

UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

FACULTAD DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DE NEGOCIO BASADO EN LA NORMA ISO 22301 PARA LOS SERVICIOS DIGITALES DEL GADIC SUSCAL

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

AUTOR: JUAN DIEGO SIGUENCIA URGILES

DIRECTOR: ING. DANNY PATRICIO ANDRADE CARDENAS

CAÑAR-ECUADOR

2026

DIOS, PATRIA, CULTURA Y DESARROLLO



UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

FACULTAD DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PLAN DE CONTINUIDAD DE NEGOCIO BASADO EN LA NORMA ISO 22301 PARA LOS SERVICIOS DIGITALES DEL GADIC SUSCAL

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

AUTOR: JUAN DIEGO SIGUENCIA URGILES

DIRECTOR: ING. DANNY PATRICIO ANDRADE CÁRDENAS

CAÑAR- ECUADOR

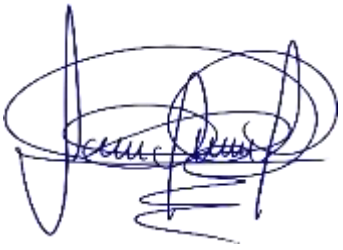
2026

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Juan Diego Siguencia Urgiles portador de la cédula de ciudadanía Nº **030233549-2** Declaro ser el autor de la obra: **"Plan de continuidad de negocios basada en la norma ISO 22301 para los servicios digitales del GADIC Suscal",** sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 29 de septiembre 2026



Juan Diego Siguencia Urgiles

C.I. 0302335492

CERTIFICADO DEL TUTOR

Certifico que el presente trabajo denominado **" Plan de continuidad de negocios basada en la norma ISO 22301 para los servicios digitales del GADIC Suscal** " realizado por **Juan Diego Siguencia Urgiles,** con documento de identidad No. **030233549-2**, previo a la obtención del título profesional de Ingeniero en Sistemas de Información, 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, 29 de septiembre 2026

Ing. Danny Patricio Andrade Cárdenas
DIRECTOR DEL TRABAJO INVESTIGATIVO
UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

DEDICATORIA

Dedico este trabajo, con todo mi amor y gratitud, a mi familia, quienes han sido mi mayor fortaleza y el motivo para seguir adelante durante cada etapa de mi vida.

De manera muy especial, a mi madre, Aleja S., por ser el pilar fundamental de mi vida. Por cada sacrificio realizado, por sus consejos, sus oraciones y, sobre todo, por creer siempre en mí. Gracias, mamá, por enseñarme a no rendirme frente a las dificultades y por acompañarme incondicionalmente en cada paso. Este logro no es solamente mío; también es suyo, porque detrás de cada meta alcanzada están su esfuerzo, su amor y todo aquello que ha hecho por mí.

A mi hermana Alicia LS, por estar siempre a mi lado, por su cariño, comprensión y apoyo incondicional. Gracias por acompañarme tanto en los buenos momentos como en aquellos días difíciles en los que una palabra de aliento significaba mucho. Es una parte muy importante de mi vida y también de este logro.

A mi hermano Carlos y su familia, con mucho cariño, por formar parte de mi vida y acompañarme a lo largo de este camino.

A Danny A. y Mery P., quienes, a pesar de la distancia, siempre encontraron la manera de estar presentes. Gracias por sus palabras de aliento, por preocuparse por mí, por brindarme su apoyo sincero y por acompañarme desde lejos durante este proceso. Su cariño y apoyo tuvieron un significado especial en este camino y los llevo con gratitud en este logro.

A todos ustedes dedico la culminación de una etapa que significó años de esfuerzo, sacrificios, aprendizajes y perseverancia. Cada página de este trabajo representa un paso hacia un sueño que hoy se hace realidad y que tengo la felicidad de compartir con quienes han estado a mi lado.

Con todo mi amor y gratitud, este logro también es para ustedes.

Por Juan Diego Siguencia Urgiles

AGRADECIMIENTO

En primer lugar, agradezco a Dios, por brindarme la vida, la fortaleza, la sabiduría y la perseverancia necesarias para superar cada desafío y permitirme culminar con éxito esta importante etapa de mi formación profesional.

A mi familia, por su amor, apoyo incondicional, paciencia y confianza. Gracias por acompañarme durante este camino, por motivarme a seguir adelante en los momentos difíciles y por ser una fuente permanente de inspiración para alcanzar mis metas.

A mis amigos, por su amistad, apoyo y por compartir conmigo momentos importantes durante esta etapa universitaria. Sus palabras de ánimo y compañía hicieron que este proceso fuera más llevadero y significativo.

Expreso también mi sincero agradecimiento a la Universidad Católica de Cuenca, por brindarme la oportunidad de formarme profesionalmente, así como por los conocimientos, experiencias y herramientas adquiridas a lo largo de mi carrera.

A todos los docentes, por compartir sus conocimientos, experiencias y enseñanzas, contribuyendo de manera significativa a mi formación académica y profesional. Cada enseñanza recibida ha sido parte fundamental de este logro.

De manera especial, agradezco a mi tutor de tesis, Ing. Danny Andrade Cárdenas, por su orientación, dedicación, paciencia y acompañamiento durante el desarrollo de este trabajo. Sus recomendaciones y conocimientos fueron fundamentales para la culminación de esta investigación.

Finalmente, agradezco a todas las personas que, directa o indirectamente, contribuyeron a la realización de este trabajo de titulación. A todos ustedes, mi más sincero agradecimiento.

RESUMEN

El Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal (GADIPCS) presta servicios digitales recaudación tributaria, catastro, registro de la propiedad, portal web y sistemas internos que dependen de una infraestructura tecnológica sin procedimientos formales para su restablecimiento ante interrupciones. Esta investigación tuvo como objetivo diseñar un Plan de Continuidad de Negocio basado en la norma ISO 22301:2019 para dichos servicios. Se adoptó un enfoque cualitativo con diseño de estudio de caso único, de nivel descriptivo y orientación diagnóstica, aplicando una lista de verificación de 66 controles de la ISO/IEC 27002:2022, la revisión documental y el inventario y análisis de riesgos de los activos tecnológicos con la metodología MAGERIT versión 3. El diagnóstico evidenció un cumplimiento global del 60,6 %, con capacidades técnicas instaladas pero un 20 % en continuidad de las actividades institucionales y cumplimiento nulo en gestión de incidentes. De 36 activos inventariados se identificaron 15 críticos; el acceso no autorizado al firewall perimetral alcanzó nivel crítico y la dependencia de un único proveedor de conectividad, nivel alto. La propuesta (PCN-GADIPCS-001) define salvaguardas que reducen el riesgo promedio de 14,3 a 6,4, parámetros de recuperación por servicio con la recaudación tributaria como prioridad uno (RTO de 8 horas, RPO de 4 horas), estrategias de continuidad, un equipo con roles y suplentes, niveles de severidad y criterios de activación, un procedimiento de respuesta en cinco fases, un programa anual de pruebas y formatos operativos, con trazabilidad a las cláusulas 4 a 10 de la norma.

Palabras clave: continuidad de negocio, ISO 22301, servicios digitales, gobierno autónomo descentralizado, análisis de riesgos.

ABSTRACT

The Decentralized, Intercultural, and Participatory Autonomous Government of the Suscal Canton (GADIPCS) provides digital services for tax collection, cadastras management, property registration, its website, and internal systems that rely on a technological infrastructure lacking formal procedures for recovery in the event of disruptions. The study aimed to design a Business Continuity Plan based on the ISO 22301:2019 standard for these services. A qualitative approach was adopted, using a single-case study design with a descriptive level and diagnostic orientation, applying a checklist of 66 controls from ISO/IEC 27002:2022, documentary review, and an inventory and risk analysis of technological assets using the MAGERIT version 3 methodology. The assessment revealed an overall compliance rate of 60.6 %, with technical capabilities in place but 20% compliance with the continuity of institutional activities and zero compliance with incident management. Of the 36 assets inventoried, 15 were identified as critical; unauthorized access to the perimeter firewall reached a critical level, and reliance on a single connectivity provider reached a high level. The proposal (PCN-GADIPCS-001) defines safeguards that reduce the average risk from 14.3 to 6.4, service-specific recovery parameters, with tax collection as the top priority (8-hour RTO, 4-hour RPO), continuity strategies, a team with designated roles and alternates, severity levels and activation criteria, a five-phase response procedure, an annual testing program, and operational forms, all traceability to clauses 4 through 10 of the standard.

Keywords: business continuity, ISO 22301, digital services, decentralized autonomous government, risk analysis.

ÍNDICE

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD I
CERTIFICADO DEL TUTOR II
DEDICATORIA III
AGRADECIMIENTO IV
RESUMEN V
ABSTRACT VI
ÍNDICE VII
ÍNDICE DE TABLAS X
ÍNDICE DE ILUSTRACIONES XI
INTRODUCCIÓN XII
1.1 Planteamiento del problema 1
Formulación del problema 2
1.2 Antecedentes de la Investigación 3
1.3 Justificación de la investigación 4
1.4 Objetivos 5
Objetivos General 5
Objetivos Específicos 5
1.5 Limitaciones 6
1.6 Delimitaciones 6
CAPÍTULO II 8
2 MARCO TEÓRICO 8
2.1 Fundamentos de la continuidad de negocio 8
Concepto de continuidad de negocio 9
Importancia del Plan de Continuidad de Negocio en el sector público 9
Continuidad digital y resiliencia institucional 10
Componentes generales de un Plan de Continuidad de Negocio 10
2.2 Servicios digitales en gobiernos locales 11
Gobierno digital y prestación de servicios públicos 12
Servicios digitales críticos en un GAD municipal 12
Riesgos de interrupción en servicios digitales municipales 13
2.3 Norma ISO 22301 y familia de normas de continuidad 13
Estructura de ISO 22301:2019 13
ISO 22313:2020 como guía de aplicación 15

ISO/TS 22317:2021 para el Análisis de Impacto al Negocio 15
ISO/TS 22332:2021 para planes y procedimientos 16
ISO/IEC 27031:2025 y la preparación TIC para la continuidad 16
2.4 Gestión de riesgos tecnológicos y ciberseguridad 17
Riesgos tecnológicos en servicios digitales públicos 17
Ciberseguridad y continuidad de servicios digitales 17
Activos, amenazas y vulnerabilidades 18
2.5 Análisis de Impacto al Negocio 19
Objetivos del BIA 19
RTO, RPO, MTPD y MBCO 20
Dependencias críticas 20
2.6 Estrategias de continuidad y recuperación 21
Estrategias tecnológicas 21
Estrategias organizacionales 22
Comunicación durante interrupciones 22
2.7 Pruebas, ejercicios y mejora continua 22
Tipos de pruebas del BCP 22
Mejora continua 23
2.8 Normativa ecuatoriana aplicable 23
Gobiernos Autónomos Descentralizados 24
Protección de datos personales 24
Normas de Control Interno 24
2.9 Comparación de normas y marcos aplicables 25
CAPÍTULO III 28
3 MARCO METODOLÓGICO 28
3.1 Enfoque de la Investigación 28
3.2 Nivel de la Investigación 28
3.3 Unidad de Análisis y Fuentes de Información 29
3.4 Técnicas e Instrumentos de Recolección 30
Lista de verificación de la línea base de seguridad (ISO/IEC 27002) 30
Revisión documental 32
Inventario y valoración de activos con MAGERIT 32
Articulación de los instrumentos con la norma ISO 22301 32
3.5 Tratamiento de la Información 33
3.6 Análisis e Interpretación de Resultados del Diagnóstico 34

Fortalezas identificadas 36
Brechas críticas identificadas 37
3.7 Levantamiento y Valoración de Activos del Área de TIC 37
3.8 Análisis de Riesgos de los Activos Críticos según MAGERIT 39
Escalas de valoración 40
Identificación de amenazas y cálculo del riesgo 40
3.9 Fases de la Metodología 43
CAPÍTULO IV 44
4 PROPUESTA 44
4.1 Introducción 44
4.2 Objetivo de la Propuesta 44
4.3 Alcance del Plan 45
4.4 Tratamiento del Riesgo: Salvaguardas Propuestas 45
4.5 Análisis de Impacto al Negocio (BIA) 46
Criterios de impacto 47
Determinación de parámetros de recuperación 47
Recursos mínimos de recuperación 48
4.6 Estrategias de Continuidad 49
4.7 Plan de Respuesta y Recuperación 50
Equipo de continuidad y responsabilidades 50
Niveles de severidad y criterios de activación 51
Fases del procedimiento de respuesta 52
Registro y comunicación 53
4.8 Programa de Pruebas y Ejercicios 54
4.9 Mantenimiento y Mejora Continua 54
4.10 Verificación del Cumplimiento de la Norma ISO 22301:2019 55
Conclusiones 56
Recomendaciones 58
Referencias 60
ANEXOS 63
Anexo F. Protocolo de investigación 64
Anexo A1 77
Anexo A2 81
Anexo B 83
Anexo C 93

Anexo D..... 101
Anexo E.....105

ÍNDICE DE TABLAS

Tabla 1. Componentes generales de un Plan de Continuidad de Negocio.....11
Tabla 2. Estructura de la norma ISO 22301:2019.....14
Tabla 3. Activos, amenazas y vulnerabilidades en el contexto institucional.....18
Tabla 4. Objetivos del Análisis de Impacto al Negocio.....19
Tabla 5. Tipos de pruebas del Plan de Continuidad de Negocio.....23
Tabla 6. Comparación de normas y marcos de referencia aplicables.....26
Tabla 7. Resultados de la lista de verificación por dominio de control ISO/IEC 27002.....35
Tabla 8. Distribución del inventario de activos por categoría MAGERIT.....38
Tabla 9. Activos críticos del GADIC SUSCAL (valor global igual o superior a 9).....39
Tabla 10. Escalas de probabilidad e impacto aplicadas al análisis de riesgos.....40
Tabla 11. Matriz de riesgos de los activos críticos del GADIC SUSCAL.....41
Tabla 12. Fases metodológicas para el diseño del BCP del GADIC SUSCAL.....43
Tabla 13. Salvaguardas propuestas para los activos críticos.....46
Tabla 14. Parámetros de recuperación de los servicios digitales del GADIC SUSCAL.....47
Tabla 15. Recursos mínimos y dependencias por servicio digital.....49
Tabla 16. Estrategias de continuidad por servicio digital crítico.....50
Tabla 17. Estructura del equipo de continuidad del negocio.....51
Tabla 18. Niveles de severidad y criterios de activación del plan.....51
Tabla 19. Programa anual de pruebas del Plan de Continuidad de Negocio.....54
Tabla 20. Trazabilidad entre las cláusulas de la ISO 22301:2019 y la propuesta.....55

ÍNDICE DE ILUSTRACIONES

Figura 1. Ciclo de gestión de la continuidad del negocio según ISO 22301 15

Figura 2. Relación temporal entre RPO, RTO, MTPD y MBCO 20

Figura 3. Nivel de cumplimiento por dominio de control ISO/IEC 27002 36

Figura 4. Mapa de riesgos de los activos críticos del GADIC SUSCAL 42

Figura 5. Objetivos de recuperación de los servicios digitales del GADIC SUSCAL 48

Figura 6. Secuencia de respuesta y recuperación ante incidentes disruptivos 53

INTRODUCCIÓN

Los servicios digitales del Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal (GADIC SUSCAL), como la recaudación tributaria, el catastro, el registro de la propiedad y el portal web institucional, dependen de una infraestructura tecnológica que puede interrumpirse por fallas, ciberataques o desastres. Al no existir procedimientos formales para restablecerlos, la institución se expone a tiempos de recuperación prolongados, pérdida de información y afectación de la atención a la ciudadanía.

Frente a esta situación, el presente trabajo diseña un Plan de Continuidad de Negocio basado en la norma ISO 22301:2019 para los servicios digitales del GADIC SUSCAL, a partir de un diagnóstico de la situación actual, el inventario y análisis de riesgos de los activos tecnológicos con la metodología MAGERIT y un Análisis de Impacto al Negocio.

El documento se organiza en cuatro capítulos: el Capítulo I plantea el problema, los objetivos y el alcance; el Capítulo II desarrolla el marco teórico; el Capítulo III presenta la metodología y los resultados del diagnóstico; y el Capítulo IV contiene la propuesta del plan, seguida de las conclusiones, recomendaciones, referencias y anexos.

CAPÍTULO I

1.1 Planteamiento del problema

En el contexto actual de transformación digital, las instituciones públicas han incorporado de manera progresiva tecnologías de la información para optimizar sus procesos administrativos, mejorar la eficiencia operativa y fortalecer la atención a la ciudadanía. La modernización de la gestión pública puede atribuirse al proceso de digitalización, sin embargo, se ha producido una dependencia excesiva en los sistemas informáticos, plataformas digitales y servicios tecnológicos, convirtiéndolos en aspectos críticos para el funcionamiento de las instituciones (United Nations Department of Economic and Social Affairs, 2024).

Esta dependencia de la tecnología pone a las instituciones en riesgo de muchas maneras que pueden interrumpir las operaciones normales. Estudios recientes muestran que fallos en la infraestructura tecnológica, cortes de energía, amenazas cibernéticas o incluso un error de un empleado pueden generar interrupciones en los servicios digitales y afectar el acceso a la información y la prestación de servicios públicos (Elliott et al., 2010). Estas interrupciones pueden causar pérdida de ingresos y generar una percepción negativa de los servicios gubernamentales. También pueden erosionar la confianza que los ciudadanos depositan en su gobierno.

En tales casos, la gestión de la continuidad del negocio está completamente integrada en las organizaciones actuales, ya que les ayuda a planificar, reducir y responder a las interrupciones. Muchos estudios indican que la planificación formal de la continuidad es fundamental, ya que la incapacidad de una organización para recuperarse rápidamente de un incidente aumenta el tiempo de inactividad y afecta negativamente las operaciones en curso (Torabi et al., 2016).

En lo que respecta a las autoridades locales, este problema es aún más crítico porque los servicios digitales desempeñan un papel fundamental en la administración y recaudación de ingresos, en la prestación de servicios a la ciudadanía y en la gestión de datos institucionales. En el caso del GADIC SUSCAL, los servicios digitales que sostienen sus procesos institucionales,

administrativos y de servicio público principalmente el sistema de recaudación de tasas e impuestos, el sistema de catastros y avalúos, el portal web institucional con sus formularios en línea y servicios de transparencia, y la infraestructura tecnológica que los soporta han presentado interrupciones ocasionadas por cortes de energía eléctrica, fallas de conectividad y problemas en los servidores. Cuando estos eventos ocurren, la recuperación de los servicios se realiza de manera empírica, pues depende del conocimiento individual del personal técnico y no de procedimientos documentados ni de tiempos de recuperación definidos, por lo que el restablecimiento puede extenderse desde varias horas hasta más de un día. Estas interrupciones paralizan la recaudación y los trámites que dependen de los sistemas, generan reclamos ciudadanos por la falta de atención oportuna y ocasionan retrasos operativos y potenciales pérdidas económicas para la institución, sin que exista un registro formal de incidentes que permita dimensionar su impacto real.

La ausencia de un plan estructurado dificulta la identificación de los servicios esenciales, la definición de tiempos objetivos de recuperación, la asignación de responsabilidades y el diseño de estrategias para hacer frente a incidentes. Esto puede provocar la interrupción de servicios cruciales, afectar la gestión institucional y representar una amenaza para la integridad de la información.

Por lo tanto, se requiere diseñar un plan de continuidad del negocio alineado con la norma ISO 22301 para los servicios digitales del GADIC SUSCAL, que fortalezca la capacidad de la institución para prevenir, responder y recuperarse de incidentes disruptivos, y que contribuya a mantener la continuidad de los servicios mientras se desarrolla la resiliencia organizacional.

Formulación del problema

Actualmente, el GADIC SUSCAL no cuenta con un Plan de Continuidad de Negocio estructurado para sus servicios digitales, lo que representa una debilidad institucional ante posibles eventos disruptivos como fallas tecnológicas, cortes de energía, incidentes de ciberseguridad, errores humanos o pérdida de conectividad. Esta situación resulta especialmente crítica considerando que los servicios digitales son fundamentales para la gestión administrativa,

la atención ciudadana, el acceso a la información institucional y la continuidad operativa de los procesos públicos.

La ausencia de un plan formal basado en la norma ISO 22301 limita la capacidad del GADIC SUSCAL para identificar servicios críticos, establecer responsables, definir tiempos de recuperación, organizar procedimientos de respuesta y reducir el impacto de interrupciones tecnológicas. Por ello, se vuelve necesario diseñar un Plan de Continuidad de Negocio que permita fortalecer la resiliencia institucional y garantizar la disponibilidad de los servicios digitales ante situaciones adversas.

¿Cómo debe estructurarse un Plan de Continuidad de Negocio basado en la norma ISO 22301 para fortalecer la continuidad de los servicios digitales del GADIC SUSCAL frente a eventos disruptivos?

1.2 Antecedentes de la Investigación

En un escenario global, Religia y Utama (2024), en su trabajo titulado "Un Marco Innovador para el Plan de Continuidad del Negocio en Organizaciones del Sector Público", propone la integración de la norma ISO 22301:2019 y la guía NIST SP 800-34 Rev. 1 para contextualizar los planes de continuidad de negocio de las organizaciones del sector público. La relevancia del estudio radica en que considera la continuidad de los servicios públicos desde el punto de vista tecnológico, reconociendo que, ante escenarios disruptivos, los sistemas de información son vitales para mantener el funcionamiento de las instituciones. Esto explica por qué proporciona una referencia metodológica para este proyecto preliminar, dado que GADIC SUSCAL también necesita desarrollar un Plan de Continuidad del Negocio con el objetivo de salvaguardar sus servicios digitales.

En otro ejemplo, Dakic et al. (2024), escriben sobre “Planificación de la Continuidad del Negocio (BCP) y Planificación de la Recuperación ante Desastres (DRP)”, y describen la planificación de la continuidad del negocio y la recuperación ante desastres. Este aspecto establece prioridades para la preservación de operaciones y la recuperación de la organización después de una interrupción. El estudio analiza aspectos como la evaluación del riesgo, el análisis del impacto empresarial, así como las estrategias de recuperación, y son muy importantes para el diseño del Plan de Continuidad del Negocio de GADIC SUSCAL,

particularmente en la especificación de métodos y procedimientos para la restauración de servicios digitales esenciales.

En el contexto nacional, Santos (2024), en el trabajo “Desarrollo del plan de continuidad de negocio de acuerdo a los estándares vigentes, para el data center de la carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito”, desarrolla un Plan de Continuidad de Negocio para un centro de datos académico, considerando normas como ISO 22301, COBIT e ITIL. El proyecto incluye análisis de impacto al negocio, evaluación de riesgos, identificación de amenazas lógicas, físicas y humanas, así como planes de recuperación de desastres y contingencia. Este antecedente es pertinente porque ofrece una referencia ecuatoriana para estructurar un BCP aplicado a infraestructura tecnológica, lo cual se relaciona con los servicios digitales del GADIC SUSCAL.

A nivel local/provincial, Buscán et al. (2022), en el estudio “Modelo de plan de continuidad de negocio de las Cooperativas segmento B del cantón Cañar”, desarrollaron un modelo de Plan de Continuidad de Negocio para cooperativas de ahorro y crédito del cantón Cañar. El trabajo tuvo como propósito diseñar un modelo basado en estándares reconocidos para garantizar la continuidad de los servicios ofrecidos por estas instituciones, incluyendo el estudio teórico de normativas, el diagnóstico de la situación actual y la construcción de una herramienta preventiva para responder ante incidentes. Este antecedente es especialmente relevante para el anteproyecto, ya que se desarrolla en el contexto provincial de Cañar y ofrece una referencia cercana para aplicar la continuidad de negocio a servicios tecnológicos e institucionales.

