UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DE NEGOCIO (BCP) PARA LOS SERVICIOS DIGITALES DEL GADIC DEL CANTÓN CAÑAR

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

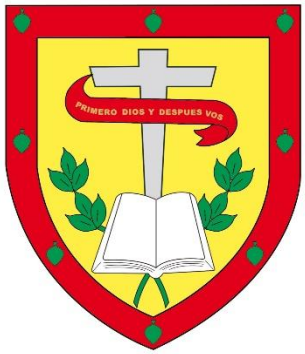
AUTORA: MIRELLA ESTEFANIA ALULEMA VALVERDE

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES

CAÑAR - ECUADOR

2025

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DE NEGOCIO (BCP) PARA LOS SERVICIOS DIGITALES DEL GADIC DEL CANTÓN CAÑAR

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

AUTORA: MIRELLA ESTEFANIA ALULEMA VALVERDE

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES

CAÑAR - ECUADOR

2025

PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUDITORÍA Y RESPONSABILIDAD

Mirella Estefania Alulema Valverde, portador(a) de la cedula de ciudadanía N°18 0302352281. Declaro ser el autor de la obra: "**Plan de continuidad de Negocio (BCP) para los servicios digitales del GADIC del cantón Cañar**" sobre la cual me hago responsable sobre sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 18 de noviembre de 2025

Mirella Estefania Alulema Valverde

C.I. 0302352281

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo denominado **"Plan de continuidad de Negocio (BCP) para los servicios digitales del GADIC del cantón Cañar "** realizado por **Mirella Estefania Alulema Valverde,** con documento de identidad No. 0302352281, previo a la obtención del título profesional de licenciada en Administración de Empresas, ha sido asesorado, supervisado y desarrollado bajo mi tutoría en todo su proceso, cumpliendo con la reglamentación pertinente que exige la Universidad Católica de Cuenca y los requisitos que determina la investigación científica.

Cañar, 18 noviembre de 2025

Ing. Cristhian Humberto Flores Urgiles

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

DEDICATORIA

Es un honor para mí dedicar y expresar mi más profundo agradecimiento a las que han sido parte fundamental en este viaje en mi vida académica.

Especialmente, a mis padres José Alulema y Alicia Valverde, a quienes les debo todo lo que soy. Mismos que con su amor incondicional, apoyó constante y sabias enseñanzas ha sido el pilar fundamental en mi vida. Gracias a su ejemplo de esfuerzo, perseverancia y dedicación he logrado alcanzar esta meta que representa no solo un logro personal, sino también el fruto de todo su sacrificio y su amor.

AGRADECIMIENTO

A mis padres, José Alulema y Alicia Valverde, Mi gratitud más profunda y sentida les pertenece a ustedes. Este logro es la prueba de su amor incondicional, la paciencia que tuvieron durante mis ausencias y el aliento constante que me ofrecieron en los momentos de mayor duda. Gracias por ser el refugio seguro donde siempre encontré la fuerza para seguir adelante. Esta tesis lleva impresa, en cada página, su fe en mí. Sin su apoyo moral y espiritual, simplemente no habría sido posible

RESUMEN

El Plan de Continuidad de Negocio (BCP) para los servicios digitales del GAD Intercultural del Cantón Cañar tiene como objetivo garantizar la disponibilidad continua de los servicios críticos, reduciendo el impacto de eventos disruptivos como fallos tecnológicos, ciberataques o desastres naturales. Este plan, basado en la norma ISO 22301, establece estrategias de recuperación que incluyen redundancia de servidores, respaldo de datos y protocolos de comunicación, además de incorporar la capacitación constante del personal y simulacros periódicos para asegurar la efectividad del plan. La implementación del BCP fortalece la resiliencia organizacional, mejora la respuesta ante incidentes y asegura la continuidad operativa de los servicios esenciales del GADIC. Asimismo, el plan se desarrolla bajo un enfoque metodológico mixto, integrando análisis documental, diagnóstico tecnológico y evaluación de riesgos basados en las normas ISO/IEC 27005, ISO 31000 y la metodología MAGERIT, permitiendo una gestión integral de la continuidad operativa y la recuperación de servicios digitales.

Palabras clave: Plan de Continuidad de Negocio (BCP)**,** disponibilidad continua**,** eventos disruptivos**,** norma ISO 22301**.**

ABSTRACT

The Business Continuity Plan (BCP) for the digital services of the Intercultural GAD of Cañar Canton aims to ensure the continuous availability of critical services, thereby reducing the impact of disruptive events such as technological failures, cyberattacks, or natural disasters. Based on the ISO 22301 standard, this plan establishes recovery strategies that include server redundancy, data backup, and communication protocols, as well as ongoing staff training and periodic drills to ensure its effectiveness. The implementation of the BCP strengthens organizational resilience, improves incident response, and ensures the operational continuity of the essential services provided by the GADIC. Furthermore, the plan is developed using a mixed methodological approach that integrates documentary analysis, technological diagnosis, and risk assessment based on ISO/IEC 27005, ISO 31000, and the MAGERIT methodology, enabling comprehensive management of operational continuity and the recovery of digital services.

Keywords: Business Continuity Plan (BCP), continuous availability, disruptive events, ISO 22301 standard.

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

INTRODUCCIÓN

Este estudio de investigación implica la construcción de un Plan de Continuidad del Negocio (BCP) para el GAD Intercultural del Cantón Cañar, específicamente en el ámbito de los servicios digitales. Esta investigación, en el ámbito de los servicios digitales, se centra en las obstrucciones y la preservación operativa de los servicios durante un evento disruptivo dentro del continuo. Los capítulos de este estudio, la situación, el marco teórico, la metodología y la implementación propuesta del BCP muestran claramente la culminación de los esfuerzos.

El capítulo 1 presenta el panorama que rodea al GAD Intercultural del Cantón Cañar, GADIC, donde no existe un BCP, por lo tanto, la provisión de servicios digitales a la población permanece amenazada en su continuidad. Se encuentra la situación de riesgo ante eventos como fallos técnicos, ataques informáticos, desastres naturales, los cuales afectan el funcionamiento y la confianza de la población. Los objetivos de la investigación y las preguntas que guiarán el plan en desarrollo también se enuncian en esta sección.

El Capítulo 2, Marco Teórico, ofrece el relato más completo de principio a fin en relación con los principios y marcos normativos que conciernen a la continuidad de negocios. Se analiza la relevancia de un Plan de Continuidad de Negocios en la administración pública, las normas internacionales más relevantes como ISO 22301, y se describen los elementos que se deben considerar para la elaboración de un plan de continuidad efectivo. Se aborda, además, la implementación de planes y las ventajas que se obtienen, tales como la resiliencia organizacional y la mejor utilización de los recursos tecnológicos.

El Capítulo 3, Metodología, expone el enfoque de investigación que se ha tomado para el desarrollo del plan de continuidad de negocios. El proceso metodológico se describe en las fases del diagnóstico de la infraestructura tecnológica, el análisis de impacto

empresarial, gestión de riesgos y el diseño de estrategias de continuidad. Se definen las herramientas y técnicas usadas, que incluyen ISO 22301 y la metodología MAGERIT para la estructuración y evaluación del plan.

Finalmente, el Capítulo 4: Propuesta, aborda el diseño particular del BCP para el GADIC. En este apartado se diseña el programa BCP, se identifican funciones y responsabilidades, se elabora las estrategias de recuperación y lo planes de comunicación

Se plantean las políticas que, de manera proactiva, se implementarán para el mantenimiento del BCP. Asimismo, las estrategias de capacitación, prueba y mantenimiento del plan que se continuarán de manera activa y permanente. La propuesta busca, dentro los enfoques y normativas planteados en el marco teórico, asegurar la continuidad operativa de los servicios digitales en un escenario adverso.

CAPÍTULO I

1.1. Planteamiento del problema

En un entorno de alta digitalización en el que una parte relevante de los procesos administrativos, operacionales y de atención al cliente se desarrollan a través de la tecnología, la falta de un BCP puede convertirse en una vulnerabilidad en el caso de que surjan contingencias, tales como fallos técnicos, ciberataques, desastres naturales y cortes de electricidad.

Esta falta de previsión en la planificación disminuye la posibilidad de que la institución pueda llevar a cabo una respuesta oportuna y efectiva a una eventualidad que, en caso de que se produzca, no sólo pondría en riesgo la disponibilidad de los servicios, sino que podría también afectar la confianza de los ciudadanos en la eficiencia de la gestión pública. Por todo lo antes expuesto, resulta fundamental el establecimiento de un BCP que permita la identificación y priorización de los servicios críticos, la definición de protocolos de recuperación y la reducción de los tiempos de inactividad.

1.1.1 Formulación del problema

A pesar de la creciente dependencia de los servicios digitales dentro de las instituciones públicas, muchas organizaciones aún no tienen planes o marcos comprensivos para garantizar la continuidad operativa del negocio frente a incidentes imprevistos, lo que deja al GAD Intercultural del Cantón Cañar (GADIC) sin un Plan de Continuidad del Negocio (BCP) como una debilidad operativa discernible que puede llevar a interrupciones en el servicio, afectando en última instancia la entrega de servicios, dañando la reputación de brindar servicios al público y erosionando la confianza institucional.

La falta de mecanismos tecnológicos, como servidores de respaldo disponibles y otros sistemas de alta disponibilidad, también reduce gravemente la capacidad organizativa para

soportar desastres naturales y ciberataques. Esto también impide que la organización realice una gestión proactiva de riesgos y que implemente rápidamente estrategias de mitigación de riesgos cuando los incidentes amenazan la estabilidad operativa de los servicios digitales.

En ese sentido, resulta relevante la elaboración de un BCP por el GADIC, dado que esto resaltará su resiliencia institucional, pero, también, la continuidad de la prestación de servicios digitales fundamentales de forma ininterrumpida. En este sentido, la pregunta principal de esta investigación se formula de la siguiente manera: ¿En qué se traduce la mejora de la capacidad del GAD Intercultural del Cantón Cañar, por medio de la implementación de un Plan de Continuidad de Negocio que considere la Norma ISO 22301, la prestación de servicios digitales fundamentales ante situaciones de interrupción?

1.2. Antecedentes de la Investigación

El trabajo de Sapper et al. (2023) titulado "Propuesta de un Plan de Continuidad del Negocio para el Registro del Dominio de Primer Nivel de Internet del Paraguay (NIC-PY)" elabora un modelo de BCP para una entidad pública respecto a la alineación de las referencias COBIT 2019 e ICANN. En este se incluyen prácticas básicas como el inventario de procesos críticos, servicios, amenazas, riesgos, personas responsables, así como la captura de RTO y RPO. También se describen procedimientos de evaluación, contención, recuperación, comunicación y seguimiento post-incidente. Para este proyecto, esta indagación ofrece un antecedente relevante en el sentido de que la BCP, al contexto institucional gobernanza de TI en el GADIC de Cañar, constituye una importante referencia a las buenas prácticas internacionales.

Durán (2022), en su obra titulada “Metodología para determinar los tiempos de recuperación objetivos de los activos de información críticos en una estrategia de continuidad del negocio en el sector servicios en Colombia” propone un enfoque metodológico para

establecer los tiempos de recuperación objetivos de los activos de información críticos ante la interrupción de servicios clave. En este documento se analiza el sector servicios, se caracteriza la criticidad de los activos de información y se estudian los marcos regulatorios de ISO 22301, ISO 27005, MAGERIT y NIST 800-30. También se desarrolla una herramienta web para automatizar el cálculo del RTO del servicio y proporcionar sugerencias para mejorar la disponibilidad del servicio. En cuanto al presente trabajo, esta investigación sirve como un referente metodológico clave, particularmente en las áreas de evaluación de activos críticos, evaluación y gestión de riesgos, y la formulación de enfoques pragmáticos para la continuidad operativa.

El trabajo de (Santos, 2024) en la Universidad Politécnica Salesiana que se centra en el título "Plan de Continuidad de Negocios [1] para la Carrera de Computación aplicando ISO 22301, COBIT e ITIL" propone un Plan de Continuidad de Negocios para el Centro de Datos de la Carrera de Computación aplicando los marcos ISO 22301, COBIT e ITIL. En el documento se contiene un análisis de impacto empresarial [2], identificación de activos críticos empresariales, cálculos de objetivos de tiempo de recuperación (RTO y RPO), evaluación de riesgos lógicos, físicos y humanos. Además, se implementaron FMEA, HAZOP y la matriz RACI para responsabilidades como herramientas de gestión de responsabilidades. Esto ha creado una importante base metodológica y técnica para diseñar la arquitectura del BCP, con un enfoque en la infraestructura digital orientada a servicios en entornos académicos.

El trabajo de Zuñiga (2021) "Plan de continuidad del negocio referente a la gestión de la seguridad de la información para el proceso de la Dirección de

[1] BCP
[2] BIA

Tecnologías e Información de la empresa CDA basado en el estándar 27031" proporciona un modelo de continuidad para una organización pública desde la perspectiva de la seguridad de la información, principalmente basado en las directrices del estándar 27031 así como del 27001 y MAGERIT. El autor identifica, categoriza y evalúa el activo crítico y estrategias complejas para la recuperación de incidentes para garantizar y mantener la continuidad y la resiliencia del servicio del sistema de TI. Este estudio es relevante para el trabajo presente porque proporciona una base establecida y clara sobre la tecnología de riesgos en instituciones públicas para ser persistente en la capacidad de respuesta ante interrupciones empresariales y para diseñar marcos de continuidad del negocio.

Para el trabajo de Díaz Parco (2022),, además del cumplimiento de la normativa ISO 22301:2019, se elaboró un Plan de Continuidad del Negocio para el departamento de Tecnologías de la Información de la empresa TELECOMSEC, utilizando la metodología MAGERIT en la gestión de riesgos.. El proyecto también contempla la realización de un análisis de impacto al negocio[3] para identificar los procesos críticos y desarrollar derivadas estrategias de prevención, contención y recuperación ante incidentes tecnológicos. Asimismo, se definen actividades de prueba, mantenimiento y concienciación del plan. Esta resulta un antecedente significativo para el presente proyecto en la medida que incorpora enfoques normativos similares y, aunque aborda la continuidad operativa en entornos tecnológicos, lo hace desde el ámbito privado.

Araujo (2019) desarrolló una propuesta de Plan de Continuidad del Negocio [4] para los sistemas informáticos del Servicio Nacional de Contratación Pública [5], utilizando como base las normas ISO 22301 e ISO 27005. La investigación incluyó un análisis del contexto

[3] BIA
[4] BCP

[5] SERCOP

institucional, identificación de procesos críticos, evaluación de amenazas y riesgos tecnológicos, así como el diseño de estrategias de recuperación. Este trabajo constituye un valioso antecedente para el presente estudio, por su aplicabilidad en el ámbito público ecuatoriano y por el enfoque integral en la protección de servicios tecnológicos críticos.

1.3. Justificación de la investigación

Actualmente no se cuenta con BCP que garantice la presentación ininterrumpida de los servicios digitales ante posibles contingencias como fallas tecnológicas, desastres naturales o ciberataques. Esta carencia representa un riesgo significativo, ya que una interrupción podría afectar la atención a la ciudadanía, los procesos administrativos y operativos de la institución.

Por esta razón, es fundamental desarrollar un BCP que permita fortalecer la capacidad de respuestas institucional, reducir el tiempo de inactividad y asegurar la continuidad de los servidores esenciales. Este estudio contribuirá a identificar debilidades, proponer soluciones concretas y establecer medidas que beneficien tanto al personal como a los usuarios de los servicios digitales

1.4. Objetivos

1.4.1 Objetivo General

Desarrollar un Plan de Continuidad de Negocio (BCP) para los servicios digitales GADIC Cañar.

1.4.2 Objetivos Específicos

Realizar un análisis documental de la parte del marco teórico; así como de la infraestructura tecnológica y de los procedimientos operativos vigentes en el GADIC del cantón Cañar

Evaluar la factibilidad y pertinencia de la implementación de servidores redundantes y otros mecanismos de alta disponibilidad.

Diseñar una propuesta para el desarrollo de un BCP para el GADIC del cantón Cañar.

1.5. Limitaciones

- El tiempo para terminar el proyecto es muy corto.
- Acceso restringido a la documentación o información confidencial.

1.6. Delimitaciones

- El estudio se enfoca únicamente en los servicios digitales gestionados por el GADIC del cantón Cañar.
- La metodología aplicada se basa en la norma ISO 22301 para continuidad del negocio y en MAGERIT para el análisis de riesgos.

2. CAPÍTULO II

MARCO TEÓRICO

2.1. Fundamentos del Plan de Continuidad de Negocio (BCP)

2.1.1 Concepto de Continuidad de Negocio

El Plan de Continuidad del Negocio (BCP) se refiere al “conjunto de procedimientos que permiten a una organización atender actividades que pueden afectar al personal, interrumpir sus procesos operativos o poner en riesgo la prestación de servicios digitales a la ciudadanía” (Sapper, Capli, & Legal, 2023)). La implementación de este plan asegura la

continuidad institucional y contribuye a reducir los impactos negativos frente a posibles contingencias.

2.1.2 Importancia del BCP en las organizaciones públicas

El Plan de Continuidad de Negocio[6], tiene un especial interés en el ámbito del sector público, ya que habilita la prestación continua y sin interrupciones de servicios esenciales durante la ocurrencia de eventos que interrumpen la actividad normal (disruptivos) (Campos, Esquivel, & Varela, 2021). Mientras en el sector privado se procura cuidar un activo financiero, en el caso de las instituciones públicas, estos deben salvar los derechos de los ciudadanos y la estabilidad operativa de la institución.

