UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS INFORMÁTICA

F.A.F.I.

"*EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA INGENIERÍA EN SISTEMAS"*

Tema:

LA CONTINUIDAD DEL NEGOCIO BASADO EN ISO 22301 EN LOS SERVICIOS TECNOLÓGICOS DEL GAD MUNICIPAL DEL CANTÓN MOCACHE,2023

Autor:

NAVARRETE YEPEZ OVER STEVEN

Tutor:

ING. MEJÍA VITERI JOSÉ TEODORO

LOS RÍOS - BABAHOYO - ECUADOR

RESUMEN

El presente estudio de abordará diversos aspectos relacionados con la continuidad del negocio (BCP) en los servicios tecnológicos del GAD Municipal del cantón Mocache. Se definieron conceptos clave, como el BCP, se exploró la evolución histórica de estos planes, se describió la gestión de la continuidad del negocio (BCM), se destacaron los beneficios de la continuidad del negocio en el sector público, se presentó la norma ISO 22301 y su estructura, se explicó el concepto de Plan de Emergencia y Plan de Contingencia, y se mencionaron las normas internacionales relacionadas con la continuidad operativa. Además, se examinaron los tipos de amenazas en TI. Con esta base teórica, es posible comprender mejor la importancia de la continuidad del negocio en el contexto de los servicios tecnológicos del GAD Municipal de Mocache. La planificación y gestión adecuadas de la continuidad del negocio son esenciales para garantizar que los servicios críticos no se vean interrumpidos, especialmente en el sector público, donde la continuidad de los servicios es fundamental para el bienestar de la comunidad.

Palabras Clave: continuidad, servicios, ISO22301, contingencia, GAD, Municipal

ABSTRACT

This study will address various aspects related to business continuity (BCP) in the technological services of the Municipal GAD of the Mocache canton. Key concepts were defined, such as the BCP, the historical evolution of these plans was explored, business continuity management (BCM) was described, the benefits of business continuity in the public sector were highlighted, the ISO standard was presented 22301 and its structure, the concept of Emergency Plan and Contingency Plan was explained, and international standards related to operational continuity were mentioned. Additionally, the types of IT threats were examined. With this theoretical basis, it is possible to better understand the importance of business continuity in the context of the technological services of the Municipal GAD of Mocache. Proper business continuity planning and management are essential to ensure that critical services are not disrupted, especially in the public sector where continuity of services is critical to the well-being of the community.

Índice

1 PROBLEMÁTICA

La creciente dependencia de los servicios tecnológicos en las operaciones gubernamentales y la necesidad de mantener la continuidad de estos servicios frente a posibles interrupciones las mismas que se centran en las necesidades y prioridades locales. En este contexto, el Gobierno Autónomo Descentralizado (GAD) Municipal del cantón Mocache se enfrenta al desafío de garantizar la continuidad de sus servicios tecnológicos en caso de eventos disruptivos y mejorar los servicios de tal manera que puedan abordar una amplia gama de temas y prioridades como se enfocan los servicios tecnológicos internacionales.

El GAD Municipal del cantón Mocache, al igual que muchas otras entidades gubernamentales, depende en gran medida de la disponibilidad y eficiencia de sus sistemas y servicios tecnológicos para brindar servicios esenciales a la comunidad, gestionar datos críticos y mantener la operatividad interna. Sin embargo, la falta de un sistema formal de gestión de la continuidad del negocio o equivalente podría exponer al GAD a riesgos significativos.

El planteamiento del problema radica en la necesidad de evaluar la preparación del GAD Municipal del cantón Mocache en términos de continuidad del negocio en el ámbito de los servicios tecnológicos. Esto incluye la identificación de vulnerabilidades potenciales, la capacidad de respuesta ante eventos disruptivos.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

- Evaluar la capacidad del Gobierno Autónomo Descentralizado (GAD) Municipal del cantón Mocache en la gestión de la continuidad del negocio basado en la norma ISO 22301 en el ámbito de los servicios tecnológicos, con el fin de garantizar la disponibilidad de los servicios críticos ante eventos disruptivos.

2.2 OBJETIVOS ESPECIFICOS

- Diagnosticar los sistemas críticos y los procesos operativos del GAD Municipal del cantón Mocache, identificando los riesgos potenciales que puedan afectar la continuidad del negocio.

- Identificar los posibles riesgos asociados a la gestión de la continuidad del negocio en los servicios tecnológicos del GAD Municipal de Mocache.

- Crear el Plan de Continuidad del Negocio basado en las Normas ISO 22301 en los servicios tecnológicos del GAD Municipal de Mocache.

3 JUSTIFICACIÓN

Para llevar a cabo el estudio de caso sobre "La continuidad del negocio basado en ISO 22301 en los servicios tecnológicos del Gad Municipal del cantón Mocache", encontramos una base sólida en la necesidad imperante de asegurar la continuidad de los servicios tecnológicos esenciales en el contexto de la administración municipal. En la actualidad, la dependencia de los servicios tecnológicos es crucial para el GAD Municipal del cantón Mocache en la prestación de servicios públicos, la gestión de datos críticos y la comunicación con la comunidad. Sin embargo, esta dependencia conlleva riesgos significativos, desde posibles fallos técnicos hasta ciberamenazas, que podrían tener un impacto adverso en las operaciones gubernamentales y en la satisfacción de los ciudadanos.

La norma ISO 22301 proporciona un marco internacionalmente reconocido para la gestión de la continuidad del negocio, y su implementación puede ayudar al GAD Municipal del cantón Mocache a mitigar estos riesgos, mejorar su capacidad de respuesta y garantizar la continuidad de los servicios críticos. La ISO 22301 en comparación de otras normas se centra específicamente en ayudar a las organizaciones a planificar, implementar y mantener un sistema de gestión de la continuidad del negocio efectivo. Esto significa que está diseñada para ayudar a las organizaciones a asegurarse de que puedan mantener sus operaciones esenciales incluso en situaciones de crisis o desastres.

Este estudio también es relevante en términos de cumplimiento normativo, transparencia y eficiencia en el uso de recursos públicos, y tiene el potencial de servir como un ejemplo de buenas prácticas en la gestión de la continuidad del negocio en el sector público, beneficiando tanto a la entidad gubernamental como a la comunidad que sirve.

4 LÍNEA DE INVESTIGACIÓN

El enfoque en esta investigación se orienta hacia la aplicación de las tecnologías inteligentes de software y hardware para fortalecer la resiliencia y eficiencia del Gobierno Autónomo Descentralizado (GAD) Municipal del cantón Mocache en sus servicios tecnológicos. Con la creciente dependencia de los servicios tecnológicos en la administración gubernamental y los riesgos asociados a posibles interrupciones, este estudio se convierte en un componente esencial para explorar la factibilidad de implementar un sistema de gestión de la continuidad del negocio basado en la norma ISO 22301. Dicho sistema buscará asegurar la disponibilidad y confiabilidad de los servicios tecnológicos críticos, al tiempo que se alinea con las mejores prácticas en el campo de la tecnología y la innovación. Este enfoque se presenta como una oportunidad de aplicar los conocimientos en sistemas de información y tecnologías inteligentes para abordar una problemática real en la gestión gubernamental, mejorando la resiliencia del GAD Municipal del cantón Mocache y optimizando la prestación de servicios tecnológicos esenciales para la comunidad local.

4.1 Línea de investigación

Sistema de información y comunicación, emprendimiento e innovación.

4.2 Sub línea de investigación

Redes y tecnologías inteligentes de software y hardware.

5 MARCO CONCEPTUAL

5.1 Definición de un Plan de Continuidad del Negocio BCP

Un BCP, o Plan de Continuidad de Negocio (por sus siglas en inglés, Business Continuity Plan), es un conjunto de procedimientos y estrategias diseñadas para garantizar que una organización pueda mantener sus operaciones esenciales y servicios críticos en funcionamiento, incluso en situaciones adversas o de crisis. El objetivo principal del BCP es minimizar el impacto de eventos imprevistos, como desastres naturales, interrupciones tecnológicas o emergencias, para que la organización pueda recuperarse y seguir funcionando de manera efectiva. El BCP incluye medidas para la prevención, respuesta, recuperación y restauración de las operaciones normales de la empresa. (IBM Services, 2020).

5.2 Evolución del Plan de Continuidad de Negocio

Evolución del Plan de Continuidad de Negocio La evolución del Plan de Continuidad de Negocio (BCP) ha sido significativa a lo largo de los años. (Incibe, 2022). Aquí hay una breve visión de su evolución:

1. Orígenes: Los primeros planes de continuidad de negocio surgieron en las décadas de 1960 y 1970, principalmente en grandes organizaciones y en industrias altamente reguladas como la banca y la industria nuclear. Estos planes se centraban en la recuperación de sistemas críticos de procesamiento de datos.
2. Década de 1980: Con la creciente dependencia de las tecnologías de la información, los BCP comenzaron a incluir enfoques más amplios, incorporando la recuperación de sistemas informáticos y telecomunicaciones. También se expandieron a empresas de diferentes tamaños y sectores.
3. Década de 1990: A medida que los desafíos cibernéticos y las amenazas tecnológicas aumentaron, los BCP se volvieron más sofisticados en la protección de datos y la ciberseguridad. Además, se comenzaron a aplicar estándares y mejores prácticas en la gestión de la continuidad del negocio.
4. Década de 2000: Se establecieron estándares internacionales, como la norma ISO 22301, que proporciona un marco estructurado para el BCP. La conciencia sobre la

importancia de la continuidad del negocio creció debido a eventos como los ataques del 11 de septiembre y desastres naturales.

5. Década de 2010: Los BCP se integraron cada vez más en la gestión general de riesgos de una organización. Hubo una mayor atención a la resiliencia empresarial, que abarca no solo la recuperación de desastres, sino también la preparación para interrupciones operativas de cualquier tipo.
6. Década de 2020: La pandemia de COVID-19 destacó la importancia de la planificación de la continuidad del negocio, ya que muchas organizaciones se vieron obligadas a adaptarse rápidamente para mantener sus operaciones en medio de la crisis. La evolución del BCP refleja la creciente complejidad de las operaciones empresariales y la necesidad de adaptarse a un entorno en constante cambio. Hoy en día, los BCP son más holísticos, integrados en la gestión de riesgos y abordan una amplia gama de amenazas para garantizar la resiliencia de las organizaciones.

5.3 Gestión de la Continuidad del Negocio (BCM)

La Gestión de la Continuidad del Negocio (BCM, por sus siglas en inglés, Business Continuity Management) es un enfoque estratégico y sistemático para garantizar que una organización pueda mantener sus operaciones críticas y servicios esenciales en funcionamiento durante situaciones adversas o de crisis. (Simmerman, 2022). Aquí hay algunos aspectos clave de la BCM:

1. Identificación de Riesgos y Amenazas: La BCM comienza por identificar y evaluar los riesgos y amenazas que podrían afectar a la organización. Esto puede incluir eventos como desastres naturales, ciberataques, interrupciones en la cadena de suministro y otros.
2. Análisis de Impacto en el Negocio (BIA): El BIA es una parte fundamental de la BCM. Consiste en analizar cómo la interrupción de las operaciones afectaría a la organización en términos de pérdidas financieras, impacto en la reputación y cumplimiento de regulaciones. Esto ayuda a priorizar las áreas críticas que deben protegerse.
3. Desarrollo de Estrategias de Continuidad: Con base en el BIA, se desarrollan estrategias y planes de acción para garantizar la continuidad de las operaciones críticas. Esto puede incluir la implementación de sistemas de respaldo, la capacitación del personal y la identificación de ubicaciones alternativas de trabajo.
4. Implementación de Medidas Preventivas y de Recuperación: Se establecen medidas preventivas para reducir la probabilidad de que ocurran eventos adversos, así como

medidas de recuperación para minimizar el tiempo de inactividad en caso de que ocurran. Esto puede involucrar la creación de planes de contingencia y la inversión en tecnologías de respaldo.