1.3 Justificación de la investigación

Este proyecto es necesario para fortalecer la operación continua de los servicios digitales de GADIC SUSCAL. Esto se debe a que la institución ofrece servicios en línea, formularios e información procesal transparente que dependen de recursos tecnológicos para asistir a los ciudadanos. Por lo tanto, se requieren sistemas digitales ininterrumpidos para facilitar la operación continua de la gestión municipal, el servicio público y el acceso y consulta de los servicios institucionales.

Desde un punto de vista tecnológico, la integración de un plan de continuidad del negocio ayuda a una organización a estructurar procesos para identificar funciones esenciales, evaluar

riesgos, cuantificar efectos, determinar prioridades de recuperación y diseñar mecanismos de respuesta a diversos incidentes. ISO 22301 presenta una estructura para que las organizaciones reconozcan interrupciones y realicen análisis de impacto para planificar e implementar medidas para anticipar y tratar riesgos, y centrarse en la recuperación de interrupciones imprevistas, incluidos desastres naturales e incidentes cibernéticos.

El proyecto ayudará al GADIC SUSCAL mediante la provisión de una propuesta técnica que limite la necesidad de improvisar al abordar incidentes tecnológicos, mejore la gestión de la prevención de riesgos y aumente la capacidad de recuperación de los servicios digitales. Además, el estudio tendrá valor académico y metodológico porque combinará la revisión conceptual, la evaluación institucional y el diseño de un Plan de Continuidad del Negocio (PCN) basado en ISO 22301, cuya validación se realizará mediante la revisión de la propuesta por parte de los responsables del área de tecnologías de la información del GADIC SUSCAL.

1.4 Objetivos

Objetivos General

Diseñar un Plan de Continuidad de Negocio basado en la ISO 22301 para los servicios digitales del GADIC SUSCAL, mediante diagnóstico de la situación actual de los servicios digitales, el análisis de impacto al negocio y la evaluación de riesgos, y la definición de estrategias de prevención, respuesta y recuperación, con el fin de fortalecer la disponibilidad operativa y la resiliencia tecnológica institucional ante eventos disruptivos.

Objetivos Específicos

- Realizar un estudio teórico sobre continuidad de negocio, servicios digitales, riesgos tecnológicos, análisis de impacto al negocio, recuperación ante desastres y norma ISO 22301, con el fin de establecer la base conceptual y metodológica del proyecto.
- Diagnosticar la situación actual de los servicios digitales del GADIC SUSCAL, identificando activos tecnológicos, procesos críticos, amenazas, vulnerabilidades, riesgos y dependencias operativas que puedan afectar la continuidad de los servicios institucionales.

- Realizar el análisis de riesgos en base a la metodología MAGERIT y basado en la identificación de los activos del área de TICS.
- Diseñar un Plan de Continuidad de Negocio basado en la ISO 22301, incorporando estrategias de prevención, respuesta, recuperación, responsables, tiempos objetivos de recuperación y procedimientos para mantener o restablecer los servicios digitales críticos del GADIC SUSCAL.

1.5 Limitaciones

- Disponibilidad de tiempo, dado que esta investigación se realizará en un tiempo aproximado de tres meses, lo que podría limitar la profundidad del diagnóstico de los servicios digitales del GADIC SUSCAL.
- Disponibilidad de información institucional sobre incidentes tecnológicos previos, dado que la ausencia de registros formales de interrupciones podría condicionar la precisión del análisis de impacto al negocio y de la evaluación de riesgos.
- Acceso a la información institucional, ya que el análisis de activos tecnológicos, riesgos, vulnerabilidades y servicios digitales dependerá de la disponibilidad de documentación y colaboración del personal responsable.

1.6 Delimitaciones

- Este estudio se centrará en los servicios digitales del GADIC SUSCAL, delimitados al sistema de recaudación tributaria, el sistema de catastros y avalúos, el registro de la propiedad, el portal web institucional con sus formularios en línea y servicios de transparencia, y la infraestructura tecnológica que los soporta.

- El presente trabajo se limita solo a la elaboración de una propuesta de Plan de Continuidad de Negocio, cuya implementación quedará sujeta a la evaluación del GADIC SUSCAL.
- La investigación se centrará en los responsables del área de tecnologías de información y servicios digitales del GADIC SUSCAL, mas no en otras áreas administrativas que no estén directamente relacionadas con la continuidad de los servicios digitales.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Fundamentos de la continuidad de negocio

La continuidad de negocio constituye un enfoque de gestión orientado a garantizar que una organización pueda mantener o recuperar sus servicios esenciales ante eventos disruptivos. Estos eventos pueden ser de origen tecnológico, natural, humano, operativo o cibernético, y pueden afectar la disponibilidad de procesos, sistemas, infraestructura, información y servicios institucionales. En el ámbito público, la continuidad de negocio adquiere especial relevancia porque las instituciones estatales y los gobiernos locales tienen la responsabilidad de asegurar la prestación de servicios a la ciudadanía aun durante situaciones de crisis, fallas tecnológicas o interrupciones operativas. Cedergren y Hassel (2025) señalan que la gestión de continuidad de negocio ha sido adoptada progresivamente por organizaciones del sector público debido a su utilidad para sostener funciones esenciales durante crisis, aunque aún existen desafíos relacionados con liderazgo, compromiso institucional, capacitación, coordinación entre actores y restricciones de recursos.

La norma ISO 22301:2019 define los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Continuidad de Negocio. Aunque fue publicada en 2019, se justifica su uso dentro de esta investigación porque continúa siendo la norma internacional vigente y principal referencia para la implementación de sistemas de continuidad de negocio. Esta norma permite proteger a la organización frente a interrupciones, reducir la probabilidad de ocurrencia de eventos disruptivos, preparar la respuesta institucional y facilitar la recuperación cuando la interrupción se materializa (International Organization for Standardization, 2019).

En los gobiernos locales, la continuidad de negocio debe orientarse especialmente a los servicios digitales que permiten la interacción entre la institución y la ciudadanía, tales como portales institucionales, formularios en línea, normativa y gaceta digital, servicios básicos e instrumentos de planificación. La creciente dependencia de estos canales digitales para la gestión pública local convierte su disponibilidad en una condición necesaria para la prestación continua de servicios (United Nations Department of Economic and Social Affairs, 2024).

Concepto de continuidad de negocio

La continuidad de negocio puede definirse como la capacidad de una organización para continuar entregando productos y servicios dentro de niveles aceptables previamente definidos después de una interrupción. Esta definición se relaciona directamente con la capacidad institucional de anticiparse, prepararse, responder y recuperarse frente a eventos que puedan afectar sus procesos críticos. De acuerdo con ISO 22301:2019, un sistema de gestión de continuidad de negocio debe establecer políticas, objetivos, análisis, estrategias, procedimientos y mecanismos de mejora continua para asegurar que la organización pueda responder ante disrupciones (International Organization for Standardization, 2019).

En instituciones públicas, la continuidad de negocio no se limita a proteger infraestructura física o tecnológica, sino que también implica garantizar la continuidad de servicios ciudadanos, procesos administrativos, atención institucional, gestión documental y comunicación pública. Cedergren y Hassel (2025) sostienen que las organizaciones públicas cumplen un rol esencial dentro de sistemas sociales amplios, por lo que su capacidad de continuidad influye no solo en la institución, sino también en la comunidad que depende de sus servicios.

Importancia del Plan de Continuidad de Negocio en el sector público

El Plan de Continuidad de Negocio constituye un documento estructurado que define procedimientos, responsables, recursos, estrategias y acciones para mantener o recuperar servicios críticos frente a escenarios de interrupción. Su importancia radica en que permite reducir tiempos de inactividad, proteger información, coordinar respuestas institucionales, minimizar impactos operativos y mantener la confianza de la ciudadanía.

En el sector público, la continuidad de negocio tiene una función social. No se trata únicamente de mantener en funcionamiento equipos tecnológicos, sino de asegurar que los trámites, servicios, datos y canales de comunicación institucional permanezcan disponibles para la población. Hassel y Cedergren (2024) explican que la continuidad de negocio debe ampliarse hacia contextos de múltiples actores, debido a que las funciones sociales críticas dependen de redes de instituciones, proveedores, infraestructura tecnológica y usuarios finales.

La continuidad de los servicios digitales públicos también se relaciona con la transformación digital del Estado. El índice de gobierno digital de la Organización para la Cooperación y el Desarrollo Económicos destaca que el gobierno digital es esencial para transformar procesos y servicios públicos, mejorar la capacidad de respuesta y fortalecer la confiabilidad del sector público, especialmente en contextos de crisis donde los gobiernos deben continuar operando y entregar servicios oportunos a ciudadanos y empresas (OECD, 2024).

Continuidad digital y resiliencia institucional

La continuidad digital se refiere a la capacidad de mantener disponibles los servicios, sistemas, datos y plataformas digitales que soportan la gestión institucional. En gobiernos locales, esta continuidad depende de infraestructura tecnológica, conectividad, respaldos, sistemas de información, seguridad, personal técnico, proveedores, procedimientos documentados y capacidad de respuesta.

La Encuesta de Gobierno Electrónico 2024 de Naciones Unidas destaca que el fortalecimiento del gobierno electrónico local es crucial para una transformación digital integral, debido a que los gobiernos locales suelen ser el primer punto de contacto entre las personas y el Estado. Asimismo, resalta que los municipios deben contar con capacidades suficientes para entregar servicios digitales efectivos, sostenibles e inclusivos (United Nations Department of Economic and Social Affairs, 2024).

En el contexto ecuatoriano, la Política Pública para la Transformación Digital del Ecuador 2025-2030 incorpora ejes relacionados con interoperabilidad, tratamiento de datos, datos personales, datos abiertos, seguridad de la información y confianza digital. Estos elementos son coherentes con la necesidad de que los gobiernos autónomos descentralizados planifiquen la continuidad de sus servicios digitales, especialmente cuando los procesos administrativos y ciudadanos dependen cada vez más de plataformas tecnológicas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2025).

Componentes generales de un Plan de Continuidad de Negocio

Un Plan de Continuidad de Negocio debe contener componentes técnicos, organizacionales y procedimentales. ISO/TS 22332:2021 proporciona lineamientos para desarrollar y mantener planes y procedimientos de continuidad, incluyendo roles, recursos,

estrategias, procedimientos de respuesta, comunicación y mejora continua. Esta especificación técnica es aplicable a organizaciones públicas, privadas o sin fines de lucro, por lo que resulta pertinente para un GAD municipal (International Organization for Standardization, 2021b)(véase Tabla 1).

Tabla 1

Componentes generales de un Plan de Continuidad de Negocio

Componente	Descripción	Aplicación en el GADIC SUSCAL
Política de continuidad	Declaración institucional que establece el compromiso con la continuidad de servicios.	Define el compromiso del GAD con la disponibilidad de servicios digitales ciudadanos.
Alcance del BCP	Delimita procesos, servicios, sistemas y áreas incluidas.	Servicios digitales, portal web, formularios, información pública y sistemas administrativos.
Análisis de impacto al negocio	Identifica procesos críticos y consecuencias de interrupción.	Determina qué servicios digitales requieren recuperación prioritaria.
Evaluación de riesgos	Analiza amenazas, vulnerabilidades, impactos y probabilidad.	Considera fallas eléctricas, ciberataques, pérdida de datos y errores humanos.
Estrategias de continuidad	Define alternativas para mantener o recuperar servicios.	Respaldos, servicios alternos, procedimientos manuales y comunicación ciudadana.
Planes de respuesta	Establece acciones durante la interrupción.	Activación del equipo responsable y ejecución de procedimientos.
Plan de comunicación	Define mensajes, canales y responsables de comunicación.	Información a ciudadanía, autoridades y unidades internas.
Pruebas y ejercicios	Verifica la efectividad del plan.	Simulacros, pruebas de recuperación y revisión de respaldos.
Mejora continua	Actualiza el plan según hallazgos y cambios institucionales.	Ajustes periódicos conforme a infraestructura, procesos y normativa.

Nota. Elaboración propia con base en ISO 22301:2019, ISO 22313:2020 e ISO/TS 22332:2021.

2.2 Servicios digitales en gobiernos locales

Los servicios digitales públicos son aquellos procesos institucionales que utilizan tecnologías de información para entregar información, trámites, atención, formularios, consultas, documentos o mecanismos de interacción a la ciudadanía. En los gobiernos locales, estos servicios pueden incluir información institucional, pagos, trámites de agua potable, catastros,

permisos, control territorial, formularios, participación ciudadana, atención ciudadana, transparencia y gestión documental.

El Banco Mundial, mediante el GovTech Maturity Index, evalúa la madurez digital del sector público en cuatro áreas: sistemas gubernamentales centrales, prestación de servicios públicos en línea, participación ciudadana digital y habilitadores GovTech. Esta clasificación permite comprender que la continuidad de servicios digitales no es un asunto aislado del área tecnológica, sino parte de la capacidad institucional para sostener la prestación pública mediante infraestructura, datos, procesos y mecanismos digitales (World Bank, 2022).

Gobierno digital y prestación de servicios públicos

El gobierno digital implica el uso estratégico de tecnologías digitales para mejorar la prestación de servicios, fortalecer la transparencia, promover la participación ciudadana y optimizar procesos internos. La OECD (2024) sostiene que la transformación digital del sector público requiere una visión estratégica, liderazgo, coordinación y colaboración entre actores públicos y privados.

En los gobiernos autónomos descentralizados, la existencia de portales institucionales, servicios en línea, formularios, información pública y secciones de transparencia evidencia la necesidad de garantizar la continuidad digital como condición para sostener la prestación de servicios públicos y la confianza ciudadana en los canales electrónicos del Estado (World Bank, 2022).

Servicios digitales críticos en un GAD municipal

Los servicios digitales críticos son aquellos cuya interrupción afecta la atención ciudadana, la gestión administrativa, el cumplimiento legal, la transparencia o la prestación de servicios públicos. En un GAD municipal, pueden considerarse críticos los servicios relacionados con atención ciudadana, agua potable, formularios institucionales, control territorial, publicaciones oficiales, acceso a información pública, gestión documental, trámites en línea y sistemas internos de administración.

Entre los servicios municipales que habitualmente se prestan por medios digitales se encuentran los relacionados con agua potable, desarrollo y control territorial, formularios institucionales, gaceta digital, ordenanzas e instrumentos de planificación como el PDOT y el

PUGS. Estos elementos suelen formar parte del alcance de un BCP, debido a que representan canales digitales de información y gestión institucional (United Nations Department of Economic and Social Affairs, 2024).

Riesgos de interrupción en servicios digitales municipales

Los servicios digitales municipales pueden verse afectados por diferentes riesgos: fallas de energía, errores de configuración, caída de servidores, pérdida de conectividad, daños físicos, ausencia de respaldos, ciberataques, malware, ransomware, errores humanos, falta de personal especializado y dependencia de proveedores externos. En instituciones públicas, estos riesgos pueden afectar la continuidad de trámites, la disponibilidad de información y la confianza ciudadana.

El NIST Cybersecurity Framework 2.0, publicado en 2024, establece una guía para que organizaciones públicas y privadas gestionen, prioricen y comuniquen riesgos de ciberseguridad. Aunque no reemplaza a ISO 22301, complementa el enfoque de continuidad al fortalecer la gestión de riesgos tecnológicos, especialmente en servicios digitales expuestos a amenazas cibernéticas (National Institute of Standards and Technology, 2024).

2.3 Norma ISO 22301 y familia de normas de continuidad

La Norma ISO 22301:2019 constituye el estándar internacional principal para los Sistemas de Gestión de Continuidad de Negocio. Su aplicación permite que una organización establezca un sistema documentado para protegerse frente a interrupciones, responder ante incidentes, recuperar actividades críticas y mejorar continuamente sus capacidades de resiliencia. La norma es aplicable a organizaciones de cualquier tamaño, naturaleza o sector, por lo que resulta pertinente para instituciones públicas y gobiernos locales (International Organization for Standardization, 2019).

Estructura de ISO 22301:2019

ISO 22301 sigue la estructura de alto nivel utilizada por normas internacionales de sistemas de gestión. Sus componentes principales incluyen contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Esta estructura

permite integrar el sistema de continuidad con otros sistemas de gestión, como seguridad de la información o gestión de riesgos.

Tabla 2

Estructura de la norma ISO 22301:2019

Sección ISO 22301	Enfoque	Aplicación en servicios digitales
Contexto de la organización	Comprender necesidades, partes interesadas y alcance.	Identificar áreas municipales, ciudadanía, proveedores y servicios digitales críticos.
Liderazgo	Compromiso, política y responsabilidades.	Definir autoridades responsables del BCP y equipo de continuidad.
Planificación	Riesgos, oportunidades y objetivos.	Definir escenarios de interrupción y objetivos de recuperación.
Soporte	Recursos, competencias, comunicación y documentación.	Capacitar personal, documentar procedimientos y asegurar recursos tecnológicos.
Operación	BIA, evaluación de riesgos, estrategias y planes.	Desarrollar BIA, planes de recuperación y procedimientos de continuidad digital.
Evaluación del desempeño	Seguimiento, medición, auditoría y revisión.	Evaluar pruebas, indicadores, simulacros y revisiones del BCP.
Mejora	Acciones correctivas y mejora continua.	Actualizar el plan según cambios tecnológicos o incidentes reales.

Nota. Elaboración propia con base en ISO 22301:2019.

Figura 1

Ciclo de gestión de la continuidad del negocio según ISO 22301



Nota. Elaboración propia con base en International Organization for Standardization (2019).

ISO 22313:2020 como guía de aplicación

ISO 22313:2020 proporciona orientación para aplicar los requisitos de ISO 22301. Su propósito es facilitar la comprensión e implementación del Sistema de Gestión de Continuidad de Negocio mediante recomendaciones basadas en buenas prácticas internacionales. Esta norma no reemplaza a ISO 22301, sino que ayuda a interpretar sus requisitos y adaptarlos al contexto organizacional (International Organization for Standardization, 2020).

En las instituciones públicas, ISO 22313 puede orientar la implementación práctica del BCP, especialmente en aspectos como identificación de partes interesadas, análisis del contexto, definición de objetivos, selección de estrategias de continuidad, documentación de procedimientos y mejora continua.

ISO/TS 22317:2021 para el Análisis de Impacto al Negocio

ISO/TS 22317:2021 proporciona directrices para implementar y mantener un proceso formal y documentado de Análisis de Impacto al Negocio, conocido como BIA. Esta

especificación técnica no prescribe un único método, sino que permite adaptar el proceso a las necesidades, objetivos, recursos y restricciones de cada organización. Además, es aplicable a organizaciones públicas, privadas y sin fines de lucro (International Organization for Standardization, 2021a).

En el contexto de un gobierno local, el BIA permite identificar qué servicios digitales son críticos, cuánto tiempo pueden estar interrumpidos, qué recursos se requieren para recuperarlos y qué consecuencias tendría su indisponibilidad. Esto resulta fundamental para definir prioridades, objetivos de recuperación y estrategias realistas.

ISO/TS 22332:2021 para planes y procedimientos

ISO/TS 22332:2021 ofrece directrices para desarrollar y mantener planes y procedimientos de continuidad de negocio. Su utilidad radica en que orienta la definición de roles, recursos, estructura de respuesta, contenido del plan, documentación, almacenamiento, revisión y actualización (International Organization for Standardization, 2021b).

Para una institución municipal, esta especificación técnica puede apoyar la construcción de procedimientos concretos para escenarios como caída del portal web, pérdida de acceso a sistemas internos, fallas de conectividad, pérdida de datos o indisponibilidad de servicios digitales.

ISO/IEC 27031:2025 y la preparación TIC para la continuidad

ISO/IEC 27031:2025 describe conceptos y principios de preparación de las tecnologías de información y comunicación para la continuidad de negocio. Esta norma reemplaza la versión 2011 y establece un marco para mejorar la capacidad de los servicios TIC de apoyar la continuidad institucional. Su inclusión en el presente capítulo es pertinente porque el tema se enfoca en servicios digitales, los cuales dependen directamente de infraestructura tecnológica, sistemas, comunicaciones y datos (International Organization for Standardization & International Electrotechnical Commission, 2025).

La norma ISO/IEC 27031:2025 considera objetivos como RTO, RPO y MBCO dentro de la planificación de continuidad TIC, lo que permite conectar los requerimientos de continuidad institucional con la recuperación de servicios digitales (International Organization for Standardization & International Electrotechnical Commission, 2025).

2.4 Gestión de riesgos tecnológicos y ciberseguridad

La gestión de riesgos tecnológicos es el proceso mediante el cual se identifican, analizan, evalúan y tratan amenazas que pueden afectar sistemas, datos, redes, infraestructura y servicios digitales. En un BCP, esta gestión permite anticipar escenarios de interrupción y definir controles preventivos, detectivos, correctivos y de recuperación.

ISO 31000:2018 proporciona directrices para gestionar riesgos en cualquier tipo de organización. Aunque fue publicada antes del rango 2022-2026, se justifica su uso porque continúa siendo el estándar internacional base para la gestión de riesgos y sirve como complemento metodológico para ISO 22301 (International Organization for Standardization, 2018).

Riesgos tecnológicos en servicios digitales públicos

Los riesgos tecnológicos pueden surgir por causas internas o externas. Entre los más relevantes para servicios digitales públicos se encuentran fallas de servidores, pérdida de energía, interrupciones de internet, errores de configuración, accesos no autorizados, malware, ransomware, fallas de respaldo, pérdida de información, errores humanos y dependencia de proveedores.

La Contraloría General del Estado del Ecuador, mediante las Normas de Control Interno, establece criterios relacionados con la continuidad de tecnología de información, incluyendo planes de respuesta a riesgos, asignación de roles críticos, escenarios de contingencia, control de cambios, continuidad de operaciones, centros alternos y recuperación de información desde respaldos. Esta normativa es clave para justificar el desarrollo de un BCP en entidades públicas ecuatorianas (Contraloría General del Estado, 2023).

Ciberseguridad y continuidad de servicios digitales

La ciberseguridad se relaciona directamente con la continuidad de servicios digitales, debido a que un incidente de seguridad puede causar interrupciones, fuga de datos, pérdida de disponibilidad o afectación de la confianza ciudadana. ISO/IEC 27001:2022 establece requisitos para un Sistema de Gestión de Seguridad de la Información, basado en la protección de

confidencialidad, integridad y disponibilidad (International Organization for Standardization & International Electrotechnical Commission, 2022a).

NIST CSF 2.0 complementa este enfoque mediante funciones de gobernanza, identificación, protección, detección, respuesta y recuperación. Para un GAD municipal, estas funciones pueden utilizarse como referencia para fortalecer la seguridad de plataformas digitales, respaldos, accesos, sistemas de información y respuesta a incidentes (National Institute of Standards and Technology, 2024).

Activos, amenazas y vulnerabilidades

Los activos de información son recursos que tienen valor para la institución, como bases de datos, portales web, servidores, equipos de red, sistemas administrativos, documentos digitales, credenciales, respaldos y personal especializado. Las amenazas son eventos potenciales que pueden afectar estos activos, mientras que las vulnerabilidades son debilidades que podrían ser explotadas (véase Tabla 3).

Tabla 3

Activos, amenazas y vulnerabilidades en el contexto institucional

Activo	Amenaza	Vulnerabilidad asociada	Impacto posible
Portal web institucional	Caída del servicio	Hosting sin redundancia o mantenimiento insuficiente	Pérdida de acceso ciudadano a información pública.
Base de datos municipal	Pérdida o corrupción de datos	Respaldos incompletos o no probados	Afectación de trámites y registros administrativos.
Red institucional	Interrupción de conectividad	Dependencia de un solo proveedor	Indisponibilidad de sistemas internos y atención digital.
Equipos de usuario	Malware o ransomware	Falta de actualización o capacitación	Pérdida de información y propagación de incidentes.
Credenciales de acceso	Acceso no autorizado	Contraseñas débiles o sin doble factor	Exposición o modificación indebida de información.
Personal técnico	Ausencia o rotación	Dependencia de conocimiento individual	Dificultad para recuperar servicios.

Nota. Elaboración propia con base en ISO/IEC 27001:2022, NIST CSF 2.0 e ISO 22301:2019.

