posibles interrupciones de sus operaciones.

¿Cómo se evalúan y priorizan los riesgos de interrupción de la Cooperativa de Ahorro y Crédito Achik Inti?	Actualmente no hay un proceso formal establecido para evaluar y priorizar los riesgos de interrupción en la cooperativa.	La cooperativa no tiene un proceso formal establecido para evaluar y priorizar los riesgos de interrupción en sus operaciones. Esto sugiere que la cooperativa no ha identificado ni evaluado sistemáticamente los riesgos que podrían afectar sus operaciones y a sus clientes, y, por lo tanto, no ha implementado medidas de mitigación adecuadas para minimizar estos riesgos.
¿Cómo se garantiza la protección de la información confidencial de la Cooperativa de Ahorro y Crédito Achik Inti en caso de interrupciones o desastres?	Actualmente, no se realiza un análisis formal de riesgos para identificar y mitigar posibles interrupciones del servidor principal en la Cooperativa Inti. Sin embargo, se cuenta con un servidor auxiliar disponible en caso de que ocurran interrupciones en el servidor principal.	La respuesta indica que, aunque la cooperativa no tiene un proceso formal de análisis de riesgos, ha implementado medidas para mitigar los posibles riesgos de interrupción del servidor principal. Estas medidas incluyen la disponibilidad de un servidor auxiliar en caso de interrupciones. Esto sugiere que la cooperativa ha tomado medidas para garantizar la continuidad del negocio y la protección de la información confidencial en caso de interrupciones o desastres, aunque no ha realizado una evaluación formal de riesgos.

¿Cómo se preparan los empleados para manejar situaciones de interrupción de las operaciones en la Cooperativa de Ahorro y Crédito Achik Inti?	Los empleados se preparan para manejar situaciones de interrupción de las operaciones a través de un programa de capacitación.	La cooperativa tiene un programa de capacitación para preparar a sus empleados para manejar situaciones de interrupción de las operaciones. Este programa puede incluir la capacitación en planes de contingencia, la gestión de riesgos y la respuesta a incidentes de seguridad informática. Al capacitar a los empleados para manejar situaciones de interrupción, la cooperativa puede estar mejor preparada para mantener la continuidad del negocio y proteger a sus clientes en caso de interrupciones en sus operaciones.

Entrevista realizada al director de área de TI		
Pregunta	**Respuesta**	**Interpretación**
¿Cree usted que el departamento de TI tiene riesgos tecnológicos que puedan afectar los diferentes procesos de la cooperativa?	Efectivamente, el área de TI representa un componente crucial para el funcionamiento de la cooperativa, con la ausencia de un sistema informático operativo, no se podría llevar a cabo ninguna de sus actividades.	El área de TI tiene un alto nivel de riesgo tecnológico, ya que cualquier falla o interrupción en los sistemas informáticos podría afectar significativamente los diferentes procesos de la cooperativa y comprometer su continuidad operativa.
¿Dentro del departamento de TI cual son los procesos más críticos que afecten el normal desempeño de los servicios?	Los procesos más críticos se relacionan con la gestión de usuarios, incluyendo la creación, habilitación y asignación de permisos y roles, Copia de seguridad de los servidores	La gestión de usuarios y la copia de seguridad de los servidores son procesos críticos dentro del departamento de TI que deben ser cuidadosamente gestionados y monitoreados para asegurar el correcto funcionamiento de la cooperativa.
Ante la identificación de amenazas informáticas ¿El departamento de TI	No se tiene tiempos de respuesta	Se determina que el departamento de TI no cuenta con un plan de respuesta estandarizado

tiene estandarizado los tiempos de recuperación en caso de que se llegaran a ejecutar esas amenazas?		en caso de amenazas informáticas, lo que puede ser una vulnerabilidad para la seguridad y continuidad operativa de la organización.
¿Dentro del área de TI Tiene definido un manual de procesos o procedimientos en la institución?	El departamento de TI tiene documentado los procesos más críticos y más utilizados, tales como la creación de usuarios, el mantenimiento y recuperación de bases de datos, la reactivación de sistemas y la realización de respaldos.	Tener un manual de procesos o procedimientos documentados es fundamental para garantizar la consistencia y la calidad en la realización de las tareas, así como para facilitar la capacitación y el entrenamiento de los nuevos miembros del departamento de TI.
¿El departamento de TI cuenta con procesos bien definidos y con sus respectivos responsables? Cuales.	Dentro del departamento de TI, el Ingeniero José Iglesias es el encargado directo de la gestión de esta área. Sin embargo, en el manual de procedimientos de TI, se establecen los roles y responsabilidades de otras áreas de la organización, como Recursos Humanos y Gerencia, quienes están vinculados a los procesos de TI	La respuesta indica que el departamento de TI cuenta con procesos bien definidos y que se asignan roles y responsabilidades claras a las diferentes áreas de la organización para asegurar una adecuada coordinación y colaboración en los procesos de TI.

	y tienen claro cuáles son sus respectivas funciones en este ámbito.	
¿La cooperativa cuenta con un plan de control operacional de seguridad de información ante la presencia de amenazas o riesgos?	La cooperativa ha implementado diversas medidas de seguridad como la asignación de roles específicos de usuarios para el acceso a las computadoras, la limitación del acceso a ciertas páginas de redes sociales, la instalación de un firewall y un sistema de cableado adecuado.	De acuerdo a la respuesta se determina que la cooperativa ha implementado medidas de seguridad para proteger la información, pero no queda claro si cuenta con un plan de control operacional de seguridad de información ante la presencia de amenazas o riesgos.
¿Cuál es el papel de la tecnología de la información en la continuidad del negocio en la Cooperativa de Ahorro y Crédito Achik Inti?	La tecnología de la información es el responsable de proporcionar y garantizar el correcto funcionamiento de los sistemas y herramientas necesarias para el desarrollo de las actividades de la organización, así como de proteger la información y los datos de la cooperativa.	La tecnología de la información es esencial para la continuidad del negocio en la cooperativa, ya que es responsable de proporcionar sistemas y herramientas para las actividades de la organización, y proteger su información y datos.

3.7.2. Análisis general de la entrevista

Una vez analizado las preguntas planteadas en la entrevista tanto al gerente como al encargado del área de Tecnología de la Información (TI), se ha podido constatar que los datos obtenidos presentan una alta fiabilidad y validez para la toma de decisiones. En particular, los resultados obtenidos a partir de las entrevistas permiten identificar los procesos más críticos en el área de TI y las medidas de seguridad de la información implementadas en la organización.

Las preguntas se enfocan en temas relacionados con la tecnología de la información y su papel en la cooperativa de ahorro y crédito Achik Inti. Las respuestas indican que la cooperativa maneja información confidencial y crítica, y que no cuenta con un plan formal de continuidad del negocio o gestión de riesgos de seguridad de la información. Sin embargo, se señala que la cooperativa ha implementado medidas para mitigar posibles riesgos y ha establecido roles y responsabilidades claras para cada proceso en la organización. También se menciona que la cooperativa tiene un programa de capacitación para preparar a sus empleados para manejar situaciones de interrupción de las operaciones. Por otra parte, la entrevista al director de área de TI indica que el departamento de TI es crucial para el correcto funcionamiento de la cooperativa, ya que maneja información crítica y realiza procesos críticos como la gestión de usuarios y la copia de seguridad de servidores. Sin embargo, también se identifican vulnerabilidades en cuanto a la falta de un plan de respuesta estandarizado ante amenazas informáticas y la falta de claridad sobre si la cooperativa cuenta con un plan de control operacional de seguridad de información. Aunque se confirma que el departamento de TI tiene procesos bien definidos y roles y responsabilidades claros, lo que puede mejorar la eficiencia y coordinación en los procesos de TI.

3.8. Selección de la norma para la gestión de Continuidad de negocio

De acuerdo a la matriz comparativa realizada en el capítulo 2, entre la norma ISO 22301 y VS NIST SP 800 – 34 se determina que la norma que más se acopla al desarrollo del proyecto es la ISO 22301 puesto que se enfoca en la organización en su conjunto y ayuda a garantizar que la toma de decisiones esté cubierta por la continuidad de negocio, lo que permite que la organización esté mejor preparada para responder y recuperarse de interrupciones imprevistas en sus operaciones.

3.9. Selección de la metodología para análisis y gestión de riesgo

En base a una investigación realizada por Kelly Bermúdez y Edber Bailón en su proyecto de "Análisis en seguridad informática y seguridad de la información basado en la Norma ISPO/IEC 27001" y una matriz comparativa con diferentes metodologías de gestión de riesgo se determina que la metodología MAGERIT es una metodología que abarca de forma completa, las pautas a seguir para el análisis de riesgos y a su vez se alinea a los estándares de gestión de riesgos ISO 27005 e ISO 31000, por la cual se opta por la utilización de dicha metodología para el desarrollo del presente trabajo investigativo.

CAPÍTULO IV

4. PROPUESTA

En este capítulo se expone el desarrollo de la propuesta de un plan de continuidad de negocio para la cooperativa de ahorro y crédito “Achik Inti”, el objetivo de esta guía es servir como referencia para futuras implementación del BCP en pequeñas, medianas y grandes empresas en el ámbito nacional.

Después de realizar una comparación entre diferentes enfoques y normativas para llevar a cabo un Plan de Continuidad de Negocio, así como un análisis y gestión de riesgos en el capítulo III, se ha optado por utilizar la norma ISO 22301 como guía para desarrollar el BCP y la metodología MAGERIT para llevar a cabo el análisis de riesgos.

4.1. Elaboración de un Plana de Continuidad de negocio siguiendo las directrices establecidas en la normativa ISO 22301.

4.1.1. Etapa 1: Creación del programa BCP

Para iniciar con la creación del Plan de Continuidad de Negocios, se ha establecido la designación de líderes para el BCP, quienes son:

- Gerente general de la Cooperativa de Ahorro y Crédito “Achik Inti”.
- Personal encargado del área de Tecnología de la Información de la Cooperativa.

El propósito principal de realizar un BCP es educar a todo el personal administrativo y de servicio de la Cooperativa de Ahorro y Crédito “ACHIK INTI”, así como a los responsables involucrados en el Plan de Continuidad de Negocios (BCP), sobre los pasos a seguir en caso de un incidente que afecte los servicios informáticos y las operaciones de la organización.

4.1.2. Etapa 2: Comprensión De La Organización

Durante esta etapa se evaluó la situación actual del área de TI de la Cooperativa de Ahorro y Crédito ACHIK INTI.

4.1.2.1. Antecedentes

La cooperativa de ahorro y crédito "ACHIK INTI" Ltda. Nace por las ideas de grupo jóvenes indígenas emprendedores, fue entonces que esta sociedad comenzó con reuniones semanales, como no se contaban con recursos suficientes para emprender grandes proyectos, se empezó con aportes económicos mensuales con lo cual se reunió un capital iniciándose con otorgamiento de préstamo a corto plazo especialmente a las personas de caso de recursos económicos de las parroquias y comunidades de la Provincia de Cañar; entonces se nació la mencionada cooperativa que pertenece a la nacionalidad kichwa del pueblo Cañari. (Achik Inti, s.f)

La cooperativa se constituyó en la Cuidad de Cañar, Provincia de Cañar, mediante de ACUERDO MINISTERIAL N° 0001- DPC-COOP- 011, inscrita en el Registro General de la Cooperativa con el número de orden 7572. El 9 de mayo del 2011, siendo su capital inicial de Treinta mil Dólares de los Estados Unidos de Norte América $30.000 con un número de 15 socios fundadores. (Achik Inti, s.f)

La cooperativa actualmente viene trabajando en vinculación con las comunidades dando mayores beneficios en la agricultura, ganadería, artesanía, asociación de grupos de mujeres y jóvenes emprendedores buscando un mejor ingreso económico sustentable.