5. Pruebas y Ejercicios: La BCM implica realizar pruebas y ejercicios regulares para asegurarse de que los planes funcionen según lo previsto. Esto ayuda a identificar debilidades y áreas de mejora.
6. Mantenimiento Continuo: La gestión de la continuidad del negocio no es un esfuerzo único, sino un proceso continuo. Los planes deben actualizarse regularmente para reflejar cambios en la organización y en el entorno operativo.
7. Integración en la Cultura Organizacional: Para que la BCM sea efectiva, debe ser parte de la cultura organizacional. Esto implica la concienciación de los empleados y su participación activa en la preparación y respuesta ante situaciones adversas.
8. Cumplimiento Normativo: En algunos sectores y regiones, existen regulaciones específicas que requieren que las organizaciones tengan planes de continuidad del negocio. Cumplir con estas regulaciones es parte importante de la BCM. La Gestión de la Continuidad del Negocio es esencial para garantizar que una organización pueda resistir y recuperarse de eventos adversos y seguir prestando sus servicios críticos de manera efectiva. Proporciona una estructura sólida para la preparación y la resiliencia empresarial.

5.4 Beneficios de la Implementación

La implementación de la Continuidad del Negocio (BC) en el sector público ofrece una serie de beneficios significativos, que van más allá de simplemente garantizar la supervivencia de las operaciones en situaciones de crisis. (AmericanExpress, 2022). Algunos de los beneficios clave incluyen:

1. Servicios Ininterrumpidos para la Comunidad: La BC asegura que los servicios públicos críticos, como salud, educación, seguridad y servicios sociales, no se vean interrumpidos en situaciones de emergencia. Esto garantiza la seguridad y el bienestar de la comunidad.
2. Mantenimiento de la Confianza Pública: La capacidad del gobierno para mantener la continuidad de sus servicios en momentos de crisis refuerza la confianza de la población en su capacidad de respuesta y liderazgo.
3. Cumplimiento Normativo: En muchos lugares, existen regulaciones que exigen a las entidades gubernamentales tener planes de BC. Cumplir con estas regulaciones evita sanciones legales y asegura la transparencia y la rendición de cuentas.

4. Reducción de Pérdidas Económicas: La interrupción de los servicios públicos puede resultar en pérdidas económicas significativas para una comunidad o región. La BC ayuda a minimizar estas pérdidas al mantener las operaciones funcionando.
5. Preparación para Desastres: El sector público está a menudo en la primera línea en situaciones de desastre. La BC garantiza que los funcionarios estén preparados y capacitados para responder de manera eficaz.
6. Optimización de Recursos: Los planes de BC pueden ayudar a optimizar la asignación de recursos en momentos de crisis, asegurando que se prioricen las áreas más críticas.
7. Reducción de Tiempo de Recuperación: Tener planes de BC sólidos acorta el tiempo necesario para recuperarse después de un incidente, lo que significa que los servicios se restablecen más rápidamente.
8. Flexibilidad en la Gestión de Crisis: La BC prepara a los líderes del sector público para tomar decisiones informadas y flexibles durante una crisis, lo que puede marcar la diferencia en la resolución efectiva de problemas.
9. Protección de la Reputación: La forma en que el sector público gestiona las crisis puede afectar su reputación a largo plazo. La BC ayuda a proteger y preservar la imagen pública de la organización.
10. Apoyo a la Recuperación de la Comunidad: La BC puede extenderse más allá de las operaciones gubernamentales para apoyar la recuperación de la comunidad en su conjunto, promoviendo la estabilidad y la resistencia. La implementación de la Continuidad del Negocio en el sector público es esencial para garantizar la prestación efectiva de servicios, la resiliencia en momentos de crisis y la protección de la comunidad y la reputación gubernamental.

5.5 Norma ISO 22301

La norma ISO 22301 es un estándar internacional que establece los requisitos para un Sistema de Gestión de la Continuidad del Negocio (SGCN). Su objetivo principal es proporcionar un marco sistemático y efectivo para que las organizaciones puedan prepararse, responder y recuperarse de eventos que puedan interrumpir sus operaciones normales. (NQA, 2022). Aquí hay información clave sobre la norma ISO 22301:

1. Ámbito de Aplicación: La ISO 22301 es aplicable a organizaciones de cualquier tipo y tamaño, ya sean del sector público o privado. Su enfoque es la gestión de la continuidad del negocio en general.
2. Estructura: La norma ISO 22301 sigue una estructura similar a otras normas de sistemas de gestión ISO, como la ISO 9001 (Gestión de la Calidad) y la ISO 14001

(Gestión Ambiental). Esto facilita la integración de la gestión de la continuidad del negocio en la gestión general de la organización.

3. Principales Requisitos: Algunos de los principales requisitos de la norma ISO 22301 incluyen la identificación de riesgos y amenazas, el análisis de impacto en el negocio (BIA), la implementación de medidas de mitigación, la planificación de la continuidad, las pruebas y ejercicios, y la revisión y mejora continua.
4. Objetivos de la ISO 22301: La norma busca asegurar que una organización pueda mantener sus operaciones críticas en funcionamiento, minimizar el impacto de las interrupciones, garantizar la disponibilidad de recursos esenciales y acelerar la recuperación después de un evento disruptivo.
5. Certificación: Las organizaciones pueden buscar la certificación conforme a la ISO 22301 a través de organismos de certificación acreditados. Esto demuestra su cumplimiento de los requisitos de la norma y su compromiso con la gestión de la continuidad del negocio.
6. Beneficios: La implementación de la ISO 22301 ofrece una serie de beneficios, como la mejora de la resiliencia de la organización, la reducción del tiempo de inactividad, la protección de la reputación, el cumplimiento normativo y la optimización de la asignación de recursos.
7. Adaptabilidad: La norma es lo suficientemente flexible como para adaptarse a las necesidades y circunstancias específicas de cada organización. Esto significa que puede ser implementada de manera escalable y personalizada. La norma ISO 22301 es una herramienta valiosa para las organizaciones que desean establecer un sistema eficaz de gestión de la continuidad del negocio. Ayuda a garantizar que estén preparadas para enfrentar y recuperarse de situaciones de crisis y eventos disruptivos.

5.6 Estructura de la Norma ISO

La norma ISO 22301 sigue una estructura común con otras normas de sistemas de gestión ISO. Esta estructura es conocida como la "Estructura de Alto Nivel" (High-Level Structure, HLS) y se implementa para facilitar la integración de múltiples sistemas de gestión en una organización. (SFAI, 2022). La estructura de la norma ISO 22301 es la siguiente:

1. Alcance: Aquí se define el alcance del sistema de gestión de la continuidad del negocio (SGCN), es decir, qué partes de la organización y actividades están cubiertas por el sistema.
2. Referencias Normativas: En este apartado se mencionan las normas y documentos de referencia relevantes para la aplicación de la ISO 22301.

3. Términos y Definiciones: Se proporcionan definiciones clave que ayudan a comprender los conceptos específicos utilizados en la norma.
4. Contexto de la Organización: Esta sección aborda la necesidad de que la organización comprenda su contexto interno y externo, así como las expectativas y necesidades de las partes interesadas relevantes.
5. Liderazgo: Aquí se establecen los requisitos relacionados con el compromiso de la alta dirección en la implementación y mantenimiento del SGCN. Esto incluye la asignación de roles y responsabilidades.
6. Planificación: En esta sección se detallan los requisitos para la identificación de riesgos y oportunidades, así como la definición de objetivos de continuidad del negocio.
7. Soporte: Se abordan los recursos necesarios para el SGCN, incluida la competencia del personal y la comunicación interna y externa.
8. Operación: Esta sección se enfoca en la implementación de los planes de continuidad, incluida la gestión de cambios y la preparación para la respuesta ante incidentes.
9. Evaluación del Desempeño: Se establecen los requisitos para evaluar la eficacia del SGCN a través de la supervisión, la medición, la revisión y la auditoría interna.
10. Mejora: Aquí se abordan los procesos de mejora continua, incluida la corrección de no conformidades y la revisión por la dirección. Esta estructura es común en muchas normas ISO para sistemas de gestión, lo que facilita la integración y la gestión eficaz de múltiples sistemas dentro de una organización. Al seguir esta estructura, la ISO 22301 se alinea con las mejores prácticas en la gestión de la continuidad del negocio y la resiliencia empresarial.

5.7 Plan de Emergencia

Un Plan de Emergencia es un documento o conjunto de procedimientos diseñados para gestionar y responder eficazmente a situaciones de emergencia o crisis que puedan ocurrir en una organización. Su objetivo principal es proteger la vida, la seguridad y el bienestar de las personas, así como minimizar los daños a la propiedad y los impactos negativos en las operaciones de la organización. (Torres, 2023). Aquí hay aspectos clave de un Plan de Emergencia:

1. Objetivos Claros: Un plan de emergencia debe tener objetivos bien definidos, como evacuar a las personas en caso de incendio, proporcionar atención médica en caso de lesiones, o gestionar la respuesta a un desastre natural.

2. Identificación de Riesgos y Escenarios: Debe incluir una lista de posibles amenazas o escenarios de emergencia que la organización podría enfrentar, como incendios, inundaciones, terremotos, amenazas cibernéticas, entre otros.
3. Roles y Responsabilidades: Debe especificar quiénes son los responsables de llevar a cabo cada tarea durante una emergencia, desde los líderes de equipo hasta los primeros socorristas y coordinadores de evacuación.
4. Procedimientos de Respuesta: Deben detallarse los procedimientos paso a paso para responder a cada tipo de emergencia. Esto incluye cómo notificar a las autoridades pertinentes y cómo coordinar la evacuación o el tratamiento de heridos.
5. Comunicación: Debe incluir un plan de comunicación que especifique cómo se notificará a las personas afectadas, al personal y a las partes interesadas externas, como clientes o proveedores, durante una emergencia.
6. Recursos y Suministros: Debe enumerar los recursos necesarios para llevar a cabo las operaciones de respuesta de emergencia, como equipo médico, extintores, equipos de comunicación de respaldo, etc.
7. Entrenamiento y Ejercicios: Es importante incluir programas de entrenamiento y simulacros regulares para asegurarse de que el personal conozca sus roles y sepa cómo responder en una emergencia.
8. Evaluación y Mejora Continua: Después de cada incidente o simulacro, se deben realizar evaluaciones para identificar áreas de mejora en el plan de emergencia. El plan debe actualizarse en consecuencia.
9. Documentación y Distribución: El Plan de Emergencia debe estar bien documentado y accesible para todo el personal relevante. También puede ser necesario proporcionar copias a las autoridades locales o regionales.
10. Coordinación Externa: En algunos casos, puede ser necesario coordinar la respuesta de emergencia con otras organizaciones o agencias gubernamentales, por lo que el plan debe incluir mecanismos de coordinación externa. Un Plan de Emergencia efectivo es esencial para garantizar la seguridad de las personas y la protección de los activos de una organización en situaciones de crisis. Su diseño y actualización deben ser una prioridad para cualquier empresa u entidad.