La falta de un BCP disminuye la capacidad de respuesta ante situaciones como fallas tecnológicas, desastres naturales o ciberataques, lo que impacta de forma negativa la gestión institucional (Chuqui, Monteros, & Durazno-Chumbay, 2024). Por esta razón, normativas como la ISO 22301 sugieren realizar la gestión de procesos críticos frontales mediante su identificación, establecimiento de tiempos de recuperación[7] y elaboración de planos de respuesta.

Sumado a esto, el BCP ayuda en la organización en el plano de la resiliencia, fortaleciendo la organización y fomentando la adopción de buenas prácticas. Según Sapper (2023) se puede citar que “el mantenimiento de la continuidad digital, disminución de tiempos de inactividad y el resguardo de la confianza pública” son algunos de los beneficios de la implementación del BCP.

2.1.3 Beneficios de implementar un BCP

[6] BCP
[7] RPO

La gestión de continuidad del negocio ofrece una serie de beneficios clave para las organizaciones, especialmente aquellas que dependen de servicios digitales críticos, como los municipios. En primer lugar, proporciona un marco estructurado que prepara a todos los miembros de la institución para responder adecuadamente ante incidentes, asegurando el cumplimiento de normas internas y regulaciones externas. (Hurtado Rodríguez & Paspuel Pusda , 2023)

En este sentido, entre sus beneficios estratégicos destacan la resiliencia organizacional, la mejora del desempeño institucional y la capacidad de garantizar la continuidad de operaciones críticas. Además, refuerza la confianza de las partes interesadas y de la ciudadanía al asegurar que los servicios no se verán interrumpidos inesperadamente. (Sangama Reyna, 2024)

La implementación del BCP favorece una planificación estratégica más eficiente, respalda la gestión de riesgos y facilita la comprensión profunda de las funciones esenciales de la organización, especialmente a través del análisis de impacto al negocio (BIA). Asimismo, garantiza la disponibilidad y protección de los activos tecnológicos, contribuye a reducir las pérdidas operativas y financieras, y fortalece la imagen institucional frente a situaciones adversa. (Villarreal Morales, Coro Villarreal, Fernández Sánchez, & Cueva Martinez, 2024)

2.1.4 Componentes clave de un BCP

Entre los principales componentes de un Plan de Continuidad del Negocio (BCP), es necesario destacar que este constituye un documento estructurado y dinámico que establece cómo una organización garantizará la disponibilidad de sus funciones y servicios críticos ante eventos disruptivos. Su eficacia depende de la integración de componentes clave e interdependientes que permiten prepararse, responder y recuperarse frente a interrupciones

imprevistas. Asimismo, estos elementos conforman una estrategia integral para fortalecer las operaciones organizacionales, la cual debe enmarcarse dentro de un ciclo de mejora continua que asegure su actualización y alineación con los cambios tecnológicos, operativos y normativos que enfrenta la entidad. (Castillo Cruz, 2024)

- **Evaluación de riesgos:** Consiste en identificar las amenazas potenciales que podrían afectar los procesos críticos y analizar la probabilidad e impacto de su ocurrencia. La gestión de riesgos permite establecer controles preventivos, defectivos y correctivos para mitigar posibles incidentes . (Campos, Esquivel, & Varela, 2021)

- **Estrategias de continuidad:** Se definen a partir de los resultados del BIA y el análisis de riesgos. Estas estrategias incluyen medidas como la replicación de servicios, respaldo de datos, redundancia de sistemas, alojamiento alternativo, acuerdos con proveedores y planes de operación manual temporal (Castillo Cruz, 2024)

- Plan de respuesta y recuperación: Incluye procedimientos específicos para actuar antes, durante y después de una interrupción. Establece roles, responsabilidades, rutas de comunicación, recursos de emergencia, y protocolos de activación del plan. (Araujo, 2019)

- **Pruebas, mantenimiento y mejora:** Un BCP no debe ser un documento estático. Requiere pruebas periódicas (simulacros, análisis de fallos, auditorías internas) para validar su eficacia, así como revisiones regulares que garanticen su pertinencia ante cambios tecnológicos, normativos o estructurales . (Díaz, 2022)

- **Concienciación y formación:** La efectividad del BCP depende de la preparación del personal. Es fundamental implementar programas de capacitación continua, asignar

responsables clave, y asegurar que todos los involucrados conozcan sus funciones en caso de una contingencia. (Álvarez Pincay , Bernal Álava, & Álvarez Villacreses, 2024)

2.2. Análisis de impacto en el negocio Business Impact Analisis (BIA)

El Análisis de Impacto en el Negocio (Business Impact Analysis – BIA) es un proceso fundamental dentro de la gestión de la continuidad operativa, ya que permite identificar las funciones críticas de una organización, evaluar las consecuencias de su interrupción y establecer prioridades para la recuperación. Su propósito es cuantificar el impacto que tendría una interrupción sobre los procesos esenciales y determinar los niveles mínimos aceptables de operación, así como los recursos requeridos para restablecerlos en un tiempo determinado. (Araujo, 2019)

El BIA permite establecer dos parámetros clave: el RTO (Recovery Time Objective), que define el tiempo máximo tolerable de interrupción de una actividad, y el RPO (Recovery Point Objective), que indica el punto en el tiempo al cual deben restaurarse los datos para asegurar la continuidad sin pérdidas significativas (Castillo Cruz, 2024). A partir del análisis se identifican los procesos de negocio, los recursos asociados (infraestructura tecnológica, personal, proveedores, información) y los impactos potenciales en áreas como el servicio al ciudadano, las obligaciones legales, las finanzas institucionales y la imagen pública. (Allauca Lidioma , 2023)

2.2.1 Objetivos de BIA

El Análisis de Impacto en el Negocio tiene como propósito principal identificar los procesos esenciales de una organización y comprender las consecuencias que generaría su interrupción, lo que permite priorizar su recuperación en función de la criticidad operativa. A través de este análisis se determinan parámetros como el tiempo máximo permitido para

restaurar actividades y la cantidad de información que puede perderse sin afectar gravemente la continuidad institucional. (Araujo, 2019)

2.2.2 Proceso de negocio clave

a) **Identificación de procesos críticos**

Se identifican las funciones esenciales para el cumplimiento de los objetivos institucionales, aquellas que, si se interrumpen, afectarían significativamente la operación del GAD y la prestación de servicios a la ciudadanía. (Santos, 2024)

b) **Evaluación de impactos operativos:**

Se analizan las consecuencias de la interrupción de cada proceso, considerando efectos en áreas como la atención ciudadana, cumplimiento legal, ingresos municipales, imagen institucional y continuidad administrativa. (Díaz, 2022)

c) **Determinación de los tiempos de recuperación:**

Se establecen los parámetros de recuperación:

- **RTO (Recovery Time Objective):** tiempo máximo tolerable para reanudar la actividad.
- **RPO (Recovery Point Objective):** punto máximo aceptable de pérdida de datos.

d) **Identificación de recursos y dependencias:**

Se reconocen los recursos necesarios para cada proceso crítico, incluyendo personal, infraestructura tecnológica, información, proveedores externos y sistemas asociados. (Zuñiga, 2021)

e) **Análisis y documentación de resultados:**

Se elabora un informe técnico que clasifica los procesos según su criticidad y recomienda prioridades de recuperación. Este informe es la base para definir estrategias en el Plan de Continuidad del Negocio. (Triana Botia & Castro, 2023)

f) **Actualización y revisión periódica:**

El BIA no es un proceso estático; requiere ajustes constantes ante cambios en la estructura organizacional, incorporación de nuevas tecnologías o modificación de servicios institucionales.

2.3 Gobierno digital y servidos públicos electrónicos

El gobierno digital indica que el Estado ha comenzado a usar e integrar tecnologías de la información a la hora de ofrecer servicios de una manera más eficaz, más específica a la demanda social en términos de accesibilidad, transparencia y eficiencia. En este orden de ideas, la evolución en la prestación de servicios públicos electrónicos otorga a los ciudadanos la oportunidad de finalizar trámites y acceder a información en línea, también disminuye los tiempos de respuesta, la geográficanización y mejora la respuesta participativa. Sin embargo, como en todo proceso, la evolución digital también expone a las instituciones a riesgos que, de no ser adecuadamente gestionados, pueden poner en riesgo la operación de procesos críticos y afectar la confianza del público. (Allauca Lidioma , 2023)

2.3.1 Digitalización de servicios públicos.

Las entidades del gobierno aumentan la eficiencia, accesibilidad y transparencia de sus servicios, sistematizando la digitalización. Pero el uso y la integración de la tecnología no son colectivamente suficientes, también es necesaria la reconfiguración de los recursos que se tiene en procesos internos para entregar un mejor servicio al ciudadano (Triana Botia

& Castro, 2023) Servicios digitales para pagos en línea, solicitud de permisos, atención al cliente, gestión del suelo y participación ciudadana. Este avance permite reducir costos operativos, eliminar tiempos innecesarios y fortalecer la gobernanza pública mediante la apertura de canales virtuales. No obstante, esta dependencia tecnológica implica nuevas responsabilidades en cuanto a la seguridad, disponibilidad y continuidad de los sistemas. (Allauca Lidioma , 2023)

2.3.2 Importancia de la disponibilidad de plataformas digitales en gobiernos locales

La disponibilidad continua de las plataformas digitales es un factor crítico para los gobiernos locales, ya que estas herramientas son esenciales para mantener el funcionamiento administrativo y la atención a la ciudadanía. En instituciones como el GADIC, que ofrecen servicios en línea para recaudar tributos, emitir documentos, brindar información o gestionar trámites, cualquier interrupción tecnológica puede generar retrasos, insatisfacción ciudadana y pérdida de confianza institucional.

Además, la disponibilidad está estrechamente relacionada con el derecho de acceso a servicios públicos, por lo que garantizar la operatividad de estas plataformas no solo responde a una necesidad técnica, sino también a una obligación social y legal. Ante este panorama, contar con un BCP que contemple escenarios de falla, estrategias de recuperación y asignación de recursos es indispensable para sostener la calidad de los servicios digitales ofrecidos. (Álvarez Pincay , Bernal Álava, & Álvarez Villacreses, 2024)

2.3.3 Vulnerabilidades en sistemas de atención ciudadana

A pesar de los beneficios que ofrece la digitalización, los sistemas de atención ciudadana también presentan vulnerabilidades que pueden poner en riesgo la continuidad de

los servicios y la integridad de la información gestionada. Entre las principales amenazas se encuentran (Camacho Piña & Gutierrez Alvarado , 2021)

2.4 Gestión de riesgos tecnológicos

La gestión de riesgos tecnológicos es un componente clave en los planes de continuidad operativa, sobre todo en instituciones públicas que dependen de plataformas digitales para ofrecer servicios esenciales. Este proceso busca anticiparse a las amenazas derivadas del uso de tecnologías, evaluando su impacto sobre los activos y procesos institucionales, con el fin de reducir posibles consecuencias negativas. (Álvarez Pincay , Bernal Álava, & Álvarez Villacreses, 2024) Entre los riesgos más comunes se encuentran los ataques cibernéticos, fallos en la infraestructura tecnológica, desastres naturales y errores humanos. Para abordarlos de manera estructurada, se aplican marcos internacionales como la norma ISO 31000 y la ISO/IEC 27005, que ofrecen metodologías para identificar, analizar y controlar estas amenazas de forma sistemática y alineada con los objetivos de continuidad y seguridad institucional. (Iza, 2021)

2.4.1 Principales amenazas tecnológicas al sector publico

- **Ransomware:** Es uno de los ciberataques más peligrosos y comunes que enfrentan las entidades públicas hoy en día. Este tipo de software malicioso accede a los sistemas de una organización y luego los encripta, bloqueando a los usuarios y bloqueando el acceso a sus archivos, bases de datos y plataformas operativas, posteriormente los atacantes exigen un pago o rescate económico —generalmente en criptomonedas— a cambio de proporcionar la clave de descifrado. (Garzon Quito, 2021)

- **Phishing**: El phishing es una técnica de ciberdelito que consiste en engañar a los usuarios a través de correos electrónicos o enlaces falsos que pretenden ser legítimos,

para obtener información sensible como contraseñas, información personal o credenciales institucionales. Este tipo de amenaza es muy común en el sector público y los ciberdelincuentes explotan la ignorancia o negligencia del personal para comprometer los sistemas, permitiendo el acceso no autorizado o la instalación de software malicioso. La protección contra este riesgo requiere capacitación continua, la implementación de autenticación multifactor y la instalación de filtros de seguridad diseñados para detectar y eliminar intentos de suplantación. (Garzon Quito, 2021)

- **Malware:** El malware consiste en software malicioso diseñado para violar la seguridad de un sistema informático, sin el conocimiento del usuario, para infligir daño, interrumpir procesos, espiar al usuario o robar información sensible. En el sector público, el malware puede comprometer los datos institucionales, interrumpir los servicios digitales del sector público y permitir que se ejecuten otros ataques cibernéticos complejos. (Chuqui, Monteros, & Durazno-Chumbay, 2024)

  El malware puede distribuirse a través de archivos adjuntos de correos electrónicos, descargas no verificadas o debilidades del sistema que no han sido parcheadas, por eso tener software antivirus actualizado, prohibiciones de ejecución, segmentación de red y políticas de uso seguro reducirá en gran medida el riesgo. . (Garzon Quito, 2021)

- **Ataques DDoS** (denegación de servicio) Los ataques de denegación de servicio distribuido (DDoS) consisten en saturar deliberadamente los servidores o redes de la institución mediante un alto volumen de solicitudes simultáneas que provocan la interrupción de los servicios digitales, temporal o totalmente . (Camacho Piña & Gutierrez Alvarado , 2021) En el sector público, estos ataques pueden provocar que plataformas críticas como softwares de portal, sistemas de atención a ciudadanos o

incluso servicios financieros queden inoperativos. Su impacto va más allá de la continuidad operativa; erosiona la confianza de los usuarios. Las medidas de defensa activa consisten en la implementación de herramientas de vigilancia, infraestructura redundante, filtros de tráfico y planes de respuesta a incidentes coordinados. (Zuñiga, 2021)

- **Fallas en la infraestructura tecnológica:** Las deficiencias en la infraestructura tecnológica incluyen interrupciones eléctricas y fallas en servidores, enrutadores y redes que afectan directamente la continuidad de los procesos institucionales. Tales incidentes pueden paralizar servicios esenciales, interrumpir el acceso a plataformas digitales o resultar en una pérdida de información. En entidades del sector público, donde muchos procesos dependen de la conectividad y el flujo operativo de los sistemas, estos eventos representan un riesgo considerable. (Campos, Esquivel, & Varela, 2021).

- **Errores humanos:** Estos continúan invocando un riesgo de seguridad tecnológica para una institución porque las amenazas potenciales pueden ser involuntarias, como configuraciones incorrectas, eliminación de datos o contraseñas débiles. En el sector de servicios públicos, estos problemas provienen de la falta de capacitación, ignorancia de los protocolos o exceso de confianza. (Camacho Piña & Gutierrez Alvarado , 2021)

- **Falta de copias de seguridad o sistemas de recuperación:** La falta de copias de seguridad de recuperación adecuadas o eficientes es una debilidad crítica de gobernanza dentro de los sistemas automatizados del sector público. Sin la capacidad de recuperar datos y restaurar servicios, incluso durante fallas técnicas, ciberataques a sistemas automatizados o errores humanos, una organización corre el riesgo de

tiempos de inactividad disruptivos prolongados y la pérdida de información invaluable. Las copias de seguridad no confiables ponen en peligro la continuidad operativa y socavan la confianza pública. Para mitigar el riesgo de interrupción del servicio, las instituciones públicas deben implementar políticas operativas para respaldar información a intervalos regulares, almacenamiento seguro fuera del sitio y pruebas de restauración para garantizar una recuperación oportuna. (Zuñiga, 2021)

2.4.2 Herramientas para la gestión de riesgos Tecnológicos

La gestión de los riesgos tecnológicos en las instituciones públicas consiste en la adopción de medidas y la utilización de metodologías en la identificación, evaluación, tratamiento y seguimiento de amenazas que ponen en riesgo la continuidad operacional. Esto permite enfrentar los riesgos tanto internos como externos de forma ordenada, a los tomadores de decisión y, de forma clara y eficiente, la asignación de recursos (Garzón Quito, 2021). En este marco, entre las principales herramientas y metodologías utilizadas para la gestión de riesgos tecnológicos se destacan las siguientes. (Garzon Quito, 2021)

- **MAGERIT:** La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT, del Ministerio de Administración Pública de España, se ocupa de la identificación y valoración de los riesgos que impactan los activos de información de una organización. MAGERIT es una valiosa herramienta en el sector público, y en las instituciones en general, ya que permite construir un análisis más técnico y ordenado a partir de un catálogo más detallado sobre activos, amenazas y salvaguardas. El informe del CCN (2020) establece que MAGERIT tiene en cuenta la evaluación y el impacto de las contramedidas de riesgo que permiten la continuidad de los servicios digitales y su adaptación flexible a la organización, independientemente de su tamaño y complejidad. (Cubillos Mora, 2023)

- **ISO27005:** La norma ISO/IEC 27005 ofrece directrices para la gestión del riesgo de seguridad de la información dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001. Al abordar de forma sistemática la identificación, análisis y tratamiento, descubre y puede manejar de forma efectiva todo riesgo que afecte la confidencialidad, integridad y disponibilidad de la información. Tiene gran importancia para la administración de información sensible y se basa en sistemas digitales, constituyendo un gran valor en la protección de información contra ataques cibernéticos, errores de operación y fallas técnicas en la administración de sistemas, sobre todo para los gobiernos locales. Esta norma permite la alineación de la gestión del riesgo en los objetivos de seguridad y continuidad de la operación del negocio. (Villarreal Morales, Coro Villarreal, Fernández Sánchez, & Cueva Martinez, 2024)

- **ISO31000:** establece un marco general para la gestión del riesgo en cualquier tipo de organización, sin considerar su tamaño, sector, o ubicación geográfica. Enfoque en la integración del proceso de gestión del riesgo en las decisiones de estrategia, operación, y cumplimiento en todas las dimensiones. ISO 31000 establece y permite a las administraciones públicas evaluar su riesgo y ordenadamente priorizar las acciones de riesgo. Principios como el enfoque, la mejora continua, la gestión, el riesgo, la transparencia, la evidencia y la exposición al riesgo, entre otros. Si bien no está dirigida exclusivamente a riesgos tecnológicos, su aplicación es fundamental para establecer una cultura de prevención que sustente la implementación de normas más específicas como la ISO/IEC 27005. (Ortiz Alulema, 2020)

2.4.2.1 Tabla comparativa de Magerit, ISO27005 y ISO3100

Para realizar el análisis comparativo entre las metodologías y normas de gestión de riesgos, se definieron cinco criterios de análisis: enfoque principal, fases, ámbito de aplicación, fortalezas y limitaciones. La elección de estos criterios responde a la necesidad de valorar de manera integral cómo cada norma aborda el ciclo de gestión de riesgos. El enfoque principal permite identificar la orientación conceptual de la norma; las fases describen las etapas metodológicas a seguir; el ámbito de aplicación evidencia el contexto y alcance en que puede implementarse; las fortalezas destacan los aspectos diferenciadores y ventajas; mientras que las limitaciones permiten reconocer los retos y restricciones de su implementación. Estos criterios se fundamentan en lineamientos internacionales sobre gestión de riesgos, como la norma ISO 31000 (2018), la ISO/IEC 27005 (2022) y las recomendaciones del CCN-STIC 830 (2020), los cuales enfatizan la necesidad de un enfoque sistemático, aplicable y crítico en la evaluación de riesgos.