La cooperativa se encuentra en la ciudad de Cañar, en la intersección de la calle Guayaquil y 10 de agosto. Su objetivo es brindar un servicio de alta calidad a cualquier persona natural o

jurídica, sin importar su raza, condición social, cultura, religión, entre otros aspectos. Asimismo, la cooperativa busca promover la interculturalidad del pueblo indígena, mestizo y afro ecuatoriano.

- **Misión Empresarial**

  Somos una institución financiera solidaria, honesta, que facilitamos el desarrollo integral sustentable impulsando un nuevo modelo económico mediante otorgamiento de créditos agiles, oportunos y de ahorro, mejorando la calidad de vida de nuestros socios y clientes, con personal capacitado y competente que brinda sus productos y servicios con agilidad, calidad para el buen vivir. (Achik Inti, s.f)

- **Visión Empresarial**

  Ser una Cooperativa líder en el mercado local y nacional promoviendo el Ahorro y Solucionando las necesidades de Crédito de consolidada como una alternativa de desarrollo integral para nuestros socios y la comunidad que cuenta con directivos y personal comprometidos en trabajo en equipo. (Achik Inti, s.f)

4.1.2.2. Organigrama de la cooperativa

Los socios son los encargados de liderar la Cooperativa de Ahorro y Crédito "ACHIK INTI" a través de la Asamblea General, donde se les informa sobre los aspectos más importantes en el ámbito financiero. A continuación, se presenta el organigrama de la cooperativa.

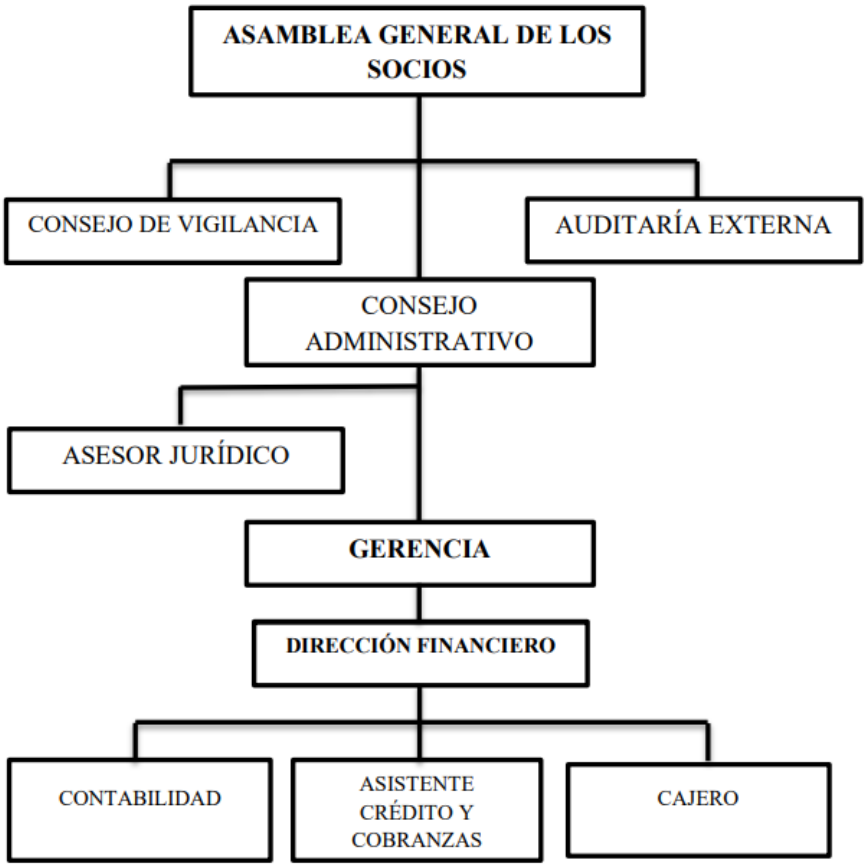


Ilustración 7: *Organigrama Institucional*

Fuente: *Cooperativa de Ahorro y Crédito Achik Inti.*

4.1.2.3. *Identificación y análisis de procesos organizacionales y sus interrelaciones*

Se recopilaron datos proporcionados por el jefe del departamento de Tecnología de la Información (TI) de la cooperativa, los cuales se describen a continuación, con el fin de identificar los procesos organizacionales.

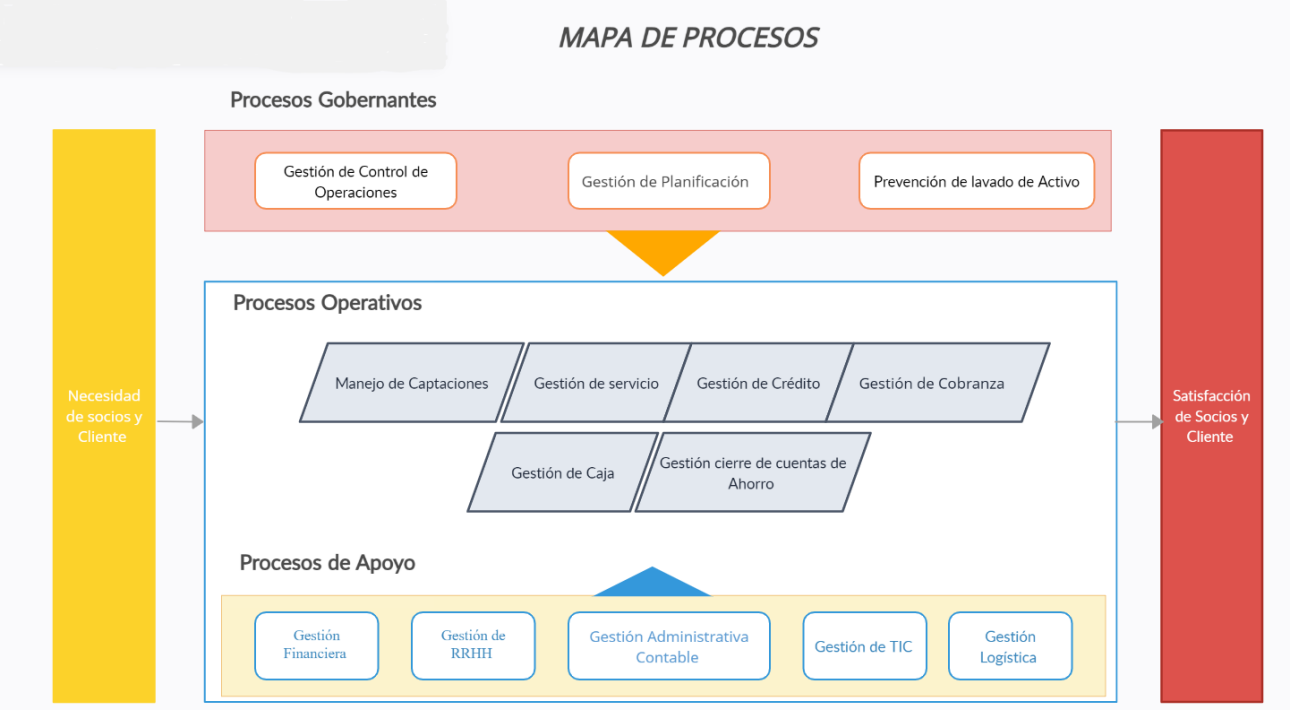


***Ilustración 8**: Mapa de Procesos Cooperativa de Ahorro y crédito Achik Inti.*

***Autor:** Propio*

La gráfica previa muestra claramente que la cooperativa “Achik Inti”. tiene 14 grandes procesos establecidos. Dentro de estos, 3 están relacionados con la gestión y dirección de la organización, mientras que 6 se enfocan en la producción de bienes o servicios y los 5 restantes se consideran procesos de apoyo. Una vez identificados los macro-procesos de la cooperativa Achik Inti., se describen los procesos y subprocesos del área de Tecnología de la Información (TI) que brindan soporte.

4.1.3. Evolución del impacto del negocio y análisis de riesgo utilizando la metodología MAGERIT.

Tras completar la comprensión y el análisis de los procesos establecidos en la cooperativa, se realiza una evaluación utilizando la metodología MAGERIT para determinar cómo el negocio puede verse afectado y qué riesgos están presentes. Al utilizar MAGERIT, se obtiene una

comprensión completa de las implicaciones y peligros que pueden surgir, lo que permite tomar decisiones informadas para mitigar los riesgos y garantizar la continuidad.

A continuación, se muestra una tabla con una escala detallada de diez valores, donde 0 se interpreta como un valor insignificante (en términos de riesgo) y 10 se interpreta como un valor de riesgo extremo.

Tabla 3: *Escala cuantitativa y cualitativa para la determinar los valores de los procesos*

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
De 6 a 8	Alto	Daño grave
De 3 a 5	Medio	Daño importante
De 1 a 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Nota: Escala de valores para determinar los procesos críticos de la Cooperativa.

Tipo de Procesos	Macro proceso	Proceso	Subproceso	Criterios de valoración												
				[pi]información de carácter personal	[lpo]Obligaciones legales	[si]Seguridad	[cei]intereses comerciales o económicos	[da]Interrupción de servicio	[po] Orden público	[olm] Operaciones	[adm]Administración y gestión	[lg]Pérdida de confianza(reputación)	[crm] Persecución de delitos	[rto]Tiempo de recuperación del servicio	[lbl.nat] Información clasificada(nacional)	Total
Procesos Gobernantes	Gestión Planificación	Plan estratégico institucional		4	5	1	7	1	1	1	6	3	1	0	8	38
		Plan Operativo Anual		3	5	1	6	1	1	1	6	3	1	0	8	36
	Gestión de Control de Operaciones	Comités Normativos Internos y externos	Asamblea general de Representantes	2	1	0	3	0	0	0	3	1	0	0	8	18
			Consejo de Administración	2	3	1	3	0	0	1	5	1	0	0	8	24
			Concejo de Vigilancia	1	1	1	0	0	1	1	0	1	0	4	8	18
			Comité de Cumplimiento	2	3	1	1	0	0	1	1	1	0	0	8	18
			Comité de administración integral de riesgos	1	1	1	1	0	1	1	7	1	0	0	7	21
			Comité de crédito	1	9	7	7	1	0	1	7	3	1	0	8	45
	Prevención de lavados de activos	Reglamento Interno del trabajo		3	3	1	1	0	0	1	1	1	0	0	8	19
		Gestión para la prevención de lavado de activos		4	5	7	2	0	1	1	1	1	4	1	8	35
Procesos Operativos	Manejo Captaciones	Gestión de cuentas de ahorro	Apertura de cuentas de ahorro	2	3	9	1	3	0	7	3	1	0	7	9	45
			Mantenimiento y actualización de datos	2	1	1	1	3	0	1	1	0	0	7	8	25
			Cierre de cuentas de ahorro	2	1	1	1	3	0	1	1	1	0	7	8	26
		Gestión de inversiones	Apertura de depósito a Plazo Fijo	3	1	1	1	3	0	1	1	1	0	7	8	27
			Renovación de depósito a Plazo Fijo	3	1	1	1	3	1	1	1	1	0	7	8	28
	Gestión de Crédito	Crédito de consumo	Crédito de consumo ordinario	4	3	1	2	1	1	3	1	1	0	7	8	32
			Crédito de consumo prioritario	4	3	1	2	1	1	3	1	1	0	7	8	32
		Microcrédito	Microcrédito acumulado simple	5	1	1	2	3	1	3	1	1	0	7	8	33
			Microcrédito acumulado ampliada	5	1	1	2	3	1	3	1	1	0	7	8	33

