UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PROPUESTA PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN EL ÁMBITO DE TI PARA EMMAIPC-EP DEL CANTÓN CAÑAR , BASADO EN LA NORMA ISO 22301

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

AUTOR: JULIO CÉSAR PINGUIL SIMBAINA.

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

PROPUESTA PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO EN EL ÁMBITO DE TI PARA EMMAIPC-EP DEL CANTÓN CAÑAR, BASADO EN LA NORMA ISO 22301

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

AUTOR: JULIO CÉSAR PINGUIL SIMBAINA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2024

PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Julio César Pinguil Simbaina portador de la cédula de ciudadanía **Nº** 0302422696. Declaro ser el autor de la obra: **Propuesta para la gestión de continuidad del negocio en el ámbito de TI para EMMAIPC-EP del cantón Cañar**, **basado en la norma ISO 22301** sobre la cual me hago responsable sobre sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 18 de noviembre de 2024

Julio César Pinguil Simbaina

C.I: 0302422696

CERTIFICACIÓN PREVIA REVISIÓN DE LECTORES

Cañar, 24 de septiembre del 2024

En mi calidad de Director del Trabajo de Titulación: **Propuesta para la gestión de continuidad del negocio en el ámbito de TI para EMMAIPC-EP del cantón Cañar**, **basado en la norma ISO 22301** elaborado por Julio César Pinguil Simbaina portador de la cédula de ciudadanía Nº 0302422696, estudiante de la Carrera de Ingeniería en Sistemas en la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica;

Certifico:

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

Ing. Cristhian Flores Urgilés, Mgs

DIRECTOR DEL TRABAJO INVESTIGATIVO

DEDICATORIA

Con amor y gratitud, dedico este trabajo a las personas más importantes de mi vida, quienes han sido mi inspiración y fortaleza en cada paso de este camino.

A mi padre Juan Pinguil, por su ejemplo de esfuerzo y perseverancia, y a mi madre Cecilia Simbaina, por su amor incondicional, sus consejos y por enseñarme que los sueños se alcanzan con dedicación y sacrificio.

A mis hijos Jadiel Pinguil y Judith, quienes representan la razón de mi esfuerzo y mi mayor motivación para ser mejor cada día.

A mis hermanos Aurora Pinguil, Mirian Pinguil, Juan Pinguil y Jorge Pinguil, quienes han compartido conmigo momentos difíciles y alegres, brindándome siempre su apoyo incondicional.

A cada uno de ustedes, gracias por ser mi pilar y fuente de inspiración. Sin su amor y aliento constante, este logro no habría sido posible.

AGRADECIMIENTO

Con gratitud y humildad, quiero expresar mi sincero agradecimiento a todas las personas e instituciones que contribuyeron a la culminación de esta etapa importante de mi vida.

En primer lugar, agradezco profundamente a Dios, quien me ha dado la fortaleza y sabiduría para superar los desafíos y avanzar con determinación.

A mi tutor, Ing. Cristhian Flores, por su valiosa orientación, paciencia y compromiso durante todo el proceso de elaboración de esta tesis. Sus conocimientos y consejos fueron fundamentales para alcanzar los objetivos planteados.

Extiendo mi agradecimiento a los docentes de la carrera de Ingeniería en Sistemas de Información, quienes, a lo largo de estos años de formación, compartieron su experiencia y conocimientos, ayudándome a crecer tanto profesional como personalmente. Su dedicación y pasión por la enseñanza son un ejemplo inspirador.

Finalmente, agradezco a mi familia y amigos por su apoyo incondicional, especialmente en los momentos difíciles. Gracias por creer en mí y motivarme a seguir adelante. Este logro es también de ustedes.

RESUMEN

El presente trabajo de tesis aborda la gestión de la continuidad del negocio en el área de TI de EMMAIPC-EP, enfocándose en garantizar la resiliencia operativa ante posibles interrupciones. Los objetivos específicos incluyen diagnosticar el estado actual de la infraestructura de TI y las prácticas de continuidad del negocio, elaborar un marco de gestión de riesgos de TI que identifique y priorice amenazas, y diseñar un plan de acción para la implementación de estrategias de recuperación de desastres y continuidad del negocio que sean prácticas, escalables y sostenibles. La metodología utilizada fue de carácter descriptivo y evaluativo, combinando un análisis cualitativo de la situación actual con un enfoque cuantitativo para medir el impacto de los riesgos identificados. Se realizó un diagnóstico exhaustivo de la infraestructura de TI y de las prácticas de gestión actuales mediante encuestas y entrevistas al personal clave, lo que permitió identificar deficiencias críticas en la preparación para la continuidad operativa. Con base en estos hallazgos, se desarrolló un marco de gestión de riesgos de TI alineado con estándares internacionales, y se diseñó un plan de acción específico que incluye estrategias de recuperación escalables y sostenibles. El resultado de esta investigación proporciona a EMMAIPC-EP una base sólida para fortalecer su capacidad de respuesta ante incidentes, asegurando la continuidad de sus operaciones críticas y protegiendo sus activos más valiosos en situaciones de crisis.

Palabras Clave: continuidad del negocio, gestión de riesgos, infraestructura de TI.

ABSTRACT

This thesis addresses business continuity management in the IT department of EMMAIPC-EP, focusing on ensuring operational resilience in the event of possible disruptions. The specific objectives include diagnosing the current state of IT infrastructure and business continuity practices, developing an IT risk management framework that identifies and prioritizes threats, and designing an action plan for implementing practical, scalable, and sustainable disaster recovery and business continuity strategies. The methodology used was descriptive and evaluative, combining qualitative analysis of the current situation with a quantitative approach to measure the impact of the identified risks. A comprehensive diagnosis of the IT infrastructure and current management practices was conducted through surveys and interviews with key personnel, which helped identify critical deficiencies in the preparedness for operational continuity. Based on these findings, an IT risk management framework aligned with international standards was developed, and a specific action plan was designed, including scalable and sustainable recovery strategies. The results of this investigation provide EMMAIPC-EP with a solid foundation to strengthen its incident response capabilities, ensuring the continuity of its critical operations and protecting its most valuable assets in crises.

***Keywords*:** business continuity, risk management, IT infrastructure.

INDICE

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD 3
CERTIFICACIÓN PREVIA REVISIÓN DE LECTORES 4
DEDICATORIA 5
AGRADECIMIENTO 6
RESUMEN 7
ABSTRACT 8
INTRODUCCIÓN 13
CAPÍTULO I 14
MARCO REFERENCIAL 14
1. Planteamiento del problema 14
1.1. Formulación del problema 15
1.2. Antecedentes de la Investigación 15
1.3. Justificación de la investigación 16
1.4. Objetivos 17
1.4.1. Objetivo General 17
1.4.2. Objetivos Específicos 17
1.5. Limitaciones 17
1.6. Delimitaciones 17
CAPÍTULO II 19
MARCO TEÓRICO 19
2.1. Plan de continuidad de negocio (BCP) 19
2.2. Plan de Recuperación de Desastres (DRP) 19
2.3. Gestión de Riesgos de TI 20
2.3.1. Amenazas de TI 21
2.3.2. Vulnerabilidades de TI 21
2.3.3. Riesgos de TI 21
2.4. Metodologías de Gestión de Riesgos Informáticos 22
2.4.1. OCTAVE 22
2.4.2. MAGERIT 24
2.4.3. ISO 27005 25
2.4.4. CRAMM 27
2.4.5. Matriz comparativa de las metodologías de Gestión de Riesgos Informáticos 28

2.5.1. Desafíos en las tecnologías de la Información 29
2.6. Resiliencia Organizacional 30
2.6.1. Componentes de la Resiliencia Organizacional 30
2.7. Normativas y Estándares Relevantes para la Gestión de Continuidad del Negocio 31
2.7.1. ISO 22301 31
2.7.2. ISO/IEC 27001 33
2.7.3. ITIL 34
2.7.4. COBIT 35
2.7.5. Matriz comparativa de las normativas de la gestión de continuidad de negocio 36
CAPÍTULO III 38
3.1. Enfoque de la investigación 38
3.2. Nivel de la investigación 38
3.3. Población y muestra 39
3.4. Técnicas e instrumentos de recolección 39
3.5. Tratamiento de la información 40
3.6. Resultados 40
3.7. Análisis general de la encuesta 44
CAPÍTULO IV 45
PROPUESTA 45
4.1. Título de la propuesta 45
4.2. Presentación 45
4.3. Creación del Plan de Continuidad de Negocio bajo la norma ISO 22301 46
4.3.1. Contexto de la Organización 46
4.3.2. Identificación de los procesos de la empresa EMMAIPC-EP 49
4.3.2. Alcance del Plan de Continuidad de Negocio 49
4.3.3. Análisis de Riesgos y Evaluación de Impacto en el Negocio (BIA) 50
4.3.3. Análisis de Impacto en el Negocio (BIA) 76
CONCLUSIONES 81
RECOMENDACIONES 82
Referencias 83
ANEXOS 85
Anexo 2. Protocolo de la investigación 104

Anexo 2. Autorizacion de publicacion en el repositorio institucional ..... **¡Error! Marcador no definido.**

Anexo 3. Certificado de Ingles 3

Anexo 4. Certificado Turniting..... 4

ÍNDICE DE TABLAS

Tabla 1. Matriz comparativa de metodologías de gestión de riesgos. Fuente: Autoría Propia..... 28

Tabla 2. Matriz comparativa de normativas de la gestión de continuidad de negocio. Fuente: Autoría Propia. 36

Tabla 3. Valores para evaluar los procesos críticos de la EMMAIPC-EP. Fuente: Autoría Propia..... 50

Tabla 4. Calificación de procesos. Fuente: Autoría Propia 52

Tabla 5. Identificación de activos de TI. Fuente: Autoría Propia..... 56

Tabla 6. Escalas de valor para la calificación de los activos. Fuente: Autoría Propia .. 58

Tabla 7. Escala de valor para los riesgos. Fuente: Autoría Propia 59

Tabla 8. Evaluación de activos de TI. Fuente: Autoría Propia..... 60

Tabla 9. Identificación de amenazas de los activos críticos de TI. Fuente: Autoría Propia 61

Tabla 10. Escala de probabilidad. Fuente: Autoría Propia 65

Tabla 11. Escala de impacto. Fuente: Autoría Propia 66

Tabla 12. Escala de valoración del riesgo. Fuente: Autoría propia..... 67

Tabla 13. Análisis de riesgos. Fuente: Autoría Propia 67

Tabla 14. Salvaguardas. Fuente: Autoría Propia 72

Tabla 15. Escala de Tiempos de Recuperación. Fuente: Autoría Propia 79

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Fases de gestión de Riesgos de TI. Fuente: (Cornejo, 2023) 21
Ilustración 2. Fases de la metodología OCTAVE. Fuente: Autoría Propia..... 23
Ilustración 3. Fases de la norma ISO 27005. Fuente: (Selliliar, 2024) 26
Ilustración 4. Ciclo PHVA y SGCN. Fuente: (CertiProf, 2023, pág. 17) 32
Ilustración 5. Fases del Plan de Continuidad del Negocio. Fuente: Autoría propia..... 46
Ilustración 6. Organigrama de la EMMAIPC-EP. Fuente: (EMMAIPC-EP, 2018) 48
Ilustración 7. Organigrama Institucional EMMAIPC-EP. Fuente: (EMMAIPC-EP, 2018) ..... **¡Error! Marcador no definido.**
Ilustración 8. Mapa de procesos EMMAIPC-EP. Fuente (EMMAIPC-EP, 2018) **¡Error! Marcador no definido.**

INTRODUCCIÓN

A continuación, se realiza una breve descripción de los capítulos presentados en el documento:

Capítulo I: Se aborda la explicación del problema de investigación, proporcionando un análisis detallado de la situación actual de la gestión de la continuidad del negocio en el ámbito de TI para EMMAIPC-EP. Este capítulo también incluye los antecedentes que justifican la importancia de esta investigación, así como los objetivos general y específicos que guían el estudio. Además, se definen las limitaciones y delimitaciones del alcance de la investigación, estableciendo los parámetros dentro de los cuales se desarrollará el trabajo.

Capítulo II: Contiene el marco teórico, donde se exploran los conceptos fundamentales relacionados con la gestión de la continuidad del negocio, la gestión de riesgos en TI, y las normativas internacionales como ISO 22301 que rigen estas prácticas. Este capítulo proporciona la base conceptual necesaria para comprender los desafíos y oportunidades en la implementación de un Plan de Continuidad del Negocio (BCP) en EMMAIPC-EP.

Capítulo III: Presenta el marco metodológico utilizado en la investigación. Se describe la metodología empleada, la cual es de carácter descriptivo y evaluativo, combinando técnicas cualitativas y cuantitativas. Se detalla el proceso de recopilación de datos, incluyendo encuestas realizadas al personal clave de EMMAIPC-EP, así como el análisis de los resultados obtenidos que fundamentan el diagnóstico del estado actual de la infraestructura y las prácticas de gestión de TI en la organización.

Capítulo IV: En este capítulo se desarrolla el diseño y propuesta del Plan de Continuidad del Negocio (BCP) específico para EMMAIPC-EP. Se describen las estrategias de recuperación de desastres y continuidad del negocio, adaptadas a las necesidades de la organización. Además, se detallan las fases de implementación del plan, incluyendo la identificación de riesgos, la priorización de activos críticos, y la planificación de contingencias, con el objetivo de garantizar la resiliencia operativa y el cumplimiento normativo.

CAPÍTULO I

MARCO REFERENCIAL

1. Planteamiento del problema

En un entorno empresarial cada vez más dependiente de la tecnología, la capacidad de una organización para continuar operando frente a interrupciones es fundamental. EMMAIPC-EP, una entidad pública en el cantón Cañar, no es la excepción. Esta dependencia creciente de los sistemas informáticos plantea desafíos significativos en términos de gestión de la continuidad del negocio[1] (GCB), especialmente en el ámbito de la tecnología de la información (TI)[2].

Actualmente, EMMAIPC-EP enfrenta varias vulnerabilidades en su infraestructura de TI, incluyendo sistemas desactualizados, falta de planes de recuperación de desastres bien definidos, y una capacitación insuficiente del personal en prácticas de GCB. La falta de un marco estructurado para la gestión de la continuidad del negocio en TI podría resultar en interrupciones operativas significativas, pérdida de datos críticos y, en última instancia, un deterioro en la prestación de servicios esenciales a la comunidad. La necesidad de abordar estos riesgos es urgente dado el papel crucial que juega EMMAIPC-EP en el desarrollo y mantenimiento de infraestructura pública esencial y servicios administrativos en el cantón Cañar. Sin embargo, la organización carece de una estrategia comprensiva que integre políticas, procedimientos y recursos efectivos para asegurar la continuidad operativa de sus sistemas de TI frente a diversas contingencias.

Este trabajo busca desarrollar una propuesta integral para la gestión de la continuidad del negocio en el ámbito de TI en EMMAIPC-EP, que no solo aborde las brechas actuales, sino que también establezca un marco sostenible para responder eficazmente a incidentes futuros. La investigación se centrará en identificar las vulnerabilidades críticas, evaluar los riesgos asociados y proponer soluciones prácticas y escalables que puedan ser adoptadas para fortalecer la resiliencia organizacional de EMMAIPC-EP.

[1] Gestión de la Continuidad del Negocio (GBC)
[2] Tecnologías de la Información

1.1. Formulación del problema

Basado en lo anterior, se genera la siguiente pregunta:

- ¿Cómo puede la empresa EMMAIPC-EP implementar el marco de gestión de la continuidad de negocio en TI que sea efectivo y sostenible, garantizando la continuidad de sus operaciones críticas bajo cualquier circunstancia?

1.2. Antecedentes de la Investigación

Un trabajo realizado por Vega (2024) describe una metodología basada en la norma ISO/IEC 27031 para la elaboración de un plan de continuidad de negocios que va desde la identificación de riesgos y la evaluación del impacto hasta la implementación y pruebas del plan.

Este documento permite comprender la importancia de un plan de continuidad de negocios de una determinada empresa con el objetivo que pueda recuperarse de eventos disruptivos y minimizar el impacto en sus operaciones, clientes y reputación. Además, la metodología utilizada en el documento servirá de guía para estructurar la propuesta de plan de continuidad de negocio para TI en la empresa EMMAIPC-EP.

Zuñiga (2021) se centra en la gestión de la continuidad del negocio (GBC) en el contexto de la seguridad de la información, basándose en el estándar ISO/IEC 27031, un estándar internacionalmente reconocido para la GBC en el ámbito de TI. El documento aborda consideraciones específicas para la implementación de la GBC en el ámbito de TI, como la identificación de riesgos de seguridad de la información, la evaluación del impacto de estos riesgos y la implementación de medidas de control para mitigarlos.

Basado en lo anterior, este documento permitirá comprender cómo el plan de continuidad de negocio se relaciona con la seguridad de la información y cómo se puede implementar un plan efectivo para proteger los activos de información de EMMAIPC-EP.

Araujo, G (2019), presenta un trabajo de investigación denominado, “Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador”, en el que proporciona un marco teórico y conceptual sólido sobre la gestión de la continuidad del negocio (GBC), incluyendo definiciones, conceptos clave, modelos y buenas prácticas.

Los autores describen una metodología detallada para la elaboración de un plan de continuidad del negocio, desde la identificación de riesgos y la evaluación del impacto hasta la implementación y pruebas del plan.

Este documento permitirá fundamentar el trabajo de investigación a través de las bases sólidas teóricas, además de normas, guías, herramientas y estudios de caso.

1.3. Justificación de la investigación

La gestión de la continuidad del negocio en el ámbito de la tecnología de la información (TI) es crítica para la sostenibilidad y eficiencia de cualquier organización, especialmente en el sector público, donde los servicios deben ser continuos y fiables para satisfacer las necesidades de la comunidad. EMMAIPC-EP, al ser una entidad pública encargada de la administración y desarrollo infraestructural del cantón Cañar, requiere de sistemas de TI robustos y resistentes a diversas contingencias.

La creciente dependencia de las operaciones de EMMAIPC-EP en sistemas tecnológicos hace indispensable la implementación de un marco sólido de gestión de la continuidad del negocio que pueda garantizar la mínima interrupción de los servicios críticos y la rápida recuperación en casos de desastres o fallos sistémicos. A pesar de esta necesidad, se observa una falta de políticas y procedimientos actualizados que enfrenten estos retos de manera efectiva. La relevancia de esta investigación radica en su capacidad para fortalecer la resiliencia de EMMAIPC-EP frente a interrupciones, protegiendo así los datos críticos y servicios esenciales que impactan directamente en la vida cotidiana de los ciudadanos del cantón. Además, un plan de gestión de la continuidad del negocio adecuadamente diseñado y aplicado no solo mejorará la capacidad de respuesta frente a emergencias, sino que también fomentará una cultura de preparación y mejora continua dentro de la organización.