Norma	Enfoque Principal	fases	Ámbito de Aplicación	Fortalezas	Limitaciones
MAGERIT	Análisis y gestión de riesgos en sistemas de información	-Identificación de activos - Valoración de activos - Análisis de amenazas - Evaluación de impacto - Análisis de salvaguardas - Estimación de riesgos	Entidades públicas y privadas (especialmente del entorno hispano)	- Metodología estructurada y detallada	MAGERIT
ISO 31000	Gestión integral de riesgos	¡Establecimiento del contexto - Identificación de riesgos - Análisis y evaluación	Todo tipo de organizaciones y sectores	- Enfoque genérico y adaptable	ISO 31000

		- Tratamiento del riesgo - Seguimiento y revisión -Comunicación			
ISO/IEC 27005	Gestión de riesgos en seguridad de la información	-Contexto organizacional - Identificación de riesgos -Análisis y evaluación -Tratamiento del riesgo - Aceptación y comunicación - Monitoreo y revisión	Organizaciones que implementan ISO/IEC 27001	- Específica para TI y seguridad de la información	ISO/IEC 27005

Tabla 1 Tabla comparativa de Margerit, ISO27005 y ISO3100 Fuente: Autor Propio

La elección de la ISO/IEC 27005 se fundamenta en los criterios previamente establecidos. En primer lugar, por su enfoque metodológico, ya que está específicamente orientada a la gestión de riesgos en seguridad de la información, lo que la convierte en un referente directo para este estudio. En segundo lugar, en cuanto a su alcance y aplicabilidad, se integra de manera coherente con las demás normas del sistema de gestión, especialmente con la ISO/IEC 27001, lo que garantiza una implementación armónica y consistente. Finalmente, su reconocimiento internacional la posiciona como un estándar ampliamente aceptado, lo que refuerza la validez de su selección dentro del análisis comparativo.

2.5 Metodologías para la Gestión de la Continuidad del Negocio

La gestión de la continuidad del negocio requiere la aplicación de normas y metodologías reconocidas internacionalmente, las cuales proporcionan lineamientos claros para el diseño, implementación y mantenimiento de planes efectivos de continuidad. Estas metodologías permiten a las organizaciones anticiparse a interrupciones, minimizar sus impactos y asegurar la prestación de servicios críticos en todo momento.

Entre las principales normas y estándares aplicables se encuentran:

2.5.1 ISO 22301

Botia y Castro (2023) mencionan que la norma ISO 22301 es la norma internacional que otorga los requisitos para la implementación de un Sistema de Gestión de Continuidad del Negocio (SGCN) y que su propósito principal es dotar a las organizaciones de las herramientas necesarias para que puedan gestionar, de la mejor manera posible, las interrupciones críticas de sus operaciones y así minimizar los impactos prolongados, permitiendo que la recuperación se realice dentro de un tiempo razonable.

2.5.2 Objetivos de la norma ISO 22301

Tiene como principal objetivo la creación de un marco sólido que facilite la implementación de un Sistema de Gestión de la Continuidad del Negocio (SGCN) permitiendo así a una organización el gestionar, responder y recuperarse de un evento que les sea disruptivo. En el caso de las organizaciones del sector público (por ejemplo, gobiernos locales), se busca la garantía de que los servicios digitales esenciales permanezcan en funcionamiento o que sea posible la recuperación dentro de un tiempo aceptable. (Cordova Montesdeoca & Solano Cobos, 2021)

2.5.3 Requisitos clave de la norma ISO 22301

ISO 22301 gira en torno a los requisitos que las organizaciones deben abordar para desarrollar e implementar un sistema de gestión para la continuidad. Estos abarcan desde la comprensión del contexto dentro de la organización, sus partes interesadas y sus expectativas, hasta las políticas, roles, responsabilidades y los recursos necesarios. (Triana Botia & Castro, 2023)

2.5.4 Implementación de estrategias de continuidad

En el contexto de ISO 22301, la definición y despliegue de acciones necesarias para asegurar que los procesos centrales de la organización continúen operando durante una

interrupción severa describe la implementación de estrategias de continuidad. (Santos, 2024) Estas estrategias deben basarse en los resultados del BIA y de la evaluación de riesgos, permitiendo así establecer mecanismos proporcionales al nivel de criticidad y vulnerabilidad de cada servicio.

Entre las estrategias más comunes se encuentran:

- Redundancia tecnológica y respaldo de datos
- Ubicaciones alternativas de operación
- Planes de comunicación con actores internos y externos
- Recuperación ante desastres (Disaster Recovery)
- Capacitación del personal y roles definidos ante incidentes. (Durán, 2022)

3. CAPITULO III

MARCO METODOLOGICO

3.1 Enfoque de la Investigación

La investigación adopta un enfoque mixto, permitiendo analizar la situación actual del GADIC del cantón Cañar respecto a sus servicios digitales y proponer un Plan de Continuidad de Negocio. Se estudian aspectos documentales, tecnológicos y operativos desde una perspectiva técnica, complementados con herramientas cuantitativas como análisis de riesgos y evaluaciones de impacto, con el fin de garantizar la continuidad operativa ante eventos disruptivos.

3.2 Nivel de la Investigación

La investigación se desarrolla en un nivel descriptivo, la cual se caracteriza técnicamente el estado actual de los servicios digitales, infraestructura y procesos críticos del GADIC. En la fase propositiva, se diseña un Plan de Continuidad de Negocio (BCP) basado en estándares como la ISO 22301, orientado a garantizar la continuidad operativa y la disponibilidad sostenida de los servicios ante eventos disruptivos.

3.3 Población y Muestra

En el presente estudio, la población no está constituida por el personal técnico o administrativo, sino por los activos de información del Departamento de TIC del GADIC del Cantón Cañar, los cuales representan los elementos sujetos a análisis dentro del proceso investigativo.

Para la recolección de información se emplea un muestreo no probabilístico por criterio, apoyado en informantes clave como el jefe de TIC y analistas de sistemas, quienes aportan con conocimientos técnicos relevantes sobre los servicios digitales críticos. En este sentido, la muestra se delimita a los activos de información seleccionados para ser evaluados,

considerando su importancia dentro de la continuidad operativa y la gestión de riesgos tecnológicos.

3.4. Herramientas e instrumentos de recolección

Para la recolección de información se emplearon técnicas documentales y de observación directa, que permitieron analizar el entorno tecnológico de la institución y los recursos disponibles para la gestión de continuidad operativa.

Se aplicó la observación técnica en los entornos de red, servidores, centros de datos y estaciones de trabajo, con el fin de identificar las condiciones actuales de operación, disponibilidad energética y medidas de seguridad implementadas.

Además, se recurrió a la revisión documental, examinando registros internos, políticas institucionales, inventarios de activos tecnológicos y manuales operativos. Esta revisión permitió determinar la existencia de protocolos relacionados con la gestión de riesgos, respaldos de información y políticas de recuperación ante fallos.

3.5. Tratamiento de la Información

Se emplearon técnicas como la entrevista semiestructurada al Jefe de TIC, la revisión documental de normativa y procedimientos, y la observación directa de la infraestructura tecnológica. También se aplica una matriz de análisis de riesgos bajo criterios de confidencialidad, integridad y disponibilidad

3.6. Entrevista

Se emplearon técnicas como la entrevista semiestructurada al Jefe de TIC, la revisión documental de normativa y procedimientos, y la observación directa de la infraestructura tecnológica. También se aplica una matriz de análisis de riesgos bajo criterios de confidencialidad.

1. ¿Cuáles son los principales sistemas o servicios digitales de los que depende actualmente la gestión operativa del GAD Intercultural del Cantón Cañar?

Los principales sistemas son el Sistema Integrado Municipal (SIM), el sistema de recaudación tributaria, el sistema catastral, el portal web institucional y los servicios de correo electrónico corporativo. Estos sistemas son fundamentales para la atención ciudadana, la gestión administrativa y la recaudación municipal. Además, se cuenta con la infraestructura de servidores físicos y virtuales, así como con los servicios de conectividad y red que soportan todas las operaciones internas.

2. ¿Qué procedimientos o mecanismos se aplican para realizar copias de seguridad de la información institucional?

Actualmente se realizan copias de seguridad diarias de las bases de datos principales en servidores locales, complementadas con respaldo semanal en discos externos. Algunos sistemas, como el de recaudación y catastro, cuentan con copias automáticas parciales. Sin embargo, se requiere fortalecer la automatización y almacenamiento en la nube para garantizar una mayor seguridad y disponibilidad de los respaldos.

3. En caso de una falla del sistema o pérdida de datos, ¿cuánto tiempo estiman que tomaría restablecer los servicios digitales más importantes?

El tiempo estimado de recuperación varía según el sistema afectado. En el caso del sistema de recaudación tributaria y el SIM, el restablecimiento podría tardar entre dos y cuatro horas, dependiendo del tipo de falla. En servicios secundarios, como el portal web institucional, el tiempo podría extenderse hasta seis horas. No obstante, es necesario implementar un plan de recuperación formal que reduzca los tiempos de inactividad.

4. ¿Qué medidas de seguridad existen para prevenir accesos no autorizados o ataques informáticos a los sistemas institucionales?

Se cuenta con firewalls perimetrales, antivirus corporativo y perfiles de usuario con contraseñas personalizadas. Asimismo, se controlan los accesos mediante roles administrativos diferenciados en los sistemas internos. No obstante, aún se requiere incorporar medidas más avanzadas, como la autenticación multifactor, la segmentación de red y políticas más estrictas de actualización y parches de seguridad.

5. ¿Se cuenta con alguna metodología o procedimiento formal para identificar y evaluar los riesgos tecnológicos dentro del GADICC?

Actualmente no existe un procedimiento formal documentado. Sin embargo, el área TIC realiza revisiones periódicas de vulnerabilidades y registra los principales incidentes. Con el desarrollo del Plan de Continuidad de Negocio (BCP) se busca formalizar la evaluación de riesgos tecnológicos aplicando metodologías como MAGERIT e integrándolas a las políticas institucionales de seguridad de la información.

6. ¿Qué tipo de infraestructura eléctrica o sistemas de respaldo se utilizan para asegurar la continuidad de los servicios ante cortes de energía?

El centro de datos principal cuenta con sistemas UPS que permiten mantener la operatividad durante cortes breves de energía. En casos de interrupciones prolongadas, se dispone de una planta eléctrica institucional que puede sostener los servicios básicos. Sin embargo, se requiere mejorar el monitoreo remoto de energía y asegurar que todos los equipos críticos estén conectados a fuentes de respaldo adecuadas.

7. ¿Cómo se coordinan las acciones del área TIC con las demás direcciones del GADICC cuando ocurre una interrupción o falla tecnológica?

Cuando ocurre un incidente, el área TIC comunica de inmediato la situación a las direcciones afectadas y coordina la priorización de los servicios a restablecer. Generalmente, se da prioridad a los sistemas de recaudación, catastro y atención ciudadana. Las decisiones se toman en conjunto con la Dirección Administrativa y la Dirección Financiera, aunque es necesario establecer un protocolo formal de comunicación y respuesta.

8. Desde su experiencia, ¿qué aspectos considera prioritarios para mejorar la disponibilidad, seguridad y recuperación de los servicios digitales institucionales?

Es prioritario implementar un sistema integral de respaldo automatizado, fortalecer las políticas de ciberseguridad, establecer un servidor espejo para los sistemas críticos y crear un centro alterno de contingencia. Además, es fundamental capacitar al personal técnico y administrativo en el manejo de incidentes tecnológicos y mantener actualizado el Plan de Continuidad de Negocio para responder con rapidez ante emergencias.

3.6 Análisis e Interpretación de Resultados

La siguiente tabla presenta el análisis e interpretación de las respuestas obtenidas en la entrevista realizada al Jefe de Tecnologías de la Información (TIC) del GAD Intercultural del Cantón Cañar.

Este análisis permite comprender la situación actual de la infraestructura tecnológica, las medidas de seguridad, los procedimientos de respaldo y las acciones institucionales relacionadas con la continuidad operativa.

Los resultados contribuyen directamente a la formulación del Plan de Continuidad de Negocio (BCP), ya que permiten identificar los activos más vulnerables y las necesidades prioritarias de mejora tecnológica.

Pregunta	Análisis
¿Cuáles son los principales sistemas o servicios digitales de los que depende actualmente la gestión operativa del GAD Intercultural del Cantón Cañar?	Se evidencia una fuerte dependencia de sistemas institucionales como el SIM, el sistema catastral, el de recaudación tributaria y el portal web. Esto confirma la necesidad de establecer estrategias de respaldo y recuperación que garanticen la continuidad de los servicios municipales
¿Qué procedimientos o mecanismos se aplican para realizar copias de seguridad de la información institucional?	Existen prácticas básicas de respaldo local, aunque de manera parcial. Se requiere una mejora en la automatización de copias de seguridad y el uso de almacenamiento en la nube para reducir el riesgo de pérdida de datos.
¿En caso de una falla del sistema o pérdida de datos, ¿cuánto tiempo estiman que tomaría restablecer los servicios digitales más importantes?	Los tiempos de recuperación son moderados, de dos a seis horas, dependiendo del sistema. Esto indica que aún no existe una estrategia formal de recuperación (RTO y RPO) documentada y que el BCP será clave para optimizar estos tiempos.
¿ Qué medidas de seguridad existen para prevenir accesos no autorizados o ataques informáticos a los sistemas institucionales?	Las medidas actuales son básicas (firewall y antivirus). Es necesario fortalecer la seguridad con mecanismos de autenticación multifactor, segmentación de red y actualización continua de software.
¿ Se cuenta con alguna metodología o procedimiento formal para identificar y evaluar los riesgos tecnológicos dentro del GADIC?	No existe una metodología formal implementada, aunque el área TIC realiza controles internos. Este hallazgo justifica la aplicación del método MAGERIT dentro del BCP para establecer una gestión de riesgos estructurada.
¿Qué tipo de infraestructura eléctrica o sistemas de respaldo se utilizan para asegurar la continuidad de los servicios ante cortes de energía?	La institución dispone de UPS y planta eléctrica, pero no todos los equipos críticos están integrados a estos sistemas. Se recomienda implementar monitoreo energético y ampliar la cobertura de respaldo.
¿Cómo se coordinan las acciones del área TIC con las demás direcciones del GADICC cuando ocurre una interrupción o falla tecnológica?	La coordinación actual es reactiva y depende de la comunicación directa con las áreas afectadas. El BCP permitirá definir protocolos formales de respuesta y comunicación interdepartamental.
¿Desde su experiencia, ¿qué aspectos considera prioritarios para mejorar la disponibilidad, seguridad y recuperación de los servicios digitales institucionales?	El jefe de TIC prioriza la automatización de respaldos, la actualización de equipos, la capacitación del personal y la creación de un centro alterno de contingencia. Estas acciones se alinean con las estrategias propuestas en el Plan de Continuidad de Negocio.

