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 INFORMACIÓN

DESARROLLO DE UN PLAN DE CONTINUIDAD PARA EL DEPARTAMENTO DE TIC EN EL MUNICIPIO DE CAÑAR

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

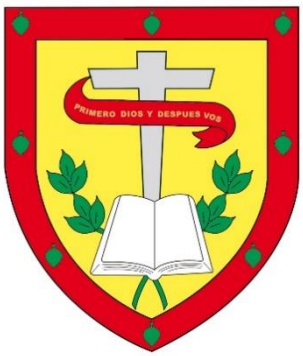
AUTOR: LUIS FRANCISCO GUASCO LOJA.

DIRECTOR: ING. JOSÉ ANTONIO CARRILLO ZENTENO.

CAÑAR - ECUADOR

2024

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 INGENIERIA EN SISTEMAS DE INFORMACIÓN

DESARROLLO DE UN PLAN DE CONTINUIDAD PARA EL DEPARTAMENTO DE TIC EN EL MUNICIPIO DE CAÑAR

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: LUIS FRANCISCO GUASCO LOJA.

DIRECTOR: ING. JOSE ANTONIO CARRILLO ZENTENO.

CAÑAR – ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARACIÓN DE AUTORÍA Y RESPONSABILIDAD

Luis Francisco Guasco Loja portador de la cédula de ciudadanía **N° 0302291703** Declaro ser el autor de la obra: **"Desarrollo de un Plan de Continuidad para el Departamento de TIC en el municipio de Cañar"**, asumo toda la responsabilidad por todas las perspectivas y opiniones expresadas al respecto. Afirmo que se ha ejercido con debido cuidad para reconocer y defender los derechos de propiedad intelectual de partes externas. Además, eximo a la Universidad Católica de Cuenca de cualquier responsabilidad potencial que pueda surgir en relación con este trabajo.

Finalmente, declaro que este trabajo se cumplió con las normas legales, éticas y bioéticos que rigen la investigación, que no contraviene normativa nacional o internacional dentro del campo de investigación. En consecuencia, también asumo la responsabilidad por cualquier problema de cumplimiento asociado y eximo a la Universidad Católica de Cuenca por cualquier reclamación resultante.

Cañar, 28 de noviembre de 2024

Luis Francisco Guasco Loja
C.I. 0302291703

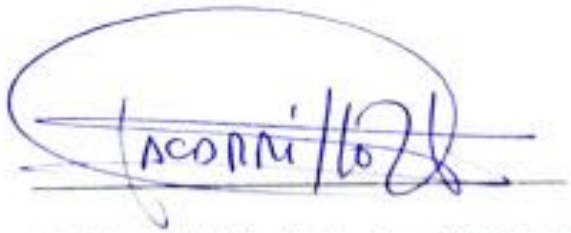
CERTIFICACIÓN PREVIA REVISIÓN DE LECTORES

Cañar, 28 de septiembre del 2024

En mi calidad de director del Trabajo de Titulación: **"Desarrollo de un Plan de Continuidad para el Departamento de TIC en el municipio de Cañar"**, elaborado por **Luis Francisco Guasco Loja,** con CI. **0302291703**, estudiante de la Carrera de Ingeniería en Sistemas en la Unidad Académica de Información, Ciencia de la Computación, e Innovación Tecnológica.

Certifico:

Que, el trabajo de Titulación está apto para el proceso de revisión de los lectores dignados por Dirección de Carrera.



Ing. José Antonio Carrillo Zenteno, MSIG, MTI.

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA

DEDICATORIA

A Dios por concederme la vida, la salud y por guiarme hasta este punto de mi trayectoria de formación profesional. Su sabiduría y perspicacia me han permitido aprender de los errores a mejorar mi formación para el futuro, tanto personal como profesionalmente.

A mis padres Francisco Guasco y Isaura Loja, quienes me enseñaron el mejor camino conforme a las Sagradas Escrituras que hoy me ha formado un profesional con valores y principios cristianos, a mis hermanas/os que día a día me brindaron apoyo durante mi formación profesional, por brindarme la ayuda y motivarme a seguir adelante a pesar de las dificultades encontradas en el camino.

A mi amada esposa que, durante la última etapa de mi vida estudiantil ha sido mi gran ayuda, que me impulsa a seguir adelante brindándome el apoyo incondicional, moral y éticamente para poder culminar con mi carrera universitaria, de manera especial a mi hijo quien ha sido la mayor fuente de inspiración para lograr culminar mi carrera y como profesional ser un ejemplo y modelo a seguir para él.

Por último dedico a toda mi familia, amigos y familia cristiana en general quienes a lo largo de mi carrera me han brindado sus valiosos consejos, estima y oraciones que Dios los bendiga grandemente.

AGRADECIMIENTO

Un agradecimiento a la Universidad Católica de Cuenca por permitirme convertirme en un profesional, gracias a cada docente de la carrera de Ingeniería de Sistemas de Información extensión Cañar quienes formaron parte de este proceso de aprendizaje que con paciencia y esmero me ayudaron en mi formación profesional.

A mi familia, expreso mi más sincero agradecimiento por su amor incondicional y su confianza en mí, que han sido una fuente de inmensa fortaleza y motivación a lo largo de mis esfuerzos. Estoy realmente en deuda con mis padres, Francisco Guasco e Isaura Loja, por su orientación y apoyo constantes, así como con mis hermanas/os por sus sacrificios desinteresados y su aliento, que me han llevado al éxito. Además, estoy profundamente agradecido a mi esposa Lourdes Guamán y a mi hijo Isaías por su paciencia y comprensión, que han sido fundamentales para ayudarme a superar los desafíos de este arduo viaje hacia el logro y la realización de este trabajo.

De manera especial, expreso mi sincero agradecimiento a mi director de tesis, Ing. José Antonio Carrillo Zenteno, por su excepcional tutoría, su paciencia inquebrantable y su constante aliento a lo largo de todo el proceso de investigación. Sus meritorios consejos y su dedicación han sido fundamentales para el desarrollo de este trabajo. Gracias a su tutoría y compromiso, la investigación se ha enriquecido con profundidad y calidad, lo que subraya el papel crucial que desempeña un supervisor dedicado en el crecimiento académico y los logros de un estudiante.

RESUMEN

Esta investigación tiene como objetivo desarrollar un plan de continuidad de negocio para el Departamento de Tecnologías de la Información y Comunicación (TIC) del Municipio de Cañar. La investigación aborda la importancia de contar con un plan estructurado para mitigar los riesgos asociados a los procesos críticos del municipio. Se realiza un análisis de riesgos utilizando la metodología MAGERIT, lo que permite identificar las amenazas y vulnerabilidades de los activos tecnológicos del municipio. A partir de este análisis, se proponen contramedidas y salvaguardas para mitigar los riesgos identificados. El estudio se basa en la norma ISO 22301, que proporciona un marco para la creación de planes de continuidad de negocio enfocados en la resiliencia organizacional. Aunque el plan de continuidad no se implementa en esta investigación, se propone un modelo de gestión que puede ser adoptado por el municipio para fortalecer su infraestructura tecnológica y garantizar la continuidad operativa en caso de incidentes. Además, se resalta la importancia de crear una cultura organizacional que priorice la seguridad y la continuidad de los servicios municipales, involucrando a todas las partes interesadas en el proceso de planificación. La aplicación de la norma ISO 22301 y el análisis de riesgos con MAGERIT son fundamentales para establecer un plan robusto y adaptado a las necesidades específicas del Municipio de Cañar, asegurando la protección y recuperación de los servicios críticos ante situaciones adversas.

Palabras Clave: plan de continuidad, TIC, municipio de Cañar, ISO 22301, gestión de riesgos.

ABSTRACT

This research aims to develop a business continuity plan for the Department of Information and Communication Technologies (ICT) of the Municipality of Cañar. The research addresses the importance of having a structured plan for mitigate the risks associated with the municipality's critical processes. An analysis of the risks using the MAGERIT methodology, which allows to identify threats and vulnerabilities of the municipality's technological assets. Based on this analysis, propose countermeasures and safeguards to mitigate the identified risks. The study is based on the ISO 22301 standard, which provides a framework for creating management plans business continuity plans focused on organizational resilience. Although the business continuity plan continuity is not implemented in this research, a management model is proposed that can be adopted by the municipality to strengthen its technological infrastructure and ensure operational continuity in the event of incidents. In addition, the importance of to create an organizational culture that prioritizes security and continuity of services municipal, involving all stakeholders in the planning process. The Application of the ISO 22301 standard and risk analysis with MAGERIT are essential to establish a robust plan adapted to the specific needs of the Municipality of Cañar, ensuring the protection and recovery of critical services in emergency situations adverse.

Keywords: continuity plan, ICT, municipality of Cañar, ISO 22301, risk management.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

Introducción

En la actualidad, las instituciones tanto públicas como privadas se enfrentan a un entorno dinámico en el que la adaptación continua se vuelve indispensable. La infraestructura tecnológica ha sido fundamental en el avance de estas organizaciones, facilitando operaciones más eficientes y servicios más accesibles. No obstante, la dependencia creciente de la tecnología expone a las instituciones a una variedad de riesgos que pueden interrumpir sus operaciones. Factores como desastres naturales, fallos humanos y ciberataques pueden afectar significativamente la disponibilidad y la integridad de los servicios. Por lo tanto, se vuelve crucial para las administraciones locales, como el municipio de Cañar, desarrollar y mantener un plan de continuidad que asegure la resiliencia operativa ante cualquier contingencia.

La falta de un plan de continuidad en el departamento de Tecnologías de la Información y la Comunicación (TIC) del municipio de Cañar podría tener consecuencias graves, como la pérdida de acceso a información y datos esenciales. Sin un plan adecuado, la capacidad de la organización para tomar decisiones informadas y proporcionar servicios a la comunidad puede verse comprometida. Esto no solo afecta a los residentes que dependen de los servicios digitales del municipio, sino también a los empleados, quienes podrían enfrentar dificultades en la ejecución eficiente de sus tareas. Por ende, la ausencia de un marco de continuidad pone en riesgo la efectividad operativa y la satisfacción de los usuarios.

Para abordar estas deficiencias, es fundamental desarrollar un plan de continuidad integral que permita al departamento de TIC gestionar adecuadamente los riesgos y mantener la operación durante eventos adversos. Este plan debe incluir directrices claras y estrategias específicas para responder a incidentes, minimizando el impacto y

asegurando una recuperación efectiva. Un enfoque proactivo en la planificación garantizará que el municipio pueda mantener sus funciones críticas y servicios esenciales incluso frente a interrupciones imprevistas, mejorando así su resiliencia y capacidad de respuesta.

Considerando el entorno cambiante y los desafíos específicos enfrentados por el municipio de Cañar, es vital implementar revisiones periódicas y ajustes continuos al plan de continuidad. La ausencia de representación de TI en los comités y la percepción de soporte insuficiente subrayan la necesidad de una adaptación constante para garantizar la relevancia y eficacia del plan. Las revisiones y actualizaciones periódicas permitirán al municipio ajustar el plan a nuevas circunstancias y mantenerlo alineado con las necesidades emergentes y las demandas del entorno organizacional.

Este estudio tiene como objetivo desarrollar un plan de continuidad para el departamento de TIC del municipio de Cañar, fundamentado en las mejores prácticas y normas aplicables. La implementación de estrategias basadas en el análisis de riesgos y vulnerabilidades permitirá enfrentar de manera efectiva los desafíos que puedan surgir, protegiendo así la operatividad y los intereses tanto del departamento de TIC como de los residentes del cantón. Por tal razón el desarrollo del Plan de Continuidad del Negocio (BCP) se ejecutarán de acuerdo con la norma ISO 22301, que es reconocida como el punto de referencia internacional inaugural para el Sistema de Gestión de la Continuidad del Negocio, comúnmente conocido como SGCN. Esta norma en particular delinea un marco complejo y completo para llevar a cabo un análisis empresarial exhaustivo, seleccionar las estrategias de recuperación adecuadas, desarrollar planes viables e implementar pruebas rigurosas y protocolos de mantenimiento continuo para garantizar la eficacia y la resiliencia de los esfuerzos de continuidad empresarial.

CAPITULO I

Marco Referencial

1.1 Planteamiento del Problema

En la era contemporánea, tanto las instituciones públicas como las privadas están progresando significativamente al adaptarse a los cambios continuos. El avance de la infraestructura tecnológica ha contribuido en gran medida a su desarrollo. Sin embargo, es crucial reconocer que todas las instituciones son susceptibles de sufrir interrupciones en sus operaciones y servicios. Estas interrupciones pueden deberse a diversos factores, como los desastres naturales, los errores humanos y los ciberataques. En consecuencia, es imperativo que los municipios establezcan un plan de continuidad dentro de su departamento de Tecnologías de la Información y la Comunicación (TIC). Esta medida estratégica garantiza que la administración local pueda cumplir con sus funciones críticas, salvaguardar los datos, mantener la disponibilidad continua de los servicios digitales esenciales y prestar servicios cruciales durante y después de diversas situaciones de emergencia o desastres.

La ausencia de un plan de continuidad bien definido para el departamento de TIC del municipio de Cañar puede tener graves repercusiones. Esto puede provocar que la información y los datos vitales almacenados en los sistemas informáticos del municipio se vuelvan inaccesibles. Esto puede tener un impacto perjudicial en los procesos de toma de decisiones y en la prestación de servicios, incluidos los servicios y aplicaciones en línea que se proporcionan a los residentes. Como consecuencia, los usuarios pueden sufrir inconvenientes e insatisfacción debido a las interrupciones del servicio. Además, los

empleados municipales pueden encontrar dificultades para ejecutar sus responsabilidades de manera eficiente, lo que obstaculiza la productividad general dentro de la organización.

A la luz de estos desafíos, la implementación de un plan de continuidad integral es esencial para mitigar los riesgos y garantizar el funcionamiento sin problemas de los servicios en caso de interrupciones o desastres. Este enfoque proactivo permitirá al Departamento de Tecnologías de la Información y la Comunicación (TIC) del municipio de Cañar desempeñar un papel fundamental en la gestión administrativa y la prestación de servicios a los ciudadanos. Al establecer protocolos y mecanismos sólidos para abordar las posibles interrupciones, el municipio puede mejorar su resiliencia y mantener la eficiencia operativa incluso ante circunstancias imprevistas.

1.2 Formulación del Problema

¿Cómo alinear un plan de continuidad con la gestión estratégica del municipio de Cañar utilizando las buenas prácticas de la institución?

1.3 Antecedentes de la Investigación

Para el propósito de este esfuerzo de investigación, es esencial hacer referencia a varios proyectos de investigación que se centran en temas similares para validar los hallazgos de la investigación. El objetivo principal es ofrecer soluciones prácticas a los problemas actuales mediante la formulación de un plan de continuidad para el departamento de Tecnología de la Información y la Comunicación (TIC) en el ámbito municipal. Los trabajos de investigación posteriores sirven como puntos de referencia cruciales para mejorar el marco conceptual relacionado con el plan de continuidad:

Renzo Giancarlo Correa Salazar realizó un estudio titulado “Diseño de un plan de continuidad para los servicios críticos en el área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC

27031:2011" en la Universidad Peruana de Ciencias Aplicadas (UPC) en Lima, Perú, en 2019. En esta investigación, Salazar destaca la importancia del plan de continuidad para analizar y abordar los desafíos comerciales dentro de los servicios críticos de TI. El plan facilitó mejorar los tiempos de recuperación y restauración al apreciar los riesgos, las vulnerabilidades y las amenazas. También condujo a la identificación de estrategias de continuidad adecuadas y soluciones alternativas para la operación y la administración de los servicios de TI críticos. (Salazar, 2019)

Este estudio aclara el papel fundamental de un plan de continuidad dentro del departamento de TIC de una organización.

Paola Alexandra Díaz Parco, de la Universidad Técnica de Ambato, llevó a cabo un proyecto titulado "Plan de continuidad empresarial (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC" en Ambato en 2022. El objetivo del proyecto era desarrollar un BCP guiado por la norma ISO 22301:2019 para salvaguardar los activos de información vitales y los procesos críticos en el sector de TI de TELECOMSEC. Las estrategias diseñadas en el plan se centran en evitar, contener y recuperarse de eventos imprevistos, al tiempo que garantizan la disponibilidad ininterrumpida del servicio. (Díaz Parco, 2022)

Los hallazgos de este proyecto arrojan luz sobre la importancia de implementar un BCP en el departamento de TI de las organizaciones.

María Fernanda Farinango, investigadora de la Universidad Técnica del Norte, llevó a cabo un proyecto titulado "Desarrollo de un plan de contingencia de servicios de TI para la Dirección de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, aplicando el marco de trabajo ITIL V3 en Ibarra en 2023". Este plan se basa en ITIL, que ofrece pautas para administrar los

servicios de tecnología de la información de manera eficiente. Hace hincapié en la administración de los procesos y en la documentación de las directrices esenciales para el desarrollo basadas en el BCP, lo que ayuda a recuperar y restablecer las funciones críticas dentro de un plazo específico tras una interrupción imprevista. (Farinango, 2023)

Este proyecto de investigación proporcionará información valiosa para mejorar las operaciones del departamento de TIC en el entorno municipal mediante la implementación de un plan de continuidad efectivo.

1.4 Justificación de la Investigación

Hoy en día, en el panorama empresarial contemporáneo, las empresas y organizaciones no se ven afectadas únicamente por acontecimientos como incendios o averías tecnológicas. Más bien, es en el escalón estratégico de la institución donde la reputación y el valor de las partes interesadas son determinantes cruciales. A escala nacional, muchas entidades, públicas o privadas, independientemente de su estructura jerárquica, se enfrentan a la pérdida de información por diversos riesgos o amenazas inherentes. Estos peligros han causado un daño considerable a las instituciones afectadas, pero no se han tomado medidas proactivas para aliviar los impactos de estos riesgos.

