UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Plan de continuidad del negocio de los activos tecnológicos hardware y software"

Trabajo de Integración Curricular previo a la obtención del título de Ingenieras en Ciencias de la Computación

AUTORAS: Hurtado Rodríguez Jazmín Estefanía

Paspuel Pusda Lupe Fernanda

TUTOR: Ing. Guano Cárdenas Carlitos Alberto Msc.

Tulcán, 2023

CERTIFICADO DEL TUTOR

Certifico que las estudiantes Hurtado Rodríguez Jazmín Estefanía y Paspuel Pusda Lupe Fernanda con el número de cédula 0401900485 y 0450026323 respectivamente han desarrollado el Trabajo de Integración Curricular: "Plan de Continuidad del negocio de los activos tecnológicos hardware y software"

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva.

_____

Msc. Guano Cárdenas Carlitos Alberto

TUTOR

Tulcán, marzo del 2023

AUTORÍA DE TRABAJO

El presente Trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingenieras en la carrera de Computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Nosotras, Hurtado Rodríguez Jazmín Estefanía y Paspuel Pusda Lupe Fernanda con cédula de identidad número 0401900485 y 0450026323 respectivamente declaramos que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que hemos llegado son de nuestra absoluta responsabilidad.

Hurtado Rodríguez Jazmín Estefanía	Paspuel Pusda Lupe Fernanda
AUTORA	**AUTORA**

Tulcán, marzo del 2023

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Nosotras Hurtado Rodríguez Jazmín Estefanía y Paspuel Pusda Lupe Fernanda declaramos ser autoras de los criterios emitidos en el Trabajo de Integración Curricular: "Plan de continuidad del negocio de los activos tecnológicos hardware y software" y exime expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.

Hurtado Rodríguez Jazmín Estefanía	Paspuel Pusda Lupe Fernanda
AUTORA	**AUTORA**

Tulcán, marzo del 2023

AGRADECIMIENTO

Todo esfuerzo tiene su recompensa, "si luchas, puedes perder; si no luchas, estás perdido." Mago More

Gracias a Dios por guiarnos en este camino para batallar por nuestros sueños con entendimiento, fortaleza y valentía.

Agradecemos a la Universidad Politécnica Estatal del Carchi por extendernos una educación de calidad para la formación como profesionales y a los docentes de la carrera de Computación en especial a Msc. Marco Yandún, Msc. Jorge Miranda, Msc. Samuel Lascano, Msc. Georgina Arcos quienes han compartido su dedicación y conocimientos con perseverancia.

Nuestro agradecimiento, muy sincero a nuestro tutor de tesis el Msc. Carlitos Guano, quien ha sido una guía de orientación y conocimiento para el cumplimiento de nuestra investigación.

Al Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar, de manera especial al Ing. Andrés Villarruel, jefe de la Unidad de Tecnología y Comunicación (TIC), por brindarnos la ayuda correspondiente para el desarrollo y supervisión del presente proyecto de titulación.

A nuestros padres, quienes nos han apoyado de manera incondicional, con sus valores y ejemplo.

A nuestros hermanos y hermanas que nos brindaron motivación, apoyo y compañía en los distintos momentos que se atravesó en el proceso de formación académica.

Jazmín Estefanía Hurtado Rodríguez

Lupe Fernanda Paspuel Pusda

DEDICATORIA

A Dios por permitirme continuar y acompañarme cada día, ser mi fortaleza en tiempos de caos y felicidad en momentos maravillosas de mi vida.

A mis padres Jaime y Marco, que siempre me han apoyado incondicionalmente y han luchado por mí en toda adversidad. Son mi mayor admiración y motivación para seguir adelante. Gracias por su amor.

A mi grande amor mi madre Sonia que es el pilar fundamental y mis fuerzas de salir adelante.

A mis hermanos, a mis abuelitos y toda mi familia por las palabras de ánimo para continuar.

Jazmín Estefanía Hurtado Rodríguez

Quiero dedicar el presente proyecto a Dios y a la virgen María quienes han sido mi guía y fortaleza a lo largo de mi vida. A mi padre Felipe Paspuel y en especial a mi madre María Pusda quien ha estado conmigo en todo el proceso de mis estudios de nivel superior con su cariño, esfuerzo, dedicación, amor, apoyo incondicional y sacrificio que me han ayudado a ser una mejor persona con valores que me han inculcado desde pequeña.

A mi familia y amigos, por motivarme y apoyarme en cada momento con sus palabras de aliento y fortaleciéndome de cierta manera en la etapa de estudios universitarios.

Lupe Fernanda Paspuel Pusda

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El Plan de Continuidad del Negocio (BCP) planteado para la Unidad de Tecnología y Comunicación (TIC) del Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar, está orientado en detallar la forma en la que la institución se mantenga disponible durante las interrupciones o amenazas. El Plan de continuidad del negocio es un instrumento de referencia con estrategias proyectadas y establecidas de los activos tecnológicos que permiten enfrentar a un incidente en el menor tiempo posible sin afectación a la organización. En cuanto, es importante para la investigación conocer la situación actual del municipio sobre su infraestructura tecnológica, roles del personal y servicios, para locual se realizó el levantamiento de información de la institución. Por lo tanto, la factibilidad del apoyo personal directivo y el jefe de la Unidad de TIC de la institución es sustancial para la aplicación de instrumentos de recolección de información. Al igual se llevó el análisis de impacto del negocio BIA (Business Impact Analysis) para identificar procesos y activos tecnológicos críticos de la institución que deben tener prioridad para la recuperación dentro de tiempo máximo tolerable. Posteriormente, se realizó el análisis de riesgos de activos críticos de la Unidad de TIC del GAD Municipal del Cantón Bolívar, utilizando metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). De acuerdo con la fase de valoración de riesgos, se establecieron estrategias y se diseñó el Plan de continuidad del negocio considerando él antes, durante y después de un escenario, tomando como referencia la norma internacional ISO 22301:2019. Finalmente se definió: comité de crisis, plan de prueba, así como plan de mantenimiento y capacitación.

Palabras clave: Análisis de riesgos, BIA, Cláusulas de norma ISO 22301:2019, Continuidad del negocio, tiempos de recuperación, amenazas, riesgos, paralización.

ABSTRACT

The Business Continuity Plan (BCP) proposed for the Technology and Communication Unit (ICT) of the Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar is oriented to detail how the institution remains available during interruptions or threats. The BCP is a reference instrumentthat consists of projected and established strategies for technological assets that allow an organization to deal with an incident as quickly as possible without affecting the organization. In this case, the investigation needs toknow the current situation of the municipality in terms of its technological infrastructure, staff roles, and services, for which the information of the institution was gathered. Accordingly, the feasibility of the support of management personnel and the head of the ICT Unit of the institution is substantial for the application of information collection instruments. Moreover, the Business Impact Analysis (BIA) was conducted to identify critical technological assets of the institution that must be recovered within the maximum acceptable timeframe. Subsequently, the risk analysis of critical assets of the ICT Unit GAD was performed using the Methodology for Information Systems Risk Analysis and Management (MAGERIT). Likewise, the risk assessment phase helped establish strategies and develop the Business Continuity Plan, considering it before, during, and after a scenario, taking the international standard ISO 22301:2019 as a reference. Finally, it was defined: as a crisis committee, test plan, maintenance and training.

Keywords: Risk analysis, BIA, ISO 22301:2019 clauses, Business continuity, recovery timeframe, threats, risks, stoppage.

INTRODUCCIÓN

Actualmente el plan de continuidad del negocio. Según Disaster Recovery Journal (2022) menciona que Continuidad del Negocio (CN) es la disciplina clave que permite crear y mejorar la resiliencia de las organizaciones. Originalmente, el Plan de Continuidad era un gran documento informativo que se enfocaba en la respuesta, pero también en por qué esa respuesta era importante. Por lo tanto, el plan incluye las principales amenazas y riesgos que enfrenta la organización, así como las prioridades de recuperación.

> También define las estrategias de recuperación de los roles requeridos para estas respuestas, los protocolos operativos y las responsabilidades para los planes de mantenimiento, capacitación y prueba. Ahora el plan ha cambiado de rumbo y se enfoca principalmente en responder a eventos, es decir, ya no está orientado a una gran cantidad de información, sino que el contenido es muy ligero y fácil de recordar y mover. (p. 1).

La continuidad de negocio es la capacidad que tiene una organización para continuar con la entrega tanto de productos como de servicios en los niveles previamente definidos y aceptables una vez que se haya presentado un incidente disruptivo. Esta definición se establece en la norma ISO 22301, es un estándar internacional de la Organización Internacional de Normalización (ISO).

Para este proyecto se toma en cuenta varios aspectos que fueron abarcados en este documento. El presente trabajo tiene como finalidad el desarrollo de un plan de continuidad del negocio de los activos tecnológicos hardware y software. El cual debe regirse a las Normas de Control Interno de la Contraloría General del Estado (NCICGE) que cada institución debe contar para ello se utiliza la norma internacional ISO 22301:2019((Sistema de Gestión de Continuidad del Negocio), la cual está orientada a salvaguardar los principales activos tecnológicos y procesos críticos) y las cláusulas de esta norma las cuales nos permiten trabajar con la continuidad del negocio del área de TIC del Municipio de Bolívar, Provincia del Carchi.

Algunos trabajos encontrados hacen referencia al plan de continuidad del negocio que debe tener toda institución, sea esta pública o privada para el manejo de los

activos en caso de algún problema como menciona, incluso existen varios marcos de referencia y metodología, pero el plan no tiene una secuencia establecida.

Con el objetivo de Desarrollar un Plan de continuidad del negocio de los activos tecnológicos hardware y software para la Unidad de Tecnología y Comunicación TIC del GAD Municipal del Cantón Bolívar, se utiliza un enfoque mixto apoyándose a los tipos de investigación. El trabajo está orientado a la idea a defender: El Plan de continuidad de negocio del área de Tecnología de Información y Comunicación de Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar, ayudara a manejar incidentes y desastres para el fortalecimiento de la disponibilidad de los activos tecnológicos hardware y software.

El trabajo cuenta con 7 capítulos organizados para respaldar el plan, los cuales se mencionan a continuación:

En el primer capítulo: el problema hace referencia a la causa y efecto de lo que está presente la Unidad de TIC del GAD Municipal del Cantón Bolívar, en la justificación está el por qué este proyecto es factible y los beneficiarios directos e indirectos, con sus respectivos objetivos y preguntas de investigación.

El segundo capítulo comprende la fundamentación teórica la cual nos permite apoyarnos, aquí se específica el tema del plan de continuidad de negocio juntamente con referencia bibliográfica.

Tercer Capítulo La metodología que se va a utilizar es el enfoque mixto, con tipos de investigación descriptiva, documental, acción, etc. Juntamente con varios instrumentos que permiten realizar el levantamiento de información de los activos tecnológicos hardware y software.

Para finalizar Cuarto Capítulo resultados y discusión se muestra los resultados obtenidos durante el trabajo de investigación y el desarrollo de la propuesta con sus respectivas fases.

Los capítulos Quinto, sexto y séptimo conclusiones y recomendaciones, referencias bibliográficas, anexos en donde se evidencia la documentación del plan de continuidad del negocio.

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las empresas e instituciones han evolucionado a través de constantes cambios principalmente, infraestructura tecnológica que han beneficiado al desarrollo, sin embargo, todas las empresas se enfrentan a situaciones de interrupciones de las actividades o servicios, debido a desastres naturales, ciberataques o error humano, entre otros. En la mayoría de grandes, medianas y pequeñas empresas, se evidencia la jerarquía e importancia de la existencia de un plan de continuidad del negocio (BCP) el cual garantizan responder a cualquier riesgo.

En Estados Unidos, las entidades públicas y privadas utilizan portales de servicios tecnológicos que cuentan con un plan de continuidad del negocio permitiendo anticiparse, en cuyo caso de detectar amenazas, riesgos y vulnerabilidades de los activos tecnológicos software y hardware puesto que es un país con mayor número de ataques cibernéticos dirigido a los estados gubernamentales y empresariales.

En Ecuador según Ortiz (2019). Las páginas web de entidades estatales fueron blanco de ataques por denegación de servicio por lo cual existió denuncias por parte de los clientes, ocasionando saturación a los sistemas informáticos y la operatividad de la infraestructura tecnológica.