Tabla 2 Análisis e Interpretación de Resultados Fuente: Autor Propio

3.7 Fases de la metodología

1. Fase de planificación: definición de objetivos, delimitación de la población y muestra, y selección de técnicas e instrumentos de recolección de información.
2. Fase de recolección de datos: levantamiento de información a través de entrevistas, cuestionarios, análisis documental y revisión de normativa.
3. Fase de procesamiento y análisis: clasificación, depuración y sistematización de la información recopilada, aplicando criterios de análisis comparativo y categorización temática.
4. Fase de validación: contraste de los hallazgos con expertos en el área de TIC y continuidad del negocio, asegurando la fiabilidad de los resultados.
5. Fase de interpretación y conclusiones: integración de los resultados obtenidos con el marco teórico y normativo, extrayendo conclusiones y recomendaciones aplicables al contexto de estudio.

CAPÍTULO IV

4. PROPUESTA

4.1 Introducción

La presente propuesta se fundamenta en la norma ISO 22301 y consiste en el diseño de un Plan de Continuidad de Negocio (BCP) para el GAD Intercultural del Cantón Cañar, orientado a garantizar la prestación ininterrumpida de sus servicios digitales. El objetivo principal es proteger la continuidad de los procesos críticos, reducir los tiempos de inactividad y fortalecer la resiliencia institucional frente a fallas técnicas, ciberataques y desastres naturales.

En este contexto, se plantea un texto orientado tanto al presente como al futuro, en el cual se establece el marco del diseño del Plan de Continuidad de Negocio. En dicho proceso, se incluye el análisis de impacto en el negocio (BIA), la planificación de la continuidad operativa y la evaluación de escenarios críticos en el tiempo. De esta manera, se pretende dotar al GAD Intercultural del Cantón Cañar de una herramienta práctica que le permita garantizar la operatividad de los servicios digitales y, en consecuencia, fortalecer la confianza de la ciudadanía y la eficiencia administrativa frente a posibles contingencias.

4.1.2 Objetivo de la propuesta

El objetivo principal es que el GAD Intercultural del Cantón Cañar cuente con un Plan de Continuidad de Negocios (BCP) que garantice la disponibilidad y recuperación de sus servicios digitales críticos (qué). Dicho plan se elaborará conforme a la norma ISO 22301, considerando la gestión de riesgos y el análisis de impacto al negocio (cómo). De esta manera, se pretende reducir la vulnerabilidad institucional, fortalecer la capacidad de

respuesta ante incidentes y asegurar la continuidad en la prestación de servicios a la ciudadanía.

4.1.3 Alcance del BCP

El Plan de Continuidad de Negocios (BCP) de la Dirección Intercultural del GAD del Cantón Cañar abarca todas las funciones orientadas a la atención ciudadana, tanto en el ámbito digital como en los procesos administrativos y de servicio. Su alcance incluye el aseguramiento de la disponibilidad de las plataformas críticas, los sistemas de información, la infraestructura tecnológica en los servidores y las copias de respaldo de los datos institucionales. Asimismo, el BCP contempla a los grupos de interés que intervienen en la gestión de riesgos y establece las directrices necesarias para la prevención, respuesta y recuperación ante incidentes que puedan afectar la continuidad operativa de la entidad.

4.1.4 Metodología aplicada para la propuesta

La metodología aplicada en la presente propuesta se fundamenta en el uso de documentos y estándares institucionales de orden internacional, los cuales garantizan la continuidad de las funciones organizacionales y la adecuada gestión de riesgos y tecnologías. En este contexto, se considera de especial relevancia la norma ISO 22301, que proporciona el marco para el diseño e implementación de un sistema de gestión de continuidad de negocio, definiendo los requisitos necesarios para su correcta aplicación. Complementariamente, se integra el modelo MAGERIT, que aporta un enfoque estructurado para el análisis y la gestión de riesgos en los sistemas de información, fortaleciendo así la resiliencia institucional frente a posibles contingencias.

En la Tabla 3 se presentan las fases metodológicas consideradas para el diseño del Plan de Continuidad de Negocios, las cuales se fundamentan en los lineamientos de la norma ISO

22301. Dichas fases permiten estructurar de manera ordenada el proceso de diagnóstico, planificación y ejecución de acciones orientadas a garantizar la continuidad de los servicios críticos del GAD Intercultural del Cantón Cañar.

Tabla 3. Metodología para la propuesta. Fuente: Autoría Propia.

Etapa	**Descripción**
Diagnóstico inicial	Recolección de información sobre la infraestructura tecnológica, los servicios digitales y los procesos críticos del GADIC mediante entrevistas, observación y revisión documental.
Análisis de Impacto al Negocio (BIA)	Identificación de funciones esenciales, determinación de parámetros de recuperación (RTO y RPO) y priorización de procesos según su criticidad.
Gestión de riesgos	Evaluación de amenazas y vulnerabilidades tecnológicas mediante MAGERIT, ISO 27005 e ISO 31000, estableciendo el nivel de riesgo y controles necesarios.
Estrategias de continuidad	Definiendo medidas como servidores redundantes, respaldos de datos, sitios alternativos y protocolos de comunicación para asegurar la continuidad del servicio.
Plan de respuesta y recuperación	Estableciendo procedimientos ordenados y oportunos, roles y responsabilidades para responder a contingencias
Pruebas, mantenimiento y mejora continua	Ejecución periódica de simulacros, auditorías y actualizaciones del plan para asegurar eficacia y adaptación a nuevas tecnologías y cambios organizacionales.

4.2 Fases de la propuesta

Fase 1. Análisis y diagnóstico

La fase de análisis y diagnóstico se centra en identificar los servicios digitales, la infraestructura tecnológica disponible y los procesos críticos para el negocio. Asimismo, establece la línea base del plan mediante la evaluación del grado de dependencia institucional respecto a sus herramientas tecnológicas y de información.

Fase 2. Análisis de impacto al negocio (BIA)

La fase de análisis de impacto al negocio (BIA) consiste en la identificación de las funciones críticas de la organización y en la valoración de las consecuencias que generaría su interrupción en ámbitos administrativos, legales y operativos. Asimismo, en esta fase se definen los parámetros de recuperación, como el RTO (Recovery Time Objective) y el RPO (Recovery Point Objective), que sirven de referencia para establecer la capacidad de resiliencia de la institución.

Fase 3. Gestión de riesgo tecnológicos

La fase de gestión de riesgos tecnológicos se fundamenta en la norma ISO/IEC 27005, la cual establece un marco metodológico para la identificación, análisis y evaluación de riesgos en los sistemas de información. En esta etapa se describen las amenazas y vulnerabilidades que pueden afectar a los servicios digitales, así como la estimación del nivel de riesgo asociado. El propósito de la fase es priorizar los riesgos más relevantes y establecer lineamientos generales para la definición de controles preventivos, detectivos y correctivos que contribuyan a la continuidad de las operaciones críticas de la organización.

Fase 4. Estrategias de continuidad

La fase de estrategias de continuidad tiene como propósito definir las medidas generales orientadas a garantizar la continuidad de los servicios considerados críticos. En esta etapa se establecen lineamientos relacionados con la redundancia de los recursos, la disponibilidad de respaldos de información, la identificación de sitios alternos de operación y la preparación de protocolos de comunicación y coordinación institucional frente a posibles contingencias.

Fase 5. Plan de respuesta u recuperación

La fase de plan de respuesta y recuperación se orienta a la definición de los procedimientos generales que deben considerarse antes, durante y después de un evento disruptivo. En esta etapa se establecen lineamientos sobre la asignación de responsabilidades, la disponibilidad de recursos de emergencia y los mecanismos de comunicación con las partes interesadas, tanto internas como externas, con el fin de garantizar la reanudación ordenada de las operaciones críticas.

Fase 6. Mantenimiento y mejora continua

La fase de mantenimiento y mejora continua se orienta a garantizar que el Plan de Continuidad de Negocio mantenga su vigencia y pertinencia en el tiempo. En esta etapa se establece la necesidad de un enfoque dinámico que permita la actualización constante del plan frente a los cambios tecnológicos, normativos y organizacionales, asegurando así su alineación con la realidad institucional y su capacidad de respuesta ante nuevos escenarios de riesgo.

4.3 Desarrollo del plan de continuidad de Negocio en base a la metodología ISO 22301

4.3.1. Creación del programa BCP

Se designa al jefe del Departamento de Tecnologías de la Información como responsable principal del BCP, en coordinación con el gerente de TI. Juntos conformarán un Comité de

Continuidad y Gestión de Riesgos, encargado de coordinar acciones de prevención, mitigación y respuesta ante incidentes. El propósito es que todo el personal administrativo y operativo conozca los procedimientos del plan y actúe de manera ordenada ante cualquier contingencia.

4.3.2 Comprensión de la empresa

- **Misión**

Construimos una sociedad intercultural, equitativa, justa, brindamos servicios con amabilidad, nos apoyamos en la cooperación local e internacional y comunicamos oportunamente todas nuestras acciones.

- **Visión**

Cantón intercultural, comunicativo, justo, con una sociedad satisfecha por los servicios recibidos.

4.3.3. Estructura Orgánica

La estructura orgánica del Gobierno Autónomo Descentralizado Intercultural del Cantón Cañar (GADICC) responde a un modelo jerárquico y funcional que permite la gestión eficiente de los recursos municipales y la prestación de servicios a la ciudadanía. Está conformada por niveles estratégicos, ejecutivos, asesores y operativos que articulan las distintas direcciones y unidades administrativas, de acuerdo con sus competencias institucionales.

Este esquema organizativo garantiza la coordinación entre los procesos gobernantes, habilitantes, agregadores de valor y desconcentrados, promoviendo una administración pública moderna, inclusiva y transparente. En este marco, la Unidad de Tecnologías de la Información y las Telecomunicaciones cumple un papel clave como soporte transversal,

asegurando la continuidad operativa de los servicios digitales y el fortalecimiento de la gestión institucional.

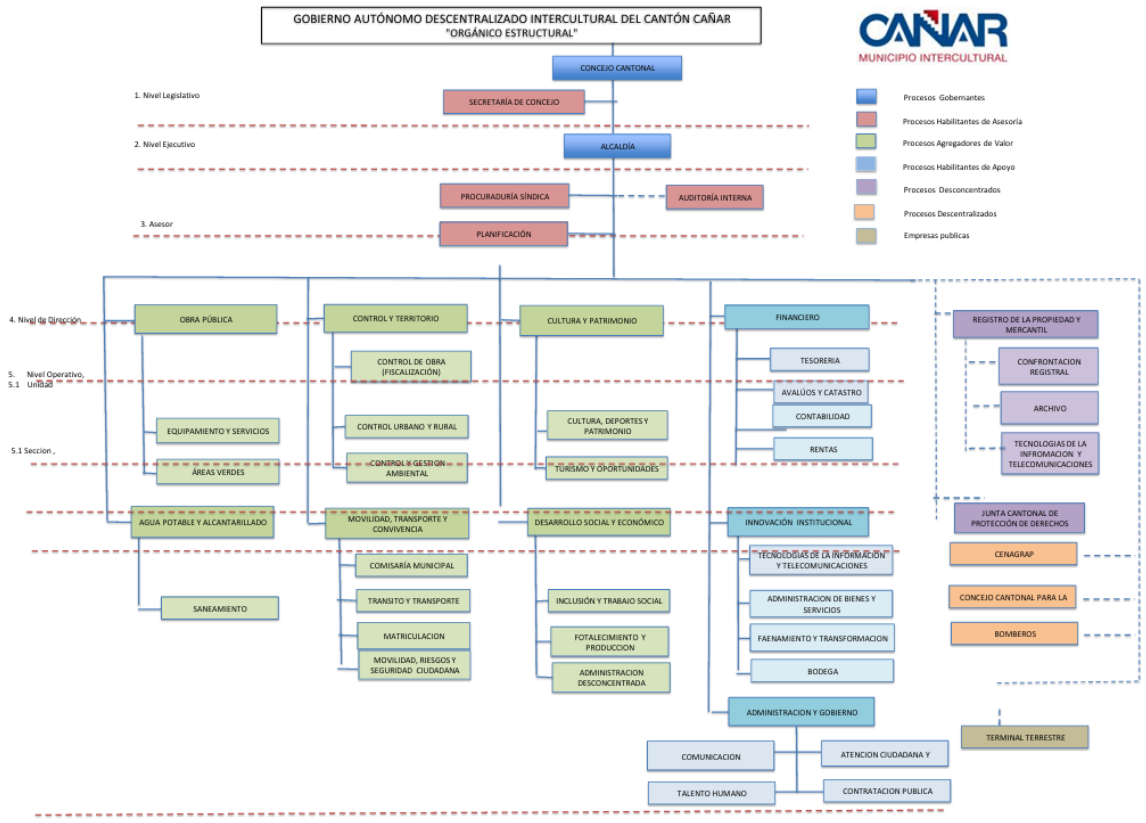


Ilustración 1. Organigrama estructural del GADICC

4.3.4. Estructura del Área de Tecnologías de la Información y Telecomunicaciones

El área de Tecnologías de la Información y Telecomunicaciones del GAD Intercultural del Cantón Cañar es responsable de administrar los sistemas informáticos, la red institucional y la seguridad tecnológica. Su estructura, encabezada por el Asesor de Tecnologías de la Información y Telecomunicaciones, permite coordinar de forma eficiente las actividades de desarrollo, soporte y mantenimiento.

Bajo su dirección operan dos ejes principales: Desarrollo de Sistemas, a cargo del Analista Informático de Desarrollo y el Analista Técnico de Desarrollo, responsables del diseño y actualización de aplicaciones institucionales; y Redes, Soporte y Seguridad, liderado

por el Analista Informático de Redes, Soporte y Seguridad, con apoyo del Analista Técnico de Soporte, encargado de la conectividad, asistencia a usuarios y respaldo de datos.

Esta estructura garantiza la gestión continua de los servicios tecnológicos, la atención oportuna de incidentes y el soporte esencial para la implementación del Plan de Continuidad de Negocio (BCP) del GADICC.

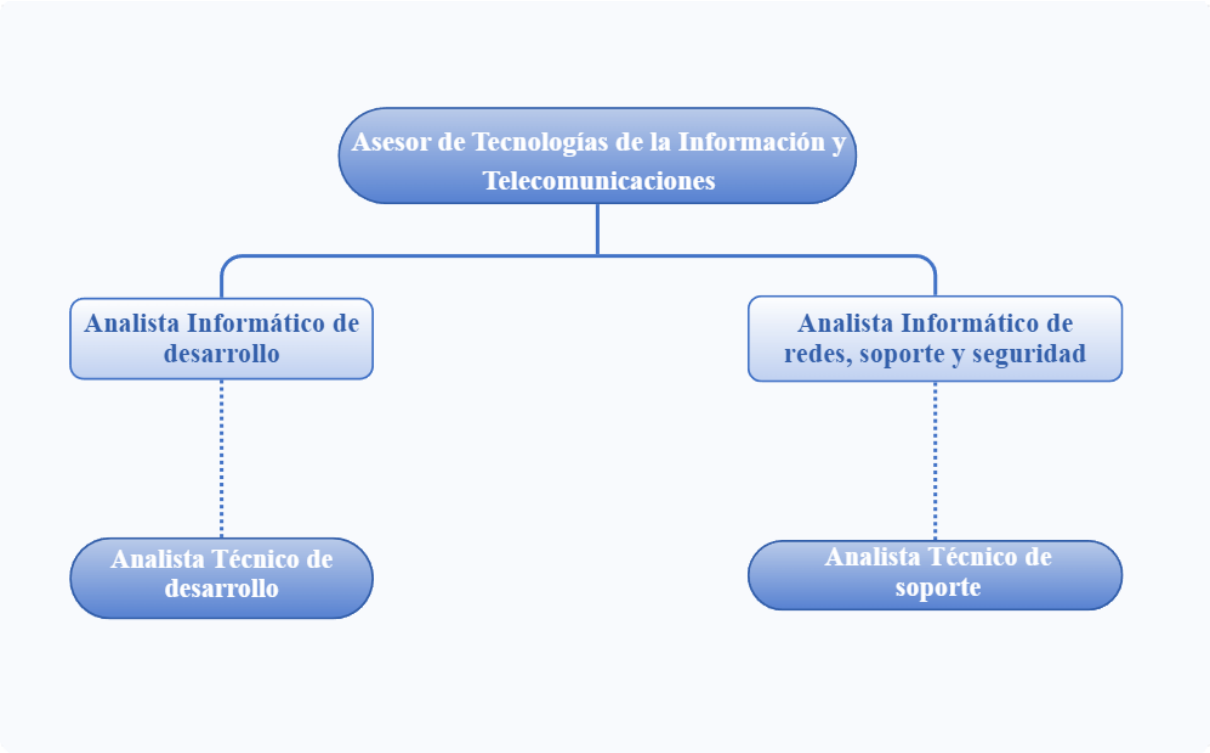


Ilustración 2. Organigrama del área de TIC

4.3.5. Identificación de Procesos

La figura presentada a continuación muestra el mapa de procesos del GAD Intercultural del Cantón Cañar, el cual ilustra de manera estructurada los principales procesos institucionales y su organización funcional.

Este mapa es una herramienta estratégica que permite visualizar la interrelación de las direcciones y unidades clave dentro del GADICC, enfocándose en los procesos operativos y de soporte que garantizan la eficacia y eficiencia de la gestión pública.