En este contexto, el presente trabajo se lleva a cabo con el objetivo general de formular un plan de continuidad empresarial (BCP), que se elaborará meticulosamente utilizando la norma ISO 22301 como punto de referencia fundamental, con un énfasis específico en la salvaguardia y protección de los activos de información más importantes, así como de los procesos operativos críticos inherentes al sector de las tecnologías de la información y la comunicación (TIC) del municipio de Cañar, empleando una amplia gama de metodologías estratégicas diseñadas para anticipar, mitigar y recuperarse de manera efectiva de ocurrencia de eventos adversos imprevistos, garantizando al mismo

tiempo que dichas intervenciones puedan llevarse a cabo dentro de un plazo predeterminado que no comprometa la disponibilidad continua y la integridad operativa de su oferta de servicios.

Posteriormente, el municipio implementará las estrategias o protocolos delineados en el plan de continuidad para responder de manera efectiva a cualquier riesgo o vulnerabilidad potencial en el menor tiempo posible. Este enfoque proactivo no solo salvaguarda los intereses del departamento de TIC y del municipio, sino que también beneficia indirectamente a todos los residentes del cantón Cañar.

1.5 Objetivos

1.5.1 Objetivo General

Desarrollar un plan de continuidad para el departamento de TIC en el municipio de Cañar.

1.5.2 Objetivos Específicos

- Fundamentar mediante un estudio teórico el plan de continuidad para el departamento de TIC.
- Analizar los riesgos, vulnerabilidades y amenazas para la determinación de estrategias de continuidad.
- Elaborar un plan de continuidad según los resultados del análisis de riesgos, vulnerabilidades y amenazas.

1.6 Limitaciones

Es evidente una deficiencia en la colaboración entre los empleados del departamento de TIC, lo que resulta en una falta de intercambio de datos y comunicación confiables.

Esta falta de colaboración dificulta la eficiencia y la eficacia de las operaciones del departamento, lo que genera posibles ineficiencias y reduce la productividad.

Además, la falta de documentación adecuada que describa los procesos de TIC agrava aún más el problema, ya que limita la transparencia, el intercambio de conocimientos y la capacidad de mejorar y racionalizar las operaciones dentro del departamento

1.7 Delimitaciones

- La investigación se realizará en beneficio para el departamento de TIC del municipio de Cañar.
- Este plan de continuidad se desarrolla con una propuesta para el departamento de TIC en el municipio de Cañar, para optimizar las amenazas, riesgos y vulnerabilidades en el servicio.

CAPITULO II

2. MARCO TEORICO

2.1 Generalidades

Hoy en día, la implementación de un plan de continuidad empresarial es de suma importancia en varias organizaciones, ya que es responsable de garantizar la continuación sin problemas de las operaciones críticas y mejorar el proceso de recuperación ante cualquier forma de desastre o interrupción que pueda ocurrir dentro de las empresas o instituciones. Este plan está diseñado para establecer un marco sólido que consiste en medidas de protección, respaldo y recuperación destinadas a proteger los datos, los sistemas y las redes de información de las posibles amenazas.

Al igual que muchas entidades contemporáneas, el municipio de Cañar depende en gran medida de las tecnologías de la información y la comunicación (TIC) para llevar a cabo sus actividades esenciales del día a día. La ocurrencia de fallas o desastres que afecten a estos sistemas puede afectar profundamente a la capacidad operativa de la ciudad, provocando reveses financieros, dañar la reputación y poner en peligro el bienestar público. Ante este escenario, la formulación de un plan de continuidad dentro del Departamento de TIC es imprescindible para garantizar la resiliencia del municipio frente a los incidentes que representan una amenaza para la infraestructura tecnológica de dicho departamento.

Para gestionar eficazmente el plan de continuidad, es crucial establecer y mantener acciones específicas que estén orientadas a cumplir con los requisitos de información más críticos. Estas acciones abarcan varios elementos clave, que incluyen:

1. Identificación de datos, sistemas y redes críticos que son esenciales para las operaciones del municipio.

2. Desarrollo de procedimientos integrales de respaldo y recuperación para proteger la información vital en caso de cualquier incidente adverso.
3. Implementación de medidas de seguridad sólidas para evitar el acceso no autorizado y proteger los datos confidenciales de posibles infracciones.
4. Pruebas y evaluaciones periódicas del plan de continuidad para garantizar su eficacia y relevancia a la hora de abordar los riesgos emergentes.
5. Capacitación de los miembros del personal para mejorar su conciencia y preparación para abordar las cuestiones relacionadas con la continuidad.
6. Colaboración con las partes interesadas y los socios pertinentes para racionalizar los esfuerzos y mejorar la coordinación en tiempos de crisis.
7. Establecimiento de canales de comunicación claros para facilitar la respuesta rápida y la difusión de información crítica durante las situaciones de emergencia.
8. Integración de las lecciones aprendidas de incidentes pasados para mejorar continuamente el proceso de planificación de la continuidad.
9. Cumplimiento de los requisitos reglamentarios y los estándares de la industria para mantener la integridad y confiabilidad del plan de continuidad.

Al adherirse a estas acciones y principios esenciales, el municipio de Cañar puede fortalecer su resiliencia ante posibles interrupciones y garantizar la continuidad de sus operaciones vitales frente a las adversidades:

2.2 Análisis de Impacto en el Negocio (BIA)

El análisis de impacto en el negocio (BIA) tiene una importancia significativa, ya que proporciona información sobre las posibles consecuencias que una empresa puede enfrentar en caso de un desastre. Esta fase implica la tarea crucial de identificar y

categorizar tanto los recursos como los procesos críticos en función de su impacto en la organización. Para llevar a cabo este proceso de manera efectiva, es muy recomendable realizar entrevistas con los responsables del departamento de TIC. Estas personas poseen información valiosa sobre el impacto específico que tendría un fracaso en sus respectivos sectores. En consecuencia, esta información permite a las autoridades tomar decisiones bien informadas con respecto a la asignación de inversiones para garantizar la continuidad del negocio.

Numerosos estudiosos han definido la BIA como un examen exhaustivo de las repercusiones que se producirían si los procesos esenciales de una empresa se detuvieran durante un período específico. Esto incluye determinar qué aspectos deben restaurarse, los costos asociados y las estrategias de recuperación. A diferencia de la evaluación de riesgos, que se centra principalmente en evaluar cómo una organización podría verse afectada por las amenazas a la seguridad mediante la identificación, el análisis y la evaluación de dichos riesgos en función de su gravedad y probabilidad de aparición. La BIA, por otro lado, es un proceso más especializado que se concentra en reconocer los diversos tipos de impactos que podrían ocurrir y en comprender las repercusiones en las operaciones en el departamento de TIC. Al profundizar en estos detalles, las organizaciones pueden comprender mejor qué áreas podrían verse afectadas y las consiguientes implicaciones en sus procesos. (Caizaguano, 2018)

En el pasado, se consideraba esencial evaluar los posibles resultados que los riesgos reconocidos podían tener en las operaciones comerciales, tanto internamente dentro del departamento de TI como externamente en toda la organización. Para llevar a cabo un análisis exhaustivo, es imprescindible tener en cuenta los pasos secuenciales que se describen a continuación.

- Identificación de procesos del negocio

Cuenca: Av. de las Américas y Tarqui. *Telf: 2830751, 2824365, 2826563* **Azogues:** Campus Universitario "Luis Cordero El Grande", (Frente al Terminal Terrestre). *Telf: 593 (7) 2241 - 613, 2243-444, 2245-205, 2241-587* **Cañar:** Calle Antonio Ávila Clavijo. *Telf: 072235268, 072235870* **San Pablo de la Troncal:** Cdla. Universitaria km.72 Quinceava Este y Primera Sur *Telf: 2424110* **Macas:** Av. Cap. José Villanueva s/n *Telf: 2700393, 2700392*

- Evaluación de impactos operacionales y financieros
- Identificación de procesos críticos
- Establecimiento de los tiempos de recuperación
- Identificación de requerimientos de recursos críticos
- Identificación de procedimientos alternos. (pág. 14)

Tras la difusión de esta fase, es aconsejable compilar un informe completo en el que se describan las funciones y los procedimientos críticos del servicio. Esta documentación debe incluir detalles fundamentales sobre los recursos y los plazos de recuperación necesarios para que las entidades puedan mantener sus operaciones y, por lo tanto, garantizar la continuidad de los servicios empresariales. El análisis del impacto empresarial implica la delineación de una serie de medidas interconectadas destinadas a identificar con precisión las repercusiones de las interrupciones y a tomar decisiones informadas sobre los procedimientos que se consideran indispensables para la organización y que tienen un impacto directo en la empresa en caso de una calamidad. (Jaramillo Camacho, 2022)

2.3 Plan de continuidad de Negocio (BCP).

La disciplina que prepara a una organización para mantener la continuidad del negocio durante los desastres mediante la ejecución de un plan de continuidad del negocio, este plan es crucial para la sostenibilidad y la resiliencia a largo plazo de la organización frente a eventos imprevistos. (Hurtado & Paspuel, 2023)

Esta disciplina no solo garantiza la continuidad de las operaciones independientemente del tamaño de la organización, sino que también considera varios aspectos críticos como la infraestructura de las TIC, los recursos humanos, los sistemas de comunicación, el mobiliario, la logística, los sistemas industriales y la infraestructura

física. Cada área requiere un plan de continuidad personalizado, ya que las estrategias para enfrentar un almacén logístico inundado difieren significativamente de las necesarias para restablecer la energía en una sala de servidores si se suspende el suministro eléctrico.

El plan de continuidad empresarial se elabora meticulosamente para delinear objetivamente los procesos clave de la empresa y alinear los intereses de la alta dirección y las diversas unidades organizativas, garantizando que los diferentes departamentos apoyen los mismos procesos básicos y desarrollen estrategias de respuesta a emergencias eficientes. Si bien se reconoce que la gestión de riesgos no puede ofrecer un control total sobre todos los posibles imprevistos, sí ayuda a evitar numerosos incidentes que podrían representar una amenaza para la continuidad empresarial. Básicamente, un plan de continuidad empresarial sirve como una estrategia de gestión de riesgos que no solo mitiga las emergencias, sino que también proporciona a la empresa las tácticas y los recursos necesarios para resistir los eventos perturbadores y recuperarse de ellos. La seguridad desempeña un papel fundamental en un plan de continuidad empresarial al facilitar la recuperación y el restablecimiento de los activos de la empresa. (Gutiérrez Mendoza, 2022)

El ámbito de la planificación de la continuidad abarca procedimientos documentados que guían a una organización al responder, recuperarse, restaurar y volver a los niveles operativos predefinidos tras cualquier interrupción. Por lo general, esto se refiere a los recursos, servicios y actividades esenciales para mantener la continuidad de los servicios de TI críticos que presta la organización. También abarca la capacidad de los componentes de TIC de la organización para mantener las operaciones empresariales críticas con un nivel aceptable durante un período específico después de una interrupción. (Salazar, 2019)

Como lo describe (Salazar, 2019) la Universidad Francisco de Paula Santander ofrece una definición precisa de la planificación de emergencias como un enfoque estratégico que comprende un conjunto de procedimientos destinados a identificar soluciones alternativas y facilitar el rápido restablecimiento de los servicios organizacionales en caso de un incidente. Además, la UFPS introduce conceptos clave que deben tenerse en cuenta en el contexto de la planificación de la continuidad. Estos incluyen:

- **Ataque:** término que designa cualquier evento o acción que pretenda interrumpir el funcionamiento normal de los servicios de TI.
- **Incidente:** un evento que se materializa en forma de amenaza, como un corte de energía en una empresa.
- **Integridad**: garantizar que toda la información alojada en los sistemas de TI permanezca inalterada.
- **Continuidad:** refleja la capacidad del sistema para mantenerse estable después de un incidente, manteniendo sus operaciones y funcionalidad. (pág. 11)

2.3.1 Continuidad del negocio:

Capacidad de una organización para mantener sus operaciones críticas en funcionamiento durante y después de una interrupción o desastre. Es el objetivo principal del plan de continuidad, ya que garantiza que el municipio de Cañar pueda seguir brindando sus servicios esenciales a la ciudadanía, incluso en situaciones adversas. (Farinango, 2023)

La continuidad del negocio se puede definir como una situación en la que las operaciones de una empresa sean de forma continua y sin interrupción. Eventos de gran importancia o impacto, como algunos que han ocurrido en los últimos años (ataques

terroristas, pandemias o desastres naturales), resaltan el riesgo de nuevas perturbaciones o perturbaciones significativas en el sector financiero y la necesidad de mitigar su impacto. resolver el problema de forma global y coordinada.

La continuidad en todo tipo de negocios hoy en día es importante, ya que se prioriza el servicio al cliente, el desempeño financiero y la supervivencia en el mercado para mantenerse por delante de la competencia que existirá en el futuro cercano. (Gutiérrez Mendoza, 2022)

2.3.2 Gestión de continuidad.

Es un procedimiento complejo y detallado que profundiza en la identificación de los posibles impactos que representan una amenaza para una organización, al tiempo que establece un enfoque estructurado para mejorar la resiliencia y la capacidad de organizar una respuesta bien coordinada que garantice la protección de las partes interesadas clave, la reputación, la marca y el valor general derivado de las actividades de la organización. (Hurtado & Paspuel, 2023)

Según (Farinango, 2023) La Gestión de la Continuidad del Servicio de TI es la clave para la prestación de servicios que ofrece ITIL. La gestión se centra en prevenir, prever y gestionar la planificación de eventos. Su principal objetivo es mantener el más alto nivel operativo de los servicios de TI antes y durante el evento.

El objetivo es minimizar el tiempo de inactividad, el costo y el impacto comercial que puede ocurrir en caso de una falla mediante el uso de procesos eficientes y estandarizados para aplicar en caso de un incidente inminente. La Gestión de la Continuidad del Negocio (BCM) incluye ITSCM y otros procesos de mitigación de riesgos. Por lo que los equipos de TI necesitan trabajar juntos para crear:

Planificación de la continuidad del negocio (BCP): Esto incluye la planificación de la prevención y recuperación de incidentes de TI a nivel de desastre.

Análisis de impacto empresarial (BIA): Determina el impacto potencial de un desastre de TI en el negocio.

Administración de la continuidad del negocio (BCM): Garantiza la continuidad de las actividades esenciales del negocio, minimizando el impacto en sus objetivos estratégicos, la reputación y la rentabilidad.

La gestión de la continuidad del negocio requiere desarrollar un plan integral que abarque varias facetas asociadas al mantenimiento de las operaciones durante interrupciones imprevistas, denominado plan de continuidad del negocio. La Planificación de la Continuidad del Negocio (BCP) es el proceso de identificar y proteger los procesos y recursos comerciales críticos que mantienen los procesos comerciales en un nivel aceptable mientras protegen todos los recursos y preparan procedimientos para garantizar la supervivencia de la organización. Cuando una empresa se enfrenta a una amenaza. Es un proceso continuo que se utiliza para identificar los desastres y vulnerabilidades de una organización, la probabilidad de que ocurran desastres, los objetivos estratégicos y las posibles consecuencias del éxito, y la efectividad de los controles y estrategias aplicables para mejorar el desempeño y la eficiencia. Este plan tiene ocho elementos cruciales que desempeñan un papel fundamental en la definición del marco de la gestión de la continuidad de las operaciones, incluyendo la revisión de la continuidad de las operaciones, el análisis de riesgos, la estrategia de continuidad de las operaciones, el plan de recuperación ante desastres y la identificación de requisitos de capacitación de los empleados (Montalban Ordoñez, 2022)

2.3.3 Estrategias de continuidad.

Una estrategia de continuidad se puede conceptualizar como un enfoque estructurado que facilita la restauración y el funcionamiento perpetuo de las funciones vitales de una entidad en medio de una calamidad o una interrupción significativa. Es imperativo que las organizaciones diseñen e implementen meticulosamente estrategias de continuidad sólidas para garantizar la resiliencia y la sostenibilidad figure los desafíos imprevistos. (Jaramillo Camacho, 2022)

Además, se puede deducir que las estrategias de continuidad son:

La asignación de los recursos y las acciones necesarios para hacer frente a las interrupciones del servicio, las medidas destinadas a reducir la probabilidad y el impacto de dichos incidentes.

Sin embargo, es crucial reconocer que la ejecución de estas estrategias presenta desafíos específicos, como: La asignación de recursos suficientes, la capacitación del personal en materia de continuidad y la revisión continua de los planes, colaborar con diferentes departamentos y entidades externas, adoptar tecnologías de vanguardia, realizar simulaciones y realizar pruebas de recuperación son algunas de las iniciativas que pueden reforzar la continuidad dentro del departamento. Mediante la identificación de los riesgos, la implementación de medidas preventivas, la asignación de responsabilidades claras y la colaboración con expertos en la materia, es posible garantizar la continuidad operativa y lograr el éxito de los proyectos dentro del departamento. (Jaramillo Camacho, 2022)

2.4 Plan de Recuperación ante Desastres:

El plan de recuperación comprende las acciones esenciales que se deben implementar después de la detección y posterior contención de una amenaza. El objetivo principal de

este plan es devolver las condiciones de las entidades y las personas a su estado anterior a la amenaza. Este plan sirve de guía para los procedimientos recomendados para llevar a cabo la contención de amenazas o desastres tras un incidente. Define la información esencial requerida para el restablecimiento efectivo de los equipos y las operaciones a sus niveles de funcionamiento originales. (Farinango, 2023)

Un plan de recuperación ante desastres (DRP) está diseñado como una lista de verificación o instrucciones de trabajo en caso de un desastre a nivel de infraestructura. Describe las políticas, recursos, procesos y procedimientos que el Equipo de Respuesta a Desastres de Tecnología y TI utilizará en respuesta a cualquier incidente o incidente inesperado. La protección de datos se basa en la prestación de un Plan de Recuperación ante Desastres (PRD) y se proporcionarán a terceros ajenos al departamento técnico copias idénticas que contengan los datos personales de los miembros del equipo de recuperación o de cualquier otro miembro del PRD. Si es necesario verificar la definición de miembro, se puede invitar a una tercera empresa a ver una copia del DRP desde una computadora en el sistema de información del departamento, sin permitir el procesamiento de datos personales o su contenido. También se procesará información confidencial del sistema, configuraciones, contraseñas y direcciones IP de red.