5.8 Plan de Contingencia

Un Plan de Contingencia es un conjunto de procedimientos y estrategias diseñadas para abordar y mitigar los efectos de eventos no deseados o imprevistos que pueden afectar las operaciones normales de una organización. A diferencia de un Plan de Emergencia, que se

centra en situaciones críticas y de vida o muerte, un Plan de Contingencia aborda una variedad de escenarios que pueden causar interrupciones significativas, pero no necesariamente representan una amenaza inmediata para la vida o la seguridad. (Martins, 2022). Aquí hay aspectos clave de un Plan de Contingencia:

1. Identificación de Escenarios de Contingencia: Un Plan de Contingencia debe comenzar identificando los posibles escenarios de contingencia que podrían afectar a la organización. Estos pueden incluir, por ejemplo, la pérdida de datos críticos, una interrupción en la cadena de suministro o una huelga laboral.
2. Evaluación de Impacto: Para cada escenario de contingencia, se debe evaluar el impacto potencial en las operaciones, la reputación y las finanzas de la organización. Esto implica considerar las pérdidas financieras, el tiempo de inactividad y otros factores relevantes.
3. Desarrollo de Estrategias de Contingencia: Con base en la evaluación de impacto, se desarrollan estrategias y planes de acción específicos para abordar cada escenario de contingencia. Estos planes pueden incluir la asignación de recursos, la comunicación con partes interesadas y la implementación de medidas preventivas.
4. Roles y Responsabilidades: Se especifican los roles y responsabilidades de las personas y equipos encargados de implementar el Plan de Contingencia. Esto asegura una respuesta coordinada y eficaz en caso de contingencia.
5. Recursos y Suministros: Se identifican los recursos y suministros necesarios para implementar las estrategias de contingencia. Esto puede incluir personal adicional, equipo de respaldo o suministros de emergencia.
6. Comunicación: El Plan de Contingencia debe incluir un plan de comunicación que especifique cómo se informará a las partes interesadas internas y externas durante una contingencia. La comunicación oportuna y precisa es esencial.
7. Pruebas y Ejercicios: Al igual que con un Plan de Emergencia, se deben realizar pruebas y ejercicios regulares para asegurarse de que el Plan de Contingencia funcione según lo previsto.
8. Actualización y Mantenimiento: Los planes de contingencia no son estáticos y deben revisarse y actualizarse periódicamente para reflejar cambios en la organización y en el entorno operativo.
9. Coordinación con Otros Planes: El Plan de Contingencia puede ser parte de un sistema más amplio de gestión de la continuidad del negocio que incluye un Plan de Emergencia y otros planes relacionados. Un Plan de Contingencia efectivo es esencial

para garantizar que una organización pueda adaptarse y responder de manera efectiva a situaciones no previstas que podrían afectar su capacidad para funcionar de manera normal. Ayuda a minimizar el impacto de eventos adversos y a mantener la resiliencia empresarial.

5.9 Normas internacionales relacionadas a la continuidad operativa

Existen varias normas internacionales relacionadas con la continuidad operativa y la gestión de la continuidad del negocio. Estas normas proporcionan marcos y directrices para ayudar a las organizaciones a establecer y mantener sistemas efectivos de gestión de la continuidad del negocio. (GlobalSuite Solutions, 2023). Algunas de las normas más importantes en este ámbito son:

1. ISO 22301 - Gestión de la Continuidad del Negocio: Como mencioné anteriormente, la norma ISO 22301 establece requisitos y directrices para un Sistema de Gestión de la Continuidad del Negocio (SGCN). Es una de las normas más ampliamente reconocidas y utilizadas en este campo.
2. ISO 22313 - Guía para la Implementación de la ISO 22301: Esta norma proporciona orientación específica sobre cómo implementar los requisitos de la ISO 22301. Ofrece consejos detallados para ayudar a las organizaciones a desarrollar y mantener un SGCN eficaz.
3. ISO 27001 - Seguridad de la Información: Aunque no es exclusivamente una norma de continuidad del negocio, la ISO 27001 incluye requisitos relacionados con la gestión de la continuidad operativa en el contexto de la seguridad de la información. Ayuda a garantizar que las organizaciones puedan proteger la disponibilidad de la información crítica.
4. ISO 31000 - Gestión del Riesgo: La ISO 31000 proporciona directrices sobre la gestión del riesgo en general. Si bien no se centra exclusivamente en la continuidad del negocio, es fundamental para identificar, evaluar y tratar los riesgos que pueden amenazar la continuidad operativa.
5. NFPA 1600 - Norma sobre Preparación y Respuesta a Emergencias, Continuidad y Resiliencia del Negocio: Esta norma desarrollada por la Asociación Nacional de Protección contra Incendios (NFPA) de los Estados Unidos ofrece pautas para la preparación, la respuesta y la continuidad en caso de emergencias y desastres.
6. BS 25999 (Reemplazada por la ISO 22301): La norma británica BS 25999 fue la precursora de la norma ISO 22301 y proporcionaba pautas similares para la gestión de

la continuidad del negocio. Aunque fue reemplazada por la ISO 22301, algunas organizaciones todavía pueden hacer referencia a ella. Estas normas son valiosas para las organizaciones que desean establecer y mejorar sus sistemas de gestión de la continuidad del negocio. Proporcionan un marco estructurado y reconocido internacionalmente para ayudar a proteger la resiliencia de la organización ante situaciones adversas y eventos disruptivos.

5.10 Tipos de Amenazas en TI

En el campo de la tecnología de la información (TI), existen diversos tipos de amenazas que pueden poner en peligro la seguridad, la integridad y la disponibilidad de sistemas y datos. (Ambit, 2021). Algunas de las amenazas más comunes en TI incluyen:

1. Malware: Este término engloba una variedad de software malicioso, como virus, troyanos, gusanos y ransomware, diseñados para dañar, robar o bloquear el acceso a sistemas y datos.
2. Ataques de Denegación de Servicio (DDoS): Los ataques DDoS buscan inundar un sistema o una red con tráfico falso o sobrecargarlos, lo que resulta en la indisponibilidad de servicios y recursos.
3. Ingeniería Social: Los atacantes utilizan técnicas de manipulación psicológica para engañar a las personas y obtener acceso a sistemas o información confidencial.
4. Phishing: Los correos electrónicos de phishing intentan engañar a los usuarios para que divulguen información personal o credenciales de inicio de sesión al hacerse pasar por entidades legítimas.
5. Hacking y Ataques de Fuerza Bruta: Los hackers pueden intentar acceder ilegalmente a sistemas utilizando técnicas de fuerza bruta para adivinar contraseñas o explotar vulnerabilidades.
6. Malware Móvil: Similar al malware en computadoras, el malware móvil se dirige a dispositivos móviles, como teléfonos inteligentes y tabletas, con el fin de robar información o tomar el control.
7. Ransomware: Este tipo de malware cifra los archivos del usuario y exige un rescate para desbloquearlos, lo que puede causar la pérdida de datos o interrupciones en las operaciones.
8. Ataques Zero-Day: Se refieren a vulnerabilidades de software que aún no se han descubierto públicamente y, por lo tanto, no tienen soluciones de seguridad disponibles.

9. Intercepción de Tráfico: Los atacantes pueden interceptar y monitorear el tráfico de red para robar datos confidenciales, como contraseñas o información financiera.
10. Ataques de Inyección de Código: Estos ataques incluyen la inyección de código malicioso en aplicaciones web o bases de datos para obtener acceso no autorizado o causar daños.
11. Ataques de Suplantación de Identidad (Spoofing): Los atacantes pueden hacerse pasar por sistemas legítimos o usuarios para engañar a otros sistemas o usuarios.
12. Vulnerabilidades de Software y Parches Inadecuados: La falta de actualizaciones de seguridad o la existencia de vulnerabilidades no parcheadas pueden dejar sistemas expuestos a amenazas. Estas son solo algunas de las amenazas comunes en el campo de la TI. La seguridad de la información es esencial para protegerse contra estas amenazas y garantizar la integridad y la disponibilidad de sistemas y datos.

6 MARCO METODOLÓGICO

El presente estudio se basa en un enfoque de investigación cualitativo. Se eligió este enfoque debido a su idoneidad para explorar en profundidad la gestión de la continuidad del negocio en el contexto de los servicios tecnológicos del GAD Municipal del cantón Mocache. La investigación cualitativa permite una comprensión detallada de los procesos y las prácticas, lo que es esencial para abordar los objetivos de este estudio.

6.1 Recopilación de Datos

La recopilación de datos se llevó a cabo utilizando múltiples métodos, incluyendo:

Entrevistas Semiestructuradas: Se realizaron entrevistas con los responsables de la gestión de servicios tecnológicos del GAD Municipal del cantón Mocache. Estas entrevistas permitieron obtener información detallada sobre la planificación de la continuidad del negocio, las amenazas identificadas y las estrategias de mitigación.

Revisión de Documentos: Se revisaron documentos internos relacionados con la gestión de la continuidad del negocio, como planes de emergencia, planes de contingencia y registros de incidentes anteriores.

Observación Participante: Se llevó a cabo una observación participante limitada para comprender la dinámica interna de la organización y cómo se abordan las situaciones de crisis en tiempo real.

6.2 Procedimientos de Análisis

Los datos recopilados se analizaron utilizando un enfoque de análisis de contenido. Las entrevistas se transcribieron y se aplicó codificación temática para identificar patrones, temas y conceptos clave relacionados con la continuidad del negocio en los servicios tecnológicos. Se utilizaron herramientas de software para facilitar el análisis y la organización de los datos.

6.3 Ética y Validación

Se obtuvo el consentimiento informado de los participantes y se garantizó la confidencialidad de la información proporcionada. Además, se utilizó el principio de triangulación,

comparando múltiples fuentes de datos (entrevistas, documentos y observación) para garantizar la validez y la fiabilidad de los resultados.

6.4 Limitaciones del Estudio

Es importante reconocer que este estudio tiene algunas limitaciones. La investigación se centró en un solo caso, lo que puede limitar la generalización de los hallazgos a otros contextos. Además, la disponibilidad de datos podría haber sido influenciada por la cooperación de los participantes.

6.5 Contribución a la Investigación

Este estudio contribuye al conocimiento existente al proporcionar una comprensión detallada de la gestión de la continuidad del negocio en el sector público, específicamente en el ámbito de los servicios tecnológicos en una región propensa a desastres naturales.

7 RESULTADOS

7.1 Variables evaluadas

7.1.1 Entrevista

En esta discusión clave, se evaluaron temas esenciales para prepararse ante diversas situaciones en nuestra investigación. El Ingeniero Jorge Luis Peñafiel, encargado de Servicios Tecnológicos en el municipio del cantón Mocache, desempeñó un papel fundamental al compartir valiosos conocimientos y perspectivas. Su experiencia en servicios tecnológicos municipales aportó información valiosa que enriqueció nuestra comprensión actual y orientó futuras investigaciones y estrategias, considerando las circunstancias específicas del GAD Municipal del cantón Mocache.

Se indico mediante esta variable que es satisfactorio porque la infraestructura de red en el municipio del cantón Mocache es segura. Las conexiones de internet de alta velocidad y la adopción de medidas de seguridad cibernética avanzadas, como firewalls y sistemas de detección de intrusiones, protegen eficazmente los sistemas informáticos locales. Esto es crucial para prevenir ataques cibernéticos y garantizar la seguridad de la información del municipio y de sus residentes.