	Gestión de Cobranza	Gestión de Cobranzas	Gestión de cobranzas Preventiva	5	5	1	2	3	1	3	1	1	0	7	8	37
		Gestión de Cobranzas Extrajudicial	Gestión de Cobranzas Extrajudicial	8	7	10	1	7	1	7	3	3	4	1	8	60
	Gestión de Servicio	Gestión de servicios en cajas	Atención servicios financieros	2	1	1	1	1	1	1	1	0	0	7	4	20
			Atención de servicios no financieros	2	1	1	1	1	1	1	1	0	0	7	4	20
			Gestión de Cuadres y Conciliaciones de caja y bodega	6	3	1	1	3	1	3	1	1	4	1	8	33
Procesos de Apoyo	Gestión financiera	Administración del portafolio de inversiones		3	1	1	2	1	1	1	1	1	0	1	8	21
		Administración de Contabilidad	Contabilización y registro	6	3	3	1	3	1	1	1	2	4	1	4	30
			Generación de estados financieros	8	7	10	1	7	1	7	3	3	4	1	8	60
			Pago de obligaciones tributarias	8	7	10	1	7	1	7	3	3	4	1	9	61
			Generación de estructuras	1	3	1	1	1	1	1	1	1	1	1	4	17
	Gestión de Recursos humano	Incorporación del talento humano	Selección	2	3	1	1	1	0	1	1	1	1	0	4	16
			Contratación	3	1	1	1	1	0	1	1	1	1	0	4	15
			Inducción	1	1	1	1	1	0	1	1	1	1	0	4	13
		Permanencia del talento humano	Capacitación	1	1	1	1	1	0	1	1	1	1	1	4	14
			Administración de beneficios	2	1	1	1	1	1	1	1	1	1	1	4	16
		Desvinculación del talento Humano		2	3	1	0	1	1	3	1	3	1	1	4	21
		Administración de nomina		1	1	1	1	1	1	1	1	1	1	1	4	15
		Administración de dietas y viáticos		1	1	1	1	1	1	1	1	1	1	1	4	15
	Gestión de tecnologías de información	Gestión de tecnologías de la información y seguridad informática	Administración de servidores del sistema financiero.	6	7	10	9	9	3	7	7	9	4	7	8	86
			Respaldo y restauración de información de los servidores	6	9	10	9	9	1	9	7	7	4	7	8	86
			Administración de cuentas de correo institucional de los colaboradores.	3	1	1	3	9	1	3	3	1	4	7	8	44

		Procedimiento para mantenimiento software y hardware.	8	7	10	1	7	1	7	3	3	4	1	8	60
		Soporte Ofimático.	3	1	3	3	1	1	1	1	3	4	7	8	36
Gestión administrativa Contable	Administración de adquisición de bienes y servicios		4	3	1	2	1	1	1	1	1	1	4	4	24
	Gestión de activos fijos e inventarios		4	1	1	2	3	1	1	1	1	1	4	4	24
	Gestión de servicios administrativos varios		4	1	1	2	1	1	1	1	1	1	4	4	22

Después de evaluar los subprocesos, se realiza una suma y se establece su nivel de importancia. Una vez identificados los procesos críticos, se definen y evalúan los activos necesarios para llevarlos a cabo.

4.1.3.1. Identificación de activos

Resulta crucial clasificar todos los activos según su función correspondiente. El departamento de Tecnología de la Información de la Cooperativa dispone de diversos recursos de gran importancia para el progreso del proyecto.

Se realizó una clasificación de los activos en dos categorías para facilitar su recopilación: los activos primarios, que incluyen los procesos clave de la cooperativa que son relevantes para el análisis de riesgos y el activo secundario que consta de diversas categorías que incluyen: hardware, software, redes informáticas, personal y estructuras organizativas.

Se utilizó el libro II de Magerit Versión 3, titulado "Catálogo de elementos", como base para la caracterización de los activos de información.

Código activo	Denominación	Descripción	Caracterización	Propietario
Ac - 001	BBDD - sistema financiero	Datos relacionados con las operaciones financieras de la organización.	[D] Datos / Información	Director Financiero
Ac - 002	BBDD – Recaudador de leche	Información referente a los productos con los que cuenta la empresa	[D] Datos / Información	Director Comercial
Ac - 003	Achik Emprende	Sistema con información de emprendimientos.	[SW] Software - Aplicaciones informáticas	Responsable de desarrollo de productos
Ac - 004	Achik Movil	Sistema móvil para que los usuarios puedan realizar sus transacciones	[SW] Software - Aplicaciones informáticas	Responsable de desarrollo de productos
Ac - 005	Servidor de Base de Datos	Para el almacenamiento de datos de los diferentes estados de la aplicación y sus usuarios.	[essential] Activos esenciales	Jefe Departamento Tecnologías de la Información y comunicación
Ac - 006	Sistema Operativo Servidor de Base de Datos	Programa principal sobre el cual se encuentra instalado los diferentes motores de Base de Datos	[SW] Software - Aplicaciones informáticas	Jefe Departamento Tecnologías de la Información y comunicación

Ac - 007	Personal del Departamento de Tecnologías de la Información y Comunicación	Persona encargada de Administrar el Departamento	[P] Personal	Responsable de RRHH
Ac - 008	cableado estructurado	Cuenta con un sistema de cableado estructurado de una forma ordenada y planeada de realizar cableados que permite conectar equipos de procedimiento de datos, computadoras etc.	[COM] Redes de comunicaciones	Jefe Departamento Tecnologías de la Información y comunicación
Ac - 0009	Equipos de control de acceso	Sistema que restringe o permite el acceso de un usuario a un área específica de la cooperativa validando la identificación por medio de diferentes tipos de lectura.	[HW]Equipamiento informático (hardware)	
Ac – 010	Servidor HP DL380 GEN 10	Para el almacenamiento de datos de los diferentes estados de la aplicación y sus usuarios.	[HW]Equipamiento informático (hardware)	

4.1.3.2. Escala de calificación de los activos de información

Para evaluar los activos, se empleó un enfoque mixto que incluye tanto aspectos cuantitativos como cualitativos, cuyos detalles se presentarán en las siguientes tablas:

En términos cuantitativos, se usan valores numéricos, lo que facilita los análisis financieros al permitir una comparación entre los riesgos asumidos y los costos de las posibles soluciones.

Por otro lado, la escala cualitativa emplea una serie de criterios para describir la gravedad de los posibles resultados y la probabilidad de su ocurrencia.

Tabla 4: *Evaluación cuantitativa de los activos*

Valor		Criterio
De 9 a 10	Extremo	Daño extremadamente grave
De 6 a 8	Alto	Daño grave
De 3 a 5	Medio	Daño importante
De 1 a 2	Bajo	Daño menor
0	Despreciable	Irrelevante (No Afecta)

Una vez que se ha determinado la escala de valor, se procede a la evaluación de los activos en base a las dimensiones críticas relacionadas con la seguridad de la información (Confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

El valor total del activo crítico se determinará utilizando la siguiente fórmula:

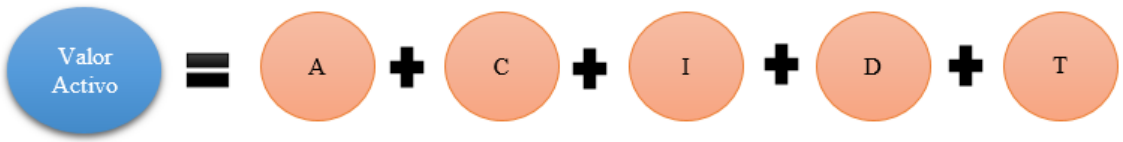


Ilustración 9*:Fórmula para calcular el valor de Activo*

Fuente*: Autoría Propia*

A continuación, se muestra una tabla de intervalo, con la cual se determina si el activo es crítico o no, con una escala detallada de valores que van de 1 al 50, donde 1 a 10 se interpreta como un valor bajo (en términos de riesgo) y 41-50 se interpreta como un valor de riesgo extremo.

Tabla 5: *Escala de valoración de un activo de información. Fuente: (MAGERIT, 2012)*

INTERVALO	CALIFICACIÓN	DESCRIPCION (SE PRODUCE/HACE DAÑO)
De 1 a 10	Bajo	Menor/leve
De 11 a 20	Medio	Importante
De 21 a 30	Alto	Grave
De 31 a 40	Muy alto	Desastroso o muy grave
De 41 a 50	Extremo	daño extremadamente grave

Código activo	Tipo de Activo	Activo	Autenticidad	Confidencialidad	Integridad	Disponibilidad	Trazabilidad	Total
Ac - 001	[D] Datos / Información	BBDD - sistema financiero	10	10	10	10	10	50
Ac - 002		BBDD – Recaudador de leche	9	10	5	7	4	35
Ac - 003	[SW] Software - Aplicaciones informáticas	Achik Emprende	8	9	5	6	3	31
Ac - 004		Achik Móvil	8	10	8	10	6	42
Ac - 005		Servidor de Base de Datos	8	9	10	10	8	45
Ac - 006		Sistema Operativo Servidor de Base de Datos	8	10	8	9	5	40
Ac - 007	[COM] Redes de comunicaciones	Cableado Estructurado	10	9	8	10	7	44
Ac - 008	[HW]Equipamiento informático (hardware)	Equipos de control de acceso	10	9	8	10	3	40
Ac – 009		Servidor HP DL380 GEN 10	10	10	10	10	9	49
Ac – 010	[P] Personal	Personal del Departamento de Tecnologías de la Información y Comunicación	8	10	10	10	10	48

4.1.3.3. Identificación de las amenazas según la metodología MAGERIT

Posteriormente a la identificación de los activos, se avanza hacia la categorización de las amenazas, definiéndolas en términos de su probabilidad de materialización y el perjuicio potencial causado. En esta etapa, se introduce un inventario exhaustivo de amenazas dirigidas a los activos de un sistema de información, en el que se ilustra el código identificativo de la amenaza, las categorías de activos susceptibles a dicha amenaza y las dimensiones de seguridad de la información que podrían verse impactadas.