Los planes de recuperación se dividen en dos categorías distintas que abarcan tanto los desastres naturales como los provocados por el hombre, los cuales tienen el potencial de atrapar a una organización sin previo aviso o ataques cibernéticos, sabotajes. Si se produce un desastre o un ataque realizado por el hombre, las empresas que han tomado las medidas necesarias para desarrollar y poner en marcha un plan de recuperación ante desastres (DRP) tienen más probabilidades de soportar la terrible experiencia con interferencia mínima en su eficiencia operativa y sin perder datos. (Jaramillo Camacho, 2022)

De acuerdo con el estudio del plan de recuperación de desastres se pudo deducir que las acciones y procedimientos a considerar para la restauración de las operaciones y servicios del departamento de TIC son:

- Para la implementación de estrategia de recuperación se definirá los recursos humanos, materiales y tecnológicos necesarios.
- Considerando las operaciones de recuperación, desarrollar las estrategias de recuperación detalladamente para cada sistema, dato o proceso crítico.
- Establecer paso a paso los procedimientos de recuperación de cada sistema, dato o proceso crítico

2.5 Evaluación de Riegos

La identificación de riesgos se considera una tarea crucial para ejecutar dentro del marco de gestión de riesgos de una organización. Esta tarea implica una especificación detallada de las amenazas reales presentes en el plan de un proyecto, incluidas las estimaciones, los cronogramas, la asignación de recursos, las restricciones presupuestarias y otros factores relevantes. Para simplificar el proceso de identificación de riesgos, es imprescindible crear un mapa de riesgos que ayude a identificar los riesgos más críticos que requieren atención inmediata, acompañado de una descripción completa de los riesgos y las posibles consecuencias que podrían conllevar.

Tras la identificación y clasificación de los riesgos, el paso siguiente implica el desarrollo de un análisis específico para determinar el impacto en función de la probabilidad de que ocurran en el entorno organizacional. Se pueden emplear varias herramientas y metodologías para llevar a cabo el análisis de los riesgos, lo que facilita la evaluación tanto de la probabilidad como de las consiguientes consecuencias. Estos procesos y técnicas ayudan colectivamente al director a tomar decisiones bien informadas

cuando se enfrenta a los riesgos. El análisis específico contribuye aún más a la estrategia general de gestión de riesgos al proporcionar información valiosa sobre las posibles implicaciones de los riesgos identificados en los objetivos y las operaciones de la organización. (Allaico, 2021)

2.5.1 Riesgo.

El peligro se refiere a la posibilidad de causar un efecto distinto en el establecimiento. El riesgo calculado sirve como una métrica asociada a la combinación de métricas calculadas de vulnerabilidad e impacto, y ambas se entrelazan con la correlación entre el activo y la amenaza a la que pertenece el riesgo calculado. (Jaramillo Camacho, 2022)

Es la posibilidad de que ocurra un evento inesperado, cuyas consecuencias pueden ser catastróficas, graves, menores o insignificantes. Además, las organizaciones pueden abordarlos utilizando cuatro estrategias: trasladarlo, adueñarse de él, eliminarlo e implementar medidas de mitigación. (Gutiérrez Mendoza, 2022)

Según (Reyna Carrión, 2023) define que el riesgo es la posibilidad de estropear un recurso vulnerable, un área u organización completa. Los cálculos de riesgo están fuertemente influenciados por el impacto y son un proceso complejo, y se clasifican.

Riesgo inherente: Fallo material por falta de controles compensatorios.

Riesgos de control: Hay errores que no pueden ser controlados por el sistema de control implementado.

Riesgos de detección: Los auditores abusan de los procedimientos de detección de errores, y dan la impresión de que no hay errores cuando en realidad hay.

Riesgos relacionados con las auditorías.

El riesgo es una estimación de la amenaza que cuando se materializa tiene efecto perjudicial con diferentes rutas de ataque. (pág. 16)

2.5.2 Gestión de riesgos:

Proceso de identificar, analizar, evaluar y tratar los riesgos que pueden afectar a una organización. Es fundamental para el desarrollo de un plan de continuidad efectivo, ya que permite comprender los riesgos potenciales a los que está expuesto el departamento de TIC y tomar medidas para mitigarlos. (Jaramillo Camacho, 2022)

La gestión de riesgos define principios que permiten a una organización desarrollar, implementar y mejorar continuamente con un modelo de trabajo que integra los procesos de análisis de riesgos aplicando estrategias, planes, documentos, políticas y valores mundiales, a través de organizaciones. (Farinango, 2023)

El análisis y la gestión de riesgos implican técnicas sistemáticas que permiten el examen exhaustivo de los riesgos del sistema de información y la posterior recomendación de medidas adecuadas para mitigar estos riesgos dentro de una organización. El empleo de un marco de análisis y gestión de riesgos requiere una evaluación exhaustiva de las implicaciones de las posibles violaciones de seguridad en los aspectos operativos de la empresa, destacando así los riesgos actuales presentes. Además, este método implica la identificación de diversas amenazas que podrían comprometer la integridad de los sistemas de información, así como la evaluación de la susceptibilidad del sistema a estas amenazas identificadas. (Allaico, 2021)

Los riesgos que se pueden dar en el departamento de TIC son los siguientes:

- Desastres naturales que pueden dañar los datos, la infraestructura física, los sistemas en el municipio.

- Perdida de energía eléctrica que interrumpe las operaciones del departamento de TC debido a los coretes por mantenimientos, fallas de red eléctrica por eventos climáticos.
- Riesgos físicos por robo, sabotaje (daños intencionales), incendios ocasionados por personas malintencionadas.
- Fallas humanas como errores involuntarios, falta de atención o cuidado, actos maliciosos por parte del personal del departamento.
- Riesgos tecnológicos debido a un ataque cibernético, fallas en el hardware y software, perdida de datos.
- Riesgos externos que se podría dar por desastres en otras áreas, por depender de proveedores, cambios regulatorios.

2.6 Metodología de gestión y análisis de riesgos

La gestión y el análisis de riesgos son componentes fundamentales para garantizar la continuidad de las operaciones en cualquier organización, especialmente en el ámbito de las Tecnologías de la Información.

2.6.1 Margerit

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología desarrollada por el gobierno español para la identificación, evaluación y tratamiento de los riesgos asociados a los sistemas de información. Su objetivo es proporcionar un marco estructurado que permita gestionar los riesgos de forma efectiva, asegurando la protección de los activos de información en las organizaciones. MAGERIT se enfoca en la continuidad de los servicios y en la mitigación de las amenazas y vulnerabilidades que puedan afectar a los sistemas

tecnológicos, y se basa en la evaluación de impactos y probabilidades de ocurrencia de los riesgos. (Caizaguano, 2018)

2.6.2 Cram

CRAM (Critical Risk Assessment Methodology) es una metodología orientada a la evaluación de riesgos críticos en sistemas informáticos y tecnológicos. Su propósito principal es identificar y analizar los riesgos que podrían tener un impacto significativo en la seguridad y funcionamiento de los sistemas. CRAM proporciona un proceso detallado para clasificar y priorizar los riesgos según su gravedad, ayudando a las organizaciones a enfocar sus esfuerzos en la mitigación de aquellos que presentan mayor amenaza para la operación y la seguridad.

2.6.3 Octave

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología de evaluación de riesgos enfocada en la seguridad de la información. Desarrollada por el Software Engineering Institute de la Universidad Carnegie Mellon, OCTAVE se centra en la identificación y evaluación de las amenazas, vulnerabilidades y activos críticos dentro de una organización. A diferencia de otras metodologías, OCTAVE es una aproximación autoevaluativa que permite a las organizaciones identificar sus propios riesgos mediante la recopilación de información interna y la participación activa de los responsables de la gestión de los sistemas. (Díaz Parco, 2022)

2.7 Implementación de Medidas de Seguridad

La implementación de medidas de seguridad adecuadas es crucial para proteger los sistemas, las redes, los datos y los activos críticos del departamento contra las amenazas internas y externas. Al mitigar estos riesgos, la implementación de medidas de seguridad

ayuda a reducir la probabilidad de interrupciones del servicio, pérdidas de información y otros incidentes disruptivos que podrían afectar la continuidad de las operaciones.

Es necesario considerar e implementar varias categorías de medidas de seguridad en el departamento:

1. **Controles de acceso:** Es absoluto aplicar controles de acceso estrictos para limitar el acceso a los sistemas, redes y datos del departamento únicamente al personal autorizado. Esto se puede lograr mediante la utilización de protocolos de contraseñas sólidos, mecanismos de autenticación multifactorial y controles de acceso basados en funciones.
2. **Protección de datos:** Se deben establecer medidas para mantener la confidencialidad, la integridad y la disponibilidad de los datos departamentales. Esto implica actividades como el cifrado de datos, las copias de seguridad periódicas de los datos, la aplicación de las restricciones de acceso a los datos y la mejora del conocimiento del personal sobre las mejores prácticas de seguridad de los datos.
3. **Seguridad de la red:** Es fundamental proteger la red del departamento contra las ciberamenazas y los ataques. Esto implica implementar firewalls, implementar sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusiones (IPS), segmentar la red y garantizar las actualizaciones periódicas del software y el firmware de los dispositivos de red.
4. **Seguridad de las aplicaciones:** Es esencial proteger las aplicaciones departamentales contra las vulnerabilidades y los ataques maliciosos. Esto incluye la realización de pruebas de seguridad en las aplicaciones, la actualización constante del software de las aplicaciones, la aplicación de los

controles de acceso a las aplicaciones y la formación del personal sobre los protocolos de seguridad de las aplicaciones.

5. **Seguridad física:** Es fundamental proteger los activos físicos del departamento, como los servidores, los equipos y los dispositivos de red. Esto incluye controlar el acceso físico a las instalaciones del departamento, instalar sistemas de seguridad perimetral y establecer protocolos para el manejo y la eliminación seguros de los dispositivos.

6. **Sensibilización y capacitación:** Es exigente sensibilizar y capacitar al personal departamental sobre las amenazas a la seguridad informática, las mejores prácticas de seguridad y los protocolos de respuesta a incidentes. Esta capacitación es vital para garantizar que los miembros del personal comprendan los posibles riesgos y estén equipados para responder de manera efectiva en caso de una violación de la seguridad.

Al integrar estas medidas de manera efectiva, el departamento puede fortalecer sus activos críticos, mitigar el riesgo de interrupciones del servicio y mantener la continuidad del negocio ante eventos disruptivos imprevistos. Este enfoque proactivo de la seguridad no solo protege al departamento, sino que también garantiza la resiliencia de sus operaciones ante los cambiantes desafíos de seguridad.

2.8 Formación y Capacitación del Personal

El objetivo principal del plan de formación se centra inicialmente en el personal del departamento de TIC, en particular en aquellas personas que están estrechamente relacionadas con los esfuerzos de continuidad del negocio. Estas personas desempeñan un papel crucial a la hora de fortalecer los conocimientos existentes o de mantenerse al tanto de los últimos avances en el ámbito técnico. La persona que dirija el departamento

de TIC asumirá la responsabilidad de identificar las áreas clave que requieren capacitación y transmitirá esta información por correo electrónico.

Es imprescindible que la programación de las sesiones de formación y la selección de los participantes se planifiquen meticulosamente para garantizar que no se interrumpan las operaciones comerciales en curso. Se adoptará un enfoque integral para facilitar una comunicación eficaz en relación con el plan de continuidad empresarial, que abarque la difusión de información a través de varios canales, como la correspondencia por correo electrónico, los vídeos instructivos y las sesiones informativas interactivas. Al aprovechar estas diversas herramientas de comunicación, la organización tiene como objetivo garantizar que todas las partes interesadas estén bien informadas y participen en el proceso de mejora de las estrategias de continuidad empresarial. (Díaz Parco, 2022)

2.9 Pruebas y Simulacros

Las pruebas se centran en evaluar los procedimientos descritos en el plan de continuidad, con el objetivo de especificar cada elemento que se evaluará en los servicios de tecnología de la información de la organización. Es crucial que estos procesos se hayan implementado correctamente en la empresa para garantizar que las soluciones implementadas se alineen con los requisitos reconocidos. A la hora de considerar las autoevaluaciones, estas pueden llevarse a cabo si hay personas competentes dentro de la organización o, alternativamente, pueden llevarlas a cabo un especialista o un equipo de profesionales de continuidad externos, lo que se considera, en general, el curso de acción más recomendable. Las empresas se someten a transformaciones continúas debido a los avances en la tecnología, los cambios en los procesos y la evolución de los productos en el marco del plan de continuidad y la infraestructura de la organización.

Según (Jaramillo Camacho, 2022), cualquier alteración que se produzca dentro de la organización requiere una evaluación para determinar su impacto en la capacidad de la

organización para perseverar o recuperarse. Las entidades empresariales revisan constantemente sus prioridades operativas para implementar diversas estrategias que incluyan servicios y proyectos destinados a mejorar la eficiencia y maximizar la utilidad de las materias primas y los recursos; el enfoque más eficaz en este sentido es garantizar la continuidad de la planificación. Los cambios en curso deben evaluarse meticulosamente mediante procedimientos de gestión, y es de suma importancia documentar y evaluar con precisión las alternativas dentro de los procesos; el mantenimiento forma parte integral de la conversión facilitada por la planificación. La fase final consiste en evaluar la capacidad de la empresa para responder a un escenario calamitoso que afecte a sus recursos, probando así la eficacia y los tiempos de respuesta del plan de continuidad para validar su alineación con la evolución de los procedimientos que se están ejecutando. (Jaramillo Camacho, 2022)

Las fases de las pruebas del Plan de Continuidad del Negocio (BCP) se aplicará en el proyecto actual para garantizar la continuidad de los servicios de TIC críticos. La fase inicial, denominada fase de preparación del proyecto, comienza con la creación del documento del plan de recuperación del cliente e incluye actividades como la celebración de reuniones con los proveedores y la realización de revisiones de los centros de recuperación física. Durante esta fase, el equipo de continuidad empresarial debe visitar sitios alternativos, cuando proceda, para familiarizarse con la infraestructura, los sistemas, los equipos y los recursos disponibles. Posteriormente, la fase de ejecución de la prueba define la fecha, la hora y el método específicos de la prueba que se implementará, centrándose en la recuperación de los servicios de TIC críticos. Tras la ejecución de la prueba, los resultados se analizan cuidadosamente en la fase de evaluación de prueba para determinar si se han alcanzado los objetivos de la prueba. Además, se compila un informe de evaluación exhaustivo del ensayo, en el que se destacan las

principales conclusiones y recomendaciones para futuras mejoras en el proceso de planificación de la continuidad. (Montalban Ordoñez, 2022)

Según (Montalban Ordoñez, 2022) menciona que los tipos de pruebas pueden variar en complejidad según su planificación, hay cinco tipos de pruebas.

- **Las pruebas de simulación** están diseñadas para validar el plan de continuidad operativa de los servicios de TIC críticos. Su objetivo principal es garantizar que toda la información relevante esté presente para una recuperación exitosa y que esta información se mantenga actualizada. Además, estas pruebas tienen como objetivo confirmar la disponibilidad de personal responsable para llevar a cabo las actividades de recuperación. Las simulaciones también implican la creación de escenarios hipotéticos para probar el plan a fondo.
- **Las pruebas de escritorio**, por otro lado, tienen como objetivo simular un entorno libre de estrés para los participantes. Estas pruebas son de naturaleza más simple y se centran en permitir que los participantes se familiaricen con el plan en un entorno agradable.
- **Las pruebas de revisión** pertenecen a la categoría de complejidad moderada y están destinadas a familiarizar a los miembros del equipo con sus funciones, responsabilidades, procedimientos e interacciones en equipo. Brindan la oportunidad de identificar áreas de mejora en función de las experiencias de los participantes.
- **La prueba operativa de áreas críticas** está diseñada para crear una situación controlada en la que se puedan evaluar los procesos comerciales en un área

específica, como el departamento de TIC. Este tipo de prueba es de complejidad moderada.

- **Las pruebas de simulacro**, por otro lado, tienen como objetivo simular una contingencia a gran escala que afecte a todas las áreas críticas cubiertas por la PCO. Estas pruebas son muy complejas y evalúan varios aspectos, como la activación del plan, la transferencia de recursos, la respuesta de los empleados y el regreso a las operaciones normales. (pág. 146)

2.10 Revisión y Actualización Periódica

La revisión y actualización periódicas del Plan de Continuidad es crucial para garantizar su eficacia y alineación con los requisitos cambiantes del Departamento de TIC y el Municipio de Cañar. Es imperativo llevar a cabo revisiones y actualizaciones periódicas del plan para garantizar que el Departamento de TIC esté adecuadamente equipado para hacer frente a cualquier posible incidente perturbador que pueda poner en peligro las funciones críticas del departamento y la continuidad empresarial general del municipio. Mediante el monitoreo y las revisiones consistentes del plan, el departamento puede asegurarse de que posee una estrategia sólida y actual que le permite responder con prontitud a los incidentes y mitigar el impacto en sus operaciones y servicios, salvaguardando así los intereses y las partes interesadas del municipio.