La propuesta de esta tesis se justifica también en la necesidad de alinear las prácticas de gestión de TI con las normativas nacionales e internacionales sobre gestión de riesgos y continuidad del negocio, promoviendo así el cumplimiento normativo y la eficiencia operativa. En consecuencia, esta investigación aportará valor práctico y teórico, proporcionando un modelo replicable para otras entidades del sector público que enfrentan desafíos similares en la gestión de la continuidad de sus operaciones de TI.

1.4. Objetivos

1.4.1. Objetivo General

Desarrollar una propuesta de gestión de la continuidad del negocio específicamente adaptada al ámbito de TI de EMMAIPC-EP del cantón Cañar.

1.4.2. Objetivos Específicos

- Diagnosticar el estado actual de la infraestructura de TI y las prácticas de gestión de la continuidad del negocio en EMMAIPC-EP.
- Elaborar un marco de gestión de riesgos de TI que identifique, evalúe y priorice las amenazas potenciales a la continuidad operacional de EMMAIPC-EP.
- Diseñar un plan de acción para la implementación de estrategias de recuperación de desastres y continuidad del negocio que sean prácticas, escalables y sostenibles.

1.5. Limitaciones

- Restricciones en el acceso a la información confidencial o sensible de la infraestructura de TI de la empresa EMMAIPC-EP.
- La propuesta dependerá de las tecnologías actuales y capacidades del sistema de TI existentes en la empresa.

1.6. Delimitaciones

- El presente estudio se centra exclusivamente en la gestión de la continuidad del negocio en el área de TI, excluyendo otros aspectos no tecnológicos de la continuidad operativa de la empresa. La investigación se limitará a la empresa EMMAIPC-EP del cantón Cañar, no se extenderá a otras entidades o empresas fuera de este contexto.
- Es importante mencionar que la propuesta se desarrollará y evaluará con datos y contextos que sean relevantes hasta el momento actual y próximo futuro, sin

intentar prever cambios tecnológicos u organizacionales a largo plazo que podrían alterar las condiciones actuales.

CAPÍTULO II

MARCO TEÓRICO

La gestión de la continuidad del negocio (BCP) en el ámbito de las Tecnologías de la Información (TI), busca asegurar que las operaciones de los sistemas informáticos en todas las funciones operativas y estratégicas queden funcionales luego de haberse enfrentado a incidentes críticos.

Para comprender de mejor manera, esta disciplina es necesario explorar conceptos fundamentes relacionados con el BCP, abordando además normativas y estándares relevantes como la ISO 22301, que determina los requisitos para sistemas de gestión de la continuidad del negocio.

2.1. Plan de continuidad de negocio (BCP)

Es un documento esencial que contiene los procesos y procedimientos que una organización debe seguir en caso de un incidente o crisis que puede interrumpir o detener las operaciones comerciales o de tecnologías de la Información. Un BCP tiene como fin permitir que la organización mantenga o recupere de forma inmediata sus operaciones críticas luego de una interrupción (Rodríguez Rodríguez, 2020).

> El plan de continuidad del negocio inicia con la identificación, socialización y aprobación de los escenarios de emergencia para los cuales la Entidad definirá, actividades, responsables y recursos en caso de materialización de la situación de emergencia, continua con la evaluación de impacto al negocio de los procesos institucionales para establecer orden de recuperación de los procesos afectados, sigue con la ejecución de pruebas y simulacros de las actividades de respuesta planificadas y termina con la evaluación de los resultados de las pruebas y formulación de planes de mejoramiento del plan de continuidad de negocio (Intranet, 2023, pág. 7).

2.2. Plan de Recuperación de Desastres (DRP)

Un Plan de Recuperación de Desastres, es un documento estructurado que contiene instrucciones detalladas con el objetivo de responder a incidentes imprevistos que causan la pérdida de los sistemas de información y tecnología crítica para el negocio.

Este documento se centra específicamente en la recuperación de los sistemas de TI y datos luego de un desastre.

Galindo (2020), manifiesta que, para desarrollar un DRP se comienza con una Evaluación de Riesgos y un Análisis de Impacto en el Negocio (BIA) para identificar los sistemas de TI críticos y evaluar los posibles desastres que podrían afectarlos, determinando el impacto en las operaciones del negocio. Luego, se establecen los Objetivos de Punto de Recuperación (RPO) y Tiempo de Recuperación (RTO) para cada sistema y proceso crítico. A continuación, se diseñan estrategias de recuperación que pueden incluir soluciones como sitios de recuperación de desastres y sistemas de respaldo. Estos planes se documentan detalladamente, asignando roles y responsabilidades al equipo de recuperación. La implementación involucra poner en marcha estas soluciones, seguida por pruebas y simulacros regulares para asegurar la eficacia del plan y familiarizar al personal con sus roles. Finalmente, el DRP se mantiene y actualiza regularmente para adaptarse a cambios en la tecnología, los procesos del negocio, y el entorno operativo, garantizando que el plan permanezca relevante y efectivo.

2.3. Gestión de Riesgos de TI

La gestión de riesgos de TI es un proceso crucial para cualquier organización que dependa significativamente de la tecnología. Su objetivo es identificar, evaluar y priorizar riesgos relacionados con la tecnología de la información, y luego implementar estrategias adecuadas para mitigar o manejar estos riesgos, asegurando así la continuidad y eficiencia de las operaciones del negocio (Ferguson Castro, 2023).

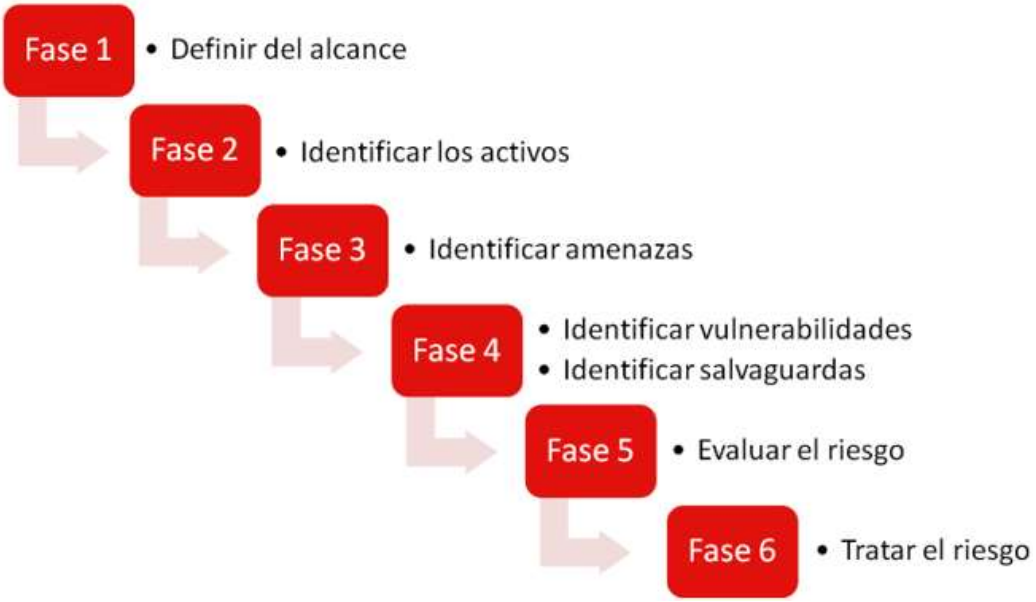


Ilustración 1. Fases de gestión de Riesgos de TI. Fuente: (Cornejo, 2023)

2.3.1. Amenazas de TI

Las amenazas de TI representan los potenciales peligros que pueden comprometer la seguridad, la integridad, y la disponibilidad de los sistemas de información de una organización. Estas amenazas pueden provenir de múltiples fuentes y adoptar diversas formas, desde ataques cibernéticos hasta errores humanos o desastres naturales (Velthuis & González, 2020).

2.3.2. Vulnerabilidades de TI

Las vulnerabilidades de TI son debilidades o fallos en los sistemas de información que pueden ser explotados por amenazas, como los ataques cibernéticos, para causar daño o robar datos. Estas vulnerabilidades pueden estar presentes en el software, hardware, o en los procesos y políticas que rigen la infraestructura de TI. Identificar y mitigar estas vulnerabilidades es crucial para proteger los activos de una organización y garantizar la continuidad de las operaciones (García, 2023).

2.3.3. Riesgos de TI

Los riesgos informáticos hacen referencia a cualquier amenaza o vulnerabilidad asociada con la utilización de la tecnología, que pueden llegar afectar los pilares básicos de la seguridad informática en una determinada organización. Llegando a causar pérdidas financieras, daño a la reputación, infracciones legales, entre otros.

Existen varios tipos de riesgos como los de seguridad cibernética; riesgos de infraestructura que hacen referencia a malfuncionamientos o fallos en los componentes críticos; riesgos operativos, son aquellos que se refieren a las equivocaciones cometidas por el personal, como la configuración incorrecta de sistemas o manejo inadecuado de datos; riesgos de cumplimiento, cuando se incumplen las normas y regulaciones; riesgos estratégicos, que son aquellos que tienen que ver con las inversiones en tecnología que no se alinean con las necesidades o estrategias de negocio de la organización; riesgos de desastres naturales como los terremotos, inundaciones, incendios y otros desastres que pueden causar daño a la infraestructura tecnológica (Alouffi, y otros, 2021).

2.4. Metodologías de Gestión de Riesgos Informáticos

Las metodologías de gestión de riesgos de TI son esenciales para identificar, evaluar, mitigar y monitorear los riesgos asociados con los sistemas de información de una organización. Estas metodologías ayudan a garantizar la integridad, confidencialidad y disponibilidad de los datos, al tiempo que soportan la continuidad de las operaciones de negocio (Serrano Saenz, 2023).

2.4.1. OCTAVE

Es un marco de autoevaluación que prioriza la evaluación de riesgos basada en los activos. Se centra en las necesidades y estrategias de seguridad de la organización, involucrando activamente a los responsables de negocio y personal técnico (Parra, 2019).

a) 2.4.1.1. Fases de la metodología OCTAVE

Fase 1: Crear Perfiles de Activos

- **Identificación de Activos Críticos**: Identificar los activos de información que son esenciales para las operaciones de la organización.

- **Determinar la Seguridad**: Establecer qué nivel de confidencialidad, integridad y disponibilidad es necesario para cada activo crítico.

Fase 2: Identificar Amenazas

- **Evaluación de Amenazas y Vulnerabilidades**: Identificar amenazas a la seguridad de los activos críticos y evaluar las vulnerabilidades que podrían ser explotadas por dichas amenazas.
- **Determinar y Priorizar Riesgos**: Evaluación del impacto y la probabilidad de las amenazas identificadas para determinar los riesgos asociados.

Fase 3: Desarrollar Estrategias de Mitigación y Planes de Protección

- **Desarrollar Estrategias de Seguridad**: Planificar y diseñar estrategias para mitigar los riesgos identificados.
    - **Preparar Planes de Protección de Activos**: Elaborar e implementar planes detallados para la protección de los activos (Muñoz Gutiérrez

, 2022).

Ilustración 2. Fases de la metodología OCTAVE. Fuente: Autoría Propia.

2.4.2. MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología desarrollada inicialmente por el Consejo Superior de Administración Electrónica de España. Está diseñada para ayudar a las organizaciones, especialmente en el sector público, a identificar, analizar y gestionar los riesgos asociados con sus sistemas de información. MAGERIT es una herramienta clave para proteger los activos de información y garantizar la continuidad de las operaciones y servicios (Gómez, Candau, & Mañas, 2013).

Esta metodología tiene como objetivos identificar riesgos, valorar el impacto, ayudar en la toma de decisiones y cumplir con requerimientos legales.

b) 2.4.2.1. Fases de la metodología MAGERIT

Fase 1: Preparación

- **Definir el Alcance del Análisis**: Determinar qué partes del sistema de información serán evaluadas.
- **Comprometer a la Dirección**: Asegurar el apoyo y la participación de los niveles superiores de gestión.

Fase 2: Análisis

- **Identificación de Activos**: Catalogar todos los elementos del sistema de información que son esenciales para la organización.
- **Evaluación de Amenazas**: Identificar todos los posibles peligros que podrían afectar a esos activos.

- **Análisis de Vulnerabilidades**: Determinar las debilidades que podrían ser explotadas por las amenazas.
- **Estimación de Riesgos**: Evaluar la probabilidad de que las amenazas exploten las vulnerabilidades y el impacto que esto tendría.

Fase 3: Gestión

- **Planificación de Tratamiento de Riesgos**: Desarrollar e implementar estrategias para mitigar, transferir, aceptar o evitar los riesgos identificados.
- **Implementación de Medidas de Protección**: Ejecutar las estrategias de tratamiento de riesgos, como controles técnicos, organizativos, legales o de otro tipo.
- **Monitoreo y Revisión**: Vigilar continuamente la eficacia de las medidas implementadas y revisar periódicamente el proceso de gestión de riesgos (Gastelo Fernandez & Rodríguez Flores , 2023).

2.4.3. ISO 27005

De acuerdo con la ISO / IEC (2022), la norma ISO 27005 se centra en la gestión de la seguridad de la información, incluyendo la identificación, evaluación y tratamiento de los riesgos, entre sus fases se encuentran las siguientes:

1. **Identificación de riesgos**: Esto involucra identificar los activos de información que requieren protección, así como las amenazas y vulnerabilidades que podrían comprometer esos activos.
2. **Evaluación de riesgos**: Esto implica determinar el impacto potencial y la probabilidad de los riesgos identificados.

3. **Tratamiento de riesgos**: Esto implica seleccionar y aplicar controles para mitigar los riesgos a un nivel aceptable.

4. **Aceptación de riesgos**: Los riesgos que no se pueden mitigar o que se consideran aceptables después de la aplicación de los controles se aceptan.

5. **Comunicación de riesgos**: Los riesgos, así como las decisiones tomadas para tratarlos y aceptarlos, se comunican a todas las partes interesadas.

6. **Monitoreo y revisión de riesgos**: Los riesgos y la eficacia de los controles se revisan y monitorean regularmente para asegurarse de que la gestión de riesgos se mantiene efectiva (García & Alexey, 2022).

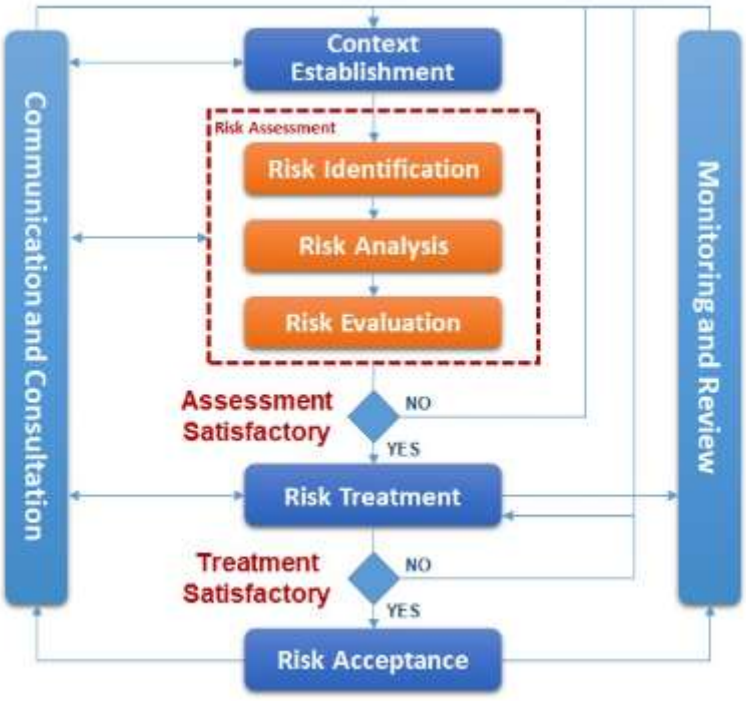


Ilustración 3. Fases de la norma ISO 27005. Fuente: (Selliliar, 2024)

2.4.4. CRAMM

CRAMM (CCTA Risk Analysis and Management Method) es una metodología de análisis y gestión de riesgos desarrollada originalmente por la Central Computer and Telecommunications Agency (CCTA) del Reino Unido. Está diseñada para evaluar y gestionar los riesgos de seguridad de la información y los sistemas asociados. CRAMM combina las técnicas de evaluación de riesgos con un enfoque sistemático para implementar y mantener controles de seguridad adecuados (ENISA, 2024).

c) 2.4.4.1. Fases de la metodología CRAMM

1. **Recopilación de Información**: Recoger datos sobre el entorno de TI, los procesos de negocio y los requisitos legales y reglamentarios.
2. **Valoración de Activos**: Determinar la importancia de cada activo en términos de confidencialidad, integridad y disponibilidad.
3. **Identificación de Amenazas y Vulnerabilidades**: Analizar las formas en que los activos podrían verse amenazados o vulnerados.
4. **Evaluación de Riesgos**: Calcular la probabilidad de que ocurran incidentes y su potencial impacto.
5. **Desarrollo de una Estrategia de Seguridad**: Recomendar y priorizar controles basados en la evaluación de riesgos.
6. **Implementación y Revisión de Controles**: Poner en práctica las medidas de seguridad y revisarlas periódicamente para asegurar su efectividad (Castro Acosta, 2023).

2.4.5. Matriz comparativa de las metodologías de Gestión de Riesgos Informáticos

Tabla 1. Matriz comparativa de metodologías de gestión de riesgos. Fuente: Autoría Propia

Característica	OCTAVE	MAGERIT	ISO 27005	CRAMM
Enfoque	Evaluación basada en activos con participación de diversos niveles organizativos.	Análisis y gestión centrado en la administración pública, adaptable a otras organizaciones.	Gestión de riesgos de seguridad de la información con un enfoque exhaustivo.	Gestión de riesgos detallada con un enfoque estructurado y sistemático.
Objetivo	Mejorar la protección de la información mediante el involucramiento activo del personal.	Identificar, analizar y gestionar riesgos en sistemas de información.	Proporcionar directrices sobre cómo gestionar riesgos de seguridad de la información.	Evaluación y control de los riesgos de seguridad para proteger los activos de información.
Metodología	Fases de creación de perfiles de activos, identificación de amenazas y desarrollo de estrategias.	Fases de preparación, análisis y gestión.	Análisis y evaluación del riesgo, tratamiento y monitoreo continuo.	Fases de análisis de riesgos, evaluación de riesgos y gestión de riesgos.
Herramientas	Enfoque participativo sin herramientas específicas; utiliza tablas y entrevistas para recopilar datos.	A menudo acompañada por herramientas como PILAR para la simulación y análisis de riesgos.	No prescribe herramientas específicas; se centra en el proceso y las mejores prácticas.	Incluye software específico para facilitar el análisis y la gestión de riesgos.
Sector de Aplicación	Flexible, aplicable a cualquier sector.	Desarrollada por y para el sector público en España, pero adaptable a	Aplicable a cualquier organización que necesite gestionar la	Originalmente desarrollado para el sector público en el Reino Unido, pero usado

		cualquier organización.	seguridad de la información.	ampliamente en varios sectores.
Reconocimiento Internacional	Ampliamente reconocido, especialmente en EE.UU.	Principalmente en España y Latinoamérica.	Reconocimiento global como parte de la familia de estándares ISO/IEC 27000.	Fuerte en el Reino Unido y países de la Commonwealth, pero conocido a nivel mundial.

d) 2.5. Tecnologías de la Información

Las tecnologías de la información (TI) comprenden el conjunto de herramientas, procesos y metodologías utilizadas en la recolección, procesamiento, almacenamiento y distribución de información. Incluyen tanto hardware (dispositivos físicos y componentes), software (programas y sistemas operativos), redes de comunicaciones (Internet, redes corporativas) como los datos almacenados y procesados. Las TI juegan un papel crucial en todos los sectores de la sociedad moderna, impactando los negocios, la educación, el gobierno, el entretenimiento, entre otros (Javier, Carmen, & Alejandro, 2023).