En la Provincia de Pichincha, los ataques cibernéticos se han incrementado ocasionando pérdidas económicas y afectando a los servicios tecnológicos que presta los portales web de la Presidencia, secretaría de asuntos internos Banco Central (Patiño,2019).

Al igual, el Servicio de Contratación Pública del Estado se vio afectado directamente por las vulnerabilidades de las plataformas y no se contaba con un plan de continuidad de negocio para los sistemas de información y de la infraestructura tecnológica, evidenciando la paralización de varios servicios (Vásquez,2018).

Los ataques más concurrentes fueron en el año 2019, por lo cual el estado ecuatoriano para mantener software y hardware monitoreados pidió reforzar medidas de ciberseguridad y un plan de continuidad para actuar frente a una emergencia evitando pérdidas o interrupción de los servicios tecnológicos.

Las tecnologías de información están sujetas a diferentes vulnerabilidades, riesgos y amenazas las cuales pueden ser causadas por el humano o razones de carácter natural pueden ser identificadas,

En el caso de la Provincia del Carchi a partir del mes de julio del 2022 se ha evidenciado movimientos telúricos, los cuales afectado directamente a este territorio. Las vulnerabilidades son mayores frente a este problema provocando un negativo proceso de disponibilidad de diferentes instituciones.

El Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Bolívar-Carchi ha incremento el uso de la tecnología, cuenta con una amplia infraestructura, el cual está compuesta hardware y software que alojan información de los procesos que realiza la institución, al igual, servicios de procesos operativos tales como: Registro de la Propiedad, Impuestos prediales, permisos de uso y ocupación del suelo para realizar actividades e impuestos patente municipal, actualización catastral entre otras actividades.

En esta entidad pública se ha evidenciado la paralización de los servicios informáticos internos y externos originando molestias de los usuarios, servidores y directivos municipales, limitando al desarrollo de las actividades, incidiendo en pérdidas de tiempo, problemas económicos e información desactualizada.

Estas razones antes mencionadas, se debe que la Unidad de Tecnología y Comunicación (TIC) de GAD Municipal cuenta con planes de continuidad del negocio indefinidos y no se encuentran medidas, procedimientos o estrategias específicas, que garantice la recuperación pronta para la continuidad de las actividades ante riesgos y amenazas que pueden ser provocadas de forma directa como indirecta.

1.2. FORMULACIÓN DEL PROBLEMA

El actual plan de continuidad del negocio del área de la Unidad de Tecnología y Comunicación (TIC) es inadecuado con las necesidades de esta, lo que provoca un

deficiente manejo de incidentes y desastres dejando en riesgo la disponibilidad de los activos tecnológicos hardware y software del GAD Municipal del Cantón Bolívar 2021– 2022.

1.3. JUSTIFICACIÓN

El presente proyecto de investigación pretende por medio de un Plan de Continuidad del Negocio asegurar la disponibilidad de los activos tecnológicos hardware y software del GAD Municipal, cuando repentinamente ocurre incidentes inesperados (desastres naturales, accidentales, intencionales y tecnológicos). En el Plan se tomará en cuenta la Norma ISO 22301:2019(Sistema de Gestión de Continuidad del Negocio), la cual está orientada a salvaguardar los principales activos tecnológicos y procesos críticos de la Unidad de TIC, pretendiendo no paralizar el desarrollo de las actividades y los servicios que presta el GAD Municipal del Cantón Bolívar y se encuentren preparados ante cualquier incidente mediante estrategias que asegure la restauración de hardware y software en el menor tiempo posible de forma rápida, eficiente y oportuna certificando la disponibilidad, integridad y confidencialidad de la información.

Es decir, de esta manera el GAD, ejecutará acciones o medidas que se encuentren planificadas en el Plan de continuidad del negocio afrontando ante un posible riesgo o vulnerabilidad en el menor tiempo posible.

Este proyecto es factible de desarrollar puesto que dispone de la autorización del alcalde del Municipio de Bolívar. Del mismo modo, se cuenta con la disponibilidad de acceso de información requerida de la infraestructura, activos tecnológicos hardware, software y servicios por parte de la Unidad de Tecnología de Información y Comunicación. Además, es económicamente factible debido que el proyecto es asumido por las investigadoras.

Los beneficiarios directos del desarrollo de la investigación es la Unidad de Tecnología y Comunicación (TIC), de igual manera los beneficiarios indirectos es la ciudadanía de Cantón Bolívar.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

- Desarrollar el Plan de continuidad del negocio de los activos tecnológicos hardware y software basado en la norma ISO 22301:2019 para la Unidad de TIC del GAD Municipal del Cantón Bolívar, mediante estrategias de prevención, contención, recuperación y transferencia ante incidentes, asegurando la disponibilidad de los servicios.

1.4.2. Objetivos Específicos

- Fundamentar bibliográficamente la investigación, a través de la utilización de fuentes primarias o secundarias de medios online y físicos que sustente teóricamente la investigación.
- Realizar el análisis de impacto del negocio (BIA) para identificar los procesos críticos ante la posibilidad de un desastre de modo que interrumpa la disponibilidad de los activos tecnológicos hardware y software para mitigar el impacto recibido a la Unidad de Tecnología y Comunicación TIC.
- Analizar los riesgos, vulnerabilidades y amenazas que están expuestos los activos tecnológicos hardware y software de la institución para la determinación de estrategias de recuperación mediante la metodología MAGERIT.
- Generar una tabla de la aplicación de la pre y post propuesta para evidenciar el nivel de madurez de la Unidad TIC del GAD Municipal del Cantón Bolívar.

1.4.3. Preguntas de Investigación

- ¿De qué manera la fundamentación bibliográfica a través de la utilización de fuentes primarias o secundarias de medios online y físicos ayudará a sustentar teóricamente la investigación?

- ¿El análisis de impacto del negocio (BIA) permite identificar los procesos críticos ante la posibilidad de un desastre de modo que interrumpa la disponibilidad de los activos tecnológicos hardware y software para mitigar el impacto recibido a la Unidad de Tecnología y Comunicación TIC?

- ¿La aplicación de la metodología MAGERIT en el Análisis de los riesgos, vulnerabilidades y amenazas que están expuestos los activos tecnológicos hardware y software de la institución, permite la determinación de estrategias de recuperación?

- ¿Mediante la aplicación de una pre y post propuesta se podrá evidenciar el nivel de madurez de la Unidad TIC del GAD Municipal del Cantón Bolívar?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

En el presente proyecto se detallan diferentes investigaciones que se han realizado en referente a la implementación del uso de un plan de continuidad de negocio y el impacto positivo que han tenido.

El Plan de continuidad del negocio es muy importante debido a que cada organización se encuentra disponible durante o después de escenarios de emergencia o actividades independientes del origen del problema, para ello se debe identificar, evaluar y controlar los riesgos: Para evitar o reducir impactos, interrupciones, imagen de la organización y disminuyendo pérdidas financieras (Díaz, 2022). Se hace énfasis en la metodología utilizada la cual recomienda utilizar la norma ISO 22301, juntamente con la metodología MAGERIT, que sirven como instrumento de evaluación inicial y final para determinar los parámetros internos y externos.

Pincay (2021) en su trabajo de titulación "Desarrollo de un Plan de Continuidad del Negocio Basado en la norma ISO 22301, en la Empresa "CONSTRUPROYECS.A.", la cual menciona que el desarrollo del plan se debe tomar en cuenta el levantamiento de información, y el uso correcto de la metodología en este caso la norma ISO 22301:2019 la cual detalla el análisis de riesgos, impacto del negocio, permitiendo dar solución frente a eventos inesperados y seguir con la continuidad de los procesos.

Araujo (2019) en su tesis "Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador" menciona que: El presente trabajo de investigación aborda la importancia de desarrollar un plan de continuidad del negocio en la Agencia Nacional de Contrataciones Públicas, con el objetivo principal de identificar los principales procesos técnicos, riesgos e interacciones y amenazas que enfrentan, para desarrollar un plan de continuidad del negocio basado en la situación real de la entidad.

Debe existir una gestión de riesgos suficiente y una visión clara para retomar las operaciones de ingeniería ante peligros específicos que puedan presentarse como la presencia de desastres naturales como terremotos, sismos, incendios, inundaciones o delincuencia, instituciones que afecten el funcionamiento deseado de la compañía (p. 14).

En la tesis anterior menciona la importancia de tener un plan de continuidad del negocio identificando amenazas, vulnerabilidades y así adaptarse eficientemente para generar el plan y estar preparados y hace uso del estándar 22301 que contribuye a la seguridad y resiliencia en los sistemas de continuidad de negocio.

Rázuri (2019), en su tesis "Desarrollo de un Sistema de Gestión de Continuidad de Negocio en una entidad financiera, basado en la ISO 22301" menciona que: Uno de los conceptos clave relacionados con la continuidad del negocio es el de recuperación ante desastres. Este concepto fue creado en los años setenta. En ese momento, el centro de datos se consideraba un "punto único de falla" (SPFO) en el sentido de que se desarrollaron diferentes servicios a través de los cuales diferentes proveedores brindaban acceso común al entorno de recuperación de respaldo de la computadora, llamado centro de respaldo. Durante las décadas de 1980 y 1990, este servicio se hizo cada vez más popular en el mercado, lo que indica que mientras más dependientes de la tecnología se volvían las organizaciones, mayor era el impacto, siempre y cuando no contaban con la infraestructura y los sistemas de acceso a la información. En este contexto, la compañía analiza que las disrupciones que afectan a las tecnologías de la información pueden provocar daños importantes por una dependencia excesiva de las mismas (p.9).

En esta tesis hace referencia a la continuidad del negocio enfocada a la redención de información ante calamidades, se nos comenta que a partir de los años ochenta y noventa la recuperación informática era conocida como centro de respaldos, a partir de esta situación es cuando las empresas analizan que las interrupciones de sistemas generan pérdidas significativas.

Vallery (2019) en su tesis "Awareness and importance of developing business continuity plans for disaster risks by companies at bayhead harbour, durban, South África" menciona que: El carácter disciplinario integrado de esta investigación ha hecho que no exista un modelo de BCP que exista, que podría resumir completamente la idea de este estudio. Diferente, por lo tanto, se seleccionan

modelos teóricos de BCP para explicar el trasfondo conceptual de Planificación de la Continuidad del Negocio. Luego se extraen diferentes aspectos de los modelos BCP e integrado con una fase continua de gestión de desastres previa al desastre (preparación) para mejorar explicar la naturaleza de esta investigación. Los marcos teóricos discutidos en el estudio están relacionados a la gestión de desastres concentrándose específicamente en la fase previa al desastre (preparación) del círculo de gestión de desastres para explicar la importancia de establecer un BCP antes de que ocurra una catástrofe (p. 20)

El principal objetivo y general de esta búsqueda es el desarrollo un plan de continuidad del negocio antes de que ocurra alguna catástrofe dentro de la organización ya sea de manera natural o por interferencia humana.

Ibukunoluwa Akinbola. (2018), en su plan de tesis "A Step towards Resilience, Creating a Business Continuity Plan for White Rock Finland KY", nos dice que:

El Plan de Continuidad es el objetivo primordial de la tesis, identificando los posibles impactos dirigidos a la empresa debido a una interrupción. Este estudio brindará información sobre la planificación de la continuidad del negocio y los procedimientos para implementar un plan de negocios continuo. Un BCP es uno de los componentes cruciales de cualquier estrategia de recuperación después de una interrupción. Lamentablemente, no todas las organizaciones desarrollan un plan de continuidad (p. 5).

En la mayoría de las empresas es aconsejable usar un plan de continuidad para poder responder de manera eficiente ante alguna situación de desastres, el BCP es un documento importante con información crítica y de importancia para la empresa, en el cual se debe contar con información detallada de todos los procesos y servicios.

Yufra, (2018), en su tesis "Impacto e implementación del modelo de continuidad de servicio de mesa de ayuda en un terminal Portuario del Callao" menciona que: No obstante, como todo servicio, es sensible y vulnerable a los diversos peligros a los que está expuesto, creando así un objeto de investigación capaz de hacer frente a las amenazas. Las diferencias y similitudes entre desastres y eventos están determinadas por cada negocio o empresa en función de los enfoques comerciales clave. También mencionó que en los últimos años se ha desarrollado el concepto de protección unificada contra desastres o incidentes y la gestión de servicios relacionados con las tecnologías de la información. Sin embargo, cuando el

marco ITIL examina el contenido relacionado con desastres, su enfoque se basa en la participación del servicio.