2.5 Análisis de Impacto al Negocio

El Análisis de Impacto al Negocio, conocido como BIA, es una actividad fundamental dentro de la continuidad de negocio. Su objetivo es identificar procesos, servicios, recursos y dependencias críticas, evaluando las consecuencias de una interrupción sobre la organización. ISO/TS 22317:2021 establece directrices para implementar un BIA documentado y adaptable al tipo, tamaño y naturaleza de la organización (International Organization for Standardization, 2021a).

En un gobierno local, el BIA permite determinar qué servicios digitales deben recuperarse primero, qué impactos tendría su interrupción y qué recursos son necesarios para restablecerlos. Además, permite establecer parámetros como el tiempo máximo tolerable de interrupción, el objetivo de tiempo de recuperación y el objetivo de punto de recuperación.

Objetivos del BIA

El BIA tiene como objetivos principales identificar servicios críticos, estimar impactos, priorizar actividades, reconocer dependencias y definir requerimientos de recuperación. En una institución pública, los impactos no deben evaluarse solo desde una perspectiva económica, sino también desde dimensiones operativas, legales, reputacionales, sociales y de atención ciudadana (véase Tabla 4).

Tabla 4

Objetivos del Análisis de Impacto al Negocio

Categoría de impacto	Descripción	Ejemplo en servicios digitales
Operativo	Afectación a procesos internos o atención ciudadana.	Interrupción del portal o formularios digitales.
Legal o normativo	Incumplimiento de obligaciones de transparencia o protección de datos.	No disponibilidad de información pública o pérdida de datos personales.
Reputacional	Pérdida de confianza ciudadana.	Reclamos por falta de atención o información.
Social	Afectación al acceso ciudadano a servicios municipales.	Imposibilidad de consultar trámites o información de servicios.
Tecnológico	Indisponibilidad de sistemas, datos o infraestructura.	Caída de servidores, fallas de conectividad o pérdida de respaldos.

Nota. Elaboración propia con base en ISO/TS 22317:2021.

RTO, RPO, MTPD y MBCO

Los parámetros de recuperación permiten definir objetivos claros dentro del BCP. El RTO, u Objetivo de Tiempo de Recuperación, indica el tiempo máximo en que un servicio debe ser restablecido. El RPO, u Objetivo de Punto de Recuperación, indica la cantidad máxima aceptable de pérdida de datos medida en tiempo. El MTPD, o periodo máximo tolerable de interrupción, representa el límite máximo de tiempo antes de que la interrupción genere consecuencias inaceptables. ISO/IEC 27031:2025 también incorpora el concepto de MBCO, u objetivo mínimo de continuidad de negocio, relacionado con el nivel mínimo aceptable de operación durante una interrupción (International Organization for Standardization & International Electrotechnical Commission, 2025).

Figura 2

Relación temporal entre RPO, RTO, MTPD y MBCO



Nota. Elaboración propia con base en International Organization for Standardization (2022a) e International Organization for Standardization e International Electrotechnical Commission (2025).

Dependencias críticas

Las dependencias críticas son recursos internos o externos necesarios para mantener o recuperar un servicio. En servicios digitales municipales, estas dependencias pueden incluir

energía eléctrica, internet, servidores, hosting, bases de datos, proveedores tecnológicos, personal de TI, sistemas de respaldo, equipos de comunicación y documentación técnica.

El enfoque multi-actor de la continuidad de negocio destaca que la recuperación de servicios esenciales no depende de una sola organización, sino de redes de actores interdependientes. Hassel y Cedergren (2024) resaltan que los servicios críticos actuales requieren considerar proveedores, usuarios, infraestructura compartida y coordinación interinstitucional.

2.6 Estrategias de continuidad y recuperación

Las estrategias de continuidad son alternativas planificadas para mantener o recuperar servicios críticos frente a escenarios de interrupción. Estas estrategias deben responder a los resultados del análisis de impacto al negocio y de la evaluación de riesgos, con el propósito de definir acciones, procedimientos y recursos que permitan sostener o restablecer las operaciones esenciales. En este sentido, ISO/TS 22332:2021 establece directrices para desarrollar y mantener planes y procedimientos de continuidad del negocio, orientados a responder de manera estructurada ante eventos disruptivos y apoyar la recuperación de las actividades críticas (International Organization for Standardization, 2021b).

Estrategias tecnológicas

Las estrategias tecnológicas pueden incluir respaldos periódicos, redundancia de servidores, alojamiento alternativo, servicios en la nube, enlaces de internet secundarios, protección eléctrica, restauración de bases de datos, control de cambios, mantenimiento preventivo y monitoreo de disponibilidad.

En gobiernos locales de tamaño reducido, estas estrategias deben adaptarse a los recursos y capacidades institucionales. No sería realista proponer infraestructuras de alta complejidad si el presupuesto o personal técnico son limitados; por ello, el plan debe priorizar soluciones viables, como respaldo documentado, pruebas de recuperación, acuerdos con proveedores, procedimientos manuales temporales y comunicación institucional clara.

Estrategias organizacionales

Las estrategias organizacionales incluyen conformación del equipo de continuidad, definición de roles, responsables de activación, autoridades de decisión, cadena de comunicación, capacitación y procedimientos de escalamiento. ISO/TS 22332:2021 señala que la alta dirección debe asignar una persona con autoridad adecuada para liderar el desarrollo de planes y procedimientos de continuidad, además de asegurar competencias y recursos (International Organization for Standardization, 2021b).

Comunicación durante interrupciones

La comunicación durante una interrupción es fundamental para evitar desinformación, reclamos innecesarios y pérdida de confianza. El plan debe establecer mensajes, responsables, canales, tiempos y públicos objetivos. Entre los canales posibles se encuentran sitio web, redes sociales institucionales, correo electrónico, teléfonos de atención, comunicados internos y avisos físicos si fuera necesario.

2.7 Pruebas, ejercicios y mejora continua

Un BCP no debe considerarse válido únicamente por estar escrito. Debe ser probado, actualizado y mejorado. Las pruebas permiten verificar si los procedimientos funcionan, si los responsables conocen sus roles, si los respaldos pueden restaurarse, si los canales de comunicación son adecuados y si los tiempos definidos son realistas.

ISO/TS 22332:2021 establece que los planes de continuidad deben mantenerse listos y mejorarse mediante pruebas regulares. Asimismo, las Normas de Control Interno de la Contraloría General del Estado ecuatoriana señalan que el plan de continuidad de tecnología de información debe mantenerse actualizado mediante procedimientos de control de cambios y reflejar permanentemente los requerimientos actuales de la organización (Contraloría General del Estado, 2023).

Tipos de pruebas del BCP

Las pruebas pueden incluir revisión documental, simulacros de escritorio, pruebas técnicas de restauración, pruebas de comunicación, pruebas de respaldo, pruebas de recuperación

de sistemas y ejercicios integrales. Cada prueba debe documentarse y generar hallazgos, responsables y acciones correctivas (véase Tabla 5).

Tabla 5

Tipos de pruebas del Plan de Continuidad de Negocio

Tipo de prueba	Objetivo	Resultado esperado
Revisión documental	Verificar que el plan esté actualizado y completo.	Versión vigente del BCP validada.
Simulacro de escritorio	Evaluar toma de decisiones y roles.	Identificación de vacíos en coordinación.
Prueba de respaldo	Confirmar que los datos pueden recuperarse.	Evidencia de restauración exitosa.
Prueba de comunicación	Validar canales y mensajes.	Comunicación oportuna a usuarios internos y ciudadanía.
Prueba técnica	Recuperar un servicio o sistema específico.	Medición real de RTO y RPO.
Ejercicio integral	Evaluar respuesta completa ante un escenario.	Informe de lecciones aprendidas y acciones de mejora.

Nota. Elaboración propia con base en ISO/TS 22332:2021 y Normas de Control Interno de la Contraloría General del Estado.

Mejora continua

La mejora continua permite que el BCP evolucione conforme cambian los servicios digitales, la infraestructura, el personal, los riesgos y la normativa. Cedergren y Hassel (2025) sostienen que las organizaciones públicas no solo deben anticipar amenazas previsibles, sino también desarrollar capacidad adaptativa ante crisis no previstas. Esto implica que el BCP debe combinar planificación formal con flexibilidad operativa.

2.8 Normativa ecuatoriana aplicable

La construcción de un Plan de Continuidad de Negocio para servicios digitales municipales debe considerar el marco normativo ecuatoriano. Este marco no reemplaza a ISO 22301, pero define obligaciones relacionadas con gestión pública, protección de datos, control interno y prestación de servicios ciudadanos.

Gobiernos Autónomos Descentralizados

El Código Orgánico de Organización Territorial, Autonomía y Descentralización regula la organización, competencias y funciones de los gobiernos autónomos descentralizados. Aunque se trata de una norma anterior al periodo 2022–2026, se justifica su uso porque continúa siendo el marco legal base de los GAD en Ecuador. En el contexto del BCP, su relevancia radica en que los gobiernos locales deben garantizar la prestación de servicios públicos dentro de sus competencias, por lo que resulta necesario fortalecer sus capacidades institucionales, operativas y de gestión para asegurar la continuidad de los servicios ante escenarios de interrupción (Consejo Nacional de Competencias, 2025).

Protección de datos personales

La Ley Orgánica de Protección de Datos Personales del Ecuador regula el tratamiento de datos personales dentro del territorio nacional y establece obligaciones para responsables y encargados del tratamiento. En servicios digitales municipales, esta ley es relevante porque los trámites, formularios, registros y sistemas pueden contener información personal de ciudadanos (Asamblea Nacional del Ecuador, 2021).

Por ello, el BCP debe contemplar mecanismos para proteger datos personales durante interrupciones, restauraciones, respaldos, accesos de emergencia y recuperación de sistemas. Una recuperación mal ejecutada puede restablecer el servicio, pero también exponer información sensible, por lo que la continuidad debe coordinarse con la seguridad de la información.

Normas de Control Interno

Las Normas de Control Interno de la Contraloría General del Estado establecen lineamientos para la gestión pública ecuatoriana. En materia de tecnología de información, estas normas incluyen elementos de continuidad operativa, respuesta a riesgos, control de cambios, recuperación de información y planes de recuperación de desastres. Por tanto, constituyen un soporte normativo directo para justificar un BCP en las entidades publicas ecuatorianas (Contraloría General del Estado, 2023).

2.9 Comparación de normas y marcos aplicables

Con el propósito de seleccionar los referentes más adecuados para la elaboración del Plan de Continuidad de Negocio, se presenta una comparación de normas y marcos aplicables (véase Tabla 6).

Tabla 6

Comparación de normas y marcos de referencia aplicables

Norma / Marco	Enfoque	Aporte al BCP	Ventajas / Limitaciones	Aplicabilidad al GADIC SUSCAL
ISO 22301:2019	Sistema de Gestión de Continuidad de Negocio.	Define requisitos para implementar, mantener y mejorar un BCMS.	Norma certificable y reconocida internacionalmente ; requiere adaptación al tamaño institucional.	Muy alta, eje central del plan.
ISO 22313:2020	Guía de aplicación de ISO 22301.	Orienta la interpretación práctica de requisitos.	Facilita la implementación; no es certificable.	Alta, como guía metodológica.
ISO/TS 22317:2021	Análisis de Impacto al Negocio.	Define directrices para realizar BIA.	Permite identificar servicios críticos; no prescribe un método único.	Muy alta, para priorizar servicios digitales.
ISO/TS 22332:2021	Planes y procedimientos de continuidad.	Orienta la construcción de planes documentados.	Útil para definir roles, recursos y procedimientos; requiere información interna.	Muy alta, para estructurar el BCP.
ISO/IEC 27031:2025	Preparación TIC para continuidad.	Conecta continuidad institucional con servicios TIC.	Actual y específica para continuidad digital; requiere capacidad técnica.	Muy alta, por el enfoque en servicios digitales.
ISO/IEC 27001:2022	Seguridad de la información.	Protege confidencialidad, integridad y disponibilidad.	Norma vigente y certificable; su alcance es seguridad, no continuidad total.	Alta, como complemento de seguridad.
NIST CSF 2.0	Ciberseguridad.	Gestiona riesgos, respuesta y recuperación.	Actual, flexible y aplicable al sector público; no es certificable ISO.	Media-alta, como complemento.
Normas de Control Interno Ecuador	Control institucional público.	Exigen continuidad TI, recuperación y control de cambios.	Aplicación directa en entidades públicas ecuatorianas; no desarrollan una metodología BCP completa.	Muy alta, por obligatoriedad pública.

Nota. Elaboración propia con base en ISO 22301:2019, ISO 22313:2020, ISO/TS 22317:2021, ISO/TS 22332:2021, ISO/IEC 27031:2025, ISO/IEC 27001:2022, NIST CSF 2.0 y Normas de Control Interno.

En función del análisis comparativo, se determina que ISO 22301:2019 debe ser el marco principal para el diseño del Plan de Continuidad de Negocio del GADIC SUSCAL, debido a que establece los requisitos formales de un sistema de continuidad. Sin embargo, su aplicación debe complementarse con ISO/TS 22317:2021 para el BIA, ISO/TS 22332:2021 para la construcción de procedimientos, ISO/IEC 27031:2025 para continuidad TIC, ISO/IEC 27001:2022 para seguridad de la información y las Normas de Control Interno ecuatorianas para adecuación al sector público nacional.

CAPÍTULO III

3 MARCO METODOLÓGICO

3.1 Enfoque de la Investigación

La presente investigación adopta un enfoque cualitativo, desarrollado bajo el diseño de estudio de caso único de carácter instrumental, en el que la unidad de análisis es el Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal (GADIC SUSCAL) y, de manera específica, el estado de sus controles de seguridad de la información y de sus activos tecnológicos. Este diseño resulta pertinente porque el objeto de estudio no son percepciones individuales susceptibles de agregación estadística, sino condiciones institucionales verificables mediante evidencia documental y técnica.

El componente cualitativo se sustenta en la revisión de la documentación institucional del área de Tecnologías de la Información y Comunicación inventario de bienes informáticos, descripción de la infraestructura tecnológica y documentación de configuración, complementada con la verificación técnica realizada junto al responsable del área, quien actúa como fuente acreditada de comprobación y no como sujeto muestral.

La investigación incorpora además una cuantificación descriptiva de carácter censal, sin pretensión inferencial. Esta cuantificación se aplica sobre dos conjuntos completos: los 66 controles de seguridad derivados de la norma ISO/IEC 27002, verificados uno a uno mediante una escala ordinal de tres valores (Sí, No, En proceso), y los 36 activos tecnológicos inventariados, valorados en las cinco dimensiones de seguridad definidas por la metodología MAGERIT en una escala de 0 a 10. Al tratarse de la totalidad de los elementos que componen ambos conjuntos, y no de una muestra extraída de ellos, los porcentajes e índices obtenidos describen el estado real del caso estudiado y no constituyen estimaciones sujetas a error muestral ni a pruebas de significancia estadística.

3.2 Nivel de la Investigación

El estudio se desarrolla en un nivel descriptivo con orientación diagnóstica, coherente con el diseño de estudio de caso adoptado. Es descriptivo porque caracteriza el estado actual de

la seguridad de la información, de los activos tecnológicos y de la capacidad de continuidad de los servicios digitales del GADIC SUSCAL, observando la realidad institucional tal como se presenta y sin manipular variables ni establecer relaciones causales entre ellas.

Su orientación diagnóstica se expresa en el propósito de identificar fortalezas y brechas que fundamenten decisiones posteriores: los resultados constituyen la línea base sobre la cual se construye la propuesta de Plan de Continuidad de Negocio basado en la norma ISO 22301. Congruentemente con este nivel, no se formulan hipótesis ni se aplican pruebas estadísticas inferenciales, por cuanto el propósito del estudio es caracterizar un caso institucional determinado y no contrastar supuestos sobre una población mayor.

3.3 Unidad de Análisis y Fuentes de Información

La unidad de análisis de la investigación es el GADIC SUSCAL, y dentro de él, el área de Tecnologías de la Información y Comunicación, responsable de administrar la plataforma tecnológica institucional y los servicios digitales delimitados en el Capítulo I.

El universo de elementos examinados está conformado por dos conjuntos finitos y plenamente identificables: los 66 controles de seguridad agrupados en los 12 dominios de la norma ISO/IEC 27002, y los 36 activos tecnológicos registrados en el inventario institucional de bienes informáticos. En ambos casos se trabajó con la totalidad de los elementos, por lo que el procedimiento corresponde a un censo documental y no a un muestreo; en consecuencia, no se aplican criterios de representatividad muestral ni cálculos de error de estimación.

Las fuentes de información fueron dos y operan de manera complementaria. La primera es la documentación institucional del área de TIC, que constituye la evidencia primaria del estudio. La segunda es el responsable del área de TIC, quien participó en calidad de fuente técnica de verificación: su función fue acreditar el estado de implantación de cada control y confirmar los datos del inventario, no emitir valoraciones subjetivas destinadas a un tratamiento estadístico. Esta condición se sustenta en que el GADIC SUSCAL cuenta con una única área de TIC y en que dicho servidor es el único funcionario con conocimiento técnico integral de la infraestructura, los sistemas de información y las prácticas de operación institucionales.

La verificación se realizó el 21 de julio de 2026, conforme consta en el instrumento institucional con código A001, versión 01. Se reconoce como limitación la dependencia de una fuente técnica única, riesgo que fue mitigado mediante la triangulación de cada respuesta con la evidencia documental disponible. Asimismo, al tratarse de un estudio de caso único, los hallazgos deben interpretarse como un diagnóstico específico del GADIC SUSCAL y no como generalizaciones aplicables a otros gobiernos autónomos descentralizados.

3.4 Técnicas e Instrumentos de Recolección

La recolección de información combinó tres técnicas complementarias, cada una asociada a un marco normativo distinto y a una función específica dentro del diseño del Plan de Continuidad de Negocio. Conviene precisar desde el inicio que la norma rectora del presente trabajo es la ISO 22301:2019, y que ninguno de los instrumentos aplicados en este capítulo pretende sustituirla: su función es proveer los insumos de contexto y de inventario que la propia norma exige como punto de partida.

En efecto, la cláusula 4 de la ISO 22301:2019 establece que la organización debe comprender su contexto interno y externo, así como las necesidades y expectativas de las partes interesadas, antes de definir cualquier estrategia de continuidad. Los instrumentos de este capítulo responden precisamente a ese requisito: la lista de verificación basada en ISO/IEC 27002 caracteriza la línea base de seguridad sobre la que operan los servicios digitales; la revisión documental describe la plataforma tecnológica institucional; y el inventario MAGERIT identifica y valora los activos que sostienen dichos servicios. Los instrumentos propiamente orientados a la continuidad el Análisis de Impacto al Negocio conforme a ISO/TS 22317:2021 y la definición de estrategias conforme a ISO/TS 22332:2021 se aplican en el Capítulo IV, según la secuencia establecida en la Tabla 12.

Lista de verificación de la línea base de seguridad (ISO/IEC 27002)

El instrumento principal es una lista de verificación de cumplimiento conformada por 66 ítems de comprobación, agrupados en 12 dominios de control derivados de la norma ISO/IEC 27002: políticas de seguridad, aspectos organizativos, seguridad ligada a los recursos humanos, gestión de activos, control de accesos, seguridad física y ambiental, seguridad en la operativa, seguridad en las telecomunicaciones, gestión de incidentes, continuidad de las actividades

institucionales, adquisición, desarrollo y mantenimiento de sistemas, y cumplimiento. Cabe precisar que la edición 2013 de la norma organiza los controles en catorce dominios; para efectos del presente diagnóstico se consolidaron en doce, integrando los controles criptográficos dentro del dominio de control de accesos y los relativos a las relaciones con proveedores dentro de los aspectos organizativos, por corresponder en ambos casos a prácticas que la institución gestiona de forma conjunta. Esta agrupación no suprime ningún control verificado y se declara expresamente para efectos de trazabilidad.

Cada ítem se verifica en una escala ordinal de tres valores: Sí, cuando existe evidencia de que el control está implantado; No, cuando el control no existe; y En proceso, cuando se encuentra en implementación parcial. A diferencia de una encuesta de opinión, el instrumento no registra percepciones sino la constatación del estado de cada control, contrastada con la documentación institucional. Su aplicación permite calcular el índice de cumplimiento por dominio y el índice de cumplimiento global de la institución, entendidos como medidas descriptivas del caso estudiado.

Es necesario delimitar con precisión el alcance de este instrumento. La ISO/IEC 27002 no es una norma de continuidad de negocio y no se emplea aquí como tal: su aplicación se limita a establecer la línea base de seguridad de la información del GADIC SUSCAL, dado que los servicios digitales cuya continuidad se busca garantizar operan sobre esa base de controles. La relación entre ambas normas no es, sin embargo, meramente contextual. La propia ISO/IEC 27002 incorpora un dominio dedicado a los aspectos de seguridad de la información en la gestión de la continuidad del negocio, que en la edición 2022 se expresa en los controles 5.29, sobre seguridad de la información durante una disrupción, y 5.30, sobre preparación de las TIC para la continuidad del negocio. Ese dominio es, precisamente, uno de los que registra menor cumplimiento en el diagnóstico, hallazgo que constituye evidencia directa de la carencia que motiva la presente investigación.

El puente normativo entre la seguridad de la información y la continuidad operativa lo aporta la ISO/IEC 27031, analizada en el Capítulo II, la cual establece los requisitos de preparación de las tecnologías de la información y comunicación para la continuidad del negocio y articula los controles de la ISO/IEC 27002 con el sistema de gestión definido por la ISO 22301. En consecuencia, el diagnóstico de seguridad no fundamenta por sí solo el Plan de Continuidad

de Negocio: lo antecede y lo condiciona, aportando el estado de los controles sobre los cuales deberán apoyarse las estrategias de continuidad formuladas en el Capítulo IV.

Revisión documental

La revisión documental abarcó el inventario institucional de bienes informáticos y la documentación técnica de la infraestructura del GADIC SUSCAL, que incluye la segmentación de la red interna en 12 VLAN, los servidores físicos HPE, la plataforma de virtualización VMware, el almacenamiento en red NAS Synology, el firewall perimetral y el software institucional licenciado. Esta técnica proporcionó la evidencia necesaria para consolidar el inventario de activos y contrastar los resultados de la lista de verificación con la realidad documentada de la plataforma tecnológica.

Inventario y valoración de activos con MAGERIT

Para el levantamiento de activos se utilizó la metodología MAGERIT versión 3, desarrollada por la administración pública española y ampliamente aplicada en el análisis y gestión de riesgos de los sistemas de información. A partir del catálogo de elementos del Libro II de la metodología, cada activo identificado en la documentación institucional fue codificado dentro de una de las diez categorías del catálogo y valorado en cinco dimensiones de seguridad: disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), en una escala de 0 a 10. El valor global de cada activo corresponde a la dimensión con mayor puntuación, criterio que evita subestimar activos cuyo riesgo se concentra en una sola dimensión.

Articulación de los instrumentos con la norma ISO 22301

Los tres instrumentos descritos se articulan de manera secuencial con los requisitos de la norma rectora. La lista de verificación ISO/IEC 27002 y la revisión documental responden a la cláusula 4 de la ISO 22301:2019, referida a la comprensión de la organización y de su contexto. El inventario y la valoración de activos mediante MAGERIT proveen la información requerida por la cláusula 8.2, relativa al análisis de impacto en el negocio y a la apreciación del riesgo, al identificar los recursos que sostienen los servicios digitales y su criticidad relativa. Sobre esa base, las cláusulas 8.3 a 8.5 estrategias y soluciones de continuidad, planes y procedimientos, y programa de ejercicios se desarrollan en el Capítulo IV con el apoyo de las especificaciones técnicas ISO/TS 22317:2021 e ISO/TS 22332:2021.