2.5.1. Desafíos en las tecnologías de la Información

Los desafíos en las tecnologías de la información incluyen la necesidad de fortalecer la seguridad cibernética para proteger sistemas contra ataques maliciosos, salvaguardar la privacidad de datos personales frente a amenazas y vulnerabilidades, abordar la brecha digital que afecta el acceso equitativo a las tecnologías, y mantenerse actualizados frente al rápido cambio tecnológico que caracteriza a este sector. Estos retos exigen que tanto organizaciones como profesionales se mantengan en constante aprendizaje y adaptación, garantizando así la relevancia y la competencia en un ambiente altamente dinámico (CCNA, 2024).

2.6. Resiliencia Organizacional

Este término hace mención a la capacidad de una empresa o institución para anticipar, prepararse, responder y adaptarse a incidentes inesperados o cambios abruptos de manera eficaz y eficiente. Esta capacidad permite a las organizaciones no solo sobrevivir a adversidades, sino también aprender, evolucionar y fortalecerse a partir de ellas. La resiliencia no es solo una reacción a las crisis; involucra la creación de un ambiente que fomente la innovación constante y el aprendizaje continuo, asegurando que la organización pueda mantenerse sostenible y competitiva en el largo plazo (Montero, 2021).

2.6.1. Componentes de la Resiliencia Organizacional

1. **Gestión de Riesgos**: Identificar, evaluar y gestionar riesgos proactivamente para minimizar impactos negativos sobre las operaciones.
2. **Planificación de Continuidad del Negocio**: Desarrollar y ejecutar estrategias que aseguren la continuidad de las operaciones críticas bajo cualquier circunstancia.
3. **Adaptabilidad**: Capacidad de ajustar operaciones y estrategias rápidamente en respuesta a cambios en el entorno externo.
4. **Cultura Organizacional**: Promover una cultura que valore la anticipación de desafíos, el aprendizaje constante, y la innovación.
5. **Liderazgo Comprometido**: Liderazgo que promueva, apoye y priorice la resiliencia como parte integral de la gestión de la organización.
6. **Colaboración y Comunicación**: Asegurar una comunicación efectiva dentro y fuera de la organización para mejorar la coordinación y la respuesta rápida en situaciones de crisis.

7. **Capacidades Tecnológicas**: Implementar y mantener tecnologías que soporten operaciones resilientes y seguras.
8. **Recursos Financieros**: Gestionar de manera prudente los recursos financieros para poder afrontar y recuperarse de situaciones adversas (Becerra Santiago, 2023).

2.7. Normativas y Estándares Relevantes para la Gestión de Continuidad del Negocio

Para elaborar un plan de continuidad de negocio, existen algunas normativas y estándares diseñados para proporcionar un marco metodológico que las empresas pueden seguir con el fin de asegurar la resiliencia y la capacidad de respuesta frente a interrupciones.

2.7.1. ISO 22301

ISO 22301 es la norma internacional para los Sistemas de Gestión de la Continuidad del Negocio (SGCN). Esta norma específica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema documentado que gestione la continuidad del negocio en el contexto de la gestión de riesgos generales de una organización (Crask, 2024).

e) 2.7.1.1. Fases de la norma ISO 22301

ISO 22301 y su Sistema de Gestión de Continuidad del Negocio utilizan el ciclo PHVA (planificar, hacer, verificar, actuar), lo que implica realizar actividades de planificación, implementación, operación, monitoreo, revisión, y mantenimiento, con el fin de asegurar una mejora continua en la eficacia del sistema (Sevillano, 2021).

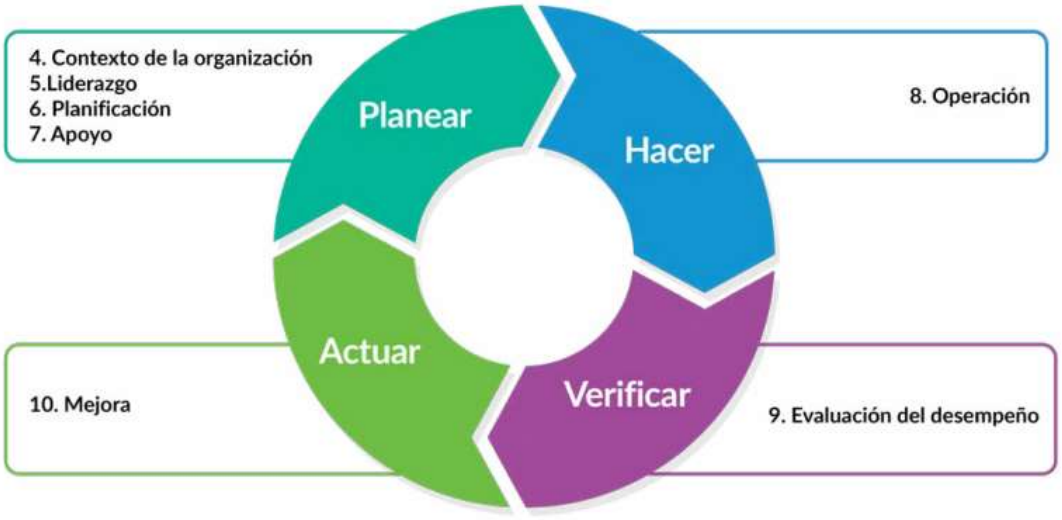


Ilustración 4. Ciclo PHVA y SGCN. Fuente: (CertiProf, 2023, pág. 17)

Los pasos para implementar un Sistema de Gestión de Continuidad del Negocio (SGCN) basado en la norma ISO 22301 son los siguientes:

1. Compromiso de la alta dirección:

- La alta dirección debe demostrar su compromiso con el SGCN asignando los recursos necesarios y creando una cultura de gestión de riesgos.

2. Política de continuidad del negocio:

- Se debe establecer una política de continuidad del negocio que defina los objetivos del SGCN y el compromiso de la organización con la continuidad del negocio.

3. Análisis de impacto en el negocio (BIA):

- Se debe realizar un BIA para identificar los procesos críticos para el negocio y el impacto potencial de las interrupciones en esos procesos.

4. Evaluación de riesgos:

- Se deben identificar, evaluar y priorizar los riesgos que podrían afectar la continuidad del negocio.

5. Desarrollo e implementación del plan de continuidad:

- Se deben desarrollar e implementar planes de continuidad para abordar los riesgos identificados en la evaluación de riesgos.

6. Pruebas y ejercicios de continuidad:

- Se deben realizar pruebas y ejercicios de continuidad para garantizar que los planes de continuidad sean efectivos.

7. Monitoreo y revisión:

- El SGCN debe ser monitoreado y revisado periódicamente para garantizar que sigue siendo efectivo y adecuado para la organización.

8. Mejora continua:

- El SGCN debe mejorarse continuamente mediante la identificación e implementación de oportunidades de mejora (nqa, 2021) (ISO, 2019).

2.7.2. ISO/IEC 27001

"ISO 27001 es una norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en una empresa" (ISO 27001, 2024).

ISO (2023) determina que:

Esta norma facilita a diferentes empresas u organizaciones un sistema que gestiona los riesgos relacionados con la seguridad de los datos que se manejan a través de pasos para establecer, implantar, mantener y mejorar de forma continua un sistema de

gestión de seguridad de la información (Wijayarathne, 2022). Para implementar la ISO 27001, se requiere de las siguientes fases:

1. Definición de Alcance y política de seguridad: Determinar qué áreas y activos de la organización estarán cubiertos por el SGSI.
2. Evaluación de riesgos: Realizar la identificación de riesgos, y posteriormente el análisis y evaluación de estos.
3. Gestión de Riesgos: Esta fase implica el tratamiento de riesgos e implementación de controles apropiados para mitigar los riesgos identificados a un nivel aceptable, basándose en la declaración de aplicabilidad.
4. Implementación del Sistema de Gestión de Seguridad de la Información: Establecer y documentar procesos y procedimientos operativos que respalden los controles de seguridad.
5. Evaluación del Desempeño: Involucra la monitorización y revisión de controles y auditorías internas periódicas.
6. Revisión por la Dirección: Revisión regular del sistema.
7. Mejora Continua: En esta fase se establece y documenta procesos y procedimientos operativos que respalden los controles de seguridad (nqa, 2024).

2.7.3. ITIL

Es un conjunto de prácticas para la gestión de servicios de TI (ITSM) que se enfoca en alinear los servicios de TI con las necesidades de los negocios. ITIL describe procesos, procedimientos, tareas y listas de verificación que no son específicos de ninguna organización individual, pero pueden ser implementados por una organización

para establecer un nivel mínimo de competencia, medir el desempeño y mejorar la calidad en la prestación de servicios de TI.

ITIL establece siete principios guía que pueden ayudar a cualquier organización en su toma de decisiones y en la mejora de sus iniciativas de gestión de servicios, entre ellas están: enforcarse en el valor; comenzar donde se está; progresar iterativamente con retroalimentación; colaborar y trabajar holísticamente; mantenerlo simple y práctico; optimizar y automatizar. Además cuenta con cuatro dimensiones (organizaciones y personas; información y tecnología; socios y proveedores; flujos de valor y procesos), estas representan áreas de enfoque que deben ser consideradas para garantizar un sistema de gestión de servicios equilibrado (Baud, 2017).

2.7.4. COBIT

COBIT es un framework ampliamente reconocido para la gestión y gobernanza de las tecnologías de información (TI). Desarrollado originalmente por la ISACA (Information Systems Audit and Control Association), COBIT proporciona un conjunto de prácticas, herramientas y modelos de procesos que ayudan a las organizaciones a maximizar el valor de sus inversiones en TI, al mismo tiempo que minimizan los riesgos asociados.

Este modelo ayuda a las organizaciones a alinear las estrategias de TI con los objetivos de negocio; gestionar los recursos de TI de una manera efectiva; lograr el cumplimiento de las regulaciones y leyes relacionadas y a optimizar los riesgos relacionados con la tecnología de información (Isaca, 2012).

2.7.5. Matriz comparativa de las normativas de la gestión de continuidad de negocio

Tabla 2. Matriz comparativa de normativas de la gestión de continuidad de negocio. Fuente: Autoría Propia.

Criterio	ISO 22301	ISO 27001	ITIL	COBIT
Enfoque Principal	Gestión de la Continuidad del Negocio	Gestión de la Seguridad de la Información	Gestión de Servicios de TI	Gobernanza y Gestión de TI
Objetivo	Asegurar la continuidad de operaciones críticas.	Proteger la confidencialidad, integridad y disponibilidad de la información.	Mejorar la calidad del servicio de TI.	Alinear la estrategia de TI con la estrategia del negocio y gestionar riesgos.
Alcance de Aplicación	Cualquier tipo de organización que busque asegurar la continuidad operacional.	Organizaciones que necesitan proteger información sensible.	Organizaciones con servicios de TI críticos.	Organizaciones que necesitan gobernar y gestionar su TI efectivamente.
Componentes Clave	Planes de continuidad, políticas, objetivos y procedimientos.	Políticas de seguridad, controles y gestión de riesgos de seguridad de la información.	Procesos de gestión de servicios, roles, y funciones de TI.	Principios, estructuras de gobernanza, y procesos de gestión de TI.
Documentación Requerida	Planes de respuesta a incidentes, estrategias de recuperación.	Políticas de seguridad, declaración de aplicabilidad.	Libros de mejores prácticas que cubren diversas áreas de gestión de servicios.	Mapas de procesos, objetivos de control, métricas y modelos de madurez.

Beneficios Específicos	Reduce tiempo de inactividad durante interrupciones. Mejora la resiliencia organizacional.	Ayuda a prevenir violaciones de seguridad y reduce riesgos asociados.	Incrementa la eficiencia operativa y mejora la satisfacción del cliente.	Mejora la toma de decisiones y optimiza los recursos de TI.

La tabla 2 proporciona un resumen detallado y un análisis comparativo de cuatro marcos y normativas relevantes para un BCP, mismos que son utilizados por organizaciones de diferentes sectores para asegurar que los sistemas informáticos y los procesos de negocio puedan resistir y recuperarse de interrupciones no planificadas.

Cada uno de estos estándares tiene un enfoque y aplicaciones específicas:

- **ISO 27001** se concentra en la seguridad de la información.
- **ITIL** ofrece prácticas para la gestión de servicios de TI.
- **COBIT** enfoca en la gobernanza y gestión integral de TI.

Sin embargo, la norma **ISO 22301** es destacado como el estándar más adecuado y específico para la gestión de la continuidad del negocio. Este estándar internacional proporciona un marco específico que no sólo ayuda a las organizaciones a prepararse para desastres o interrupciones, sino que también guía la implementación y operación de un sistema de gestión de la continuidad del negocio efectivo. ISO 22301 está diseñado para garantizar que las actividades críticas de una organización puedan continuar durante y después de incidentes críticos, facilitando una rápida recuperación, lo que lo convierte en la mejor opción para empresas que buscan enfocarse específicamente en la continuidad del negocio.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Enfoque de la investigación

La presente tesis tiene como objetivo desarrollar una propuesta para la gestión de la continuidad del negocio en el ámbito de las tecnologías de la información (TI) para EMMAIPC-EP del cantón Cañar, empleando un enfoque mixto que combina métodos cuantitativos y cualitativos. Este enfoque permite identificar y evaluar de manera integral los riesgos potenciales que puedan afectar la operación continua de los sistemas de TI de la empresa, así como diseñar e implementar estrategias y planes de contingencia para mitigar estos riesgos. La investigación incluye el análisis estadístico de datos relevantes y encuestas con expertos para obtener una visión completa y detallada de la situación actual y las necesidades específicas de EMMAIPC-EP. A través de esta propuesta, se busca fortalecer la resiliencia de la empresa, garantizando la continuidad operativa y minimizando el impacto de posibles interrupciones en sus procesos críticos.

3.2. Nivel de la investigación

La investigación se lleva a cabo a un nivel descriptivo y propositivo, con el objetivo de proporcionar una comprensión detallada de la situación actual de la gestión de la continuidad del negocio en el ámbito de las tecnologías de la información (TI) en EMMAIPC-EP del cantón Cañar. A nivel descriptivo, la investigación se enfoca en identificar y caracterizar los riesgos y vulnerabilidades existentes en los sistemas de TI de la empresa, así como en documentar las prácticas y procedimientos actuales de gestión de la continuidad del negocio. A nivel propositivo, la investigación se orienta a desarrollar y recomendar estrategias y planes de acción específicos que mejoren la capacidad de la empresa para responder a eventos disruptivos y asegurar la continuidad operativa de sus

procesos críticos. Este enfoque permite no solo diagnosticar la situación actual, sino también ofrecer soluciones prácticas y viables para fortalecer la resiliencia de EMMAIPC-EP.

3.3. Población y muestra

La población y el universo de esta investigación están constituidos por el encargado del área de tecnologías de la información (TI) de EMMAIPC-EP del cantón Cañar. Dado el enfoque específico de la investigación en la gestión de la continuidad del negocio en el ámbito de TI, se ha determinado que la persona más adecuada para proporcionar la información requerida es el encargado de TI.

3.4. Técnicas e instrumentos de recolección

Para la recolección de datos en esta investigación, se utilizará la técnica de la encuesta, la cual se aplicará exclusivamente al encargado del área de tecnologías de la información (TI) de EMMAIPC-EP del cantón Cañar. La encuesta ha sido diseñada para obtener información detallada y relevante sobre los procedimientos actuales de gestión de la continuidad del negocio, los riesgos y vulnerabilidades identificados, y las estrategias de mitigación implementadas. El instrumento de recolección consistirá en un cuestionario estructurado con preguntas tanto cerradas como abiertas, permitiendo así recopilar datos cuantitativos y cualitativos que proporcionen una comprensión integral del tema investigado. Esta metodología asegura la obtención de datos precisos y específicos, fundamentales para el desarrollo de una propuesta efectiva y adaptada a las necesidades de la empresa.

3.5. Tratamiento de la información

La información recolectada a través de la encuesta aplicada al encargado del área de tecnologías de la información (TI) de EMMAIPC-EP del cantón Cañar será analizada de manera detallada utilizando una matriz de análisis. Los datos obtenidos de las preguntas cerradas y abiertas se organizarán en esta matriz, lo que permitirá identificar y evaluar de manera sistemática los riesgos, vulnerabilidades y estrategias actuales en la gestión de la continuidad del negocio en el ámbito de TI. La matriz facilitará el análisis cualitativo y cuantitativo de las respuestas, permitiendo al estudiante extraer conclusiones significativas y elaborar recomendaciones bien fundamentadas. Este proceso asegurará que la información sea tratada de manera coherente y efectiva, proporcionando una base sólida para la propuesta de mejora en la continuidad del negocio para EMMAIPC-EP.

3.6. Resultados

Se realizó una encuesta al Ing. Guillermo Loja, jefe de TI de la empresa EMMAIPC-EP, con la finalidad de recopilar información sobre los procesos, principales riesgos y activos importantes.

A continuación, se presenta los resultados de la encuesta realizada y su interpretación:

Encuesta EMMAIPC CAÑAR, BIBLIÁN, EL TAMBO Y SUSCAL	
Objetivo:	Recopilar información sobre la gestión de la continuidad del negocio en el ámbito de las tecnologías de la información (TI) en EMMAIPC-EP.
Nombre:	Ing. Guillermo Loja
Fecha:	07/06/2024
SECCIÓN 1	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
¿La empresa cuenta con un plan de continuidad del negocio (BCP) específico para TI?	

NO

Si la respuesta anterior es "Sí", ¿con qué frecuencia se revisa y actualiza el BCP?

- Mensualmente ☐
- Trimestralmente ☐
- Anualmente ☐
- Otro: _____

¿Cuáles son los principales riesgos identificados que pueden afectar la continuidad del negocio en el área de TI? (Seleccione todos los que apliquen)

- Fallos en el hardware [X]
- Fallos en el software [X]
- Ciberataques ☐
- Desastres naturales ☐
- Errores humanos [X]
- Otros: Capacitación regular del personal en el ámbito de seguridad informática.

¿Qué estrategias o medidas se han implementado para mitigar estos riesgos?

No se ha implementado ninguna estrategia

¿Se han realizado simulacros o pruebas del plan de continuidad del negocio?