		DIMENSIONES					ACTIVOS										
Código	Amenaza	A	C	I	D	T	INF	SER	D	K	S	SW	HW	COM	M	AUX	L	p
[N. I]	Fuego				◆								X		X	X	X	
[N.2]	Daños Por Agua				◆								X		X	X	X	
[1.1]	Fuego				◆								X		X	X	X	
[1.2]	Daños Por Agua				◆								X		X	X	X	
[1.5]	Avería De Origen Físico O Lógico				◆							X	X		X	X		
[1.6]	Corte Del Suministro Eléctrico				◆								X		X	X		
[1.8]	Fallo De Servicios De Comunicaciones				◆									X				
[1.10]	Degradación De Los Soportes De Almacenamiento De La Información				◆											X		
[E.1]	Errores De Los Usuarios		◆	◆	◆				X	X	X	X			X			
[E.3]	Errores De Monitorización (Lag)			◆		◆												X
[E.4]	Errores De Configuración			◆					X									
[E.7]	Deficiencia S En La Organización				◆													X
[E.8]	Difusión De Software Dañino		◆	◆	◆							X						
[E.10]	Errores De Secuencia			◆							X	X		X				
[E.14]	Escapes De Información		◆															
[E.15]	Alteración Accidental De La Información			◆					X	X	X	X		X	X			
[E.18]	Destrucción De Información			◆					X	X	X	X		X	X			
[E.19]	Fugas De Información		◆						X	X	X	X		X	X		X	X
[E.20]	Vulnerabilidades De Los Programas (Software)		◆	◆	◆							X						
[E.21]	Errores De Mantenimiento / Actualización De Programas {Software)			◆	◆							X						
[E.23]	Errores De Mantenimiento / Actualización De Equipos				◆								X		X	X		
[E.25]	Pérdida De Equipos		◆		◆								x		x	x		
[E.28]	Lnd Isponibilidad Del Personal				◆													X
[A.4]	Manipulación De La Configuración	◆		◆	◆				X									
[A.5]	Suplantación De La Identidad Del Usuario	◆	◆	◆					X	X	X	X	X	X				
[A.6]	Abuso De Privilegios De Acceso		◆	◆	◆				X	X	X	X	X	X				
[A.8]	Difusión De Software Dañino		◆	◆								X						
[A.10]	Alteración De Secuencia			◆							X	X		X				
[A. 11]	Acceso No Autorizado		◆	◆					X	X	X	X	X	X	X	X	X	
[A.12]	Análisis De Tráfico		◆											X				
[A.14]	Interceptación De Información (Escucha)		◆											X				
[A.15]	Modificación Deliberada De La Información			◆					X	X	X	X		X	X		X	
[A.18]	Destrucción De Información		◆						X	X	X	X			X		X	
[A.22]	Manipulación De Programas		◆	◆	◆							X						
[A.23]	Manipulación De Los Equipos		◆		◆								X		X	X		
[A.24]	Denegación De Servicio				◆						X		X	X				
[A.25]	Robo		◆		◆								X		X	X		
[A.26]	Ataque Destructivo				◆								X		X	X	X	
[A.27]	Ocupación Enemiga		◆		◆												X	
[A.28]	Isponibilidad Del Personal				◆													X
[A.29]	Extorsión		◆	◆	◆													X
[A.30]	Ingeniería Social (Picaresca)		◆	◆	◆													X

Ilustración 10: *Catalogo de amenazas; Fuente: (MAGERIT, 2012, págs. 25-47)*

CÓDIGO	ACTIVO	COD. A.	AMENAZA
Ac - 001	BBDD - sistema financiero	[I.5]	Avería de origen físico o lógico
		[I.10]	Degradación de los soportes de almacenamiento de la información
		[E.1]	Errores de los usuarios
		[E.4]	Errores de configuración
		[E.10]	Errores de secuencia
		[E.15]	Alteración accidental de la información
		[E.18]	Destrucción de información
		[E.19]	Fugas de Información
		[E.28]	Indisponibilidad del personal
		[A.5]	Suplantación de la identidad del usuario
		[A.11]	Acceso no autorizado
		[A.18]	Destrucción de información
		[A.25]	Robo
		[A.29]	Extorsión
Ac – 004	Achik Móvil	[A.5]	Suplantación de identidad del Usuario
		[A.6]	Abuso de privilegios de acceso
		[A.26]	Ataque destructivo
		[E.4]	Errores de configuración
		[E.8]	Difusión de software dañino
		[A.11]	Acceso no Autorizado
Ac - 002	Servidor de Base de Datos	[N.1]	Fuego
		[N.2]	Daños por agua
		[I.1]	Fuego
		[I.2]	Daños por agua
		[I.5]	Avería de origen físico o lógico
		[I.6]	Corte del suministro eléctrico
		[I.10]	Degradación de los soportes de almacenamiento de la información
		[E.1]	Errores de los usuarios
		[E.4]	Errores de configuración
		[E.8]	Difusión de software dañino
		[E.18]	Destrucción de información
		[E.20]	Vulnerabilidades de los programas (software)
		[E.23]	Errores de mantenimiento / actualización de equipos
		[A.7]	Uso no previsto
		[A.8]	Difusión de software dañino
		[A.12]	Análisis de tráfico
		[E.19]	Fugas de Información
		[E.24]	Caída del sistema por agotamiento de recursos

		[A.24]	Denegación de servicio
Ac - 005	Cableado Estructurado	[I.8]	Avería de origen físico o lógico
		[I.6]	Corte del suministro eléctrico
		[E.1]	Fallos de servicios de comunicación
		[A.24]	Denegación de Servicio
		[A.12]	Análisis del trafico
Ac - 007	Servidor HP DL380 GEN 10	[I.5]	Avería de origen físico o lógico
		[I.8]	Fallo de servicios de comunicaciones
		[I.10]	Degradación de los soportes de almacenamiento de la información
		[E.1]	Errores de los usuarios
		[E.3]	Errores de monitorización (log)
		[E.4]	Errores de configuración
		[E.8]	Difusión de software dañino
		[E.15]	Alteración accidental de la información
		[E.18]	Destrucción de información
		[E.20]	Vulnerabilidades de los programas (software)
		[E.21]	Errores de mantenimiento / actualización de programas (software)
		[A.4]	Manipulación de la configuración
		[A.5]	Suplantación de la identidad del usuario
		[A.10]	Alteración de secuencia
		[A.18]	Destrucción de información
Ac - 010	Director de Departamento de Tecnologías de la Información y Comunicación	[A.28]	Indisponibilidad del personal
		[A.29]	Extorción
		[A.30]	Ingeniería Social
		[E.19]	Fuga de Información
		[E.7]	Deficiencia en la Organización
		[E.3]	Errores de monitorización
		[A.25]	Robo

4.1.3.4. Análisis y gestión de riesgos

Procediendo al análisis de las amenazas potenciales a los activos, el siguiente paso es la evaluación de estos activos. En la matriz de evaluación, se registran los activos que están actualmente en posesión de la organización, junto con las amenazas asociadas y la calificación de la probabilidad de que dichas amenazas se materialicen. Además, se evalúa el nivel de impacto resultante y el grado de riesgo correspondiente si estas amenazas llegaran a concretarse.

Estas evaluaciones serán cuantificadas según los criterios especificados en las tablas de valoración expuestas a continuación.

El proceso de evaluación de amenazas y activos se realiza de la siguiente manera:

- Identificación de Activos: Se identifican y enumeran todos los activos importantes de la empresa.
- Identificación de Amenazas: Se identifican las amenazas potenciales a cada activo.
- Evaluación de la Probabilidad de la Amenaza: Se evalúa la probabilidad de que cada amenaza identificada ocurra.
- Evaluación del Impacto de la Amenaza: Se evalúa el potencial impacto que cada amenaza tendría sobre el activo correspondiente.
- Calificación del Riesgo: Finalmente, se asigna una calificación de riesgo a cada amenaza, basada en la combinación de la probabilidad de la amenaza y el impacto potencial.

Las calificaciones específicas para cada uno de estos aspectos se determinan en función de las tablas de valoración proporcionadas, que asignan valores numéricos a diferentes niveles de probabilidad, impacto y riesgo.

Tabla 6: *Rango de Valoración para determinar la probabilidad de ocurrencia; Autor: Propio*

Probabilidad	Descripción	Frecuencia	Valor
Raro	Podría presentarse solo en circunstancias excepcionales.	No se presenta en los últimos 5 años	1
Improbable	Probabilidad de ocurrencia baja	1 vez en 5 años	2
Posible	Podría presentarse en algún momento	1 en 2 Años	3
Probable	Se puede presentar frecuentemente	Una vez al Año	4
Casi Seguro	Probabilidad de ocurrencia muy Alta	Más de 1 vez al Año	5

Tabla 7: Rango de valoración para determinar el impacto; Autor: Propio

Impacto	Descripción	Valor
Insignificante	La materialización del riesgo contiene efectos nulos, es decir que no afecta el cumplimiento del objetivo.	1
Menor	Al presentarse tendría consecuencias mínimas sobre la empresa.	2
Moderado	Si se presentara tendría medianas consecuencias sobre la empresa.	3
Mayor	La materialización del riesgo causa un daño mayor en la ejecución de procesos y el cumplimiento de los objetivos.	4
Catastrófico	La materialización del riesgo dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos.	5

El cálculo de intervalos se obtiene mediante porcentajes, que definen el riesgo que corresponde al valor del riesgo máximo: Valor de Probabilidad multiplicado por el Impacto:

Riesgo	Descripción	Nivel
Bajo	El riesgo es aceptable	1 - 6
Medio	El riesgo es tolerable	7- 14
Alto	El riesgo es inadmisible, requiere la implementación inmediata de controles en la entidad	15 - 25

Tabla 8: Matriz de Riesgo

ACTIVO	COD. A.	AMENAZA	Impacto	Probabilidad	Riesgo
BBDD - sistema financiero	[I.5]	Avería de origen físico o lógico	3	2	6
	[I.10]	Degradación de los soportes de almacenamiento de la información	5	4	20
	[E.1]	Errores de los usuarios	4	3	12
	[E.4]	Errores de configuración	5	4	20
	[E.10]	Errores de secuencia	1	2	3
	[E.15]	Alteración accidental de la información	5	2	10
	[E.18]	Destrucción de información	5	2	10
	[E.19]	Fugas de Información	5	3	15
	[E.28]	Indisponibilidad del personal	5	2	10
	[A.5]	Suplantación de la identidad del usuario	4	3	12
	[A.11]	Acceso no autorizado	5	4	20
	[A.18]	Destrucción de información	5	2	10
	[A.25]	Robo	4	1	4
Achik Móvil	[A.5]	Suplantación de identidad del Usuario	5	3	15
	[A.6]	Abuso de privilegios de acceso	4	1	4
	[A.26]	Ataque destructivo	4	2	8
	[E.4]	Errores de configuración	4	1	4
	[E.8]	Difusión de software dañino	5	4	20
	[A.11]	Acceso no Autorizado	5	3	15
Servidor de Base de Datos	[N.1]	Fuego	5	1	5
	[N.2]	Daños por agua	5	1	5
	[I.5]	Avería de origen físico o lógico	4	1	4
	[I.6]	Corte del suministro eléctrico	5	3	15
	[I.10]	Degradación de los soportes de almacenamiento de la información	5	1	5
	[E.1]	Errores de los usuarios	5	1	4
	[E.4]	Errores de configuración	4	2	8
	[E.8]	Difusión de software dañino	5	4	20
	[E.18]	Destrucción de información	5	1	5
	[E.20]	Vulnerabilidades de los programas (software)	4	1	4
	[E.23]	Errores de mantenimiento / actualización de equipos	3	1	3
	[A.7]	Uso no previsto	4	2	8
	[A.12]	Análisis de tráfico	2	1	2
	[E.19]	Fugas de Información	5	1	5