El mapa de procesos también ayuda a identificar las áreas críticas dentro del Plan de Continuidad de Negocio (BCP), especialmente aquellas relacionadas con la gestión de servicios digitales y la infraestructura tecnológica, esenciales para asegurar la continua prestación de servicios a la ciudadanía y el adecuado funcionamiento de los procesos administrativos.

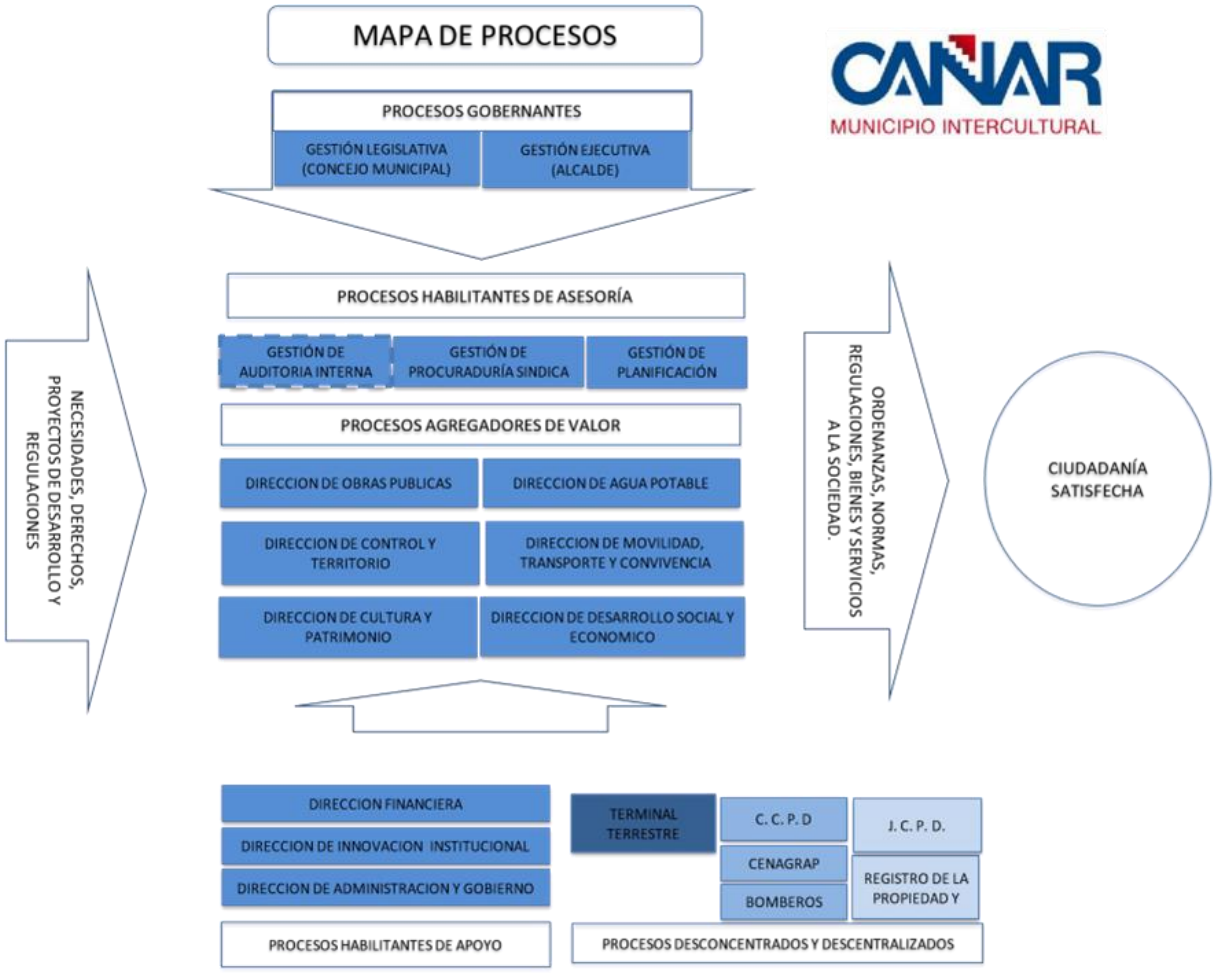


Tabla 5. Unidades Institucionales y procesos vinculados a los servicios digitales

En el marco del Plan de Continuidad de Negocio (BCP), se identificaron los procesos clave dentro del GAD Intercultural del Cantón Cañar que dependen de los servicios digitales para garantizar la operatividad del municipio.

Estos procesos fueron seleccionados tomando en cuenta su importancia estratégica y su impacto directo en la administración pública y los servicios al ciudadano. La implementación de tecnologías de la información y comunicación (NTIC) permite automatizar y optimizar estos procesos, mejorando la eficiencia de la gestión municipal, facilitando la interacción con la ciudadanía y garantizando la continuidad operativa de los servicios más críticos, tales como la gestión tributaria, trámites administrativos y control territorial.

Tabla 4. Identificación de procesos digitales clave. Elaboración propi con base al organigrama institucional del GADICC

Unidad / Dirección	**Proceso relacionado con servicios digitales**	**Descripción / Función principal**
Gestión Legislativa (Concejo Municipal)	Gestión de normativas digitales	Desarrollo de plataformas legales y normativas electrónicas para la ciudadanía.
Gestión Ejecutiva (Alcaldía)	Implementación de políticas tecnológicas	Alineación de la estrategia tecnológica con las políticas institucionales para la digitalización de servicios.
Dirección de Obras Públicas	Gestión digital de infraestructura pública	Uso de plataformas para el seguimiento y gestión de proyectos de infraestructura urbana y rural.

Dirección de Agua Potable	Gestión de redes y monitoreo	Digitalización de los sistemas de gestión y control de redes de agua potable.
Dirección de Control y Territorio	Administración digital de terrenos y catastros	Digitalización del proceso de gestión territorial mediante SIG y plataformas de gestión de catastros.
Dirección de Innovación Institucional	Implementación de soluciones tecnológicas	Aceleración de proyectos de digitalización, incluyendo la creación de APIs y soluciones móviles.
Dirección Financiera	Sistema de recaudación electrónica	Digitalización de pagos, facturación y gestión tributaria mediante plataformas electrónicas.
Dirección de Administración y Gobierno	Gestión de trámites en línea	Facilitación de trámites administrativos para los ciudadanos a través de plataformas electrónicas.
Dirección de Seguridad Ciudadana	Control y gestión digital de emergencias	Implementación de plataformas de monitoreo y respuesta ante incidentes.
Terminal Terrestre	Gestión de transporte público digital	Plataforma para el control y gestión digital de servicios de transporte público y movilidad urbana.

4.4. Identificación de activos GADICC

La identificación de activos críticos es un componente clave del Plan de Continuidad de Negocio (BCP), ya que permite priorizar la protección de aquellos elementos que son indispensables para garantizar la operatividad de los servicios digitales.

En este caso, los activos primarios incluyen la información institucional (bases de datos, registros digitales), los sistemas de gestión tributaria y catastral, y los servidores y redes que soportan las plataformas tecnológicas del GADICC.

Los activos de apoyo incluyen los equipos de cómputo, personal capacitado y proveedores externos que, aunque no son directamente parte del sistema tecnológico, son necesarios para el funcionamiento adecuado y la continuidad operativa de los servicios digitales.

Tabla 5 Identificación de activos GADICC

Tipo de activo	Activo específico	Descripción funcional	Unidad responsable
Información	Base de datos institucional (Catastro, Finanzas, Trámites)	Información crítica sobre predios, pagos y contribuciones; esencial para la gestión administrativa y fiscal.	Dirección TIC / Finanzas / Catastro
Información	Registros de trámites electrónicos	Registra todos los procesos y solicitudes	Atención Ciudadana / TIC

		gestionados electrónicamente por los ciudadanos.	
Aplicaciones	Sistema de recaudación tributaria	Plataforma para la gestión de impuestos, pagos en línea y facturación electrónica.	Dirección Financiera
Aplicaciones	Sistema catastral	Herramienta para el registro y gestión de propiedades y terrenos, vital para el desarrollo urbano y rural.	Dirección de Catastro
Infraestructura	Servidores físicos y virtuales	Equipos de procesamiento y almacenamiento de datos institucionales, virtualizados para garantizar disponibilidad.	Dirección TIC

Infraestructura	Red de comunicaciones e internet	Conectividad interna y externa que soporta todos los sistemas, comunicaciones y procesos digitales.	Dirección TIC
Infraestructura	Equipos de cómputo y periféricos	Estaciones de trabajo para personal, accesos a sistemas y software administrativo.	Dirección TIC / Unidades operativas
Infraestructura	Sistema eléctrico y UPS	Soporte energético para asegurar el funcionamiento continuo de los servidores y sistemas críticos.	Dirección Administrativa
Recursos humanos	Personal técnico y administrativo	Encargados de operar, mantener y asegurar la continuidad de los sistemas y servicios digitales.	Dirección TIC / Unidades usuarias

Servicios externos	Proveedores de software y servicios en la nube	Servicios de infraestructura tecnológica externa y licencias de software esenciales para el funcionamiento de sistemas.	Dirección TIC / Compras Públicas

4.5 Evaluación de riesgos basados en la metodología Margerit

Para valorar los activos y los riesgos identificados, se aplicó una combinación de escalas cualitativas y cuantitativas, siguiendo los lineamientos de la metodología MAGERIT v3 y los principios de la gestión del riesgo ISO/IEC 27005.
Estas escalas permiten asignar valores numéricos a la probabilidad de ocurrencia de una amenaza y al impacto potencial que tendría sobre los activos críticos.

La combinación de ambos factores facilita el cálculo del nivel de riesgo mediante la relación:

$$\textbf{Riesgo} = \textbf{Probabilidad} \times \textbf{Impacto}$$

A continuación, se presentan las escalas empleadas para la valoración:

Tabla 6 Valores de la probabilidad

Nivel	Valor Probabilidad	Descripción cualitativa
Muy baja	1	El evento es poco probable; no existen antecedentes similares en la institución.

Baja	2	Puede presentarse en situaciones excepcionales.
Media	3	Posibilidad moderada de ocurrencia; existen incidentes aislados.
Alta	4	Probabilidad considerable de que ocurra; se han registrado eventos similares.
Muy alta	5	Ocurrencia casi segura o frecuente.

Tabla 7 Escala de valores de impacto

Nivel	Valor Impacto	Descripción cualitativa
Muy bajo	1	Afectación mínima, sin interrupción perceptible del servicio.
Bajo	2	Interrupción leve o temporal con mínima afectación operativa.
Medio	3	Afecta parcialmente los servicios digitales o procesos internos.
Alto	4	Afecta significativamente la operación institucional y la atención al usuario.
Crítico	5	Interrupción total de los servicios digitales o pérdida de información sensible.

4.5.1 Evaluación de riesgos Tecnológicos

Para valorar los activos y los riesgos identificados, se aplicó una combinación de escalas cualitativas

Con base en las escalas de probabilidad e impacto definidas anteriormente, se construye la matriz de evaluación del riesgo, que permite determinar la severidad o criticidad de cada evento adverso.

Tabla 8 Evaluación de riesgos tecnológicos

Valor	Nivel de riesgo	Descripción e interpretación
1 – 5	**Bajo**	Riesgo menor; el evento no afecta de manera significativa los servicios digitales. Puede aceptarse con medidas de control básicas y monitoreo continuo.
6 – 10	**Medio**	Riesgo moderado que podría afectar parcialmente la operación institucional. Requiere aplicar medidas preventivas y revisión periódica.
11 – 15	**Alto**	Riesgo significativo que puede interrumpir servicios digitales clave o generar pérdidas de datos. Debe ser gestionado con planes de mitigación y controles inmediatos.
16 – 20	**Muy Alto**	Riesgo severo que compromete la disponibilidad y continuidad de los sistemas. Se requieren acciones urgentes de contingencia y recuperación.
21 – 25	**Extremo**	Riesgo intolerable; puede provocar pérdida total de información o colapso de servicios. Debe eliminarse o transferirse de inmediato mediante medidas estructurales o tecnológicas.

4.5.2 Evaluación de riesgos .

En esta etapa se identifican las amenazas que podrían causar daños y las debilidades que hacen vulnerables a los activos de la institución. Luego, se analiza qué tan probable es que ocurran esos eventos y qué impacto tendrían sobre los servicios digitales.

Con esta información, se determina el nivel de riesgo de cada activo y se pueden definir medidas de prevención y recuperación para reducir los efectos negativos y asegurar que los servicios continúen funcionando ante cualquier imprevisto**.**

Tabla 9 Resultado evaluación de los riesgos

Activo	**Amenaza identificada**	**Vulnerabilidad asociada**	**Probabilidad (1–5)**	**Impacto (1–5)**	**Nivel de riesgo**
Base de datos institucional (Catastro, Finanzas, Trámites)	Ciberataque (ransomware, hacking)	Falta de copias de seguridad automáticas o actualización regular	4	5	20
Sistema de recaudación tributaria	Fallo en servidor / corte de energía prolongado	Dependencia de un único servidor sin redundancia crítica	3	5	15
Sistema catastral	Pérdida de datos o	No hay respaldo externo o en	4	4	16

	corrupción de base de datos	tiempo real de la base de datos			
Portal web institucional	Ataque DDoS (denegación de servicio)	No hay protección adecuada contra ataques externos (firewall débil)	3	4	12
Red de comunicaciones e Internet	Interrupción del servicio de ISP o conexión caída	Dependencia de un solo proveedor de Internet (ISP)	4	3	12
Equipos de cómputo y periféricos	Malware, virus, error humano	Antivirus desactualizado o falta de protección perimetral	3	3	9
Servidores físicos y virtuales	Fallos técnicos, sobrecarga o fallo de hardware	Falta de monitoreo de temperatura o energía (UPS insuficiente)	3	5	15

Sistema eléctrico y UPS	Cortes prolongados de energía	No existe sistema de energía alternativo o planta de emergencia	4	5	20
Personal técnico y administrativo	Errores humanos, falta de capacitación	Falta de capacitación en nuevas herramientas o procesos tecnológicos	3	4	12
Proveedores de servicios en la nube	Interrupción del servicio, incumplimiento de SLA	Dependencia de un solo proveedor o falta de contrato de respaldo	3	4	12
SIGAME (Sistema de Gestión y Control de Vehículos)	Interrupción del servicio o pérdida de datos	Falta de respaldo de datos y vulnerabilidad en la base de datos	3	4	12

Sistema de control y gestión de vehículos	Fallos del sistema o mal funcionamiento de los equipos	Mantenimiento insuficiente de hardware o software obsoleto	3	3	9
Sistema de control de personal	Error de entrada de datos o manipulación incorrecta	Falta de controles de acceso a sistemas o registro de actividades	3	3	9
Sistema Integrado Municipal (SIM)	Ciberataque (ransomware, hacking)	Vulnerabilidad en la protección de contraseñas y falta de cifrado	4	5	20
Sistema web SIM	Ataque DDoS o caída de servidor	No se implementa firewall adecuado ni protección contra inyecciones SQL	4	4	16

Correo electrónico institucional	Acceso no autorizado o robo de credenciales	Contraseñas débiles o falta de autenticación multifactor	3	4	12
Web institucional	Infiltración por vulnerabilidad en el CMS	Ausencia de actualizaciones de seguridad y plugins desactualizados	3	4	12

El análisis realizado permitió identificar los principales activos tecnológicos del GAD Intercultural del Cantón Cañar y los riesgos que podrían afectar su correcto funcionamiento. Entre los activos con mayor nivel de riesgo se encuentran la base de datos institucional, el Sistema Integrado Municipal (SIM) y el sistema eléctrico y UPS, los cuales alcanzan valores de riesgo de 20, considerados críticos por su alta probabilidad de ocurrencia y el fuerte impacto que tendrían sobre los servicios digitales.

Otros activos, como los servidores físicos y virtuales, el sistema catastral y los sistemas web, presentan niveles de riesgo altos, lo que evidencia la necesidad de fortalecer las medidas de respaldo, la protección contra ataques informáticos y la disponibilidad energética.

Asimismo, se identificaron activos con riesgo medio, como los equipos de cómputo, el sistema de control de personal y el sistema de control de vehículos, donde las vulnerabilidades se relacionan principalmente con la falta de mantenimiento preventivo y actualización de software.

En conjunto, los resultados muestran que la institución depende en gran medida de su infraestructura tecnológica, por lo que es esencial implementar estrategias de prevención y recuperación que permitan reducir los niveles de riesgo y asegurar la continuidad operativa de los servicios municipales ante posibles incidentes.

4.5.3 Salvaguardas propuestas para los activos tecnológicos críticos

Las salvaguardas son medidas preventivas, detectivas y correctivas que se aplican para proteger los activos tecnológicos ante los riesgos identificados en la evaluación previa. Su objetivo es reducir la probabilidad de que ocurra un incidente y minimizar el impacto que este podría generar en los servicios digitales del GAD Intercultural del Cantón Cañar.

Estas acciones buscan fortalecer la seguridad, disponibilidad y confiabilidad de los sistemas más importantes para la gestión municipal, garantizando que los procesos continúen funcionando incluso frente a fallos, ataques informáticos o interrupciones del servicio.

Las salvaguardas propuestas en la siguiente tabla se han determinado considerando el nivel de riesgo de cada activo y las capacidades actuales de la institución, priorizando aquellas que resultan más eficaces y viables dentro de la infraestructura tecnológica existente.