Durante la fase inicial, es imprescindible establecer un proceso sólido para la supervisión e identificación continuas de las posibles amenazas a la seguridad de los sistemas de tecnología de la información y la comunicación (TIC). Este proceso debe incluir comprobaciones y evaluaciones periódicas para garantizar que cualquier vulnerabilidad se detecte y aborde con prontitud. Además, la organización debe priorizar la revisión periódica de su plan de continuidad para validar su eficacia y relevancia ante la evolución de las amenazas. Esta revisión debe realizarse a intervalos predefinidos para

garantizar que el plan se mantenga actualizado y alineado con el panorama de seguridad actual.

A lo largo de cada fase del proceso de prueba, es crucial documentar meticulosamente todas las observaciones, problemas y soluciones encontradas. Esta documentación sirve como un valioso repositorio de datos históricos que puede facilitar en gran medida una recuperación rápida en caso de una interrupción del sistema o un desastre. Además, los registros detallados desempeñan un papel clave a la hora de realizar análisis exhaustivos posteriores al incidente para identificar los puntos fuertes y débiles del plan de continuidad. Al documentar cada paso dado durante el proceso de prueba, las organizaciones pueden comprender mejor su resiliencia operativa y su preparación para mitigar las amenazas a la seguridad. La documentación exhaustiva de los resultados de las pruebas permite a las organizaciones hacer un seguimiento de su progreso a lo largo del tiempo e identificar patrones o problemas recurrentes que requieren atención. En general, la documentación exhaustiva de las actividades de prueba es esencial para mejorar la postura general de seguridad de la organización y garantizar la eficacia de su plan de continuidad. (Salazar, 2019)

2.11 Vulnerabilidades.

Las vulnerabilidades se perciben como debilidades en un sistema que pueden ser explotadas por entidades malintencionadas para transformar las amenazas potenciales en riesgos tangibles que podrían causar un daño significativo a la organización. Estas vulnerabilidades, en lugar de ser fuentes confirmadas de daño, se consideran elementos dentro de un espectro de circunstancias que pueden afectar a los activos de la empresa. Las vulnerabilidades pueden deberse a deficiencias físicas y lógicas del sistema, derivadas de factores como la ubicación del sistema, la calidad de su instalación, configuración y mantenimiento, así como la ausencia de programas esenciales o la

presencia de protocolos de seguridad anticuados y mal definidos. (Jaramillo Camacho, 2022)

El objetivo principal del análisis y la gestión de los riesgos relacionados con las computadoras es mitigar la probabilidad de pérdidas organizacionales mediante la identificación de los componentes específicos del sistema que requieren protección, la identificación de las vulnerabilidades que comprometen la integridad del sistema y el reconocimiento de las diversas amenazas que representan riesgos para su seguridad y funcionalidad. Este enfoque proactivo tiene como objetivo fortalecer las defensas de la organización contra las posibles ciberamenazas y vulnerabilidades, mejorando así su resiliencia general ante la evolución de los desafíos de seguridad. Al evaluar y abordar sistemáticamente las vulnerabilidades del sistema, las organizaciones pueden reforzar su postura en materia de ciberseguridad y minimizar la probabilidad de que se produzcan ciberincidentes que puedan interrumpir las operaciones y comprometer los datos confidenciales.

En esencia, la gestión de vulnerabilidades es un aspecto fundamental de las estrategias integrales de mitigación de riesgos, ya que permite a las organizaciones identificar, evaluar y corregir de forma proactiva las posibles debilidades de sus sistemas antes de que puedan ser explotadas por actores malintencionados. Mediante la identificación sistemática y la priorización de las vulnerabilidades, las organizaciones pueden asignar los recursos de manera eficaz para abordar los riesgos más críticos, mejorando así su resiliencia general en materia de ciberseguridad y reduciendo el impacto potencial de las ciberamenazas en sus operaciones y activos. Al incorporar las prácticas de gestión de vulnerabilidades en su marco más amplio de gestión de riesgos, las organizaciones pueden mejorar su capacidad para detectar y responder a las

ciberamenazas emergentes, salvaguardando así sus activos críticos y manteniendo la confianza de sus partes interesadas. (Allaico, 2021)

2.12 Amenaza.

Los eventos que aprovechan una vulnerabilidad dentro de un sistema tienen el potencial de iniciar un incidente dentro de una organización y provocar daños tangibles o pérdidas intangibles para sus recursos. Estos eventos abarcan una variedad de acciones, incluidas las interrupciones de las operaciones normales o los casos en los que no se toman las medidas necesarias, lo que aumenta la probabilidad de que se produzcan consecuencias negativas. (Allaico, 2021)

En seguridad informática, una amenaza se define como uno o más factores que pueden afectar gravemente a un sistema, si están presentes, incluidas amenazas físicas y lógicas graves o de bajo nivel. Las amenazas lógicas se refieren a diversas formas de software, utilidades de seguridad, puntos de acceso ilícitos, malware y entidades similares, y pueden interrumpir las operaciones estándar del sistema. Por el contrario, las amenazas físicas abarcan un amplio espectro de riesgos que pueden tener consecuencias perjudiciales para una organización, incluidos, entre otros, el robo, el deterioro de la infraestructura, las condiciones climáticas desfavorables y la ocurrencia de calamidades tanto naturales como provocadas por el hombre. (Farinango, 2023)

Según (Gutiérrez Mendoza, 2022) menciona que cualquier acto que aproveche vulnerabilidades para atacar la seguridad de los sistemas de información. Sin embargo, esto podría afectar negativamente a ciertos elementos de nuestro sistema. Las amenazas pueden provenir de diversas fuentes, como ataques malintencionados (por ejemplo, fraudes, robos, virus), desastres naturales (por ejemplo, incendios, inundaciones) o descuidos y elecciones organizacionales (por ejemplo, un manejo incorrecto de las contraseñas o la falta de uso del cifrado). Estas amenazas, vistas desde una perspectiva

organizacional, pueden provenir tanto de dentro de la organización como de fuentes externas.

Los eventos inesperados o intencionales ya sean el resultado de un error humano o de una intención malintencionada, tienen el potencial de infligir una amplia gama de efectos perjudiciales en los sistemas y recursos informáticos, que incluyen, entre otros, pérdidas materiales y financieras. Estos eventos pueden interrumpir las operaciones, comprometer los datos confidenciales y socavar la seguridad y la funcionalidad generales de los sistemas en cuestión. Dentro del ámbito de las ciberamenazas, existen varias clasificaciones que ayudan a diferenciar la naturaleza y el impacto de estos incidentes, lo que contribuye a una comprensión más matizada de los riesgos y vulnerabilidades a los que se enfrenta el panorama digital. (Reyna Carrión, 2023)

De acuerdo con las siguientes definiciones tenemos los tipos de amenazas como:

- **Amenazas Naturales:** terremotos, incendios, inundaciones, tormentas, entre otros.
- **Agentes externos:** virus informático, destrucción terrorista, fraude, ataque criminal, conflicto social.
- **Agentes Internos:** poco capacitados o descontentos, colaboradores irresponsables, mal uso de los recursos del sistema.

2.13 Confidencialidad.

La confidencialidad se refiere al uso de la información por personas o instalaciones debidamente autorizadas. Para garantizar la confidencialidad se basa en tres tipos de mecanismos como son: autenticación, autorización y cifrado.

La Organización para la Cooperación y el Desarrollo Económico (OCDE) define la confidencialidad como "la divulgación de cualquier dato o información únicamente a

personas, entidades o mecanismos autorizados en momentos autorizados y de manera autorizada". Se podrán tomar ciertas medidas como contraseñas, palabras clave, tiempos de acceso, carpetas o sitios definidos, etc. para garantizar la confidencialidad de la información. (Farinango, 2023)

Busca prevenir el acceso no autorizado ya sea en forma voluntaria o no voluntaria a la información. El compromiso de la confidencialidad puede manifestarse a través de varias vías, incluida, entre otras, la divulgación deliberada de información confidencial que pertenece a la entidad. Estas violaciones de la confidencialidad pueden tener consecuencias perjudiciales para las operaciones y la reputación de la organización. (Farinango, 2023)

2.14 Integridad.

Su finalidad es garantizar que los datos o procesos no sean modificados por personas no autorizadas y que los datos sean coherentes tanto interna como externamente. La integridad de la información significa que los datos conservan su originalidad, asegurando que la información no haya sido alterada por personas u organizaciones no autorizadas, en otras palabras, la entrega del mensaje no puede ser alterada mientras se procesa. ha llegado al destino.

La inmutabilidad de la información es uno de los principios básicos de la seguridad porque determina el porcentaje de confiabilidad de la información a menos que la información sea modificada o cambiada bajo el control de personal autorizado. Una de las principales amenazas a las que se enfrentan las empresas a la hora de gestionar la información son los cambios repentinos en los datos (por ejemplo, cuentas bancarias). (Farinango, 2023)

2.15 Disponibilidad.

Busca garantizar la disponibilidad confiable y puntual de datos o activos para las personas adecuadas, enfatizando así la importancia de establecer mecanismos que apoyen el flujo continuo de información y recursos dentro de las estructuras organizacionales, con el objetivo final de mejorar la eficiencia operativa y la productividad. (Farinango, 2023).

2.16 Norma ISO 22301.

La ISO 22301, representa la versión más actualizada y autorizada de un conjunto de regulaciones que delinea las mejores prácticas destinadas a proporcionar a las organizaciones un marco sólido para gestionar y mitigar de manera efectiva los posibles efectos adversos derivados de cualquier posible interrupción de sus funciones operativas; además, el objetivo principal de esta norma va más allá de la mera reducción del impacto de dichas interrupciones, ya que también abarca la función crítica de ayudar a las organizaciones a comprender de manera integral y analizar meticulosamente los tipos específicos de impactos que pueden ocurrir, así como evaluar la magnitud de estos impactos, lo que permite a las organizaciones determinar el nivel de impacto que están dispuestas a aceptar, junto con la variedad de posibles interrupciones a las que pueden enfrentarse, lo que requiere la implementación de un sistema de gestión de la continuidad del negocio personalizado que se alinee con sus requisitos operativos y necesidades organizacionales únicos. (Enríquez Bastidas, 2024).

En particular, la norma ISO 22301 es versátil y puede ser implementada por organizaciones de cualquier tamaño, ya sea que se dediquen a la provisión de bienes o servicios, ya que ofrece un enfoque estructurado y preciso de los procesos esenciales de preparación, prevención, gestión y recuperación de situaciones que podrían ser extremadamente complejas y difíciles de manejar. La principal ventaja de adoptar esta norma es su capacidad para prevenir eficazmente la improvisación en respuesta a las

crisis, fomentando así un enfoque más organizado y estratégico de la continuidad empresarial. La importancia de estar adecuadamente preparado para cualquier situación crítica o imprevista, de acuerdo con la norma ISO 22301 y sus recomendaciones asociadas relacionadas con el Plan de Continuidad del Negocio (BCP), surge como un factor crítico de suma importancia dentro del marco operativo de cualquier organización. El objetivo principal tal como se describe en la norma ISO 22301, es proporcionar a las organizaciones la orientación y el apoyo necesarios para protegerse de manera efectiva, mitigar los riesgos o recuperarse de cualquier evento no planificado o disruptivo que pueda amenazar sus operaciones. (Díaz Parco, 2022)

2.16.1 Beneficios de la Norma ISO 22301.

El texto subraya la importancia fundamental que ha adquirido la gestión estratégica de los eventos potencialmente peligrosos en relación con la capacidad general de las empresas para identificar, evaluar y gestionar dichos riesgos de manera eficaz y, aunque estos eventos o amenazas pueden ser de naturaleza diversa e incluso altamente impredecibles, con frecuencia se caracterizan por su potencial de perturbar significativamente las operaciones comerciales habituales, y es esencial señalar que estas amenazas van en aumento y abarcan desafíos contemporáneos como los ciberataques y pandemias globales, como las crisis recientes que han afectado al mundo, así como diversas formas de desastres naturales, que en conjunto subrayan la necesidad de que las organizaciones anticipen de manera proactiva estos riesgos e implementen herramientas y estrategias sólidas que puedan gestionar y mitigar eficazmente los impactos durante estos períodos de mayor incertidumbre, garantizando así la resiliencia y la continuidad de las actividades comerciales frente a tales desafíos. (Enríquez Bastidas, 2024)

CAPITULO III

3. MARCO METODOLÓGICO

3.1 Enfoque de la Investigación

Este trabajo investigativo emplea un enfoque mixto que integra lo cualitativo y lo cuantitativo, utilizando el análisis documental para explorar y detallar los riesgos que podrían comprometer la continuidad de las operaciones del Departamento de TIC del Municipio de Cañar, mientras que la parte cuantitativa se enfoca en evaluar dichos riesgos mediante herramientas como matrices de impacto y probabilidad, así como el análisis de impacto al negocio (BIA), permitiendo una evaluación integral para establecer prioridades y diseñar estrategias efectivas de mitigación.

3.2 Nivel de Investigación

El nivel de la investigación será descriptivo, ya que se realizará un levantamiento de información del Departamento de TIC del Municipio de Cañar, además de la identificación y descripción de los riesgos que enfrenta dicho departamento, lo cual permitirá comprender las posibles afectaciones a la continuidad de sus operaciones y diseñar estrategias adecuadas de mitigación.

3.3 Población y Muestra

La investigación se centra específicamente en el Departamento de TIC del Municipio de Cañar, donde trabajan cuatro profesionales en el área, delimitando claramente el enfoque del estudio.

3.4 Técnicas e Instrumentos de Recolección

La investigación se basó en una revisión íntegra del marco teórico sobre los temas relacionados al desarrollo del plan de continuidad que permitan obtener información precisa y completa para la gestión estratégica del departamento de TIC.

Entre las técnicas utilizadas están:

- **Entrevista:** La entrevista se realiza al jefe de TIC, para profundizar en sus perspectivas, requisitos, preocupaciones y expectativas en relación con la continuidad del negocio y la protección de los sistemas de TIC. Su participación permite recopilar información detallada y datos exhaustivos sobre la forma en que estas partes interesadas perciben y priorizan la resiliencia y la seguridad de la infraestructura de las TIC.

3.5 Selección de la norma para la gestión de Continuidad de negocio

Tras realizar una comparación detallada entre la norma ISO 22301 y el estándar NIST SP 800-34 en el capítulo 2, se concluye que la norma ISO 22301 es la más adecuada para el desarrollo de este proyecto. Esto se debe a su enfoque integral hacia la organización, garantizando que las decisiones se alineen con la continuidad del negocio. De esta manera, la ISO 22301 proporciona a la organización las herramientas necesarias para estar mejor preparada ante cualquier interrupción inesperada, asegurando una respuesta y recuperación más eficientes.

3.6 Selección de la metodología para análisis y gestión de riesgo

Para el análisis y gestión de riesgos en este proyecto se seleccionó la metodología MAGERIT, debido a su enfoque estructurado y adecuado para los riesgos relacionados con la tecnología de la información. MAGERIT facilita la identificación, evaluación y tratamiento de riesgos en los activos de información, considerando tanto amenazas externas como vulnerabilidades internas. Además, permite definir medidas de seguridad y controles para mitigar los riesgos, lo que es esencial para asegurar la continuidad de los servicios tecnológicos en el Departamento de TIC del Municipio de Cañar

3.7 ANALISIS E INTERPRETACIÓN DE LOS DATOS

Tabla 1 Entrevista al Analista Informático de Desarrollo

Gobierno Autónomo Descentralizado Intercultural del Cantón	**EMPRESA:**	**CÓDIGO:**
CAÑAR CANTÓN INTERCULTURAL	Departamento de TIC del Municipio de Cañar	**FECHA: 18/07/2024**
	ENTREVISTA: Jefe de TI	**VERSIÓN:** Ing. Danny Andrade

Estimado entrevistado:
El propósito de esta encuesta es comprender en detalle los procesos y recursos críticos que integran la cadena de valor de su empresa.