- Sí ☐

- No [X]

Si la respuesta anterior es "Sí", ¿con qué frecuencia se realizan estos simulacros?

- Mensualmente
- Trimestralmente
- Anualmente
- Otro: _____

SECCIÓN 2	**EVALUACIÓN Y MEJORA**

¿Considera que la empresa necesita un plan formal de continuidad del negocio en TI para asegurar la operatividad ante eventos disruptivos?

- Sí [X]
- No [ ]

¿Qué recursos adicionales (tecnológicos, humanos, financieros) considera necesarios para mejorar la gestión de la continuidad del negocio en TI?

Inversión en infraestructura de respaldo, formación continua para el personal en gestión de continuidad, mejorar la infraestructura de red y el servidor, además del proveedor de servicios de internet ya que el proveedor tiene un servicio inestable.

SECCIÓN 3	**DIAGNÓSTICO PARA LA IMPLEMENTACIÓN DE LA ISO 22301**

¿La empresa cuenta con personal capacitado en la implementación y gestión de sistemas de continuidad del negocio según la ISO 22301?

- Sí [ ]
- No [X]

¿Cuáles son los procesos críticos de negocio que dependen directamente de los sistemas de TI?

Facturación y gestión de multas, atención al cliente y sistemas de comunicación interna.

¿Qué sistemas y aplicaciones son esenciales para la operación continua de la empresa?

El sistema de facturación

¿Qué impacto tendría la interrupción de estos sistemas y aplicaciones en la operación de la empresa?

- Muy Alto [X]
- Alto [ ]
- Medio [ ]
- Bajo [ ]
- Muy bajo

¿Existe un inventario actualizado de todos los activos de TI críticos?

- Sí [ ]
- No [X]

¿Qué procedimientos de respaldo y recuperación de datos están actualmente en vigor?

Realización de copias de seguridad de todos los datos

¿Cuál es el tiempo estimado de recuperación para los sistemas críticos en caso de una interrupción?

- Menos de 1 hora [ ]
- 1-4 horas [ ]
- 4-24 horas [ ]
- Más de 24 horas [X]

¿Qué procedimientos existen para la comunicación y coordinación en caso de una interrupción de TI?

Ningún procedimiento

¿Qué áreas o departamentos de la empresa deben ser priorizados en la recuperación de servicios de TI?

Operaciones de campo (para la recolección de basura), atención al cliente (para la comunicación con los usuarios), y finanzas (para la gestión de pagos y facturación).

3.7. Análisis general de la encuesta

La encuesta revela que EMMAIPC-EP enfrenta desafíos significativos en la gestión de la continuidad del negocio en el ámbito de TI. Actualmente, la empresa no cuenta con un Plan de Continuidad del Negocio (BCP) específico para TI, y no se han implementado estrategias efectivas para mitigar riesgos críticos como fallos en el hardware, desastres naturales y errores humanos. Además, no se han realizado simulacros o pruebas del BCP, lo que sugiere una falta de preparación ante incidentes reales.

La necesidad de un plan formal es reconocida internamente, y se identifican áreas clave de mejora, como la inversión en infraestructura de respaldo, la formación continua del personal y la estabilización del servicio de internet. Sin embargo, la empresa carece de personal capacitado en la norma ISO 22301, lo que limita su capacidad para implementar un BCP alineado con estándares internacionales.

La interrupción de sistemas críticos tendría un impacto muy alto, y la falta de un inventario actualizado de activos dificulta la gestión eficiente de la continuidad del negocio. Finalmente, se destacan las áreas de operaciones de campo, atención al cliente y finanzas como prioritarias para la recuperación en caso de un incidente, pero se carece de procedimientos claros para la comunicación y coordinación durante una interrupción de TI.

CAPÍTULO IV

PROPUESTA

4.1. Título de la propuesta

"Propuesta para la gestión de la continuidad del negocio en el ámbito de TI para EMMAIPC-EP del cantón Cañar"

4.2. Presentación

La continuidad del negocio es un componente esencial para garantizar la resiliencia y sostenibilidad de una organización, especialmente en el ámbito de las tecnologías de la información (TI). En un mundo cada vez más interconectado y dependiente de los sistemas digitales, cualquier interrupción en los servicios puede tener repercusiones significativas en la operación y reputación de una entidad. En este contexto, el presente capítulo tiene como objetivo principal desarrollar una propuesta integral para la gestión de la continuidad del negocio en el ámbito de TI para EMMAIPC-EP del cantón Cañar.

La propuesta se basa en un análisis exhaustivo de la situación actual de la infraestructura y los procesos de TI de la entidad, identificando las principales vulnerabilidades y áreas críticas que podrían afectar la operatividad ante eventos disruptivos. Además, se a la norma ISO 22301, para establecer un marco sólido y estructurado que permita a EMMAIPC-EP mantener sus funciones esenciales durante y después de un incidente.

A lo largo de este capítulo, se presentarán las fases de implementación del plan de continuidad, incluyendo la identificación de riesgos, la evaluación de impacto en el negocio, el desarrollo de estrategias de mitigación y recuperación, así como la creación de un equipo de respuesta y la planificación de pruebas y ejercicios. De esta manera, se busca no solo proteger los activos tecnológicos de la organización, sino también asegurar la continuidad de sus operaciones y servicios hacia la comunidad.

Este plan de continuidad del negocio no es una solución estática, sino un documento vivo que debe actualizarse y ajustarse continuamente para reflejar los cambios en el entorno tecnológico y organizacional. La propuesta aquí presentada se configura como un primer paso hacia un modelo de gestión proactivo y preventivo, que posiciona

a EMMAIPC-EP como una entidad preparada para enfrentar cualquier desafío que pueda comprometer su misión y objetivos estratégicos.

Para la elaboración del BCP, se seguirán los siguientes pasos:

Ilustración 5. Fases del Plan de Continuidad del Negocio. Fuente: Autoría propia

4.3. Creación del Plan de Continuidad de Negocio bajo la norma ISO 22301

4.3.1. Contexto de la Organización

La Empresa Pública Municipal Mancomunada de Aseo Integral de los cantones de Cañar, Biblián, El Tambo y Suscal EMMAIPC-EP, fue creada el 29 de diciembre del 2011 mediante ordenanza municipal en cada uno de los cantones que establece como principios básicos para la empresa orientar y conseguir mayor eficiencia en la prestación de los servicios de aseo y limpieza de la ciudad.

EMMAIPC-EP ha promovido una serie de acciones para buscar soluciones respecto a la problemática en el manejo de los desechos sólidos cada uno de los esfuerzos cuentan con el apoyo de los gobiernos autónomos descentralizados municipales y de los diferentes actores de la sociedad. Su gestión se orienta con criterios de eficiencia, eficacia, racionalidad, y rentabilidad social; preservando el ambiente, promoviendo el desarrollo sustentable, integral y descentralizado de las actividades económicas de acuerdo a lo que establece la Constitución de la República. La Empresa Pública tiene su domicilio en la ciudad de Cañar, además cuenta con oficinas en las zonas A, B, C, D y brinda sus servicios

en el territorio mancomunado; además tiene convenios interinstitucionales que permiten optimizar el servicio (EMMAIPC, 2024).

f) 4.3.1.1. Misión

Mantener a Cañar, Biblián, El Tambo y Suscal, limpias y saludables, a través de una gestión integral de residuos y desechos sólidos de calidad, con la participación activa de su personal comprometido con el desarrollo sostenible e innovador, mejorando continuamente nuestros servicios con la coparticipación de todos sus habitantes (EMMAIPC, 2024).

g) 4.3.1.2. Visión

Ser referente en la gestión de residuos y desechos sólidos a nivel internacional, sustentados en la innovación, la eficacia y eficiencia de sus procesos, siendo un ente facilitador de la minimización, reducción, reutilización y reciclaje, asegurando la satisfacción de sus usuarios, y contribuyendo al equilibrio ecológico (EMMAIPC, 2024).

h) 4.3.1.3. Organigrama de la empresa EMMAIPC-EP

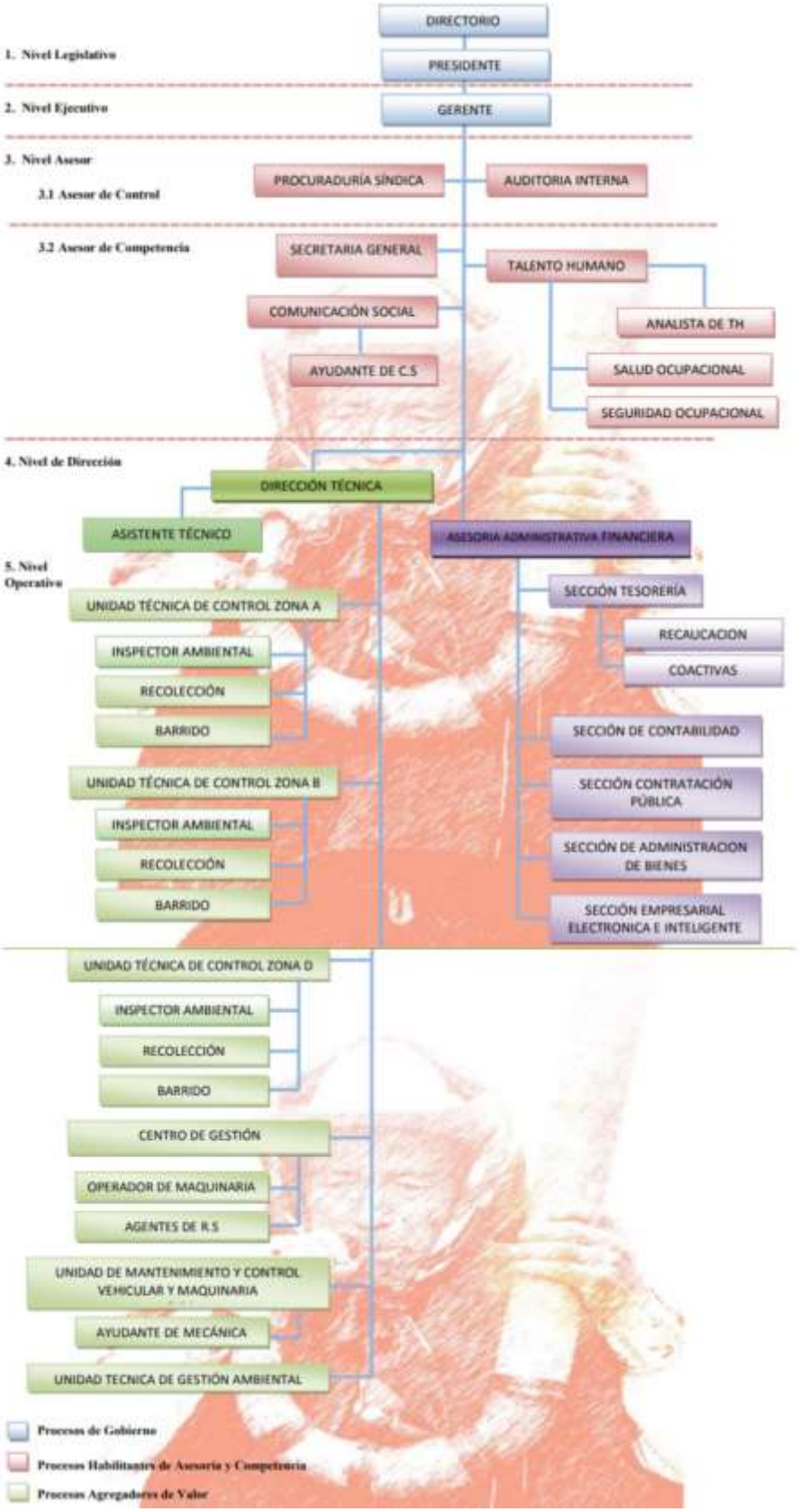


Ilustración 6. Organigrama de la EMMAIPC-EP. Fuente: (EMMAIPC-EP, 2018)

4.3.2. Identificación de los procesos de la empresa EMMAIPC-EP

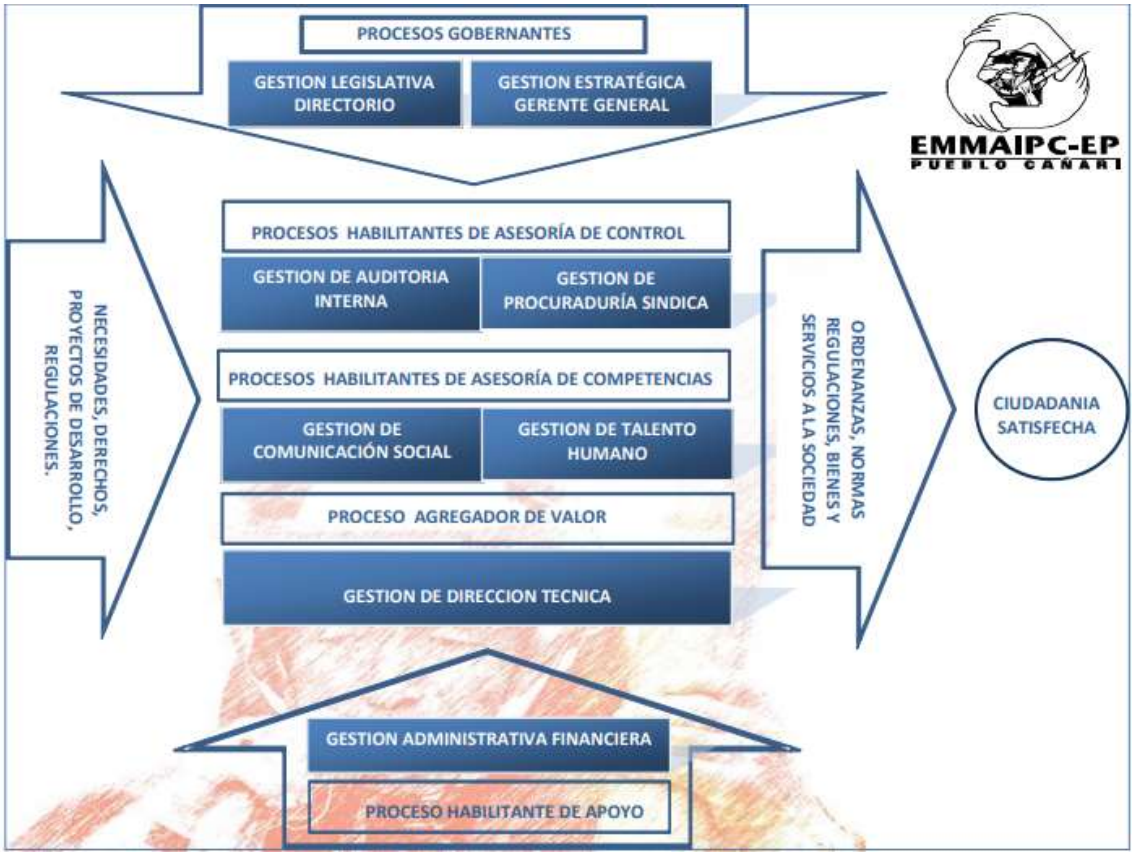


Ilustración 7. Mapa de procesos EMMAIPC-EP. Fuente (EMMAIPC-EP, 2018)

4.3.2. Alcance del Plan de Continuidad de Negocio

- **Objetivo del Alcance**

El Plan de Continuidad del Negocio tiene como objetivo garantizar la continuidad operativa de los procesos críticos de tecnología de la información (TI) ante cualquier interrupción significativa, ya sea provocada por desastres naturales, fallas tecnológicas, errores humanos, ciberataques, o cualquier otra amenaza potencial.

- **Áreas y Procesos Cubiertos:**
    - **Infraestructura de TI:** Servidor, redes, almacenamiento de datos, sistemas de comunicaciones y otros componentes críticos de infraestructura.
    - **Aplicaciones y Sistemas Críticos:** Sistemas de facturación, plataformas de soporte técnico y cualquier otra aplicación esencial para la continuidad de las operaciones.

- **Servicios de Datos y Comunicaciones:** Protección y recuperación de datos, incluyendo sistemas de respaldo y recuperación de datos, y sistemas de comunicación esenciales.
- **Personal Clave:** Equipos y roles críticos para la continuidad del negocio, incluyendo personal de TI, gerencia y personal operativo esencial.
- **Proveedores y Terceros:** Coordinación con proveedores de servicios esenciales y terceros que apoyan las operaciones críticas.

- **Límites del Alcance:**
  - **Exclusiones:** Procesos no críticos para la continuidad inmediata de las operaciones de TI, como proyectos de desarrollo de software a largo plazo, actividades de mantenimiento de rutina que no afecten directamente la continuidad, y sistemas no esenciales que puedan ser restaurados con prioridad baja.
  - **Delimitación Geográfica:** Incluye las instalaciones de EMMAIPC-EP únicamente en el cantón Cañar.

4.3.3. Análisis de Riesgos y Evaluación de Impacto en el Negocio (BIA)

Esta fase se llevará a cabo a través de la metodología MAGERIT, misma que fue escogida en el capítulo II. A continuación, se presentan las tablas que contienen la escala de valor para calificar a los procesos.