Ati, T, (2018), en su tesis "Diseño del plan de recuperación de desastres y continuidad del negocio basado en ITIL, COBIT y de acuerdo a la norma ISO 22301, para el centro de procesamiento de datos (CPD)" menciona que:

En el progreso del proyecto se identificarán activos críticos, conjuntamente se presenta los procesos y ordenamientos a realizarse ante cualquier posible eventualidad sorpresiva que trasgreda a la interrupción de servicios prestados incluido la pérdida de información guardada dentro del CPD, asimismo se asegura que la huella a los usuarios de aquellos servicios e información sea mínima, de tal modo que estos no se vean afectados a gran escala bajo circunstancias de distintos acontecimientos. Con la finalidad de reducir las interrupciones y pérdidas de servicios tales como información y otros datos, se bosqueja el plan de recuperación para desastres y conjuntamente la continuidad del negocio, a través del cual se permita la localización de los activos físicos y lógicos que son frágiles, de tal manera poder enfrentar futuros desastres que entorpezcan, afectan y atentan a la integridad de las cargos normales del Centro de Procesamiento de Datos, para que este sea capaz de reanudar de manera rápida sus funciones, e incluir la prevención ante eventos que afecten al servicio.

A lo largo del tiempo, las empresas e instituciones han experimentado la importancia de crear un plan alternativo que pueda funcionar independientemente del sistema, ya que cualquier trámite conlleva el riesgo de dificultad, pérdida de información y no confirmación de servicios por parte de agentes internos o externos. El objeto de operar y prestar servicios como servicios de apoyo debe contar con un plan de continuidad del negocio que establezca operaciones para las típicas interrupciones, desastres y contingencias críticas de trabajo

(Egúsquiza y Kong 2017) en su trabajo final "Implementación del modelo de gestión de continuidad de servicios TI basado en ITIL v3" menciona que: Su investigación radica con base en la metodología ITIL (Biblioteca de Infraestructura de Tecnología de la Información), se probaron simulaciones controladas para la implementación del modelo de continuidad. El estudio fue claramente exploratorio y desarrolló las actividades y procesos necesarios para lograr la madurez en la gestión de

la continuidad, dando como resultado la documentación y capacitación necesaria para mejorar los procesos de desastres de cualquier índole.

En este proyecto el autor trata de que se efectúe la colección de información y elaboración de los procesos que manejan las TI. Además, realiza toda la observación del negocio ejecutando las buenas prácticas de ITIL y las ventajas del modelo de gestión de continuidad.

Según (Ghannam, 2017), en su plan final "Challenges and Opportunities of Having an IT Disaster Recovery Plan", se encamina en el análisis del enfoque del plan de recuperación fante desastres que podrían ocurrir en las tecnologías de información.

Este documento desarrollado en Suiza presenta una visión de la efectividad de los planes de recuperación para riesgos previsibles en los servicios de tecnología de la información de TI. En este estudio los resultados fueron examinados cualitativamente para determinar la seguridad del plan de recuperación de desastres, identificar las principales prioridades cubiertas por la gestión de continuidad y, básicamente, centrarse en la disponibilidad de sitios, mano de obra, tecnología de apoyo y servicios.

Mediante esta investigación, el autor menciona que, después de estar utilizándolo como herramientas el juicio de expertos y entrevistas sobre el tema, existen varios desafíos en la medición de la seguridad de los planes de recuperación, principalmente la toma de decisiones y el tiempo de interrupción del servicio.

Por último, la investigación de Segovia (2017) en su tesis "Developing a Framework for Business Continuity Management within Local Government" menciona que:

Esta tesis explora la teoría y la práctica y gestión de la continuidad del negocio (BCM); en particular, traspasando de las experiencias de gerentes dentro del sector del gobierno local. La sección 1.2 proporciona una introducción y descripción general de la disciplina BCM y la motivación detrás del estudio. Un DRP que es un sistema con el cual varias organizaciones o entidades se prearan para posibles desastres de cualquier tipo que puedan dañar la infraestructura.

La detalla el propósito de la investigación e identifica la brecha de conocimiento antes de definir las preguntas de investigación, el componente 1.4 hace referencia a la metodología de investigación. La unidad 1.5 proporciona una sinopsis de los marcos teóricos utilizados en este estudio y justifica por qué son relevantes y

significativos para esta investigación. La sección 1.6 proporciona un esquema estructural del conjunto tesis (p. 11).

El autor Segovia en su tesis dice que la realización de un plan de continuidad basado en las experiencias de los gerentes es muy práctica dentro del sector del gobierno local además nos da una introducción a lo que es la disciplina BCM y la motivación tras el estudio.

2.2. MARCO TEÓRICO

Plan de Continuidad del Negocio (BCP)

La planificación de la continuidad del negocio se enfoca en mantener o restaurar las operaciones en caso de un evento imprevisto que amenace los servicios proporcionados por CPD, minimizando el impacto en el crecimiento del negocio y reduciendo el tiempo de respuesta a incidentes, para que tenga la oportunidad de iniciar acciones críticas.

El plan de continuidad es el que permite la recuperación de las operaciones en caso de una contingencia y la interrupción de la continuidad, mediante un conjunto de prácticas, criterios, normas, etc. (Zapata, 2020)

La planificación o plan de la continuidad se centra en garantizar la continuidad del negocio en caso de imprevistos repentinos. Lo que intenta este programa es no frenar la productividad de la empresa y tratar de que lo que está pasando en ese momento no nos afecte en la medida de lo posible.

A continuación, se muestra una imagen de como ha evolucionado no norma ISO 22301ª lo largo de la historia.

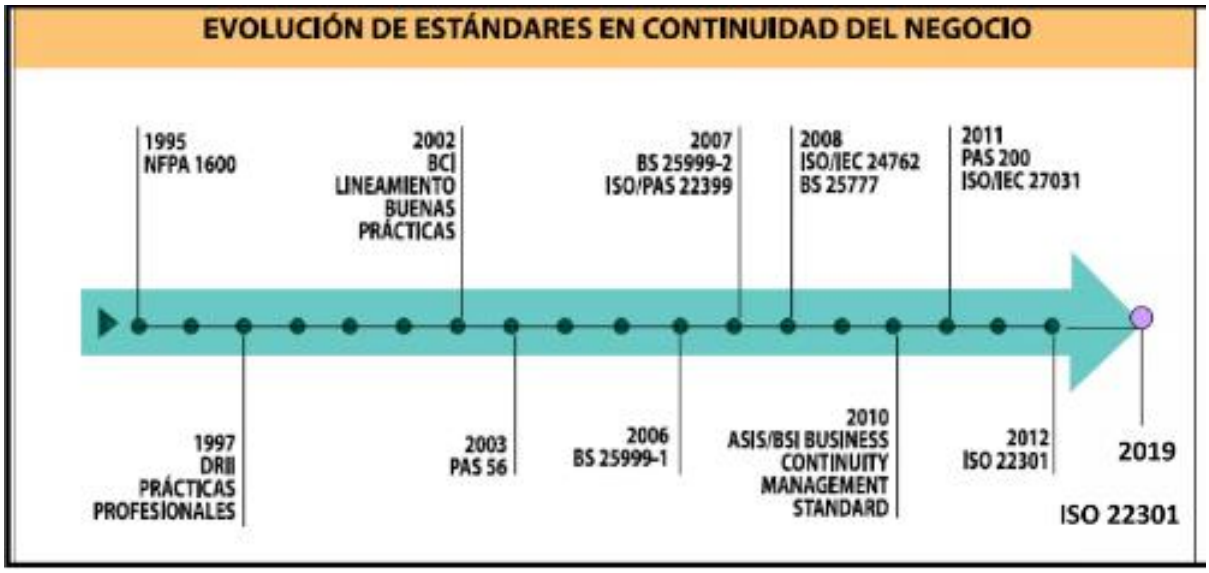


Figura 1. Evolución norma ISO 22301

Fuente: *(Sistema de Gestión, 2020)*

NFPA 1600, surge desde 1995, el más antiguo de los lineamientos, el cual estableció criterios para la continuidad de las empresas.

> Prácticas Profesionales para la gestión del Negocio, publicado por Disaster Recovery Institute International (DRII). De igual manera la: Buena práctica para la continuidad del negocio surgió en 2002, publicado por el Business Continuity Institute (BCI) PAS 56 elaboro recomendaciones para la anticipación de incidentes (Primala Sistema de Gestión, 2020).

Lineamiento BS 25999-1, se puso en conocimiento la fase de vida de la continuidad del negocio. También el estándar Bs 25999-2, fue el primer estándar internacional auditable y certificable, Definiendo requisitos basados en buenas prácticas (Primala Sistema de Gestión, 2020).

> ISO/IEC/ 24762 y BS25777 publicadas en el año 2008, las cuales permitía la comunicación ante la recuperación de desastres y la otra un código de buenas prácticas.
>
> ASIS/BSI lineamiento basado en BS 25999 y determina los requerimientos para la gestión de continuidad del negocio. En el año 2011 el PAS 200 (Gestión de Crisis- Lineamientos y Buena práctica) establecido para concurrir a las empresas para manipular la crisis.

El comité técnico TC/223, el 15 de mayo de 2012 fue publica la primera versión de la norma ISO 22301:2012 Sistemas De Gestión De La Continuidad Del Negocio, reemplazando a la 25999-2(Primala Sistema de Gestión,2020).

Beneficios de implementar la gestión de continuidad del negocio

Proporciona los elementos clave para que todos los miembros de la agencia estén preparados y sepan cómo enfrentar la situación y cumplir con las normas y reglamentos internos.

La capacidad de asegurar a las partes interesadas para la continuidad.

Resiliencia y excelente desempeño organizacional

La operación de la empresa con una planificación estratégica y gestión de riesgos.

Conocimiento del trabajo de la organización con el análisis de áreas críticas.

Mantiene la disponibilidad de activos tecnológicos, garantizando su protección,

Reduce pérdidas financieras y de tiempo, mejorando la imagen corporativa (Szarfman, 2020).

Propósito del Plan de Continuidad del negocio

El propósito de este tipo de Plan es el que se debe priorizar al personal, información, procesos y la empresa, para cumplir esto se debe tomar estrategias que permitan minimizar las pérdidas de información o datos, malestares de cliente y servidores, recuperando los procesos de manera oportuna, manteniendo el perfil público.

Sistema de Gestión de la continuidad del Negocio (SGCN) en la organización ISO 22301:2019

La norma ISO 22301:2019 se puede implementar en grande, mediante y pequeñas empresas privadas, públicas, en cualquier sector de la industria (EDUACIÓN, Financiero Telecomunicaciones, etc.).

Las metodologías de análisis y gestión de riesgos son compatibles con MAGERIT, CRAMM, ISO 31000:2018.

A continuación, se muestra una tabla con las metodologías relacionadas con el plan de continuidad de negocio en una breve descripción de estas.

Tabla 1. Normas, metodología de un Plan de Continuidad del Negocio

NORMA TÉCNICA	DESCRIPCIÓN
ISO 22301	Es una norma que ofrece un marco completo en referente, con los conceptos básicos que permiten el desarrollo y gestión la continuidad del negocio. Esta regla de continuidad empresarial posee una gran característica ante el mundo empresarial y es que la ISO 22301 otorga certificación.
ITIL	Es un conjunto de conceptos y mejores prácticas referentes a la gestión de servicios TI que se vuelven flexibles de tal manera que se adecuan a las necesidades del negocio en el que se las aplique. Dentro de sus procesos y funciones ideados para obtener la calidad y eficiencia en las operaciones de las tecnologías de la información se establece la Gestión de la continuidad de los servicios de TI
COBIT	Es un marco de trabajo para gobernanza y gestión de TI, esta norma posibilita que el TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos de control encaminados a asegurar la continuidad operativa de una organización del sector público como privado
ISO 27031	Esta norma describe los conceptos y principios de la tecnología de información y comunicación las directrices para la preparación de TIC para la continuidad del negocio. Además, proporciona un marco de métodos, procesos para identificar y especificar todos los aspectos para mejorar la preparación de las TIC con el objetivo de garantizar la continuidad de negocio en todo tipo de organización.

NORMA TÉCNICA	DESCRIPCIÓN
ISO 22399	Esta norma es un complemento para la ISO 22301 sobre el plan de continuidad de negocio, engloba una guía para desarrollar criterios adecuados permitiendo a las organizaciones e instituciones estar competentes ante incidentes y de esta manera se mantenga la gestión continuidad operativa

Fuente: (Olarte, 2016)

Para poder elegir la norma que aprovechó como guía para el desarrollo del BCP propuesto, se analizaron varias normas y estándares internacionales los cuales tienen relación con la continuidad del negocio. En la tabla a continuación, se muestra un cuadro comparativo en base al cumplimiento de parámetros técnicos de los estándares y normas estudiadas bibliográficamente.