PREGUNTAS	**RESPUESTA**
1. ¿El municipio cuenta con un plan de continuidad de negocio para el Departamento de TIC?	Contamos con un plan básico de continuidad de negocio, pero aún estamos en proceso de afinar y documentar todos los procedimientos específicos para el Departamento de TIC
2. ¿El Departamento de TIC tiene procesos bien definidos y con responsables asignados?	Sí, aunque algunos procesos están bien definidos, aún estamos trabajando en la formalización y documentación completa de todos los procedimientos, especialmente los que involucran a otras áreas del municipio.
3. ¿El municipio realiza la gestión de riesgos de seguridad de la información en el Departamento de TIC?	Se gestiona los riesgos de seguridad de la información y tenemos un plan de tratamiento de riesgos que estamos implementando gradualmente en todo el departamento.
4. En caso de que se presenten problemas con los equipos o suspensiones de servicio, ¿el Departamento de TIC tiene procedimientos definidos para minimizar el impacto en las operaciones del municipio?	Estoy consciente de los riesgos potenciales que podrían afectar a la empresa, como la energía eléctrica que podría afectar a los equipos.
5. ¿Con qué frecuencia realiza el análisis de riesgos y la evaluación de la continuidad del servicio en el Departamento de TIC?	Realizamos el análisis de riesgos de manera semestral, pero aún no tenemos un proceso definido para la evaluación continua. Sin embargo, se está trabajando en establecer revisiones mensuales.
6. ¿Ha identificado el Departamento de TIC los factores determinantes de los riesgos que enfrenta el municipio?	hemos identificado algunos riesgos críticos, como posibles fallas en el servidor y ataques cibernéticos, pero aún estamos trabajando en una evaluación más exhaustiva y en su documentación
7. ¿Conoce el municipio la probabilidad de ocurrencia y el impacto de los riesgos tecnológicos en los servicios proporcionados?	tenemos una comprensión general de los riesgos tecnológicos, y aunque no todos están documentados en detalle, estamos utilizando herramientas para mejorar la evaluación y planificación.
8. ¿Qué tipo de información maneja el Departamento de TIC en el municipio?	El Departamento de TIC maneja principalmente información administrativa, de recursos humanos y de servicios prestados a los ciudadanos, con un enfoque particular en la protección de datos personales.
9. ¿Cuáles considera que son los tipos de información más críticos en el Departamento de TIC?	La información de los ciudadanos y la información administrativa relacionada con la gestión de servicios

	municipales son las más críticas, ya que afectan directamente a la prestación de servicios esenciales.
10. ¿El Departamento de TIC cuenta con una estrategia de seguridad física y control de acceso para proteger los activos tecnológicos?	tenemos controles de acceso físico, como tarjetas de seguridad para ingresar a áreas restringidas y cámaras de vigilancia. Además, las áreas donde se encuentran los servidores están protegidas con cerraduras y sistemas de seguridad adicionales.
11. En caso de una amenaza informática o un incidente, ¿el Departamento de TIC tiene tiempos de recuperación establecidos y procedimientos claros?	Aún no tenemos tiempos de recuperación estandarizados, pero estamos trabajando en establecer un plan de respuesta ante incidentes y tiempos de recuperación para minimizar el impacto en los servicio
12. ¿El Departamento de TIC tiene alguna estrategia para realizar pruebas o simulacros de continuidad del negocio?	Actualmente no realizamos simulacros regulares, pero estamos implementando un plan para llevar a cabo pruebas de recuperación de desastres y simulacros de interrupciones para mejorar nuestra capacidad de respuesta
13. ¿Cómo maneja el Departamento de TIC las amenazas externas, como ciberataques, y qué medidas de protección están implementadas?	El Departamento de TIC cuenta con medidas básicas de protección como un firewall, antivirus, y filtros de contenido. Sin embargo, estamos trabajando en fortalecer estas medidas y en incorporar nuevas tecnologías de detección y respuesta ante ciberataques.

Análisis de la entrevista:

La entrevista al Jefe de TI del Municipio de Cañar destacó avances en la gestión de riesgos y continuidad del negocio, pero también reveló áreas de mejora. Aunque existe un plan básico de continuidad, aún se encuentra en desarrollo y falta formalizar procesos y asignar responsabilidades de manera integral. La gestión de riesgos está en fase de implementación y necesita un enfoque más estructurado. El municipio tiene procedimientos documentados para la respuesta ante incidentes, pero no realiza simulacros regulares. La seguridad física está bien gestionada. En resumen, el municipio debe fortalecer la documentación, evaluación de riesgos y realizar simulacros para mejorar la resiliencia ante interrupciones tecnológicas.

CAPITULO IV

PROPUESTA

En el siguiente capítulo se presenta la propuesta para la elaboración de un plan de continuidad de negocio específicamente diseñado para el Municipio de Cañar. El objetivo de esta guía es servir como referencia y facilitar el desarrollo del BCP para el municipio, pudiendo adaptarse también a otras entidades públicas de diferentes tamaños a nivel nacional.

Luego de realizar un análisis comparativo de metodologías y estándares para la creación de un Plan de Continuidad de Negocio y para la gestión y análisis de riesgos, se ha decidido adoptar la norma ISO 22301 como la base para el desarrollo del BCP y la metodología MAGERIT para la evaluación de riesgos dentro del contexto del Municipio de Cañar.

4. Desarrollo de un plan de continuidad de negocio en base a la metodología ISO 22301

4.1 Creación de programa BCP

Para la elaboración del Plan de Continuidad de Negocio (BCP) en el Municipio de Cañar, se comenzó por definir a los líderes clave para este proceso, quienes serán responsables de su implementación y supervisión.

- **Jefe del departamento de tecnologías de la información**

El responsable principal del BCP será el jefe del área de TI, quien, junto con el gerente de TI, tendrá la tarea de conformar un comité de evaluación o comité de riesgos. Este equipo será el encargado de gestionar las acciones necesarias en caso de que se presenten riesgos que puedan afectar las operaciones del municipio.

El objetivo principal de la creación del BCP es garantizar que todo el personal administrativo y operativo del Municipio de Cañar, así como los responsables involucrados en el Plan de Continuidad de Negocio, conozcan claramente los procedimientos a seguir ante cualquier incidente que pueda impactar los servicios informáticos y las operaciones municipales.

4.2 Comprensión de la Empresa

- **Visión**

Cañar se constituye como una arista intercultural, sociable, con justicia, con un mundo satisfecho por los servicios que recibe.

- **Misión**

Construir una sociedad equitativa, intercultural, justa, que brinde servicios prestados con amabilidad, apoyados en la cooperación local e internacional con comunicación oportuna para todas las operaciones.

4.2.1 Estructura Orgánica

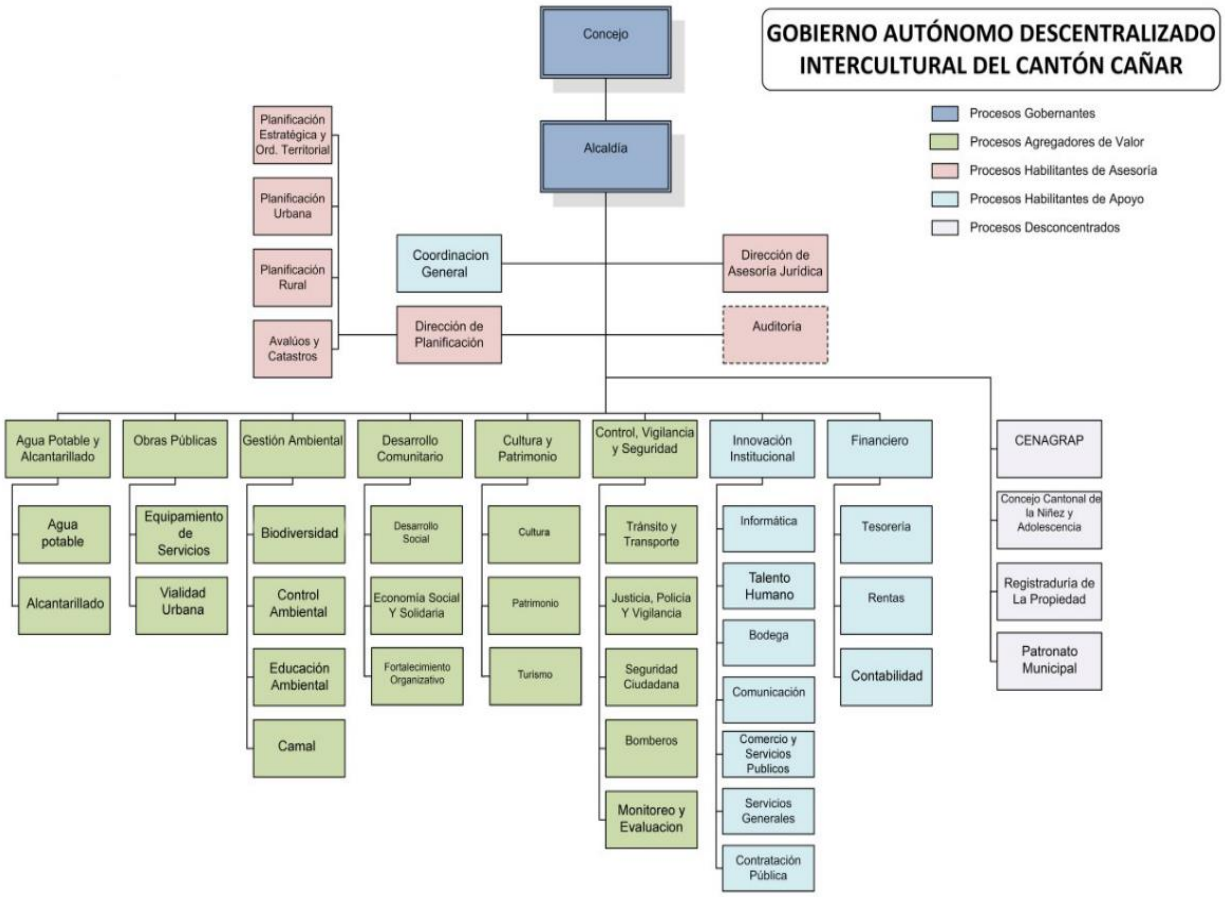


Ilustración 1 Organigrama estructural del GADIC Cañar

4.2.2 Metas y Objetivos de la Unidades Administrativas

GADMUNICIPAL DE CAÑAR

PROCESOS GOBERNANTES NIVEL DIRECTIVO

- Secretaria del concejo cantonal (1)
- Dirección de administración y Gobierno (1)

PROCESOS AGREGADORES DE VALOR NIVEL OPERATIVO

- Dirección de obras públicas (4)
- Dirección de agua potable
- Dirección de Territorio y control
- Dirección de movilidad
- Dirección de desarrollo social economía popular y solidaria
- Dirección de cultura y patrimonio
- Innovación Institucional
- Financiero
- Administración y gobierno

PROCESOS DESCONCENTRADOS

- Junta para la protección de derechos
- Concejo para la protección de derechos
- Centro de atención de Sistemas de agua rural (CENAGRAP)
- Registro de la propiedad
- Empresa Municipal de terminal terrestre

NIVEL DE APOYO ASESORÍA

- Asesoria Jurídica
- Dirección de Planificación

Ilustración 2 Metas y Objetivos GAD Cañar. Fuente: Información de sitio oficial LOTAIP 2021- GAD Municipal de Cañar (https: www.canar.gob.eclotaip-año-2021) Autor: Propio

4.2.3 Organigrama del municipio

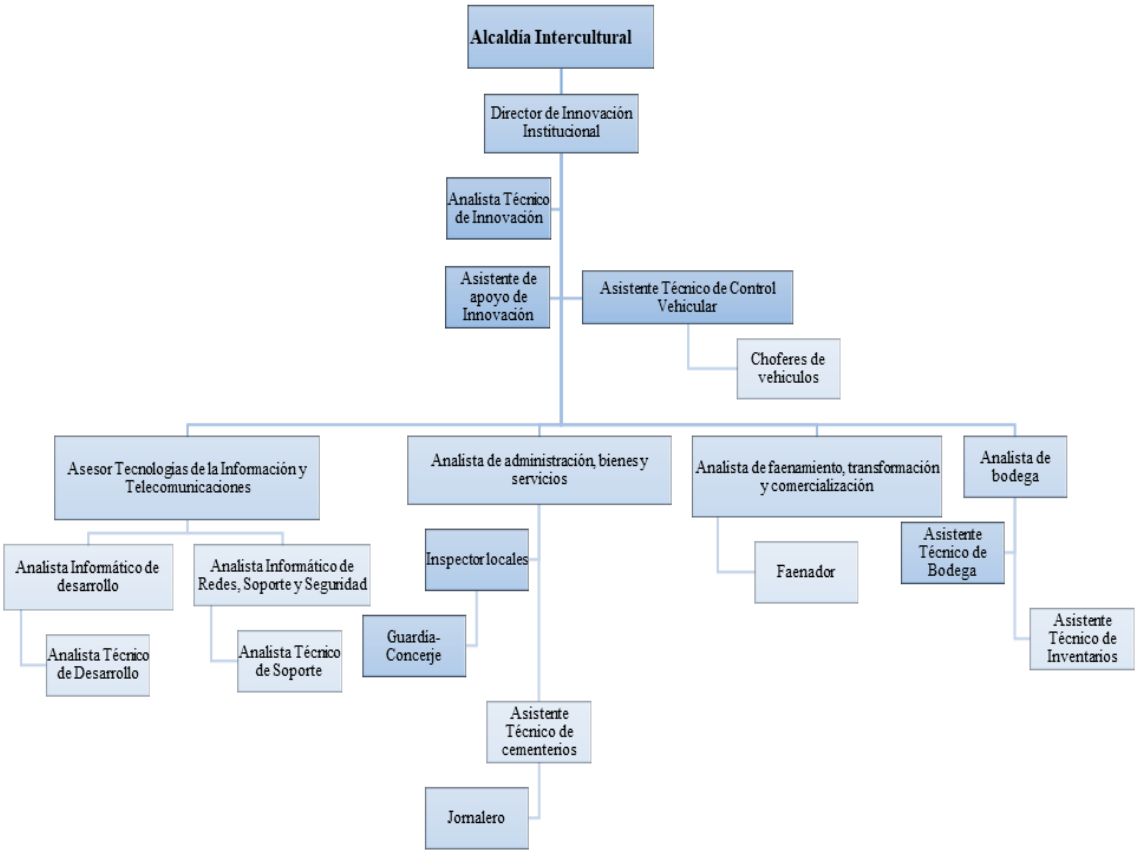


Ilustración 3 4 Identificación de tecnología de información y comunicación Fuente: Información de sitio oficial LOTAIP 2021- GAD Municipal de Cañar (https: www.canar.gob.eclotaip-ano-2021) Autor: Guamán (2021)

4.2.4 Organigrama del departamento de TIC

La unidad de Tecnologías de la Información y Comunicaciones del GAD Municipal de Cañar, conocida como "Asesoría de Tecnologías de la Información y Comunicaciones", se encuentra bajo la supervisión del Director de Innovación Institucional del GAD Cantonal de Cañar. Su función dentro de la estructura organizativa se considera un proceso de apoyo. Según el Estatuto Integral de Gestión Organizacional del GAD Cantonal de Cañar, el Asesor de Tecnologías de la Información y Telecomunicaciones tiene la responsabilidad de realizar análisis, presentar propuestas, diseñar y supervisar la implementación de proyectos innovadores que busquen mejorar la eficiencia del GAD

cantonal en el ámbito de las TIC, enfocándose en proporcionar soluciones tecnológicas para los procesos del GAD Municipal de Cañar.

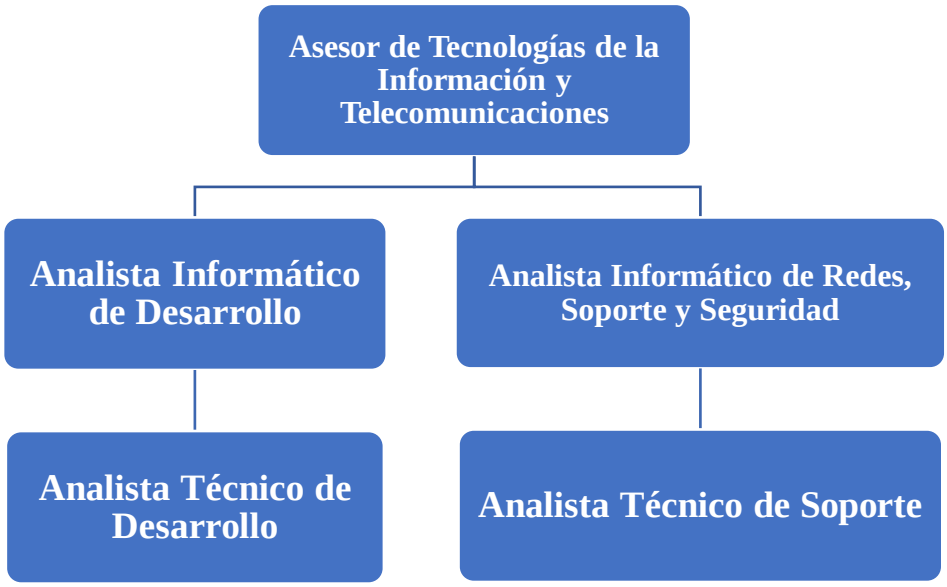


Ilustración 4 Estructura Orgánica del Departamento de TIC del GAD Municipal del Cañar

4.2.5 Personal de TI

El Departamento de TIC del municipio de Cañar está estructurado para asegurar una división clara de responsabilidades en áreas críticas para la continuidad operativa. En la cúspide de la jerarquía se encuentra el Asesor de Tecnologías de la Información y Telecomunicaciones, quien establece las directrices y coordina la estrategia tecnológica del municipio. Este rol implica una visión integral y orientada a la alineación de los recursos tecnológicos con los objetivos organizacionales, lo que resulta fundamental para responder ante posibles interrupciones operativas.

Los Analistas de Desarrollo y Redes cumplen roles especializados en el desarrollo de aplicaciones, gestión de redes, seguridad y soporte técnico, permitiendo una respuesta rápida y técnica ante necesidades específicas. En particular, el Subsistema de Desarrollo y el Subsistema de Mantenimiento aseguran que el desarrollo de software y el soporte a infraestructura estén en constante mejora y listos para adaptarse a cambios o incidentes,

promoviendo la resiliencia del municipio en situaciones de crisis. Esta estructura, con roles bien definidos, fortalece el enfoque del departamento hacia la eficiencia y seguridad tecnológica.