Tabla 3. Valores para evaluar los procesos críticos de la EMMAIPC-EP. Fuente: Autoría Propia

Valor Cuantitativo	Valor Cualitativo	Descripción
1	No aplica	No aplica criterio de importancia para el proceso
2	Muy bajo	El activo afecta procesos
4	Bajo	Las pérdidas o afectación seria menores y no incurrirán en sanciones pecuniarias
6	Medio	Las pérdidas o afectación pueden ser moderadas

8	Alto	Uno o varios procesos pueden ser seriamente afectados. Las pérdidas o afectación causan sanciones
10	Crítico	La organización se ve seriamente afectada y puede generar sanciones elevadas y afectar la credibilidad de la organización y sus procesos

Tabla 4. Calificación de procesos. Fuente: Autoría Propia

Tipo de Procesos	Macro proceso	Proceso	Subproceso	Criterios de valoración												
				[pi]	[Ipo]	[si]Seguridad	[cei]intereses comerciales o económicos	[da]Interrupción de servicio	[po] Orden público	[olm]	[adm]Administración y gestión	[lg]Pérdida de confianza(reputación)	[crm] Persecución de delitos	[rto]Tiempo de recuperación del servicio	[Ibl.nat] Información clasificada(nacional)	Total
Procesos Gobernantes	Gestión Legislativa Directorio	Elaboración de políticas Institucionales	Análisis de necesidades normativas.	1	10	6	1	1	1	4	6	6	1	6	4	47
			Redacción y revisión de políticas.	1	10	6	2	1	2	4	6	4	1	4	6	47
		Aprobación de Normativas y Reglamentos	Evaluación y aprobación de propuestas normativas.	2	10	4	2	2	4	6	6	6	2	6	6	56
	Gestión Estratégica Gerente General	Planeación y desarrollo de estrategias organizacionales	Dirección y toma de decisiones estratégicas	4	4	6	6	1	1	2	6	6	1	2	4	45
			Definición de objetivos estratégicos	1	8	4	6	4	1	2	10	8	1	6	4	55
			Supervisión de la ejecución de estrategias	1	2	4	6	4	1	4	10	4	1	4	2	37
			Establecimiento de indicadores clave de desempeño (KPIs).	4	4	4	8	4	2	8	10	6	2	6	2	60

			Ajustes y realineación de estrategias en función del desempeño y cambios en el entorno.	4	4	4	8	6	2	8	10	8	2	6	2	64
Procesos Operativos	Gestión de auditoría Interna	Revisión de Cumplimiento Normativo	Evaluación del cumplimiento de leyes y regulaciones aplicables.	2	10	8	4	4	4	6	8	4	4	6	4	64
			Auditorías internas de conformidad.	2	10	4	1	2	2	6	8	6	4	8	4	57
		Evaluación de Riesgos y Controles Internos	Identificación y análisis de riesgos organizacionales.	4	10	8	8	8	4	10	8	8	6	8	6	88
			Revisión y prueba de controles internos.	4	10	8	6	6	4	8	8	6	6	8	4	78
		Informe y Seguimiento de Auditorías	Elaboración de informes de auditoría con hallazgos y recomendaciones.	1	8	6	1	1	4	4	8	1	1	4	4	43
			Monitoreo del cumplimiento de recomendaciones y acciones correctivas.	2	6	4	2	1	1	4	8	1	2	2	4	37
	Gestión de Procuraduría síndica	Asesoría Legal y Consultoría	Asesoramiento en cuestiones legales y cumplimiento normativo.	4	10	2	2	4	2	1	6	4	2	1	1	39
			Elaboración y revisión de documentos legales y contratos.	4	10	4	2	1	1	4	4	2	2	4	4	42
		Representación Judicial y Extrajudicial	Representación de la EMMAIPC-EP en procesos judiciales y administrativos.	2	10	6	8	4	1	1	4	2	1	6	1	46
			Negociación y resolución de disputas legales.	4	8	4	6	4	1	1	2	2	1	4	1	38
	Gestión de talento humano	Reclutamiento y Selección	Análisis de necesidades de personal.	4	6	2	6	4	4	6	6	4	2	4	1	49
			Publicación de vacantes y gestión de aplicaciones.	2	4	1	6	4	2	8	8	6	4	6	2	53
			Proceso de entrevistas y selección de candidatos.	8	8	4	6	4	2	6	8	6	2	2	2	58

		Capacitación y Desarrollo	Diseño y ejecución de programas de formación.	4	6	4	6	2	1	6	2	2	4	4	4	45
		Gestión del Desempeño	Definición de objetivos y metas individuales.	4	2	4	6	1	1	8	4	1	1	2	4	38
			Implementación de planes de mejora y desarrollo profesional.	6	6	4	6	4	2	6	8	6	2	4	1	55
		Relaciones Laborales y Bienestar	Implementación de políticas de bienestar y salud laboral.	6	8	8	6	4	2	8	8	6	2	4	1	63
	Gestión de Comunicación Social	Manejo de la comunicación institucional	Gestión de redes sociales	4	6	4	8	4	4	6	6	8	2	6	2	60
			Relaciones públicas	4	6	4	8	4	6	6	6	8	2	6	2	62
			Capacitación y desempeño	2	6	2	4	2	1	6	6	4	1	4	1	39
			Revisión de cumplimiento normativo	4	10	6	6	4	4	6	8	8	4	6	4	70
Procesos Agregado de Valor	Gestión de Dirección técnica	Soporte técnico (TI)	Manejo del servidor	8	10	10	10	10	6	10	10	8	6	10	6	104
			Gestión de Solicitudes de Servicio	4	6	8	6	10	2	8	6	6	2	10	2	70
			Mantenimiento Preventivo y Correctivo	6	8	8	8	10	4	10	8	8	4	10	4	88
			Gestión de la Seguridad de TI	8	10	10	8	8	4	10	8	10	6	8	6	96
		Planificación y Ejecución de proyectos técnicos	Identificación y Priorización de Proyectos	2	4	4	6	4	2	6	8	4	2	4	2	48
			Ejecución y Monitoreo de Proyectos	2	6	6	8	8	2	8	10	8	2	8	2	70
Procesos	Gestión Administrativa Financiera	Contabilidad y Finanzas	Registro Contable	4	10	8	8	8	4	8	8	8	6	8	2	82
			Elaboración de Estados Financieros	4	10	8	10	8	4	8	10	10	8	8	1	89

		Gestión de Tesorería	Gestión de Liquidez	4	10	8	10	8	2	10	10	8	4	10	4	88
			Inversiones y Financiamiento	4	10	8	10	8	2	8	10	8	4	8	4	84

i) 4.3.3.1. Identificación de Activos

Para garantizar la continuidad de las operaciones y la seguridad de la información en la EMMAIPC-EP, se ha llevado a cabo una clasificación detallada de todos los activos tecnológicos. Esta clasificación, fundamentada en el libro II de Magerit Versión 3, divide los activos en dos grandes grupos: los activos primarios, que corresponden a los procesos críticos para el negocio, y los activos secundarios, que incluyen componentes tangibles como hardware, software y redes, así como recursos intangibles como el personal y la estructura organizativa.

Tabla 5. Identificación de activos de TI. Fuente: Autoría Propia

ID Activo	Activo	Descripción	Caracterización	Custodio
Act - 001	Servidor	Equipo informático central que proporciona una amplia gama de servicios y recursos a los usuarios de la organización.	[HW]Equipamiento informático (hardware)	Responsable de TI
Act - 002	Sistema de facturación	Aplicación informática diseñada para generar, gestionar y enviar facturas a los usuarios de la empresa. Este sistema automatiza los procesos de facturación, garantizando la precisión, eficiencia y cumplimiento de las normativas fiscales vigentes.	[SW] Software - Aplicaciones informáticas	Jefe de Contabilidad
Act - 003	Sistema Informático SIGAME	SIG-AME, o Sistema Integral de Gestión para Municipalidades Ecuatorianas, es una plataforma informática desarrollada por la Asociación de Municipalidades Ecuatorianas (AME) con el objetivo de optimizar y automatizar los procesos administrativos y financieros de los Gobiernos Autónomos Descentralizados (GAD) a nivel nacional.	[SW] Software - Aplicaciones informáticas	Responsable del área de tesorería

Act - 004	Router Mikro Tik	Permite conectar el servidor y los dispositivos de red con el fin de determinar una comunicación eficiente y segura entre ellos.	[HW]Equipamiento informático (hardware)	Responsable de TI
Act - 005	Página Web	Es un portal de información municipal diseñada para mantener a los ciudadanos del Pueblo Cañari informados sobre los servicios de gestión de residuos sólidos que ofrece la empresa	[essential] Activos esenciales	Encargado del departamento de comunicación social
Act - 006	Personal del Departamento de Tecnologías de la Información y Comunicación	Persona encargada de Administrar el Departamento	[P] Personal	Responsable de TI
Act - 007	cableado estructurado	La empresa EMMAIPC-EP, posee una infraestructura de cableado estructurada para conectar dispositivos electrónicos	[COM] Redes de comunicaciones	Responsable de TI

Act - 0009	Reloj Biométrico	Dispositivo de control de acceso que se utiliza para asegurar el registro preciso de los horarios de entrada y salida del personal.	[HW]Equipamiento informático (hardware)	Responsable de TI

j) 4.3.3.2. Identificación de Amenazas y Vulnerabilidades de los servicios de TI

La siguiente fase de identificación de amenazas y vulnerabilidades de los activos es crucial en la elaboración de un Plan de Continuidad del Negocio (BCP), ya que proporciona la base sobre la cual se construyen las estrategias y procedimientos para garantizar la continuidad de las operaciones en caso de incidentes.

Para ello, se determinan escalas de valor cuantitativas y cualitativas que permitirán calificar a los activos.

Tabla 6. Escalas de valor para la calificación de los activos. Fuente: Autoría Propia

Valor Cuantitativo	Valor Cualitativo	Descripción
1-2	Muy Bajo	El activo causa un daño irrelevante

3-4	Bajo	El activo puede afectar una tarea aislada de la operación o del proceso
5-6	Medio	El activo puede afectar de forma parcial una operación o un proceso.
7-8	Alto	Uno o varios procesos pueden ser seriamente afectados. Las pérdidas o afectación causan sanciones
9-10	Muy Alto	La empresa se ve seriamente afectada y puede generar sanciones elevadas y afectar su credibilidad

Una vez determinada, la escala de valoración, se procede a evaluar a los activos en base a los pilares de la seguridad de la información como son la confidencialidad, disponibilidad, autenticidad, trazabilidad e integridad.

Además, se presenta una tabla con una escala para valorar el riesgo con valores desde 1-10 que se consideran como un riesgo muy bajo y 41-50 como un valor de riesgo crítico.

Tabla 7. Escala de valor para los riesgos. Fuente: Autoría Propia

Valor	IMPORTANCIA
1-10	Muy Bajo
11-20	Bajo
21-30	Medio
31-40	Alto
41-50	Crítico

Tabla 8. Evaluación de activos de TI. Fuente: Autoría Propia

ID Activo	Activo	Tipo de Activo	Confidencialidad	Disponibilidad	Autenticidad	Trazabilidad	Integridad	Total
Act - 001	Servidor	[HW]Equipamiento informático (hardware)	10	10	10	8	10	48
Act - 002	Sistema de facturación	[SW] Software - Aplicaciones informáticas	8	10	9	9	10	46
Act - 003	Sistema Informático SIGAME		8	10	7	8	8	41
Act - 004	Router Mikro Tik	[HW]Equipamiento informático (hardware)	6	9	6	7	8	36
Act - 005	Página Web	[essential] Activos esenciales	6	8	8	8	10	40

Act 006	-	Personal del Departamento de Tecnologías de la Información y Comunicación	[P] Personal	10	10	8	10	10	48
Act 007	-	cableado estructurado	[COM] Redes de comunicaciones	8	10	8	8	8	42
Act 0009	-	Reloj Biométrico	[HW]Equipamiento informático (hardware)	6	8	6	6	8	32

Identificados los activos más críticos del área de TI de la EMMAIPC-EP, se procede a la identificación de las amenazas bajo la metodología de Magerit, tomando en cuenta el catálogo de amenazas que esta metodología proporciona.

Tabla 9. Identificación de amenazas de los activos críticos de TI. Fuente: Autoría Propia

ID Activo	Activo	Tipo de Activo	ID Amenaza	Amenaza
			[N.1]	Fuego
			[N.2]	Daños por agua

Act - 001	Servidor	[HW]Equipamiento informático (hardware)	[I.1]	Fuego
			[I.2]	Daños por agua
			[I.5]	Avería de origen físico o lógico
			[I.6]	Corte del suministro eléctrico
			[I.10]	Degradación de los soportes de almacenamiento de la información
			[E.1]	Errores de los usuarios
			[E.4]	Errores de configuración
			[E.8]	Difusión de software dañino
			[E.18]	Destrucción de información
			[E.20]	Vulnerabilidades de los programas (software)
			[E.23]	Errores de mantenimiento / actualización de equipos
			[A.7]	Uso no previsto
			[A.8]	Difusión de software dañino
			[A.12]	Análisis de tráfico
			[E.19]	Fugas de Información
			[E.24]	Caída del sistema por agotamiento de recursos

			[A.24]	Denegación de servicio
Act - 002	Sistema de facturación	[SW] Software - Aplicaciones informáticas	[E.1]	Errores de los usuarios
			[E.15]	Alteración Accidental de la Información
			[E.20]	Vulnerabilidades de los programas (software)
			[E.21]	Errores de Mantenimiento/ Actualización de programas
			[A.6]	Abuso de privilegios de acceso
			[A.22]	Manipulación de programas
Act - 003	Sistema Informático SIGAME		[E.1]	Errores de los usuarios
			[E.19]	Fugas de Información
			[E.20]	Vulnerabilidades de los programas (software)
			[E.21]	Errores de Mantenimiento/ Actualización de programas
	Personal del Departamento de Tecnologías		[A.28]	Indisponibilidad del personal
			[A.29]	Extorsión
			[A.30]	Ingeniería Social

Act - 006	de la Información y Comunicación	[P] Personal	[E.19]	Fuga de Información
			[E.7]	Deficiencia en la Organización
			[E.3]	Errores de monitorización
			[A.25]	Robo
Act - 007	cableado estructurado	[COM] Redes de comunicaciones	[I.8]	Avería de origen físico o lógico
			[I.6]	Corte del suministro eléctrico
			[E.1]	Fallos de servicios de comunicación
			[A.24]	Denegación de Servicio
			[A.12]	Análisis del trafico

Análisis de Riesgos

En el entorno dinámico y competitivo de hoy, la protección de los activos críticos de la empresa es fundamental para asegurar la continuidad del negocio y el logro de los objetivos estratégicos. EMMAIPC-EP, comprometida con la excelencia operativa y la seguridad, ha emprendido un exhaustivo análisis de riesgos enfocado en sus activos más valiosos. Este apartado aborda el análisis de riesgos de estos activos críticos, utilizando una metodología que evalúa la probabilidad de ocurrencia y el impacto potencial de diversos riesgos.

El análisis de riesgos se fundamenta en dos componentes esenciales: la probabilidad y el impacto. La probabilidad se refiere a la posibilidad de que un evento de riesgo ocurra, basándose en factores históricos, tendencias actuales y la exposición a amenazas específicas. El impacto, por otro lado, mide las consecuencias potenciales de dicho evento, evaluando el grado de daño que podría causar a los activos críticos y, por ende, a la organización en su conjunto.

Mediante la evaluación conjunta de estos dos factores, se obtiene una visión integral del riesgo que permite priorizar las acciones de mitigación y asignar los recursos de manera efectiva. Este análisis no solo identifica las áreas de vulnerabilidad, sino que también proporciona una base sólida para desarrollar estrategias de gestión de riesgos que fortalezcan la resiliencia de EMMAIPC-EP. En la tabla siguiente, se detallarán los resultados del análisis, destacando los activos críticos evaluados y los riesgos identificados.

Tabla 10. Escala de probabilidad. Fuente: Autoría Propia

Probabilidad	**Descripción**	**Valor**
Raro	Podría presentarse solo en circunstancias excepcionales.	1
Improbable	Probabilidad de ocurrencia baja	2

Posible	La amenaza podría presentarse en algún momento	3
Probable	Se puede presentar frecuentemente	4
Casi Seguro	Probabilidad de ocurrencia muy Alta	5

Tabla 11. Escala de impacto. Fuente: Autoría Propia

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

Tabla 12. Escala de valoración del riesgo. Fuente: Autoría propia

Riesgo	Descripción	Valor
Bajo	Riesgo aceptable	**1-4**
Medio	Riesgo tolerable	**5-8**
Alto	Riesgo inaceptable	**9-12**
Crítico	Riesgo inadmisible	**13-16**

En la siguiente matriz, se analiza la probabilidad y el impacto de cada amenaza de acorde a los rangos de valoración de las tablas.

Tabla 13. Análisis de riesgos. Fuente: Autoría Propia

ID Activo	Activo	ID Amenaza	Amenaza	Probabilidad	Impacto	Riesgo
		[N.1]	Fuego	1	4	4
		[N.2]	Daños por agua	1	3	3

Act 001 - Servidor	[I.1]	Fuego	1	3	3
	[I.2]	Daños por agua	1	3	3
	[I.5]	Avería de origen físico o lógico	2	4	8
	[I.6]	Corte del suministro eléctrico	3	5	15
	[I.10]	Degradación de los soportes de almacenamiento de la información	1	3	3
	[E.1]	Errores de los usuarios	2	4	8
	[E.4]	Errores de configuración	2	4	8
	[E.8]	Difusión de software dañino	1	5	5
	[E.18]	Destrucción de información	1	5	5
	[E.20]	Vulnerabilidades de los programas (software)	2	4	8
	[E.23]	Errores de mantenimiento / actualización de equipos	2	5	10
	[A.7]	Uso no previsto	1	3	3
	[A.8]	Difusión de software dañino	1	4	4
	[A.12]	Análisis de tráfico	2	4	8
	[E.19]	Fugas de Información	2	4	8

		[E.24]	Caída del sistema por agotamiento de recursos	2	5	10
		[A.24]	Denegación de servicio	3	5	15
Act 002	Sistema de facturación	[E.1]	Errores de los usuarios	2	4	8
		[E.15]	Alteración Accidental de la Información	1	4	4
		[E.20]	Vulnerabilidades de los programas (software)	2	5	10
		[E.21]	Errores de Mantenimiento/ Actualización de programas	2	5	10
		[A.6]	Abuso de privilegios de acceso	2	4	8
		[A.22]	Manipulación de programas	2	5	10
Act 003	Sistema Informático SIGAME	[E.1]	Errores de los usuarios	2	4	8
		[E.19]	Fugas de Información	2	4	8
		[E.20]	Vulnerabilidades de los programas (software)	1	5	5
		[E.21]	Errores de Mantenimiento/ Actualización de programas	2	5	10
	Personal del Departamento de	[A.28]	Indisponibilidad del personal	2	4	8
		[A.29]	Extorsión	2	5	10

Act 006	Tecnologías de la Información y Comunicación	[A.30]	Ingeniería Social	3	5	15
		[E.19]	Fuga de Información	1	5	5
		[E.7]	Deficiencia en la Organización	1	5	5
		[E.3]	Errores de monitorización	1	3	3
		[A.25]	Robo	1	5	5
Act 007	cableado estructurado	[I.8]	Avería de origen físico o lógico	2	5	10
		[I.6]	Corte del suministro eléctrico	3	5	15
		[E.1]	Fallos de servicios de comunicación	2	4	8
		[A.24]	Denegación de Servicio	1	4	4
		[A.12]	Análisis del trafico	1	4	4

Controles

En el proceso de análisis de riesgos llevado a cabo para los activos críticos de la EMMAIPC-EP, se ha identificado una serie de amenazas que, de materializarse, podrían tener un impacto significativo en la continuidad del negocio, particularmente en el ámbito de TI. Utilizando la metodología Magerit, se han evaluado la probabilidad y el impacto de estas amenazas, lo que ha permitido clasificar los riesgos asociados en diferentes niveles de criticidad.

Los riesgos que se encuentran en las categorías más altas (marcados en colores tomate y rojo) representan una amenaza considerable para la operatividad y la seguridad de la infraestructura tecnológica. Estos riesgos no solo tienen una alta probabilidad de ocurrencia, sino que también podrían causar daños significativos que comprometerían la disponibilidad, integridad y confidencialidad de los sistemas de información y servicios críticos.

En respuesta a esta evaluación, se hace imperativo la implementación de controles específicos y efectivos que permitan mitigar estos riesgos de manera proactiva. Estos controles deben ser diseñados y aplicados con el objetivo de reducir tanto la probabilidad de ocurrencia como el impacto potencial de las amenazas identificadas. En las secciones siguientes, se describirán las medidas de control propuestas para cada uno de los riesgos críticos, incluyendo tanto acciones preventivas como correctivas, con el fin de asegurar la continuidad del negocio y la resiliencia de las operaciones de TI ante posibles incidentes.