Tabla 2. Parámetros técnicos de normas internacionales

PARÁMETROS	ITIL	COBIT	ISO 22301	ISO 22399	ISO 27031
Ciclo PDCA	X	X	X	X	X
Alcance	X	X	X	X	X
Referencias	X	X	X	X	X
Términos y definiciones	X	X	X		X
Sistema de Gestión de Continuidad del Negocio			X		

PARÁMETROS	ITIL	COBIT	ISO 22301	ISO 22399	ISO 27031
Política			X	X	
Planificación	X	X	X	X	X
Riesgo		X	X	X	
BIA		X	X	X	
Estrategia	X		X		X
Implementación	X	X	X	X	X
Identificación de recursos		X	X	X	X
Roles y responsabilidades	X	X	X	X	X
Plan de Continuidad			X		
Monitorización	X	X	X	X	X
Evaluación de normativa			X	X	
Pruebas	X	X	X	X	X
Auditoría	X	X	X	X	
Mejora continua	X	X	X	X	X

Fuente: (Olarte, 2016)

Nota. La tabla mostrada anteriormente hace una comparación entre parámetros y técnicas que cumple cada norma que está relacionada a la continuidad del negocio.

Observando el cuadro comparativo anterior, se puede apreciar todos los parámetros de cada una de las nomas, además de visualizar cuales cumplen con todos o su mayoría, al igual que ver su incompletitud. Entonces se aprecia que la norma ISO 22301 cumple con todas las medidas necesarias para poder ejecutar de una manera adecuada la gestión de continuidad de negocio. Esta guía considera todos los servicios, activos y procesos de la organización en relación con ITIL el cual tiene un enfoque del proceso de gestión de continuidad de los servicios de tecnologías de la información.

Cabe visualizar que COBIT hace énfasis en el desempeño regulatorio para colocar valor al área de TI por medio de un dominio de entrega, de servicio y soporte. La norma ISO 27031 expone prácticas enfocadas claramente en la continuidad de TIC en caso de eventos disruptivos por lo cual es considerada un complemento de la norma ISO 22301. En conclusión, la norma ISO 22399 es de gran ayuda y se la usa como guía para que las instituciones y organizaciones instauren criterios propios de desempeño ante a incidentes y en base a los mismos seleccionen las opciones de continuidad de los servicios.

Tabla 3. Criterios de valoración de nivel de gestión de continuidad del negocio

Ponderación	Calificación	Descripción
Entre 0 y 1	En preparación	El área en cuestión no cumple con los criterios establecidos en la ISO 22301. Es necesario precisar una metodología de trabajo para dar inicio con el Sistema de Gestión de Continuidad de un Negocio

Ponderación	Calificación	Descripción
Entre 1,1 - 2	Básico	La organización enfrenta varios de los criterios que son introducciones al SGCN, no obstante, aún no se desempeña de manera adecuada con las exigencias mínimas, las cuales están establecidas en la norma ISO 22301
Entre 2,1 – 3	Establecido	Dentro del espacio en cuestión se ha definido varios de los aspectos y criterios primordiales de un SGCN, basándose en los principales requerimientos de la norma ISO 22301. Además, tiene un contingente básico para poder responder a posibles eventualidades que se presenten.
Entre 3,1 – 4	Administrativo	El SGCN cumple con los requerimientos que están establecidos en la norma ISO 22301, lo cual da paso a iniciar con la certificación en el lapso de un mediano plazo
Entre 4,1 - 5	Optimizado	La organización tiene un Sistema de Gestión de Continuidad de un Negocio completo, en el que están considerados todos los requisitos de la norma ISO 22301.
Entre 4,1 - 5	Optimizado	Se visualiza la evidencia y apoyo por parte de los directivos por lo cual se logra certificar a la institución u empresa en un periodo de corto plazo

Fuente: (Araujo, 2019)

Nota. Se muestra la valoración del nivel de gestión en los cuales se valorará la continuidad de negocio, siendo esto una escala de 0 a 5 siendo cero en preparación, 5 cinco en estar al día con el cumplimiento de un BCP.

Tipos de amenazas en TI

El Instituto Nacional de Ciberseguridad, reduce el término amenaza como una circunstancia desfavorable, por lo tanto, una vez que ha ocurrido este incidente se generan consecuencias negativas sobre los activos tales como indisponibilidad, el mal funcionamiento o pérdida de valor de estos. Las diferentes amenazas pueden originarse por causas naturales, accidentales o intencionadas (INCIBE, 2020).

A su vez también se considera como amenaza a toda y cada una de las acciones que aprovechan una vulnerabilidad para poder atacar, infiltrarse o penetrar un sistema informático. En su gran mayoría las amenazas descienden en fuente de ataques externos, no obstante, también existen amenazas que se encuentran dentro de la organización (internas) como hurto de información o uso inadecuado de los sistemas a los que tiene acceso.

Machicao (2019) dentro de su proyecto antepuesto al final de investigación define una amenaza como un dispositivo o acciones que puedan comprometer la seguridad de la información. Dicho de otra manera, una amenaza puede materializarse en el caso de existir una vulnerabilidad para explotar. El autor describe a tres tipos de amenazas:

- A los actos causados por la criminalidad común y motivación política
- Evento de origen físico
- Eventos derivados de la negligencia e impericia de los usuarios/as y decisiones institucionales

En el libro II Catálogo de elementos (Ministerio de Hacienda y Administraciones Públicas, 2012), de la metodología MAGERIT describe un listado de posibles amenazas, las cueles están presentes de manera no visible en toda empresa ya sea de tamaño mediano, pequeño o grande, estas amenazas se clasifican en diferentes tipos tales como son los desastres naturales, errores y fallos no intencionados, ataques intencionados y de origen industrial. Para poder ver el tipo de amenaza y su respectiva clasificación según MAGERIT revise el anexo número 4.

Riesgos del Área de Tecnología y Comunicación

Los riesgos en los últimos 10 años que se ha presentado en la institución son incendios, vientos fuertes, robo, vandalismo, daño de hardware y archivos, falla de hardware, corrupción de archivos, errores, virus, terremotos, acceso no autorizado, fuga de información, robo de datos, fraude, alteración de información para lo cual se debe analizar los riesgos y se los debe clasificar en forma, bajo, muy bajo, alto, muy alto, medio. Se debe tomar en cuenta las causas por las cuales se presentan estos riesgos.

Riesgos de los servicios prestados de la institución

Los riesgos presentados que afectan directamente son a la base de datos, la seguridad, integridad, acceso, ataque, ataque activo, ataque pasivo, amenazas, incidentes y golpe (Breach), interrumpiendo a la paralización de los servicios prestados por la institución desde el proceso de gestión, el proceso de consultoría, el proceso de soporte, el proceso de negocio.

Riesgo de Reputación como institución pública con la paralización de servicios

La reputación de la institución con los servicios prestados, se lo identifica como un GAD de mala gestión con aspectos negativos, la cual existe molestias por parte de usuario y personal municipal causando procesos judiciales y malestares.

Control de calidad

"El control de calidad es una forma de verificar los estándares o servicios de productos durante el procesamiento y la porción para reducir la capacidad de insertar productos utilizando un error de mercado" (Orellana, 2020).

Es la forma de verificar si el servicio o el producto están siendo ejecutados de manera correcta.

Figura 2. Ciclo Plan-Do- Check-Act (PDCA)

Fuente: (Zapata, 2020)

Nota. La figura número dos del presente trabajo muestra el ciclo de calidad de gestión en cuatro pasos.

Fases Del Plan De Continuidad Del Negocio

Las fases del Plan del negocio mediante la norma ISO 22301:2019, las cuales se toma en cuenta para el desarrollo de este. A continuación, se simplifica en la Tabla 4.

Tabla 4. Fases del plan de continuidad del negocio.

FASE	DESCRIPCIÓN	OBSERVACIONES
Fase 0: Determinación del alcance	Alcance del BCP	Define las áreas donde se va a desarrollar el BCP
	Política y objetivos de la continuidad del negocio	Documentación de lo que se quiere lograr con el BCP y cómo controlar

FASE	DESCRIPCIÓN	OBSERVACIONES
	Determinación de la situación actual de la organización	Información de cómo se encuentra la organización
Fase 1: Análisis de la Organización	Análisis de impacto de la organización (BIA)	Identificación de procesos críticos
	Análisis de riesgos	Determinar los activos tecnológicos críticos
Fase 2: Determinación de estrategias de continuidad del negocio	Estrategias de continuidad del negocio	Documentación que contiene estrategias de respuesta frente a un incidente.
Fase 3: Respuesta a la contingencia	Plan de contingencia	Se debe definir como se debe registrar los incidentes
	Comité de crisis	
Fase 4: Prueba, mantenimiento, revisión	Planes de prueba y revisión	Se debe definir los escenarios y objetivos que se deben cumplir
	Plan de mantenimiento del BCP	Documentación que debe contar cuando y quien va a realizar el mantenimiento.
Fase 5: Capacitación y concienciación	Plan de capacitación y concienciación	Las necesidades de temas de capacitación del personal.

Nota. Anteriormente se muestra las faces necesarias que debe tener un plan de continuidad.

Fuente: (Zapata, 2020)

Nivel de Gestión de Continuidad del Negocio

Cláusulas establecidas en la norma 22301:2019

- Cláusula 4 – Contexto de la Organización

La necesidad del contexto de la organización, percibir necesidades y los intereses de las partes involucradas, para ello determinar la aplicación de la gestión.

- Cláusula 5 – Liderazgo

Relevancia a las responsabilidades, funciones y autoridades de la alta dirección.

- Cláusula 6 – Planificación

Se debe identificar los riesgos y oportunidades para determinar la situación de la organización y así el alcance de esta.

- Cláusula 7 – Soporte

Para tener conocimiento de los recursos es necesario tener información de esa manera se ayudaría a mantener y controlar.

- Cláusula 8 – Operación

La organización planea e inspecciona los procesos internos y externos

- Cláusula 9 –Evaluación del desempeño
- Cláusula 10 –Mejora continua
-

Tabla 5. Cláusulas de la norma ISO 22301:2019

1. ÁMBITO DE APLICACIÓN
2. REFERENCIAS NORMATIVAS
3. TÉRMINOS Y DEFINICIONES

CLÁUSULA	DIMENSIÓN
4. CONTEXTO DE LA ORGANIZACIÓN	4.1. Establecimiento de aspectos y factores internos y externos del SGCN
	4.2. Definición y establecimiento de las necesidades y expectativas de partes interesadas
	4.3. Alcance del SGCN
	4.4. Administración del Sistema de Continuidad del Negocio
5. LIDERAZGO	5.1. Compromiso, apoyo, patrocinio y gestión, por parte de los ejecutivos y la alta gerencia al SGCN
	5.2. Establecimiento y comunicación de la política de continuidad al interior de toda la organización
	5.3. Asegurar la definición de roles, responsabilidad, autoridad y rendición de cuentas del SGCN
6. PLANIFICACIÓN	6.1. Identificación y determinación oportuna de riesgos y oportunidades
	6.2. Alineación estratégica para prevenir efectos y evaluar acciones
	6.3. Definición de los objetivos del SGCN alineados a los planes y estrategias
7. APOYO	7.1. Determinar y proporcionar los recursos necesarios para atender el SGCN
	7.2. Recursos que cuentan con competencia, habilidades, experiencia y toma de conciencia para el SGCN

CLÁUSULA	DIMENSIÓN
7. APOYO	7.3. Dispone de mecanismos de comunicación interna y externa, quién, cuándo, dónde y procedimientos. 7.4. Información documentada del SGCN (creación, actualización, control)
8. OPERACIÓN	8.1. Definición, evaluación y administración de riesgos y análisis de impacto al negocio BIA 8.2. Diseño, determinación y administración de estrategias DRP y BCP para todo el SGCN 8.3. Procedimientos del SGCN, administración y respuesta a incidentes 8.4. Definición, ejecución y evaluación de ejercicios y pruebas al SGCN
9. EVALUACIÓN DE DESEMPEÑO	9.1. Evaluación y medición de todo el procedimiento de continuidad del negocio 9.2. Realización y cumplimiento de auditorías internas planificadas 9.3. Revisión y evaluación de los ejecutivos y gerencia al SGCN
10. **MEJORA**	10.1. Identificación, monitoreo y solución de no conformidades y acciones correctivas 10.2. Mejora continúa asociada al mantenimiento, actualización y conciencia sobre SGCN

Fuente: (Días, 2022)

Nota. Si se visualiza la tabla anterior, existen varias clausulas con sus respectivas dimensiones que ayudan y guían al plan de continuidad.