De este modo, ninguno de los instrumentos aplicados en el presente capítulo pretende medir por sí mismo la capacidad de continuidad de la institución, sino documentar las condiciones de partida exigidas por la ISO 22301 para el diseño del plan. La medición de la continuidad propiamente dicha, expresada en los parámetros de tiempo objetivo de recuperación (RTO), punto objetivo de recuperación (RPO) y período máximo tolerable de disrupción (MTPD), corresponde al Análisis de Impacto al Negocio desarrollado en el Capítulo IV.

Conviene precisar el alcance respectivo de cada instrumento respecto de los objetivos específicos de la investigación, por cuanto miden objetos distintos y no son intercambiables. La lista de verificación basada en ISO/IEC 27002 mide el grado de implantación de los controles de seguridad y responde al segundo objetivo específico, referido al diagnóstico de la situación actual; su producto es el nivel de cumplimiento por dominio. El inventario y la valoración de activos, junto con el análisis de riesgos desarrollado en la sección 3.8, aplican la metodología MAGERIT versión 3 sobre los activos del área de Tecnologías de la Información y Comunicación y responden al tercer objetivo específico; su producto es la matriz de riesgos con la estimación de probabilidad, impacto y nivel de exposición por activo crítico. En consecuencia, el diagnóstico del presente capítulo no se sustenta en un único instrumento: la verificación de controles establece la línea base sobre la que operan los servicios, mientras que el análisis de riesgos determina la exposición de los activos que los soportan, y ambos resultados se triangulan para fundamentar la propuesta del Capítulo IV.

3.5 Tratamiento de la Información

Los resultados de la lista de verificación fueron tabulados en una hoja de cálculo para obtener frecuencias absolutas y el índice de cumplimiento por dominio y a nivel global. Dado el carácter ordinal de la escala empleada, el tratamiento se limita a frecuencias y porcentajes, únicos estadísticos descriptivos admisibles para este nivel de medición; no se calculan medias, desviaciones ni pruebas de contraste, por no corresponder al diseño de la investigación. El índice de cumplimiento se calculó mediante la siguiente fórmula:

Cumplimiento (%) = (N.º de controles con respuesta “Sí” ÷ N.º total de controles del dominio) × 100

Se adoptó deliberadamente un criterio conservador: únicamente los controles plenamente implantados computan en el índice, mientras que los clasificados como En proceso se reportan por separado como indicador de avance parcial, sin acreditarse como cumplimiento. Este criterio evita sobrestimar la madurez institucional y resulta coherente con el propósito del estudio, que es identificar brechas de continuidad antes que exhibir niveles de conformidad.

El inventario de activos se consolidó en una matriz MAGERIT que registra el código, la categoría, el tipo, la descripción, la cantidad, el responsable, la ubicación y la valoración por dimensiones de cada activo. El valor global de cada activo se obtiene como el máximo de las cinco dimensiones valoradas, criterio que responde a la lógica de la propia metodología: la afectación de una sola dimensión basta para comprometer el activo, por lo que promediar los valores diluiría el riesgo real. Sobre esta matriz se estableció como criterio de criticidad un valor global igual o superior a 9, umbral que delimita el subconjunto de activos que recibirá tratamiento prioritario en el análisis de riesgos y en el Análisis de Impacto al Negocio del Capítulo IV. Finalmente, los resultados de la lista de verificación y del inventario fueron triangulados entre sí y con la documentación institucional, a fin de verificar su coherencia y compensar la dependencia de una fuente técnica única.

3.6 Análisis e Interpretación de Resultados del Diagnóstico

La Tabla 7 resume los resultados de la verificación de controles por dominio. De los 66 controles examinados, 40 se encuentran implantados (60,6%), 16 están en proceso de implementación (24,2%) y 10 no existen (15,2%). Los valores corresponden a la totalidad de los controles evaluados y describen el estado del caso institucional analizado.

Tabla 7

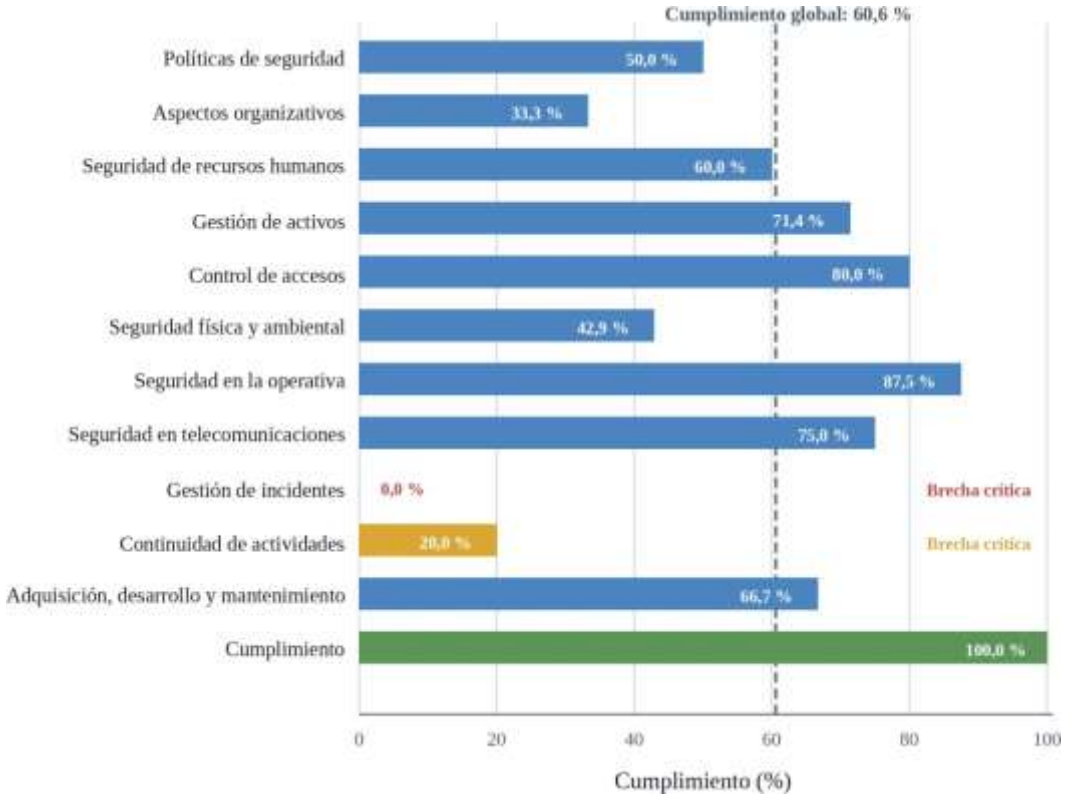
Resultados de la lista de verificación por dominio de control ISO/IEC 27002

Dominio de control	Preguntas	Sí	No	En proceso	Cumplimiento (%)
Políticas de la seguridad	4	2	1	1	50,0
Aspectos organizativos de la seguridad	6	2	1	3	33,3
Seguridad ligada a los recursos humanos	5	3	0	2	60,0
Gestión de activos	7	5	1	1	71,4
Control de accesos	10	8	0	2	80,0
Seguridad física y ambiental	7	3	2	2	42,9
Seguridad en la operativa	8	7	0	1	87,5
Seguridad en las telecomunicaciones	4	3	1	0	75,0
Gestión de incidentes de seguridad	3	0	1	2	0,0
Continuidad de las actividades institucionales	5	1	3	1	20,0
Adquisición, desarrollo y mantenimiento de sistemas	3	2	0	1	66,7
Cumplimiento	4	4	0	0	100,0
Total	66	40	10	16	60,6

Nota. Elaboración propia a partir de la verificación de controles realizada en el GADIC SUSCAL (2026).

Figura 3

Nivel de cumplimiento por dominio de control ISO/IEC 27002



Nota. Elaboración propia con base en la verificación de controles realizada en el GADIC SUSCAL (2026).

Fortalezas identificadas

Los dominios con mayor nivel de implantación son cumplimiento (100%), seguridad en la operativa (87,5%) y control de accesos (80%). La institución gestiona la legalidad de sus licencias, protege los datos personales y cumple la normativa de archivo y firma electrónica; ejecuta respaldos conforme a una política definida, verifica que sean restaurables y los almacena en una ubicación distinta de la información principal; además, mantiene la red segmentada, monitorea usos irregulares y controla las conexiones remotas. Estas capacidades constituyen una base operativa favorable sobre la cual puede apoyarse el Plan de Continuidad de Negocio.

Brechas críticas identificadas

Las debilidades se concentran precisamente en los dominios que sustentan la continuidad. En gestión de incidentes de seguridad ninguna pregunta obtuvo respuesta afirmativa: las debilidades no están documentadas, los eventos no se registran formalmente y no existen procedimientos para preservar evidencias. En continuidad de las actividades institucionales el cumplimiento alcanza apenas el 20%: el municipio no dispone de un Plan de Continuidad del Negocio formalmente aprobado, no ha efectuado un Análisis de Impacto al Negocio que determine tiempos y puntos objetivo de recuperación, y no ha conformado un equipo de continuidad con roles y suplentes definidos; la única capacidad instalada es la disponibilidad de equipamiento de reemplazo.

A estas carencias se suma la seguridad física y ambiental (42,9%), donde el área que aloja los servidores carece de protección específica frente a incendios e inundaciones y el municipio no está preparado para atender oportunamente una falla del cableado estructurado o del backbone de datos. El dominio de aspectos organizativos registra el segundo nivel más bajo del diagnóstico (33,3%): no existe un comité o instancia colegiada de seguridad de la información, no se practican auditorías independientes sobre la implantación de las políticas y la definición de propietarios y custodios de los activos se encuentra en proceso, por cuanto alcanza al equipamiento inventariable pero no a los activos de naturaleza lógica. Esta última carencia se confirma en el levantamiento de la sección 3.7, donde once de los quince activos calificados como críticos entre ellos el servidor de base de datos, el firewall y los respaldos no registran un responsable formalmente designado en la documentación institucional. El dominio de políticas de seguridad, por su parte, alcanza el 50% y evidencia la ausencia de revisión periódica de la política institucional. En conjunto, el diagnóstico confirma el problema formulado en el Capítulo I: la institución posee controles operativos aceptables, pero carece del componente formal de continuidad, lo que valida la pertinencia de diseñar el plan propuesto.

3.7 Levantamiento y Valoración de Activos del Área de TIC

A partir de la revisión documental se consolidó un inventario de 36 activos tecnológicos, distribuidos en las diez categorías del catálogo MAGERIT, tal como se presenta en la Tabla 8.

La mayor concentración corresponde al equipamiento informático, seguido del software institucional y de las redes de comunicaciones.

Tabla 8

Distribución del inventario de activos por categoría MAGERIT

Código	Categoría	N.º de activos	Ejemplos identificados
[D]	Datos / Información	3	Respaldos de la base de datos, configuración de red
[K]	Claves criptográficas	1	Certificado SSL Wildcard
[S]	Servicios	1	Páginas web institucionales
[SW]	Software	6	Servidores de aplicaciones y de base de datos, VMware
[HW]	Equipamiento informático	12	Servidores HPE, NAS Synology, switches Cisco, firewall
[COM]	Redes de comunicaciones	4	Red interna (12 VLAN), enlace WAN de Internet
[Media]	Soportes de información	3	Discos duros, discos virtuales, almacenamiento NAS
[AUX]	Equipamiento auxiliar	3	UPS, reguladores de voltaje, racks
[L]	Instalaciones	2	Edificio municipal, centro prioritario
[P]	Personal	1	Funcionarios responsables de los bienes informáticos
Total		36	

Nota. Elaboración propia a partir de la matriz MAGERIT del GADIC SUSCAL (2026).

Cada activo fue valorado en las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Aplicando el criterio de criticidad definido en el tratamiento de la información, 15 activos alcanzan un valor global igual o superior a 9 y conforman el subconjunto crítico que se muestra en la Tabla 9.

Tabla 9

Activos críticos del GADIC SUSCAL (valor global igual o superior a 9)

Código	Activo	D	I	C	A	T	Valor global
ACT-D-01	Respaldos de la base de datos	9	9	8	7	7	9
ACT-D-02	Datos de configuración de red	8	9	8	8	8	9
ACT-K-01	Certificado SSL Wildcard	7	9	8	10	8	10
ACT-S-01	Páginas web	8	8	6	9	7	9
ACT-SW-01	Software y licencias adquiridas	7	9	8	8	8	9
ACT-SW-02	Servidor de aplicaciones	8	9	8	8	8	9
ACT-SW-03	Servidor de base de datos	9	10	9	8	8	10
ACT-SW-06	VMware	9	9	8	8	7	9
ACT-HW-01	Servidores HPE	9	9	8	8	7	9
ACT-HW-02	Máquinas virtuales VMware	9	9	8	8	7	9
ACT-HW-03	Servidor NAS Synology RS1221RP	8	9	8	7	7	9
ACT-HW-09	Switches Cisco	9	8	6	6	6	9
ACT-HW-10	Firewall	9	9	9	9	9	9
ACT-COM-01	Red interna (12 VLAN)	9	8	7	6	6	9
ACT-COM-04	Enlace WAN de Internet (CNT)	9	7	6	7	7	9

Nota. Elaboración propia a partir de la matriz MAGERIT del GADIC SUSCAL (2026).

La criticidad se concentra en tres capas de la plataforma institucional: la capa de datos y respaldo, encabezada por el servidor de base de datos y sus copias de seguridad; la capa de procesamiento, integrada por los servidores físicos HPE, la plataforma de virtualización VMware y el servidor de aplicaciones; y el núcleo de comunicaciones, formado por el firewall, los switches, la red interna de 12 VLAN y el enlace WAN. El certificado SSL Wildcard y el servidor de base de datos alcanzan la valoración máxima de 10, el primero por su papel en la autenticidad de los servicios web y el segundo por sostener la integridad de la información institucional. Cabe precisar que las valoraciones registradas tienen carácter preliminar y deberán validarse con el propietario de cada activo durante el desarrollo de la propuesta.

3.8 Análisis de Riesgos de los Activos Críticos según MAGERIT

Con el inventario ya valorado, corresponde completar el ciclo de la metodología MAGERIT mediante el análisis de riesgos, etapa con la que se da cumplimiento al tercer objetivo específico de la investigación. El análisis se aplicó sobre los 15 activos que alcanzaron

un valor global igual o superior a 9, siguiendo las etapas establecidas en el Capítulo I de la metodología: identificación de amenazas por activo a partir del catálogo del Capítulo II, estimación de la probabilidad de materialización, estimación del impacto sobre la dimensión de seguridad afectada y cálculo del riesgo resultante.

Escalas de valoración

Para asegurar la trazabilidad del cálculo se adoptaron escalas discretas de cinco niveles tanto para la probabilidad como para el impacto, conforme se detalla en la Tabla 10. El riesgo se obtiene como el producto de ambos factores, resultando en un valor comprendido entre 1 y 25.

Tabla 10

Escalas de probabilidad e impacto aplicadas al análisis de riesgos

Nivel	Probabilidad	Frecuencia estimada	Impacto	Descripción del impacto
1	Muy baja	Menos de una vez cada 5 años	Muy bajo	Degradación imperceptible del servicio
2	Baja	Una vez cada 2 a 5 años	Bajo	Interrupción menor, sin afectación al ciudadano
3	Media	Una vez al año	Medio	Interrupción parcial del servicio durante horas
4	Alta	Varias veces al año	Alto	Interrupción total del servicio durante un día
5	Muy alta	Mensual o más frecuente	Muy alto	Interrupción prolongada con pérdida de información

Nota. Elaboración propia.

El nivel de riesgo resultante se interpreta según cuatro rangos: riesgo bajo entre 1 y 6, que se acepta y monitorea; riesgo medio entre 8 y 12, que requiere salvaguardas programadas; riesgo alto entre 15 y 16, que exige tratamiento prioritario; y riesgo crítico entre 20 y 25, que demanda acción inmediata. Este criterio determina el orden de aplicación de las salvaguardas propuestas.

Identificación de amenazas y cálculo del riesgo

Las amenazas se identificaron a partir de los cuatro grupos del catálogo MAGERIT: desastres naturales [N], de origen industrial [I], errores y fallos no intencionados [E] y ataques intencionados [A]. La Tabla 11 presenta el resultado del análisis para los activos críticos, consignando en cada caso la amenaza de mayor riesgo asociado.

Tabla 11

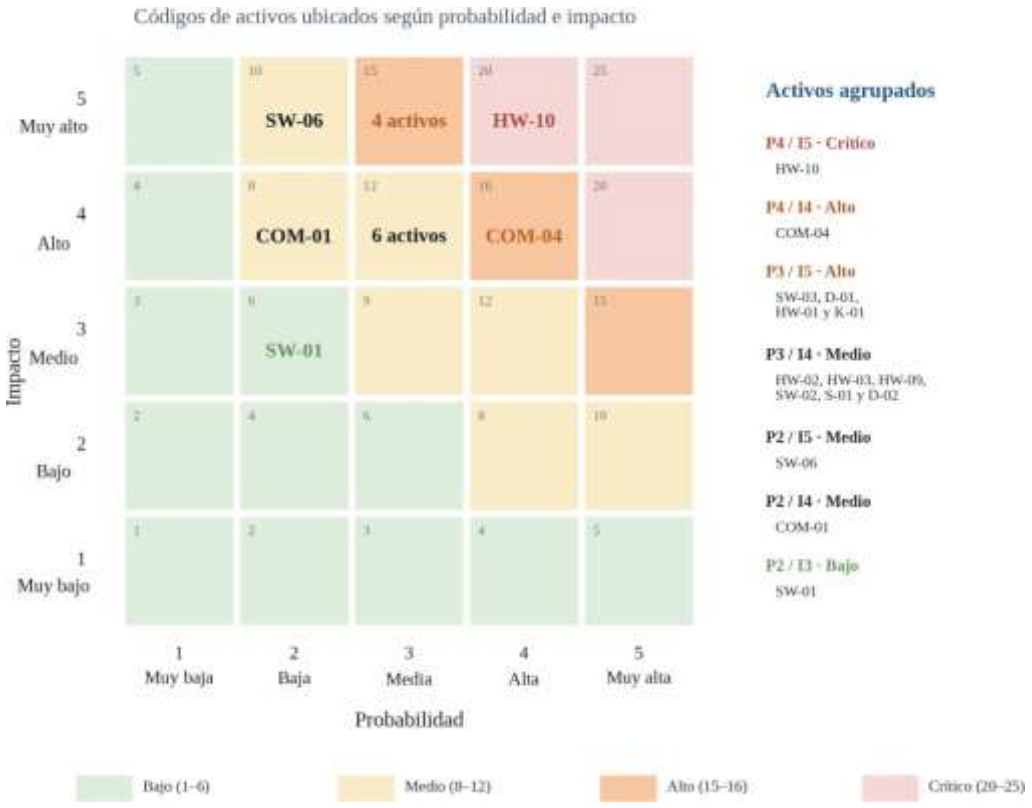
Matriz de riesgos de los activos críticos del GADIC SUSCAL

Código	Activo	Amenaza principal (MAGERIT)	P	I	Riesgo	Nivel
ACT-SW-03	Servidor de base de datos	[E.1] Errores de administración	3	5	15	Alto
ACT-D-01	Respaldos de la base de datos	[E.2] Errores del administrador de respaldos	3	5	15	Alto
ACT-HW-01	Servidores HPE	[I.5] Avería de origen físico o lógico	3	5	15	Alto
ACT-HW-10	Firewall	[A.11] Acceso no autorizado	4	5	20	Crítico
ACT-COM-04	Enlace WAN de Internet (CNT)	[I.8] Fallo de servicios de comunicaciones	4	4	16	Alto
ACT-HW-02	Máquinas virtuales VMware	[E.24] Caída del sistema por agotamiento de recursos	3	4	12	Medio
ACT-SW-06	VMware	[I.5] Avería de origen físico o lógico	2	5	10	Medio
ACT-HW-03	NAS Synology RS1221RP	[I.5] Avería de origen físico o lógico	3	4	12	Medio
ACT-HW-09	Switches Cisco	[I.6] Corte del suministro eléctrico	3	4	12	Medio
ACT-COM-01	Red interna (12 VLAN)	[E.9] Errores de reencaminamiento	2	4	8	Medio
ACT-SW-02	Servidor de aplicaciones	[A.7] Uso no previsto	3	4	12	Medio
ACT-K-01	Certificado SSL Wildcard	[E.28] Caducidad no controlada	3	5	15	Alto
ACT-S-01	Páginas web institucionales	[A.24] Denegación de servicio	3	4	12	Medio
ACT-D-02	Datos de configuración de red	[E.1] Errores de administración	3	4	12	Medio
ACT-SW-01	Software y licencias adquiridas	[E.28] Caducidad no controlada	2	3	6	Bajo

Nota. Elaboración propia a partir del catálogo de amenazas del Libro II de MAGERIT v3 y de la matriz de activos del GADIC SUSCAL (2026). Valores preliminares sujetos a validación con el responsable del área de TIC.

Figura 4

Mapa de riesgos de los activos críticos del GADIC SUSCAL



Nota. Elaboración propia con base en Ministerio de Hacienda y Administraciones Públicas (2012) y la matriz de riesgos del GADIC SUSCAL (2026).

El análisis revela que el riesgo se concentra en dos frentes. El primero es el acceso no autorizado al firewall perimetral, único activo que alcanza nivel crítico: su compromiso no afecta a un servicio aislado sino a la totalidad del perímetro, y su valoración máxima en las cinco dimensiones de seguridad confirma esa transversalidad. El segundo es la dependencia de un proveedor único de conectividad, que sitúa el fallo del enlace WAN en nivel alto pese a tratarse de un evento externo al control institucional.

Destaca asimismo que tres de los cinco riesgos de nivel alto corresponden a errores humanos de administración y no a fallos técnicos ni a ataques. Este hallazgo es consistente con el diagnóstico del Capítulo III, donde el dominio de gestión de incidentes registró cumplimiento nulo: sin procedimientos documentados ni registro formal de eventos, la operación depende del

conocimiento no formalizado de una sola persona, lo que constituye en sí mismo un punto único de falla de naturaleza organizativa.

3.9 Fases de la Metodología

El diseño del Plan de Continuidad de Negocio se organiza en seis fases secuenciales que articulan los instrumentos de diagnóstico descritos en este capítulo con los requisitos de la norma ISO 22301 y sus especificaciones técnicas complementarias, según se resume en la Tabla 12.

Tabla 12

Fases metodológicas para el diseño del BCP del GADIC SUSCAL

Fase	Descripción	Referencia normativa	Producto
1. Diagnóstico institucional	Aplicación de la lista de verificación y revisión documental para establecer la línea base de seguridad y continuidad.	ISO/IEC 27002:2022	Nivel de cumplimiento por dominio (Cap. III)
2. Inventario y valoración de activos	Identificación, codificación y valoración de los activos tecnológicos en cinco dimensiones.	MAGERIT v3, Libro II	Matriz de activos y subconjunto crítico (Cap. III)
3. Análisis de riesgos	Identificación de amenazas por activo crítico y estimación de impacto y riesgo.	MAGERIT v3, Libro I	Matriz de riesgos (Cap. III) y salvaguardas (Cap. IV)
4. Análisis de Impacto al Negocio	Determinación de servicios críticos y de los parámetros RTO, RPO y MTPD.	ISO/TS 22317:2021	BIA de los servicios digitales (Cap. IV)
5. Estrategias de continuidad	Definición de estrategias de prevención, respuesta y recuperación por servicio crítico.	ISO/TS 22332:2021	Catálogo de estrategias (Cap. IV)
6. Documentación y validación del plan	Estructuración del BCP, asignación de roles y revisión con el área de TIC.	ISO 22301:2019	Plan de Continuidad de Negocio (Cap. IV)

Nota. Elaboración propia.

Las fases 1, 2 y 3 quedan resueltas en el presente capítulo con los resultados del diagnóstico, el inventario de activos y el análisis de riesgos. Las fases 4 a 6 se desarrollan en el Capítulo IV, donde el tratamiento del riesgo, el Análisis de Impacto al Negocio y las estrategias de continuidad se integran en la propuesta del Plan de Continuidad de Negocio.