4.2.6 Identificación de Procesos

Para identificar los procesos organizacionales, se emplearon datos proporcionados por el jefe del Departamento de TI de la cooperativa, los cuales se detallan a continuación:

Tabla 2 Procesos de TI Fuente : Autor Propio

Unidad	Proceso
Asesor de Tecnologías de la Información y Telecomunicaciones	**Gestión de Proyectos de Innovación:** Planificación y supervisión de proyectos tecnológicos para mejorar los servicios del GAD Municipal.
	Planificación de Infraestructura Tecnológica: Evaluación y planificación de la infraestructura tecnológica para satisfacer demandas municipales.
	Evaluación de Riesgos Tecnológicos: Identificación y evaluación de riesgos tecnológicos para minimizar vulnerabilidades.
Analista Informático de Desarrollo	**Desarrollo de Software:** Diseño y programación de aplicaciones personalizadas para apoyar las operaciones del municipio.
	Mejora y Mantenimiento de Aplicaciones: Actualización y mejora de las aplicaciones existentes según las necesidades del municipio.
	Pruebas de Software: Realización de pruebas para asegurar calidad, seguridad y funcionalidad de las aplicaciones.
	Documentación de Software: Creación de manuales y documentación técnica para el mantenimiento de las aplicaciones.
	Gestión de Redes y Conectividad: Administración de redes y servicios de conectividad para asegurar la conectividad continua.
	Soporte Técnico a Usuarios: Soporte técnico para resolver problemas con hardware, software y equipos de red.
	Gestión de Seguridad Informática: Implementación de políticas de seguridad,

Analista Informático de Redes, Soporte y Seguridad	firewalls y antivirus para proteger la infraestructura tecnológica.
	Auditoría de Seguridad: Realización de auditorías para asegurar la seguridad y cumplimiento de normativas.
	Mantenimiento de Equipos Informáticos: Mantenimiento y reparación de hardware y actualización de software.
	Gestión de Inventarios de TI: Control y gestión de los inventarios de equipos y materiales tecnológicos.
Analista Técnico de Soporte	**Resolución de Incidentes Técnicos:** Diagnóstico y solución de problemas relacionados con equipos informáticos y software.
	Soporte en la Implementación de Nuevas Tecnologías: Asistencia en la instalación y configuración de nuevas tecnologías.

4.2.7 Identificación de Activos

Es fundamental clasificar los activos según su tipo, de acuerdo con la función que desempeñan. El Departamento de TI del GADICC dispone de diversos activos, los cuales son cruciales para el desarrollo del proyecto.

4.2.7.1 Hardware

Tabla 3 Activos de Hardware Fuente: Autor Propio

CÓDIGO	ACTIVO	DESCRIPCIÓN
A1	Red jerárquica	Esta red se encuentra estructurada y certificada en la categoría 6A
A2	Conexión -Fibra óptica	Conexión alrededor de todo el edificio del GADICC.
A3	Servidor Virtualizado	Para la ejecución de servidores de Base de Datos y servidores de Aplicaciones.
A4	Servidor Antivirus	
A5	Servidor Correo Electrónico	
A6	Servidor para Internet	
A7	Servidor de Telefonía IP	

A8	UPS	De 10 KVA, con Batería redundante
A9	Equipos Clientes	Formados por computadoras tanto de escritorio como portátiles procesadores Core i3 como mínimo

4.2.7.2 Software

Tabla 4 Activos de Software Fuente: Autor Propio

CÓDIGO	ACTIVO	DESCRIPCIÓN
A10	Licencia de Windows Server 2016	Servidores Windows, Linux.
A11	Linux-Centos	V 6.0, para servidor de correo Electrónico e internet.
A12	Licencia de Windows 10	Licencias profesionales para los clientes.
A13	Licencia de Visual Studio 2010 y 2017	
A14	Oracle Database 11G R2	
A15	Zimbra	Servidor de Correo Electrónico
A16	Elastix	Servidor para Telefonía IP
A17	Sistema Integrado de Servicios Municipales	
A18	Sistema AME (Asociación de Municipalidades Ecuatorianas)	Para la gestión contable
A19	Kaspersky	Antivirus
A20	Firewall basado en IPtables	

4.2.7.3 Recurso Humanos

Tabla 5 Recursos Humanos Fuente: Autor Propio

Ing. Nery Sanclemente	
Ing. Adrian Serrano	Analista de Desarrollo
Ing. Tito Guasco	Analista Técnico de Desarrollo
Ing. Wilson Lema	Analista Técnico de Soporte
Ing. Dany Andrade	Analista de Soporte y Redes

4.3 EVALUACION DE RIESGOS EN BASE A LA METODOLOGÍA MAGERIT.

Para valorar los activos según la metodología MAGERIT, se emplea una combinación de escalas cualitativas y cuantitativas, las cuales se presentan en las tablas a continuación:

Tabla 6 categoría nivel de riesgo

VALOR	NIVEL	
1	Muy Baja	Tomar acciones en caso de que el riego aumente
2	Baja	Riesgo aceptable
3	Media	Presenta un nivel de riesgo moderado
4	Alta	Riesgo inaceptable puede provocar perdidas que se materializa
5	Muy Alta	Riesgo inadmisible, que demanda acción de forma inmediata

Tabla 7 Escala de valoración paralos procesos e activos

INTERVALO	CUALIFICACIÓN
De 1 a 14	Medio
De 14 a 20	Alto
De 21 a 25	Critico

Tabla 8 Nivel de probabilidad

Probabilidad de ocurrencia	
Descripción	**Valor**
Muy frecuente	5
Frecuente	4
Normal	3
Poco frecuente	2
Muy poco frecuente	1

4.3.1 Valoración de riesgos a los procesos

La valoración de riesgos a los procesos es un componente clave en la gestión de la seguridad de la información, ya que permite identificar y evaluar los riesgos asociados a los procesos críticos de la entidad.

Valor de activo = autenticidad +confidencialidad +integridad +disponibilidad + trazabilidad

Tabla 9 Calificación a los procesos de TI Fuente: Autor Propio

PROCESOS	AUTENTICIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	TOTAL	valoración
Gestión de Proyectos de Innovación	3	4	4	4	3	18	medio
Planificación de Infraestructura Tecnológica	4	5	4	4	4	21	critico
Evaluación de Riesgos Tecnológicos	4	5	5	4	4	22	critico
Desarrollo de Software	4	5	5	4	4	22	critico
Mejora y Mantenimiento de Aplicaciones	4	4	5	4	4	21	critico
Pruebas de Software	4	4	5	4	3	20	alto
Documentación de Software	3	4	3	4	3	17	medio
Gestión de Redes y Conectividad	5	5	5	4	4	23	critico
Soporte Técnico a Usuarios:	4	5	5	5	4	23	critico
Gestión de Seguridad Informática	4	5	5	5	5	24	critico
Mantenimiento de Equipos Informáticos	4	4	5	4	5	22	critico
Gestión de Inventarios de TI	3	4	4	4	4	19	alto
Resolución de Incidentes	4	5	3	3	4	19	alto
Soporte en la Implementación de Nuevas Tecnologías	4	5	3	4	3	19	alto

4.3.2 Probabilidad- impacto de los procesos de TI

La siguiente matriz tiene como propósito identificar, analizar y cuantificar los riesgos que afectan los procesos de TI, facilitando la toma de decisiones sobre la asignación de recursos y la implementación de controles de seguridad

Riesgo= Probabilidad de ocurrencia * Impacto

Tabla 10 Calificación de Probabilidad- impacto de los procesos de TI

Activo	Código Amenaza	Amenaza	Probabilidad de ocurrencia	Impacto	Impacto * probabilidad	Riesgo
Planificación de Infraestructura Tecnológica	[A.11]	Acceso no autorizado	3	3	9	medio
	[A.25]	Robo	5	3	15	medio
	[E.15]	Alteración accidental de la información	4	4	16	Alto
	[E.4]	Errores de configuración	2	4	8	Bajo
	[A.18]	Destrucción de información	2	5	10	Bajo
	[E.18]	Destrucción de información	3	5	15	Medio
	[E.19]	Fugas de Información	2	2	4	Bajo
	[E.28]	Indisponibilidad del personal	2	2	4	Bajo
	[A.15]	Modificación deliberada de la información	2	3	6	Bajo
Evaluación de Riesgos Tecnológicos	[A.11]	Acceso no autorizado	2	2	4	Bajo
	[E.3]	Errores de monitorización (log)	3	4	12	medio

	[E.8]	Difusión de software dañino	3	4	12	medio
	[E.18]	Destrucción de información	2	4	8	Bajo
	[E.19]	Fugas de Información	3	3	9	Medio
	[A.4]	Manipulación de la configuración	4	4	16	Alto
	[E.4]	Errores de configuración	3	4	12	medio
	[A.22]	Manipulación de programas	3	4	12	Medio
	[E.20]	Vulnerabilidades de los programas (software)	5	4	20	Alto
	[E.21]	Errores de mantenimiento / actualización de programas (software)	3	3	9	Bajo
	[A.24]	Denegación de servicio	4	2	8	Bajo
	[I.5]	Avería de origen físico o lógico	4	5	20	Alto
Desarrollo de Software	[I.5]	Avería de origen físico o lógico	3	5	15	Medio
	[I.6]	Corte del suministro eléctrico	4	3	12	Alto
	[E.1]	Errores de los usuarios	4	4	16	Alto
	[E.4]	Errores de configuración	3	5	15	Medio
	[E.20]	Vulnerabilidades de los programas (software)	3	4	12	Medio
	[E.21]	Errores de mantenimiento / actualización de programas (software)	4	4	16	Alto
	[A.8]	Difusión de software dañino	4	5	20	Alto
	[A.22]	Manipulación de programas	4	4	16	Alto
Mejora y Mantenimiento de Aplicaciones	[I.5]	Avería de origen físico o lógico	4	4	16	Alto
	[I.8]	Fallo de servicios de comunicaciones	4	3	12	medio
	[I.10]	Degradación de los soportes de almacenamiento de la información	3	5	15	Medio

	[E.4]	Errores de configuración	2	3	6	Bajo
	[E.8]	Difusión de software dañino	3	4	12	Medio
	[E.15]	Alteración accidental de la información	3	5	15	Alto
	[E.18]	Destrucción de información	3	5	15	Alto
	[E.20]	Vulnerabilidades de los programas (software)	3	4	12	Medio
	[E.21]	Errores de mantenimiento / actualización de programas (software)	4	4	16	Bajo
	[A.4]	Manipulación de la configuración	4	3	12	medio
Gestión de Redes y Conectividad	[I.5]	Avería de origen físico o lógico	3	5	15	Medio
	[I.6]	Corte del suministro eléctrico	2	3	6	Bajo
	[I.8]	Fallo de servicios de comunicaciones	2	2	4	Bajo
	[E.1]	Errores de los usuarios	2	5	10	medio
	[E.8]	Difusión de software dañino	3	3	9	Bajo
	[E.10]	Errores de secuencia	2	3	6	Bajo
	[E.19]	Fugas de Información	3	4	12	medio
	[E.20]	Vulnerabilidades de los programas (software)	4	5	20	Alto
	[E.21]	Errores de mantenimiento / actualización de programas (software)	3	3	9	Medio
	[E.28]	Indisponibilidad del personal	4	3	12	Medio
	[A.4]	Manipulación de la configuración	4	4	16	Alto
	[A.8]	Difusión de software dañino	4	4	16	Alto
	[A.11]	Acceso no autorizado	4	4	16	Alto

	[A.15]	Modificación deliberada de la información	4	4	16	Alto
	[A.18]	Destrucción de información	2	5	10	Medio
	[A.25]	Robo	2	5	10	Medio
Soporte Técnico a Usuarios	[E.25]	pérdida de equipos	3	4	12	medio
	[A.5]	Suplantación de la identidad del usuario	2	3	6	Bajo
	[A.11]	Acceso no autorizado	5	3	15	medio
	[A.23]	Manipulación de los equipos	4	4	16	Alto
	[A.25]	Robo	2	4	8	Bajo
	[I.8]	Fallo de servicios de comunicaciones	2	2	4	Bajo
	[E.23]	Errores de mantenimiento / actualización de equipos	3	2	6	Medio
Equipos de control de acceso	[I.1]	Fuego	2	3	6	Medio
	[A.5]	Suplantación de la identidad del usuario	3	5	15	Medio
	[A.11]	Acceso no autorizado	4	4	16	Alto
	[A.23]	Manipulación de los equipos	3	3	9	Medio
	[A.25]	Robo	1	4	4	Bajo
	[A.26]	Ataque destructivo	3	4	12	medio
	[E.23]	Errores de mantenimiento / actualización de equipos	2	3	6	Bajo
	[E.25]	pérdida de equipos	4	4	16	Medio
	[A.5]	Suplantación de la identidad del usuario	4	3	12	medio
	[A.11]	Acceso no autorizado	2	4	8	Bajo

	[A.23]	Manipulación de los equipos	3	3	9	Medio
	[A.26]	Ataque destructivo	3	4	12	Medio
Gestión de Seguridad Informática	[N.1]	Fuego	4	4	16	Bajo
	[I.5]	Avería de origen físico o lógico	2	2	4	Bajo
	[I.6]	Corte del suministro eléctrico	3	4	12	medio
	[I.8]	Fallo de servicios de comunicaciones	3	2	6	Bajo
	[A.30]	Ingeniería social (picaresca)	3	3	9	Bajo
	[E.23]	Errores de mantenimiento / actualización de equipos	3	4	12	Medio
	[E.25]	pérdida de equipos	1	3	3	Bajo
	[A.5]	Suplantación de la identidad del usuario	1	2	2	Bajo
	[A.11]	Acceso no autorizado	1	1	1	Bajo
	[A.23]	Manipulación de los equipos	1	1	1	Bajo
	[A.25]	Robo	1	2	2	Bajo
	[A.26]	Ataque destructivo	2	2	4	Bajo
Mantenimiento de Equipos Informáticos	[A.8]	Difusión de software dañino	2	5	10	medio
	[A.22]	Manipulación de programas	2	4	8	Medio
	[I.1]	Fuego	2	3	6	Medio
	[I.2]	Daños por agua	2	4	8	Medio
	[I.5]	Avería de origen físico o lógico	2	2	4	Bajo
	[I.6]	Corte del suministro eléctrico	3	4	12	medio
	[I.8]	Fallo de servicios de comunicaciones	2	2	4	Bajo
	[E.23]	Errores de mantenimiento / actualización de equipos	3	2	6	Medio

	[E.25]	pérdida de equipos	1	3	3	Bajo
	[A.5]	Suplantación de la identidad del usuario	1	2	2	Bajo
	[A.28]	Indisponibilidad del personal	3	3	9	medio
	[A.23]	Manipulación de los equipos	1	1	1	Bajo
	[A.25]	Robo	4	2	8	Bajo
	[A.26]	Ataque destructivo	3	2	6	Bajo

4.3.3 Contramedidas y salvaguardas para los procesos de TI

A continuación, se presenta una tabla con las contramedidas y salvaguardas propuestas por MAGERIT para cada uno de los activos y las amenazas que podrían surgir en cualquier momento, tanto dentro como fuera de la organización. El objetivo de estas medidas es establecer controles eficaces para actuar de manera inmediata ante posibles daños.

Tabla 11 Salvaguardas para los procesos de TI

Activo	Código Amenaza	Amenaza	Nivel de Riesgo	salvaguarda
Planificación de	[E.15]	Alteración accidental de la información	Alto	Políticas de respaldo automáticas, y controles de acceso para evitar modificaciones accidentales.

Infraestructura Tecnológica				
	[A.4]	Manipulación de la configuración	Alto	Control de cambios y auditoría en configuraciones críticas, herramientas de gestión de configuración
	[E.20]	Vulnerabilidades de los programas (software)	Alto	Parches de seguridad regulares y análisis de vulnerabilidades con herramientas especializadas.
	[I.5]	Avería de origen físico o lógico	Alto	Redundancia de hardware y sistemas de recuperación ante desastres.
Desarrollo de Software	[I.6]	Corte del suministro eléctrico	Alto	Uso de UPS (sistemas de alimentación ininterrumpida) y generadores de respaldo.
	[E.1]	Errores de los usuarios	Alto	Formación continua y conciencia sobre seguridad para los empleados.
	[E.21]	Errores de mantenimiento / actualización de programas (software)	Alto	Realizar copias de seguridad completas antes de realizar actualizaciones o mantenimiento.
	[A.8]	Difusión de software dañino	Alto	Uso de antivirus y soluciones de detección de malware, además de políticas de control de acceso.
	[A.22]	Manipulación de programas	Alto	Control de acceso basado en roles (RBAC) para restringir la modificación de programas.
Mejora y Mantenimiento de Aplicaciones	[I.5]	Avería de origen físico o lógico	Alto	Redundancia de hardware y respaldo de datos. Implementar una estrategia de recuperación ante desastres.
	[E.15]	Alteración accidental de la información	Alto	Uso de versiones y control de cambios para registrar modificaciones, además de la implementación de copias de seguridad.
	[E.18]	Destrucción de información	Alto	Implementación de cifrado de datos y políticas de eliminación segura de información.
Gestión de Redes y Conectividad	[E.20]	Vulnerabilidades de los programas (software)	Alto	Aplicación de parches de seguridad periódicamente y uso de herramientas de análisis de vulnerabilidades.
	[A.4]	Manipulación de la configuración	Alto	Implementación de gestión de configuraciones con control de versiones y auditorías regulares.
	[A.8]	Difusión de software dañino	Alto	Uso de antivirus y soluciones de detección de malware, además de políticas de control de acceso

	[A.11]	Acceso no autorizado	Alto	Implementar autenticación multifactor (MFA), y control de acceso basado en roles (RBAC).
	[A.15]	Modificación deliberada de la información	Alto	Implementación de controles de acceso y auditoría de actividades de usuarios.
Soporte Técnico a Usuarios	[A.23]	Manipulación de los equipos	Alto	Control de cambios y auditoría en configuraciones críticas, herramientas de gestión de configuración.
Equipos de control de acceso	[A.11]	Acceso no autorizado	Alto	Implementar autenticación multifactor (MFA), y control de acceso basado en roles (RBAC).