Tabla 14. Salvaguardas. Fuente: Autoría Propia

ID Activo	Activo	ID Amenaza	Amenaza	Riesgo	CONTROL
		[I.6]	Corte del suministro eléctrico	15	- Aseguramiento de la disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	10	- Monitoreo proactivo de recursos - Escalabilidad automática

Act 001	- Servidor	[A.24]	Denegación de servicio	15	- Protecciones Generales - Implementación de sistemas de prevención y detección de intrusiones - Redundancia y balanceo de carga
Act 002	- Sistema de facturación	[E.20]	Vulnerabilidades de los programas (software)	10	- Actualización y parches - Análisis de Vulnerabilidades - Segregación de Entornos
		[E.21]	Errores de Mantenimiento/ Actualización de programas	10	- Gestión de cambios
		[A.22]	Manipulación de programas	10	- Control de acceso - Registro de Auditoría - Monitoreo Continuo
Act 003	- Sistema Informático SIGAME	[E.21]	Errores de Mantenimiento/ Actualización de programas	10	- Automatización de procesos - Planificación de mantenimiento
Act 006	- Personal del Departamento de Tecnologías de la Informa	[A.30]	Ingeniería Social	15	- Capacitación en concienciación de seguridad - Políticas de seguridad
		[A.29]	Extorsión	10	- Formación y concienciación

	ción y Comunicación				
Act 007	- cableado estructurado	[I.8]	Avería de origen físico o lógico	10	- Protección de los Equipos Informáticos - Aseguramiento de la disponibilidad - Protección de las Aplicaciones Informáticas
		[I.6]	Corte del suministro eléctrico	15	- Aseguramiento de la disponibilidad

La tabla presenta una evaluación detallada de los riesgos asociados a varios activos críticos en una infraestructura de TI, proporcionando una visión clara de las amenazas que podrían comprometer la seguridad y la operatividad de estos activos. Se incluye un análisis cuantitativo del riesgo, acompañado de controles específicos diseñados para mitigar o eliminar dichas amenazas.

- **Servidor:**

- **Corte del suministro eléctrico:** Esta amenaza presenta un alto riesgo de impacto crítico en la operatividad del servidor. Los controles propuestos incluyen el aseguramiento de la disponibilidad del suministro eléctrico a través de fuentes de alimentación redundantes, como UPS o generadores, y la planificación de contingencias para garantizar la continuidad del servicio.

- **Caída del sistema por agotamiento de recurso:** Identificada como una amenaza de riesgo medio, este evento podría degradar significativamente el rendimiento del servidor. Los controles implementados incluyen un monitoreo proactivo de recursos, la implementación de escalabilidad automática para ajustar dinámicamente los recursos disponibles, y la optimización del uso de estos recursos.

- **Denegación de servicio:** Esta amenaza crítica podría incapacitar el servidor por completo. Se han propuesto controles robustos, como la implementación de sistemas de prevención y detección de intrusiones (IPS/IDS), junto con la

redundancia y el balanceo de carga para distribuir las solicitudes de manera eficiente y evitar sobrecargas.

- **Sistema de facturación:**

- **Vulnerabilidades de los programas (software):** Las vulnerabilidades en el software utilizado para la facturación representan un riesgo medio que puede ser explotado por atacantes. Los controles incluyen la aplicación regular de parches de seguridad, análisis continuos de vulnerabilidades, y la segregación de entornos para minimizar el impacto de posibles fallos de seguridad en el entorno de producción.
- **Errores de Mantenimiento/Actualización de programas:** El riesgo de errores durante el mantenimiento o la actualización del software es mitigado mediante la gestión de cambios, planificación cuidadosa de mantenimientos, y la automatización de procesos para reducir la intervención manual.
- **Manipulación de programas:** Para mitigar el riesgo de manipulación de software, se propone implementar controles de acceso estrictos, monitoreo continuo, y el uso de auditorías de registros para detectar y responder rápidamente a cualquier actividad no autorizada.

- **Sistema Informático SIGAME:**

- **Errores de Mantenimiento/Actualización de programas:** Similar al sistema de facturación, se considera un riesgo medio que puede ser manejado mediante automatización, planificación y revisión exhaustiva de los procesos de actualización y mantenimiento.

- **Personal del Departamento de Tecnología de la Información y Comunicación:**

- **Ingeniería Social:** Este riesgo alto debido a posibles ataques de ingeniería social es abordado con un enfoque en la capacitación continua del personal en conciencia de seguridad y la implementación de políticas estrictas que dificulten la manipulación psicológica por parte de actores maliciosos.
- **Extorsión:** El control propuesto para esta amenaza está diseñado para mitigar el riesgo de extorsión a través de la capacitación regular y efectiva del personal sobre

cómo identificar, evitar y reportar intentos de extorsión. La formación debe incluir escenarios de extorsión típicos, las tácticas que los extorsionadores podrían utilizar, y las mejores prácticas para proteger tanto la información personal como la corporativa.

- **Cableado estructurado:**

- **Amenazas como averías de origen físico o lógico:** El cableado estructurado es vulnerable a fallos físicos o lógicos, y se han implementado controles como la protección de los equipos y el monitoreo para asegurar la disponibilidad continua del servicio.

1.1.2 4.3.3. Análisis de Impacto en el Negocio (BIA)

El Análisis de Impacto en el Negocio (BIA) es un proceso fundamental para identificar y evaluar los efectos potenciales que diversas amenazas o interrupciones podrían tener sobre las operaciones críticas de EMMAIPC-EP. El objetivo principal del BIA es proporcionar una comprensión clara de las consecuencias de la inactividad o degradación de los activos críticos de TI y establecer las prioridades para la recuperación y continuidad del negocio.

a) 4.3.3.1. Identificación de actividades críticas

Los procesos críticos dentro de EMMAIPC-EP han sido identificados a través del análisis de riesgos previo. Estos procesos son esenciales para la continuidad de las operaciones diarias y para el cumplimiento de los objetivos estratégicos de la empresa.

Los procesos críticos dentro de EMMAIPC-EP han sido identificados a través del análisis de riesgos previo. Estos procesos son esenciales para la continuidad de las operaciones diarias y para el cumplimiento de los objetivos estratégicos de la empresa. Entre estos procesos destacan:

- **Facturación y Gestión Financiera:** La capacidad de emitir facturas y gestionar transacciones financieras es fundamental para la estabilidad económica de la organización.

- **Operaciones del Servidor Principal:** Los servidores son el núcleo de la infraestructura de TI, y su inactividad puede paralizar varias funciones operativas.

- **Gestión de Información del Personal:** La integridad y disponibilidad de la información relacionada con el personal es crucial para la toma de decisiones y la administración de recursos humanos.
- **Gestión de TI y Comunicación:** Este proceso incluye la gestión de sistemas críticos y comunicaciones, que son esenciales para el funcionamiento de todos los demás procesos.

b) 4.3.3.2. Evaluación del impacto de la interrupción

El impacto de la interrupción de estos procesos se evalúa en términos de varios criterios, incluidos los financieros, operacionales, reputacionales, y legales. A continuación, se detalla el impacto de las principales amenazas identificadas en los activos críticos:

- **Corte del suministro eléctrico en el Servidor:**
    - **Impacto Financiero:** La falta de acceso a los servidores puede detener todas las operaciones de facturación, resultando en pérdida de ingresos y retrasos en la gestión financiera.
    - **Impacto Operacional:** Interrupciones en el servidor pueden causar la inactividad total de sistemas críticos, impidiendo el acceso a aplicaciones esenciales y datos almacenados.
    - **Impacto Reputacional:** Reiteradas interrupciones pueden afectar la confianza de los clientes y socios comerciales.
    - **Impacto Legal:** La falta de disponibilidad de información podría llevar a incumplimientos normativos y posibles sanciones.
- **Denegación de Servicio (DoS) en el Servidor:**
    - **Impacto Financiero:** Una denegación de servicio exitosa puede resultar en la pérdida de ingresos debido a la incapacidad de procesar transacciones en línea.
    - **Impacto Operacional:** La operación del negocio se ve severamente afectada, causando posibles interrupciones prolongadas.
    - **Impacto Reputacional:** La percepción del cliente puede deteriorarse rápidamente si no se aborda el problema de manera efectiva.

- **Impacto Legal:** Las interrupciones pueden causar incumplimiento de contratos y normativas de tiempo de servicio (SLA).

- **Extorsión relacionada con el Personal del Departamento de TI:**
  - **Impacto Financiero:** La extorsión puede llevar a la divulgación de información confidencial o malversación de fondos, lo que puede resultar en pérdidas financieras significativas.
  - **Impacto Operacional:** Puede resultar en la inhabilidad para mantener la seguridad de la información o en el deterioro de la moral y productividad del personal.
  - **Impacto Reputacional:** La imagen de la organización puede ser gravemente dañada si la extorsión resulta en la pérdida o fuga de información crítica.
  - **Impacto Legal:** El mal manejo de datos sensibles bajo extorsión podría implicar violaciones legales, con consecuencias que varían desde multas hasta litigios.

c) 4.3.3.3. Determinación de objetivos de tiempo de recuperación y objetivos de punto de recuperación

Basado en el análisis de impacto, los procesos de recuperación se priorizarán de la siguiente manera:

1. **Restablecimiento del Servidor y Suministro Eléctrico:** Debido a la dependencia crítica de este activo, la recuperación del servidor se prioriza para asegurar que los sistemas operativos clave vuelvan a estar en línea lo antes posible.
2. **Mitigación de Denegaciones de Servicio:** La implementación de contramedidas inmediatas para restablecer el servicio en caso de un ataque DoS es crucial para minimizar la interrupción y restaurar la normalidad operativa.
3. **Respuesta ante Extorsión:** Acciones inmediatas para contener la situación y proteger la información crítica son esenciales para salvaguardar la integridad de la organización.

d) 4.3.3.4. Establecimiento de Tiempos de Recuperación

En el contexto de la planificación de la recuperación de desastres para EMMAIPC-EP, es esencial establecer tiempos de recuperación claros para cada uno de los activos críticos involucrados. Estos tiempos, conocidos como **Recovery Time Objectives (RTO)**, representan el período máximo de inactividad que la organización puede tolerar antes de que la falta de disponibilidad de un activo crítico afecte significativamente las operaciones.

La tabla a continuación presenta los RTO definidos para los activos más importantes dentro de la infraestructura de TI de EMMAIPC-EP, junto con la prioridad asignada para su recuperación. Estos tiempos de recuperación se han establecido teniendo en cuenta la criticidad de cada activo para la continuidad del negocio, así como el impacto potencial de su inactividad en términos financieros, operacionales, reputacionales y legales.

La correcta implementación de estos tiempos de recuperación permitirá a la organización priorizar sus esfuerzos de restauración en caso de un desastre, asegurando que los activos más vitales sean devueltos a un estado operativo dentro del tiempo permitido para minimizar el daño al negocio.

Tabla 15. Escala de Tiempos de Recuperación. Fuente: Autoría Propia

ACTIVO CRÍTICO	PROCESO AFECTADO	RTO (TIEMPO DE RECUPERACIÓN OBJETIVO)	PRIORIDAD
Servidor Principal	Operaciones del servidor, almacenamiento de datos, aplicaciones críticas	4 horas	Alta
Sistema de Facturación	Emisión de facturas, gestión financiera	6 horas	Alta
Sistema Informático SIGAME	Gestión de información, monitoreo de operaciones	8 horas	Media

Personal del Departamento de Tecnología	Gestión de TI, respuesta a incidentes	12 horas	Media
Cableado Estructurado	Conectividad de red y comunicaciones	24 horas	Media
Suministro Eléctrico (UPS y Generadores)	Continuidad de la energía para todos los sistemas	Inmediato (0 horas)	Crítica
Centro de Datos Alternativo	Sitio de recuperación de desastres	24 horas	Alta
Sistema de Respaldo de Datos	Recuperación de datos críticos	2 horas	Alta

---

A continuación, se realiza un análisis más detallado de la tabla anterior:

- **Servidor Principal:** Dado que el servidor aloja las aplicaciones críticas y el almacenamiento de datos, debe ser restaurado dentro de las 4 horas posteriores a un desastre para minimizar la interrupción del negocio.
- **Sistema de Facturación:** Es crucial para las operaciones financieras de la organización, por lo que debe estar operativo dentro de las 6 horas.
- **Sistema Informático SIGAME:** Afecta la gestión de la información y operaciones críticas, pero puede tolerar un tiempo de recuperación ligeramente mayor de hasta 8 horas.
- **Personal del Departamento de Tecnología:** Aunque es vital para la gestión de incidentes, el equipo puede tardar hasta 12 horas en estar completamente operativo, ya que la prioridad inmediata recae en la restauración de sistemas.
- **Cableado Estructurado:** Las redes y comunicaciones pueden soportar un tiempo de recuperación de 24 horas, aunque su restauración es crucial para el funcionamiento total.

- **Suministro Eléctrico:** Es crítico mantener el suministro de energía sin interrupciones, por lo que debe ser inmediato (0 horas de RTO).
- **Centro de Datos Alternativo:** En caso de un desastre mayor, el centro de datos alternativo debe estar operativo dentro de las 24 horas para asegurar la continuidad del negocio.
- **Sistema de Respaldo de Datos:** La recuperación de los datos críticos debe ser prioritaria y completarse en un máximo de 2 horas para evitar pérdida de información valiosa.

2. CONCLUSIONES

El diagnóstico realizado reveló que la infraestructura de TI en EMMAIPC-EP presenta deficiencias importantes en términos de preparación para la continuidad del negocio. Actualmente, la organización carece de un Plan de Continuidad del Negocio (BCP) formal, y las prácticas de gestión de TI no están alineadas con estándares internacionales, lo que deja a la entidad vulnerable a interrupciones operativas. Además, la falta de un inventario actualizado de activos críticos y la ausencia de capacitación específica en gestión de la continuidad del negocio reflejan una necesidad urgente de mejorar la infraestructura y las prácticas de TI para garantizar la resiliencia operativa.

Para abordar estas deficiencias, se desarrolló un marco de gestión de riesgos de TI que permitirá identificar, evaluar y priorizar de manera eficaz las amenazas que podrían comprometer la continuidad operativa de EMMAIPC-EP. Este marco proporciona una base sólida para mitigar los riesgos más críticos, como fallos en la infraestructura, desastres naturales y errores humanos, los cuales anteriormente no se gestionaban adecuadamente. La implementación de este marco fortalecerá la capacidad de la organización para anticiparse y responder proactivamente a incidentes que puedan afectar

la operación de sus sistemas críticos, consolidando así una estrategia de continuidad más robusta y efectiva.

El plan de acción diseñado para EMMAIPC-EP ofrece estrategias de recuperación de desastres y continuidad del negocio que son prácticas, escalables y adaptadas a las necesidades específicas de la organización. Este plan establece procedimientos claros para la restauración de operaciones críticas en caso de un incidente, asegurando que la organización pueda mantener la continuidad de sus servicios esenciales. Además, las estrategias propuestas son sostenibles a largo plazo y pueden ser ajustadas conforme la organización crezca o cambien sus necesidades, lo que garantiza una protección continua frente a potenciales amenazas operacionales.

3. **RECOMENDACIONES**

Es crucial que EMMAIPC-EP desarrolle e implemente un BCP específico para el área de TI, alineado con la norma ISO 22301, que contemple la identificación de riesgos, la evaluación del impacto en el negocio y la definición de procedimientos de recuperación y continuidad operativa.

Además, se recomienda formar al personal en la gestión de la continuidad del negocio y en la implementación de normativas como ISO 22301, para asegurar que estén preparados para actuar eficazmente ante cualquier incidente que pueda afectar la operatividad de la organización.

4. REFERENCIAS

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). Una revisión sistemática de la literatura sobre seguridad de la computación en la nube: amenazas y estrategias de mitigación. *IEEE Access* , 57792-57807.

Baud, J. L. (2017). *ITIL V3 preparación para la certificación ITIL Foundation V3 : más de 400 preguntas-respuestas.* Ediciones ENI.

Becerra Santiago, M. S. (2023). La resiliencia organizacional: un enfoque para la alta dirección. *Revista Ciencia Administrativa*, 75.

CCNA. (09 de 05 de 2024). *ccnadesdecero.es*. Obtenido de ccnadesdecero.es: https://ccnadesdecero.es/arquitecturas-red-en-evolucion/

CertiProf. (08 de 08 de 2023). *img1.wsimg.com.* Obtenido de img1.wsimg.com: https://img1.wsimg.com/blobby/go/e34bb864-bd76-46c5-9487-25939ec9b0ad/downloads/Material%2Bpara%2BEstudiante%2BISO%2B22301.pdf?ver=1716822568053

Cornejo, Y. (2023). Análisis de Riesgos de TI y Seguridad de la Información. *Academia Cibers*.

Crask, J. (2024). *Business Continuity Management: A Practical Guide to Organization Resilience and ISO 22301.* Kogan Page Publishers.

Ferguson Castro, N. (20 de 11 de 2023). *burjcdigital.urjc.es.* Obtenido de burjcdigital.urjc.es: https://burjcdigital.urjc.es/handle/10115/26187

García, A. E. (2023). *Seguridad de Equipos Informáticos. Edición 2024.* Madrid: RA-MA Editorial.

García, A., & Alexey, I. (01 de 01 de 2022). *repositorio.ucv.edu.pe.* Obtenido de repositorio.ucv.edu.pe: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/103847/Abad_GIA-SD.pdf?sequence=1&isAllowed=y

Gastelo Fernandez, E. J., & Rodríguez Flores , A. H. (01 de 01 de 2023). *repositorio.uss.edu.pe.* Obtenido de repositorio.uss.edu.pe: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10888/Gastelo%20Fernandez%20Edin%20%26%20Rodr%c3%adguez%20Flores%20Alfredo.pdf?sequence=1&isAllowed=y

Gómez, M. A., Candau, J., & Mañas, J. A. (2013). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Intranet. (01 de 01 de 2023). *www.funcionpublica.gov.co.* Obtenido de www.funcionpublica.gov.co: https://www.funcionpublica.gov.co/documents/34645357/34702994/Documento_tecnico_plan_continuidad_v5.pdf/937700b4-0ee6-d6e5-213d-5fcf190e9d3b?t=1685653157524#:~:text=Plan%20de%20continuidad%20de%20negocio,objetivos%20de%20continuidad%20del%20negocio.

ISO. (2019). *ISO 22301 Security and resilience — Business continuity management systems — Requirements.* Switzerland.

ISO. (22 de 05 de 2023). *www.iso.org*. Obtenido de www.iso.org: https://www.iso.org/es/contents/data/standard/08/28/82875.html

ISO 27001. (31 de 03 de 2024). *normaiso27001.es.* Obtenido de normaiso27001.es: https://normaiso27001.es/

ISO/IEC . (01 de 10 de 2022). *cdn.standards.iteh.ai.* Obtenido de cdn.standards.iteh.ai: https://cdn.standards.iteh.ai/samples/80585/7bca93ac16fd426a9bc717cadc9284d9/ISO-IEC-27005-2022.pdf

Montero, F. V. (2021). *Resiliencia organizacional (2ª ed.).* GEDISA.