CAPÍTULO IV

4 PROPUESTA

4.1 Introducción

El presente capítulo desarrolla la propuesta de Plan de Continuidad de Negocio para los servicios digitales del GADIC SUSCAL, construida sobre los hallazgos del diagnóstico presentado en el Capítulo III. Mientras aquel capítulo estableció la línea base de seguridad, consolidó el inventario de activos y determinó los niveles de riesgo, este desarrolla las fases 4 a 6 de la secuencia metodológica definida en la Tabla 12: el tratamiento del riesgo mediante salvaguardas, el Análisis de Impacto al Negocio, la definición de estrategias de continuidad y la estructuración documental del plan.

El diagnóstico demostró una asimetría relevante: la institución alcanza niveles aceptables de cumplimiento en controles operativos respaldos, control de accesos y segmentación de red, pero apenas un 20% en el dominio de continuidad de las actividades institucionales y un 0% en gestión de incidentes. Esto significa que el GADIC SUSCAL posee capacidades técnicas instaladas, pero carece del marco formal que las organice ante una disrupción. La propuesta aprovecha esa condición: no parte de cero, sino que estructura y formaliza capacidades ya existentes.

La propuesta se formula conforme a la norma ISO 22301:2019, con el apoyo de las especificaciones técnicas ISO/TS 22317:2021 para el Análisis de Impacto al Negocio e ISO/TS 22332:2021 para el diseño de planes y procedimientos, y toma como insumo directo la matriz de riesgos obtenida mediante la metodología MAGERIT versión 3 en el Capítulo III.

4.2 Objetivo de la Propuesta

Diseñar un Plan de Continuidad de Negocio basado en la norma ISO 22301:2019 que permita al GADIC SUSCAL mantener o restablecer sus servicios digitales críticos dentro de

tiempos objetivo definidos ante la ocurrencia de un incidente disruptivo, mediante la identificación de riesgos sobre los activos tecnológicos, la determinación de los parámetros de recuperación de cada servicio, la definición de estrategias de prevención y respuesta, y la asignación formal de roles y procedimientos de actuación.

4.3 Alcance del Plan

El Plan de Continuidad de Negocio propuesto aplica a los servicios digitales del GADIC SUSCAL delimitados en el Capítulo I: el sistema de recaudación tributaria, el sistema de catastros y avalúos, el registro de la propiedad, el portal web institucional con sus formularios en línea y servicios de transparencia, y la infraestructura tecnológica que los soporta. Comprende los 15 activos identificados como críticos en la Tabla 9 y al personal del área de Tecnologías de la Información y Comunicación responsable de su operación.

Quedan fuera del alcance los procesos administrativos no soportados por medios digitales, los servicios prestados por terceros sobre los cuales la institución no ejerce control técnico directo salvo en lo referente a los acuerdos de nivel de servicio que deban exigírseles y la ejecución material del plan, cuya implementación queda sujeta a la aprobación de la máxima autoridad institucional conforme se estableció en las delimitaciones de la investigación.

4.4 Tratamiento del Riesgo: Salvaguardas Propuestas

El análisis de riesgos desarrollado en el Capítulo III identificó los niveles de exposición de los activos críticos del GADIC SUSCAL. Corresponde ahora definir su tratamiento, primera componente de la propuesta, por cuanto las salvaguardas condicionan las estrategias de continuidad formuladas más adelante.

Para cada riesgo de nivel medio, alto o crítico se definieron salvaguardas conforme al criterio de tratamiento de MAGERIT, priorizando aquellas de carácter preventivo sobre las correctivas. La Tabla 13 presenta las salvaguardas propuestas y el riesgo residual estimado tras su aplicación.

Tabla 13

Salvaguardas propuestas para los activos críticos

Código	Activo	Salvaguarda propuesta	Riesgo actual	Riesgo residual
ACT-HW-10	Firewall	Autenticación de doble factor para administración, registro de accesos, revisión trimestral de reglas y respaldo cifrado de la configuración	20	8
ACT-COM-04	Enlace WAN	Contratación de enlace secundario con proveedor alterno y conmutación automática ante indisponibilidad del principal	16	8
ACT-SW-03	Servidor de base de datos	Respaldos incrementales diarios verificados, control de cambios formal y segregación de credenciales administrativas	15	6
ACT-D-01	Respaldos	Aplicación del esquema 3-2-1, pruebas de restauración documentadas y custodia externa de una copia	15	5
ACT-HW-01	Servidores HPE	Contrato de soporte con tiempo de respuesta comprometido, monitoreo de salud del hardware y equipamiento de reemplazo disponible	15	9
ACT-K-01	Certificado SSL	Registro centralizado de vencimientos con alertas automáticas a 60, 30 y 15 días	15	4
ACT-HW-02	Máquinas virtuales	Instantáneas programadas, monitoreo de consumo de recursos y umbrales de alerta	12	6
ACT-HW-09	Switches Cisco	Verificación mensual de UPS, mantenimiento preventivo y configuración respaldada	12	6
ACT-S-01	Páginas web	Protección ante denegación de servicio, limitación de peticiones y monitoreo de disponibilidad	12	6

Nota. Elaboración propia.

La aplicación del conjunto de salvaguardas reduce el riesgo promedio de los activos críticos de 14,3 a 6,4, situándolo en el rango de riesgo bajo. Ninguna salvaguarda elimina el riesgo por completo, lo que resulta coherente con el enfoque de la ISO 22301: la continuidad no presupone la ausencia de disrupciones, sino la capacidad de responder ante ellas dentro de tiempos tolerables.

4.5 Análisis de Impacto al Negocio (BIA)

El Análisis de Impacto al Negocio constituye el núcleo de la propuesta y se desarrolla conforme a la especificación técnica ISO/TS 22317:2021. Su finalidad es determinar, para cada servicio digital, el período máximo tolerable de disrupción y los parámetros objetivo de

recuperación, estableciendo así el orden en que los servicios deben ser restablecidos tras un incidente.

Criterios de impacto

La valoración del impacto consideró tres criterios pertinentes al carácter público de la institución: el impacto económico, expresado en la interrupción de la recaudación y en posibles sanciones; el impacto en el servicio al ciudadano, medido por la imposibilidad de completar trámites; y el impacto legal y reputacional, derivado del incumplimiento de las obligaciones de transparencia y de las Normas de Control Interno de la Contraloría General del Estado. El impacto se estima en función del tiempo transcurrido desde la interrupción, reconociendo que su severidad no es constante sino creciente.

Determinación de parámetros de recuperación

La Tabla 14 presenta el resultado del análisis para los cinco servicios digitales dentro del alcance. El período máximo tolerable de disrupción (MTPD) expresa el tiempo tras el cual el impacto se vuelve inaceptable para la institución; el tiempo objetivo de recuperación (RTO) define el plazo dentro del cual el servicio debe restablecerse, necesariamente inferior al MTPD; y el punto objetivo de recuperación (RPO) determina la pérdida máxima de información admisible, expresada como antigüedad del último respaldo utilizable.

Tabla 14

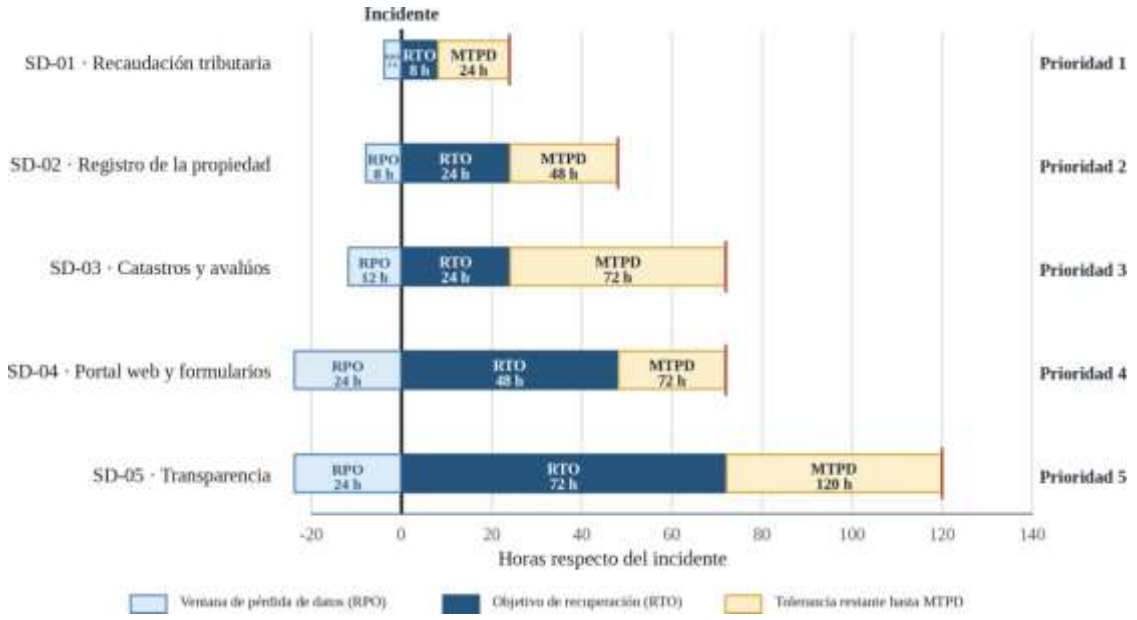
Parámetros de recuperación de los servicios digitales del GADIC SUSCAL

Código	Servicio digital	Impacto	MTPD	RTO	RPO	Prioridad
SD-01	Sistema de recaudación tributaria	Muy alto	24 h	8 h	4 h	1
SD-02	Registro de la propiedad	Alto	48 h	24 h	8 h	2
SD-03	Sistema de catastros y avalúos	Alto	72 h	24 h	12 h	3
SD-04	Portal web y formularios en línea	Medio	72 h	48 h	24 h	4
SD-05	Servicios de transparencia	Medio	120 h	72 h	24 h	5

Nota. Elaboración propia conforme a ISO/TS 22317:2021. Los valores constituyen una propuesta técnica que deberá ser validada y aprobada por los responsables de cada proceso institucional antes de la adopción del plan.

Figura 5

Objetivos de recuperación de los servicios digitales del GADIC SUSCAL



Nota. Elaboración propia con base en International Organization for Standardization (2021a) y el análisis de impacto al negocio del GADIC SUSCAL (2026).

La priorización sitúa al sistema de recaudación tributaria en primer lugar por dos razones convergentes: es la fuente directa de ingresos propios del municipio y su interrupción genera atención presencial acumulada que la institución no puede absorber. Su RPO de cuatro horas exige una frecuencia de respaldo superior a la práctica habitual de copia diaria, lo que constituye uno de los principales requerimientos técnicos derivados de esta propuesta.

En el extremo opuesto, los servicios de transparencia admiten un MTPD de cinco días por tratarse de información de consulta cuya indisponibilidad temporal no impide la ejecución de trámites, aunque su incumplimiento prolongado sí acarrea consecuencias ante los organismos de control.

Recursos mínimos de recuperación

Para cada servicio se identificaron los recursos indispensables para su restablecimiento dentro del RTO comprometido, conforme se detalla en la Tabla 15. Esta identificación permite verificar la coherencia entre los parámetros propuestos y la capacidad instalada.

Tabla 15

Recursos mínimos y dependencias por servicio digital

Servicio	Recursos mínimos requeridos	Dependencias externas
SD-01	Servidor de base de datos, servidor de aplicaciones, red interna, enlace WAN, técnico de TIC	Proveedor de conectividad, energía eléctrica
SD-02	Servidor de base de datos, servidor de aplicaciones, red interna	Sistema nacional de registro
SD-03	Servidor de base de datos, almacenamiento NAS, red interna	Cartografía institucional
SD-04	Servidor web, certificado SSL, enlace WAN, firewall	Proveedor de conectividad
SD-05	Servidor web, enlace WAN	Portal de transparencia nacional

Nota. Elaboración propia.

El análisis de dependencias evidencia que cuatro de los cinco servicios dependen del enlace WAN y tres del servidor de base de datos, lo que confirma la concentración de criticidad detectada en el análisis de riesgos y justifica que las salvaguardas asociadas a ambos activos reciban tratamiento prioritario.

4.6 Estrategias de Continuidad

Conforme a la especificación técnica ISO/TS 22332:2021, las estrategias de continuidad se formularon para cada servicio crítico atendiendo a tres momentos: la prevención, orientada a reducir la probabilidad de ocurrencia; la respuesta, destinada a contener el incidente y mantener un nivel mínimo de operación; y la recuperación, dirigida al restablecimiento completo dentro del RTO. La Tabla 16 sintetiza las estrategias propuestas.

Tabla 16

Estrategias de continuidad por servicio digital crítico

Servicio	Prevención	Respuesta	Recuperación
SD-01	Respaldo incremental cada 4 horas, monitoreo de disponibilidad y mantenimiento preventivo trimestral	Habilitación de caja recaudadora en modalidad manual con registro diferido	Restauración sobre servidor virtual alterno y conciliación de transacciones diferidas
SD-02	Respaldo diario verificado y control de cambios sobre la base de datos	Suspensión temporal de inscripciones con registro en bitácora física	Restauración de la base de datos y validación de integridad registral
SD-03	Respaldo diario y réplica del almacenamiento en NAS	Atención con certificados emitidos manualmente sobre el último respaldo disponible	Restauración del servicio y actualización de la información catastral
SD-04	Monitoreo de disponibilidad, control de vencimiento del certificado SSL y protección ante denegación de servicio	Publicación de aviso institucional en redes sociales y atención presencial	Redespliegue del portal y verificación de formularios en línea
SD-05	Respaldo semanal de los contenidos publicados	Comunicación formal al organismo de control sobre la indisponibilidad	Republicación de los contenidos conforme al calendario de transparencia

Nota. Elaboración propia.

Las estrategias de respuesta incorporan deliberadamente mecanismos manuales de contingencia. Esta decisión responde a la realidad institucional: al no disponer el GADIC SUSCAL de un sitio alterno de procesamiento, la continuidad del servicio al ciudadano durante la ventana de recuperación solo puede sostenerse mediante procedimientos degradados debidamente documentados, cuya posterior conciliación con los sistemas restablecidos debe quedar formalmente prevista.

4.7 Plan de Respuesta y Recuperación

Equipo de continuidad y responsabilidades

El diagnóstico determinó que la institución no ha conformado un equipo de continuidad con roles y suplentes definidos. La propuesta establece una estructura mínima de cuatro roles, dimensionada conforme a la capacidad real del municipio y sin requerir contratación adicional de personal, según se detalla en la Tabla 17.

Tabla 17

Estructura del equipo de continuidad del negocio

Rol	Cargo asignado	Responsabilidades principales	Suplente
Coordinador del BCP	Responsable del área de TIC	Declara la activación del plan, dirige la respuesta y autoriza el cierre del incidente	Director administrativo
Responsable técnico	Técnico de soporte de TIC	Ejecuta los procedimientos de recuperación y restauración de respaldos	Responsable del área de TIC
Enlace institucional	Director administrativo	Coordina con las áreas afectadas y gestiona los recursos necesarios	Secretario general
Responsable de comunicación	Encargado de comunicación social	Informa a la ciudadanía y a los organismos de control	Enlace institucional

Nota. Elaboración propia. La asignación nominal de los cargos deberá formalizarse mediante resolución de la máxima autoridad institucional.

La designación de suplentes atiende a una vulnerabilidad detectada en el Capítulo III: la concentración del conocimiento técnico en un único funcionario. La existencia formal de suplentes no elimina esa dependencia, pero establece la obligación de documentar los procedimientos de modo que resulten ejecutables por una persona distinta de quien los diseñó.

Niveles de severidad y criterios de activación

La activación del plan no procede ante cualquier incidencia técnica. La Tabla 18 define tres niveles de severidad con sus respectivos criterios y responsables de decisión, evitando tanto la activación innecesaria como la demora ante eventos que sí la requieren.

Tabla 18

Niveles de severidad y criterios de activación del plan

Nivel	Criterio	Acción	Decisión
Nivel 1 – Menor	Degradación de un servicio no crítico o interrupción inferior a 2 horas	No se activa el plan; se registra en la bitácora de incidentes	Responsable técnico
Nivel 2 – Mayor	Interrupción de un servicio crítico con duración estimada superior al 50% de su RTO	Activación parcial del plan y convocatoria del equipo de continuidad	Coordinador del BCP
Nivel 3 – Crítico	Interrupción simultánea de dos o más servicios críticos, pérdida de datos o compromiso del perímetro de seguridad	Activación total del plan y notificación a la máxima autoridad	Coordinador del BCP y máxima autoridad

Nota. Elaboración propia.

Fases del procedimiento de respuesta

El procedimiento de respuesta se organiza en cinco fases consecutivas. La detección comprende la identificación del evento por monitoreo o por reporte de usuario y su registro inmediato en la bitácora de incidentes. La evaluación determina el servicio afectado, estima la duración de la interrupción y asigna el nivel de severidad conforme a los criterios establecidos. La contención aplica las medidas necesarias para impedir la propagación del incidente y activa los procedimientos manuales de contingencia previstos en las estrategias de respuesta.

La recuperación ejecuta los procedimientos técnicos correspondientes al servicio afectado, restaurando los respaldos disponibles y verificando la integridad de la información restablecida. Finalmente, el cierre comprende la validación funcional del servicio con el área usuaria, la conciliación de las transacciones registradas manualmente durante la contingencia, la declaración formal de normalización por parte del Coordinador del BCP y el registro de las lecciones aprendidas.

Figura 6

Secuencia de respuesta y recuperación ante incidentes disruptivos



Nota. Elaboración propia con base en International Organization for Standardization (2021b).

Registro y comunicación

Todo incidente debe documentarse en un formulario de registro que consigne la fecha y hora de detección, el servicio afectado, el nivel de severidad asignado, las acciones ejecutadas, el tiempo real de recuperación y la comparación de este con el RTO comprometido. Esta comparación es el insumo que alimenta el proceso de mejora continua y permite verificar si los parámetros establecidos en el BIA resultan alcanzables en la práctica o requieren revisión.

La comunicación se estructura en tres destinatarios: interna, dirigida a las áreas afectadas mediante los canales institucionales; externa, orientada a la ciudadanía a través del portal y las redes sociales cuando la interrupción supere las cuatro horas en un servicio de atención directa; y de control, remitida a la máxima autoridad y, cuando corresponda, a los organismos de control en incidentes de nivel 3.

4.8 Programa de Pruebas y Ejercicios

La cláusula 8.5 de la ISO 22301:2019 establece que la organización debe someter a prueba sus procedimientos de continuidad para verificar su eficacia. Un plan no ejercitado carece de valor demostrable, y esta consideración resulta particularmente pertinente en el caso analizado, donde el diagnóstico evidenció que la institución nunca ha verificado formalmente su capacidad de recuperación. La Tabla 19 propone el programa anual de ejercicios.

Tabla 19

Programa anual de pruebas del Plan de Continuidad de Negocio

Tipo de prueba	Frecuencia	Objetivo	Responsable
Prueba de restauración de respaldos	Trimestral	Verificar que los respaldos son restaurables dentro del RPO comprometido	Responsable técnico
Ejercicio de mesa (tabletop)	Semestral	Revisar la comprensión de roles y procedimientos ante un escenario simulado	Equipo de continuidad
Simulacro de conmutación de enlace	Semestral	Comprobar la operatividad del enlace secundario de conectividad	Responsable técnico
Simulacro funcional de recuperación	Anual	Ejecutar la recuperación completa del servicio SD-01 midiendo el RTO real	Equipo de continuidad

Nota. Elaboración propia.

Cada ejercicio debe generar un informe que consigne los tiempos alcanzados, las desviaciones respecto de los parámetros comprometidos y las acciones correctivas derivadas. El simulacro funcional anual constituye la prueba de mayor valor probatorio, pues es la única que permite contrastar empíricamente los RTO propuestos en el BIA con la capacidad real de la institución.

4.9 Mantenimiento y Mejora Continua

El Plan de Continuidad de Negocio constituye un documento vivo cuya vigencia depende de su actualización. Se establece una revisión ordinaria anual, a cargo del Coordinador del BCP, que comprende la verificación del inventario de activos, la revisión de los parámetros de recuperación y la actualización de la asignación de roles. Procede además una revisión extraordinaria ante la ocurrencia de un incidente de nivel 3, la incorporación de un nuevo

servicio digital al alcance, un cambio sustancial en la infraestructura tecnológica o una modificación de la estructura orgánica institucional.

La mejora continua se articula mediante el ciclo planificar-hacer-verificar-actuar previsto en la cláusula 10 de la ISO 22301:2019. Los informes de ejercicios y los registros de incidentes reales constituyen las entradas del proceso, mientras que las acciones correctivas derivadas deben incorporarse formalmente al plan y comunicarse al equipo de continuidad.

4.10 Verificación del Cumplimiento de la Norma ISO 22301:2019

A fin de demostrar la conformidad de la propuesta con la norma rectora, la Tabla 20 establece la trazabilidad entre las cláusulas de la ISO 22301:2019 y los apartados del presente trabajo que las desarrollan.

Tabla 20

Trazabilidad entre las cláusulas de la ISO 22301:2019 y la propuesta

Cláusula ISO 22301:2019	Elemento desarrollado	Ubicación en el trabajo
4. Contexto de la organización	Diagnóstico institucional y línea base de seguridad	Capítulo III, secciones 3.4 a 3.6
5. Liderazgo	Definición del equipo de continuidad y asignación de responsabilidades	Sección 4.7.1
6. Planificación	Análisis de riesgos y definición de salvaguardas	Secciones 3.8 y 4.4
7. Apoyo	Recursos mínimos, competencias y esquema de comunicación	Secciones 4.5.3 y 4.7.4
8.2 Análisis de impacto y apreciación del riesgo	BIA con MTPD, RTO y RPO por servicio	Sección 4.5
8.3 Estrategias y soluciones	Estrategias de prevención, respuesta y recuperación	Sección 4.6
8.4 Planes y procedimientos	Procedimiento de respuesta, niveles de severidad y registro	Sección 4.7
8.5 Programa de ejercicios	Programa anual de pruebas y simulacros	Sección 4.8
9. Evaluación del desempeño	Medición del RTO real frente al comprometido	Secciones 4.7.4 y 4.8
10. Mejora	Revisión ordinaria y extraordinaria del plan	Sección 4.9

Nota. Elaboración propia.

La trazabilidad evidencia que la propuesta cubre las cláusulas 4 a 10 de la norma en su dimensión de diseño documental. Corresponde precisar que las cláusulas 9 y 10 solo alcanzan

cumplimiento pleno mediante la operación efectiva del plan durante al menos un ciclo anual, lo que excede el alcance de la presente investigación conforme se estableció en las delimitaciones del Capítulo I.

Conclusiones

El estudio teórico desarrollado permitió establecer la base conceptual y metodológica del proyecto, delimitando la continuidad del negocio como una disciplina distinta de la seguridad de la información y de la recuperación ante desastres. La revisión comparativa de los marcos de referencia disponibles determinó que la norma ISO 22301:2019 constituye el estándar rector, complementado por la especificación ISO/TS 22317:2021 para el análisis de impacto, la ISO/TS 22332:2021 para el diseño de planes y procedimientos, la ISO/IEC 27031 como puente entre la seguridad de la información y la continuidad operativa, y la metodología MAGERIT versión 3 para el análisis de riesgos. Esta selección normativa resultó determinante para el resto del trabajo, por cuanto definió tanto los instrumentos aplicados en el diagnóstico como la estructura de la propuesta.

El diagnóstico de la situación actual evidenció un nivel de cumplimiento global del 60,6% sobre los 66 controles de seguridad verificados, con 40 controles implantados, 16 en proceso de implementación y 10 inexistentes. El hallazgo más relevante no radica en la cifra global sino en su distribución: mientras los dominios operativos alcanzan niveles altos cumplimiento normativo con 100%, seguridad en la operativa con 87,5% y control de accesos con 80%, los dominios que sustentan directamente la continuidad registran los valores más bajos, con 20% en continuidad de las actividades institucionales y cumplimiento nulo en gestión de incidentes de seguridad. El GADIC SUSCAL dispone, por tanto, de capacidades técnicas instaladas, pero carece del marco formal que las organice ante una disrupción, lo que confirma el problema formulado en el Capítulo I.