Análisis de Impacto del negocio (BIA)

El análisis el impacto y gestionar los riesgos se debe tomar en cuenta los grupos de: riesgos internos y externos.

Riesgos internos: riesgos de recursos humanos, tecnologías de información y comunicaciones, financieros, tiempo, etc.

Riesgos externos: pérdida de imagen, reputación, riesgo de entorno de negocio, normativa.

Figura 3. Componentes del BIA

Fuente: (Zapata, 2020)

Nota. La anterior figura muestra los componentes del análisis de impacto del negocio, es un componente esencial en el BCP. Tomado de la web.

En términos de continuidad comercial, el término "objetivo de punto de restauración" (también conocido como RPO) es importante. Las precauciones que ayudan a las empresas a mantenerse protegidas y capaces de reaccionar rápidamente ante incidentes de seguridad son fundamentales para minimizar o eliminar por completo cualquier daño que afecte sus operaciones normales.

Es importante contar con un sistema que pueda responder con eficacia y rapidez ante cualquier situación grave imprevista, restableciendo así el normal desarrollo de la organización sin afectar la continuidad de las actividades empresariales (ISOTools, 2021).

La recuperación de información es muy importante para las empresas, para que estén protegidas y que se puedan reaccionar ante algún incidente.

Para establecer un análisis de impacto en el negocio, es necesario aclarar los siguientes conceptos: Un objetivo de punto de restauración o RTO (tiempo de recuperación para operaciones con condiciones mínimas tolerables), un tiempo de recuperación objetivo o MTD (tiempo máximo aceptable hasta la falla) en caso de un impacto catastrófico en la empresa y sus procesos antes de impactar en cada negocio) y tiempo de inactividad o Máximo Aceptable RPO (relación que define la cantidad máxima de información que se puede perder sin consecuencias inaceptables, como parte de una estrategia de respaldo y según lo determine la organización) (Instituto Nacional de Ciberseguridad, 2017).

Análisis de Riesgo

Normas y metodologías de análisis de riesgos

Considerando el estudio y análisis comparativo de metodologías para el desarrollo de Auditorías Informáticas realizado por Cabrera (2021), se confirma que existe un sin número de métodos y normas para analizar una observación de riesgos. En presente contexto se hace referencia a MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), OCTAVE (Operational Critical, Threat, Asset and Vulnerability Evaluation), MEHARI (Método Armonizado de Análisis de Riesgos), NIST SP 800:30 (National Institute of Standards and Technology), y muchas más existentes. Cabe recalcar que cada una de las metodologías poseen sus propias características y al instante de elegir una de las opciones, se debe examinar la utilización de una de ellas, la cual permita realizar un análisis acorde a la información disponible dentro de una organización. Para llevar de manera correcta el proceso de análisis de riesgos, es fundamental que se realice una socialización sobre la metodología seleccionada a todos y todas las partes involucradas.

En la siguiente Tabla, se describen algunas metodologías prestas para el análisis de riesgo, además, está detallando el cumplimiento de distintos parámetros considerados y necesarios en el desarrollo de esta fase.

Tabla 6. Cuadro comparativo de metodologías de análisis de riesgos

Parámetro	ISO 27005	OCTAVE	NIST 800 30	MAGERIT	MEHARI	ISO 31000	Microsoft security Management
Caracterización del estado actual de la seguridad de los sistemas y de la organización	X		X		X	X	
Identificación y valoración de activos críticos	X	X		X		X	X
Identificación de vulnerabilidades y amenazas de la organización		X	X	X		X	X
Identificación de recursos clave y vulnerabilidades que ocasionan riesgos	X	X	X	X			
Identificación, estimación y valoración del riesgo	X	X	X	X		X	X
Determinación y evaluación del impacto				X	X	X	
Tratamiento del riesgo	X	X	X	X		X	

Parámetro	ISO 27005	OCTAVE	NIST 800 30	MAGERIT	MEHARI	ISO 31000	Microsoft security Management
Comunicación del riesgo	X			X	X	X	X
Monitoreo y revisión	X	X	X	X	X	X	X
Documentación de resultados			X	X		X	

Fuente: (Olarte, 2016)

Nota. En el presente cuadro se observa cuáles son las normas que cumplen con todos los criterios, así mismo las que carecen en su varios aspectos o parámetros.

Tomando como base la comparativa anteriormente, para el desarrollo del proyecto se utilizó la metodología MAGERIT, por engloba miento y debido al alcance completo que brinda en el análisis y gestión de riesgos. Además, posee una amplia documentación concerniente a recursos de información, amenazas y tipos de activos que tiene la empresa u organización en cuestión. Esta metodología permite analizar los riesgos de las maneras cuantitativa y cualitativa y es de libre uso.

Motaki (2016) en la evaluación realizada dentro de su plan de trabajo e investigación, obtiene como conclusión que la metodología MAGERIT es la más adecuada para las infraestructuras críticas, también toma en cuenta que ofrece un entorno amigable para el usuario.

La metodología MAGERIT en versión 3 fue desarrollada por el Consejo Superior de Administración Electrónica y en la actualidad está siendo revisada desde la Secretaría General de Administración Digital con la gran colaboración y participación del Centro Criptológico Nacional en España. Además, es una metodología de carácter público que puede ser utilizada de manera libre sin autorización previa. También es objetiva en cumplir con la primicia de gestión de seguridad basada en riesgos, de igual manera cumple con el requisito de análisis y gestión de riesgos, a su vez considera la relación con las TI para cumplir metas,

proporcionar servicios y alcanzar los objetivos de la organización. MAGERIT realiza el Proceso de Gestión de Riesgos guiándose en la normativa ISO 31000.

Esta metodología se centraliza en cumplir los siguientes objetivos:

- Se centra en concienciar a los responsables de las organizaciones de información sobre la existencia de riesgos y la gran necesidad de gestionarlos para evitar pérdidas de diferente tipo.
- Enforcarse en ofrecer un método sistemático para examinar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a revelar, planificar el tratamiento eficaz y oportuno para mantener los riesgos bajo un estricto control
- Instruir de la mejor manera a la organización ante procesos de evaluación, certificación, acreditación y auditoría

El proceso de la realización del pertinente análisis de riesgos, el uso de MAGERIT aporta una gran ayuda. principalmente se identifican los activos, amenazas, detección de las defensas y consecutivamente permite desarrollar acciones para controlar y reducir los riesgos encontrados dentro del área (Cabrejos, 2020).

En la revista tecnológica y científica de la Universidad Estatal Península de Santa Elena, se exhibe un artículo donde se emplea la metodología MAGERIT para describir el proceso de gestión y análisis de riesgos de los sistemas de información de las organizaciones del sector público y privado de modo general. Aquí se evidencian las ventajas y pasos que deben ser ejecutados previamente para la preparación y elaboración de un Plan de Contingencia (Ferruzola et al., 2019).

Santa María (2020), en su trabajo investigativo desplego la propuesta de un plan de continuidad basado en la metodología MAGERIT el cual tiene por objetivo el reducir los riesgos operativos de tecnologías de la información. Para ello se llevó a cabo el análisis de los riesgos operativos de TI que existen dentro de la organización, el esquema de la propuesta del plan de continuidad para reducir los riesgos operativos de TI y la ratificación el modelo propuesto.

Uno de los primordiales para la creación y desarrollo de un BCP es la evaluación y el análisis de riesgos. Dentro del presente proyecto se ha formulado utilizar la metodología de análisis y gestión de riesgos MAGERIT versión 3. Cabe aclarar que el proceso de gestión de riesgos de esta metodología se centraliza en un esquema de

trabajo en el que las decisiones se definen tomando en cuenta los riesgos derivados del uso de tecnologías de la información (Imbaquingo et al., 2016).

Nivel de gestión inicial de continuidad del negocio

Un modelo de madurez es considerado como un mapa o guía que proporciona los pasos para que la organización implemente buenas prácticas, conocer la situación actual y planificar procesos de mejora. Esto quiere decir que para conocer el valor inicial de madurez de la institución referente a gestión de continuidad del negocio es necesario mediar los valores obtenidos en cada una de las cláusulas correspondientes.

Las cláusulas por tomar en cuenta son adaptadas de (Olarte 2016) las cuales son:

- Contexto de la organización
- Liderazgo
- Planificación
- Apoyo
- Operación
- Evaluación de desempeño
- Mejora

Cada una tiene su valor y criterio personal, de acuerdo con la valoración global y en base a resultados en la pirámide se puede seleccionar el área en el cual se encuentra la institución pública u empresa para la cual se está desarrollando el plan de gestión de continuidad del negocio. De acuerdo a la selección podrá darse un criterio valorado el cual indique y mediante la información que se conocerá en qué fase se encuentra la empresa y posterior a ello se continuara el desarrollo del BCP.

Figura 4. Criterio de valoración del nivel de gestión de continuidad

Fuente: (Olarte, 2016)

Nota. En forma de pirámide de manera ascendente se muestra el nivel de madurez de gestión inicial de continuidad de negocio.

Modelo de madurez

El presente modelo de madurez permite evaluar la etapa en el que se está un determinado proceso o actividad. Cada uno de estos estados se corresponde con un nivel de madurez que, debidamente, va desde el nivel uno a cinco

En el primer nivel o fase de preparación: los procesos consisten en una serie de actividades que no tienen un orden o un ejecutante definido y Su éxito depende de la capacidad de los empleados de la organización, no del uso de procesos probados. Según Conrado (2019) recalca que, en este nivel, los productos y servicios son eficientes, pero su producción a veces excede el costo y el tiempo.

En este nivel llamado básico: se realizan, procesos, planificación, se miden y controlan. Las normas, las descripciones y los procedimientos de los procesos pueden variar, y la disciplina establecida de gestión de procesos ayuda a mantener las prácticas existentes y ejecutar y gestionar proyectos de acuerdo con planes documentados.

En la fase tres o nivel 3: establecido los procesos que se definen, en los cuales comprenden y se realiza la documentación mediante procedimientos, herramientas y técnicas. Según Conrado (2019) ratifica que los estándares, las descripciones y las tareas se derivan de los procesos de toda la empresa y se llevan a cabo de manera uniforme en toda la organización, los procesos son predecibles cualitativamente.

En el nivel llamado administrado o fase cuatro: Según Conrado (2019) menciona que:

Los subprocesos o subcrevenores asisten por el rendimiento general y el control, los indicadores de calidad y rendimiento de rendimiento también se determinan como criterios de gestión de procesos a lo largo del ciclo de vida. Las mediciones se basan en las necesidades del cliente, los usuarios finales, la organización y los medios para implementar el proceso, tratando de apoyar la toma de decisiones futuras. Esto nos indica que las variaciones son identificadas, corregidas en su finalidad el rendimiento es predecible y controlado.

La última área conocida con el nombre de nivel optimizado: es el nivel con mayor madure, los procesos son mejorados continuamente basado en mediciones cuantitativas de causas comunes de variación del proceso. En este nivel se tiene como objetivo, mejorar el rendimiento con mejoras tecnológicas innovadoras. La organización responde de manera eficiente a cambios y oportunidades, compartiendo aprendizajes y conocimientos para la mejora continua la cual es rol de todos los empleados (Conrado, 2019).

Escala de Tiempos de Recuperación

La tabla de tiempo de recuperación nos permite determinar en la cantidad de horas y minutos aceptable que puede tolerar la institución. Se aprecia la escala de tiempos definida y las fases a la que pertenecen cada uno de ellos.

Figura 5. Escala de tiempos de recuperación.

Fuente: (Rubén, 2020)

En la Tabla 7, se alistan los tiempos de recuperación situados para el análisis de cada proceso.