Es evidente que el municipio del cantón Mocache ha tomado medidas significativas para garantizar que los servicios tecnológicos sean accesibles para todos los ciudadanos, incluyendo aquellos con discapacidades, aunque todavía existen áreas de mejora.

Existen desafíos que afectan la coherencia de la información. Uno de los problemas comunes es la falta de estandarización en la entrada de datos, lo que puede llevar a inconsistencias en la información almacenada. La capacitación y la promoción de prácticas de entrada de datos coherentes pueden contribuir a resolver este problema

Desde una perspectiva tecnológica, es evidente que en el municipio de Mocache existe una preocupación limitada en lo que respecta a la escalabilidad de los servicios tecnológicos y su

capacidad para adaptarse a un aumento en la demanda de usuarios y datos. Esto puede ser motivo de inquietud en un entorno tecnológico en constante evolución.

En el municipio del cantón Mocache existe una percepción bastante limitada de que los servicios tecnológicos cumplen con las regulaciones y estándares específicos. Esto puede ser motivo de preocupación, ya que el cumplimiento de estas normativas es fundamental para garantizar la legalidad y la calidad de los servicios tecnológicos ofrecidos.

Se observa que en el municipio de Mocache existe un nivel medio de preparación para garantizar que los servicios tecnológicos sean accesibles para todos los ciudadanos, incluyendo aquellos con discapacidades. Aunque se han tomado algunas medidas, aún hay margen para mejorar la accesibilidad de manera más completa

Es esencial reconocer la importancia de la disponibilidad continua de los servicios críticos, especialmente en el ámbito gubernamental, donde la prestación de servicios es fundamental para la comunidad. Sin embargo, parece haber una falta de enfoque en la planificación y la preparación para mantener estos servicios en funcionamiento en situaciones de emergencia o interrupciones.

Desde una perspectiva tecnológica, es evidente que en el municipio de Mocache se ha demostrado una planificación satisfactoria en lo que respecta al mantenimiento regular y las actualizaciones de los sistemas tecnológicos. Esta es una práctica esencial para garantizar la eficacia y la seguridad de los servicios digitales ofrecidos a la comunidad.

Se puede observar que en el municipio de Mocache se están llevando a cabo muy pocas iniciativas innovadoras o estratégicas para ofrecer soluciones tecnológicas efectivas, especialmente dentro de las restricciones presupuestarias existentes. Esta falta de enfoque en la innovación puede limitar el potencial de mejora en los servicios tecnológicos municipales.

Se ha demostrado un reconocimiento de la importancia de la seguridad cibernética y la necesidad de abordar las vulnerabilidades de manera proactiva. Esto se refleja en la adopción de medidas de seguridad, como firewalls y sistemas de detección de intrusiones, que ayudan a proteger los sistemas contra amenazas cibernéticas.

7.1.2 Observación participante

En el análisis de la situación en el GAD Municipal del cantón Mocache, se observan varios aspectos relacionados con la gestión de la tecnología y los servicios. Por un lado, se ha establecido un marco de políticas de seguridad de datos, aunque se identifica una debilidad en la falta de documentación detallada sobre medidas específicas. Además, se nota un nivel de preparación medio en términos de seguridad cibernética, pero se carece de un plan integral de respuesta a incidentes.

En cuanto a la integración de sistemas y bases de datos, se evidencia que se lleva a cabo en áreas clave, como la gestión de residentes, aunque existe margen para optimizar la eficiencia en esta área. Además, se percibe que la infraestructura tecnológica actual podría no ser suficiente para manejar un aumento significativo en la demanda de usuarios y datos, lo que plantea desafíos de escalabilidad.

En el ámbito de la accesibilidad, se han tomado medidas medianamente efectivas, pero se requiere una mejora en la implementación práctica, especialmente para atender las necesidades de personas con discapacidades cognitivas.

Por otra parte, se observa una falta de medidas y protocolos para garantizar la disponibilidad continua de servicios críticos, lo que resalta la necesidad de desarrollar una estrategia de continuidad del negocio. En cuanto al mantenimiento regular y actualizaciones de sistemas tecnológicos, se realiza un mantenimiento rutinario.

En el ámbito de la innovación tecnológica, se identifica una limitación en los enfoques actuales y se destaca la necesidad de adoptar un enfoque más estratégico para encontrar soluciones efectivas dentro de las restricciones presupuestarias. Finalmente, aunque se cuenta con un nivel medio de preparación en cuanto a estrategias de seguridad y mantenimiento de sistemas, se reconoce la necesidad de un enfoque más integral en la planificación para mejorar la eficacia y la protección de los sistemas.

7.2 Conclusión de las variables evaluadas

La necesidad de aplicar un plan de continuidad de negocio en el municipio del cantón Mocache se deriva de varias observaciones clave en la evaluación. Aunque se reconoce la seguridad de la infraestructura de red y la adopción de medidas avanzadas de seguridad

cibernética, existen desafíos que podrían afectar la coherencia de la información, la escalabilidad de los servicios tecnológicos y el cumplimiento de regulaciones específicas. Además, se identificó una falta de enfoque en la planificación y preparación para mantener servicios críticos en funcionamiento durante emergencias o interrupciones. La necesidad de un plan de continuidad de negocio se vuelve evidente para abordar estas áreas de mejora, garantizando la disponibilidad continua de servicios esenciales y fortaleciendo la capacidad del municipio para hacer frente a posibles situaciones de crisis.

7.3 Plan de continuidad del negocio

1. Introducción

La necesidad de realizar un plan de continuidad de negocio basado en la norma ISO 22301 en los servicios tecnológicos de un Gobierno Autónomo Descentralizado (GAD) Municipal del cantón Mocache es la falta de preparación para hacer frente a interrupciones significativas en las operaciones.

Este problema se manifiesta cuando una organización subestima o ignora los riesgos que podrían interrumpir sus servicios tecnológicos, como ciberataques, desastres naturales, fallos de hardware, cortes de energía, entre otros. Como resultado, la entidad puede carecer de planes efectivos para garantizar la continuidad de sus operaciones tecnológicas en situaciones de crisis. La falta de preparación puede llevar a consecuencias graves, como la pérdida de datos críticos, la interrupción de servicios esenciales para la comunidad y la incapacidad de recuperarse de manera eficiente después de una interrupción. Además, puede dañar la reputación de la entidad y socavar la confianza de los ciudadanos y las partes interesadas.

1.1. Propósito y Objetivos

1.1.1. Propósito

El propósito fundamental del plan de continuidad de negocio (BCP, por sus siglas en inglés) basado en la norma ISO 22301 es asegurar que el GAD municipal de Mocache pueda mantener o restablecer sus operaciones críticas en caso de interrupciones significativas o desastres.

1.1.2. Objetivos

Garantizar la recuperación de servicios tecnológicos críticos después de una situación de riesgo o una interrupción dentro del GAD Municipal del cantón MOCACHE

1.2. Alcance

Este plan de continuidad de negocio tiene por alcance el Departamento de Tecnologías de la Información (TI) y equipos vinculados con los servicios tecnológicos que ofrece el GAD municipal de Mocache.

2. Comprensión de la Organización

El objetivo final de la compresión de organización dentro del Gad Municipal del cantón Mocache es mejorar la eficiencia, la transparencia y la capacidad de respuesta del gobierno local, lo que, a su vez, puede traducirse en un mejor servicio para la comunidad.

2.1 Perfil de la Organización

2.1.1. Información Básica:

Nombre: Gobierno Autónomo Descentralizado Municipal de Mocache

Ubicación: Cantón Mocache, Provincia de Los Ríos, Ecuador

Fecha de Creación: 28 de mayo de 1996

Misión:

"Nuestra misión es servir y mejorar la calidad de vida de los ciudadanos del cantón Mocache, proporcionando servicios públicos eficientes, promoviendo el desarrollo sostenible, fomentando la participación ciudadana y garantizando la transparencia en la gestión municipal. Trabajamos incansablemente para crear un entorno seguro, próspero y vibrante en el que todos los habitantes puedan prosperar y sentirse orgullosos de ser parte de esta comunidad."

Visión:

"Nuestra visión es convertir al cantón Mocache en un modelo de desarrollo sostenible y progresivo en la región, reconocido por su calidad de vida, su infraestructura moderna, su gestión eficiente y su participación ciudadana activa. Vemos un futuro en el que nuestra comunidad disfrute de un ambiente limpio y saludable, oportunidades económicas, educación de calidad y una convivencia armoniosa, donde las generaciones presentes y futuras prosperen juntas y contribuyan al bienestar común."

2.1.2 Organización y Estructura:

Alcalde: Yenny Domínguez

Concejo Municipal:

- Manuel Antón Asesor Jurídico
- Sr. Gonzalo Álvarez M. Vocal Principal
- Sr. Máximo Aguayo S. Vocal Principal

- Sr. Rigoberto España L. Vocal Alterno
- Sra. Gladys Carriel, Vocal Alterna

2.2. Contexto del Negocio

El contexto de negocio del Gad Municipal de Mocache, es dinámico y puede cambiar con el tiempo, la participación ciudadana y la transparencia son elementos cruciales para tener en cuenta en la gestión municipal.

- Entorno Externo:

1. Económico: El cantón Mocache esta influenciado por factores económicos como tasas de desempleo, ingresos promedio de la población, actividad agrícola y comercial local, así como la situación económica a nivel nacional.

2. Político y Legal: La administración del Gad municipal debe cumplen con las leyes y regulaciones locales, provinciales y nacionales. Además, las decisiones políticas a nivel nacional pueden afectar el presupuesto y las políticas locales.

3. Social y Demográfico: Factores como el crecimiento demográfico, la composición de la población, las tasas de migración y las necesidades sociales del cantón son importantes para la planificación y la prestación de servicios.

4. Ambiental: La gestión ambiental es crucial para la sostenibilidad del municipio, incluyendo la protección de recursos naturales y la mitigación de riesgos ambientales.

5. Cultural: Incluyendo tradiciones, costumbres y valores de la comunidad como su festividad de cantonización y otras que se festejan en el trascurso del año influye en la toma de decisiones y las políticas culturales locales.

- Entorno Interno:

1. Recursos y Presupuesto: Los recursos disponibles, incluyendo el presupuesto del Gad municipal, influyen en la capacidad del municipio para proporcionar servicios y llevar a cabo proyectos.

2. Estructura Organizativa: La organización interna del gobierno municipal, incluyendo departamentos y unidades, afecta la eficiencia y la toma de decisiones.

3. Participación Ciudadana: La colaboración y la participación activa de la comunidad mocacheña son fundamentales para el éxito de las políticas y proyectos.

4. Cultura Organizativa: La cultura de la organización, los valores y la ética de trabajo de los empleados dentro de Gad Municipal del cantón Mocache impactan en la eficacia y la calidad de los servicios prestados.
5. Historia y Trayectoria: La historia y las experiencias pasadas del municipio pueden proporcionar información importante para la toma de decisiones y la planificación estratégica.
6. Proyectos y Objetivos: Los proyectos en curso y los objetivos a largo plazo de desarrollo son parte fundamental del contexto de negocio, ya que determinan las prioridades de la administración.
7. Relaciones y Cooperación: Las relaciones con otras entidades gubernamentales, organizaciones locales y sectores privados influyen en la capacidad del municipio para llevar a cabo proyectos y programas.