	[E.24]	Caída del sistema por agotamiento de recursos	5	1	5
	[A.24]	Denegación de servicio	5	2	10
Cableado Estructurado	[I.8]	Avería de origen físico o lógico	5	3	15
	[I.6]	Corte del suministro eléctrico	5	2	10
	[E.1]	Fallos de servicios de comunicación	5	3	15
	[A.24]	Denegación de Servicio	4	1	4
	[A.12]	Análisis del trafico	4	1	4
Servidor HP DL380 GEN 10	[I.5]	Avería de origen físico o lógico	4	2	8
	[I.8]	Fallo de servicios de comunicaciones	4	1	4
	[I.10]	Degradación de los soportes de almacenamiento de la información	5	2	10
	[E.1]	Errores de los usuarios	3	1	3
	[E.3]	Errores de monitorización (log)	3	1	3
	[E.4]	Errores de configuración	4	1	4
	[E.8]	Difusión de software dañino	5	3	15
	[E.15]	Alteración accidental de la información	5	1	5
	[E.18]	Destrucción de información	5	1	5
	[E.20]	Vulnerabilidades de los programas (software)	4	1	4
	[E.21]	Errores de mantenimiento / actualización de programas (software)	4	1	4
	[A.4]	Manipulación de la configuración	5	2	10
	[A.5]	Suplantación de la identidad del usuario	4	1	4
	[A.10]	Alteración de secuencia	3	2	6
	[A.18]	Destrucción de información	5	2	10
Director de Departamento de Tecnologías de la Información y Comunicación	[A.28]	Indisponibilidad del personal	5	2	10
	[A.29]	Extorción	5	2	10
	[A.30]	Ingeniería Social	4	1	4
	[E.19]	Fuga de Información	5	2	10
	[E.7]	Deficiencia en la Organización	5	1	5
	[E.3]	Errores de monitorización	3	1	3
	[A.25]	Robo	5	1	5

4.1.3.5. Salvaguardas y contramedidas

En la tabla siguiente, se establecen las medidas de protección proporcionadas por MAGERIT para cada uno de los activos, además de las diversas amenazas potenciales que pueden manifestarse en cualquier momento, ya sea interna o externamente, en la organización.

La intención principal detrás de este análisis exhaustivo es facilitar la implementación de sistemas de control efectivos y proporcional a los riesgos detectados. De este modo, en caso de que se materialicen incidentes perjudiciales, la organización tiene la capacidad de responder de una manera rápida y adecuada, reduciendo la probabilidad de daño a sus operaciones y, en consecuencia, minimizando el impacto a la continuidad de sus actividades.

ACTIVO	COD. A.	AMENAZA	Riesgo	SALVAGUARDA
BBDD- sistema financiero	[I.10]	Degradación de los soportes de almacenamiento de la información	20	- (HW) Protección de los Equipos Informáticos - Se aplican perfiles de seguridad
	[E.1]	Errores de los usuarios	12	PS.AT Formación y concienciación
	[E.4]	Errores de configuración	20	H. tools.CC Herramienta de chequeo de configuración
	[E.15]	Alteración accidental de la información	10	- D Protección de la Información - H. tools Herramientas de seguridad
	[E.18]	Destrucción de información	10	Aseguramiento de la disponibilidad
	[E.19]	Fugas de Información	15	- MP. A Aseguramiento de la disponibilidad - MP.IC Protección criptográfica del contenido
	[E.28]	Indisponibilidad del personal	10	- PS Gestión del Personal - PS. A Aseguramiento de la disponibilidad
	[A.5]	Suplantación de la identidad del usuario	12	- D Protección de la Información - D.I Aseguramiento de la integridad
	[A.11]	Acceso no autorizado	20	D. I Aseguramiento de la integridad
Achik Móvil	[A.5]	Suplantación de identidad del Usuario	15	D.I Aseguramiento de la integridad
	[A.26]	Ataque destructivo	8	HW. A Aseguramiento de la disponibilidad
	[E.8]	Difusión de software dañino	20	SW Protección de las Aplicaciones Informáticas
	[A.11]	Acceso no Autorizado	15	D. I Aseguramiento de la integridad
Servidor de Base de Datos	[I.6]	Corte del suministro eléctrico	15	L.A Aseguramiento de la disponibilidad
	[E.4]	Errores de configuración	8	H. tools.CC Herramienta de chequeo de configuración
	[E.8]	Difusión de software dañino	20	SW Protección de las Aplicaciones Informáticas

	[A.7]	Uso no previsto	8	H Protecciones Generales
	[A.24]	Denegación de servicio	10	
Cableado Estructurado	[I.8]	Avería de origen físico o lógico	15	- HW Protección de los Equipos Informáticos - HW. A Aseguramiento de la disponibilidad - SW Protección de las Aplicaciones Informáticas
	[I.6]	Corte del suministro eléctrico	10	L.A Aseguramiento de la disponibilidad
	[E.1]	Fallos de servicios de comunicación	15	- COM.A Aseguramiento de la disponibilidad - COM Protección de las Comunicaciones
Servidor HP DL380 GEN 10	[I.5]	Avería de origen físico o lógico	8	H Protecciones Generales
	[I.10]	Degradación de los soportes de almacenamiento de la información	10	- H Protecciones Generales - HW Protección de los Equipos Informáticos - D Protección de la Información
	[E.8]	Difusión de software dañino	15	SW Protección de las Aplicaciones Informáticas
	[A.4]	Manipulación de la configuración	10	SW.SC Se aplican perfiles de seguridad
	[A.18]	Destrucción de información	10	Aseguramiento de la disponibilidad
Director de Departamento de Tecnologías de la Información y Comunicación	[A.28]	Indisponibilidad del personal	10	-PS Gestión del Personal -PS.AT Formación y concienciación PS. A -Aseguramiento de la disponibilidad
	[A.29]	Extorción	10	PS.AT Formación y concienciación
	[E.19]	Fuga de Información	10	MP. A Aseguramiento de la disponibilidad

Una vez finalizada la evaluación de los procesos, subprocesos y activos, así como la identificación y valoración de las amenazas con sus correspondientes medidas de protección, como se puede apreciar en las tablas previamente presentadas, se procede a la elaboración de una matriz integrada.

En esta matriz se reflejan los procesos críticos derivados de la evaluación realizada en la cooperativa.

Estos procesos estarán sustentados por los activos que presenten un alto grado de relevancia y significación dentro de la estructura operativa de la organización. Estos activos críticos son esenciales para asegurar una ejecución eficiente y efectiva de dichos procesos, proporcionando la infraestructura, información, o capacidades necesarias para el desarrollo exitoso de las actividades previstas.

Proceso	Subproceso	ACTIVO	COD. A.	AMENAZA	Riesgo	SALVAGUARDA
Administración de Contabilidad	Generación de estados financieros	BBDD- sistema financiero	[I.10]	Degradación de los soportes de almacenamiento de la información	20	- (HW) Protección de los Equipos Informáticos - Se aplican perfiles de seguridad
			[E.1]	Errores de los usuarios	12	PS.AT Formación y concienciación
			[E.4]	Errores de configuración	20	H. tools.CC Herramienta de chequeo de configuración
			[E.15]	Alteración accidental de la información	10	- D Protección de la Información - H. tools Herramientas de seguridad
			[E.18]	Destrucción de información	10	Aseguramiento de la disponibilidad
			[E.19]	Fugas de Información	15	- MP. A Aseguramiento de la disponibilidad - MP.IC Protección criptográfica del contenido
			[E.28]	Indisponibilidad del personal	10	- PS Gestión del Personal - PS. A Aseguramiento de la disponibilidad
			[A.5]	Suplantación de la identidad del usuario	12	- D Protección de la Información - D.I Aseguramiento de la integridad
			[A.11]	Acceso no autorizado	20	D. I Aseguramiento de la integridad
Gestión de tecnologías de la información y seguridad informática	Procedimiento para mantenimiento software y hardware.	Achik Móvil	[A.5]	Suplantación de identidad del Usuario	15	D.I Aseguramiento de la integridad
			[A.26]	Ataque destructivo	8	HW. A Aseguramiento de la disponibilidad
			[E.8]	Difusión de software dañino	20	SW Protección de las Aplicaciones Informáticas
			[A.11]	Acceso no Autorizado	15	D. I Aseguramiento de la integridad
	Administración de servidores del sistema financiero.	Servidor de Base de Datos	[I.6]	Corte del suministro eléctrico	15	L.A Aseguramiento de la disponibilidad
			[E.4]	Errores de configuración	8	H. tools.CC Herramienta de chequeo de configuración
			[E.8]	Difusión de software dañino	20	SW Protección de las Aplicaciones Informáticas
			[A.7]	Uso no previsto	8	H Protecciones Generales
			[A.24]	Denegación de servicio	10	

		Cableado Estructurado	[I.8]	Avería de origen físico o lógico	15	- HW Protección de los Equipos Informáticos - HW. A Aseguramiento de la disponibilidad - SW Protección de las Aplicaciones Informáticas
			[I.6]	Corte del suministro eléctrico	10	L.A Aseguramiento de la disponibilidad
			[E.1]	Fallos de servicios de comunicación	15	- COM.A Aseguramiento de la disponibilidad - COM Protección de las Comunicaciones
	Respaldo y restauración de información de los servidores	Servidor HP DL380 GEN 10	[I.5]	Avería de origen físico o lógico	8	H Protecciones Generales
			[I.10]	Degradación de los soportes de almacenamiento de la información	10	- H Protecciones Generales - HW Protección de los Equipos Informáticos - D Protección de la Información
			[E.8]	Difusión de software dañino	15	SW Protección de las Aplicaciones Informáticas
			[A.4]	Manipulación de la configuración	10	SW.SC Se aplican perfiles de seguridad
			[A.18]	Destrucción de información	10	Aseguramiento de la disponibilidad
	Soporte Ofimático.	Director de Departamento de Tecnologías de la Información y Comunicación	[A.28]	Indisponibilidad del personal	10	-PS Gestión del Personal -PS.AT Formación y concienciación PS. A -Aseguramiento de la disponibilidad
			[A.29]	Extorción	10	PS.AT Formación y concienciación
			[E.19]	Fuga de Información	10	MP. A Aseguramiento de la disponibilidad

4.1.4. Etapa 3: Definir Las Estrategias Para La Gestión De La Continuidad Del Negocio

Tras la identificación y asignación de los activos de importancia crítica dentro de sus respectivos procesos operativos, se procede a la elaboración de una matriz de contingencia. En esta se delinean estrategias de recuperación tecnológica, con el objetivo de proporcionar una respuesta óptima y eficaz a las exigencias de la mitigación de riesgos. También incorpora criterios como el Tiempo Objetivo de Restauración (RTO) y el Punto Objetivo de Recuperación (RPO) para los distintos procesos.