Activo	**Riesgo identificado**	**Salvaguarda preventiva**	**Salvaguarda detectiva**	**Salvaguarda correctiva**
Sistema de recaudación tributaria	Fallo en servidor / corte de energía prolongado	Implementar redundancia de servidores (backups y servidores secundarios).	Monitoreo remoto de servidores y energía para alertas de	Restauración de datos a partir de la última copia de seguridad en 2 horas.

			posibles fallos.	
Sistema catastral	Pérdida de datos o corrupción de base de datos	Implementar copias de seguridad automáticas cada hora en servidores externos.	Monitoreo continuo de integridad de datos con alertas automáticas ante corrupción.	Recuperación de datos desde la nube o servidor secundario en menos de 3 horas.
Portal web institucional	Ataque DDoS (denegación de servicio)	Instalar un firewall avanzado y sistemas de protección ante ataques DDoS.	Análisis de tráfico en tiempo real y monitoreo de patrones anormales.	Restaurar servicio desde un servidor espejo o balanceo de carga en 4 horas.
Red de comunicaciones e Internet	Interrupción del servicio de ISP o conexión caída	Contratación de proveedores alternativos de ISP con enlaces redundantes.	Monitoreo constante de conectividad para identificar interrupciones rápidamente.	Conmutación automática a proveedor secundario (failover) en menos de 1 hora.

Servidores físicos y virtuales	Fallos técnicos, sobrecarga o fallo de hardware	Implementar virtualización y almacenamiento distribuido para evitar cuellos de botella.	Monitoreo constante de servidores para detectar fallos de hardware o sobrecargas.	Recuperación de servicio con máquinas virtuales secundarias en 2 horas.
Sistema eléctrico y UPS	Cortes prolongados de energía	Instalar generadores de energía alternativos y sistemas UPS de respaldo en todas las áreas críticas.	Monitoreo remoto de sistemas de UPS y energía para detectar fallos a tiempo.	Activar generadores de respaldo automáticamente al detectar corte de energía.
Personal técnico y administrativo	Errores humanos, falta de capacitación	Capacitación continua en ciberseguridad y procedimientos de emergencia.	Revisión de logs de acceso y actividad de usuarios para detectar errores.	Restauración de configuraciones o reentrenamiento tras incidentes técnicos.

Proveedores de servicios en la nube	Interrupción del servicio, incumplimiento de SLA	Firmar acuerdos de nivel de servicio (SLA) con cláusulas de recuperación ante desastres.	Monitoreo constante de la infraestructura en la nube para identificar fallos.	Activar servicio alternativo en la nube o proveedores secundarios en 4 horas.
SIGAME (Sistema de Gestión y Control de Vehículos)	Interrupción del servicio o pérdida de datos	Respaldo automático de datos en servidores externos.	Monitoreo de la integridad de datos y alertas ante inconsistencias.	Recuperación de datos desde la copia de seguridad en 3 horas.
Sistema de control y gestión de vehículos	Fallos del sistema o mal funcionamiento de los equipos	Mantenimiento preventivo regular de hardware y software.	Sistema de alertas automáticas ante fallos del sistema de gestión de vehículos.	Reemplazo de equipo o actualización de software según diagnóstico de error.

4.5.4 Estrategias para la gestión del BCP: Tiempos de recuperación (RTO y RPO)

La definición de estrategias de gestión dentro del Plan de Continuidad de Negocio (BCP) permite establecer los procedimientos necesarios para garantizar la recuperación operativa de los servicios digitales del GAD Intercultural del Cantón Cañar ante eventos disruptivos.

Estas estrategias están orientadas a mantener la disponibilidad de los sistemas críticos, minimizar la pérdida de información y asegurar la prestación continua de los servicios públicos digitales**.**

Activo / Servicio digital	**RTO (Tiempo máximo de recuperación)**	**RPO (Pérdida máxima de datos aceptable)**	**Estrategia de recuperación**	**Responsable Principal**
Base de datos institucional (Catastro, Finanzas, Trámites)	2 horas	30 minutos	Copia en tiempo real y respaldo en la nube para recuperación rápida.	Dirección TIC / Finanzas / Catastro

Sistema de recaudación tributaria	2 horas	30 minutos	Redundancia de servidores y replicación automática de datos.	Dirección Financiera
Sistema catastral	3 horas	1 hora	Respaldo diario y copia en servidores secundarios.	Dirección de Catastro
Portal web institucional	3 horas	1 hora	Servidor espejo con balanceo de carga y copias automáticas.	Comunicación / TIC
Red de comunicaciones e Internet	1 hora	No aplica	Proveedor secundario de ISP y conmutación automática (failover).	Dirección TIC
Equipos de cómputo y periféricos	6 horas	4 horas	Reinstalación desde imagen de sistema y repositorios de software.	Dirección TIC / Unidades operativas
Servidores físicos y virtuales	2 horas	30 minutos	Virtualización y servidores de respaldo para recuperación rápida.	Dirección TIC

Sistema eléctrico y UPS	0.5 horas	No aplica	Generador alterno de energía y monitoreo de UPS.	Dirección Administrativa
Personal técnico y administrativo	6 horas	4 horas	Reentrenamiento inmediato en herramientas y sistemas críticos.	Dirección TIC / Unidades usuarias
Proveedores de servicios en la nube	4 horas	1 hora	Acuerdo con SLA y proveedores alternos para asegurar recuperación rápida.	Dirección TIC / Compras Públicas
SIGAME (Sistema de Gestión y Control de Vehículos)	3 horas	1 hora	Copia automática y respaldo externo en la nube.	Dirección de Transporte / TIC
Sistema de control y gestión de vehículos	4 horas	2 horas	Sistema de respaldo y copias de seguridad diarias.	Dirección de Transporte / TIC
Sistema de control de personal	4 horas	2 horas	Respaldo manual y automatizado de los registros de personal.	Dirección de Talento Humano / TIC

Sistema Integrado Municipal (SIM)	2 horas	30 minutos	Replicación de datos en tiempo real y servidores secundarios.	Dirección TIC
Sistema web SIM	4 horas	1 hora	Balanceo de carga y restauración desde servidores espejo.	Dirección TIC
Correo electrónico institucional	1 hora	No aplica	Redundancia de servidores de correo y copia de seguridad periódica.	Dirección TIC
Web institucional	3 horas	1 hora	Servidor espejo y copia de seguridad diaria.	Comunicación / TIC

Los valores definidos en la tabla reflejan los tiempos máximos de tolerancia a la interrupción (RTO) y los puntos máximos de pérdida de información (RPO) que el GADICC puede admitir sin afectar la prestación de sus servicios digitales esenciales.

Los activos con RTO y RPO más bajos como la base de datos institucional y el sistema de recaudación son considerados críticos y, por tanto, deben contar con mecanismos de respaldo automatizados, redundancia de servidores y disponibilidad inmediata de personal técnico para su recuperación.

Estas estrategias constituyen la base operativa del Plan de Continuidad de Negocio (BCP), garantizando la resiliencia tecnológica y la sostenibilidad del servicio público digital en el Cantón Cañar.

4.5.5 Priorización de Recuperación de Servicios Digitales

Una vez determinados los tiempos de recuperación (RTO) y los puntos máximos de pérdida de datos (RPO), es necesario establecer un orden de prioridad para la restauración de los servicios digitales críticos del GAD Intercultural del Cantón Cañar.

Esta priorización permite optimizar los recursos disponibles durante una contingencia y asegurar que los sistemas más relevantes para la gestión municipal y la atención ciudadana se restablezcan en primer lugar.

La priorización se define considerando tres criterios principales:

1. Nivel de criticidad del servicio.
2. Dependencia tecnológica e institucional.
3. Impacto operativo y ciudadano ante la interrupción.

Tabla 10 Priorización de recuperación de los servicio digitales

Prioridad	Activo / Servicio digital	Nivel de criticidad	RTO (Tiempo máximo de	RPO (Pérdida máxima de datos aceptable)	Estrategia principal de recuperación	Responsable Principal
1	Base de datos institucional (Catastro, Finanzas, Trámites)	Crítico	2 horas	30 minutos	Copia en tiempo real y respaldo en la nube para recuperación rápida.	Dirección TIC / Finanzas / Catastro
2	Sistema de recaudación tributaria	Muy alto	2 horas	30 minutos	Redundancia de servidores y replicación automática de datos.	Dirección Financiera
3	Sistema Integrado Municipal (SIM)	Muy alto	2 horas	30 minutos	Replicación de datos en tiempo real y servidores secundarios.	Dirección TIC
4	Sistema catastral	Alto	3 horas	1 hora	Respaldo diario y copia en servidores secundarios.	Dirección de Catastro

5	Portal web institucional	Alto	3 horas	1 hora	Servidor espejo con balanceo de carga y copias automáticas.	Comunicación / TIC
6	Red de comunicaciones e Internet	Muy alto	1 hora	No aplica	Proveedor secundario de ISP y conmutación automática (failover).	Dirección TIC
7	Servidores físicos y virtuales	Alto	2 horas	30 minutos	Virtualización y servidores de respaldo para recuperación rápida.	Dirección TIC
8	Sistema eléctrico y UPS	Muy alto	0.5 horas	No aplica	Generador alterno de energía y monitoreo de UPS.	Dirección Administrativa
9	Sistema web SIM	Alto	4 horas	1 hora	Balanceo de carga y restauración desde servidores espejo.	Dirección TIC

10	Correo electrónico institucional	Alto	1 hora	No aplica	Redundancia de servidores de correo y copia de seguridad periódica.	Dirección TIC
11	SIGAME (Sistema de Gestión y Control de Vehículos)	Alto	3 horas	1 hora	Copia automática y respaldo externo en la nube.	Dirección de Transporte / TIC
12	Sistema de control y gestión de vehículos	Medio	4 horas	2 horas	Sistema de respaldo y copias de seguridad diarias.	Dirección de Transporte / TIC
13	Sistema de control de personal	Medio	4 horas	2 horas	Respaldo manual y automatizado de los registros de personal.	Dirección de Talento Humano / TIC
14	Equipos de cómputo y periféricos	Medio	6 horas	4 horas	Reinstalación desde imagen de sistema y repositorios de software.	Dirección TIC / Unidades operativas

4.5.6 Plan de Respuesta y Recuperación ante Incidentes

El Plan de Respuesta y Recuperación ante Incidentes constituye el componente operativo del Plan de Continuidad de Negocio (BCP) del GAD Intercultural del Cantón Cañar.

Su objetivo es establecer los procedimientos, responsables y tiempos de acción necesarios para restablecer los servicios digitales institucionales tras un evento disruptivo, asegurando la continuidad de las operaciones críticas y minimizando la pérdida de información.

Este plan se activa ante cualquier incidente que afecte la disponibilidad, integridad o confidencialidad de los sistemas tecnológicos, tales como:

- Fallos eléctricos prolongados.
- Ataques informáticos (malware, ransomware, DDoS).
- Daños físicos en servidores o red de comunicaciones.
- Errores humanos o fallos en la configuración del sistema.

4.1.1 Estructura operativa del plan

La ejecución del plan se organiza en tres niveles jerárquicos:

1. Comité de Continuidad Institucional (Nivel Estratégico):
    - Autoriza la activación del BCP.
    - Evalúa el impacto del incidente.
    - Coordina la comunicación institucional con autoridades y ciudadanía.
    - Conformado por: alcalde, director de Planificación, director Administrativo y Asesor de Tecnologías de la Información.
2. Equipo Técnico de Recuperación (Nivel Operativo):

- Ejecuta las acciones técnicas de respaldo, restauración y verificación.
- Supervisa el cumplimiento de los tiempos RTO y RPO.
- Conformado por: Analistas informáticos, personal técnico de soporte y redes.

3. Usuarios Clave de Áreas Afectadas (Nivel de Apoyo):
   - Validan la restauración de los sistemas y datos.
   - Reportan incidencias durante la fase de recuperación.
   - Incluye personal de Finanzas, Catastro, Comunicación y Atención Ciudadana.

4.5.7 Fases del plan de respuesta

Tabla 11 Fases del plan de respuesta

Fase	Descripción	Acciones principales	Responsable
1. Activación	Se identifica el incidente y se determina si cumple los criterios para activar el BCP.	Notificar al Comité de Continuidad, registrar el evento y evaluar el impacto inicial.	Asesor TIC / Auditor Interno
2. Evaluación inicial	Se analiza la extensión del daño y se determina el alcance operativo.	Clasificar el tipo de incidente (leve, moderado, grave) y activar el protocolo correspondiente.	Equipo Técnico
3. Contención	Se aíslan los sistemas afectados para evitar propagación del problema.	Desconectar equipos comprometidos, bloquear accesos y ejecutar medidas de emergencia.	Analistas de Soporte / Seguridad

4. Recuperación	Se restauran servicios, aplicaciones y datos desde respaldos verificados.	Aplicar procedimientos de restauración, validar integridad de datos y probar funcionalidad.	Dirección TIC / Analistas
5. Validación y retorno a la operación normal	Se confirma la funcionalidad completa de los sistemas y se documentan las lecciones aprendidas.	Elaborar informe técnico, actualizar políticas y registrar tiempos de recuperación.	Comité de Continuidad

4.5.8 Comunicación y registro

Durante la activación del BCP se deben ejecutar los siguientes mecanismos de comunicación institucional:

- Comunicación inmediata al Comité de Continuidad y a la Autoridad Máxima (Alcaldía).
- Emisión de boletín interno notificando a los departamentos sobre los servicios afectados.
- Registro de cada evento en el Formato de Incidente Tecnológico (FIT), que documenta: fecha, hora, responsable, causa raíz y acciones realizadas.
- Comunicación externa a la ciudadanía, en caso de interrupciones prolongadas, mediante el portal web institucional o redes sociales oficiales.

4.5.9 Monitoreo y mejora continua

El BCP debe ser revisado periódicamente para asegurar su eficacia y actualización frente a cambios tecnológicos o estructurales.

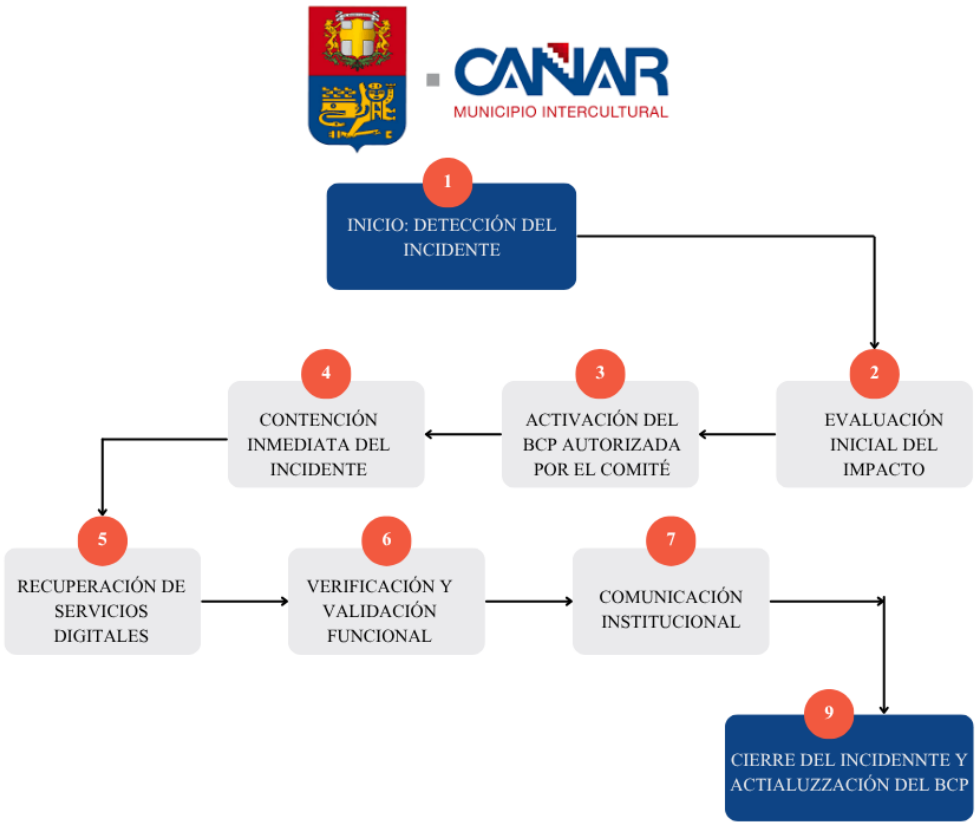
Se recomienda realizar:

- Simulacros semestrales de recuperación de servicios digitales.
- Revisión anual de procedimientos y tiempos RTO/RPO.
- Auditorías internas de cumplimiento de políticas de continuidad.
- Actualización del inventario de activos tecnológicos.

De esta manera, la implementación del presente plan de respuesta y recuperación ante incidentes fortalece la resiliencia tecnológica del GADICC, asegurando la continuidad operativa de sus servicios digitales ante cualquier eventualidad.

4.5.10 Proceso de activación y recuperación del Plan de Continuidad de Negocio (BCP)

A continuación, se describe el proceso de activación y recuperación del BCP:



La figura muestra el flujo operativo del Plan de Continuidad de Negocio (BCP) del GAD Intercultural del Cantón Cañar, el cual se inicia con la detección del incidente y continúa con la evaluación del impacto, la autorización del Comité de Continuidad, la contención técnica inmediata y la recuperación de los servicios digitales. Posteriormente, se realiza la verificación funcional, la comunicación institucional y el cierre del incidente, incorporando las lecciones aprendidas y las actualizaciones correspondientes al BCP.