Muñoz Gutiérrez , C. A. (01 de 01 de 2022). *repositorio.uisrael.edu.ec.* Obtenido de repositorio.uisrael.edu.ec: https://repositorio.uisrael.edu.ec/bitstream/47000/3363/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2022-006.pdf

Nair, A. (19 de 09 de 2019). *cdn2.hubspot.net.* Obtenido de cdn2.hubspot.net: https://cdn2.hubspot.net/hubfs/2139287/Introduction-to-Information-Security-Risk-Assessment-using-FAIR.pdf

nqa. (10 de 11 de 2021). *www.nqa.com.* Obtenido de www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-ISO-22301-Implementation-Guide.pdf

nqa. (08 de 03 de 2024). *www.nqa.com.* Obtenido de www.nqa.com: https://www.nqa.com/getmedia/ae12c945-4dbb-4b73-a4e3-996261a540af/NQA-ISO-27001-Implementation-Guide.pdf

Parra, P. A. (2019). Metodologia Octave. 1-7.

Pedrosa, J. M. (08 de 07 de 2020). *openaccess.uoc.edu.* Obtenido de openaccess.uoc.edu: https://openaccess.uoc.edu/bitstream/10609/116647/7/jmpereaTFG0620memoria.pdf

Rodríguez Rodríguez, C. G. (01 de 01 de 2020). *repository.unipiloto.edu.co.* Obtenido de repository.unipiloto.edu.co: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9547/La%20importancia%20de%20un%20plan%20de.pdf?sequence=1&isAllowed=y

Selliliar. (15 de 05 de 2024). *selliliar.live*. Obtenido de selliliar.live: https://selliliar.live/product_details/26045704.html

Serrano Saenz, Y. (01 de 06 de 2023). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/handle/10596/56740

Sevillano, F. (2021). *Ciberseguridad industrial e infraestructuras críticas.* Ediciones de la U.

Velthuis, M. G., & González, F. R. (2020). *Gobierno y Gestión de las Tecnologías y los Sistemas de Información.* Madrid: RA-MA Editorial.

Wijayarathne, S. (2022). ISO 27001 IMPLEMENTATIONS. *ResearchGate*.

5. **ANEXOS**

Anexo 1. Plan de continuidad

EMMAIPC

CAÑAR, BIBLIÁN, EL TAMBO Y SUSCAL

PLAN DE CONTINUIDAD DE NEGOCIO

2024

1. INTRODUCCIÓN

El Plan de Continuidad de Negocio (PCN) para EMMAIPC-EP está diseñado para garantizar que la organización pueda mantener operaciones críticas y minimizar el impacto de interrupciones significativas en sus procesos de negocio. Este plan se ha desarrollado en respuesta a la necesidad de proteger los activos de TI y garantizar la resiliencia ante posibles desastres, interrupciones en el suministro de energía, fallos tecnológicos, o incidentes de seguridad.

2. OBJETIVOS

2.1. Objetivo General

Garantizar la continuidad operativa de los procesos críticos de negocio ante cualquier interrupción significativa, minimizando el impacto en las operaciones, protegiendo los activos clave de la organización, y asegurando una recuperación eficiente y rápida para mantener la resiliencia organizacional y el cumplimiento de los objetivos estratégicos de EMMAIPC-EP.

2.2. Objetivos Específicos

- Identificar y priorizar los procesos críticos de negocio, determinando cuáles son los procesos y activos más esenciales para la continuidad operativa de EMMAIPC-EP, estableciendo un orden de prioridad para su recuperación en caso de una interrupción.
- Establecer tiempos de recuperación objetivo (RTO) para cada proceso crítico definiendo los períodos máximos de inactividad tolerable para cada activo y proceso crítico, asegurando que se mantengan dentro de los límites aceptables durante una interrupción.
- Desarrollar y documentar estrategias de recuperación para cada escenario de desastre: Crear procedimientos claros y detallados para la recuperación de sistemas, infraestructura y operaciones clave, adaptados a diferentes tipos de incidentes potenciales.

3. ALCANCE

La propuesta del Plan de Continuidad de Negocio para EMMAIPC-EP se enfoca en la creación de una documentación exhaustiva que establezca el protocolo a seguir en caso de un evento catastrófico o cualquier otro incidente que pueda interrumpir los servicios críticos de la empresa. Este plan detallará las responsabilidades individuales y los procedimientos necesarios para restaurar

las operaciones en el menor tiempo posible. Todos los procedimientos y estrategias delineados en este plan están alineados con los lineamientos establecidos por un BCP (Business Continuity Plan) y cumplen con las mejores prácticas internacionales, como las establecidas en la norma ISO 22301.

Contar con un BCP sólido, coherente y actualizado es crucial para minimizar el tiempo de inactividad de los servicios tecnológicos y operativos de EMMAIPC-EP, especialmente en situaciones catastróficas que puedan amenazar los recursos críticos de la organización. Este manual se elaboró específicamente para el área de Tecnología de la Información, dado que, tras un exhaustivo análisis y gestión de riesgos, se ha determinado que la mayoría de los procesos operativos y administrativos dependen directamente de la infraestructura de TI.

4. Importancia del PCN para EMMAIPC-EP

El Plan de Continuidad de Negocio (BCP) es un componente esencial para la resiliencia operativa de EMMAIPC-EP. En un entorno donde las amenazas pueden variar desde desastres naturales hasta fallos tecnológicos y ciberataques, contar con un BCP robusto asegura que la organización pueda responder de manera efectiva a incidentes inesperados, minimizando el impacto en las operaciones y protegiendo los intereses de la empresa.

Puesto que la EMMAIPC-EP depende de una infraestructura de TI que sustenta todas sus operaciones diarias. Un BCP bien diseñado protege estos activos, garantizando que los sistemas críticos, como servidores, redes de comunicación y aplicaciones clave, puedan ser restaurados rápidamente en caso de una interrupción.

La interrupción de los servicios puede tener consecuencias devastadoras, tanto en términos de reputación como de pérdidas financieras. Un BCP asegura que los procesos esenciales, como la gestión de facturación y la administración de sistemas de información, continúen funcionando o se restablezcan en el menor tiempo posible, evitando así interrupciones prolongadas.

5. Análisis de Impacto en el Negocio

El Análisis de Impacto en el Negocio (BIA) es un proceso clave en la gestión de la continuidad del negocio, diseñado para identificar y evaluar los efectos potenciales que diversas amenazas pueden tener sobre las operaciones críticas de EMMAIPC-EP. A través del BIA, se establece la relación entre los procesos críticos de negocio y el impacto que su interrupción tendría sobre la organización, permitiendo priorizar las acciones de recuperación y asegurar la continuidad operativa.

1. Identificación de Procesos Críticos

Los procesos críticos en EMMAIPC-EP son aquellos que, en caso de una interrupción, podrían afectar significativamente las operaciones, la reputación y la estabilidad financiera de la organización. Estos procesos han sido identificados a través de un análisis detallado y se clasifican de la siguiente manera:

- **Gestión de Facturación y Finanzas:** La emisión de facturas y la gestión de las finanzas son esenciales para la estabilidad económica y operativa de EMMAIPC-EP. Cualquier interrupción en estos procesos podría resultar en pérdidas financieras significativas y en problemas de liquidez.
- **Operación del Servidor Principal:** El servidor principal soporta aplicaciones críticas, bases de datos y sistemas de comunicación. Su inactividad puede paralizar varios procesos operativos esenciales, afectando la productividad y la capacidad de tomar decisiones informadas.
- **Gestión de Información del Personal:** La disponibilidad y seguridad de la información relacionada con el personal son fundamentales para la gestión de recursos humanos y para la operación efectiva de la organización.
- **Redes de Comunicación:** La conectividad de red y las comunicaciones son vitales para la coordinación interna y la interacción con clientes y proveedores. Una interrupción en las comunicaciones podría causar una desconexión que afectaría todos los aspectos operativos de la empresa.

6. Evaluación de Riesgos

La evaluación de riesgos para la empresa EMMAIPC-EP ha identificado varias amenazas críticas que pueden afectar significativamente a los activos clave de la organización. Los riesgos más altos, como los asociados con el corte del suministro eléctrico, la denegación de servicio y la ingeniería social, requieren una atención prioritaria y la implementación de controles robustos. Por otro lado, los riesgos clasificados como medios, como las vulnerabilidades del software y los errores de mantenimiento, también deben ser abordados adecuadamente para garantizar la resiliencia operativa.

La implementación efectiva de los controles propuestos reducirá tanto la probabilidad de ocurrencia como el impacto de estos riesgos, asegurando que EMMAIPC-EP pueda mantener la continuidad de sus operaciones críticas incluso en situaciones adversas.

ID Activo	Activo	ID Amenaza	Amenaza	Riesgo	CONTROL
Act-001	Servidor	[I.6]	Corte del suministro eléctrico	15	- Aseguramiento de la disponibilidad
		[E.24]	Caída del sistema por agotamiento de recursos	10	- Monitoreo proactivo de recursos - Escalabilidad automática
		[A.24]	Denegación de servicio	15	- Protecciones Generales - Implementación de sistemas de prevención y detección de intrusiones - Redundancia y balanceo de carga

Act 002	- Sistema de facturación	[E.20]	Vulnerabilidades de los programas (software)	10	- Actualización y parches - Análisis de Vulnerabilidades - Segregación de Entornos
		[E.21]	Errores de Mantenimiento/ Actualización de programas	10	- Gestión de cambios
		[A.22]	Manipulación de programas	10	- Control de acceso - Registro de Auditoría - Monitoreo Continuo
Act 003	- Sistema Informático SIGAME	[E.21]	Errores de Mantenimiento/ Actualización de programas	10	- Automatización de procesos - Planificación de mantenimiento
Act 006	- Personal del Departamento de Tecnologías de la Información y Comunicación	[A.30]	Ingeniería Social	15	- Capacitación en concienciación de seguridad - Políticas de seguridad
		[A.29]	Extorsión	10	- Formación y concienciación
Act 007	- cableado estructurado	[I.8]	Avería de origen físico o lógico	10	- Protección de los Equipos Informáticos - Aseguramiento de la disponibilidad - Protección de las Aplicaciones Informáticas
		[I.6]	Corte del suministro eléctrico	15	- Aseguramiento de la disponibilidad

7. Estrategias de Continuidad y Recuperación

Las estrategias de continuidad y recuperación son fundamentales para asegurar que EMMAIPC-EP pueda mantener sus operaciones críticas o reanudarlas rápidamente después de un incidente disruptivo. Estas estrategias se diseñan para abordar los riesgos identificados en la evaluación de riesgos y se alinean con los tiempos de recuperación objetivo (RTO) establecidos en el Análisis de Impacto en el Negocio (BIA). A continuación, se presentan las estrategias de continuidad y recuperación específicas para los activos y procesos críticos de la organización.

Tabla 16. Estrategias de Continuidad y Recuperación. Autoría: Propia

Activo/Proceso Crítico	**Estrategia**	**Objetivo**
Servidor Principal	- Respaldo Eléctrico: Implementación de UPS y generadores de respaldo.	Asegurar la disponibilidad continua del servidor y restaurarlo en un máximo de 4 horas.
	- Escalabilidad Automática y Monitoreo Proactivo.	Prevenir el agotamiento de recursos y evitar caídas del sistema.
	- Protección contra Ataques DoS: Implementación de IPS/IDS y balanceadores de carga.	Mitigar ataques DoS y minimizar el impacto en el servidor.

	- Gestión de Cambios y Automatización de Mantenimiento.	Garantizar la continuidad del sistema de facturación y restaurarlo en un máximo de 6 horas.
Sistema de Facturación	- Segregación de Entornos: Separar desarrollo, pruebas y producción.	Minimizar el riesgo de interrupciones debido a errores en el entorno de producción.
	- Análisis de Vulnerabilidades y Parches de Seguridad.	Proteger el sistema de facturación contra amenazas de seguridad.
Sistema Informático SIGAME	- Automatización y Planificación del Mantenimiento.	Mantener la operatividad del sistema SIGAME o restaurarlo dentro de 8 horas.
	- Capacitación y Preparación del Personal.	Asegurar que el personal esté preparado para mantener y restaurar el sistema SIGAME.
Personal del Departamento de TI y Comunicación	- Capacitación en Concienciación de Seguridad.	Proteger al personal clave contra amenazas de ingeniería social y mejorar la respuesta ante incidentes.
	- Implementación de Políticas de Verificación y Autenticación.	Asegurar que solo personal autorizado tenga acceso a sistemas críticos.
	- Protocolo de Respuesta Rápida.	Responder rápidamente a cualquier ataque de ingeniería social.

Cableado Estructurado y Redes de Comunicación	- Redundancia y Monitoreo.	Garantizar la integridad y disponibilidad de las redes de comunicación, con un tiempo de recuperación de 24 horas.
	- Mantenimiento Preventivo.	Identificar y resolver posibles fallos en el cableado y equipos de red antes de que se conviertan en problemas críticos.
Suministro Eléctrico	- Implementación de UPS y Generadores.	Asegurar la continuidad del suministro eléctrico para sistemas críticos, con un tiempo de recuperación inmediato.
	- Mantenimiento Regular de Equipos de Respaldo.	Mantener la operatividad de los sistemas de respaldo eléctrico.
	- Plan de Contingencia Eléctrica.	Gestionar largas interrupciones del suministro eléctrico.
Centro de Datos Alternativo	- Configuración de un Centro de Datos Alternativo.	Asegurar la operatividad del centro de datos alternativo dentro de 24 horas en caso de inhabilitación del centro principal.
	- Sincronización de Datos en Tiempo Real.	Mantener la disponibilidad y actualización de datos en ambos centros de datos.
	- Pruebas Regulares del Centro de Datos Alternativo.	Garantizar la preparación del centro de datos alternativo para emergencias.

8. Plan de Recuperación de desastres (DRP) de la EMMAIPC-EP

El DRP abarca todos los activos críticos de TI identificados en EMMAIPC-EP, incluidos los servidores, sistemas de facturación, redes de comunicación, sistemas de respaldo y el centro de datos alternativo. También cubre el suministro eléctrico de respaldo y la recuperación del personal clave en el departamento de TI.

8.1. Estructura Organizativa para la Recuperación

- **Director de TI:** Responsable de la activación del DRP y la supervisión general de la recuperación.
- **Gerente de Sistemas:** Encargado de la restauración de servidores y sistemas críticos.
- **Equipo de Red y Comunicaciones**: Responsable de la recuperación de las redes y sistemas de comunicación.
- **Equipo de Seguridad de la Información:** Asegura la integridad y la seguridad de los datos durante el proceso de recuperación.
- **Coordinador de Comunicaciones**: Gestiona la comunicación interna y externa durante la crisis.

8.2. Restauración de Sistemas Críticos

- **Recuperación del Servidor Principal:**
  - Restaurar el servidor principal utilizando los sistemas de respaldo y realizar pruebas de operatividad.
  - Si es necesario, transferir operaciones al centro de datos alternativo.
- **Recuperación del Sistema de Facturación:**
  - Implementar procedimientos de restauración para el sistema de facturación, incluyendo la aplicación de parches necesarios y la verificación de la integridad de los datos.
- **Recuperación de Redes de Comunicación:**

- Restablecer las conexiones de red y comunicación utilizando rutas de red redundantes.
- Monitorear el estado de las redes y resolver cualquier problema identificado.

9. Roles y responsabilidades

RESPONSABLES	ACTIVIDADES
Personal administrativo o de servicios de la empresa EMMAIPC-EP	Cuando se detecten incidentes, es fundamental informar de manera inmediata a cualquier miembro del equipo encargado de la gestión de incidentes, incluyendo: • **Jefe del área de Tecnologías de la Información (TI)** • **Gerente de EMMAIPC-EP** Inicialmente, se debe realizar una notificación telefónica, seguida del envío de un correo electrónico para alertar sobre cualquier incidente que pueda interrumpir las operaciones normales de la organización. El responsable designado para recibir estas alertas, ya sea por teléfono o correo electrónico, debe proceder según los siguientes protocolos: 1. **Evaluación Inmediata del Incidente:** Dentro de una hora tras recibir la alerta, el responsable debe dirigirse al lugar del incidente o iniciar una evaluación remota, dependiendo de la gravedad del mismo. 2. **Comunicación del Incidente:** Una vez identificado el incidente, el responsable deberá informar a los demás miembros del equipo o comité de evaluación de incidentes. 3. **Análisis y Evaluación:** El equipo analizará y evaluará el incidente, especialmente si el impacto no es completamente evidente. 4. **Determinación del Impacto:** El equipo determinará si el incidente podría causar la suspensión de los servicios de TI o afectar la operación de alguna de las áreas de EMMAIPC-EP. El equipo encargado de gestionar los incidentes tiene la responsabilidad de asignar el nivel de alerta correspondiente al incidente, clasificados en tres categorías: • **Nivel de Alerta Bajo:** El riesgo no afecta las operaciones ni los servicios de la organización. • **Nivel de Alerta Medio:** El riesgo afecta las operaciones de un área específica, pero no interfiere con los servicios generales de la organización. • **Nivel de Alerta Alto:** El riesgo podría comprometer los servicios tecnológicos y corporativos de EMMAIPC-EP.

Responsable del área de Tecnologías de la Información	Por lo tanto, el jefe o encargado del área de TI será responsable de comunicar el nivel de alerta, ya sea roja o amarilla, dependiendo del incidente. Este proceso debe realizarse en un lapso de 15 a 20 minutos, tras lo cual se procederá a la activación del Plan de Continuidad de Negocio. Finalmente, el Gerente General de EMMAIPC-EP debe ser informado del incidente y las acciones tomadas.
Gerente General de la EMMAIPC-EP	El Gerente General, junto con el encargado del área de TI, debe evaluar si el incidente puede ser resuelto en un plazo máximo de 2 horas; de no ser así, se informará a uno de los miembros del Comité de Administración de Crisis sobre la gravedad del incidente.

10. Planes de Acción

El apartado de Planes de Acción del Plan de Recuperación de Desastres (DRP) de EMMAIPC-EP detalla las acciones específicas y los pasos a seguir para restaurar rápidamente las operaciones críticas de la organización en caso de un desastre. Estos planes están diseñados para abordar los riesgos identificados y garantizar que cada proceso crítico sea recuperado de manera eficiente y dentro de los tiempos de recuperación objetivo (RTO) establecidos.

Cada plan de acción está estructurado para proporcionar una guía clara sobre qué debe hacerse, quién es responsable, cuánto tiempo tomará, y qué recursos serán necesarios para ejecutar la recuperación. Esta estructura asegura que, en el momento de un incidente, todos los involucrados comprendan sus roles y puedan actuar rápidamente para minimizar el impacto en la organización.