4.3.4 Valoración de riesgos a los activos

Tabla 12 Calificación a los Activos

ACTIVOS	DENOMINACION	AUTENTICIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	TOTAL	valoracion
Hardware	**Red jerárquica**	4	4	3	5	4	20	alto
	Conexión -Fibra óptica	5	4	4	4	4	21	critico
	Servidor Virtualizado	5	5	4	4	4	22	critico
	Servidor Antivirus	5	4	4	4	4	21	critico
	Servidor Correo Electrónico	4	4	4	4	4	20	alto
	Servidor para Internet	5	5	5	4	4	23	critico
	Servidor de Telefonía IP	3	4	2	2	3	14	medio
	UPS	4	3	3	3	2	15	alto
	Equipos Clientes	4	4	4	3	3	18	alto
	Licencia de Windows Server 2016	3	4	4	3	4	18	alto

Software	**Linux-Centos**	5	4	4	4	5	22	critico
	Licencia de Windows 10	4	3	4	3	3	17	alto
	Licencia de Visual Studio 2010 y 2017	4	4	4	4	4	20	alto
	Oracle Database 11G R2	5	5	5	5	5	25	critico
	Zimbra	4	4	3	3	3	17	medio
	Elastix	3	4	3	2	2	14	medio
	Sistema Integrado de Servicios Municipales	4	5	4	5	5	23	critico
	Sistema AME (Asociación de Municipalidades Ecuatorianas)	4	4	4	5	5	22	critico
	Kaspersky	4	3	4	3	4	18	medio
	Firewall basado en IPtables	5	5	4	4	4	22	critico
Recursos Humanos	**Personal de TI**	5	4	4	5	5	23	critico

4.3.4 Calculo de la Probabilidad- impacto de los Activos de TI

4.3.4.1 Software

Tabla 13 Calculo de la Probabilidad e Impacto de los activos de Software

Acttivo	Código de Amenaza	Amenaza	Probabilidad	Impacto	Riesgo
Licencia de Windows Server 2016	[E.20]	Vulnerabilidades de los programas (software)	3	4	Alto
	[A.6]	Abuso de privilegios de acceso	2	4	Alto
	[A.8]	Difusión de software dañino	2	4	Alto
	[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3	Medio
Linux-Centos	[A.7]	Uso no previsto	2	3	Medio
	[A.10]	Alteración de secuencia	2	3	Medio
	[A.11]	Acceso no autorizado	3	4	Alto
	[I.6]	Corte del suministro eléctrico	3	3	Alto
Licencia de Windows 10	[E.20]	Vulnerabilidades de los programas (software)	3	4	Alto
	[A.6]	Abuso de privilegios de acceso	3	4	Alto
	[A.12]	Análisis de tráfico	2	3	Medio
	[A.15]	Modificación deliberada de la información	2	3	Medio
Licencia de Visual Studio 2010 y 2017	[E.21]	Errores de mantenimiento / actualización de programas (software)	2	3	Medio
	[A.3]	Manipulación de los registros de actividad (logs)	2	4	Alto
	[A.5]	Suplantación de la identidad del usuario	2	4	Alto

	[I.5]	Avería de origen físico o lógico	3	3	Alto
Oracle Database 11G R2	[E.19]	Fugas de información	3	4	Alto
	[A.9]	[Re-]encaminamiento de mensajes	2	3	Medio
	[A.10]	Alteración de secuencia	2	3	Medio
	[E.15]	Alteración accidental de la información	3	3	Alto
Sistema Integrado de Servicios Municipales	[I.8]	Fallo de servicios de comunicaciones	3	4	Alto
	[A.15]	Modificación deliberada de la información	2	4	Alto
	[A.18]	Destrucción de información	2	4	Alto
	[A.7]	Uso no previsto	2	3	Medio
Sistema AME (Asociación de Municipalidades Ecuatorianas)	[A.4]	Manipulación de la configuración	2	3	Medio
	[E.18]	Destrucción de información	2	4	Alto
	[I.6]	Corte del suministro eléctrico	3	3	Alto
	[A.12]	Análisis de tráfico	2	3	Medio
Firewall basado en Iptables	[I.8]	Fallo de servicios de comunicaciones	3	3	Alto
	[A.13]	Repudio	2	3	Medio
	[A.14]	Interceptación de información (escucha)	3	4	Alto
	[A.5]	Suplantación de la identidad del usuario	3	4	Alto

4.3.4.2 Hardware

Tabla 14 Calculo de la Probabilidad e Impacto de los activos de Hardware

Activo	Código de Amenaza	Amenaza	Probabilidad	Impacto	Riesgo
Red jerárquica (Fibra óptica)	[I.8]	Fallo de servicios de comunicaciones	2	4	Alto
	[I.4]	Contaminación electromagnética	3	3	Alto
	[I.9]	Interrupción de otros servicios y suministros	2	3	Medio

	[A.12]	Análisis de tráfico	2	3	Medio
Conexión - Fibra Óptica	[I.6]	Corte del suministro eléctrico	3	3	Alto
	[A.8]	Difusión de software dañino	2	4	Alto
	[I.10]	Degradación de los soportes de almacenamiento	2	3	Medio
	[I.11]	Emanaciones electromagnéticas	2	3	Alto
Servidor Virtualizado	[I.5]	Avería de origen físico o lógico	3	3	Alto
	[A.5]	Suplantación de la identidad del usuario	2	4	Alto
	[E.19]	Fugas de información	3	3	Alto
	[A.10]	Alteración de secuencia	2	3	Medio
Servidor Antivirus	[I.6]	Corte del suministro eléctrico	3	3	Alto
	[A.8]	Difusión de software dañino	3	4	Alto
	[E.15]	Alteración accidental de la información	2	3	Medio
	[A.5]	Suplantación de la identidad del usuario	3	4	Alto
Servidor Correo Electrónico	[A.3]	Manipulación de los registros de actividad (logs)	2	3	Medio
	[E.5]	Escapes de información	3	3	Alto
	[A.14]	Interceptación de información (escucha)	2	4	Alto
	[A.11]	Acceso no autorizado	2	4	Alto
Servidor para Internet	[I.9]	Interrupción de otros servicios y suministros	3	4	Alto
	[A.7]	Uso no previsto	2	3	Medio
	[I.8]	Fallo de servicios de comunicaciones	3	3	Alto
	[A.12]	Análisis de tráfico	2	3	Medio
UPS (Uninterruptible Power Supply)	[I.6]	Corte del suministro eléctrico	3	3	Alto
	[E.5]	Escapes de información	3	4	Alto
	[I.7]	Condiciones inadecuadas de temperatura o humedad	2	3	Medio

	[A.15]	Modificación deliberada de la información	2	3	Medio
Equipos Clientes	[A.5]	Suplantación de la identidad del usuario	3	4	Alto
	[E.19]	Fugas de información	3	3	Alto
	[E.10]	Errores de secuencia	2	3	Medio
	[I.5]	Avería de origen físico o lógico	3	3	Alto

4.3.4.3 Recusrsos Humanos

Tabla 15 Calculo de la Probabilidad e Impacto de los activos de Recursos humanos

Activo	Código de Amenaza	Amenaza	Probabilidad	Impacto	Riesgo
Personal de TI	[E.28]	Indisponibilidad del personal	3	3	Alto
	[E.1]	Errores de los usuarios	3	3	Medio
	[A.9]	[Re-]encaminamiento de mensajes	2	3	Medio
	[A.12]	Análisis de tráfico	2	3	Medio

4.3.5 Contramedidas y salvaguardas para los Activos de TI

A continuación, se presenta una tabla que detalla las **salvaguardas** aplicadas a los activos del GAD Municipal de Cañar que presentan un nivel de riesgo alto**.** Estas salvaguardas se han diseñado de acuerdo con las amenazas identificadas en el análisis de riesgos, con el objetivo de mitigar los posibles impactos negativos sobre la infraestructura tecnológica y los servicios. Las medidas incluyen controles de acceso,

políticas de seguridad, actualizaciones regulares de software y monitoreo constante de los sistemas, entre otros, para garantizar la protección y disponibilidad de los activos críticos dentro de la organización.

Tabla 16 Contramedidas y salvaguardas para los Activos de TI

Activo	Código de Amenaza	Amenaza	Nivel de Riesgo	Salvaguarda
Licencia de Windows Server 2016	[E.20]	Vulnerabilidades de los programas (software)	Alto	Parcheo de seguridad regular y análisis de vulnerabilidades
Licencia de Windows 10	[E.20]	Vulnerabilidades de los programas (software)	Alto	Parcheo de seguridad regular y análisis de vulnerabilidades
Licencia de Visual Studio 2010 y 2017	[E.21]	Errores de mantenimiento / actualización de programas (software)	Alto	Implementación de actualizaciones regulares y control de versiones
Sistema Integrado de Servicios Municipales	[I.8]	Fallo de servicios de comunicaciones	Alto	Mantenimiento y supervisión de la infraestructura de comunicaciones
Kaspersky	[A.9]	[Re-]encaminamiento de mensajes	Alto	Implementación de controles de acceso y análisis de tráfico

Firewall basado en Iptables	[A.12]	Análisis de tráfico	Alto	Monitoreo constante de tráfico y filtrado de comunicaciones no autorizadas
Personal de TI	[E.28]	Indisponibilidad del personal	Alto	Planificación de continuidad del personal y capacitación regular
Licencia de Visual Studio 2010 y 2017	[A.6]	Abuso de privilegios de acceso	Alto	Implementación de controles de acceso y gestión de privilegios de usuarios

La siguiente matriz se presentan estrategias de recuperación tecnológica que puedan satisfacer eficazmente las necesidades de mitigación de riesgos. Además, se incluyen los tiempos de recuperación objetivo (RTO) y el punto de recuperación objetivo (RPO) para cada uno de los procesos.

Tabla 17 Matriz de RTO y RPO para el procesos críticos

Procesos	Subproceso	Responsable	Tiempo Máximo de Recuperación (RTO)	Tiempo Máximo de Obtención (RPO)	Salvaguarda
Planificación de Infraestructura Tecnológica	Planificación y supervisión de infraestructura	Responsable de sistemas	4 horas	2 horas	Políticas de respaldo automáticas y controles de acceso
Desarrollo de Software	Diseño y programación de aplicaciones	Responsable de desarrollo	4 horas	2 horas	Pruebas y control de calidad
Mejora y Mantenimiento de Aplicaciones	Actualización y mejora de las aplicaciones existentes	Responsable de TI	3 horas	1 hora	Actualización regular de aplicaciones
Gestión de Redes y Conectividad	Administración de redes y servicios de conectividad	Responsable de redes	2 horas	1 hora	Monitoreo de tráfico y redundancia de servicios
Soporte Técnico a Usuarios	Provisión de soporte técnico a usuarios	Técnico de soporte	2 horas	1 hora	Auditoría de actividad y registros log

Tabla 18 Matriz de RTO y RPO para los activos críticos

Activos	Subproceso	Responsable	Tiempo Máximo de Recuperación (RTO)	Tiempo Máximo de Obtención de Respaldos (RPO)	Amenaza	Nivel de Riesgo	Salvaguarda
Gestión de tecnologías de la información y seguridad informática	Administración de servidores del sistema financiero.	Responsable de sistemas	2 horas	1 hora	**[E.20] Vulnerabilidades de los programas (software)**	Alto	Parches de seguridad regular y análisis de vulnerabilidades
Gestión de tecnologías de la información y seguridad informática	Respaldo y restauración de información de los servidores	Responsable de sistemas	4 horas	1 hora	**[E.21] Errores de mantenimiento / actualización de programas (software)**	Alto	Implementación de actualizaciones regulares y control de versiones
Licencia de Windows Server 2016		Responsable de sistemas	2 horas	4 horas	**[I.8] Fallo de servicios de comunicaciones**	Alto	Mantenimiento y supervisión de la infraestructura de comunicaciones
Licencia de Visual Studio 2010 y 2017		Responsable de sistemas	2 horas	3 horas	**[A.9] [Re-]encaminamiento de mensajes**	Alto	Implementación de controles de acceso y análisis de tráfico
Sistema Integrado de Servicios Municipales		Responsable de sistemas	2 horas	2 horas	**[A.12] Análisis de tráfico**	Alto	Monitoreo constante de tráfico y filtrado de comunicaciones no autorizadas

Kaspersky		Responsable de sistemas	4 horas	2 horas	**[E.28] Indisponibilidad del personal**	Alto	Planificación de continuidad del personal y capacitación regular
Firewall basado en Iptables		Responsable de sistemas	4 horas	2 horas	**[E.20] Vulnerabilidades de los programas (software)**	Alto	Parches de seguridad regular y análisis de vulnerabilidades

Conclusiones

- A través de la aplicación de la metodología MAGERIT, se ha logrado identificar, evaluar y priorizar las amenazas tecnológicas que pueden impactar los activos más críticos dentro del municipio, especialmente en lo relacionado con la infraestructura tecnológica, las aplicaciones y la conectividad. La implementación de medidas preventivas y correctivas reduce el impacto de estas amenazas y asegura la protección de la información y los sistemas.
- Los resultados de la investigación indican que los procesos tecnológicos dentro del GAD Municipal de Cañar están alineados con los objetivos estratégicos de mejora de la infraestructura y la optimización de los servicios. Además, la mejora en la capacitación continua del personal y la actualización de las herramientas tecnológicas son factores determinantes para un buen desempeño del área de TI.
- la implementación de un Plan de Continuidad de Negocio (BCP) dentro del Departamento de Tecnologías de la Información (TI) del GAD Municipal de Cañar es esencial para garantizar la estabilidad y continuidad operativa de los servicios tecnológicos en situaciones de crisis

Recomendaciones

- Es recomendable que el GAD Municipal de Cañar implemente programas regulares de capacitación y certificación para el personal de TI, especialmente en áreas clave como seguridad informática, gestión de proyectos tecnológicos y administración de redes. Esto garantizará que el personal esté siempre actualizado en las mejores prácticas de la industria y pueda reaccionar de manera eficiente ante incidentes de seguridad.
- L
- a implementación de soluciones avanzadas de respaldo de datos, así como sistemas de recuperación ante desastres (DRP) que aseguren la integridad y disponibilidad de la información en todo momento. Estos sistemas deben estar probados y documentados para garantizar su funcionamiento adecuado en casos de emergencia.
- Se recomienda que el GAD Municipal de Cañar implemente un sistema de monitoreo proactivo que permita detectar posibles vulnerabilidades en tiempo real, sobre todo en las áreas más críticas como servidores, redes y aplicaciones. Además, la realización periódica de auditorías de seguridad y el análisis de vulnerabilidades contribuirán a mitigar los riesgos de forma preventiva, asegurando una protección constante de los activos tecnológicos.

4. Referencias Bibliográficas

Allaico, M. M. (2021). *Diseño de un plan de continuidad de negocio en la empresa Cañar net, Cañar-Ecuador.* Cañar, Ecuador: https://dspace.ucacue.edu.ec/handle/ucacue/12763.

Caizaguano, L. S. (2018). *DESARROLLO DE UNA GUÍA PARA PLANES DE CONTINUIDAD DE NEGOCIO DE TI ENFOCADO A LAS OPERADORAS MÓVILES DEL ECUADOR.*

Díaz Parco, P. (2022). *Plan de continuidad del negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC.* Ambato: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/36852.

Enríquez Bastidas, H. P. (2024). *Diseño del sistema de continuidad de negocio a través de la norma ISO 22301- 2019 para la empresa ModArte.* Ibarra.

Farinango, M. F. (2023). *Desarrollo de un plan de contingencia de servicios TI para la dirección de tecnologías de la información del Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, aplicando el marco de trabajo ITIL V3.* Ibarra, ecuador: https://repositorio.utn.edu.ec/handle/123456789/14762.

Gutiérrez Mendoza, A. J. (2022). *Diseño del plan de continuidad de negocio aplicado a seguridad de información en PYME Intervisión de Guayaquil*. Obtenido de dspace.ups.edu.ec: http://dspace.ups.edu.ec/handle/123456789/22136

Hurtado, J., & Paspuel, L. (2023). *Plan de continuidad del negocio de los activos tecnológicos Hardware y Software.* Tulcan: Universidad Politecnica Estatal del Carchi.

Jaramillo Camacho, J. A. (2022). *Diseño de un plan de continuidad de servicios del departamento de tecnologías de la información en casos excepcionales para la EP-EMAPA de la ciudad de Ambato.* Ambato, Ecuador: https://repositorio.puce.edu.ec/handle/123456789/9069.

Jaramillo, Á. G., & Díaz, P. A. (2022). *Plan de continuidad del negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC.* Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/36852

LOTAIP, G. M. (2021). *GAD Municipal de Cañar*. Obtenido de Cañar, Información de sitio oficial: https: www.canar.gob.eclotaip-año-2021

Mogrobejo, D. J. (2017). *DESARROLLO DE UN MODELO PARA LOS PROCESOS DEL ÁREA DE TENOLOGÍA DE INFORMACIÓN DE LA EMPRESA COMERCIALIZADORA DE COMBUSTIBLES "PETROLEOS Y SERVICIOS PYS C.A." UTILIZANDO COBIT 5.*

Montalban Ordoñez, W. E. (2022). *Diseño de un Plan de Continuidad Operativa de los servicios críticos del área de Sistemas y Tecnologías de la Información de la empresa Boticas y Salud, con base en la norma ISO/IEC 27031:2011.* Obtenido de http://creativecommons.org/licenses/by-nc-sa/4.0/

Quintanilla, M. A., & Crespo, G. G. (2017). *Fundamentos para Objetivos de Control en las TIC* (2 ed.). MQR.