Este flujo garantiza una respuesta estructurada ante incidentes tecnológicos, asegurando la restauración oportuna de los sistemas informáticos y la continuidad operativa

de los servicios digitales críticos, en concordancia con los lineamientos de la norma ISO 22301 y la metodología MAGERIT v3.

CONCLUSIONES

- Como parte de la primera línea del trabajo del BCP, en el GAD Intercultural del Cañar se pudo sostener la continuidad de la atención de los servicios digitales, incluso, en el caso de la atención remota, se pudo sostener con continuidad el servicio ante las fallas técnicas, desastres o ciberataques. Integrar el BCP en el GAD Intercultural Cañar logra optimizar los dispositivos tecnológicos en cuanto a su atención diaria, gracias a la atención estructurada de las actividades del BCP.
- El BCP se atendió según los criterios de la norma ISO 22301, los cuales en atención internacional el GAD Intercultural cuenta con buenas prácticas internacionalmente reconocidas. Parte de la estrategia de GADIC es la implementación de estrategias que en atención BCP, además de recuperación, se cuenta también con el ciclo del plan de mejoramiento que mide el ajuste del plan BCP.
- El equilibrio de los BCP es la recuperación y para esto su acción fortalecida es la recuperación organizacional al establecer normas de recuperación que contengan cada uno de los diferentes niveles, esto con ayuda del constante de la recuperación. Esto asegura que cualquier acción que se realice en la recuperación de diferentes sistemas podrá fortalecer la recuperación.
- Finalmente, la implementación de este BCP no solo fortalece la capacidad del GADIC para manejar los riesgos relacionados con las tecnologías, sino que también refuerza la confianza ciudadana en los servicios públicos. Al asegurar la disponibilidad ininterrumpida de los servicios digitales, el GADIC demuestra la transparencia, consistencia y efectividad con la que se prestan los servicios, reforzando su imagen institucional y fomentando la participación activa del público.

RECOMENDACIONES

- El GADIC debería establecer un sistema de capacitación continua que permita identificar los cambios que el rol de cada empleado de la institución tiene que ponerse en un marco de funciones en el caso de que un evento de contingencia requiera la institución su activación, y esto debe incluir el contingencia BCP y el protocolo de servicios, en la primera respuesta a la activación de un evento contingente deben existir simulacros y la sistematización de script para respuesta en la contingencia.

- El BCP debe tener como mínimo un cambio de versión de plantilla cada año y mayor cada vez que se dé un cambio drástico a la tecnología, a la estructura organizativa, a la normativa, o a la institución, dentro de la operativa de la institución. Las auditorías y pruebas del BCP deben ser ejecutadas y programadas en períodos que el BCP determine

- Implementación en el BCP activación de recuperación con Sistemas de alta disponibilidad, servidores en la nube de backup y otras tecnologías para poder restaurar de forma ejecutiva y expandir la logística del BCP que permite como mínimo asegurar que en caso de contingencias la operativa continúa.

BIBLIOGRAFÍA

Álvarez Pincay , D. E., Bernal Álava, Á. F., & Álvarez Villacreses, B. M. (2024). Gobierno electrónico en la prestación de servicios públicos: el caso del Departamento de Catastro del GAD (Puerto López. *Revista InveCom*, 1-10.

Ortiz Alulema, I. D. (2020). *repositorio.uasb.edu.ec.* Obtenido de repositorio.uasb.edu.ec: https://repositorio.uasb.edu.ec/bitstream/10644/7760/1/T3349-MAE-Ortiz-Implementacion.pdf

Allauca Lidioma , M. (2023). *repositorio.utc.edu.ec.* Obtenido de repositorio.utc.edu.ec: https://repositorio.utc.edu.ec/server/api/core/bitstreams/8e1c00f4-e711-4ac5-bf73-bf39a0a2a5af/content

Araujo, G. M. (01 de 02 de 2019). *repositorio.uta.edu.ec.* Obtenido de repositorio.uta.edu.ec: https://repositorio.uta.edu.ec/server/api/core/bitstreams/ff461690-a211-46ea-a741-8f3b0a43df6f/content

Camacho Piña, S., & Gutierrez Alvarado , J. C. (2021). *repository.unipiloto.edu.co.* Obtenido de repository.unipiloto.edu.co: https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/10831/ENTREGA%20PROYECTO%20DE%20GRADO%202021%20-%20FINAAL.pdf?sequence=1

Campos, L., Esquivel, J., & Varela, D. (01 de 11 de 2021). *www.ucr.ac.cr*. Obtenido de www.ucr.ac.cr: https://www.ucr.ac.cr/medios/documentos/2022/proyecto-de-graduacio%CC%81n_modelo-de-gestio%CC%81n-de-continuidad_ucr-so.pdf

Castillo Cruz, E. R. (08 de 08 de 2024). *dspace.casagrande.edu.ec.* Obtenido de dspace.casagrande.edu.ec: https://dspace.casagrande.edu.ec/server/api/core/bitstreams/1bfbbaf3-861a-4d20-8bb1-0192ed71652d/content

Chuqui, J. F., Monteros, M., & Durazno-Chumbay, B. (2024). Plan de continuidad del negocio del sistema académico Fénix, en el Instituto Superior Tecnológico del Azuay, con Condición de Superior Universitario. *ATENAS Revista Científica Técnica Y Tecnológica*, *3*(1), 19. doi:10.36500/atenas.3.005

Cordova Montesdeoca, M. D., & Solano Cobos, G. E. (2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/20096/1/UPS-CT009026.pdf

Cubillos Mora, R. A. (2023). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bitstream/handle/10596/57937/Racubillosm.pdf?sequence=1&isAllowed=y

Díaz, P. A. (20 de 10 de 2022). *repositorio.uta.edu.ec.* Obtenido de repositorio.uta.edu.ec: https://repositorio.uta.edu.ec/items/94fedeaf-96dd-4737-b22e-56d74819d3d2

Durán, S. A. (01 de 01 de 2022). *repositorio.itm.edu.co.* Obtenido de repositorio.itm.edu.co: https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/5894/SergioAndres_Duran%20Vasquez_2023.pdf?sequence=1&isAllowed=y

Garzon Quito, E. M. (2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/21396/1/UPS-CT009402.pdf

Hurtado Rodríguez, J. E., & Paspuel Pusda , L. F. (2023). *repositorio.upec.edu.ec.* Obtenido de repositorio.upec.edu.ec: https://repositorio.upec.edu.ec/server/api/core/bitstreams/0bdd7a90-f69e-4531-bb2b-56839f2cb2bc/content

Iza, L. J. (2021). *repositorio.utn.edu.ec.* Obtenido de repositorio.utn.edu.ec: https://repositorio.utn.edu.ec/bitstream/123456789/11530/2/04%20IND%20312%20TRABAJO%20GRADO.pdf

Sangama Reyna, E. J. (2024). Transformación Digital en la Gobernabilidad de América Latina. *Revista Latinoamericana De Ciencias Sociales Y Humanidades*, 2242 – 2259.

Santos, M. S. (01 de 01 de 2024). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/handle/123456789/28170

Sapper, N. E., Capli, A. G., & Legal, H. (2023). Propuesta de un plan de continuidad del negocio para el registro del dominiio de primer nivel de internet del Paraguay(NIC-PY). *Revista sobre estudios e investigaciones del saber académico, 17*(17), 7.

Triana Botia, J. D., & Castro, M. A. (2023). *repository.unipiloto.edu.co.* Obtenido de repository.unipiloto.edu.co: https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12825/Plan%20de%20Contingencia%20Servicio%20TI%20Control%20de%20Acceso%20ofrecido%20por%20Grow%20Data.pdf?sequence=5&isAllowed=y

Villarreal Morales, V., Coro Villarreal, K. E., Fernández Sánchez, E. G., & Cueva Martinez, J. P. (2024). istema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información. *Ciencia Latina Revista Científica Multidisciplinar*, 12956-12979.

Zuñiga, F. F. (01 de 01 de 2021). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bitstream/handle/10596/48686/ffzunigal.pdf?sequence=3&isAllowed=y

ANEXOS

Anexo 1: Manual del Plan de Continuidad

PLAN DE CONTINUIDAD DEL NEGOCIO

ELABORADO POR: MIRELLA VALVERDE

VERSIÓN 1.0

1. Introducción

1.1. Objetivo del Plan

El objetivo principal del Plan de Continuidad de Negocio (BCP) es garantizar la disponibilidad y funcionalidad continua de los servicios críticos del GAD Intercultural del Cantón Cañar, a través de estrategias y procedimientos claros, para mitigar el impacto de posibles incidentes disruptivos (tales como fallos de infraestructura, desastres naturales, ciberataques, etc.).

1.2. Alcance del Plan

Este plan cubre todos los servicios digitales de importancia crítica para la administración y operación del GADICC, incluyendo:

- Sistemas de recaudación tributaria
- Base de datos institucional (Catastro, Finanzas, Trámites)
- Portal web institucional
- Correo electrónico institucional
- Sistemas de control y gestión (vehículos, personal, etc.)

1.3.Propósito y Beneficios del BCP

El propósito del BCP es asegurar la recuperación eficiente y rápida de los activos tecnológicos esenciales, minimizando el tiempo de inactividad y la pérdida de datos. Los beneficios incluyen:

- Continuidad operativa sin interrupciones significativas.
- Seguridad en la gestión de datos críticos.
- Mayor confianza de la ciudadanía en los servicios públicos.
- Cumplimiento de normativas internacionales de gestión de riesgos y continuidad de negocio.

1.4. Definición de Continuidad de Negocio

La Continuidad de Negocio (BC) se refiere a la capacidad de una organización de mantener la operación ininterrumpida de servicios esenciales, aún frente a incidentes o situaciones adversas. Esto implica preparación, planificación y respuesta eficaz ante desastres o fallos en la infraestructura.

2. Marco Normativo y Metodológico

2.1 Normativas Internacionales Aplicables

Este plan se basa en las siguientes normativas y estándares internacionales:

- ISO 22301:2019 - Sistema de Gestión de Continuidad de Negocio.
- ISO/IEC 27001:2013 - Gestión de la Seguridad de la Información.
- MAGERIT v3 - Metodología de Análisis y Gestión de Riesgos en Sistemas de Información.

2.2 Metodología de Gestión de Continuidad de Negocio

La metodología aplicada en el desarrollo de este BCP sigue las mejores prácticas de la gestión de continuidad de negocio, asegurando la identificación de riesgos, la evaluación de impactos y la definición de estrategias para la recuperación de los activos críticos.

3. Evaluación de Riesgos y Activos Críticos

La Evaluación de Riesgos es una de las partes más críticas del Plan de Continuidad de Negocio (BCP), ya que permite identificar qué activos digitales son esenciales para la operación continua del GAD Intercultural del Cantón Cañar. Para cada activo, se evalúan las amenazas que pueden afectar su funcionamiento y la vulnerabilidad de los sistemas a esos eventos, asignando un nivel de riesgo que ayuda a priorizar las estrategias de mitigación.

3.1 Identificación de Activos Críticos

Se han identificado los activos más relevantes para la gestión operativa y la prestación de servicios digitales del GADICC. Estos activos son los que requieren protección prioritaria y deben tener planes de recuperación claramente definidos.

Tipo de activo	Activo específico	Descripción funcional	Unidad responsable
Información	Base de datos institucional	Información crítica sobre predios, pagos y contribuciones; esencial para la gestión administrativa y fiscal.	Dirección TIC / Finanzas / Catastro
Información	Registros de trámites electrónicos	Registra todos los procesos y solicitudes gestionados electrónicamente por los ciudadanos.	Atención Ciudadana / TIC

Aplicaciones	Sistema de recaudación tributaria	Plataforma para la gestión de impuestos, pagos en línea y facturación electrónica.	Dirección Financiera
Aplicaciones	Sistema catastral	Herramienta para el registro y gestión de propiedades y terrenos, vital para el desarrollo urbano y rural.	Dirección de Catastro
Infraestructura	Servidores físicos y virtuales	Equipos de procesamiento y almacenamiento de datos institucionales, virtualizados para garantizar disponibilidad.	Dirección TIC
Infraestructura	Red de comunicaciones e internet	Conectividad interna y externa que soporta todos los sistemas, comunicaciones y procesos digitales.	Dirección TIC
Infraestructura	Equipos de cómputo y periféricos	Estaciones de trabajo para personal, accesos a sistemas y software administrativo.	Dirección TIC / Unidades operativas
Infraestructura	Sistema eléctrico y UPS	Soporte energético para asegurar el funcionamiento continuo de los servidores y sistemas críticos.	Dirección Administrativa
Recursos humanos	Personal técnico y administrativo	Encargados de operar, mantener y asegurar la continuidad de los sistemas y servicios digitales.	Dirección TIC / Unidades usuarias
Servicios externos	Proveedores de software y servicios en la nube	Servicios de infraestructura tecnológica externa y licencias de software esenciales para el funcionamiento de sistemas.	Dirección TIC / Compras Públicas

3.2 Evaluación de Riesgos

En esta fase, se realiza una evaluación detallada de los riesgos asociados con cada uno de los activos críticos. Esto incluye la probabilidad de que se materialice una amenaza y el impacto que tendría sobre los servicios y la operación institucional.

Activo	Amenaza identificada	Vulnerabilidad asociada	Probabilidad (1–5)	Impacto (1–5)	Nivel de riesgo	Clasificación
Base de datos institucional	Ciberataque (ransomware, hacking)	Falta de copias de seguridad automáticas o actualización regular	4	5	20	Crítico
Sistema de recaudación tributaria	Fallo en servidor / corte de energía prolongado	Dependencia de un único servidor sin redundancia crítica	3	5	15	Alto
Sistema catastral	Pérdida de datos o corrupción de base de datos	No hay respaldo externo o en tiempo real de la base de datos	4	4	16	Alto
Portal web institucional	Ataque DDoS (denegación de servicio)	No hay protección adecuada contra	3	4	12	Alto

		ataques externos (firewall débil)				
Red de comunicaciones e Internet	Interrupción del servicio de ISP o conexión caída	Dependencia de un solo proveedor de Internet (ISP)	4	3	12	Alto
Equipos de cómputo y periféricos	Malware, virus, error humano	Antivirus desactualizado o falta de protección perimetral	3	3	9	Medio
Servidores físicos y virtuales	Fallos técnicos, sobrecarga o fallo de hardware	Falta de monitoreo de temperatura o energía (UPS insuficiente)	3	5	15	Alto
Sistema eléctrico y UPS	Cortes prolongados de energía	No existe sistema de energía alternativo o planta de emergencia	4	5	20	Crítico
Personal técnico y	Errores humanos,	Falta de capacitación en nuevas	3	4	12	Alto

administrativo	falta de capacitación	herramientas o procesos tecnológicos				
Proveedores externos (ISP, software)	Interrupción del servicio, incumplimiento de SLA	Dependencia de un solo proveedor o falta de contrato de respaldo	3	4	12	Alto

3.3 Análisis de Impacto al Negocio (BIA)

Este análisis identifica los impactos operativos, financieros y de imagen de la interrupción de los servicios clave. El BIA ayuda a establecer tiempos de recuperación y a definir las prioridades de recuperación de los activos.

Activo	Impacto en la operación	Efecto sobre la atención ciudadana	Efecto financiero
Base de datos institucional	Alta dependencia para el procesamiento de pagos y trámites.	Interrupción grave de servicios digitales a los ciudadanos.	Pérdida de ingresos debido a la falta de acceso a la información tributaria.
Sistema de recaudación tributaria	Afecta la generación de ingresos del GADICC.	Interrupción en la capacidad de los ciudadanos para realizar pagos.	Pérdida directa de ingresos tributarios.

Sistema catastral	Impacto en la gestión de tierras y el desarrollo urbano.	Impide a los ciudadanos acceder a información sobre propiedades.	Afecta los proyectos de desarrollo urbano y rural.
Portal web institucional	Impacto significativo en la visibilidad institucional.	Afecta la capacidad de los ciudadanos para interactuar con el municipio.	Perdida de reputación institucional y baja en la participación ciudadana.
Red de comunicaciones e Internet	Afecta todos los procesos digitales.	Limita la interacción en línea con los ciudadanos.	Pérdida temporal de acceso a servicios fundamentales.

4. Estrategias de Recuperación

Las estrategias de recuperación están alineadas con los objetivos de minimizar el impacto de los incidentes y restaurar rápidamente los servicios digitales más críticos para el GAD Intercultural del Cantón Cañar. Estas estrategias se basan en la priorización de activos críticos y los tempos de recuperación (RTO y RPO) establecidos en el manual.