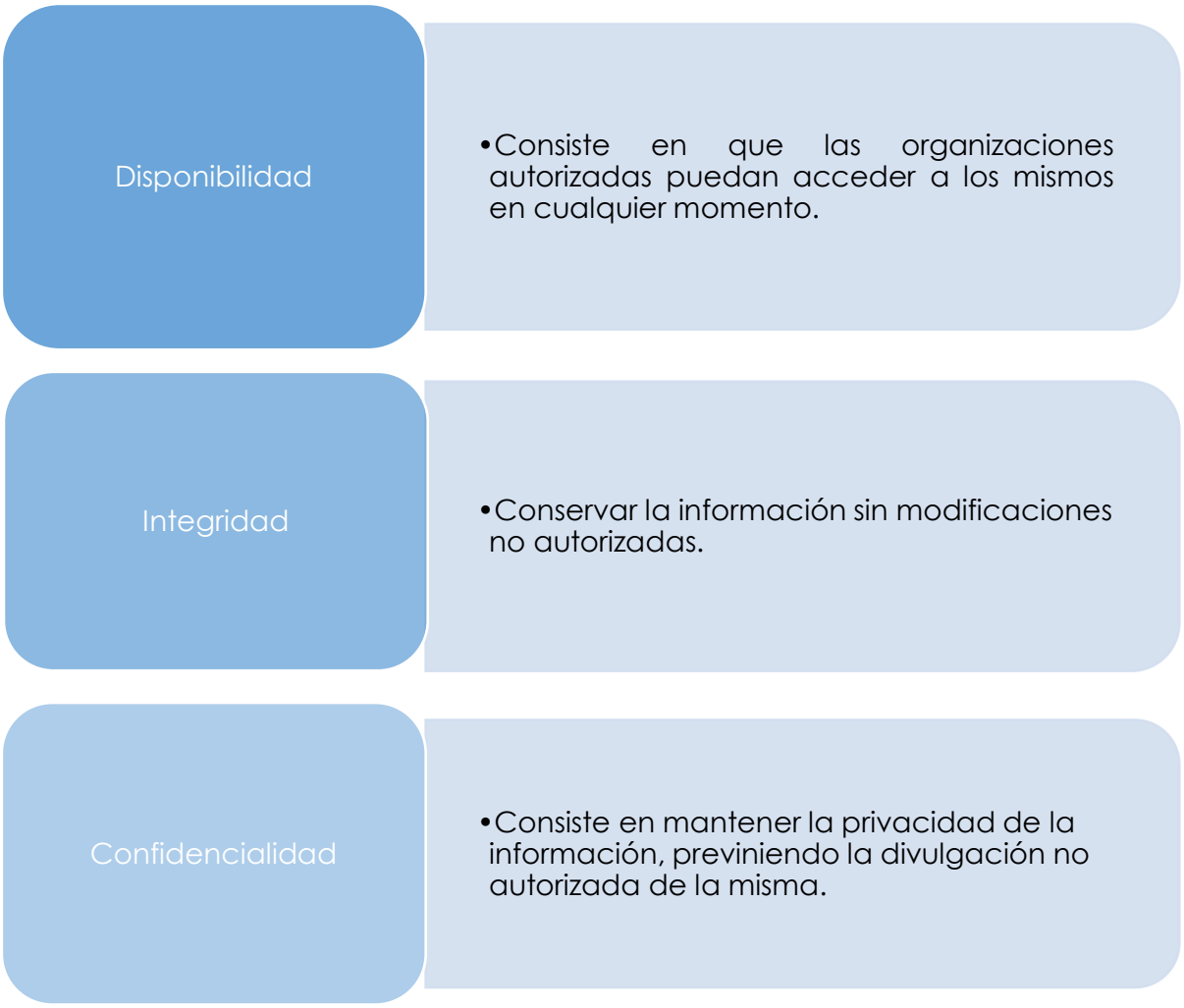
Tabla 7. Descripción de tiempos de recuperación

Tiempo de Recuperación	Descripción
RPO (Recobery Point Obcjetive)	Punto de Recuperación Objetivo Cantidad máxima aceptable de pérdida de datos que la empresa puede tolerar
RTO (Recovery Time Objetive)	Tiempo de Recuperación Objetivo Cantidad máxima aceptable necesario para que todos los sistemas vuelvan a operar
WRT (Work Recovery Time)	Tiempo de Recuperación del trabajo Cantidad máxima de tiempo tolerable necesario para verificar los procesos y la integridad de los datos.
MTD (Maximun Tolerable Downtime)	Tiempo Máximo de Inactividad Tolerable Periodo máximo de inoperatividad que puede tolerar la empresa sin causar consecuencias graves.

Fuente: (Rubén, 2020)

Análisis de riesgos

Para el análisis de riesgos se utilizó la metodología MAGERIT, que toma en consideración tres dimensiones de valoración, las cuales son:



Y nos permitió el criterio de valoración de los activos tecnológicos

Valoración de criticidad

La Valoración de cada riesgo permite determinar el nivel del valor máximo en los tres criterios: Disponibilidad, Integridad y confidencialidad de cada uno de los activos. Para la cual los criterios de valoración son:

Tabla 8. Criterio de valoración Criticidad

Criterio de Valoración CRITICIDAD		
Valor máximo de las tres características D.I.C		
Alta (A)	3	Cuando el máximo es 3
Media (M)	2	Cuando el máximo es 2
Baja (B)	1	Cuando el máximo es 1
Nula (N)	0	Cuando todos son 0

Fuente: (Díaz, 2022)

Para el criterio de valoración de disponibilidad se toma en cuenta:

Tabla 9. Criterio de valoración Disponibilidad

Criterio de Valoración DISPONIBILIDAD		
Alta (A)	3	Información cuya inaccesibilidad permanece durante una hora impide la ejecución de las actividades
Media (M)	2	Información cuya inaccesibilidad permanece durante la jornada laboral impide la operación de las actividades
Baja (B)	1	Información cuya inaccesibilidad permanece durante una semana no ocasiona pérdidas significativas
Nula (N)	0	Información cuya inaccesibilidad no afecta la actividad normal

Fuente. (Díaz, 2022)

Para el criterio de valoración de integridad se toma en cuenta:

Tabla 10. Criterio de valoración Integridad

Criterio de Valoración INTEGRIDAD		
Alta (A)	3	Información cuya modificación no autorizada podría repararse, impidiendo la realización de las actividades
Media (M)	2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo
Baja (B)	1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio
Nula (N)	0	Información cuya modificación no autorizada puede repararse fácilmente sin que esto afecte al desarrollo de las actividades

Fuente: (Díaz, 2022)

Para el criterio de valoración de confidencialidad se toma en cuenta:

Tabla 11. Criterio de valoración Confidencialidad

Criterio de Valoración CONFIDENCIALIDAD		
Alta (A)	3	Información que puede ser conocida y utilizada por un grupo reducido de personas, cuya divulgación ocasionaría un perjuicio a la empresa
Media (M)	2	Información que puede ser conocida y utilizada por determinado personal dentro de una empresa
Baja (B)	1	Información que puede ser conocida y utilizada por todo el personal de la empresa
Nula (N)	0	Información que puede ser conocida y utilizada sin autorización por cualquier persona

Fuente: (Díaz, 2022)

Elementos claves ISO 22301:2019

La ISO 22301:2019 permite minimizar cualquier posibilidad de desastres y recuperarse de manera eficiente y lo más pronto posible y también es importantes aporten a la empresa mejora y continuidad, para ellos los puntos clave son los siguientes:

Planificación de respuesta: Se enfoca en que la empresa pueda obtener una rápida y eficiente respuesta evaluando los posibles eventos que pueden estar sucediendo si existe una continuidad de negocio que proteja los activos.

Contexto de la organización: Para realizar sus actividades se centra en los aspectos internos y externos para llevar a cabo la realización de la organización con resultados óptimos positivos y efectivos.

Liderazgo: El liderazgo para continuidad es necesarios que los miembros de la empresa tengan compromiso y responsabilidad para hacer frente a las crisis.

- Definir políticas para que los trabajadores cumplan con los objetivos para la empresa. Que los riegos de la empresa sean analizados y se fomenten estrategias para lograr la eficacia y la eficiencia.
- Asegurar los recursos de la empresa para que prioricen los apoyos y mejoras.
- Que la seguridad sea segura antes un impacto, y de importancia para la empresa.

Gestión de Riesgos: Este es un método para gestionar de forma cualitativa los riegos y planificar una dirección que puedan afectar a la empresa tras un impacto y cómo afrontarlos.

Apoyo: En este punto es importante que los recursos de la empresa y actividades que conforman estén diseñados a fin de obtener el apoyo total de los involucrados, incluyendo beneficios al personal, capacitaciones, informes documentados para que estén preparados, sin esos elementos sería imposible mitigar los riesgos y las amenazas tras un evento crítico.

Control de operaciones en el sistema de gestión continuidad de negocio: El Control Operaciones tiene como objetivo contar con las actividades necesarias o acciones que garanticen eficiencia. Por ejemplo, si se disminuye los riesgos o acciones de control, para la gravedad de impactos en la empresa se debe alcanzar un nivel de impacto positivo y eficiente con el plan de control estandarizado, sus actividades lograrán un mejor desempeño y procesos óptimos para la empresa.

Evaluación de desempeño: La norma establece que se realice un seguimiento, análisis de medición para llegar a las metas establecidas. Para ello, se realiza la medición, evaluación de resultados y así mismo tenemos que verificar que las evidencias de la actividad se encuentren orden y el desempeño sea veraz y sus funciones de procesos y actividades que se estén cumpliendo a la necesidad de la empresa.

De tal forma, que las auditorías internas que se realicen estén planificadas, evaluar con la norma para que esté acorde con la alta dirección. De la misma manera, que todo lo implementado en continuidad del negocio sea efectiva e identificar cualquier falla para presentar una oportunidad de mejora.

Mejora: El ciclo de la mejora continua se da con el fin de lograr la eficiencia, por ello se pretende identificar controles que sean de beneficio para la empresa y las políticas de continuidad para su mejora continua (Pincay, 2021).

La confidencialidad

La confidencialidad, requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario acceder a la información mediante autorización y control. La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. Es necesario determinar las empresas que a menudo desarrollan diseños que deben proteger a sus competidores.

> La sostenibilidad de las organizaciones y su posicionamiento en el mercado pueden depender de forma directa a la implantación de los diseños y deben protegerlos mediante mecanismos de control de acceso que aseguren la confidencialidad de las informaciones.
>
> El objetivo de la confidencialidad es, prevenir la divulgación no autorizada de la información sobre nuestra organización. La integridad, supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización. El objetivo de la integridad es prevenir modificaciones no autorizadas de la información. La disponibilidad supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos (Toro, 2021).

Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos

autorizados. El objetivo es necesario prevenir interrupciones no autorizadas de los recursos informáticos.

La disponibilidad

Para asegurar la disponibilidad de la información y de los sistemas de TIC que la gestionan y/o procesan, las organizaciones generalmente desarrollan planes de continuidad del servicio de las TIC. Para el desarrollo de estos planes de disponibilidad, se pueden seguir las recomendaciones o métodos descritos en los estándares de seguridad más reconocidos a nivel internacional (Unir, 2022).

> Las empresas necesitan tecnología adecuada para mantener una alta productividad, y en el momento en que un sistema deja de estar disponible, el rendimiento de los otros disminuirá, mientras que aumenta el número de tickets del servicio de asistencia. Y, en tiempos de amenazas cibernéticas recurrentes, los sistemas de seguridad perimetral no pueden dejar de funcionar; si lo hacen, los usuarios y la información confidencial estarán expuestos a posibles ataques (Blockbit, 2020).

¿Qué es el Riesgo por Fenómenos de Origen Tecnológico?

De acuerdo con la Resolución 1770 de 2013 "Por la cual se crea y conforma la Comisión Técnica Asesora de Riesgos Tecnológicos CNARIT", el riesgo de origen tecnológico o riesgo tecnológico se define como los daños o las pérdidas potenciales que pueden presentarse debido a los eventos generados por el uso y acceso a la tecnología, originados en sucesos antrópicos, naturales, socio-naturales o propios de cada operación, es decir que este tipo riesgo se encuentra asociado a una gran cantidad de actividades ya sean domésticas o de tipo industrial propias de almacenamiento, transporte, producción y/o transformación de sustancias y/o materiales químicos peligrosos, combustibles, electricidad; así como actividades que requieran altas presiones y/o temperaturas, con altas posibilidades de impacto mecánico (Instituto Distrital de Gestión de Riesgos y Cambio Climático, 2021).