3. Liderazgo

3.1. Compromiso de la Alta Dirección

La continuidad del negocio requiere que la alta dirección de una organización emita una declaración formal de compromiso con la continuidad del negocio. Esta declaración muestra el compromiso de la alta dirección en apoyar y liderar la implementación de medidas de continuidad del negocio, asignar recursos necesarios y establecer políticas y procedimientos para garantizar la preparación y respuesta efectiva ante interrupciones o crisis. La continuidad del negocio y su importancia estratégica son priorizadas en la cultura organizacional a través de esta acción (López , 2019).

3.2. Política de Continuidad de Negocio

La Política de Continuidad de Negocios de una empresa indica su compromiso con la capacidad de resiliencia operativa en caso de interrupción o crisis. Esta política prioriza la continuidad del negocio como estrategia principal, asigna los recursos necesarios, cubre todas las áreas críticas, fomenta la capacitación de los empleados, garantiza el cumplimiento legal y establece responsabilidades. La alta dirección es responsable de implementar la política y asegurarse de que sea ampliamente comunicada en la organización, lo que promueve una

cultura de preparación y respuesta efectiva a situaciones adversas como el siguiente ejemplo (INCIBE, 2019).

"La Política de Continuidad de Negocio de XYZ Company" establece su firme compromiso con la resiliencia empresarial, prioriza la continuidad del negocio como estrategia clave, asigna recursos necesarios, abarca todos los aspectos críticos de la organización, promueve la capacitación de empleados y garantiza el cumplimiento legal. La alta dirección lidera su implementación y se asegura de que la política se comunique ampliamente, fomentando una cultura de preparación y respuesta efectiva ante situaciones adversas.

4. Planificación

4.1. Análisis de Riesgos y Oportunidades

4.1.1. Identificación de Activos

En el Gobierno Autónomo Descentralizado (GAD) Municipal de Mocache, Ecuador, la infraestructura tecnológica es esencial para optimizar las operaciones municipales y mejorar la prestación de servicios. La tabla que se proporciona a continuación ofrece un análisis exhaustivo de los activos tecnológicos fundamentales.

Tabla 1. Inspección de materiales activos tecnológicos existente en el Gad Municipal del cantón Mocache.

Activo	**Área responsable del activo**
Computadoras de escritorio	Departamento de Tecnologías de la Información (TI)
Computadoras portátiles	Departamento de Tecnologías de la Información (TI)
Discos duros externos	Departamento de Tecnologías de la Información (TI)
Discos duros de servidores	Departamento de Tecnologías de la Información (TI)
Impresoras	Departamento de Tecnologías de la Información (TI)
Escáneres	Departamento de Tecnologías de la Información (TI)

Parlantes	Departamento de Tecnologías de la Información (TI)
Proyectores	Departamento de Tecnologías de la Información (TI)
Cámaras	Departamento de Tecnologías de la Información (TI)
Routers	Departamento de Redes y Comunicaciones
Switches	Departamento de Redes y Comunicaciones
Armario Rackeable	Departamento de Tecnologías de la Información (TI)
Firewalls	Departamento de Tecnologías de la Información (TI)
Antivirus	Departamento de Tecnologías de la Información (TI)
Puntos de Acceso (AP)	Departamento de Redes y Comunicaciones
Cable estructurado	Departamento de Redes y Comunicaciones
Fibra óptica	Departamento de Redes y Comunicaciones
Administrador de red	Departamento de Redes y Comunicaciones
Instalación eléctrica	Departamento de Mantenimiento
Sistema operativo windows server	Departamento de Tecnologías de la Información (TI)
Correo electrónico	Departamento de Tecnologías de la Información (TI)

4.1.2. Valoración de activos

Esta evaluación se llevó a cabo con el propósito de determinar el nivel de importancia de los activos, con el objetivo de priorizar el análisis de las posibles amenazas y vulnerabilidades

asociadas. En este procedimiento, se emplea una escala de valoración que se encuentra detallada en la **Tabla 7.** (Teodoro y otros, 2016).

A continuación, se evaluará cada activo para medir su nivel de importancia.

Tabla 2. Valoración de cada activo.

Activo	**Descripción**	**Dependencia**	**Funcionalidad**	**Integridad, Funcionalidad y Disponibilidad**	**Promedio**
Computadoras de escritorio	Procesamiento de información y tareas administrativas.	4	4	3	4
Computadoras portátiles	Flexibilidad en el trabajo y ejecución de tareas fuera de la oficina.	3	4	3	3
Discos duros externos	Almacenamiento adicional y portátil de datos.	2	3	3	3
Discos duros de servidores	Almacenamiento centralizado y gestión de datos críticos.	5	5	4	5
Impresoras	Impresión de documentos para la gestión de información física.	3	3	2	3
Escáneres	Digitalización de documentos para la gestión electrónica.	2	3	2	2
Parlantes	Mejora de la comunicación interna y presentaciones multimedia.	2	2	1	2
Proyectores	Facilita presentaciones y visualización de información.	2	3	2	2
Cámaras	Vigilancia y seguridad	4	4	3	4

	visual de instalaciones y áreas públicas.				
Routers	Establecimiento y gestión de la conectividad en redes.	5	4	4	4
Switches	Conmutación eficiente para la conectividad interna de dispositivos.	5	4	4	4
Armario Rackeable	Organización y alojamiento de equipos electrónicos.	3	3	3	3
Firewalls	Protección contra amenazas cibernéticas y seguridad de red.	5	4	5	5
Antivirus	Protección contra software malicioso y amenazas informáticas.	5	4	5	5
Puntos de Acceso (AP)	Facilita la conectividad inalámbrica y la movilidad en instalaciones.	4	4	4	4
Cable estructurado	Infraestructura física para la transmisión de datos en red.	5	5	5	5
Fibra óptica	Proporciona una conexión de alta velocidad y seguridad en la transmisión de datos.	5	5	5	5
Instalación eléctrica	Proporciona la energía necesaria para el funcionamiento de equipos y sistemas.	4	3	3	3

Sistema operativo windows server	Entorno operativo para servidores, facilitando la gestión centralizada.	5	4	4	4
Correo electrónico	Facilita la comunicación interna y externa, y la gestión de la correspondencia digital.	4	4	4	4

Los resultados de la Integridad, Funcionalidad y Disponibilidad se encuentran detallados en la **Tabla 8.**

4.1.3. Identificación de amenazas y vulnerabilidades

La adopción de la norma 27005 para la identificación de amenazas y vulnerabilidades destaca como una elección estratégica para la gestión de riesgos de los servicios tecnológicos. Al utilizar esta norma, se garantiza un enfoque estandarizado que se centra especialmente en los activos más críticos para la organización. Este método no solo asegura una evaluación integral, sino que también facilita una gestión de riesgos más precisa y alineada con las mejores prácticas de seguridad (AENOR, 2018).

Tabla 3. Identificación de amenazas y vulnerabilidades de los Activo.

Fuente: ISO 27005

Tipo de Activo	Activo	Vulnerabilidades	Amenazas
Hardware	Discos duros de servidores	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información
		Ausencia de un eficiente control de cambios en la configuración	Error en el uso
		Almacenamiento sin protección	Hurto de medios o documentos
		Copia no controlada	Hurto de medios o documentos

Software	Firewalls	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
		Ausencia de pistas de auditoria	Abuso de los derechos
		Interfaz de usuario compleja	Error en el uso
		Ausencia de documentación	Error en el uso
		Configuración incorrecta de parámetros	Error en el uso
		Habilitación de servicios innecesarios	Procesamiento ilegal de datos
		Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
		Ausencia de copias de respaldo	Manipulación con software
Software	Antivirus	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
		Ausencia de pistas de auditoria	Abuso de los derechos
		Ausencia de documentación	Error en el uso
		Configuración incorrecta de parámetros	Error en el uso

		Habilitación de servicios innecesarios	Procesamiento ilegal de datos
		Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
		Ausencia de copias de respaldo	Manipulación con software
Red	Cable estructurado	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
		Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
		Punto único de falla	Falla del equipo de telecomunicaciones
Red	Fibra óptica	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
		Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
		Punto único de falla	Falla del equipo de telecomunicaciones

4.1.4. Análisis de impacto y probabilidad

La escala de medición propuesta adopta un enfoque dual al evaluar riesgos, considerando tanto la probabilidad como la facilidad de explotación. Esta estructura ofrece una herramienta completa para calificar riesgos, brindando una evaluación equilibrada que facilita la toma de decisiones informadas en la gestión de riesgos.

Tabla 4. Descripción y valorización de amenazas.

ESCALA	VALORACION	DESCRIPCION
1	Bajo	Amenazas cuya probabilidad de explotar vulnerabilidades es muy baja.
2	Medio	Amenazas que con poca frecuencia explotan vulnerabilidades.
3	Alto	Amenazas que frecuentemente explotan vulnerabilidades.

Tabla 5. Escala de evaluación de riesgo.

Fuente: ISO 27005

	Probabilidad de ocurrencia									
	– Amenaza	**Baja**			**Media**			**Alta**		
VALORACIÓN DEL ACTIVO	**Facilidad de explotación**	**Baja**	**Media**	**Alta**	**Baja**	**Media**	**Alta**	**Baja**	**Media**	**Alta**
	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

En el próximo paso, se aplicará la escala proporcionada para clasificar y determinar el nivel de acciones necesarias. Este método permitirá una evaluación sistemática y precisa, brindando un marco claro para la identificación de las respuestas requeridas. La escala facilita la toma de decisiones informadas al asignar a cada situación un grado específico que indica la urgencia y la importancia de las acciones a emprender.

Tabla 6: Análisis de Riesgos.

Activo	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Facilidad de explotación**	**Riesgo**
Discos duros de servidores	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información	2	2	6
	Ausencia de un eficiente control de cambios en la	Error en el uso	3	2	7

	configuración				
	Almacenamiento sin protección	Hurto de medios o documentos	1	1	4
	Copia no controlada	Hurto de medios o documentos	2	3	7
Firewalls	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos	2	1	5
	Ausencia de pistas de auditoria	Abuso de los derechos	3	2	7
	Interfaz de usuario compleja	Error en el uso	1	1	4
	Ausencia de documentación	Error en el uso	2	2	6
	Configuración incorrecta de parámetros	Error en el uso	3	3	8
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos	3	2	7
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	2	1	5
	Ausencia de copias de respaldo	Manipulación con software	2	3	7
Antivirus	Ausencia o insuficiencia de pruebas de	Abuso de los derechos	2	1	5

	software				
	Ausencia de pistas de auditoria	Abuso de los derechos	3	2	7
	Ausencia de documentación	Error en el uso	2	2	6
	Configuración incorrecta de parámetros	Error en el uso	3	3	8
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos	3	2	6
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software	2	1	5
	Ausencia de copias de respaldo	Manipulación con software	2	3	7
Cable estructurado	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones	1	1	4
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones	2	2	6
	Punto único de falla	Falla del equipo de telecomunicaciones	3	3	8
Fibra óptica	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones	1	1	4
	Conexión	Falla del equipo de	2	2	6

	deficiente de los cables.	telecomunicaciones			
	Punto único de falla	Falla del equipo de telecomunicaciones	3	3	8

4.1.5. Calificación de Riesgos:

La calificación de riesgo se basa en la evaluación de la probabilidad que una amenaza explote una vulnerabilidad, y esta afirmación se fundamenta en el modelo fundamental de la gestión de riesgos.