El análisis de riesgos aplicado conforme a MAGERIT versión 3 sobre el inventario de 36 activos tecnológicos permitió identificar 15 activos críticos, con valor global igual o superior a 9. El riesgo se concentra en dos frentes: el acceso no autorizado al firewall perimetral, único activo que alcanza nivel crítico con un valor de 20, cuyo compromiso afectaría la totalidad del

perímetro institucional; y la dependencia de un proveedor único de conectividad, que sitúa el fallo del enlace WAN en nivel alto. Resulta significativo que tres de los cinco riesgos de nivel alto correspondan a errores humanos de administración y no a fallos técnicos ni a ataques deliberados, hallazgo coherente con el cumplimiento nulo detectado en gestión de incidentes: sin procedimientos documentados ni registro formal de eventos, la operación depende del conocimiento no formalizado de una sola persona, lo que constituye en sí mismo un punto único de falla de naturaleza organizativa.

El Plan de Continuidad de Negocio diseñado incorpora los componentes exigidos por la norma ISO 22301:2019 y se materializa en el documento institucional PCN-GADIC SUSCAL-001. El Análisis de Impacto al Negocio determinó los parámetros de recuperación de los cinco servicios digitales, situando al sistema de recaudación tributaria como prioridad uno con un tiempo objetivo de recuperación de 8 horas y un punto objetivo de recuperación de 4 horas. La propuesta define además las estrategias de prevención, respuesta y recuperación por servicio, la estructura del equipo de continuidad con roles y suplentes, tres niveles de severidad con criterios objetivos de activación, un procedimiento de respuesta en cinco fases con instrucciones técnicas específicas, un programa anual de pruebas y siete formatos operativos de registro. Las salvaguardas propuestas reducen el riesgo promedio de los activos críticos de 14,3 a 6,4, situándolo en el rango de riesgo bajo.

En conjunto, el objetivo general de la investigación se cumplió: el GADIC SUSCAL cuenta ahora con un Plan de Continuidad de Negocio fundamentado en un diagnóstico verificable y alineado con las cláusulas 4 a 10 de la norma ISO 22301:2019, conforme acredita la tabla de trazabilidad del Capítulo IV. Corresponde precisar, no obstante, que las cláusulas 9 y 10, relativas a la evaluación del desempeño y a la mejora continua, solo alcanzan cumplimiento pleno mediante la operación efectiva del plan durante al menos un ciclo anual, lo que excede el alcance temporal de este trabajo. La contribución de la investigación consiste, por tanto, en dotar a la institución de un instrumento de gestión listo para ser adoptado, cuya eficacia deberá verificarse en su aplicación.

Recomendaciones

Se recomienda a la máxima autoridad del GADIC SUSCAL adoptar formalmente el Plan de Continuidad de Negocio mediante el acto administrativo correspondiente, designando nominalmente a los servidores que ocuparán los roles del equipo de continuidad y a sus respectivos suplentes. Sin ese acto de aprobación, el documento carece de exigibilidad y los procedimientos definidos no resultan oponibles a las unidades administrativas involucradas.

Se recomienda a la Dirección de Tecnologías de la Información y Comunicación priorizar el tratamiento de los dos riesgos de mayor nivel identificados. Respecto del firewall perimetral, corresponde implementar autenticación de doble factor para su administración, registro de accesos y revisión trimestral de reglas. Respecto de la conectividad, se sugiere gestionar la contratación de un enlace secundario con un proveedor alterno, dado que cuatro de los cinco servicios digitales dependen del enlace actual y su indisponibilidad compromete simultáneamente la mayor parte de la atención en línea.

Se recomienda formalizar la asignación de propietarios y custodios de los activos de información de naturaleza lógica, deficiencia detectada en el diagnóstico y que afecta a once de los quince activos críticos, entre ellos el servidor de base de datos, el firewall y los respaldos. Asimismo, se sugiere documentar los procedimientos técnicos de operación de modo que resulten ejecutables por un servidor distinto de quien los diseñó, a fin de mitigar la dependencia del conocimiento individual advertida en el análisis de riesgos.

Se recomienda ejecutar el programa anual de pruebas previsto en el plan, comenzando por la prueba trimestral de restauración de respaldos, y verificar en la práctica los parámetros de recuperación establecidos. En particular, el punto objetivo de recuperación de 4 horas definido para el sistema de recaudación tributaria exige una frecuencia de respaldo superior a la práctica de copia diaria, por lo que su viabilidad debe confirmarse y, de resultar necesario, ajustarse la periodicidad de los respaldos o el propio parámetro. El simulacro funcional anual constituye el único ejercicio que permite contrastar empíricamente los tiempos comprometidos con la capacidad real de la institución.

Se recomienda a futuras investigaciones evaluar la eficacia del plan tras un ciclo completo de operación, contrastando los tiempos de recuperación efectivamente alcanzados con los parámetros comprometidos, y extender el alcance del estudio a los procesos administrativos

no soportados en medios digitales. Igualmente, se sugiere replicar la metodología aplicada en otros gobiernos autónomos descentralizados de escala comparable, considerando que los resultados del presente trabajo, por corresponder a un estudio de caso único, describen la situación específica del GADIC SUSCAL y no admiten generalización directa.

Referencias

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial. https://www.asambleanacional.gob.ec/es/node/115246

Buscán Pinguil, P. C., Flores Urgilés, C. H., Pinos Castillo, L. F., & Flores Urgilés, C. M. (2022). Modelo de plan de continuidad de negocio de las Cooperativas segmento B del cantón Cañar. *Pro Sciences: Revista de Producción, Ciencias e Investigación*. https://journalprosciences.com/index.php/ps/article/view/521

Cedergren, A., & Hassel, H. (2025). Business continuity management in public sector organizations: Development, challenges, and ways forward. *Journal of Contingencies and Crisis Management, 33*(2), Article e70055. https://doi.org/10.1111/1468-5973.70055

Consejo Nacional de Competencias. (2025). *Plan Estratégico Institucional 2025–2029*. Consejo Nacional de Competencias.

Contraloría General del Estado. (2023). *Normas de Control Interno*. https://www.contraloria.gob.ec/WFDescarga.aspx?id=1487&tipo=mul

Dakic, V., Mikulic Premuzic, K., & Petrunic, R. (2024). Business continuity planning (BCP) and disaster recovery planning (DRP). En *Proceedings of the 35th DAAAM International Symposium on Intelligent Manufacturing and Automation*. DAAAM International. https://daaam.info/35th-proceedings-2024

Elliott, D., Swartz, E., & Herbane, B. (2010). *Business continuity management: A crisis management approach* (2.ª ed.). Routledge. https://doi.org/10.4324/9780203866337

Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal [GADIC SUSCAL]. (2026). *Portal institucional del GAD Suscal*. https://gadsuscal.gob.ec/

Hassel, H., & Cedergren, A. (2024). A framework for business continuity management in a multiactor context. *Journal of Contingencies and Crisis Management, 32*(2), Article e12573. https://doi.org/10.1111/1468-5973.12573

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO.

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. ISO.

International Organization for Standardization. (2020). *ISO 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*. ISO.

International Organization for Standardization. (2021a). *ISO/TS 22317:2021 Security and resilience — Business continuity management systems — Guidelines for business impact analysis*. ISO.

International Organization for Standardization. (2021b). *ISO/TS 22332:2021 Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures*. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2025). *ISO/IEC 27031:2025 Cybersecurity — Information and communication technology readiness for business continuity*. ISO.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método*. Gobierno de España.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2025). *Política Pública para la Transformación Digital del Ecuador 2025-2030*. MINTEL. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2025/03/INSTRUMENTO-

Politica-Publica-para-la-Transformacion-Digital-Ecuador-2025-2030-MINTEL-signed_f.pdf

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

OECD. (2024). *2023 OECD Digital Government Index: Results and key findings*. OECD Publishing. https://doi.org/10.1787/1a89ed5e-en

Religia, A. A., & Utama, D. N. (2024). A novel framework for business continuity plan in public sector organization. *Journal of System and Management Sciences, 14*(1), 1–14. https://doi.org/10.33168/JSMS.2024.0101

Santos Rocha, M. S. (2024). *Desarrollo del plan de continuidad de negocio de acuerdo a los estándares vigentes, para el data center de la carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito* [Tesis de grado, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. https://dspace.ups.edu.ec/

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science, 89*, 201–218. https://doi.org/10.1016/j.ssci.2016.06.015

United Nations Department of Economic and Social Affairs. (2024). *United Nations E-Government Survey 2024: Accelerating digital transformation for sustainable development*. United Nations. https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2024

World Bank. (2022). *GovTech Maturity Index, 2022 update: Trends in public sector digital transformation*. World Bank. https://www.worldbank.org/en/programs/govtech/gtmi

ANEXOS

Código	Denominación
Anexo F	Protocolo de investigación
Anexo A1	Lista de verificación de cumplimiento ISO/IEC 27002 (instrumento A001)
Anexo A2	Matriz de inventario y valoración de activos según MAGERIT v3
Anexo B	Plan de Continuidad del Negocio del GADIC SUSCAL (PCN-GADIC SUSCAL-001)
Anexo C	Formatos operativos del Plan de Continuidad del Negocio (PCN-GADIC SUSCAL-002)
Anexo D	Ficha de validación técnica de los parámetros de continuidad (instrumento A002)
Anexo E	Solicitud de autorización institucional

Anexo F. Protocolo de investigación

Anexo: Formato del Anteproyecto.

A. TÍTULO
Plan de Continuidad de Negocio basado en la Norma ISO 22301 para los servicios digitales del GADIC SUSCAL.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	x
		Auditoría Informática	
		Seguridad Informática	
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA
En el contexto actual de transformación digital, las instituciones públicas han incorporado de manera progresiva tecnologías de la información para optimizar sus procesos administrativos, mejorar la eficiencia operativa y fortalecer la atención a la ciudadanía. La modernización de la gestión pública puede atribuirse al proceso de digitalización, sin embargo, se ha producido una dependencia excesiva en los sistemas informáticos, plataformas digitales y servicios tecnológicos, convirtiéndolos en aspectos críticos para el funcionamiento de las instituciones.

Esta dependencia de la tecnología pone a las instituciones en riesgo de muchas maneras que pueden interrumpir las operaciones normales. Estudios recientes muestran que fallos en la infraestructura tecnológica, cortes de energía, amenazas cibernéticas o incluso un error de un empleado pueden generar interrupciones en los servicios digitales y afectar el acceso a la información y la prestación de servicios públicos . Estas interrupciones pueden causar pérdida de ingresos y generar una percepción negativa de los servicios gubernamentales. También pueden erosionar la confianza que los ciudadanos depositan en su gobierno.

En tales casos, la gestión de la continuidad del negocio está completamente integrada en las organizaciones actuales, ya que les ayuda a planificar, reducir y responder a las interrupciones. Muchos estudios indican que la planificación formal de la continuidad es fundamental, ya que la incapacidad de una organización para recuperarse rápidamente de un incidente aumenta el tiempo de inactividad y afecta negativamente las operaciones en curso .

En lo que respecta a las autoridades locales, este problema es aún más crítico porque los servicios digitales desempeñan un papel fundamental en la administración y recaudación de ingresos, en la prestación de servicios a la ciudadanía y en la gestión de datos institucionales. En el caso del GADIC SUSCAL, existe una dependencia clara y creciente de los servicios digitales para el avance de sus operaciones; sin embargo, no cuenta con un plan de continuidad formal para las actividades comerciales basado en estándares internacionales, lo cual representa una vulnerabilidad ante situaciones que puedan ocurrir y que obstaculicen el funcionamiento de sus sistemas.

Sin un plan estructurado, esto obstaculiza la organización de servicios esenciales, recupera definiciones de tiempo y divisiones de tareas, y el diseño de estrategias para hacer frente a incidentes. Esto puede causar la interrupción de servicios cruciales, un efecto en la gestión de una institución, y también podría representar una amenaza para la integridad de la información.

En este caso, deberíamos preparar un plan de continuidad del negocio en línea con la norma ISO 22301 para los servicios digitales de GADIC SUSCAL. Esto ayudaría a fortalecer la capacidad de la institución para proteger, responder y recuperarse de

incidentes disruptivos y contribuir a mantener la continuidad de los servicios mientras se desarrolla la resiliencia organizacional.

¿De qué manera el diseño de un plan de continuidad del negocio basado en la norma ISO 22301 contribuirá a garantizar la continuidad de los servicios digitales del GADIC SUSCAL frente a eventos disruptivos?

D. OBJETIVO GENERAL

Diseñar un Plan de Continuidad de Negocio basado en la ISO 22301 para los servicios digitales del GADIC SUSCAL, mediante el estudio teórico de la continuidad operativa, el diagnóstico de la situación actual de los servicios digitales y la definición de estrategias de prevención, respuesta y recuperación, con el fin de fortalecer la disponibilidad operativa y la resiliencia tecnológica institucional ante eventos disruptivos.

E. OBJETIVOS ESPECÍFICOS

Realizar un estudio teórico sobre continuidad de negocio, servicios digitales, riesgos tecnológicos, análisis de impacto al negocio, recuperación ante desastres y norma ISO 22301, con el fin de establecer la base conceptual y metodológica del proyecto.

Diagnosticar la situación actual de los servicios digitales del GADIC SUSCAL, identificando activos tecnológicos, procesos críticos, amenazas, vulnerabilidades, riesgos y dependencias operativas que puedan afectar la continuidad de los servicios institucionales.

Diseñar un Plan de Continuidad de Negocio basado en la ISO 22301, incorporando estrategias de prevención, respuesta, recuperación, responsables, tiempos objetivos de recuperación y procedimientos para mantener o restablecer los servicios digitales críticos del GADIC SUSCAL.

F. JUSTIFICACIÓN

Este proyecto es necesario para fortalecer la operación continua de los servicios digitales de GADIC SUSCAL. Esto se debe a que la institución ofrece servicios en línea, formularios e información procesal transparente que dependen de recursos tecnológicos para asistir a los ciudadanos. Por lo tanto, se requieren sistemas digitales ininterrumpidos para facilitar la operación continua de la gestión municipal, el servicio público y el acceso y consulta de los servicios institucionales.

Desde un punto de vista tecnológico, la integración de un plan de continuidad del negocio ayuda a una organización a estructurar procesos para identificar funciones esenciales, evaluar riesgos, cuantificar efectos, determinar prioridades de recuperación y diseñar mecanismos de respuesta a diversos incidentes. ISO 22301 presenta una estructura para que las organizaciones reconozcan interrupciones y realicen análisis de impacto para planificar e implementar medidas para anticipar y tratar riesgos, y centrarse en la recuperación de interrupciones imprevistas, incluidos desastres naturales y incidentes cibernéticos.

El proyecto ayudará al GADIC SUSCAL mediante la provisión de una propuesta técnica que limite la necesidad de improvisar al abordar incidentes tecnológicos, mejore la gestión de la prevención de riesgos y aumente la capacidad de recuperación de los servicios digitales. Además, el estudio tendrá valor académico y metodológico porque combinará la revisión conceptual, la evaluación institucional y el diseño de un Plan de Continuidad del Negocio (PCN) basado en ISO 22301, evitando incorporar una fase de validación innecesaria que no se alinea con los objetivos establecidos.

G. ALCANCE

Este estudio desarrollará un Plan de Continuidad del Negocio conforme a la ISO 22301 para los servicios digitales de GADIC SUSCAL. Para apoyar la propuesta, el estudio realizará una revisión de la literatura sobre continuidad del negocio, riesgos tecnológicos, análisis de impacto en el negocio, recuperación ante desastres y servicios digitales críticos.

Este proyecto también revisará el estado actual de los servicios digitales de la institución, teniendo en cuenta los activos tecnológicos, sistemas, plataformas digitales, formularios

en línea, procedimientos y servicios, servicios de transparencia, formularios de solicitud de servicios digitales, registro de servicios de propiedad, avalúos y registros, servicios digitales, continuidad y amenazas potenciales, dependencias operativas, vulnerabilidades y riesgos.

Finalmente, el alcance incluye el diseño del Plan de Continuidad del Negocio, que consistirá en estrategias de prevención, respuesta y recuperación; las partes interesadas involucradas; tiempo de recuperación objetivo; procedimientos para la activación del plan y comunicaciones durante un incidente; respaldo de datos; recuperación de servicios de TI; y la restauración o continuidad de servicios esenciales. Este estudio no incluirá la implementación completa del plan del BCP, la adquisición de las infraestructuras de soporte necesarias para el BCP, la certificación formal del BCP según ISO 22301, ni la fase de validación independiente del plan del BCP, ya que la versión inicial se limita al estudio teórico, diagnóstico y diseño de la propuesta.

H. CONCEPTOS RELACIONADOS

Plan de Continuidad de Negocios

El Plan de Continuidad de Negocio, conocido como BCP, es un instrumento técnico que permite establecer procedimientos para mantener o recuperar las operaciones críticas de una organización ante eventos disruptivos. En el ámbito de los servicios digitales, este plan permite definir acciones de prevención, respuesta y recuperación para proteger sistemas, datos, plataformas y servicios tecnológicos esenciales. Estudios previos sobre continuidad de negocio en Cañar han abordado el BCP como una herramienta preventiva para garantizar la continuidad de servicios de TI frente a incidentes.

Continuidad de negocio

La continuidad de negocio se relaciona con la capacidad de una organización para mantener sus procesos críticos durante una interrupción. En organizaciones públicas, esta continuidad adquiere relevancia porque los servicios institucionales dependen cada vez más de sistemas de información. Religia y Utama señalan que la digitalización fortalece

los procesos del sector público, pero también hace que los sistemas de información tengan un rol vital, debido a que una afectación puede provocar interrupciones significativas en los procesos organizacionales.

ISO 22301

La ISO 22301 es una norma internacional para sistemas de gestión de continuidad del negocio. Su propósito es apoyar a las organizaciones en la preparación, prevención, respuesta y recuperación frente a incidentes disruptivos. Además, permite identificar disrupciones, evaluar impactos, desarrollar estrategias de mitigación y establecer procedimientos de continuidad.

Sistema de Gestión de Continuidad del Negocio

El Sistema de Gestión de Continuidad del Negocio permite organizar políticas, procesos, responsabilidades, recursos y procedimientos para asegurar que una institución pueda responder de manera planificada ante interrupciones. Dentro de la ISO 22301, la operación del sistema de continuidad requiere establecer procesos, políticas y procedimientos documentados, de modo que el personal conozca claramente las acciones que debe ejecutar y se mantenga la consistencia en la respuesta institucional.

Servicios digitales críticos

Los servicios digitales críticos son aquellos sistemas, plataformas, aplicaciones o recursos tecnológicos que permiten el funcionamiento de procesos institucionales esenciales. En el caso del GADIC SUSCAL, estos pueden relacionarse con trámites en línea, consultas de deudas, registro de la propiedad, formularios, transparencia, avalúos y catastros, desarrollo territorial y otros servicios disponibles desde el portal institucional.

Riesgo tecnológico

El riesgo tecnológico se refiere a la posibilidad de que una amenaza afecte los activos digitales, sistemas, redes, bases de datos, plataformas o procesos tecnológicos de una

organización. En el contexto de continuidad de negocio, los riesgos tecnológicos deben identificarse para establecer medidas preventivas y estrategias de recuperación. Entre las posibles disrupciones que afectan a los sistemas de información se encuentran el cibercrimen, los desastres naturales, los errores humanos, las fallas de dispositivos y los errores procedimentales.

Análisis de Impacto al Negocio

El Análisis de Impacto al Negocio, conocido como BIA, permite identificar los procesos críticos de una organización y analizar los efectos que tendría una interrupción sobre ellos. En un Plan de Continuidad de Negocio, el BIA permite priorizar servicios, estimar impactos, definir tiempos objetivos de recuperación y establecer estrategias de restablecimiento. En marcos de continuidad para el sector público, el análisis de impacto es considerado un componente necesario para estructurar estrategias de contingencia y continuidad.

Recuperación ante desastres

La recuperación ante desastres, conocida como DRP, está orientada al restablecimiento de la infraestructura tecnológica, sistemas, datos, aplicaciones y servicios digitales después de un evento de interrupción. Dentro de un Plan de Continuidad de Negocio, la recuperación debe priorizar los procesos y servicios críticos según los niveles de servicio definidos, considerando roles, responsabilidades, mecanismos de comunicación y procedimientos previamente documentados. En este contexto, el DRP agrega detalles al BCP, ya que se concentra en la recuperación de los componentes tecnológicos que se ven afectados. En este sentido, el DRP complementa al BCP porque se enfoca específicamente en la recuperación técnica de los recursos tecnológicos afectados.

I. TRABAJOS RELACIONADOS

En un escenario global, Religia y Utama (2024) en su trabajo titulado "Un Marco Innovador para el Plan de Continuidad del Negocio en Organizaciones del Sector

Público", propone la integración de la norma ISO 22301:2019 y la guía NIST SP 800-34 Rev. 1 para contextualizar los planes de continuidad de negocio de las organizaciones del sector público. La relevancia del estudio radica en que considera la continuidad de los servicios públicos desde el punto de vista tecnológico, reconociendo que, ante escenarios disruptivos, los sistemas de información son vitales para mantener el funcionamiento de las instituciones. Esto explica por qué proporciona una referencia metodológica para este proyecto preliminar, dado que GADIC SUSCAL también necesita desarrollar un Plan de Continuidad del Negocio con el objetivo de salvaguardar sus servicios digitales.

En otro ejemplo, Dakic et al. (2024) escriben sobre “Planificación de la Continuidad del Negocio (BCP) y Planificación de la Recuperación ante Desastres (DRP)”, y describen la planificación de la continuidad del negocio y la recuperación ante desastres. Este aspecto establece prioridades para la preservación de operaciones y la recuperación de la organización después de una interrupción. El estudio analiza aspectos como la evaluación del riesgo, el análisis del impacto empresarial, así como las estrategias de recuperación, y son muy importantes para el diseño del Plan de Continuidad del Negocio de GADIC SUSCAL, particularmente en la especificación de métodos y procedimientos para la restauración de servicios digitales esenciales.

En el contexto nacional, Santos (2024) en el trabajo “Desarrollo del plan de continuidad de negocio de acuerdo a los estándares vigentes, para el data center de la carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito”, desarrolla un Plan de Continuidad de Negocio para un centro de datos académico, considerando normas como ISO 22301, COBIT e ITIL. El proyecto incluye análisis de impacto al negocio, evaluación de riesgos, identificación de amenazas lógicas, físicas y humanas, así como planes de recuperación de desastres y contingencia. Este antecedente es pertinente porque ofrece una referencia ecuatoriana para estructurar un BCP aplicado a infraestructura tecnológica, lo cual se relaciona con los servicios digitales del GADIC SUSCAL.

A nivel local/provincial, Buscán et al. (2022), en el estudio “Modelo de plan de continuidad de negocio de las Cooperativas segmento B del cantón Cañar”, desarrollaron un modelo de Plan de Continuidad de Negocio para cooperativas de ahorro y crédito del

cantón Cañar. El trabajo tuvo como propósito diseñar un modelo basado en estándares reconocidos para garantizar la continuidad de los servicios ofrecidos por estas instituciones, incluyendo el estudio teórico de normativas, el diagnóstico de la situación actual y la construcción de una herramienta preventiva para responder ante incidentes. Este antecedente es especialmente relevante para el anteproyecto, ya que se desarrolla en el contexto provincial de Cañar y ofrece una referencia cercana para aplicar la continuidad de negocio a servicios tecnológicos e institucionales.