Los fallos sistemáticos en los SIS no habían sido, hasta ahora, aprovechados para causar un daño deliberado. Según (Ciber Seguridad Industrial, 2021) menciona que: al menos no se habían descubierto evidencias de ello, pero esta situación ha cambiado con la llegada de un código informático dañino que hace unos años afectó a los controladores Triconex del fabricante Schneider Electric.

> Unos controladores que fueron diseñados como solución de seguridad instrumentada y cuyo sabotaje provocó la interrupción de las operaciones en, al menos, una instalación petrolífera de Oriente Medio. En este ataque dirigido no parece que tuviesen un objetivo económico claro y, sin embargo, los recursos técnicos necesarios para crear el marco del ataque han tenido que ser muy elevados.

Los riesgos tecnológicos corresponden a los daños o a las posibles pérdidas que se pueden presentar teniendo en cuenta "eventos mayores generados por el uso y acceso a la tecnología". Los riesgos tecnológicos pueden tener su origen por el uso de la tecnología ocasionados por acontecimientos "antrópicas, naturales, socio-naturales y propios de la operación". (UNGRD, 2018).

Usualmente, se suele asociar los tipos de accidentes tecnológicos exclusivamente con las instalaciones industriales o equipamientos de alta tecnología. No obstante, la experiencia de accidentabilidad en las ciudades, como es el caso del DMQ, deja entrever muchos eventos en el sector residencial y a nivel de obras civiles.

> Si bien, por su presencia y connotación los accidentes mayores ocurridos son los que mayor visibilidad y los que han llamado la atención de autoridades locales y medios de comunicación, como son los accidentes aviatorios o accidentes en grandes instalaciones industriales (Estacio, 2021).
>
> Los riesgos tecnológicos son "los daños o pérdidas potenciales que pueden presentarse debido a los eventos mayores generados por el uso y acceso a la tecnología, originados en sucesos antrópicos, naturales, socio naturales y propios de la operación" (UNGRD, 2021).

La mayoría de las iniciativas de gestión de riesgos tecnológicos centran su quehacer a lo interno de las empresas o industria que almacenan o procesan materiales peligrosos. El enfoque clásico en estos casos promueve la elaboración de diagnósticos geoespaciales de riesgos sobre los cuales se instrumentan políticas rigurosas de seguridad y/o protocolos de respuesta ante contingencias, sin embargo, debe reconocerse que comúnmente esos esfuerzos limitan su cobertura a las instalaciones de las empresas y al personal que en ella trabaja, y dejan de lado a las poblaciones que circundan a estos espacios (Liñayo, 2020).

> Pudiera decirse que la catástrofe de Chernobyl ocurrida el 26 de agosto de 1986 marcó un antes y un después en la consideración del riesgo de desastres

de origen tecnológico, y esto se debe a que esa catástrofe demostró que hemos llegado a un punto en el que un accidente industrial puede acarrear consecuencias de magnitud igual o superior a la de un desastre de origen natural (Liñayo, 2020).

La Madurez

La madurez organizacional es una consecuencia del conocimiento sobre la empresa, la experiencia de aprendizaje y de mejora de los resultados, así como de su rendimiento económico y su impacto social.

La madurez organizacional puede medirse a través de:

- **Personas:** La capacidad de realizar una gestión de personal efectiva que garantice que cada colaborador pueda alcanzar sus objetivos de trabajo.
- **Datos:** Medición de la precisión, fiabilidad y disponibilidad de los datos financieros y operativos.
- **Tecnología:** La capacidad de alinear los datos financieros, operativos y de recursos humanos para ofrecer transparencia.

La madurez organizacional es una medida de la preparación y capacidad de una organización para adaptarse a su entorno y se expresa a través de sus personas, procesos, datos y tecnologías (QuestionPro, 2020).

El modelo de madurez es el grado en el que una compañía asimila o integra buenas prácticas en lo que respecta a la dirección de diversos programas o proyectos. Comprende diversos factores, como herramientas de medición, criterios de evaluación, entre otros. Además, es muy utilizado para realizar y refinar los procesos de desarrollo de software (ESAN Graduate Schoolof Business, 2022).

El CMM describe un marco teórico de cinco niveles de procesos cada vez más organizados y sistemáticamente más maduros. Según (Uxbi. 2022). Menciona que, de este modo, la clave es identificar estos niveles, lo que a su vez permitirá señalar en cuál de ellos se encuentra una empresa.

- Nivel inicial: los procesos son desorganizados e incluso pueden llegar a ser caóticos.
- Nivel repetible: se basa en técnicas básicas de gestión de proyectos. Los procesos están definidos y documentados.
- Nivel definido: la compañía tiene su propio proceso de software estándar y cuenta con mayor atención a la documentación, integración y estandarización.

- Nivel administrado: la empresa monitorea y gestiona sus propios procesos gracias a la recolección y análisis de datos.
- Nivel de optimización: los procesos se mejoran de manera constante mediante la supervisión de los procedimientos actuales y la introducción de procesos innovadores.

Al conocer las características de cada uno de estos niveles, es posible identificar cuáles corresponden al modelo actual de la organización. Lo ideal es ubicarse entre los últimos niveles, pues esto significará la madurez de la gestión de cada proyecto y que las prácticas actuales de la compañía sean las adecuadas (ESAN Graduate Schoolof Business, 2022).

Medir constantemente la madurez de los procesos de negocio no es sólo bueno, sino necesario para cualquier empresa, pues esta evaluación es capaz de mostrar de forma más clara dónde están las fallas y cuáles son las oportunidades de mejora de la organización (Garrnet, 2019).

Ventajas de medir el nivel de madurez de los procesos de negocio

- Contribuye a traducir las estrategias de la organización en trabajo realizable.
- Permite la detección temprana de errores.
- Impulsa la mejora continua.
- Optimiza el desempeño de todos los departamentos de la empresa.
- Ayuda a gestionar mejor los cambios y mantener la competitividad.

Cómo evaluar el nivel de madurez en las empresas

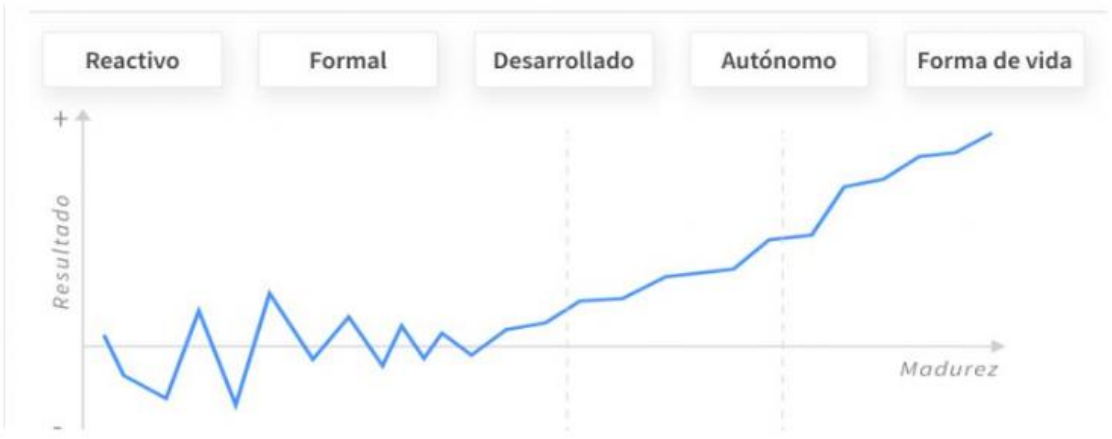


Figura 6. Nivel de madurez en las empresas

Fuente: Caletec

Para ser competitivo hay que mejorar y para mejorar hay que saber cuál es la situación actual y hasta dónde puede llegar la empresa. Un consultor especializado en mejora continua, como Caletec, analizará unos 80 conceptos relacionados con

el nivel de madurez del negocio en sus procesos internos y organización. Según (Caletec, 2018). El estudio ayudará a planificar las inversiones y el esfuerzo de mejora en función de dónde se encuentra sabiendo que podemos discernir varios estados:

- **Reactivo**: solo se realizan acciones de mejora cuando se presenta un problema de calidad en proceso o una reclamación de cliente. En este caso, se suelen aplicar soluciones sin buscar la causa raíz del problema, desaprovechando la oportunidad de solucionar el tema definitivamente.
- **Formal:** se inician actividades de estandarización y mejoras sostenidas, pero no se profundiza.
- **Desarrollado:** equipos de trabajo formados en metodologías y técnicas para la mejora continua y que buscan las causas raíz de los problemas y la sostenibilidad de las mejoras (estandarización, capacitación)
- **Autónomo:** Anticipación a los problemas y planteamiento proactivo para optimizar los procesos y maximizar su eficiencia
- **Forma de vida:** la mejora continua forma parte de la cultura de la empresa. A todos los niveles, cada uno se siente responsable de los procesos, de estudiarlos y de mejorarlos permanentemente

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

El presente proyecto se utilizó un enfoque mixto tanto cuantitativo y cualitativo los cuales permitió alcanzar los objetivos y comprobar la idea a defender, al igual para el análisis de riesgos y realizar el BIA.

En el Enfoque Cuantitativo según Sampieri (2018) menciona que: "Se utiliza la colección y recopilación de datos para poder probar hipótesis basadas en cálculos numéricos y análisis estadístico para formar el comportamiento y comprobar la teoría" (p. 2018). Haciendo referencia al enfoque antes mencionado se recolectó datos medibles y cuantificables los cuales fueron obtenidos luego de realizar el análisis de la encuesta y entrevista realizada al encargado del área tecnología y comunicación, además, se utilizó la medición de parámetros para la variable dependiente, la cual nos permitió la tabulación de los resultados de las encuestas.

El enfoque cualitativo hace referencia a diversas investigaciones, Sampieri (2018) dice que: "se puede hacer uso de recopilación y análisis de datos para clarificar las preguntas de investigación y descubrir nuevos problemas de interpretación" (p. 9). Teniendo como base lo antes mencionado se expresa puntos de vista, interpretación de los hechos mediante gráficas, tomando como punto referencial y puntual las entrevistas y encuestas, las cuales están orientadas a la recopilación de información, mismas que están dirigidas a los beneficiarios directos del proyecto, la obtención de información es característica y propia de la norma ISO 22301 por motivo que se siguió un esquema de preguntas que esta misma norma brinda, se muestran las cualidades del área de tecnología e información en estudio.

3.1.2. Tipo de Investigación

Se utilizó los siguientes tipos de investigaciones:

Investigación aplicada

Según Carvajal (2020) dice que: La finalidad de esta investigación es aplicar directamente la creación de conocimiento a los problemas de la sociedad o del sector productivo. Esta investigación se basa esencialmente en descubrimientos técnicos basados en la exploración fundamental que se ocupa del proceso de unir la teoría y el producto.

En el presente proyecto se detalló las características y propiedades con contenido verídico de los activos tecnológicos que posee la unidad de tecnología, para su análisis y adecuada identificación de medidas importantes. Además, se describió las situaciones y eventos de la Unidad de Tecnología y Comunicación que contribuyen a la propuesta del plan de continuidad del negocio. De la misma manera se aplica la descripción para la toma de acciones, constituir políticas y estrategias. Cabe menciona que este tipo de investigación ayudó a obtener conocimiento con el propósito de reformar un servicio y beneficio para el área antes mencionada.

Investigación de campo

Según Cajal (2020) dice que: La investigación de campo es la recopilación de información fuera del laboratorio o lugar de trabajo. Es decir, los datos necesarios para el estudio se obtuvieron en condiciones reales no controladas. (p. 1).

Se la realizo para identificar el campo de estudio incluso se verifico si el estudio es factible para realizarlo dentro de la institución pública seleccionada. Este estudio se lo realizo en el Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar con la utilización de técnicas para la obtención de información real en el lugar donde se realizan las diferentes operaciones y procesos que están dependientes del Unidad de TIC, la investigación de campo se la realizo con la finalidad de levantar información, diagnosticar, y documentar la investigación con datos verídicos obtenidos por las autoras.

Investigación bibliográfica

La investigación bibliográfica es de gran ayuda para todo tipo de documentos, puesto que se utilizará diferentes fuentes como artículos científicos, tesis, noticias, libros, entrevistas, que se encuentren en repositorios digitales en la red entre otros. Según Montagud (2020) menciona que: La investigación documental o conocida como bibliográfica es el estudio de adquirir, seleccionar, organizar, interpretar,

compilar y analizar la información que es objeto de investigación a partir de fuentes documentales y estas fuentes pueden ser de varios tipos. Este tipo de investigación es una técnica es cualitativa. Para la presente investigación se indago datos de diferentes fuentes verídicas, basándonos en documentos similares sobre el plan de continuidad de negocio, que aplicaban normas y metodologías distintas, nos apoyamos bibliográficamente con la norma ISO 22301del año 2019 la más actual y metodología MAGERIT la cual está enfocada en los riesgos y vulnerabilidades que pueden presentarse en una empresa o institución.