***Tabla 9**: Estrategias para los procesos críticos de Administración de Contabilidad; Autor: Propio*

Proceso	Subproceso	Estrategia Requerida	Tiempo Máximo de recuperación (RTO)	Tiempo máximo de obtención de respaldos (RPO)
Administración de Contabilidad	Generación de estados financieros	- Documentación contable que refleja la situación de la organización - Definición del personal encargado en la generación de estados financieros. - Contar con un sistema de contabilidad manual de respaldo o un sistema de contabilidad basado en la nube. - Backup Regular y Recuperación de Datos (Copia de seguridad de los datos) - Automatización de Procesos - Seguridad de la Información - Auditoría y cumplimiento - Formación y Sensibilización del personal - Recuperación de desastres	4 horas	1 horas

Tabla 10: *Estrategias para los procesos críticos de Gestión de tecnología de la información y seguridad informática;* ***Autor:*** *Propio*

Proceso	Subproceso	Estrategia Requerida	Tiempo Máximo de recuperación (RTO)	Tiempo máximo de obtención de respaldos (RPO)
Gestión de tecnologías de la información y seguridad informática	Procedimiento para mantenimiento software y hardware.	- Copias de Seguridad y Recuperación de Datos - Redundancia de Hardware y Software - Actualizaciones y Parches de Software - Manejo de Proveedores de Servicios - Capacitación del Personal	4 hora	1 hora
	Administración de servidores del sistema financiero.	- Copias de Seguridad y Recuperación de Datos - Plan de aseguramiento, capacidad y disponibilidad de la infraestructura tecnológica (instalación, configuración y administración de hardware, bases de datos, repositorios, entre otros recursos tecnológicos) con la que cuenta la institución. - Redundancia de Servidores - Plan de recuperación de desastres - Mantenimiento regular de los Servidores. - Gestión de Configuración del Servidor - Implementación de Clusters de Servidores	4 hora	1 hora
	Respaldo y restauración de información de los servidores	- Política de Respaldo Regular y Automatizado. - Estrategia de Respaldo 3-2-1 (tener al menos tres copias totales de tus datos, dos de los cuales se almacenan en diferentes dispositivos o ubicaciones y una copia fuera de sitio) - Plan de mantenimiento preventivo y correctivo de hardware y software de la Infraestructura Tecnológica. - Políticas de procedimiento de seguridad. - Pruebas de Restauración - Respaldo de Configuraciones de los Servidores	4 hora	1 hora

Todas estas estrategias de recuperación mencionadas para cada proceso están diseñadas para garantizar la continuidad de las operaciones en caso de una interrupción. Para que el plan de continuidad del negocio sea efectivo, depende únicamente de la periodicidad con la que se revise y actualice dicho plan.

Estas estrategias ayudarán a garantizar que la cooperativa de ahorro y crédito Achik Inti pueda mantener y recuperar rápidamente las operaciones en caso de una interrupción en la administración de la Gestión de tecnologías de la información y seguridad informática.

Este enfoque proactivo de gestión de la continuidad de negocio no solo minimiza el tiempo de inactividad durante una interrupción, sino que también garantiza que la Cooperativa de Ahorro y Crédito “Achik Init” esté preparada para enfrentar y recuperarse de una amplia gama de escenarios de interrupción, maximizando así su resiliencia operacional.

Conclusiones y Recomendaciones

A través del estudio teórico de las normativas del plan de continuidad de negocio, se ha logrado obtener una comprensión integral de las regulaciones y estándares vigentes en materia de continuidad empresarial. Mediante el análisis de diferentes marcos normativos y directrices, se ha identificado la importancia de contar con un plan sólido y efectivo que permita a la Cooperativa de Ahorro y Crédito Achik Inti Ltda. afrontar situaciones de riesgo y preservar la continuidad de sus operaciones. El conocimiento adquirido ha sentado las bases para el desarrollo de un plan de continuidad de negocio adaptado a las necesidades y particularidades de la cooperativa, en cumplimiento con las regulaciones y mejores prácticas establecidas.

Mediante el análisis del entorno y la identificación de los riesgos internos que presenta la Cooperativa de Ahorro y Crédito Achik Inti Ltda., se ha logrado una comprensión detallada de los factores internos que pueden generar interrupciones en el servicio. Mediante un análisis, se han identificado y evaluado los riesgos asociados a aspectos como la infraestructura tecnológica, los procesos operativos, la gestión de recursos humanos y la seguridad de la información. La detección de estos riesgos internos ha permitido establecer una base sólida para el diseño de un plan de continuidad de negocio que aborde específicamente las amenazas internas y proporcione medidas efectivas para mitigar su impacto, garantizando así la continuidad operativa de la cooperativa.

En conclusión, con la elaboración del plan de continuidad de negocio para la Cooperativa de Ahorro y Crédito Achik Inti Ltda., se ha logrado diseñar una herramienta preventiva integral que asegura la continuidad de sus procesos frente a incidentes existentes. Este plan ha sido desarrollado tomando en cuenta los riesgos previamente identificados y los estándares en el campo de la continuidad empresarial. Se han establecido estrategias para los procesos más críticos, las cuales permiten una respuesta eficiente y efectiva ante diferentes escenarios de interrupción del

servicio. La implementación de este plan brindará a la cooperativa la capacidad de minimizar los impactos de los incidentes, proteger los activos, mantener la confianza de los socios y clientes, y garantizar la continuidad de las operaciones en el cumplimiento de su misión y objetivos organizacionales.

Bibliografía

Achik Inti. (s.f). *AchikInti.fin.ec*. Obtenido de https://achikinti.fin.ec/Home/knowus

Bedoya, D. E. (01 de 01 de 2014). *repositorio.uta.edu.ec.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/6987/1/Tesis_t871mif.pdf

Camacho, J. A. (01 de 03 de 2022). *repositorio.pucesa.edu.ec.* Obtenido de repositorio.pucesa.edu.ec: https://repositorio.pucesa.edu.ec/bitstream/123456789/3565/1/77861.pdf

Carolina, M. M. (01 de 01 de 2013). *dspace.uniandes.edu.ec.* Obtenido de dspace.uniandes.edu.ec: https://dspace.uniandes.edu.ec/bitstream/123456789/4522/1/TUAMIE001-2013.pdf

Castro, M. I., Moràn, G. L., Navarrete, D. S., Cruzatty, J. E., Anzúles, G. R., Mero, C. J., . . . Merino, M. A. (01 de 10 de 2018). *3ciencias.com.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Cruz Mendoza, J. C., Jalpilla Jiménez, R., & Ramírez, S. M. (2016). *ru.dgb.unam.mx/.* Obtenido de repositorio.unam.mx: https://ru.dgb.unam.mx/handle/DGB_UNAM/TES01000710742

Cruz, P. S. (01 de 08 de 2012). *interempresas.net.* Obtenido de interempresas.net: https://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/87942/Continuidad_Negocio-ISO-22301.pdf

Duarte, J. C. (01 de 09 de 2020). *repository.unipiloto.edu.co.* Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9403/Trabajo%20de%20grado.pdf?sequence=1

Guagalango Vega, R., & Moscoso Montalvo, P. (2014). Evaluacion Tecnica de la Seguridad Informatica del Data Center de la Escuela Politecnica del Ejercito. *Ecuela Politecnica del Ejercito*.

ISOTools Excellence. (15 de marzo de 2018). *www.pmg-ssi.com*. Obtenido de www.pmg-ssi.com: https://www.pmg-ssi.com/2018/03/iso-22301-gestionar-continuidad-negocio/

MAGERIT. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de informacion Libro II - Catálogo de Elementos.* Madrid.

Molina, K. G., & Sánchez, E. R. (1 de 3 de 2015). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Muñoz, V. A., & Llanes, L. E. (01 de 07 de 2017). *repositorio.uca.edu.ni.* Obtenido de http://repositorio.uca.edu.ni/4684/1/UCANI5010.pdf

Pincay Ronquillo, J. Y. (01 de 04 de 2021). *repositorio.ug.edu.ec.* Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/51868/1/TESIS%20JENNIFFER%20PINCAY%20RONQUILLO.pdf

Rojas Bustamante, J. D. (01 de 01 de 2017). *dspace.udla.edu.ec/.* Obtenido de http://dspace.udla.edu.ec/bitstream/33000/7531/1/UDLA-EC-TMGSTI-2017-08.pdf

Tayo, L. P. (01 de 08 de 2017). *ciateq.repositorioinstitucional.mx.* Obtenido de https://ciateq.repositorioinstitucional.mx/jspui/bitstream/1020/86/1/RudasTayoLeidyP%20MDGPI%202017.pdf

Yarlequé Gutiérrez, A. (01 de 01 de 2019). *repositorioacademico.upc.edu.pe.* Obtenido de repositorioacademico.upc.edu.pe: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625709/yarleque_ga.pdf?sequence=1&isAllowed=y

Zapata Vásquez, C. F. (27 de 08 de 2020). *repositorio.espe.edu.ec.* Obtenido de Plan de Continuidad de Negocio BCP: https://repositorio.espe.edu.ec/bitstream/21000/22534/1/T-ESPE-043859.pdf

ACHIK INTI Ltda.
Cooperativa de Ahorro y Crédito

MANUAL DE CONTINUIDAD DE NEGOCIO

2023

Cooperativa de Ahorro y Credito ACHIK INTI Ltda.

INTRODUCCIÓN

La cooperativa de Ahorro y Crédito ACHIK INTI se encuentra expuesta a desafíos sustanciales que incrementan la posibilidad de incidentes que interrumpan la operatividad normal de sus servicios.

Tras una exhaustiva evaluación de los riesgos y un entendimiento más detallado de las peculiaridades y el comportamiento de la organización, se puede desplegar el plan de continuidad de operaciones empresariales.

En el presente manual de Plan de Continuidad de Negocio (BCP), se abarca planes, procedimientos y estructuras diseñadas para asegurar la continuidad de los servicios vitales de la compañía frente a cualquier eventualidad en el ámbito tecnológico.

1. OBJETIVOS

2.1.OBJETIVO GENERAL

Elevar la eficiencia de la gestión administrativa y operativa de la Cooperativa de Ahorro y ACHIK INTI Ltda., través de la implementación del plan de continuidad de negocio, que permitirá reanudar de manera efectiva los servicios vitales de la organización.

2.2.OBJETIVOS ESPECÍFICOS

- Reducir al mínimo el grado de discontinuidad en las operaciones vinculadas a los procesos vitales de la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda.
- Garantizar la restitución inmediata de las operaciones que han sido impactadas por un incidente, mitigando así los riesgos que amenazan la disponibilidad continua de dichas operaciones.
- Garantizar la seguridad de los activos, personal, tecnología y los diferentes procesos que conforman a la organización.

3. ALCANCE

La propuesta del plan de continuidad de negocio para la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda. se centra en la creación de una documentación específica que establezca el protocolo a seguir en caso de un evento catastrófico o cualquier otro incidente que pueda provocar la interrupción del servicio. Este plan detallará cada una de las obligaciones individuales y los procedimientos requeridos para reanudar el servicio en el plazo más corto posible. Todos estos

planes y procedimientos se rigen por los lineamientos establecidos por un BCP y están en concordancia con las mejores prácticas de la norma ISO 22301.

Es vital disponer de un BCP sólido, coherente y actualizado, ya que esto facilitará la reducción del tiempo de interrupción de los servicios informáticos de la cooperativa ACHIK INITI Ltda., en caso de situaciones catastróficas que podrían amenazar los recursos vitales de la organización. Este manual será elaborado específicamente para el departamento de TI, dado que, tras el análisis y la gestión de riesgos, hemos determinado que la mayoría de los procesos financieros están respaldados por dicho departamento.

4. POLÍTICA

Las directrices del BCP tienen como objetivo definir las habilidades de acción y respuesta ante la aparición de una contingencia o catástrofe que pueda llevar a la interrupción de las operaciones o servicios. De este modo, se asegurará la protección de los activos, los intereses de los socios, la reputación de la institución, entre otros aspectos esenciales.