J. METODOLOGÍA

La presente investigación adopta un enfoque mixto. Para el presente caso, los servicios digitales del GADIC SUSCAL serán estudiados desde el enfoque cualitativo, mediante la revisión documental, observación de procesos y levantamiento de información sobre activos tecnológicos, servicios críticos, amenazas, vulnerabilidades y procedimientos existentes. A su vez, se aplicará el enfoque cuantitativo para valorar el nivel de riesgo, impacto, probabilidad, criticidad de los servicios digitales y tiempos objetivos de recuperación. El nivel de investigación es descriptivo, debido a que se caracterizará la situación actual de los servicios digitales y los riesgos que pueden afectar su continuidad. El tipo de investigación es aplicado, puesto que se busca construir una propuesta técnica orientada a resolver una necesidad institucional específica: el diseño de un Plan de Continuidad de Negocio.

Para el análisis de riesgos tecnológicos se podrá emplear una matriz de probabilidad e impacto, complementada con criterios de criticidad de servicios digitales, mientras que el diseño del plan será estructurado con base en los lineamientos de la norma ISO 22301. El proceso metodológico comprenderá tres fases principales: primero, el estudio teórico sobre continuidad de negocio, riesgos tecnológicos, servicios digitales, análisis de impacto al negocio y recuperación ante desastres; segundo, el diagnóstico de la situación actual de los servicios digitales del GADIC SUSCAL; y tercero, el diseño del Plan de Continuidad de Negocio, incorporando estrategias de prevención, respuesta y recuperación, responsables, RTO, RPO y procedimientos para mantener o restablecer los servicios digitales críticos. Para la recolección de datos se utilizará revisión

documental, entrevistas y encuestas dirigidas al personal relacionado con la gestión tecnológica institucional.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						
		I	II	III	IV	V	VI	MEDIOS DE VERIFICACIÓN
1	Realizar el estudio teórico sobre continuidad de negocio, servicios digitales, riesgos tecnológicos, BIA, DRP e ISO 22301.	x	x					Capítulo de conceptos relacionados y trabajos relacionados.
2	Diagnosticar la situación actual de los servicios digitales del GADIC SUSCAL, identificando activos, procesos críticos, amenazas, vulnerabilidades, riesgos y dependencias operativas.		x	x				Informe de diagnóstico, inventario de servicios digitales, matriz de activos y matriz de riesgos.
3	Diseñar el Plan de Continuidad de Negocio basado en ISO 22301, incorporando estrategias de prevención, respuesta, recuperación, responsables, RTO, RPO				x	x	x	Documento técnico del Plan de Continuidad de Negocio para los servicios digitales del GADIC SUSCAL.

	y procedimientos de restablecimiento.							

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

M. PARTICIPANTES	
DIRECTOR:	Ing. Danny Patricio Andrade Cárdenas.
ESTUDIANTE 1	Juan Diego Siguencia Urgiles

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	17 de abril del 2026

Firmas:

Nombre: Ing. Danny Patricio Andrade Cárdenas CC: **Director del Proyecto**	Nombre: Juan Diego Siguencia Urgiles C.C.: 0302335492 **Estudiante / Egresado**

O. APROBACIÓN

Firmas:

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

P. REFERENCIAS

Buscán Pinguil, P. C., Flores Urgilés, C. H., Pinos Castillo, L. F., & Flores Urgilés, C. M. (2022). Modelo de plan de continuidad de negocio de las Cooperativas segmento B del cantón Cañar. Pro Sciences: Revista de Producción, Ciencias e Investigación. https://journalprosciences.com/index.php/ps/article/view/521

Cedergren, A., & Hassel, H. (2024). Building organizational adaptive capacity in the face of crisis: Lessons from a public sector case study. International Journal of Disaster Risk Reduction, 100, Article 104235. https://doi.org/10.1016/j.ijdrr.2023.104235

Cedergren, A., & Hassel, H. (2025). Business continuity management in public sector organizations: Development, challenges, and ways forward. Journal of Contingencies and Crisis Management, 33(2), Article e70055. https://doi.org/10.1111/1468-5973.70055

Contraloría General del Estado. (2023). Normas de Control Interno. https://www.contraloria.gob.ec/WFDescarga.aspx?id=1487&tipo=mul

Dakic, V., Mikulic Premuzic, K., & Petrunic, R. (2024). Business continuity planning (BCP) and disaster recovery planning (DRP). En Proceedings of the 35th DAAAM International Symposium on Intelligent Manufacturing and Automation. DAAAM International. https://daaam.info/35th-proceedings-2024

Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal. (s. f.). Portal institucional del GAD Suscal. Recuperado el 4 de junio de 2026, de https://gadsuscal.gob.ec/

Gobierno del Ecuador. (s. f.). Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal. Gob.EC. Recuperado el 4 de junio de 2026, de https://www.gob.ec/GADIC Suscal

Hassel, H., & Cedergren, A. (2024). A framework for business continuity management in a multiactor context. Journal of Contingencies and Crisis Management, 32(2), Article e12573. https://doi.org/10.1111/1468-5973.12573

International Organization for Standardization. (2018). ISO 31000:2018 Risk management - Guidelines. ISO.

International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements. ISO.

International Organization for Standardization. (2020). ISO 22313:2020 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301. ISO.

International Organization for Standardization. (2021a). ISO/TS 22317:2021 Security and resilience - Business continuity management systems - Guidelines for business impact analysis. ISO.

International Organization for Standardization. (2021b). ISO/TS 22332:2021 Security and resilience - Business continuity management systems - Guidelines for developing business continuity plans and procedures. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2025). ISO/IEC 27031:2025 Cybersecurity - Information and communication technology readiness for business continuity. ISO.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2025). Política Pública para la Transformación Digital del Ecuador 2025-2030. MINTEL. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2025/03/INSTRUMENTO-Politica-Publica-para-la-Transformacion-Digital-Ecuador-2025-2030-MINTEL-signed_f.pdf

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Organisation for Economic Co-operation and Development. (2024). 2023 OECD Digital Government Index: Results and key findings. OECD Publishing. https://doi.org/10.1787/1a89ed5e-en

Religia, A. A., & Utama, D. N. (2024). A novel framework for business continuity plan in public sector organization. Journal of System and Management Sciences, 14(1), 1-14. https://doi.org/10.33168/JSMS.2024.0101

República del Ecuador. (2010). Código Orgánico de Organización Territorial, Autonomía y Descentralización. Registro Oficial.

República del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial.

Santos Rocha, M. S. (2024). Desarrollo del plan de continuidad de negocio de acuerdo a los estándares vigentes, para el data center de la carrera de Computación, de la Universidad Politécnica Salesiana, Sede Quito [Tesis de grado, Universidad Politécnica Salesiana]. Repositorio Institucional UPS. https://dspace.ups.edu.ec/

World Bank. (2022). GovTech Maturity Index, 2022 update: Trends in public sector digital transformation. World Bank. https://www.worldbank.org/en/programs/govtech/gtmi

Anexo A1

Lista de verificación de cumplimiento ISO/IEC 27002 (instrumento A001)

	Gobierno Autónomo Descentralizado Intercultural Participativo del Cantón Suscal	Código: A001 Fecha: 21/07/2026 Versión: 01		
LISTA DE VERIFICACIÓN DE CONTROLES, CLASIFICADOS POR DOMINIOS.				
Dominios - ISO 27002	**CONTROL VERIFICADO**	**SI**	**NO**	**En Proceso**
Políticas de la Seguridad	¿La entidad ha expedido, mediante acto administrativo del Concejo Municipal, un instrumento que recoja formalmente sus políticas de seguridad de la información?	**X**		
	¿La política fue notificada formalmente y puesta en conocimiento de todas las direcciones y unidades del municipio?	**X**		
	¿Se ha fijado una periodicidad de revisión y actualización de la política, o su revisión ante cambios tecnológicos o incidentes relevantes?		**X**	
	¿Se verifica que el personal conozca y comprenda las políticas, más allá de su notificación formal?			**X**
Aspectos organizativos de la Seguridad de la Información.	¿Existe un comité o instancia colegiada de seguridad de la información que impulse y dé soporte a las iniciativas del municipio?		**X**	
	¿Se ha designado formalmente a una unidad o servidor responsable de administrar y custodiar la plataforma tecnológica institucional?	**X**		
	¿Están definidos los propietarios, custodios y responsabilidades sobre los activos de información de cada dependencia municipal?	X		
	¿Se mantienen acuerdos o delegaciones de cooperación con otras entidades del Estado en materia de sistemas e información?	**X**		
	¿Se practican auditorías independientes sobre la implantación de las políticas de seguridad de la información?		X	
	¿Se incorporan cláusulas de seguridad y confidencialidad en los contratos con terceros que acceden a la infraestructura tecnológica?	X		

Seguridad Ligada a los Recursos Humanos.	Ante la desvinculación o cambio de funciones de un servidor, ¿se exige la devolución de los recursos tecnológicos y la revocación de sus accesos?	**X**		
	¿Se suscriben acuerdos de confidencialidad con los servidores que acceden a información reservada?	**X**		
	¿Se ejecuta un programa continuo de capacitación y concienciación en seguridad de la información?			**X**
	¿Conocen los servidores un procedimiento formal para reportar incidentes, debilidades de seguridad o fallos de los sistemas?			**X**
	¿Se han previsto consecuencias disciplinarias frente al incumplimiento de las políticas de seguridad?		X	
Gestión de Activos.	¿Se mantiene un inventario actualizado de los bienes informáticos, con identificación, ubicación y responsable asignado?	**X**		
	¿El inventario distingue los bienes vigentes de aquellos dados de baja u obsoletos?	X		
	¿Existe un esquema institucional de clasificación de la información según su grado de protección?	**X**		
	¿Los controles de protección aplicados guardan correspondencia con el nivel de clasificación asignado?	**X**		
	¿Se han definido procedimientos de etiquetado y manejo de los activos conforme al esquema de clasificación?	X		
	¿Se protegen los soportes de información cuando salen de las instalaciones municipales?	**X**		
	¿Se regula el uso de medios extraíbles (USB, CD/DVD) en los equipos institucionales?	**X**		
	¿La creación de usuarios y la asignación de roles siguen un procedimiento formal con autorización previa?	**X**		
	¿Se han implementado perfiles diferenciados de acceso según el cargo y la dependencia?	**X**		

Control de Accesos.	¿Se revisan y depuran periódicamente los derechos de acceso vigentes de los usuarios?			**X**
	¿Se instruye a los usuarios sobre su responsabilidad en la custodia de las credenciales asignadas?	**X**		
	¿Existe una política de uso aceptable de la red y del servicio de internet institucional?	**X**		
	¿La red se encuentra segmentada de modo que el acceso a los servidores esté restringido respecto del resto del municipio?	**X**		
	¿Se ha segregado el acceso de visitantes respecto de la red institucional?	**X**		
	¿Se dispone de mecanismos de monitoreo que permitan detectar usos irregulares de la red?	**X**		
	¿Se controlan las conexiones remotas hacia la red interna desde fuera de las instalaciones?	**X**		
	¿El municipio cuenta con una política formal de uso de controles criptográficos?		X	
Seguridad Física y Ambiental.	¿El área que aloja los servidores y equipos de comunicaciones cuenta con protección específica frente a incendios, inundaciones u otros siniestros?	X		
	¿Se controla el ingreso de personas a las áreas donde se procesa o almacena información?		X	
	¿La salida de equipos, información o software de las instalaciones requiere autorización previa documentada?	**X**		
	¿Los equipos están protegidos frente a fallos e interrupciones del suministro eléctrico?	**X**		
	¿Los equipos reciben mantenimiento preventivo conforme a las especificaciones del fabricante?	X		
	¿Se aplica borrado seguro a los equipos antes de darlos de baja o reasignarlos a otro usuario?	**X**		
	¿El municipio está preparado para atender oportunamente una falla del cableado estructurado o del backbone de datos?	X		

Seguridad en la Operativa	¿Los procedimientos de operación de la plataforma tecnológica están documentados y disponibles para quienes los requieren?			X
	¿Se dispone de controles para detectar, prevenir y recuperar la operación ante código malicioso?	X		
	¿Los ambientes de desarrollo, pruebas y producción se encuentran separados?	X		
	¿Se ejecutan respaldos de la información conforme a una política definida y se verifica que sean restaurables?	X		
	¿Los respaldos se almacenan en una ubicación distinta de aquella donde reside la información principal?	X		
	¿Se controla la instalación de software en los equipos institucionales?	X		
	¿Existe un procedimiento formal de gestión de cambios sobre la plataforma tecnológica?	X		
	¿Se supervisa el uso de los recursos y se proyecta la capacidad futura de la plataforma?	X		
Seguridad en las Telecomunicaciones	¿Se protege la información que circula por los servicios web institucionales?	X		
	¿La plataforma de red cuenta con protección perimetral frente a la red pública?	X		
	¿Se protege la mensajería electrónica institucional frente a código malicioso y usos indebidos?	X		
	¿El enlace de acceso a internet cuenta con redundancia o con un proveedor alterno?		X	
Gestión de incidentes en la Seguridad de la Información.	¿Se han identificado y documentado las debilidades de seguridad de la información existentes en el municipio?			X
	¿Se registran y valoran los eventos de seguridad para sustentar decisiones y mejoras posteriores?		X	
	¿Se han definido procedimientos para preservar la información que pueda constituir evidencia ante un incidente?			X

Continuidad de las Actividades Institucionales	¿El municipio dispone de un Plan de Continuidad del Negocio formalmente aprobado?		X	
	¿Se ha efectuado un Análisis de Impacto en el Negocio que determine tiempos objetivo de recuperación y puntos de recuperación por servicio?		X	
	¿Se ha previsto la disponibilidad de equipamiento de reemplazo para reanudar la operación ante un desastre físico?	X		
	¿Se realizan pruebas o simulacros periódicos de restauración de los servicios críticos?			X
	¿Se ha conformado un equipo de continuidad con roles, suplentes y datos de contacto actualizados?		X	
Adquisición, Desarrollo y Mantenimiento de Sistemas	¿Se restringe el acceso al código fuente de los aplicativos desarrollados internamente?	X		
	¿Se dispone de herramientas de control de versiones que permitan revertir cambios sobre los aplicativos?	X		
	¿Los nuevos sistemas o versiones se someten a pruebas de aceptación antes de su paso a producción?			X
Cumplimiento	¿El municipio ha adoptado disposiciones para la protección de los datos personales de ciudadanos y servidores?	X		
	¿Se gestiona la legalidad de las licencias de software instaladas en los equipos institucionales?	X		
	¿Se cumple la normativa vigente en materia de archivo, firma electrónica y acceso a la información pública?	X		
	¿Se conserva la documentación electrónica en condiciones que garanticen su autenticidad, integridad y disponibilidad a largo plazo?	X		

El servidor abajo firmante certifica que las respuestas consignadas en el presente instrumento corresponden al estado real de implantación de los controles de seguridad de la información del GADIPCS Suscal a la fecha de verificación, y que fueron contrastadas con la documentación institucional del área de Tecnologías de la Información y Comunicación.

Verificado por: ING. ELMO JOSE VASQUEZ ESPINOZA Cargo: ANALISTA EN TICS

Firma:  **Fecha de verificación: 24 /09 / 2026**

Anexo A2

Matriz de inventario y valoración de activos según MAGERIT v3

El presente anexo contiene el inventario íntegro de activos tecnológicos del GADIC SUSCAL, levantado conforme a la metodología MAGERIT versión 3. La valoración se expresa en las cinco dimensiones de seguridad disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T) en escala de 0 a 10. El valor global corresponde al máximo de las cinco dimensiones. Se consideran críticos los activos con valor global igual o superior a 9.

Código	Tipo	Descripción	Responsable	D	I	C	A	T	Valor
ACT-D-01	backup	Respaldos de la base de datos	No especificado en los documentos	9	9	8	7	7	9
ACT-D-02	conf	Datos de configuración de red	No especificado en los documentos	8	9	8	8	8	9
ACT-D-03	test	Datos del ambiente de pruebas	No especificado en los documentos	5	7	7	6	6	7
ACT-K-01	x509	Certificado SSL WILDCARD	No especificado en los documentos	7	9	8	10	8	10
ACT-S-01	www	Páginas web	No especificado en los documentos	8	8	6	9	7	9
ACT-SW-01	sub	Software y licencias adquiridas	Responsables del inventario de bienes	7	9	8	8	8	9
ACT-SW-02	std.app	Servidor de aplicaciones	No especificado en los documentos	8	9	8	8	8	9
ACT-SW-03	std.dbms	Servidor de base de datos	No especificado en los documentos	9	10	9	8	8	10
ACT-SW-04	std.av	Antivirus Kaspersky KES Select	Responsables del inventario de bienes	7	8	6	7	8	8
ACT-SW-05	std.os	Windows Server 2019	No especificado en los documentos	8	8	7	7	7	8
ACT-SW-06	std.hypervisor	VMware	No especificado en los documentos	9	9	8	8	7	9
ACT-HW-01	mid	Servidores HPE	Responsables del inventario de bienes	9	9	8	8	7	9
ACT-HW-02	vhost	Máquinas virtuales VMware	No especificado en los documentos	9	9	8	8	7	9
ACT-HW-03	backup	Servidor NAS Synology RS1221RP	Responsables del inventario de bienes	8	9	8	7	7	9
ACT-HW-04	pc	Equipos de informática personal	Responsables del inventario de bienes	6	6	7	5	5	7
ACT-HW-05	mobile	Equipos de informática móvil	Responsables del inventario de bienes	6	6	7	5	5	7
ACT-HW-06	peripheral.print	Impresoras	Responsables del inventario de bienes	4	4	4	3	3	4
ACT-HW-07	peripheral.scan	Escáneres y equipos biométricos	Responsables del inventario de bienes	5	6	7	5	5	7
ACT-HW-08	peripheral.cctv	Grabador de video en red (NVR)	Responsables del inventario de bienes	7	7	8	6	7	8
ACT-HW-09	network.switch	Switches Cisco	Responsables del inventario de bienes	9	8	6	6	6	9

Código	Tipo	Descripción	Responsable	D	I	C	A	T	Valor
ACT-HW-10	network.firewall	Firewall	No especificado en los documentos	9	9	9	9	9	9
ACT-HW-11	network.wap	Puntos de acceso inalámbrico	Responsables del inventario de bienes	6	6	7	6	6	7
ACT-HW-12	peripheral (otros)	Equipos audiovisuales, fotográficos y de medició	Responsables del inventario de bienes	4	4	5	4	4	5
ACT-COM-01	LAN	Red interna (12 VLAN)	No especificado en los documentos	9	8	7	6	6	9
ACT-COM-02	wifi	Red inalámbrica	No especificado en los documentos	7	7	7	7	7	7
ACT-COM-03	mobile	Comunicaciones móviles	Responsables del inventario de bienes	5	5	7	6	5	7
ACT-COM-04	Internet	Enlace WAN de Internet (CNT)	No especificado en los documentos	9	7	6	7	7	9
ACT-MEDIA-01	electronic.disk	Discos duros internos y externos	Responsables del inventario de bienes	7	7	8	5	5	8
ACT-MEDIA-02	electronic.vdisk	Discos virtuales	No especificado en los documentos	8	7	7	5	5	8
ACT-MEDIA-03	electronic.san	Almacenamiento en red (NAS)	Responsables del inventario de bienes	8	8	8	6	6	8
ACT-AUX-01	ups	UPS / sistemas de alimentación ininterrumpida	Responsables del inventario de bienes	8	3	2	2	2	8
ACT-AUX-02	cabling.wire	Reguladores y transformadores de voltaje	Responsables del inventario de bienes	6	3	2	2	2	6
ACT-AUX-03	furniture	Racks	Responsables del inventario de bienes	7	5	5	4	4	7
ACT-L-01	building	Edificio Municipal	No especificado en los documentos	8	5	6	4	5	8
ACT-L-02	local	Centro Prioritario	No especificado en los documentos	6	5	5	4	4	6
ACT-P-01	ui	Funcionarios responsables de los bienes informát	Dirección de Gestión Administrativa	6	6	7	5	5	7

Fuente: Dirección de TIC del GADIC SUSCAL (2026). Total: 36 activos, de los cuales 15 alcanzan la condición de críticos.

Anexo B

Plan de Continuidad del Negocio del GADIC SUSCAL (PCN-GADIC SUSCAL-001)

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y

PARTICIPATIVO DEL CANTÓN SUSCAL

Dirección de Tecnologías de la Información y Comunicación

PLAN DE CONTINUIDAD DEL NEGOCIO PARA LOS SERVICIOS DIGITALES

Código del documento: PCN-GADIC SUSCAL-001

Versión: 01

Cantón Suscal, provincia del Cañar — Ecuador

Documento elaborado en el marco del trabajo de titulación "Plan de Continuidad de Negocio basado en la norma ISO 22301 para los servicios digitales del GADIPC Suscal", Universidad Católica de Cuenca, sede Cañar.

Control del documento

Versión	Fecha	Descripción del cambio	Elaborado por
01	__/__/____	Emisión inicial del Plan de Continuidad del Negocio	Dirección de TIC

Aprobación

Acción	Nombre	Cargo	Firma
Elaborado por		Responsable de TIC	
Revisado por		Director/a Administrativo/a	
Aprobado por		Alcalde/sa del cantón Suscal	

El presente plan entra en vigencia a partir de su aprobación mediante el acto administrativo correspondiente y deberá ser revisado con periodicidad anual.

Distribución

Destinatario	Medio de entrega
Alcaldía	Copia digital y física
Dirección Administrativa	Copia digital y física
Dirección de TIC	Copia digital y física (original)
Unidad de Comunicación Social	Copia digital

1. Objetivo

El presente Plan de Continuidad del Negocio establece las disposiciones, estrategias, roles y procedimientos que el Gobierno Autónomo Descentralizado Intercultural y Participativo del Cantón Suscal aplicará para mantener o restablecer sus servicios digitales críticos ante la ocurrencia de un incidente disruptivo, dentro de los tiempos objetivo definidos en este documento.

El plan se formula conforme a la norma ISO 22301:2019, Seguridad y resiliencia, Sistemas de gestión de la continuidad del negocio y constituye un instrumento de gestión institucional de observancia obligatoria para los servidores comprendidos en su alcance.

2. Alcance

El plan aplica a los siguientes servicios digitales institucionales y a la infraestructura tecnológica que los soporta:

- Sistema de recaudación tributaria.
- Registro de la propiedad.
- Sistema de catastros y avalúos.
- Portal web institucional y formularios en línea.
- Servicios de transparencia y acceso a la información pública.

Comprende los quince activos tecnológicos calificados como críticos en el inventario institucional y al personal de la Dirección de TIC responsable de su operación.

Quedan excluidos los procesos administrativos que no se soportan en medios digitales y los servicios prestados por terceros sobre los cuales la institución no ejerce control técnico directo, sin perjuicio de los niveles de servicio que deban exigirse contractualmente.

3. Marco normativo

- ISO 22301:2019 Sistemas de gestión de la continuidad del negocio. Requisitos.
- ISO/TS 22317:2021 Directrices para el análisis de impacto en el negocio.
- ISO/TS 22332:2021 Directrices para el desarrollo de planes y procedimientos de continuidad.
- ISO/IEC 27031 Preparación de las tecnologías de la información y comunicación para la continuidad del negocio.
- ISO/IEC 27002 Controles de seguridad de la información.
- MAGERIT versión 3 Metodología de análisis y gestión de riesgos de los sistemas de información.
- Normas de Control Interno de la Contraloría General del Estado, grupo 410, Tecnología de la Información.
- Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD).

4. Términos y definiciones

Término	Definición
MTPD	Período máximo tolerable de disrupción. Tiempo transcurrido el cual el impacto de la interrupción resulta inaceptable para la institución.
RTO	Tiempo objetivo de recuperación. Plazo dentro del cual un servicio debe ser restablecido tras una interrupción. Es siempre inferior al MTPD.
RPO	Punto objetivo de recuperación. Máxima pérdida de información admisible, expresada como la antigüedad del último respaldo utilizable.
Incidente disruptivo	Evento que interrumpe o degrada la prestación de uno o más servicios digitales institucionales.
Activación del plan	Decisión formal de aplicar los procedimientos previstos en este documento, adoptada por el Coordinador del PCN.
Operación degradada	Modalidad de atención con procedimientos manuales o alternos mientras dura la interrupción del servicio automatizado.
Normalización	Declaración formal de que el servicio ha sido restablecido y validado con el área usuaria.