- 0-1 BAJO
- 2-3 MEDIO BAJO
- 4-5 MEDIO
- 6-7 MEDIO ALTO
- 8 CRITICO

4.1.6. Desarrollo de estrategias de mitigación

1. Configuración incorrecta de parámetros en Firewalls y Antivirus:

Prevención:

Auditoría Regular: Realizar auditorías regulares de configuración en firewalls y antivirus para identificar y corregir posibles configuraciones incorrectas.

Políticas de Configuración: Establecer políticas de configuración claras y seguras para firewalls y antivirus. Asegurarse de que solo personal autorizado tenga acceso a realizar cambios.

Mitigación:

Respuesta Rápida: Desarrollar un plan de respuesta rápida para abordar configuraciones incorrectas en firewalls y antivirus tan pronto como se detecten**.**

Capacitación del Personal: Proporcionar capacitación regular al personal sobre las configuraciones adecuadas y seguras de firewalls y antivirus.

2. Punto único de falla en Cable estructurado y Fibra óptica:

Prevención:

Diseño Redundante: Implementar un diseño de red que incluya rutas y conexiones redundantes para evitar puntos únicos de falla.

Ubicación Estratégica: Colocar los puntos de conexión de cable estructurado y fibra óptica en ubicaciones estratégicas para reducir el riesgo de interrupciones.

Mitigación:

Monitoreo Continuo: Implementar sistemas de monitoreo continuo para detectar y responder rápidamente a cualquier interrupción en el cableado.

Plan de Contingencia: Desarrollar un plan de contingencia que incluya estrategias para mitigar el impacto de posibles fallos en el cableado.

Medidas Transversales:

Actualizaciones y Parches: Garantizar que todos los dispositivos, incluidos firewalls y sistemas antivirus, estén actualizados con los últimos parches de seguridad.

Concientización del Personal: Implementar programas de concientización de seguridad para educar al personal sobre la importancia de las configuraciones seguras y la prevención de puntos únicos de falla.

Consideraciones Adicionales:

Respuesta a Incidentes: Establecer un plan de respuesta a incidentes que defina los pasos a seguir en caso de un evento de seguridad.

Colaboración con Proveedores: Colaborar con proveedores de servicios de red y seguridad para garantizar que las mejores prácticas se implementen en la configuración y diseño de la infraestructura.

4.2. Requisitos Legales y Reglamentarios

Los requisitos legales y reglamentarios son leyes y reglamentos establecidos por el gobierno y los organismos reguladores que una organización debe cumplir mientras opera. Estos requisitos incluyen leyes laborales, seguridad, privacidad de datos, medio ambiente, seguridad cibernética y otros temas. Para operar legalmente y evitar sanciones, es esencial cumplir con estos requisitos. Para garantizar operaciones legales y éticas, la gestión de la conformidad legal implica identificar, seguir y mantener el cumplimiento continuo de estos requisitos (Bevan, 2019).

4.3. Objetivos de Continuidad del Negocio

Para garantizar su supervivencia y resiliencia en situaciones de interrupción o crisis, una organización busca alcanzar objetivos de continuidad comercial. Estos objetivos incluyen mantener operaciones críticas, reducir el tiempo de inactividad, proteger activos y recursos, mantener la seguridad del personal, reducir las pérdidas financieras, mantener la satisfacción del cliente, cumplir con las obligaciones legales y reglamentarias, preservar la reputación de la organización, mejorar la capacidad de recuperación y fomentar una cultura de conciencia y preparación. Al lograr estos objetivos, una organización puede mantener su capacidad de funcionar de manera segura y efectiva, incluso en situaciones difíciles. (Rodriguez , 2020).

5. Soporte

5.1. Recursos

Ejecutar un programa destinado a prevenir y reducir los riesgos de seguridad en un Gobierno Autónomo Descentralizado (GAD) en el cantón Mocache necesitará la colaboración de recursos técnicos, humanos y financieros, los cuales se describen a continuación.

Recursos Humanos:

- **Personal de Seguridad de la Información:** Especialistas en seguridad de la información para liderar y ejecutar las actividades relacionadas con la seguridad.
- **Personal de Red y Sistemas:** Ingenieros de red y administradores de sistemas para implementar y mantener la infraestructura de seguridad.
- **Equipo de Respuesta a Incidentes:** Formar y equipar a un equipo de respuesta a incidentes capaz de gestionar y mitigar eventos de seguridad.
- **Especialistas en Capacitación:** Profesionales para proporcionar formación continua al personal sobre las mejores prácticas de seguridad y configuración.

Recursos Financieros:

- **Presupuesto para Herramientas y Software:** Fondos destinados a la adquisición y mantenimiento de herramientas de monitoreo, software de seguridad y sistemas de respaldo.

- **Inversión en Infraestructura Redundante:** Recursos para la adquisición de dispositivos de red redundantes y la mejora de la infraestructura para evitar puntos únicos de falla.
- **Fondos para Capacitación:** Financiamiento para programas de capacitación y concientización en seguridad para el personal.

Recursos de Gestión:

- **Políticas y Procedimientos:** Desarrollar y mantener políticas y procedimientos claros relacionados con la seguridad de la información y la gestión de riesgos.
- **Gestión de Cambios:** Establecer procesos formales para la gestión de cambios en la configuración de firewalls y antivirus.
- **Revisión y Auditoría Regulares:** Programar revisiones y auditorías regulares para evaluar la eficacia de las medidas de seguridad implementadas.
- **Colaboración con Proveedores:** Establecer relaciones con proveedores de servicios de seguridad y red para colaboración en la implementación de mejores prácticas.

Recursos de Educación y Concientización:

- **Materiales Educativos:** Desarrollar materiales educativos sobre seguridad informática y buenas prácticas para el personal.
- **Sesiones de Capacitación:** Programar sesiones regulares de capacitación y concientización sobre seguridad para todo el personal.
- **Herramientas de Evaluación de Concientización:** Implementar herramientas para evaluar el nivel de concientización

5.2 Competencia

El aseguramiento de la competencia necesaria de las personas involucradas en la gestión de la continuidad del negocio es esencial para garantizar una respuesta efectiva ante eventos disruptivos. Algunas estrategias clave para asegurar la competencia de los equipos de gestión de la continuidad del negocio son:

- Formación Continua
- Simulacros y Ejercicios
- Certificaciones Específicas

- Participación en Comunidades Profesionales
- Mentoría y Desarrollo Profesional
- Actualización Constante sobre Amenazas y Tendencias
- Evaluación de Competencias Individuales
- Mejora Continua

5.3 Comunicación

La creación de un plan de comunicación completo es crucial para asegurar una compartición efectiva de información tanto dentro como fuera de la organización durante situaciones críticas o eventos que interrumpan el curso normal de las operaciones.

6. Implementación y Operación

6.1. Gestión del Cambio

En el contexto de la continuidad empresarial, la "gestión del cambio" se refiere al proceso que una organización implementa para manejar cambios internos que pueden afectar su capacidad para mantener operaciones críticas durante una interrupción o crisis. Para lograr esto, es necesario establecer normas y procedimientos para evaluar, planificar y llevar a cabo cambios en la organización de manera que no afecten su resiliencia y capacidad de respuesta ante situaciones adversas. La gestión del cambio es un medio para asegurarse de que los cambios internos se realicen de manera controlada y sin poner en peligro la continuidad del negocio (Instituto Nacional de Estándares y Tecnología , 2018).

6.2. Gestión de Incidentes y Crisis

La implementación de procedimientos detallados para gestionar situaciones inesperadas o emergencias que pueden interrumpir las operaciones normales de una organización. Esto incluye definir claramente los roles y responsabilidades de las personas que participan en la respuesta a incidentes y crisis. Los procedimientos establecen cómo se debe detectar, informar, evaluar y responder a situaciones que puedan afectar la continuidad del negocio para reducir el impacto y garantizar una recuperación rápida y efectiva. Esta gestión asegura que la organización esté lista para manejar operaciones críticas y lidiar con problemas imprevistos (ICS, 2010)

7. Evaluación del Desempeño

7.1. Monitoreo, Medición y Evaluación

Hay varias razones fundamentales por las que la evaluación del desempeño, que incluye auditorías internas, se realiza en el contexto de la continuidad del negocio. Al identificar áreas de mejora y vulnerabilidades, monitorear el desempeño del Sistema de Gestión de Continuidad del Negocio (SGCB), garantizar la preparación para crisis y permitir una comunicación transparente a las partes interesadas, permite la mejora continua. Además, ayuda a la organización a aprender y adaptarse mientras se esfuerza por mantener su resiliencia y capacidad de respuesta ante situaciones de interrupción (APC, 2017).

7.2. Auditorías Internas

La implementación de un programa destinado a evaluar si el Sistema de Gestión de Continuidad del Negocio (SGCB) cumple con los requisitos establecidos en el plan de continuidad y la norma ISO 22301. Estas auditorías se realizan para garantizar la conformidad con estándares, identificar incumplimientos, evaluar la eficacia de los planes, fomentar la mejora continua y asegurar la rendición de cuentas en la gestión de la continuidad de la empresa. Son esenciales para mantener y fortalecer la resiliencia y la capacidad de respuesta de la organización ante cualquier tipo de interrupción potencial (Bevan, 2019).

8. Mejora

8.1. Acciones Correctivas y Mejora Continua

El objetivo principal del proceso de Acciones Correctivas en la continuidad empresarial es identificar y corregir deficiencias y no conformidades en el Sistema de Gestión de Continuidad Empresarial (SGCB). Esto garantiza la eficacia del SGCB, la reducción de riesgos, el cumplimiento de las normas y la posibilidad de aprendizaje continuo. Además, la estrategia de "Mejora Continua" basada en comentarios y evaluaciones tiene como objetivo mejorar la resiliencia de la organización al aprender de las experiencias pasadas y adaptar el SGCB para enfrentar desafíos futuros con mayor eficacia y preparación (Inzeo, 2021).

9. Anexos y Documentación Adicional

Tabla 7. Evaluación de la Dependencia Tecnológica y sus Impactos en la Continuidad de Servicios (Teodoro y otros, 2016).

Escala	Valoración	Dependencia	Funcionalidad	Integridad, Funcionalidad y

				Disponibilidad
1	Muy Bajo	Ningún otro activo depende de este para la entrega de servicios	Activo con capacidades tecnológicas muy limitadas	La divulgación, modificación y no disponibilidad de su archivo de configuración puede afectar de forma insignificante la entrega de servicios
2	Bajo	Pocos activos dependen de este para la entrega de servicios	Activo con capacidades tecnológicas limitadas	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar en parte la entrega de servicios
3	Medio	Una mínima cantidad de activos dependen de este para la entrega de servicios	Activo con capacidades tecnológicas avanzadas	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar significativamente la entrega de servicios
4	Alto	Un número considerable de activos dependen de éste para la entrega de servicios	Activo con capacidades tecnológicas muy avanzadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar gravemente la entrega de servicios
5	Critico	Todos los activos dependen de éste para la entrega de servicios	Activo con capacidades tecnológicas de última generación	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar totalmente la entrega de servicios

Tabla 8. Resultados de Integridad, Funcionalidad y Disponibilidad.