5. REQUISITOS

- Que todo el personal administrativo y de servicio tengan conocimiento de un Plan de Continuidad de Negocio y su existencia dentro de la organización.
- Concienciación de todo el personal administrativo y de servicio sobre los procesos con los que cuenta la institución y las posibles amenazas que podrían presentarse y afectar a la cooperativa.
- Disponibilidad de los recursos necesarios para llevar a cabo el plan de respuesta rápida ante la suspensión de servicios o incidentes.

6. PRINCIPIOS

Salvaguardar los recursos más críticos de la cooperativa ACHIK INTI de diversos incidentes o desastres, sean estos naturales o causados por el hombre, que puedan surgir y provocar efectos adversos, ya sean financieros, de confianza, de pérdidas materiales, entre otros, en la organización debido a la interrupción de servicios.

Minimizar el riesgo o incidente que se llegara a presentar dentro de la organización, mediante un plan que permita volver a recuperar el servicio en el menor tiempo posible.

7. ESTRATEGIA DE PLAN DE RECUPERACIÓN ANTE INCIDENTES EN LA COOPERATIVA DE AHORRO Y CRÉDITO CAÑAR LTDA.

7.1.Resumen Del Análisis Y Gestión De Riesgos

Esta sección proporciona un resumen del análisis y la gestión de riesgos que se han llevado a cabo en la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda. Todos los detalles y descubrimientos relevantes se encuentran exhaustivamente documentados en el estudio de investigación de la tesis titulada**: "*Diseñar un Plan de Continuidad de Negocio para la Cooperativa de Ahorro y Crédito Achik Inti Ltda.*"**

7.2.Resultado del Análisis y gestión de riesgo.

Tras llevar a cabo el análisis y la gestión de riesgos, donde se identificaron los procesos esenciales de la organización, se alcanzaron los siguientes hallazgos:

- Administración de Contabilidad
  - Generación de estados financieros
- Gestión de tecnologías de la información y seguridad informática
  - Procedimiento para mantenimiento software y hardware.
  - Administración de servidores del sistema financiero.
  - Respaldo y restauración de información de los servidores

Los procesos previamente descritos se califican como los más críticos, debido a su potencial influencia en la continuidad operacional y sus posibles repercusiones financieras, humanas en la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda.

Proceso	Subproceso	ACTIVO	COD. A.	AMENAZA	Riesgo	SALVAGUARDA
Administración de Contabilidad	Generación de estados financieros	BBDD- sistema financiero	[I.10]	Degradación de los soportes de almacenamiento de la información	20	- (HW) Protección de los Equipos Informáticos - Se aplican perfiles de seguridad
			[E.1]	Errores de los usuarios	12	PS.AT Formación y concienciación
			[E.4]	Errores de configuración	20	H. tools.CC Herramienta de chequeo de configuración
			[E.15]	Alteración accidental de la información	10	- D Protección de la Información - H. tools Herramientas de seguridad
			[E.18]	Destrucción de información	10	Aseguramiento de la disponibilidad
			[E.19]	Fugas de Información	15	- MP. A Aseguramiento de la disponibilidad - MP.IC Protección criptográfica del contenido
			[E.28]	Indisponibilidad del personal	10	- PS Gestión del Personal - PS. A Aseguramiento de la disponibilidad
			[A.5]	Suplantación de la identidad del usuario	12	- D Protección de la Información - D.I Aseguramiento de la integridad
			[A.11]	Acceso no autorizado	20	D. I Aseguramiento de la integridad
Gestión de tecnologías de la información y seguridad informática	Procedimiento para mantenimiento software y hardware.	Achik Móvil	[A.5]	Suplantación de identidad del Usuario	15	D.I Aseguramiento de la integridad
			[A.26]	Ataque destructivo	8	HW. A Aseguramiento de la disponibilidad
			[E.8]	Difusión de software dañino	20	SW Protección de las Aplicaciones Informáticas
			[A.11]	Acceso no Autorizado	15	D. I Aseguramiento de la integridad
	Administración de servidores del sistema financiero.	Servidor de Base de Datos	[I.6]	Corte del suministro eléctrico	15	L.A Aseguramiento de la disponibilidad
			[E.4]	Errores de configuración	8	H. tools.CC Herramienta de chequeo de configuración
			[E.8]	Difusión de software dañino	20	SW Protección de las Aplicaciones Informáticas
			[A.7]	Uso no previsto	8	H Protecciones Generales
			[A.24]	Denegación de servicio	10	

		Cableado Estructurado	[I.8]	Avería de origen físico o lógico	15	- HW Protección de los Equipos Informáticos - HW. A Aseguramiento de la disponibilidad - SW Protección de las Aplicaciones Informáticas
			[I.6]	Corte del suministro eléctrico	10	L.A Aseguramiento de la disponibilidad
			[E.1]	Fallos de servicios de comunicación	15	- COM.A Aseguramiento de la disponibilidad - COM Protección de las Comunicaciones
	Respaldo y restauración de información de los servidores	Servidor HP DL380 GEN 10	[I.5]	Avería de origen físico o lógico	8	H Protecciones Generales
			[I.10]	Degradación de los soportes de almacenamiento de la información	10	- H Protecciones Generales - HW Protección de los Equipos Informáticos - D Protección de la Información
			[E.8]	Difusión de software dañino	15	SW Protección de las Aplicaciones Informáticas
			[A.4]	Manipulación de la configuración	10	SW.SC Se aplican perfiles de seguridad
			[A.18]	Destrucción de información	10	Aseguramiento de la disponibilidad
	Soporte Ofimático.	Director de Departamento de Tecnologías de la Información y Comunicación	[A.28]	Indisponibilidad del personal	10	-PS Gestión del Personal -PS.AT Formación y concienciación PS. A -Aseguramiento de la disponibilidad
			[A.29]	Extorción	10	PS.AT Formación y concienciación
			[E.19]	Fuga de Información	10	MP. A Aseguramiento de la disponibilidad

8. ESTRATEGIA DE CONTINUIDAD DE NEGOCIO

Se establecen los protocolos operativos para llevar a cabo cada una de las acciones pertinentes, de modo que se asegure la continuidad de los procesos y la estabilidad de los servicios ante cualquier incidente no previsto.

A continuación, se detalla el procedimiento a seguir para garantizar la continuidad de negocio en caso de sucesos imprevistos que puedan interrumpir la actividad habitual de la cooperativa.

8.1.Declaración de emergencia

Procedimiento para la declaración de emergencias	
Objetivo	Comunicar a todo el personal administrativo, de servicio y a los responsables pertinentes en la Cooperativa de Ahorro y Crédito ACHIK INTI, que están vinculados con el Plan de Continuidad de Negocio (BCP), el protocolo a implementar en caso de que un incidente afecte los servicios informáticos y operaciones de la entidad.
Alcance	La declaración de emergencia tiene lugar desde el instante en que se detecta un incidente que pueda interrumpir o detener las operaciones de la organización. A partir de ese momento, el comité de gestión de crisis debe proclamar el estado de emergencia y ordenar la puesta en marcha del Plan de Continuidad de Negocio (BCP).
Responsable operativo	Debe haber un comité de gestión de riesgos o un responsable de riesgos operativos.
Lineamiento	*Involucrados:* Personal administrativo, directivos, proveedores y guardias de seguridad que laboren en la cooperativa Achik Inti Ltda. *Evento de riesgo:* Los sucesos de peligro pueden ser provocados por acciones humanas, catástrofes naturales, entre otros. Estos eventos tienen el potencial de provocar interrupciones en los servicios.
RESPONSABLES	**ACTIVIDADES**
Personal administrativo o de servicios de la cooperativa de ahorro y crédito Cañar Ltda.	Cuando se detecten incidentes, es esencial informar de manera inmediata a cualquier integrante del equipo encargado de la evaluación de incidentes: Jefe del área de tecnologías de Información TIC Gerente de la cooperativa de ahorro y crédito Achik Inti Ltda. Inicialmente se le informará a través de una llamada telefónica, después de lo cual es necesario enviar un correo electrónico para alertar sobre cualquier incidente que pueda interrumpir las operaciones habituales de la empresa.

Jefe del departamento de tecnologías de la información	El responsable designado para la recepción de alertas de incidentes, ya sea mediante comunicación telefónica o por correo electrónico, debe proceder de acuerdo con los siguientes protocolos: Proceder al sitio del incidente o iniciar una evaluación remota, según la gravedad del incidente, debe ser una acción efectuada dentro del margen de una hora posterior a la recepción de la alerta. 1. Una vez identificado el incidente comunicara a los demás miembros del equipo o comité de evaluación de incidentes. 2. Analizan y evalúan el incidente cuando el impacto del mismo no sea totalmente evidente. 3. Determinan si la presencia del incidente ocasionara la suspensión de los servicios informáticos o la operación de alguna de las áreas de la cooperativa. El equipo encargado de gestionar los incidentes tiene la responsabilidad de asignar el grado de alerta correspondiente al incidente en cuestión. Estos grados se clasifican en tres categorías que son: • Nivel de alerta bajo En este nivel el riesgo no afecta las operaciones y servicios de la organización. • Nivel de alerta medio Es un nivel el riesgo impide las operaciones de un área en específico mas no impide o afecta los servicios de toda la organización. • Nivel de alerta alto Es el nivel el riesgo podría afectar los servicios de la cooperativa tanto tecnológico como corporativo. Por ende, el jefe o encargado del área de TI será el responsable de comunicar el nivel de alerta ya sea este alerta roja o amarilla dependiendo del incidente que se presente, esto tendrá un tiempo límite de 15 a 20 minutos posteriormente se procederá a la activación del Plan de Continuidad de negocio por último debe ser informado al Gerente General de la cooperativa.
Gerente General de la Cooperativa de Ahorro y Crédito Cañar Ltda.	El Gerente General junto al encargado del área de TI debe determinar si el incidente puede ser resuelto en el plazo máximo de 2 horas caso contrario se comunicará el incidente a uno de los miembros del Comité de Administración de Crisis sobre la gravedad del incidente.

A continuación, se delinean las tácticas de recuperación en respuesta a potenciales contextos de desastre, aplicables a los procesos y subprocesos críticos identificados a través del análisis y manejo de riesgos. Estos elementos son componentes esenciales del departamento de Tecnologías de la Información de la Cooperativa de Ahorro y Crédito ACHIK INTI.

Tabla 11: Procedimiento de operación de Gestión de tecnologías de la información y seguridad informática subproceso: Administración de servidores del sistema Financiero

<table>
<tr><th colspan="2">GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA
Subproceso: Administración de servidores del sistema Financiero</th></tr>
<tr><td>Objetivo</td><td>Estableces los lineamientos y las acciones a tomar en caso de llegar a presentarse algún incidente de riesgo, para de esta manera minimizar el impacto ocasionado.</td></tr>
<tr><td>Alcance</td><td>Para todo el personal de la cooperativa de Ahorro y Crédito ACHIK INTI Ltda.</td></tr>
<tr><td>Responsable operativo</td><td>Jefe del departamento de Recursos Humanos</td></tr>
<tr><td colspan="2">ACTIVIDADES</td></tr>
<tr><td colspan="2">Los procedimientos de administración de servidores del sistema financiero, que incluyen la creación, modificación o eliminación de cuentas de usuarios con sus correspondientes privilegios, deben ser implementados en caso de que se presenten los siguientes incidentes:
• Errores de Usuario
• Alteración accidental de la información
• Avería de origen físico y lógico
• Degradación de los soportes de almacenamiento de la información
• Indisponibilidad del personal
• Corte del suministro eléctrico
ACTIVIDADES DEL PROCESO
1. Envía el jefe del departamento de Sistemas una solicitud de creación, modificación o eliminación de una cuenta de usuarios del sistema financiero.
2. recibe la solicitud
3. aprueba dicha solicitud
4. crea un nuevo usuario en el sistema financiero, o a su vez modifica o elimina dicho usuario.
5. Cierra el caso documentando todos los eventos y la solución en la bitácora
6. Informa al jefe del departamento de Recursos Humanos.