Los planes de acción cubren los aspectos más críticos del entorno de TI de EMMAIPC-EP, incluyendo la restauración del servidor principal, el sistema de facturación, las redes de comunicación, la protección del personal de TI, y la activación del centro de datos alternativo. A través de estos planes, EMMAIPC-EP fortalece su capacidad para responder a incidentes graves, protegiendo así su infraestructura tecnológica, su operatividad y la confianza de sus clientes y partes interesadas.

10.1. Plan de acción para la recuperación del servidor principal

Acción	Descripción	Responsable	Tiempo de Ejecución	Recursos Necesarios
Evaluación del Estado de la Red	Evaluar el estado de las redes de comunicación y determinar las áreas afectadas.	Responsable de TI	1 hora	Herramientas de diagnóstico de red

Implementación de Redundancia	Activar rutas de red redundantes para restaurar la conectividad.	Responsable de TI	1 hora	Redundancia de Red
Restauración de Dispositivos de Red	Reiniciar y configurar dispositivos de red para restablecer la comunicación.	Responsable de TI	2 horas	Equipos de red, Manuales de configuración
Verificación de Conectividad	Probar la conectividad en todas las áreas afectadas para asegurar la funcionalidad completa.	Responsable de TI	1 hora	Herramientas de prueba de conectividad

Notificación de Restablecimiento	Informar al personal sobre la restauración de las redes de comunicación.	Responsable de TI	30 minutos	Sistema de mensajería

10.2. Plan de acción para la protección del personal de TI

Acción	Descripción	Responsable	Tiempo de ejecución	Recursos necesarios
Capacitación en seguridad	Realizar una sesión de capacitación de emergencia en concienciación de seguridad y respuesta a incidentes.		1 día	Material de capacitación, sala de reuniones

Implementación de Políticas de Verificación	Aplicar políticas estrictas de verificación de identidad y autenticación de solicitudes.	Responsable de TI	Inmediato	Manual de políticas, Herramientas de autenticación
Establecimiento de Protocolo de Respuesta Rápida	Crear y distribuir un protocolo de respuesta rápida ante incidentes de seguridad.	Responsable de TI	2 horas	Documentación de protocolo, Sistema de notificación
Simulaciones de Ingeniería Social	Realizar simulaciones de ataques de ingeniería social para evaluar la preparación del personal.	Responsable de TI	1 día	Herramientas de simulación, Personal de TI
Evaluación y Revisión de Políticas	Revisar y actualizar las políticas de seguridad	Responsable de TI	1 día	Informes de simulación, Reunión de revisión

	basadas en los resultados de las simulaciones.			

10.3. Plan de acción para la recuperación del Sistema de Facturación

Acción	Descripción	Responsable	Tiempo de ejecución	Recursos necesarios
Evaluación del Estado del Sistema	Evaluar rápidamente el estado del sistema de facturación y determinar las áreas afectadas.	Responsable de TI	1 día	Herramientas de diagnóstico de software
Restauración de Software	Aplicar parches de	Responsable de TI	6 horas	Respaldo de Software, Parches

	seguridad y restaurar el sistema de facturación desde los respaldos.			
Verificación de la Integridad de Datos	Comprobar la integridad de los datos para asegurar que no haya pérdidas o corrupción.	Responsable de TI	2 horas	Herramientas de verificación de datos
Pruebas Funcionales	Realizar pruebas funcionales para asegurar que el sistema de facturación esté operativo.	Responsable de TI	1 hora	Scripts de prueba, Personal de QA
Comunicación a Usuarios	Informar a los usuarios que el sistema de facturación ha sido restaurado y	Responsable de TI	30 min	Sistema de mensajería

está listo para

su uso.

6.

6.1. Anexo 2. Protocolo de la investigación

A. TÍTULO
Propuesta para la Gestión de la Continuidad del Negocio en el Ámbito de TI para EMMAIPC-EP del Cantón Cañar

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnología de información y comunicación	Energía eléctrica y tecnologías de información para la innovación y el desarrollo sostenible	Inteligencia de negocio	
		Auditoria y seguridad informática	X
		Gobierno de TI	
		Gestión de riesgo de TI	
		Redes y comunicación	
		Inteligencia de requerimientos	
		Arquitectura de Desarrollo de Software	

C. PLANTEAMIENTO DEL PROBLEMA

En un entorno empresarial cada vez más dependiente de la tecnología, la capacidad de una organización para continuar operando frente a interrupciones es fundamental. EMMAIPC-EP, una entidad pública en el cantón Cañar, no es la excepción. Esta dependencia creciente de los sistemas informáticos plantea desafíos significativos en términos de gestión de la continuidad del negocio (GCB), especialmente en el ámbito de la tecnología de la información (TI).

Actualmente, EMMAIPC-EP enfrenta varias vulnerabilidades en su infraestructura de TI, incluyendo sistemas desactualizados, falta de planes de recuperación de desastres bien definidos, y una capacitación insuficiente del personal en prácticas de GCB. La falta de un marco estructurado para la gestión de la continuidad del negocio en TI podría resultar en interrupciones operativas significativas, pérdida de datos críticos y, en última instancia, un deterioro en la prestación de servicios esenciales a la comunidad. La necesidad de abordar estos riesgos es urgente dado el papel crucial que juega EMMAIPC-EP en el desarrollo y mantenimiento de infraestructura pública esencial y servicios administrativos en el cantón Cañar. Sin embargo, la organización carece de una estrategia comprensiva que integre políticas, procedimientos y recursos efectivos para asegurar la continuidad operativa de sus sistemas de TI frente a diversas contingencias.

Este trabajo busca desarrollar una propuesta integral para la gestión de la continuidad del negocio en el ámbito de TI en EMMAIPC-EP, que no solo aborde las brechas actuales, sino que también establezca un marco sostenible para responder eficazmente a incidentes futuros. La investigación se centrará en identificar las vulnerabilidades críticas, evaluar los riesgos asociados y proponer soluciones prácticas y escalables que puedan ser adoptadas para fortalecer la resiliencia organizacional de EMMAIPC-EP.

D. OBJETIVO GENERAL

Desarrollar una propuesta de gestión de la continuidad del negocio específicamente adaptada al ámbito de TI de EMMAIPC-EP del cantón Cañar, que asegure la resiliencia operativa y la rápida recuperación de los servicios ante situaciones de interrupción.

E. OBJETIVOS ESPECÍFICOS

1. Diagnosticar el estado actual de la infraestructura de TI y las prácticas de gestión de la continuidad del negocio en EMMAIPC-EP.
2. Elaborar un marco de gestión de riesgos de TI que identifique, evalúe y priorice las amenazas potenciales a la continuidad operacional de EMMAIPC-EP.
3. Diseñar un plan de acción para la implementación de estrategias de recuperación de desastres y continuidad del negocio que sean prácticas, escalables y sostenibles.

F. JUSTIFICACIÓN

La gestión de la continuidad del negocio en el ámbito de la tecnología de la información (TI) es crítica para la sostenibilidad y eficiencia de cualquier organización, especialmente en el sector público, donde los servicios deben ser continuos y fiables para satisfacer las necesidades de la comunidad. EMMAIPC-EP, al ser una entidad pública encargada de la administración y desarrollo infraestructural del cantón Cañar, requiere de sistemas de TI robustos y resistentes a diversas contingencias.

La creciente dependencia de las operaciones de EMMAIPC-EP en sistemas tecnológicos hace indispensable la implementación de un marco sólido de gestión de la continuidad del negocio que pueda garantizar la mínima interrupción de los servicios críticos y la rápida recuperación en casos de desastres o fallos sistémicos. A pesar de esta necesidad, se observa una falta de políticas y procedimientos actualizados que enfrenten estos retos de manera efectiva. La relevancia de esta investigación radica en su capacidad para fortalecer la resiliencia de EMMAIPC-EP frente a interrupciones, protegiendo así los datos críticos y servicios esenciales que impactan directamente en la vida cotidiana de los ciudadanos del cantón. Además, un plan de gestión de la continuidad del negocio adecuadamente diseñado y aplicado no solo mejorará la capacidad de respuesta frente a emergencias, sino que también fomentará una cultura de preparación y mejora continua dentro de la organización.

La propuesta de esta tesis se justifica también en la necesidad de alinear las prácticas de gestión de TI con las normativas nacionales e internacionales sobre gestión de riesgos y continuidad del negocio, promoviendo así el cumplimiento normativo y la eficiencia operativa. En consecuencia, esta investigación aportará valor práctico y teórico, proporcionando un modelo replicable para otras entidades del sector público que enfrentan desafíos similares en la gestión de la continuidad de sus operaciones de TI.

G. ALCANCE

La presente investigación se centra en la elaboración de una propuesta de gestión de la continuidad del negocio específica para el ámbito de tecnologías de la información en EMMAIPC-EP, una entidad pública del cantón Cañar. El estudio se limitará a analizar y diseñar estrategias y procedimientos que mejoren la capacidad de respuesta y recuperación de los sistemas de TI de la entidad frente a interrupciones operativas.

H. CONCEPTOS RELACIONADOS

Gestión de la Continuidad del Negocio (GCB)

La Gestión de la Continuidad del Negocio se refiere al proceso mediante el cual las organizaciones preparan un plan para enfrentar situaciones de crisis que puedan interrumpir sus operaciones habituales. Este plan incluye la identificación de riesgos potenciales, el desarrollo de políticas y procedimientos para mitigar esos riesgos, y estrategias para garantizar que los servicios y procesos esenciales puedan continuar o ser recuperados rápidamente tras una interrupción (Kubus, Cánovas, & Escobar, 2023).

Tecnologías de la Información (TI)

El término Tecnologías de la Información (TI) se utiliza para describir el uso de sistemas computacionales y software para gestionar información. En las organizaciones, TI abarca el uso de hardware, software, redes y sistemas de almacenamiento para crear, procesar, almacenar, asegurar y intercambiar todo tipo de datos electrónicos (Keri E. Pearlson, 2024).

Plan de Recuperación de Desastres (PRD)

Un Plan de Recuperación de Desastres es un documento estructurado que contiene instrucciones detalladas sobre cómo responder a incidentes imprevistos, como desastres naturales o fallos técnicos, para asegurar la recuperación rápida y eficaz de la información y sistemas tecnológicos vitales. Este plan es crucial para minimizar el impacto negativo en las operaciones y asegurar la continuidad del negocio (Bouton, 2024) (Bolaños Vinueza, 2024).

Resiliencia Organizacional

La resiliencia organizacional se refiere a la capacidad de una empresa o entidad para resistir, adaptarse y recuperarse de adversidades o cambios, asegurando la continuidad de las operaciones bajo cualquier circunstancia. Este concepto implica no solo la recuperación ante crisis, sino también la adaptabilidad y el crecimiento continuo frente a los desafíos (Santiago, 2023).

I. TRABAJOS RELACIONADOS

Un trabajo realizado por Vega (2024) describe una metodología basada en la norma ISO/IEC 27031 para la elaboración de un plan de continuidad de negocios que va desde la identificación de riesgos y la evaluación del impacto hasta la implementación y pruebas del plan.

Este documento permite comprender la importancia de un plan de continuidad de negocios de una determinada empresa con el objetivo que pueda recuperarse de eventos disruptivos y minimizar el impacto en sus operaciones, clientes y reputación. Además, la metodología utilizada en el documento servirá de guía para estructurar la propuesta de plan de continuidad de negocio para TI en la empresa EMMAIPC-EP.

Zuñiga (2021) se centra en la gestión de la continuidad del negocio (GBC) en el contexto de la seguridad de la información, basándose en el estándar ISO/IEC 27031, un estándar internacionalmente reconocido para la GBC en el ámbito de TI. El documento aborda consideraciones específicas para la implementación de la GBC en el ámbito de TI, como la identificación de riesgos de seguridad de la información, la evaluación del impacto de estos riesgos y la implementación de medidas de control para mitigarlos.

Basado en lo anterior, este documento permitirá comprender cómo el plan de continuidad de negocio se relaciona con la seguridad de la información y cómo se puede implementar un plan efectivo para proteger los activos de información de EMMAIPC-EP.

Araujo, G (2019), presenta un trabajo de investigación denominado, “Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador”, en el que proporciona un marco teórico y conceptual sólido sobre la gestión de la continuidad del negocio (GBC), incluyendo definiciones, conceptos clave, modelos y buenas prácticas. Los autores describen una metodología detallada para la elaboración de un plan de continuidad del negocio, desde la identificación de riesgos y la evaluación del impacto hasta la implementación y pruebas del plan.

Este documento permitirá fundamentar el trabajo de investigación a través de las bases sólidas teóricas, además de normas, guías, herramientas y estudios de caso.

J. METODOLOGÍA

El presente trabajo utilizará la metodología mixta que combina técnicas cualitativas y cuantitativas para diagnosticar la situación actual de la EMMAIPC-EP en términos de gestión de la continuidad del negocio de TI. Además se realizará una exhaustiva revisión de la literatura para comprender los fundamentos teóricos de la gestión de la continuidad del negocio, con especial énfasis en el ámbito de las tecnologías de la información.

K. CRONOGRAMA DE ACTIVIDADES					
N°	ACTIVIDAD	MES			
		I	II	III	MEDIOS DE VERIFICACIÓN
1.	**Diagnosticar el estado actual de la infraestructura de TI y las prácticas de gestión de la continuidad del negocio en EMMAIPC-EP.**				
1.1.	Realizar una auditoría técnica de la infraestructura actual de TI.				Informe de auditoría que detalle el estado de la infraestructura, incluyendo hardware, software, redes y procedimientos de seguridad
1.2.	Encuestas a empleados sobre sus percepciones y conocimientos de las prácticas actuales de gestión de la continuidad del negocio.				Resultados compilados de la encuesta que reflejen las percepciones del personal y cualquier brecha de conocimiento.
2.	**Elaborar un marco de gestión de riesgos de TI que identifique, evalúe y priorice las amenazas potenciales a la continuidad operacional de EMMAIPC-EP.**				
2.1.	Desarrollo de una matriz de evaluación de riesgos específicos para TI.				Matriz de riesgo completada que clasifique los riesgos según su probabilidad e impacto.
2.2.	Realización de talleres con el personal de TI para identificar y discutir posibles amenazas y vulnerabilidades.	x			listado de riesgos identificados durante los talleres.
3.	**Diseñar un plan de acción para la implementación de estrategias de recuperación de desastres y continuidad del negocio que sean prácticas, escalables y sostenibles.**				
3.1.	Elaboración de un protocolo de respuesta ante incidentes y recuperación de desastres.		x		Documento pdf
3.2.	Diseño de programas de capacitación		x	x	Documento pdf

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. Cristhian Flores Urgilés
ESTUDIANTE 1	JULIO CÉSAR PINGUIL SIMBAINA

N. FIRMAS DE RESPONSABILIDAD

Lugar:	Cañar
Fecha:	29-04-2024

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

Firmas:

CRISTHIAN HUMBERTO FLORES URGILES

Firmado digitalmente por CRISTHIAN HUMBERTO FLORES URGILES
Fecha: 2024.04.29 19:45:39 -05'00'

Nombre: Ing. Cristhian Flores Urgilés, Mgs	Nombre: Est. Julio César Pinguil Simbaina
CC: 0301638375	C.C.: 0302422696
Director del Proyecto	**Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre:	Nombre:
CC:	C.C.:
Primer Par Revisor	**Segundo Par Revisor**

P. REFERENCIAS

Álvarez Mayorga, E. H., & Araujo Castro, G. M. (01 de 01 de 2019). *repositorio.uta.edu.ec.* Obtenido de repositorio.uta.edu.ec: https://repositorio.uta.edu.ec/handle/123456789/29843

Bolaños Vinueza, E. S. (07 de 03 de 2024). *repositorio.utn.edu.ec.* Obtenido de repositorio.utn.edu.ec: https://repositorio.utn.edu.ec/handle/123456789/15713

Bouton, M. y. (2024). 27 - Informatics and Information Technology in Disaster Medicine. En M. y. Bouton, *Medicina de desastres de En Ciottone* (págs. 164-166). Elsevier.

Keri E. Pearlson, C. S. (2024). *Managing and Using Information Systems: A Strategic Approach.* John Wiley & Sons.

Kubus, R., Cánovas, N. G., & Escobar, J. G. (2023). Plan de Continuidad del Negocio y riesgo operacional y financiero. *Revista Universitaria Europea Nº 40*, 169-198.

Santiago, M. S. (2023). La resiliencia organizacional: un enfoque para la alta dirección. *Ciencia Administrativa*, 75-80.

Vega Vargas, D. M. (01 de 03 de

2024). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/han dle/10596/60577

Zuñiga López, F. F. (01 de 01 de 2021). *repository.unad.edu.co.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bits tream/handle/10596/48686/ffzunig al.pdf?sequence=3&isAllow ed=y

Anexo 3. Certificado de Ingles

ABSTRACT

This thesis addresses business continuity management in the IT department of EMMAIPC-EP, focusing on ensuring operational resilience in the event of possible disruptions. The specific objectives include diagnosing the current state of IT infrastructure and business continuity practices, developing an IT risk management framework that identifies and prioritizes threats, and designing an action plan for implementing practical, scalable, and sustainable disaster recovery and business continuity strategies. The methodology used was descriptive and evaluative, combining qualitative analysis of the current situation with a quantitative approach to measure the impact of the identified risks. A comprehensive diagnosis of the IT infrastructure and current management practices was conducted through surveys and interviews with key personnel, which helped identify critical deficiencies in the preparedness for operational continuity. Based on these findings, an IT risk management framework aligned with international standards was developed, and a specific action plan was designed, including scalable and sustainable recovery strategies. The results of this investigation provide EMMAIPC-EP with a solid foundation to strengthen its incident response capabilities, ensuring the continuity of its critical operations and protecting its most valuable assets in crises.

***Keywords*:** business continuity, risk management, IT infrastructure.

6.2. Anexo 4. Certificado Turniting

TESIS_JULIO_PINGUIL_3.docx

INFORME DE ORIGINALIDAD

9%	8%	2%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

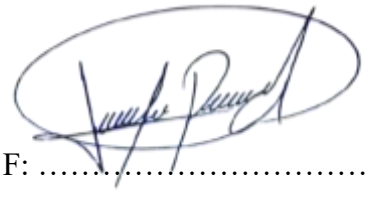
FUENTES PRIMARIAS

1	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
2	Submitted to Universidad Estatal a Distancia Trabajo del estudiante	<1%
3	tr-ex.me Fuente de Internet	<1%
4	www2.uca.es Fuente de Internet	<1%
5	sedici.unlp.edu.ar Fuente de Internet	<1%
6	www.cientec.com Fuente de Internet	<1%
7	www2.intec.edu.do Fuente de Internet	<1%
8	Submitted to Universidad Católica Boliviana "San Pablo" Trabajo del estudiante	<1%

Universidad Católica de Cuenca	**AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL**

Julio César Pinguil Simbaina portador(a) de la cédula de ciudadanía Nº **0302422696** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **Propuesta para la gestión de continuidad del negocio en el ámbito de TI para EMMAIPC-EP del cantón Cañar, basado en la norma ISO 22301** 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, **22 de noviembre del 2024**



F: ……

Julio César Pinguil Simbaina

C.I. **0302422696**