Activo	**Divulgación**	**Modificación**	**Disponibilidad**
Computadoras de escritorio	3	3	4
Computadoras portátiles	3	3	4

Discos duros externos	2	3	3
Discos duros de servidores	4	4	5
Impresoras	2	2	3
Escáneres	2	2	3
Parlantes	1	1	2
Proyectores	2	2	3
Cámaras	3	3	4
Routers	4	4	5
Switches	4	4	5
Armario Rackeable	3	3	4
Firewalls	5	5	5
Antivirus	5	5	5
Puntos de Acceso (AP)	4	4	5
Cable estructurado	5	5	5
Fibra óptica	5	5	5
Instalación eléctrica	3	3	4
Sistema operativo Windows Server	4	4	5
Correo electrónico	4	4	5

8 DISCUSION DE LOS RESULTADOS

La evaluación de riesgos realizada con los activos del Gobierno Autónomo Descentralizado (GAD) Municipal de Mocache desempeñó un papel fundamental al proporcionar una sólida base para identificar y clasificar amenazas y vulnerabilidades. Siguiendo la norma ISO 27005, esta evaluación permitió una categorización sistemática de incidentes potenciales, brindando una comprensión detallada de los riesgos asociados con los activos tecnológicos del GAD. Este enfoque estructurado no solo ayudó a priorizar la atención en áreas críticas, sino que también facilitó la implementación de medidas específicas para mitigar los riesgos identificados, fortaleciendo así la postura de seguridad y la resiliencia del GAD Municipal ante posibles amenazas.

La clasificación de riesgos en función de su probabilidad e impacto en la organización representa un enfoque estratégico para la gestión de riesgos. La medición cuidadosa de estos factores permitió asignar prioridades de manera informada, focalizando la atención en los riesgos que podrían tener el mayor impacto en la continuidad del negocio del Gobierno Autónomo Descentralizado (GAD) Municipal. Este enfoque basado en la evaluación cualitativa no solo proporcionó una visión clara de los riesgos asociados, sino que también facilitó la toma de decisiones en la implementación de medidas preventivas y correctivas, especialmente dirigidas a garantizar la continuidad de los servicios crítico.

La identificación de servicios críticos marcó el inicio de una estrategia proactiva para la gestión de riesgos en el Gobierno Autónomo Descentralizado (GAD) Municipal. La elaboración de un plan de mitigación de riesgos integral demostró un enfoque diligente y preventivo. Este plan no solo abordaba la mitigación de riesgos ya identificados, sino que también incorporaba medidas preventivas destinadas a reducir la probabilidad de ocurrencia de posibles amenazas. Esta combinación de enfoques proporcionó una estructura sólida para

fortalecer la resiliencia del GAD Municipal frente a posibles perturbaciones, garantizando así la continuidad de los servicios críticos esenciales para la comunidad y la eficiencia operativa.

La investigación ha arrojado un conjunto de soluciones prácticas y específicas para mejorar la seguridad y la gestión de activos tecnológicos en el contexto del Gobierno Autónomo Descentralizado (GAD) Municipal de Mocache. La sección 4.1.6 se centra en el desarrollo de estrategias de mitigación, presentando un plan detallado para abordar áreas críticas de riesgo. Por ejemplo, en el control de cambios en discos duros, se proponen medidas preventivas, como la implementación de un proceso formalizado y la restricción de acceso, junto con estrategias de mitigación, como auditorías periódicas y el mantenimiento de registros detallados. De manera similar, se ofrecen soluciones para garantizar un almacenamiento seguro en discos duros, realizar pruebas de software en antivirus, configurar correctamente antivirus y abordar puntos únicos de falla en fibra óptica. Estas soluciones no solo abordan riesgos potenciales, sino que también establecen prácticas recomendadas para fortalecer la resiliencia y la seguridad de la infraestructura tecnológica del GAD Municipal.

9 CONCLUSIONES

El estudio de la norma ISO 22301 demuestra que la gestión de la continuidad del negocio es fundamental para el GAD municipal del cantón Mocache y en el entorno empresarial actual ya que su enfoque está dirigido tanto a pequeñas como medianas empresas. Esta norma no solo proporciona un marco sólido para enfrentar eventos disruptivos, sino que también promueve una cultura de mejora continua para un óptimo funcionamiento de los servicios tecnológicos permitiendo al GAD Municipal del cantón Mocache prepararse de manera efectiva para hacer frente a tales desafíos.

El estudio se centró en la gestión de la continuidad del negocio en los servicios tecnológicos del GAD Municipal del cantón Mocache, utilizando un enfoque cualitativo con entrevistas, revisión de documentos y observación. El análisis de los datos destacó patrones clave en la continuidad del negocio. Aunque el estudio se limitó a un solo caso y tuvo posibles limitaciones de datos, contribuye al conocimiento al proporcionar una comprensión detallada de la gestión de la continuidad del negocio en el sector público, particularmente en servicios tecnológicos en una región propensa a riesgos críticos.

La necesidad de un plan de continuidad de negocio basado en la norma ISO 22301 en los servicios tecnológicos del GAD Municipal del cantón Mocache se deriva de una falta evidente de preparación para enfrentar interrupciones significativas. La evaluación de riesgos destacó la crítica dependencia de activos como discos duros, firewalls, antivirus, cable estructurado y fibra óptica para la funcionalidad tecnológica del municipio. La clasificación de amenazas y vulnerabilidades según la norma ISO 27005 identificó áreas críticas que demandan atención inmediata. Las soluciones propuestas, que abarcan medidas preventivas y de mitigación para activos fundamentales, establecen un enfoque integral para fortalecer la

resiliencia del GAD Municipal, garantizando la disponibilidad continua de servicios y mejorando su preparación ante posibles crisis.

10 RECOMENDACIONES

Dada la importancia de la gestión de la continuidad del negocio, según lo destacado en el estudio de la norma ISO 22301, se recomienda encarecidamente que el GAD municipal del cantón Mocache considere la implementación de esta norma en sus servicios tecnológicos como una parte integral de su estrategia para asegurar la continuidad de las operaciones y la resiliencia en el entorno empresarial actual.

Se recomienda ampliar el alcance de la investigación, desarrollar planes específicos de continuidad del negocio para servicios tecnológicos críticos, invertir en formación y concienciación, fomentar la colaboración interdepartamental, actualizar políticas y procedimientos, considerar tecnologías emergentes y establecer un sistema de seguimiento y revisión constante. Estas acciones permitirán fortalecer la resiliencia de los servicios tecnológicos en el sector público y mejorar la preparación para enfrentar riesgos críticos en una región propensa a tales desafíos.

Es esencial que las organizaciones implementen planes integrales de continuidad de negocio para proteger la seguridad y disponibilidad de sistemas críticos de TI. Esto implica invertir en la formación del personal de TI, establecer sólidos procedimientos de respuesta a incidentes y realizar pruebas regulares para asegurar la efectividad de los planes. Además, es crucial mantener los planes actualizados para adaptarse a cambios tecnológicos y amenazas, fortaleciendo la capacidad de mantener operaciones y resguardar activos en un entorno empresarial en constante cambio.

11 BIBLIOGRAFÍA

Bevan, T. (2019). *ISO 22301:2019 GUÍA DE IMPLANTACIÓN DE LA CONTINUIDAD DE NEGOCIO.* nqa GLOBAL CERTIFICATION BODY. https://doi.org/https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

AENOR. (31 de Enero de 2018). *ISO 27005 Gestión de riesgo de la seguridad de la información.* AENOR. Seguridad de la Información: https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacionISO2027005eselesCA1ndarinternacionalquese,seguridaddelainformaciC3B3ndefinidosenISO2027001.

Ambit. (10 de Noviembre de 2021). *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

AmericanExpress. (26 de Mayo de 2022). *Implementar un sistema de gestión de calidad*. https://www.americanexpress.com/es-mx/negocios/trends-and-insights/articles/beneficios-de-implementar-un-sistema-de-gestion-de-calidad/

APC, A. (2017). *MANUAL DE AUDITORÍAS INTERNAS APC COLOMBIA.* APC. https://doi.org/https://www.apccolombia.gov.co/sites/default/files/archivos_usuario/2017/c-ot-001manual_de_auditoria_internav3.pdf

GlobalSuite Solutions. (15 de Mayo de 2023). *¿Qué es la norma ISO 22301 y para qué sirve?* https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-22301-y-para-que-sirve/

IBM Services. (20 de Noviembre de 2020). *Adaptarse y responder a los riesgos con un plan de continuidad de negocio (BCP).* https://www.ibm.com/es-es/services/business-continuity/plan

ICS, I. (2010). *Introducción al Sistema de Comando de Incidentes (ICS 100).* Profepa . https://doi.org/http://www.profepa.gob.mx/innovaportal/file/212/1/ics_-_introduccion_al_sistema_de_comandos_de_incidentes_-_g.i..pdf

Incibe. (16 de Septiembre de 2022). *Fases de un Plan de Continuidad de Negocio*. https://www.incibe.es/empresas/blog/fases-plan-continuidad-negocio

INCIBE, I. (2019). *PLAN DE CONTIGENCIA Y CONTINUEDAD DE NEGOCIO.* Incibe. https://doi.org/https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Instituto Nacional de Estándares y Tecnología . (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas* . Nistgov. https://doi.org/https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

Inzeo, N. (2021). *Maneras de Mejorar las Acciones Correctivas y Preventivas (CAPA).* inspectorio.com.

López , J. (2019). *El compromiso de la alta dirección en la certificación de sisema de gestión* . visionindustrial.

Martins, J. (16 de Agosto de 2022). *Qué es un plan de contingencia y cómo crear uno en 8 pasos para evitar riesgos*. https://asana.com/es/resources/contingency-plan

NQA. (02 de Octubre de 2022). *¿Qué es la ISO 22301?* ISO 22301: https://www.nqa.com/es-pe/certification/standards/iso-22301

Rodriguez , C. (2020). *LA IMPORTANCIA DE UN PLAN DE CONTINUIDAD DEL NEGOCIO.* Repository. https://doi.org/http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9547/La%20importanciadeunplande.pdf?sequence=1&isAllowed=y

SFAI. (07 de Octubre de 2022). *¿Qué es la ISO 22301? La norma internacional de gestión de continuidad de negocio*. https://www.sfai.es/blog/que-es-la-iso-22301-la-norma-internacional-de-gestion-de-continuidad-de-negocio/

Simmerman, P. (01 de Diciembre de 2022). *¿Qué es BCM?* https://www.adl-logistica.org/que-es-bcm-gestion-de-continuidad-del-negocio-iso-223012019-sobrevivir-a-acontecimientos-extraordinarios

Teodoro, J., Gonzáles , G., Campi , I., España, Á., & España , Á. (2016). *Análisis y Evaluación del Riesgo de la Información: Caso de Estudio Universidad Técnica de Babahoyo.* Dialnet.

Torres, D. (10 de Enero de 2023). *¿Qué es el plan de emergencia de una empresa y cómo crearlo?* https://blog.hubspot.es/sales/plan-emergencia-empresa

12 ANEXOS

ANEXO 1. Entrevista al personal encargado en los servicios tecnológicos del GAD municipal de Mocache

1. ¿Puede describir las medidas de seguridad implementadas para proteger los datos sensibles del GAD Municipal del cantón Mocache?
2. ¿Qué nivel de preparación tienen para contrarrestar las últimas amenazas cibernéticas y asegurar de que se implementen medidas de seguridad actualizadas y efectivas?
3. ¿Existe una correcta integración de sistemas y bases de datos en el municipio para garantizar la coherencia de la información?
4. ¿Están preparados para que los servicios tecnológicos sean escalables y puedan adaptarse a un aumento en la demanda de usuarios y datos?
5. ¿Consideran que los servicios tecnológicos cumplen con las regulaciones y estándares específicos?
6. ¿Garantiza que los servicios tecnológicos sean accesibles para todos los ciudadanos, incluyendo aquellos con discapacidades?
7. ¿En qué escala se establecen medidas y protocolos para garantizar la disponibilidad continua de los servicios críticos?
8. ¿Con que frecuencia se gestiona y planifica el mantenimiento regular y las actualizaciones de los sistemas tecnológicos?