4.1 Estrategias de Recuperación para Activos Críticos

Activo / Servicio digital	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Estrategia de recuperación	Responsable Principal

Base de datos institucional (Catastro, Finanzas, Trámites)	2 horas	30 minutos	Copia en tiempo real y respaldo en la nube para recuperación rápida. Implementación de bases de datos replicadas.	Dirección TIC / Finanzas / Catastro
Sistema de recaudación tributaria	2 horas	30 minutos	Redundancia de servidores y replicación automática de datos. Respaldo periódico de transacciones en tiempo real.	Dirección Financiera
Sistema catastral	3 horas	1 hora	Respaldo diario en servidores de respaldo y copia en la nube. Recuperación de datos con tiempo de inactividad mínimo.	Dirección de Catastro
Portal web institucional	3 horas	1 hora	Servidor espejo con balanceo de carga y copias automáticas. Redundancia de red para asegurar la disponibilidad continua.	Comunicación / TIC
Red de comunicaciones e Internet	1 hora	No aplica	Proveedor secundario de ISP con conmutación automática (failover). Monitoreo de tráfico en tiempo real para detectar fallos rápidamente.	Dirección TIC
Equipos de cómputo y periféricos	6 horas	4 horas	Reinstalación desde imagen de sistema y repositorios de software. Actualización regular de software y hardware.	Dirección TIC / Unidades operativas
Servidores físicos y virtuales	2 horas	30 minutos	Virtualización para recuperación rápida en servidores secundarios. Implementación de RAID y almacenamiento distribuido.	Dirección TIC

Sistema eléctrico y UPS	0.5 horas	No aplica	Generador alterno de energía y monitoreo de UPS. Mantenimiento preventivo regular para evitar fallos del sistema.	Dirección Administrativa
Personal técnico y administrativo	6 horas	4 horas	Capacitación continua en sistemas críticos y procedimientos de emergencia. Plan de rotación de personal para asegurar disponibilidad.	Dirección TIC / Unidades usuarias
Proveedores de servicios en la nube	4 horas	1 hora	Acuerdo con SLA y proveedores alternos para asegurar recuperación rápida en caso de fallo del proveedor principal.	Dirección TIC / Compras Públicas
SIGAME (Sistema de Gestión y Control de Vehículos)	3 horas	1 hora	Copia automática de datos y respaldo externo en la nube. Implementación de sistemas de redundancia para evitar pérdida de información.	Dirección de Transporte / TIC
Sistema de control y gestión de vehículos	4 horas	2 horas	Sistema de respaldo para la base de datos y copias de seguridad diarias. Restauración rápida desde almacenamiento alternativo.	Dirección de Transporte / TIC
Sistema de control de personal	4 horas	2 horas	Respaldo manual y automatizado de los registros de personal. Recuperación de registros críticos con los mínimos datos posibles.	Dirección de Talento Humano / TIC
Sistema Integrado Municipal (SIM)	2 horas	30 minutos	Replicación de datos en tiempo real y servidores secundarios en diferentes ubicaciones.	Dirección TIC

Sistema web SIM	4 horas	1 hora	Balanceo de carga y restauración desde servidores espejo. Implementación de caché y almacenamiento en la nube para recuperación rápida.	Dirección TIC
Correo electrónico institucional	1 hora	No aplica	Redundancia de servidores de correo y copia de seguridad periódica. Implementación de filtros y políticas de seguridad.	Dirección TIC
Web institucional	3 horas	1 hora	Servidor espejo y copia de seguridad diaria. Protección contra ataques DDoS y firewalls avanzados.	Comunicación / TIC

Explicación de las Estrategias de Recuperación:

- **Estrategias preventivas:**
  Las estrategias preventivas están diseñadas para reducir la probabilidad de que un incidente ocurra. Se incluyen acciones como la redundancia de servidores, copia de seguridad en la nube y monitorización constante para detectar fallos antes de que afecten a los servicios.
- **Estrategias detectivas:**
  Las estrategias detectivas permiten identificar problemas en las primeras fases del incidente. La monitorización remota, las alertas automáticas y los análisis en tiempo real permiten detectar fallos, realizar diagnósticos rápidos y prevenir interrupciones mayores.
- **Estrategias correctivas:**
  Las estrategias correctivas están orientadas a restaurar los sistemas afectados. Estas incluyen procedimientos de recuperación como la restauración desde copias de seguridad, la conmutación automática a servidores alternos y la recuperación de datos desde la nube.

Tabla de Responsabilidades del BCP

Esta tabla detalla los roles y responsabilidades de cada fase del Plan de Continuidad de Negocio (BCP). Los responsables principales son unidades clave dentro del GAD Intercultural del Cantón Cañar que deben tomar acción en caso de incidentes disruptivos.

Fase del BCP	Acción a tomar	Responsable Principal	Responsable Secundario
1. Activación del BCP	**Notificación de incidente**	Comité de Continuidad Institucional (Alcaldía, Dirección de Planificación)	Dirección TIC, Dirección Administrativa
	Evaluación inicial del impacto	Comité de Continuidad Institucional	Dirección TIC / Personal clave de las áreas afectadas
	Decisión de activación del plan	Comité de Continuidad Institucional	Dirección TIC, Dirección Financiera
	Comunicación inicial a las áreas afectadas	Dirección TIC	Comunicación Institucional
2. Evaluación inicial del incidente	**Clasificación de la severidad del incidente**	Dirección TIC / Comité de Continuidad	Equipo Técnico de Recuperación
	Determinación de la causa raíz	Equipo Técnico de Recuperación	Dirección TIC
	Definición de la estrategia de recuperación	Comité de Continuidad	Dirección TIC, Dirección Financiera
3. Contención inmediata	**Aislamiento de los sistemas afectados**	Equipo Técnico de Recuperación	Dirección TIC
	Desactivación de accesos no autorizados	Dirección TIC, Equipo de Seguridad	Departamento de TI / Soporte Técnico
	Análisis preliminar de la causa raíz	Equipo Técnico de Recuperación	Dirección TIC
4. Recuperación de servicios digitales	**Restauración de datos y servicios**	Equipo Técnico de Recuperación	Dirección TIC, Dirección de Catastro, Dirección Financiera
	Verificación de la integridad de datos	Equipo Técnico de Recuperación	Dirección TIC, Personal clave de las áreas afectadas
	Activación de la infraestructura de respaldo	Dirección TIC	Dirección Administrativa

5. Validación y cierre del incidente	**Verificación funcional completa**	Dirección TIC, Equipo de Recuperación	Unidades afectadas (Finanzas, Catastro, Atención Ciudadana)
	Elaboración de informe post-incidente	Comité de Continuidad	Dirección TIC, Equipo de Recuperación
	Actualización del BCP basado en el incidente	Comité de Continuidad	Dirección TIC
	Revisión y ajustes a las estrategias de recuperación	Comité de Continuidad	Dirección TIC

En la tabla anterior, se propone que el GADICC tenga las siguientes responsabilidades:

Fase de Activación del BCP:

- Comité de Continuidad Institucional (Alcaldía, Dirección de Planificación) toma la decisión de activar el BCP y coordinar la evaluación inicial.
- Dirección TIC coordina las acciones técnicas necesarias para activar la recuperación.

Fase de Evaluación Inicial del Incidente:

- Se realiza una evaluación exhaustiva del impacto, con la clasificación de la severidad y la determinación de la causa raíz. El Comité de Continuidad decide si el plan debe ser activado completamente.

Fase de Contención Inmediata:

- Dirección TIC y el Equipo de Recuperación se encargan de aislar los sistemas afectados para evitar que el incidente se propague.

Fase de Recuperación de Servicios Digitales:

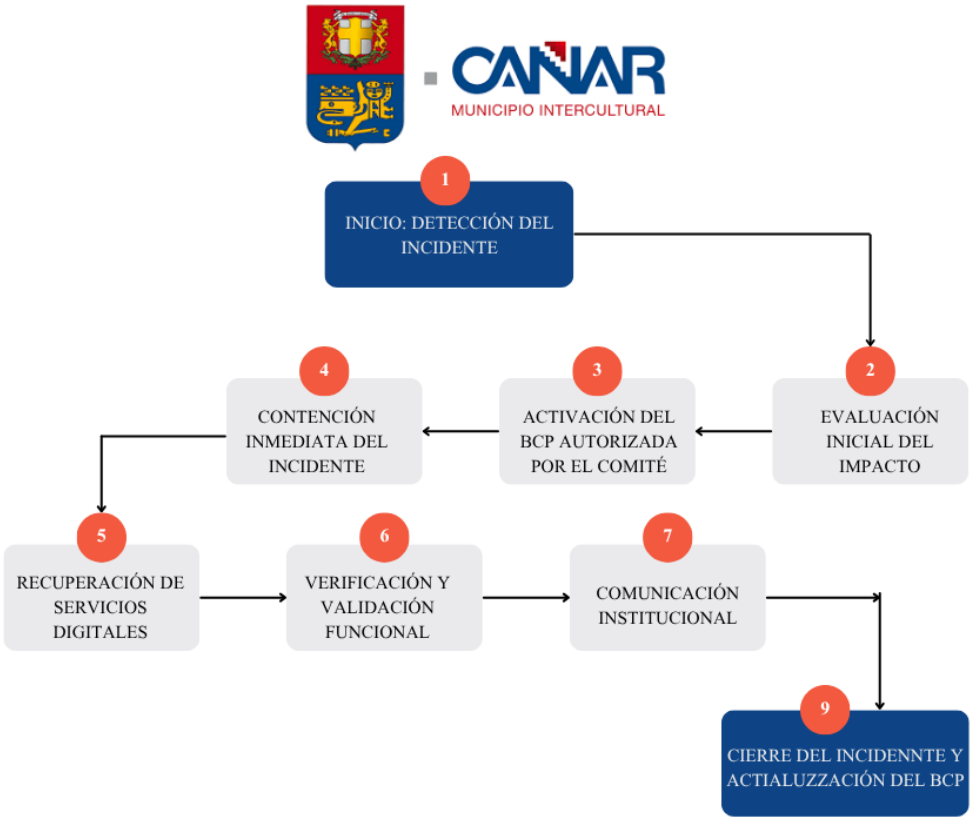
- Dirección TIC lidera la recuperación de los servicios utilizando servidores de respaldo, copias de seguridad y recuperación de datos críticos. Los responsables secundarios como Dirección Financiera y Dirección de Catastro ayudan en la validación de la integridad de los datos.

Fase de Validación y Cierre del Incidente:

- Se realiza una verificación final de que los servicios están operativos y un informe de post-incidente es preparado por el Comité de Continuidad, con lecciones aprendidas y actualizaciones en el BCP para mejorar la respuesta ante futuros incidentes.

5. Diagrama de Flujo del Proceso de Activación y Recuperación del BCP

Este diagrama de flujo reflejará el proceso desde la notificación del incidente hasta el cierre del incidente, con las fases de evaluación, contención, recuperación y validación. Los responsables principales estarán destacados en cada fase.



6. Planes de Prueba y Ejercicios del BCP

El Plan de Continuidad de Negocio (BCP) no es solo un documento estático, sino que debe ser probado regularmente para asegurar su efectividad. Las pruebas y ejercicios permiten

evaluar si los procedimientos de recuperación, los roles y las estrategias de mitigación funcionan correctamente bajo condiciones reales o simuladas.

1. **6.1 Tipos de Pruebas del BCP**

Las pruebas del BCP permiten identificar posibles fallos en la recuperación y la necesidad de ajustes en las estrategias. Existen varios tipos de pruebas, cada una con un enfoque y propósito específico:

2. **Prueba de mesa (Tabletop exercise)**:
    - Simulación de un incidente sin activación real del sistema. Los responsables discuten los pasos a seguir y evalúan los procedimientos sin intervenciones técnicas reales.
    - **Objetivo:** Asegurar que todos los involucrados entienden sus roles y las estrategias de respuesta.
3. **Prueba de simulacro (Simulation exercise)**:
    - Simulación de un incidente real donde se ejecutan las acciones del BCP en un entorno controlado. Los sistemas no son activados, pero se realizan acciones en la infraestructura de respaldo.
    - **Objetivo:** Validar la capacidad de reacción del equipo y verificar los tiempos de recuperación (RTO/RPO).
4. **Prueba funcional (Functional exercise)**:
    - Ejecución de un escenario en el que se activan algunos componentes del BCP. Los sistemas de respaldo pueden entrar en acción, y se realiza la recuperación de datos.
    - **Objetivo:** Probar los procedimientos reales de recuperación y evaluar la eficiencia operativa del BCP.

5. **Prueba completa (Full-scale exercise)**:

- Simulación completa de un incidente disruptivo, donde se ejecuta todo el proceso de activación del BCP: desde la notificación del incidente hasta la restauración de todos los servicios críticos.
- **Objetivo:** Validar completamente la efectividad del BCP, asegurando que todos los servicios y procesos de recuperación estén operativos en tiempo real.

6.2 Ejercicios y Simulacros

Los ejercicios y simulacros deben realizarse anualmente para garantizar que todos los miembros del equipo estén familiarizados con las acciones y procedimientos necesarios en caso de un incidente real. Además, deben realizarse pruebas de manera escalonada para evaluar la efectividad de cada componente del plan en función de su prioridad.

Tipo de prueba	Frecuencia	Responsable	Objetivo
Prueba de mesa (Tabletop)	Anual	Comité de Continuidad / Dirección TIC	Validar los procedimientos y roles en un entorno simulado sin acción real.
Prueba de simulacro	Semestral	Equipo Técnico de Recuperación	Evaluar la capacidad de respuesta en escenarios de menor escala.
Prueba funcional	Anual	Dirección TIC / Unidades afectadas	Validar la recuperación de servicios digitales críticos en un escenario controlado.
Prueba completa	Cada 2 años (o tras actualizaciones significativas)	Comité de Continuidad / Dirección TIC	Asegurar que todos los procesos del BCP funcionen en condiciones reales.

6.3 Documentación y Resultados de las Pruebas

Después de cada prueba o simulacro, se debe generar un **informe post-prueba** que incluya:

- Fecha y hora de la prueba
- Tipo de prueba realizada
- Descripción del escenario
- Tiempo de recuperación (RTO) y pérdida de datos (RPO)
- Lecciones aprendidas y recomendaciones de mejora
- Acciones correctivas y ajustes necesarios en el plan

Este informe servirá para ajustar el Plan de Continuidad de Negocio y mejorar la preparación ante futuros incidentes.

6. Monitoreo y Mejora Continua del BCP

El proceso de monitoreo y mejora continua asegura que el Plan de Continuidad de Negocio (BCP) se mantenga alineado con las necesidades operativas, cambios tecnológicos y desafíos emergentes. La efectividad del plan depende de su capacidad para adaptarse y mejorarse a lo largo del tiempo.

7.1 Monitoreo de la Ejecución del BCP

El monitoreo es fundamental para asegurar que el BCP esté siendo ejecutado adecuadamente y que los tiempos de recuperación (RTO) y la pérdida de datos (RPO) se estén cumpliendo según lo planeado.

Acciones principales:

Monitoreo continuo de los servicios críticos:

- Se debe llevar a cabo un monitoreo constante de la infraestructura tecnológica (servidores, redes, bases de datos) para identificar posibles fallos o vulnerabilidades.
- El monitoreo debe alertar de cualquier anomalía en los servicios digitales para activar la recuperación en caso de un incidente.

Revisión de la efectividad del BCP:

- Realizar una evaluación periódica (anual o semestral) de las acciones tomadas durante los incidentes y simulacros.
- Comparar los resultados obtenidos con los objetivos establecidos en el BCP, como tiempos de recuperación y puntos de recuperación de datos.

Revisión de los procedimientos y roles asignados:

- Verificar que los roles y responsabilidades de las unidades y el personal clave sean claramente comprendidos y estén actualizados.
- Evaluar si las estrategias de recuperación funcionan de manera eficiente y si se ajustan a las necesidades operativas.

7.2 Mantenimiento y Actualización del Plan

El BCP debe mantenerse actualizado y adaptado a los cambios internos y externos de la institución. Las mejoras continuas y la actualización regular del plan son esenciales para enfrentar nuevos riesgos y asegurar la resiliencia tecnológica del GAD Intercultural del Cantón Cañar.

Acciones principales:

1. **Revisión periódica del BCP:**

- El BCP debe revisarse al menos una vez al año, o bien cuando haya cambios significativos en la infraestructura tecnológica, los procesos institucionales o las normativas de seguridad.
- Revisar los resultados de las pruebas del BCP (simulacros, pruebas funcionales, etc.) y ajustar el plan según los hallazgos.

2. **Evaluación de riesgos emergentes:**
    - El BCP debe ser flexible y permitir incorporar nuevas amenazas, como ciberataques o fallos de infraestructura crítica.
    - Identificar y mitigar cualquier nueva vulnerabilidad que pueda afectar los servicios digitales.
3. **Capacitación continua:**
    - Se debe asegurar que el personal clave esté capacitado y entrenado en los procedimientos del BCP.
    - Realizar entrenamientos regulares y evaluaciones de desempeño para asegurar que todos los involucrados comprendan su rol y actúen eficientemente durante un incidente.

7.3 Documentación de Cambios y Mejora del BCP

Cada vez que se realicen cambios importantes en el BCP, estos deben **documentarse adecuadamente** para asegurar la trazabilidad y la mejora continua del plan.

Acciones principales:

1. **Registro de lecciones aprendidas:**
    - Después de cada incidente, simulacro o prueba, se deben documentar las lecciones aprendidas.
    - Actualizar el BCP con los ajustes necesarios para reflejar estas lecciones y mejorar la efectividad del plan.
2. **Revisión y actualización de los procedimientos:**
    - Los procedimientos, tiempos de recuperación (RTO) y puntos de recuperación (RPO) deben revisarse para asegurar que siguen siendo realistas y aplicables.
    - Documentar todos los ajustes realizados y comunicar estos cambios a los equipos responsables.

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Mirella Estefania Alulema Valverde portador(a) de la cédula de ciudadanía Nº 0302352281 En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Plan de continuidad de Negocio (BCP) para los servicios digitales del GADIC del cantón 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 éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, noviembre de 2025

F: .....

Mirella Estefania Alulema Valverde

C.I. 0302352281