Reyna Carrión, A. R. (2023). *ADMINISTRACIÓN Y DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.* Obtenido de ADMINISTRACIÓN Y DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

Salazar, C. (2019). *Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011.* Lima: https://repositorioacademico.upc.edu.pe/handle/10757/625692.

Anexos

Anexo 1. Protocolo de Investigación

UNIVERSIDAD CATOLICA DE CUENCA EXTENSIÓN CAÑAR

REDACCIÓN CIENTIFICA

DOCENTE: ING. JOSÉ ANTONIO CARRILLO ZENTENO.

ESTUDIANTE: LUIS FRANCISCO GUASCO LOJA.

TEMA: PROTOCOLO DE TRABAJO DE TITULACIÓN.

CICLO: OCTAVO.

2024.

Anexo:

1.25 Anexo 1: Protocolo de Trabajo de Titulación

A. TÍTULO
Desarrollo de un Plan de Continuidad para el Departamento de TIC en el municipio de Cañar

Marcar dependiendo el tema y a que campo se relaciona.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnología de la información y comunicación	Energía Eléctrica y Tecnologías de la Información para la Innovación y el Desarrollo Sostenible	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno Administrativo de Tecnologías de Información	
		Auditoria Informática	
		Seguridad Informática	
		Redes y Comunicación	
		Arquitectura de Hardware	
		Arquitectura de Desarrollo de Software	
		Ingeniería de Software	
		Gestión y Gobierno de Proyectos de Tecnología Informática	X
		Ingeniería de Requerimientos	
		Algoritmos y Programación	
		Ciencia exactas y naturales (Matemáticas, Física, Química, biología, etc.)	
		Modelaje y Simulación	

C. PLANTEAMIENTO DEL PROBLEMA

Hoy en día las instituciones públicas y privadas están en la evolución a gran escala mediante los constantes cambios, la infraestructura tecnológica ha beneficiado al desarrollo, pero todas las instituciones sufren situaciones de interrupción de las actividades y servicios, debido a desastres naturales, errores humanos, ciberataques. Por tal razón, el establecimiento de un plan de continuidad en el departamento de TIC dentro de los municipios garantiza que la administración local mantenga sus funciones críticas, protección de datos, disponibilidad continua de servicios digitales necesarios, servicios esenciales durante y después de diversas situaciones de desastres o emergencias.

La carencia de un plan de continuidad para el departamento de TIC en Cañar presenta consecuencias como la falta de información y los datos almacenados en los sistemas

informáticos del municipio haciendo inaccesible a dichos datos, lo que afecta la toma de decisiones y la prestación de servicios, los servicios en línea y las aplicaciones que ofrece el municipio a la ciudadanía, provocando inconvenientes y molestias a los usuarios. Otra situación que se presenta es en torno a los empleados del municipio que muchas veces no pueden realizar sus tareas de forma eficiente, lo que afecta la productividad general.

En tal virtud realizar un plan de continuidad que permita mitigar los riesgos y asegurar la operación de sus servicios en caso de una interrupción o desastres, contribuirá a que el departamento de Tecnologías de la Información y Comunicación (TIC) del municipio de Cañar juegue un papel fundamental en la gestión administrativa y la prestación de servicios a la ciudadanía.

D. OBJETIVO GENERAL

Desarrollar un plan de continuidad para el departamento de TIC en el municipio de Cañar.

E. OBJETIVOS ESPECÍFICOS

1. *Fundamentar mediante un estudio teórico el plan de continuidad para el departamento de TIC.*
2. *Analizar los riesgos, vulnerabilidades y amenazas para la determinación de estrategias de continuidad.*
3. *Elaborar un plan de continuidad según los resultados del análisis de riesgos, vulnerabilidades y amenazas.*

F. JUSTIFICACIÓN

En la actualidad las empresas o instituciones no solo son afectados por fenómenos como incendios o fallos tecnológicos, sino que es a nivel estratégico de la institución en el que la reputación y el valor de los funcionarios o accionistas son los elementos claves. A nivel nacional muchas instituciones como públicas o privadas indistintamente a su jerarquía institucional se ve afectada por perdida de información que se da por naturaleza mediante los diversos tipos de

riesgos o amenazas que han ocasionado daños significativos a la institución involucrada, sin embargo, no han buscado acciones para mitigar los riesgos que han afectado.

Por esta razón este trabajo de investigación es realizado con el propósito de desarrollar un plan de continuidad para el departamento de TIC en el municipio de Cañar para mitigar los riesgos existentes dentro de la institución, para ello es necesario entender las actividades a desarrollarse en cada una de las fases de este plan, evaluar los resultados obtenidos del análisis de riesgos, vulnerabilidades y amenaza.

De esta manera el municipio, ejecutará acciones o medidas que se encuentren en el plan de continuidad afrontando ante un posible riesgo o vulnerabilidad en el menor tiempo posible. Esto beneficia directamente al departamento de TIC, al municipio e indirectamente a toda la ciudadanía del cantón Cañar.

G. ALCANCE

Los alcances de este trabajo de investigación consisten en desarrollar un plan de continuidad para el departamento de TIC que garantice la función de los servicios que soportan procesos críticos dentro del municipio de Cañar.

H. CONCEPTOS RELACIONADOS

Para la correcta administración del plan de continuidad se deben establecer y mantener acciones que busquen cumplir con los requerimientos de mayor importancia para la información, son los siguientes:

Concepto de BCP (Plan de Continuidad de Negocio). Es la disciplina que prepara a una organización para mantener la continuidad en sus negocios en momentos de desastres, mediante la implementación de un Plan de Continuidad del Negocio. (Hurtado & Paspuel, 2023)

Vulnerabilidades.

Las vulnerabilidades se consideran como impotencias en la explotación de convertir las amenazas en un posible riesgo real que pueden causar daños graves a la empresa. Las vulnerabilidades son incertidumbres de ser causantes o no de algún daño más bien, se considera

como una condición a un conjunto de acondicionamientos que pueden causar afectaciones a los activos de la empresa. (Jaramillo Camacho, 2022)

Riesgo.

El peligro se refiere a la posibilidad de tener un impacto específico en la organización. El riesgo calculado es un indicador vinculado al par de valores calculados de vulnerabilidad e impacto, ambos vinculados a la relación entre el activo y la amenaza a la que se refiere el riesgo calculado. (Jaramillo Camacho, 2022)

Amenaza. Eventos que, aprovechando una vulnerabilidad, pueden desencadenar un incidente en la empresa, produciendo daños materiales o perdidas inmateriales en sus activos. Dentro de eventos se consideran tanto acciones, como interrupciones o falta de acción. (Allaico, 2021)

Confidencialidad. Busca prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización. (Farinango, 2023)

Integridad. Busca asegurar que no se realicen modificaciones por personas no autorizadas a los datos o procesos y que los datos sean consistentes tanto interna como externamente. La integridad de la información se refiere a que los datos conserven su originalidad, asegura que la información no ha sido modificada por personas o entidades no autorizadas, en otras palabas él envió de un mensaje no puede ser alterado mientras este se encuentre en proceso de llegar a su destino (Farinango, 2023)

Disponibilidad. Busca asegurar acceso confiable y oportuno a los datos o recursos para el personal apropiado. (Farinango, 2023)

Estrategias de continuidad.

Una estrategia de continuidad puede ser considerada como un método que posibilita la recuperación y continuidad de las tareas críticas de una organización ante un desastre o una interrupción mayor. Siendo estrategias, no solo los recursos y labores necesarios para evitar la interrupción del servicio, sino también los necesarios para minimizar la probabilidad de ocurrencia y el impacto en caso de suceder. (Jaramillo Camacho, 2022)

Continuidad del negocio: Capacidad de una organización para mantener sus operaciones críticas en funcionamiento durante y después de una interrupción o desastre. Es el objetivo principal del plan de continuidad, ya que garantiza que el municipio de Cañar pueda seguir

brindando sus servicios esenciales a la ciudadanía, incluso en situaciones adversas. (Farinango, 2023)

Gestión de riesgos: Proceso de identificar, analizar, evaluar y tratar los riesgos que pueden afectar a una organización. Es fundamental para el desarrollo de un plan de continuidad efectivo, ya que permite comprender los riesgos potenciales a los que está expuesto el departamento de TIC y tomar medidas para mitigarlos. (Jaramillo Camacho, 2022)

Gestión de la continuidad. Es un proceso integral que identifica los impactos potenciales que amenazan una organización y proporciona un marco para la construcción de la resiliencia y la capacidad para dar una respuesta eficaz que salvaguarde los intereses de sus principales partes interesadas, la reputación, la marca y el valor de la creación de actividades. (Hurtado & Paspuel, 2023)

Plan de recuperación de desastres: El plan de recuperación contempla medidas necesarias a tomar después que la amenaza se haya materializado y posteriormente controlada. Su objetivo principal es restaurar el estado de las cosas y personas, tal como se encontraban antes de la materialización de la amenaza. Dicho de otra manera, este plan es el encargado de asesorar los pasos a seguir después que un desastre haya ocurrido o de haber controlado una amenaza, en este plan se detalla la información necesaria para la restauración adecuada de los equipos y actividades a su estado normal (Farinango, 2023)

I. TRABAJOS RELACIONADOS

"Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011" Correa Salazar, Renzo Giancarlo. Universidad Peruana de Ciencias Aplicadas (UPC). Lima, Perú 2019.

El autor menciona que, mediante el plan de continuidad, se logró analizar el problema de la empresa en los servicios críticos de TI para mejorar los tiempos de recuperación y restauración, según los resultados obtenidos mediante el análisis, evaluación y tratamiento de riesgos, el análisis de vulnerabilidades y amenazas, que identificaron estrategias de continuidad adecuadas con alternativas de solución en la operación y administración de los servicios críticas de TI. (Salazar, 2019)

Este trabajo me ayuda a comprender la importancia de tener un plan de continuidad en el departamento de TIC de la institución

“Plan De Continuidad Del Negocio (BCP) Aplicado Al Departamento De Ti De La Empresa De Soluciones Tecnológicas TELECOMSEC”. Paola Alexandra Diaz Parco. Universidad técnica de Ambato. Ambato 2022.

Este proyecto se desarrolló para diseñar un BCP tomando como referencia la norma ISO 22301:2019, enfocado en proteger los principales activos de información y procesos críticos del área de TI de la empresa TELECOMSEC, mediante estrategias que permiten prevenir, contener y recuperarse ante la ocurrencia de eventos no deseados, sin comprometer la disponibilidad de sus servicios. (Díaz Parco, 2022)

“Desarrollo de un plan de contingencia de servicios TI para la Dirección de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, aplicando al marco de trabajo ITIL V3”. Farinango María Fernanda. Universidad Técnica del Norte. Ibarra 2023.

Este plan se fundamenta en ITIL, un marco de referencia que determina el manejo y las buenas prácticas para la gestión de servicios de Tecnologías de la Información (Procesos, Gente y Tecnología) Se desarrollará el mismo enfocado a la administración de procesos, para lo cual, se documentarán lineamientos importantes que permitan su desarrollo, fundamentándolo en BCP; el cual es un plan logístico práctico para que una organización recupere y restaure funciones críticas de forma parcial o total dentro de un tiempo predeterminado después de una interrupción no deseada. (Farinango, 2023)

Este trabajo me ayudara a conocer a profundidad el desarrollo del departamento de TIC dentro del municipio, ayudando establecer un plan de continuidad más eficiente.

J. METODOLOGÍA

Cuando se trata de un plan de continuidad del negocio, se enfoca en todos los procesos que deben ser ejecutadas para asegurar la continuidad de una empresa o institución en situaciones de interrupciones no deseadas y en el funcionamiento de la institución.

En el presente trabajo de investigación se empleará un enfoque mixto tanto cuantitativo como cualitativo, lo cual permitirá alcanzar los objetivos establecidos para asegurar la continuidad de los servicios en el municipio de Cañar.

La investigación será de carácter descriptivo por lo que se realizará un levantamiento de información del departamento de TIC, se realizará mediante entrevista a los encargados del departamento de TIC.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES			
		I	II	III	MEDIOS DE VERIFICACIÓN
1.	Fundamentar mediante un estudio teórico el plan de continuidad para el departamento de TIC.				
1.1.	Fundamentación teórica del plan de continuidad para el departamento de TIC.	X			Fundamentación teórica
2.	Analizar los riesgos, vulnerabilidades y amenazas para la determinación de estrategias de continuidad.				
2.1.	Realizar la recolección y análisis de datos para determinar el estado actual del departamento de TIC	X			Entrevistas con los responsables
2.2.	Analizar los riesgos, vulnerabilidades y amenazas para la determinación de estrategias de continuidad.		X		Matriz de riesgo
3.	Elaborar un plan de continuidad según los resultados del análisis de riesgos, vulnerabilidades y amenazas.				
3.1.	Elaboración del plan de continuidad según los resultados del análisis de riesgos, vulnerabilidades y amenazas.		X	X	Metodología
4.	Conclusiones y recomendaciones			X	Documentación

L. DECLARACIÓN FINAL

Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su funcionamiento, no causa perjuicio al ambiente es de nuestra autoría y no transgrede norma ética alguno.

M. PARTICIPANTES	
DIRECTOR:	Ing. José Antonio Carrillo Zenteno
ESTUDIANTE 1	Luis Francisco Guasco Loja

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	29-04-2024

Firmas:

Nombre: José Antonio Carrillo Zenteno CC: 0103304531 **Director del Proyecto**	Nombre: Luis Francisco Guasco Loja C.C.: 0302291703 **Estudiante / Egresado**

O. APROBACIÓN

Firmas:

_____	_____
Nombre:	**Nombre:**
CC:	**C.C:**
Primer Par revisor	**Segundo Par Revisor**

Bibliografía

Allaico, M. M. (2021). *Diseño de un plan de continuidad de negocio en la empresa Cañar net, Cañar-Ecuador.* Cañar, Ecuador: https://dspace.ucacue.edu.ec/handle/ucacue/12763.

Caizaguano, L. S. (2018). *DESARROLLO DE UNA GUÍA PARA PLANES DE CONTINUIDAD DE NEGOCIO DE TI ENFOCADO A LAS OPERADORAS MÓVILES DEL ECUADOR.*

Díaz Parco, P. (2022). *Plan de continuidad del negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC.* Ambato: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/36852.

Enríquez Bastidas, H. P. (2024). *Diseño del sistema de continuidad de negocio a través de la norma ISO 22301- 2019 para la empresa ModArte.* Ibarra.

Farinango, M. F. (2023). *Desarrollo de un plan de contingencia de servicios TI para la dirección de tecnologías de la información del Gobierno Autónomo Descentralizado Municipal de San Miguel de Ibarra, aplicando el marco de trabajo ITIL V3.* Ibarra, ecuador: https://repositorio.utn.edu.ec/handle/123456789/14762.

Gutiérrez Mendoza, A. J. (2022). *Diseño del plan de continuidad de negocio aplicado a seguridad de información en PYME Intervisión de Guayaquil*. Obtenido de dspace.ups.edu.ec: http://dspace.ups.edu.ec/handle/123456789/22136

Hurtado, J., & Paspuel, L. (2023). *Plan de continuidad del negocio de los activos tecnológicos Hardware y Software.* Tulcan: Universidad Politecnica Estatal del Carchi.

Jaramillo Camacho, J. A. (2022). *Diseño de un plan de continuidad de servicios del departamento de tecnologías de la información en casos excepcionales para la EP-EMAPA de la ciudad de Ambato.* Ambato, Ecuador: https://repositorio.puce.edu.ec/handle/123456789/9069.

Jaramillo, Á. G., & Díaz, P. A. (2022). *Plan de continuidad del negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC.* Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/36852

LOTAIP, G. M. (2021). *GAD Municipal de Cañar*. Obtenido de Cañar, Información de sitio oficial: https: www.canar.gob.eclotaip-año-2021

Mogrobejo, D. J. (2017). *DESARROLLO DE UN MODELO PARA LOS PROCESOS DEL ÁREA DE TENOLOGÍA DE INFORMACIÓN DE LA EMPRESA COMERCIALIZADORA DE COMBUSTIBLES "PETROLEOS Y SERVICIOS PYS C.A." UTILIZANDO COBIT 5.*

Montalban Ordoñez, W. E. (2022). *Diseño de un Plan de Continuidad Operativa de los servicios críticos del área de Sistemas y Tecnologías de la Información de la empresa Boticas y Salud, con base en la norma ISO/IEC 27031:2011.* Obtenido de http://creativecommons.org/licenses/by-nc-sa/4.0/

Quintanilla, M. A., & Crespo, G. G. (2017). *Fundamentos para Objetivos de Control en las TIC* (2 ed.). MQR.

Reyna Carrión, A. R. (2023). *ADMINISTRACIÓN Y DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.* Obtenido de ADMINISTRACIÓN Y DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN.

Salazar, C. (2019). *Diseño de un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011.* Lima: https://repositorioacademico.upc.edu.pe/handle/10757/625692.

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Luis Francisco Guasco Loja portador(a) de la cédula de ciudadanía Nº **0302291703** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Desarrollo de un Plan de Continuidad para el Departamento de TIC en el municipio de Cañar"** 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 este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, 28 de noviembre del 2024

F: .....

Luis Francisco Guasco Loja

C.I. 0302291703