9. ¿En qué medida se realizan enfoques innovadores o estratégicos para ofrecer soluciones tecnológicas efectivas dentro de las restricciones presupuestarias?
10. ¿Qué nivel de preparación se tiene para el desarrollo de estrategias para abordar vulnerabilidades de seguridad y mantener el funcionamiento óptimo de los sistemas con eficacia?

ANEXO 2. Entrevista

Tabla 9. Evaluación de la Preparación y Seguridad de los Servicios Tecnológicos en el GAD Municipal del Cantón Mocache.

Preguntas semi estructuradas	Nulo	Bajo	Medio	Satisfactorio	Alto
¿Puede describir las medidas de seguridad implementadas para proteger los datos sensibles del GAD Municipal del cantón Mocache?				X	
¿Qué nivel de preparación tienen para contrarrestar las últimas amenazas cibernéticas y asegurar de que se implementen medidas de seguridad actualizadas y efectivas?			X		
¿Existe una correcta integración de sistemas y bases de datos en el municipio para garantizar la coherencia de la información?			X		
¿Están preparados para que los servicios tecnológicos sean escalables y puedan adaptarse a un aumento en la demanda de usuarios y datos?		X			
¿Consideran que los servicios tecnológicos cumplen con las regulaciones y estándares		X			

específicos?					
¿Garantiza que los servicios tecnológicos sean accesibles para todos los ciudadanos, incluyendo aquellos con discapacidades?			X		
¿En qué escala se establecen medidas y protocolos para garantizar la disponibilidad continua de los servicios críticos?	X				
¿Con que frecuencia se gestiona y planifica el mantenimiento regular y las actualizaciones de los sistemas tecnológicos?				X	
¿En qué medida se realizan enfoques innovadores o estratégicos para ofrecer soluciones tecnológicas efectivas dentro de las restricciones presupuestarias?		X			
¿Qué nivel de preparación se tiene para el desarrollo de estrategias para abordar vulnerabilidades de seguridad y mantener el funcionamiento óptimo de los sistemas con eficacia?			X		

ANEXO 3. Observación participante

Tabla 10. Presentación de ficha de Observación.

Ficha de Observación	
Elaborado por	
Ciudad	

Empresa		
Tiempo	**Observado**	
1 día	Medidas de seguridad implementadas para proteger los datos sensibles del GAD de Mocache.	
1 día	Nivel de preparación para contrarrestar amenazas cibernéticas y asegurar medidas de seguridad actualizadas y efectivas.	
1 día	Integración de sistemas y bases de datos para garantizar la coherencia de la información en el municipio	
1 día	Preparación para la escalabilidad de los servicios tecnológicos y adaptación a un aumento en la demanda de usuarios y datos	
1 día	Cumplimiento de regulaciones y estándares en los servicios tecnológico	
1 día	Accesibilidad de los servicios tecnológicos para ciudadanos, incluyendo aquellos con discapacidades	
1 día	Establecimiento de medidas y protocolos para garantizar la disponibilidad continua de los servicios críticos	
1 día	Gestión y planificación del mantenimiento regular y las	

	actualizaciones de los sistemas tecnológicos	
1 día	Enfoques innovadores o estratégicos para ofrecer soluciones tecnológicas efectivas dentro de las restricciones presupuestarias	
1 día	Nivel de preparación para el desarrollo de estrategias de seguridad y mantenimiento efectivo de los sistemas	
Palabras clave		

ANEXO 4. Solicitud al decano para la elaboración del oficio de permiso a la autoridad de la empresa

Babahoyo, 16 de agosto del 2023

Magister
Eduardo Galeas Guijarro
DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA
En su despacho.

De mis consideraciones:

Yo: **NAVARRETE YEPEZ OVER STEVEN**, con cédula de identidad 1205486085, estudiante de la carrera de Ingeniería Sistemas de Información matriculado en el proceso de titulación periodo Abril 2023 – Septiembre 2023, le solicito a usted de la manera más comedida se sirva autorizar a quien corresponda se proceda a elaborar un oficio dirigido a Jenny Domínguez representante legal de la empresa GAD Municipal del cantón Mocache requiriendo el permiso respectivo para realizar mi Caso de estudio denominado Análisis de la continuidad del negocio basado en ISO 22301 y los servicios tecnológicos del GAD Municipal de Mocache, el cual es requisito indispensable para poder titularme.

Esperando una respuesta favorable quedo de usted muy agradecido(a).

Del señor Decano muy atentamente

Over Steven Navarrete Yépez
1205486085

RECIBIDO
UNIVERSIDAD TECNICA DE BABAHOYO
SECRETARIA FAFI
FECHA: 16-08-23 HORA: 14:50

ANEXO 5. Oficio de permiso a la autoridad de la empresa

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

2707

Babahoyo, 16 de agosto del 2023
D-FAFI-UTB-00544-2023

Señora.
Jenny Domínguez.
REPRESENTANTE LEGAL DE LA EMPRESA GAD MUNICIPAL DEL CANTÓN MOCACHE.
Ciudad. –

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El señor **OVER STEVEN NAVARRETE YEPEZ** con cédula de identidad No. **1205486085** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo junio – octubre 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional universitario de tercer nivel como Ingeniero en Sistemas de Información, solicita por intermedio del Decanato de esta Facultad el debido permiso para poder culminar su proyecto, el cual titula: **"ANÁLISIS DE LA CONTINUIDAD DEL NEGOCIO BASADO EN ISO 22301 Y LOS SERVICIOS TECNOLÓGICOS DEL GAD MUNICIPAL DE MOCACHE".**

Atentamente,

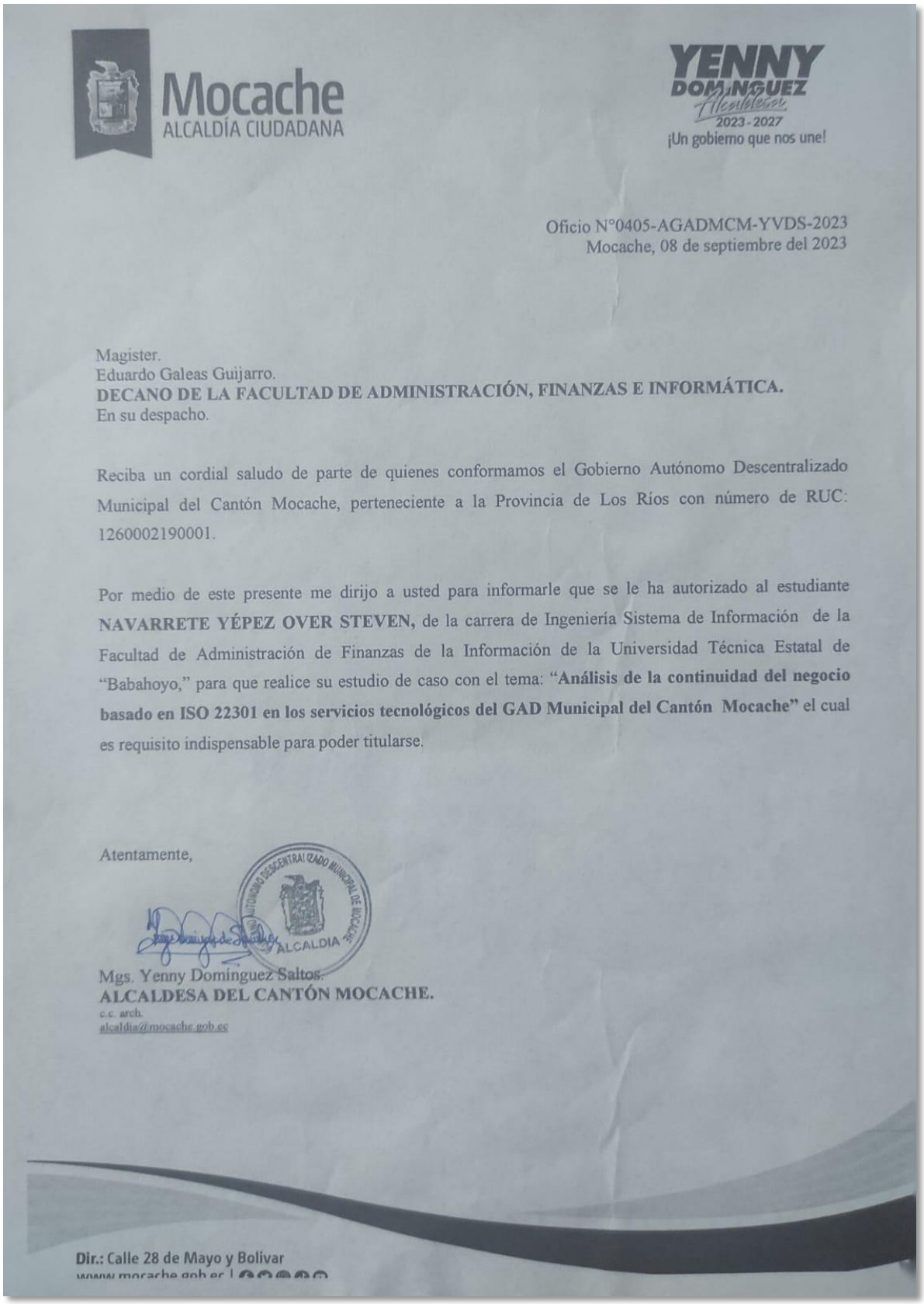
Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO
c.c: Archivo

UNIVERSIDAD TÉCNICA DE BABAHOYO
FAC. ADMINISTRACIÓN FINANZAS E INFORMÁTICA
DECANATO

GAD. M. DEL CANTÓN MOCACHE
SECRETARÍA GENERAL
RECIBIDO
28 AGO 2023 8:46
HORA
FIRMA AUTORIZADA

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Ing. Marilyn Coloma Aguilar	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

ANEXO 6. Carta de Autorización emitida por la empresa.



Mocache
ALCALDÍA CIUDADANA

YENNY DOMÍNGUEZ
Alcaldesa
2023 - 2027
¡Un gobierno que nos une!

Oficio N°0405-AGADMCM-YVDS-2023
Mocache, 08 de septiembre del 2023

Magister.
Eduardo Galeas Guijarro.
DECANO DE LA FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.
En su despacho.

Reciba un cordial saludo de parte de quienes conformamos el Gobierno Autónomo Descentralizado Municipal del Cantón Mocache, perteneciente a la Provincia de Los Ríos con número de RUC: 1260002190001.

Por medio de este presente me dirijo a usted para informarle que se le ha autorizado al estudiante **NAVARRETE YÉPEZ OVER STEVEN,** de la carrera de Ingeniería Sistema de Información de la Facultad de Administración de Finanzas de la Información de la Universidad Técnica Estatal de "Babahoyo," para que realice su estudio de caso con el tema: **"Análisis de la continuidad del negocio basado en ISO 22301 en los servicios tecnológicos del GAD Municipal del Cantón Mocache"** el cual es requisito indispensable para poder titularse.

Atentamente,

GAD AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE MOCACHE ALCALDIA

Mgs. Yenny Dominguez Saltos.
ALCALDESA DEL CANTÓN MOCACHE.
c.c. arch.
alcaldia@mocache.gob.ec

Dir.: Calle 28 de Mayo y Bolivar
www.mocache.gob.ec