5. Equipo de Continuidad del Negocio

5.1 Conformación y responsabilidades

Se conforma el Equipo de Continuidad del Negocio con la siguiente estructura. Cada rol cuenta con un suplente que asume sus funciones en caso de ausencia o imposibilidad de contacto.

Rol	Cargo asignado	Responsabilidades	Suplente
Coordinador del PCN	Responsable de TIC	Declara la activación del plan, asigna el nivel de severidad, dirige la respuesta, autoriza el cierre del incidente y declara la normalización.	Director/a Administrativo/a
Responsable técnico	Técnico de soporte de TIC	Ejecuta los procedimientos de recuperación, restaura respaldos, verifica la integridad de la información y registra los tiempos alcanzados.	Responsable de TIC
Enlace institucional	Director/a Administrativo/a	Coordina con las áreas afectadas, activa los procedimientos de operación degradada y gestiona los recursos requeridos.	Secretario/a General
Responsable de comunicación	Unidad de Comunicación Social	Informa a la ciudadanía y a los organismos de control conforme al esquema de comunicación del capítulo 11.	Enlace institucional

La designación nominal de los servidores que ocupan cada rol se formaliza mediante el acto administrativo de aprobación del presente plan y se registra en el Formato F-06, Directorio de contactos del Equipo de Continuidad.

5.2 Obligación de documentación

Los procedimientos técnicos de recuperación deberán estar documentados de modo que resulten ejecutables por un servidor distinto de quien los diseñó. La Dirección de TIC mantendrá actualizada dicha documentación y la custodiará en una ubicación accesible al Equipo de Continuidad, independiente de los sistemas cuya recuperación se persigue.

6. Riesgos identificados sobre los activos críticos

El análisis de riesgos se realizó conforme a la metodología MAGERIT versión 3 sobre los quince activos que alcanzaron un valor global igual o superior a 9 en la valoración institucional. El riesgo se calcula como el producto de la probabilidad por el impacto, en escalas de cinco niveles.

Código	Activo	Amenaza principal	P	I	Riesgo
ACT-HW-10	Firewall	[A.11] Acceso no autorizado	4	5	20 — Crítico
ACT-COM-04	Enlace WAN de Internet	[I.8] Fallo de servicios de comunicaciones	4	4	16 — Alto
ACT-SW-03	Servidor de base de datos	[E.1] Errores de administración	3	5	15 — Alto
ACT-D-01	Respaldos de la base de datos	[E.2] Errores del administrador de respaldos	3	5	15 — Alto
ACT-HW-01	Servidores HPE	[I.5] Avería de origen físico o lógico	3	5	15 — Alto
ACT-K-01	Certificado SSL Wildcard	[E.28] Caducidad no controlada	3	5	15 — Alto
ACT-HW-02	Máquinas virtuales VMware	[E.24] Agotamiento de recursos	3	4	12 — Medio
ACT-HW-03	Servidor NAS Synology	[I.5] Avería de origen físico o lógico	3	4	12 — Medio
ACT-HW-09	Switches Cisco	[I.6] Corte del suministro eléctrico	3	4	12 — Medio
ACT-SW-02	Servidor de aplicaciones	[A.7] Uso no previsto	3	4	12 — Medio
ACT-S-01	Páginas web institucionales	[A.24] Denegación de servicio	3	4	12 — Medio
ACT-D-02	Datos de configuración de red	[E.1] Errores de administración	3	4	12 — Medio
ACT-SW-06	VMware	[I.5] Avería de origen físico o lógico	2	5	10 — Medio
ACT-COM-01	Red interna (12 VLAN)	[E.9] Errores de reencaminamiento	2	4	8 — Medio
ACT-SW-01	Software y licencias	[E.28] Caducidad no controlada	2	3	6 — Bajo

7. Parámetros de recuperación de los servicios

Los siguientes parámetros constituyen el compromiso institucional de recuperación y son de obligatoria observancia para el Equipo de Continuidad.

Código	Servicio digital	Impacto	MTPD	RTO	RPO	Prioridad
SD-01	Sistema de recaudación tributaria	Muy alto	24 h	8 h	4 h	1
SD-02	Registro de la propiedad	Alto	48 h	24 h	8 h	2
SD-03	Sistema de catastros y avalúos	Alto	72 h	24 h	12 h	3
SD-04	Portal web y formularios en línea	Medio	72 h	48 h	24 h	4
SD-05	Servicios de transparencia	Medio	120 h	72 h	24 h	5

El orden de prioridad determina la secuencia de recuperación cuando la interrupción afecte simultáneamente a varios servicios.

7.1 Recursos mínimos y dependencias

Servicio	Recursos mínimos requeridos	Dependencias externas
SD-01	Servidor de base de datos, servidor de aplicaciones, red interna, enlace WAN, responsable técnico	Proveedor de conectividad; suministro eléctrico
SD-02	Servidor de base de datos, servidor de aplicaciones, red interna	Sistema nacional de registro
SD-03	Servidor de base de datos, almacenamiento NAS, red interna	Cartografía institucional
SD-04	Servidor web, certificado SSL, enlace WAN, firewall	Proveedor de conectividad
SD-05	Servidor web, enlace WAN	Portal de transparencia nacional

8. Estrategias de continuidad

Servicio	Prevención	Respuesta	Recuperación
SD-01	Respaldo incremental cada 4 horas verificado; monitoreo de disponibilidad; mantenimiento preventivo trimestral	Habilitación de caja recaudadora en modalidad manual con registro diferido	Restauración sobre servidor virtual alterno y conciliación de las transacciones diferidas
SD-02	Respaldo diario verificado; control de cambios sobre la base de datos	Suspensión temporal de inscripciones con registro en bitácora física	Restauración de la base de datos y validación de integridad registral
SD-03	Respaldo diario; réplica del almacenamiento en NAS	Emisión manual de certificados sobre el último respaldo disponible	Restauración del servicio y actualización de la información catastral
SD-04	Monitoreo de disponibilidad; control de vencimiento del certificado SSL;	Aviso institucional en redes sociales y atención presencial	Redespliegue del portal y verificación de formularios en línea

Servicio	Prevención	Respuesta	Recuperación
	protección ante denegación de servicio		
SD-05	Respaldo semanal de los contenidos publicados	Comunicación formal al organismo de control sobre la indisponibilidad	Republicación conforme al calendario de transparencia

Los procedimientos de operación degradada previstos en la columna de respuesta deben aplicarse con registro documental íntegro, a efectos de permitir la posterior conciliación con los sistemas una vez restablecidos.

9. Niveles de severidad y activación del plan

No toda incidencia técnica motiva la activación del plan. El Coordinador del PCN asigna el nivel de severidad conforme a los siguientes criterios:

Nivel	Criterio	Acción	Decide
1 — Menor	Degradación de un servicio no crítico o interrupción inferior a 2 horas	No se activa el plan. Se registra en el Formato F-01	Responsable técnico
2 — Mayor	Interrupción de un servicio crítico con duración estimada superior al 50% de su RTO	Activación parcial y convocatoria del Equipo de Continuidad	Coordinador del PCN
3 — Crítico	Interrupción simultánea de dos o más servicios críticos, pérdida de información o compromiso del perímetro de seguridad	Activación total y notificación a la máxima autoridad	Coordinador del PCN y máxima autoridad

10. Procedimiento de respuesta y recuperación

Fase	Actividades
Fase 1. Detección	Identificación del evento mediante monitoreo o reporte de usuario. Registro inmediato en el Formato F-01 con fecha, hora y servicio afectado. Notificación al Coordinador del PCN.
Fase 2. Evaluación	Determinación del servicio afectado y de la causa aparente; estimación de la duración de la interrupción; asignación del nivel de severidad; decisión de activación mediante el Formato F-02.
Fase 3. Contención	Aplicación de las medidas necesarias para impedir la propagación del incidente; aislamiento del componente afectado cuando corresponda; activación de los procedimientos de operación degradada previstos en el capítulo 8.
Fase 4. Recuperación	Ejecución de los procedimientos técnicos del capítulo 10.1 según el servicio afectado; restauración de respaldos; verificación de la integridad de la información restablecida; registro de tiempos en el Formato F-03.
Fase 5. Cierre	Validación funcional con el área usuaria; conciliación de las transacciones registradas manualmente; declaración de normalización mediante el Formato F-04; registro de lecciones aprendidas.

10.1 Procedimientos específicos por servicio

SD-01 — Sistema de recaudación tributaria (RTO 8 h / RPO 4 h)

- â¢ Verificar el estado del servidor de base de datos y del servidor de aplicaciones.
- â¢ De persistir la indisponibilidad, notificar al Enlace institucional la activación de la caja recaudadora manual.
- â¢ Identificar el último respaldo válido con antigüedad no superior a 4 horas.
- â¢ Restaurar la base de datos sobre la máquina virtual alterna y verificar la integridad de las tablas transaccionales.
- â¢ Publicar el servicio, ejecutar una transacción de prueba y validar con la Dirección Financiera.
- â¢ Conciliar e ingresar las transacciones registradas manualmente durante la contingencia.

SD-02 y SD-03 — Registro de la propiedad y catastros (RTO 24 h)

- â¢ Suspender las inscripciones y emisiones, y habilitar la bitácora física de atención.
- â¢ Restaurar la base de datos desde el último respaldo diario verificado.
- â¢ Validar la integridad registral y la correspondencia de los folios con la bitácora física.
- â¢ Reanudar el servicio e incorporar los registros diferidos.

SD-04 y SD-05 — Portal web, formularios y transparencia (RTO 48 h y 72 h)

- â¢ Comprobar la vigencia del certificado SSL y el estado del enlace WAN.
- â¢ Verificar las reglas del firewall perimetral y descartar un evento de denegación de servicio.
- â¢ Redesplegar el sitio desde el último respaldo y verificar los formularios en línea.
- â¢ Publicar el aviso de restablecimiento y, cuando corresponda, comunicar al organismo de control.

11. Comunicación

Destinatario	Contenido	Responsable	Oportunidad
Áreas afectadas	Servicio interrumpido, procedimiento de operación degradada aplicable y tiempo estimado de restablecimiento	Enlace institucional	Inmediata
Ciudadanía	Aviso de indisponibilidad y canales alternos de atención	Responsable de comunicación	Interrupción superior a 4 horas en servicios de atención directa
Máxima autoridad	Reporte del incidente, severidad y acciones adoptadas	Coordinador del PCN	Incidentes de nivel 2 y 3
Organismos de control	Comunicación formal de la indisponibilidad y de las medidas adoptadas	Coordinador del PCN	Incidentes de nivel 3 o incumplimiento de plazos legales

12. Programa de pruebas y ejercicios

La Dirección de TIC ejecutará anualmente el siguiente programa. Cada ejercicio genera un informe en el Formato F-05 con los tiempos alcanzados, las desviaciones respecto de los parámetros comprometidos y las acciones correctivas derivadas.

Tipo de prueba	Frecuencia	Objetivo	Responsable
Prueba de restauración de respaldos	Trimestral	Verificar que los respaldos son restaurables dentro del RPO comprometido	Responsable técnico
Ejercicio de mesa	Semestral	Revisar la comprensión de roles y procedimientos ante un escenario simulado	Equipo de Continuidad
Simulacro de conmutación de enlace	Semestral	Comprobar la operatividad del enlace secundario de conectividad	Responsable técnico
Simulacro funcional de recuperación	Anual	Ejecutar la recuperación completa del servicio SD-01 midiendo el RTO real	Equipo de Continuidad

13. Mantenimiento y mejora continua

El plan será revisado de forma ordinaria una vez al año por el Coordinador del PCN, comprendiendo la verificación del inventario de activos, la revisión de los parámetros de recuperación y la actualización de la asignación de roles y contactos.

Procederá revisión extraordinaria en los siguientes supuestos:

- â□ ¢ Ocurrencia de un incidente de nivel 3.
- â□ ¢ Incorporación de un nuevo servicio digital al alcance del plan.
- â□ ¢ Cambio sustancial en la infraestructura tecnológica institucional.
- â□ ¢ Modificación de la estructura orgánica que afecte los roles definidos.

Las acciones correctivas derivadas de los ejercicios y de los incidentes reales se incorporarán formalmente al plan y se comunicarán al Equipo de Continuidad, conforme al ciclo de mejora continua previsto en la cláusula 10 de la norma ISO 22301:2019.

14. Formatos anexos al plan

Código	Formato	Momento de uso
F-01	Registro de incidentes	Detección de cualquier evento disruptivo
F-02	Acta de activación del plan	Decisión de activación (niveles 2 y 3)
F-03	Bitácora de recuperación	Durante la ejecución de la recuperación
F-04	Acta de declaración de normalización	Cierre del incidente
F-05	Informe de ejercicio o prueba	Tras cada prueba programada

Código	Formato	Momento de uso
F-06	Directorio de contactos del Equipo de Continuidad	Actualización semestral
F-07	Registro de pruebas de restauración de respaldos	Cada prueba trimestral

Los formatos se encuentran en el documento "Formatos operativos del Plan de Continuidad del Negocio", código PCN-GADIC SUSCAL-002.

Anexo C

Formatos operativos del Plan de Continuidad del Negocio (PCN-GADIC SUSCAL-002)

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PARTICIPATIVO DEL CANTÓN SUSCAL

Dirección de Tecnologías de la Información y Comunicación

FORMATOS OPERATIVOS DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Código del documento: PCN-GADIC SUSCAL-002

Versión: 01

Cantón Suscal, provincia del Cañar — Ecuador

Documento elaborado en el marco del trabajo de titulación "Plan de Continuidad de Negocio basado en la norma ISO 22301 para los servicios digitales del GADIPC Suscal", Universidad Católica de Cuenca, sede Cañar.

F-01 — Registro de incidentes

Propósito: documentar todo evento disruptivo, se active o no el plan.

N.º de registro	
Fecha y hora de detección	
Detectado por	
Medio de detección	Monitoreo ( ) Reporte de usuario ( ) Otro ( )
Servicio(s) afectado(s)	SD-01 ( ) SD-02 ( ) SD-03 ( ) SD-04 ( ) SD-05 ( )
Activo(s) involucrado(s)	
Descripción del evento	
Nivel de severidad asignado	Nivel 1 ( ) Nivel 2 ( ) Nivel 3 ( )
¿Se activa el plan?	Sí ( ) No ( )
Acciones inmediatas adoptadas	
Hora de restablecimiento	
Duración total de la interrupción	
RTO comprometido / RTO real	
Registrado por (nombre y firma)	

F-02 — Acta de activación del Plan de Continuidad

Propósito: dejar constancia formal de la decisión de activar el plan en incidentes de nivel 2 o 3.

Acta N.º	
Fecha y hora de activación	
Incidente asociado (F-01 N.º)	
Nivel de severidad	
Servicios comprometidos	
Tipo de activación	Parcial ( ) Total ( )
Miembros del equipo convocados	
Procedimientos de operación degradada activados	
Tiempo estimado de restablecimiento	
Coordinador del PCN (nombre y firma)	
Notificación a la máxima autoridad	Sí ( ) No aplica ( ) Hora: _____

F-03 — Bitácora de recuperación

Propósito: registrar cronológicamente las acciones ejecutadas durante la recuperación.

Incidente asociado (F-01 N.º)	
Servicio en recuperación	
Responsable técnico a cargo	
Respaldo utilizado (fecha y hora)	
Antigüedad del respaldo / RPO comprometido	

Hora	Acción ejecutada	Resultado obtenido	Ejecutado por

F-04 — Acta de declaración de normalización

Propósito: certificar el restablecimiento del servicio y el cierre formal del incidente.

Acta N.º	
Incidente asociado (F-01 N.º)	
Servicio restablecido	
Fecha y hora de restablecimiento	
Duración total de la interrupción	
RTO comprometido / RTO real	
¿Se cumplió el RTO?	Sí ( ) No ( ) Justificación: _____
Pérdida de información verificada	Ninguna ( ) Sí ( ) Alcance: _____
Validación funcional del área usuaria	Área: _____ Responsable: _____
Conciliación de registros manuales	Concluida ( ) Pendiente ( ) No aplica ( )
Lecciones aprendidas	
Acciones correctivas propuestas	
Coordinador del PCN (nombre y firma)	

F-05 — Informe de ejercicio o prueba

Propósito: documentar los resultados de cada prueba del programa anual.

Informe N.º	
Tipo de prueba	Restauración ( ) Mesa ( ) Conmutación ( ) Simulacro funcional ( )
Fecha de ejecución	
Servicio o componente probado	
Escenario simulado	
Participantes	
Objetivo de la prueba	
Tiempo objetivo comprometido	
Tiempo real alcanzado	
Desviación observada	
Dificultades identificadas	
Acciones correctivas	
Responsable del seguimiento	
Fecha comprometida de cierre	

F-06 — Directorio de contactos del Equipo de Continuidad

Propósito: mantener disponibles los datos de contacto del equipo. Actualización semestral obligatoria.

Rol	Nombre	Cargo	Teléfono	Correo institucional
Coordinador del PCN				
Suplente del Coordinador				
Responsable técnico				
Suplente técnico				
Enlace institucional				
Suplente de enlace				
Responsable de comunicación				
Proveedor de conectividad				
Soporte de hardware				

Última actualización: ____/ ____/ _____ Responsable: _____

F-07 — Registro de pruebas de restauración de respaldos

Propósito: evidenciar la ejecución trimestral de pruebas de restauración y la verificación del RPO.

Fecha	Servicio	Respaldo probado	Tiempo de restauración	¿Íntegro?	Ejecutado por
				Sí ( ) No ( )	
				Sí ( ) No ( )	
				Sí ( ) No ( )	
				Sí ( ) No ( )	

Anexo D

Ficha de validación técnica de los parámetros de continuidad (instrumento A002)

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PARTICIPATIVO DEL CANTÓN SUSCAL

Trabajo de titulación — Universidad Católica de Cuenca, sede Cañar

FICHA DE VALIDACIÓN TÉCNICA DE LOS PARÁMETROS DE CONTINUIDAD

Código del documento: A002

Versión: 01

Cantón Suscal, provincia del Cañar — Ecuador

Documento elaborado en el marco del trabajo de titulación "Plan de Continuidad de Negocio basado en la norma ISO 22301 para los servicios digitales del GADIPCS Suscal", Universidad Católica de Cuenca, sede Cañar.

1. Objeto de la ficha

El presente instrumento tiene por objeto obtener la validación del responsable del área de Tecnologías de la Información y Comunicación del GADIPCS Suscal respecto de los parámetros de recuperación, las estrategias de continuidad y la asignación de roles propuestos en el Plan de Continuidad del Negocio, a fin de verificar su viabilidad técnica y operativa.

Fecha de aplicación	24/09/2026
Nombre del informante	ELMO VASQUEZ E.
Cargo	ANALISTA EN TICS
Años en el cargo	11
Aplicado por	

2. Validación de los parámetros de recuperación

Rol propuesto	Cargo asignado	¿Procede?	Cargo alterno sugerido

Coordinador del PCN	Responsable de TIC	Si ( ) No (X)	

Para cada servicio, indique si los valores propuestos son alcanzables con la capacidad instalada. En caso negativo, consigne el valor que considera realista.

Cód.	Servicio	MTPD	RTO	RPO	¿Alcanzable?	Valor propuesto por el informante
SD-01	Recaudación tributaria	24 h	8 h	4 h	Sí (X) No ( )	4 h
SD-02	Registro de la propiedad	48 h	24 h	8 h	Sí (X) No ( )	8 h
SD-03	Catastros y avalúos	72 h	24 h	12 h	Sí (X) No ( )	12 h
SD-04	Portal web y formularios	72 h	48 h	24 h	Sí (X) No ( )	24 h
SD-05	Servicios de transparencia	120 h	72 h	24 h	Sí (X) No ( )	24 h

3. Preguntas de verificación

3.1 ¿Con qué frecuencia se ejecutan actualmente los respaldos de la base de datos?	DIARIOS
3.2 ¿Los respaldos se verifican mediante pruebas de restauración? ¿Con qué periodicidad?	SERVIDORES DE PRUEBAS
3.3 ¿Cuánto tiempo tomó la última restauración efectivamente realizada?	5 MINUTOS
3.4 ¿Existe capacidad para levantar una máquina virtual alterna del sistema de recaudación?	SI
3.5 ¿La institución dispone o puede contratar un enlace de conectividad secundario?	SI
3.6 ¿Cuántos servidores conforman el área de TIC y cuáles son sus funciones?	3 FISICOS 7 VIRTUALES, BASE DE DATOS, APLICACIONES
3.7 ¿Existe designación formal de propietarios o custodios de los activos lógicos?	SI
3.8 ¿Se ha registrado algún incidente disruptivo en los últimos 24 meses? Descríbalo.	NO

4. Validación de la estructura de roles

Rol propuesto	Cargo asignado	¿Procede?	Cargo alterno sugerido
Responsable técnico	Técnico de soporte de TIC	Si (X) No ( )	
Enlace institucional	Director/a Administrativo/a	Si (X) No ( )	
Responsable de comunicación	Comunicación Social	Si ( ) No (X)	

5. Observaciones generales

Observaciones	

Declaro que la información consignada corresponde a la situación real del área de Tecnologías de la Información y Comunicación del GADIPCS Suscal.

Validez documento en Firmadi. Firmado electrónicamente por: ELMO JOSE VASQUEZ ESPINOZA	
Firma del informante	Firma del investigador

Anexo E

Solicitud de autorización institucional

Suscal, _____de _____de 2026

Ing.- Luis Pomaquiza Castro

Alcalde del cantón Suscal

GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL Y PARTICIPATIVO DEL CANTÓN SUSCAL

Presente.-

De mi consideración:

Yo, Juan Diego Siguencia Urgiles, portador de la cédula de ciudadanía N.º 0302335492, estudiante de la carrera de Ingeniería de Sistemas de la Universidad Católica de Cuenca, sede Cañar, me dirijo a usted con la finalidad de solicitar la autorización correspondiente para desarrollar el trabajo de titulación denominado "Plan de Continuidad de Negocio basado en la norma ISO 22301 para los servicios digitales del GADIPC SUSCAL".

El estudio tiene por objeto diseñar un plan que permita a la institución mantener o restablecer sus servicios digitales críticos ante incidentes disruptivos. Para su desarrollo se requiere el acceso a la documentación técnica del área de Tecnologías de la Información y Comunicación inventario de bienes informáticos y descripción de la infraestructura tecnológica y la colaboración del servidor responsable de dicha área para la verificación de los controles de seguridad y de los parámetros de recuperación.

Me comprometo a dar tratamiento estrictamente académico y confidencial a la información proporcionada, a no divulgar datos que puedan comprometer la seguridad de la plataforma tecnológica institucional, y a entregar a la institución un ejemplar del plan resultante, que podrá adoptar mediante el acto administrativo que estime pertinente.

Por la favorable acogida que sepa dar a la presente, anticipo mi agradecimiento.

Atentamente,

_____

Juan Diego Siguencia Urgiles

C.I. 0302335492

AUTORIZACIÓN INSTITUCIONAL

Se autoriza al peticionario el desarrollo del trabajo de titulación en los términos solicitados, disponiendo a la Dirección de Tecnologías de la Información y Comunicación brindar las facilidades del caso.

_____	_____
Alcalde/sa del cantón Suscal	Responsable de TIC

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Juan Diego Siguencia Urgiles portador de la cédula de ciudadanía N.º **0302335492** En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"Plan de continuidad de negocios basada en la norma ISO 22301 para los servicios digitales del GADIC Suscal"** 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, 29 de septiembre 2026



Juan Diego Siguencia Urgiles

C.I. 0302335492