RECURSOS CRÍTICOS
• Datos comerciales
• Datos del sistema Financiero
• Servidor de base de datos
• Director de Departamento de Tecnologías de la Información y Comunicación</td></tr>
<tr><td colspan="2">PLAN DE CONTINUIDAD</td></tr>
<tr><td>-Plan de aseguramiento, capacidad y disponibilidad de la infraestructura</td><td>Tiempo máximo de Recuperación</td></tr>
</table>

tecnológica (instalación, configuración y administración de hardware, bases de datos, repositorios, entre otros recursos tecnológicos) con la que cuenta la institución. - Evaluar rápidamente la naturaleza y el alcance de la alteración accidental de la información. Determinar qué datos se vieron afectados y cómo ocurrió la alteración. -Disponer con un generador de energía para la matriz de la cooperativa. -Contar con un Manual de permisos de usuario. -Disponer con más personal en el departamento de sistemas	1 hora

A continuación, se presenta un desglose procedimental para llevar a cabo la realización de copias de seguridad (backups) y la restauración de información en los servidores de la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda.

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA **subproceso: Respaldo y restauración de información de los servidores**	
Objetivo	Asegura que la información generada por las diferentes transacciones, no se pierda y esté disponible en caso de presentarse cualquier contingencia, como por ejemplo daños en los discos duros o eliminación accidental de la información.
Alcance	Para todo el personal de la cooperativa de Ahorro y Crédito Cañar Ltda.
Responsable operativo	Jefe del departamento de Sistemas

ACTIVIDADES

Los procedimientos de Respaldo y restauración de información de los servidores pueden tener los siguientes incidentes:

- Fuego
- Corte de suministro eléctrico
- Difusión de software dañino
- Destrucción de la información
- Avería de origen físico y lógico
- Degradación de los soportes de almacenamiento de la información
- Indisponibilidad del personal

ACTIVIDADES DEL PROCESO

1. El jefe del departamento de sistemas revisa la información a respaldar y procedimientos al que corresponde.
2. Elabora bitácora original con l información del proceso de respaldo a seguir, estimar tiempo de duración del mismo.
3. Respaldar la información en el disco duro que deberá estar custodiado en la oficina del departamento de Sistemas.
4. Anota en la bitácora la fecha, hora de inicio y fin de respaldo.
5. Si existe alguna anomalía al momento de generar el respaldo, reporta el error a proveedores del sistema para su debido reporte.

RECURSOS CRÍTICOS

- Datos comerciales
- Datos del sistema Financiero

<table>
<tr><td colspan="2">

- Servidor de base de datos
- SGBD Oracle 11g
- Sistema Operativo Servidor de Base de Datos
- Director de Departamento de Tecnologías de la Información y Comunicación

PLAN DE CONTINUIDAD
</td></tr>
<tr><td>Para evitar amenazas por Fuego ya sean estos ocasionados por fuentes de alimentación averiadas, cortocircuitos dentro del servidor de Base de Datos es recomendable la existencia de extintores que no sean dañinos a los equipos electrónicos, tener los contactos referentes al control de incendios (Bomberos), cámaras de niebla ya que ayudaran a la detección temprana de posibles incidentes por fuego.
Para la difusión de software dañino, destrucción de la información, Avería de origen físico y lógico, Degradación de los soportes de almacenamiento de la información es necesario tener un Plan de mantenimiento preventivo y correctivo de hardware y software de la Infraestructura Tecnológica.
En el caso de que no se puede hacer los respaldos por problemas con el servidor (virus o falla de la unidad de almacenamiento) es necesario seguir las normas con las que dispone la institución las cuales están definidas en el manual de Procedimientos de la cooperativa de ahorro y crédito Cañar Ltda.</td><td>Tiempo máximo de Recuperación

1 hora</td></tr>
</table>

A continuación, se presenta un desglose técnico que proporciona una visión detallada del Procedimiento para el mantenimiento de Software y Hardware en la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda., enfatizando la importancia de las actividades de mantenimiento preventivo y correctivo, la seguridad de los sistemas, la gestión de cambios y las pruebas regulares para mantener la continuidad del negocio y garantizar el óptimo funcionamiento de los sistemas y equipos críticos.

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA Subproceso: Procedimiento para mantenimiento de Software y Hardware	
Objetivo	Garantizar la disponibilidad y funcionalidad continua de los sistemas y equipos críticos para el negocio mediante un mantenimiento preventivo y correctivo eficiente y oportuno, minimizando así el tiempo de inactividad y asegurando la rápida recuperación en caso de interrupciones o desastres.
Alcance	Para todo el personal de la cooperativa de Ahorro y Crédito ACHIK INTI Ltda.
Responsable operativo	Jefe del departamento de TIC

ACTIVIDADES

Los procedimientos para mantenimiento de Software y Hardware pueden presentar los siguientes incidentes:

- Fallas de hardware
- Errores de software
- Amenazas de seguridad
- Desastres naturales o eventos catastróficos
- Errores humanos

ACTIVIDADES DEL PROCESO

1. Identificación y clasificación de los sistemas y equipos críticos: Realizar un inventario completo de los sistemas de software y hardware que son fundamentales para el funcionamiento del negocio.
2. Establecimiento de un calendario de mantenimiento preventivo: Crear un programa de mantenimiento regular que incluya actividades preventivas, como actualizaciones de software, parches de seguridad, limpieza física de equipos, pruebas de rendimiento, respaldos de datos, etc.
3. Implementación de políticas de seguridad y control de cambios: Establecer políticas y procedimientos para garantizar la seguridad de los sistemas y equipos durante el mantenimiento.
4. Realización de mantenimiento correctivo: Establecer un proceso para gestionar y resolver de manera rápida y eficiente los problemas o fallas que surjan en los sistemas y equipos críticos.
5. Planificación de pruebas y simulacros: Programar y ejecutar pruebas periódicas para evaluar la efectividad del procedimiento de mantenimiento y su integración con el BCP.
6. Capacitación y concienciación del personal: Proporcionar capacitación regular a los empleados sobre las mejores prácticas de mantenimiento, seguridad y cumplimiento del BCP.
7. Evaluación y mejora continua: Realizar revisiones periódicas del procedimiento de mantenimiento para identificar áreas de mejora.

RECURSOS CRÍTICOS

- Servidores y sistemas de almacenamiento:
- Red de comunicaciones
- Base de datos y backups
- Infraestructura de seguridad
- Equipos y dispositivos
- Director de Departamento de Tecnologías de la Información y Comunicación

PLAN DE CONTINUIDAD

-Plan de aseguramiento, capacidad y disponibilidad de la infraestructura tecnológica (instalación, configuración y administración de hardware, bases de datos, repositorios, entre otros recursos tecnológicos) con la que cuenta la institución. - Realiza evaluaciones periódicas de riesgos y análisis de impacto para identificar las vulnerabilidades y los posibles efectos de los incidentes en los recursos críticos. - Implementar un sistema regular de copias de seguridad de los datos críticos y realiza pruebas periódicas de recuperación para asegurarte de que los datos se puedan restaurar de manera efectiva en caso de pérdida o corrupción. - Realiza mantenimiento preventivo regular en los sistemas y equipos críticos para garantizar su funcionamiento óptimo.	**Tiempo máximo de Recuperación** 1 hora

De la misma manera, se presenta el desglose técnico que muestra los pasos clave involucrados en el proceso de ***Generación de estados financieros*** de la Cooperativa de Ahorro y Crédito ACHIK INTI Ltda., resaltando la importancia de la recopilación, procesamiento, conciliación, preparación, análisis y presentación de los estados financieros en conformidad con los principios contables y las regulaciones aplicables.

ADMINISTRACIÓN DE CONTABILIDAD **Subproceso: Generación de estados financieros**	
Objetivo	Garantizar la disponibilidad y exactitud oportuna de los estados financieros, incluso en situaciones de interrupciones o desastres, mediante la implementación de procesos y medidas de respaldo que aseguren la continuidad de las actividades contables y financieras.
Alcance	Para todo el personal de la cooperativa de Ahorro y Crédito ACHIK INTI Ltda.
Responsable operativo	Jefe del departamento financiero/ contable

ACTIVIDADES

La generación de estados financieros puede presentar los siguientes incidentes:

- Interrupción de sistemas y equipos
- Pérdida de datos
- Retrasos en la disponibilidad de información
- Riesgos de seguridad

  Ausencia o indisponibilidad del personal clave

ACTIVIDADES DEL PROCESO

1. Recopilación de datos financieros: Obtener y recopilar información financiera relevante, como transacciones, movimientos de cuentas, saldos de préstamos y depósitos, ingresos y gastos, entre otros
2. Registro y procesamiento contable: Ingresar y registrar los datos financieros recopilados en los sistemas contables de la cooperativa
3. Conciliación de cuentas: Realizar la conciliación periódica de cuentas, asegurando la correspondencia y el equilibrio de los saldos contables.
4. Elaboración de los estados financieros: Preparar los estados financieros básicos, como el balance general, el estado de resultados y el estado de flujos de efectivo.
5. Análisis e interpretación de los estados financieros: Realizar un análisis detallado de los estados financieros para evaluar el desempeño financiero de la cooperativa.
6. Revisión y auditoría: Realizar una revisión interna y, en algunos casos, una auditoría externa de los estados financieros.
7. Archivo y almacenamiento seguro de los estados financieros: Archivar y almacenar los estados financieros y los documentos de respaldo de manera segura y accesible.

RECURSOS CRÍTICOS

- Sistemas contables
- Datos financieros
- Personal capacitado
- Infraestructura tecnológica
- Registros y documentación
- Auditoría interna y externa

PLAN DE CONTINUIDAD	
- Para el incidente de Interrupción de sistemas y equipos el personal debe contactar al equipo de soporte técnico interno o externo para investigar y resolver la interrupción. Proporcionar toda la información relevante sobre el incidente y colaborar con ellos para restablecer los sistemas y equipos lo antes posible. - Realiza copias de seguridad regulares de los datos financieros críticos y almacénalos en ubicaciones seguras y fuera del sitio. - Establece canales de comunicación claros para informar a los involucrados sobre interrupciones, cambios en los procedimientos o cualquier situación que pueda afectar la generación de estados financieros. - Coordina con otros departamentos, como TI, recursos humanos y operaciones, para asegurar una colaboración efectiva en la implementación de las medidas de continuidad de negocios.	**Tiempo máximo de Recuperación** 1 hora

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Angélica María Loja Mayancela portador(a) de la cédula de ciudadanía Nº **0350164018** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"DISEÑO DE UN PLAN DE CONTINUIDAD DE NEGOCIO PARA LA COOPERATIVA DE AHORRO Y CRÉDITO ACHIK INTI LTDA."** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca**,** para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **15 de agosto de 2023**

F: ……..
Angélica María Loja Mayancela
C.I. **0350164018**