Investigación Explicativa

La investigación explicativa es un tiene una finalidad. Según Lifeder (2020) menciona que: este tipo de indagación es para hallar razones o motivos por los cuales ocurren los hechos del fenómeno estudiado, mediante la observación de las causas y los efectos que existen.

Tomando en cuenta lo anterior se realizó esta investigación, porque se conocerá el proceso de generar información para tener en orden y control de los activos tecnológicos que dicho departamento tiene a su disposición. En el desarrollo del Plan de continuidad del Negocio que se especificara estrategias frente un eventual incidente y los roles de los responsables para acatarlas de manera certera y segura.

3.2. IDEA A DEFENDER

El Plan de continuidad de negocio del área de Tecnología de Información y Comunicación de Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar, ayudara a manejar incidentes y desastres para el fortalecimiento de la disponibilidad de los activos tecnológicos hardware y software.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE LAS VARIABLES

Definición de las variables

El desarrollo de este proyecto se sujeta a dos variables,

Variable independiente: Plan de continuidad del negocio conjuntamente surgirán dimensiones e Indicadores.

Variable dependiente: Disponibilidad de los activos tecnológicos hardware y software.

Operacionalización de las variables

Tabla 12. Variable Independiente

VARIABLE INDEPENDIENTE: Plan de continuidad del negocio				
Definición	**Dimensión**	**Indicadores**	**Técnica**	**Instrumento**
Plan de continuidad del negocio: Está enfocado asegurar la continuidad del negocio, cuando de repente ocurre un incidente inesperado. Este plan lo que intenta es no detener la productividad de la empresa, e intentar que la situación que ha sucedido es ese momento nos afecte lo menos posible.	Inventario de activos tecnológicos, procesos o servicios	Número de activos tecnológicos	ENTREVISTA	CUESTIONARIO
	Gestión de continuidad del negocio	Valoración de Criterio inicial Valoración de Criterio final		
	Valoración de las Cláusulas de norma ISO 22301:2019	Cumplimiento de requisitos para la continuidad del negocio		
	Fases de BCP	Número de fases		
	Análisis de impacto de la organización	Identificación de procesos Nivel de criticidad de los procesos		
	Análisis de Riesgos	Identificación de vulnerabilidades y amenazas Determinación del impacto		

Fuente: Elaboración Propia

Tabla 13. Variable Dependiente

VARIABLE DEPENDIENTE: Disponibilidad de los activos tecnológicos hardware y software

Definición	Dimensión	Indicadores	Técnica	Instrumento
Dependiente: Disponibilidad de los activos tecnológicos hardware y software: Conjunto de equipos tecnológicos que estén un estado operable o funcional.	Amenazas, Riesgos de los activos	Tipos de amenazas, riesgos de los activos	ENTREVISTA	CUESTIONARIO
	Establecimiento de tiempos de recuperación	Prioridad de recuperación de los procesos		

Fuente: Elaboración Propia

3.4. MÉTODOS UTILIZADOS

Se utilizó el siguiente método:

Método de Investigación Acción

Se planifico estrategias para el desarrollo del plan de continuidad del negocio de los activos tecnológicos software, hardware del Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar.

En este proyecto se realizó la debida investigación sobre la utilización de cláusulas establecidas en la de Norma ISO 22301:2019, metodología MAGERIT para el plan de continuidad del negocio para así obtener información de cada elemento tecnológico siendo prácticos, ejerciendo algunas tareas, implicando autorreflexión e investigación y trabajar en los cambios necesarios que permitan su mejoramiento.

3.5. ANÁLISIS ESTADÍSTICO

Población y muestra

Con la finalidad de desarrollar el plan de continuidad del negocio de los activos tecnológicos hardware y software se aplicó las diferentes técnicas e instrumentos como la entrevista estructurada y para ello se realizó una selección no probabilística por conveniencia la cual abarca un total de veintinueve personas las cuales son los directores o jefes de direcciones, jefaturas y coordinaciones incluyendo la unidad de TIC del GAD Municipal de Bolívar.

Censo

Dentro de esta investigación se utilizó el método de censo debido a que no se hizo uso de una fórmula estadística para calcular y obtener la muestra, en vista de que la población a la que se aplicó el instrumento de recolección de datos es pequeña, la cual nos permitió obtener información verídica.

Tabla 14. Población del proyecto de investigación

Fase	Instrumentos	Técnica	Actores
Estudio Inicial	Cuestionario estructurado	Entrevista	Jefe de la unidad de TIC
Levantamiento de información	Hoja de calculo	Documentos Registros	Área de recaudación Secretaria general Obras publicas Departamento financiero Contabilidad Tesorería Talento humano Avalúos
Estado de madurez inicial de continuidad del negocio	Cláusulas de valoración global	Encuesta	Jefe de la unidad de TIC
Recopilación de información sobre el plan de continuidad de negocios	Cuestionario estructurado	Encuesta	Direcciones Jefaturas Coordinaciones
Realización del plan	Documentación normas	Documentos Metodología y procesos	Jefe de la unidad de TIC
Estudio final	Documentos de métodos	Documentos	Jefe de la unidad de TIC

Elaboración Propia.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1. Resultados de encuesta a las direcciones y jefaturas del GAD Municipal del cantón Bolívar.

Resultados entrevista al personal directivo

La entrevista fue realizada al personal directivo, debido a que son las personas que son usuarios que maneja directamente los activos tecnológicos hardware y software, siendo un total de tres personas.

1. **¿Conoce usted sobre el plan de continuidad del negocio?**

Resultados de los Entrevistados: Los entrevistados afirmaron que tienen conocimiento en plan de contingencia y mantenimiento, pero a la hora de un plan de continuidad tenía confundido las definiciones, al igual presentaron planes que están desactualizados desde el 2018.

Tabla 15. Conocimiento del plan de continuidad del negocio.

	Cantidad	Porcentaje
SI	**10**	**34,5%**
NO	**19**	**65,5%**
TOTAL	**29**	**100%**

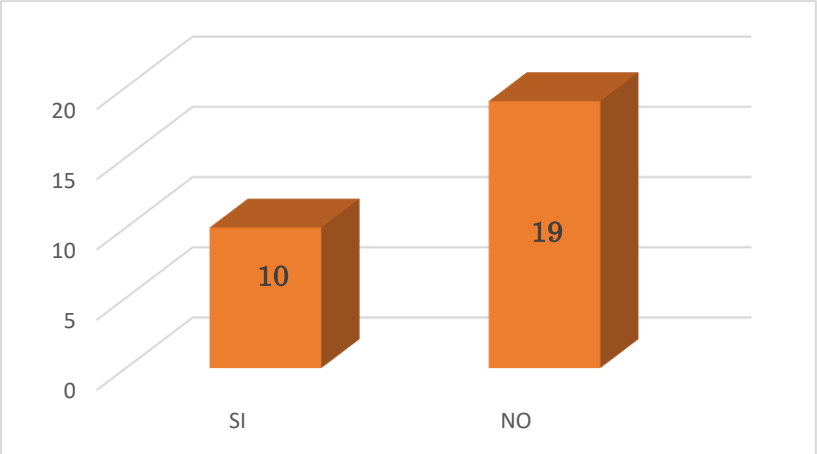


Figura 7. Resultados en forma gráfica

Análisis e Interpretación: El 34,5% del total de encuestados ha manifestado que conoce sobre el plan de continuidad del negocio. Y el 65,5 % Tomando en cuenta que no tenían claro de lo que es un plan de continuidad y sus beneficios. Cabe recalcar que se reforzó con la definición de un plan de continuidad del negocio.

2. **¿Usted considera que es útil un plan de continuidad del negocio con la norma internacional ISO 22301:2019?**

Resultados de los Entrevistados: Tenían en claro sobre las metodologías, hablaron sobre ISO de referencia para una institución pública. Y varios beneficios que fueron nombrados, documentación que debe ser presentada.

Tabla 16. Utilidad del plan de continuidad del negocio.

	Cantidad	Porcentaje
SI	**29**	**100%**
NO	**0**	**0%**
TOTAL	**29**	**100%**

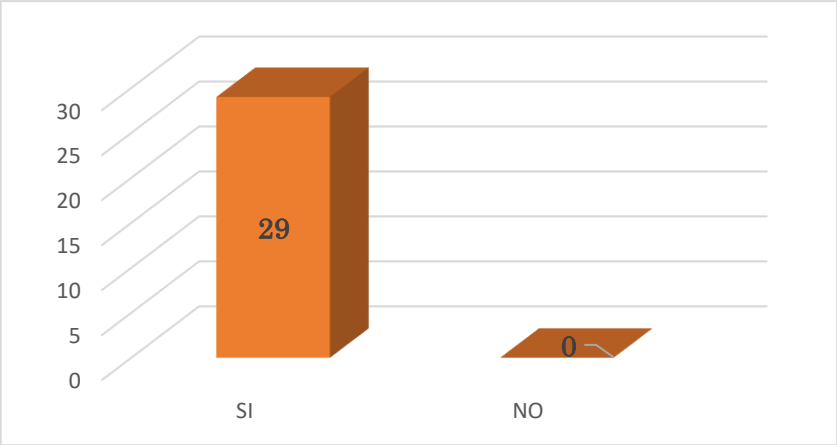


Figura 8. Resultado manera gráfica pregunta 2

Análisis e Interpretación: El 100% del total de los encuestados ha manifestado que considera útil un plan de continuidad del negocio con la norma internacional 22301:2019 para el desempeño de las actividades de la Unidad. Tomando en cuenta que contaban con planes de mantenimiento y contingencia desactualizados.

3. **¿El plan de continuidad del negocio contribuye a la disponibilidad de los activos tecnológicos de hardware y software de la Unidad Tecnológica y Comunicación TIC?**

Tabla 17. El plan de continuidad del negocio contribuye a la disponibilidad.

	Cantidad	Porcentaje
SI	**29**	**100%**
NO	**0**	**0%**
TOTAL	**29**	**100%**

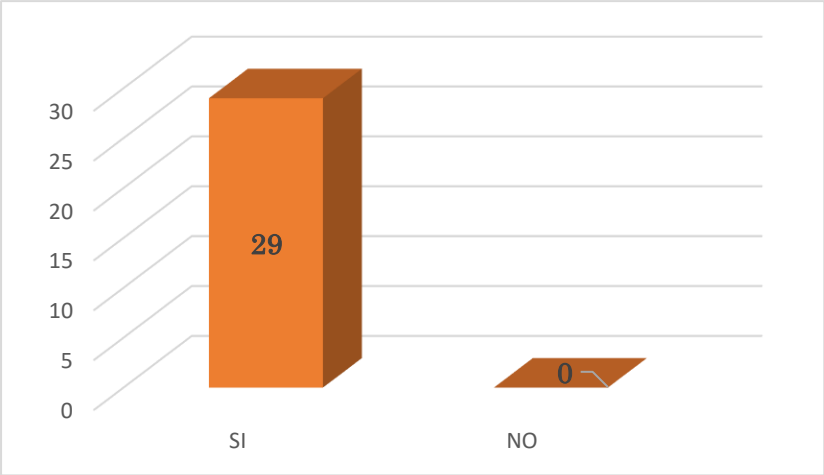


Figura 9. Resultados gráficos pregunta 3

Análisis e Interpretación: El 100% del total de encuestados ha manifestado que el plan de continuidad del negocio contribuye a la disponibilidad de los activos tecnológicos de hardware y software de la Unidad Tecnológica y Comunicación TIC. Tomando en cuenta que existen planes derivados para la disponibilidad de los servicios.

4. **¿Qué riesgos se ha presentado en el GAD Municipal de Bolívar?**

Tabla 18. Riesgos se ha presentado en el GAD Municipal de Bolívar.

	Cantidad	**Porcentaje**
Riesgo financiero	**0**	**0%**
Riesgo ambiental	**0**	**0%**
Riesgo político	**0**	**0%**
Riesgos legales	**0**	**0%**
Riesgos informáticos	**27**	**93,1%**
Otros	**2**	**6,9%**
TOTAL	**29**	**100%**

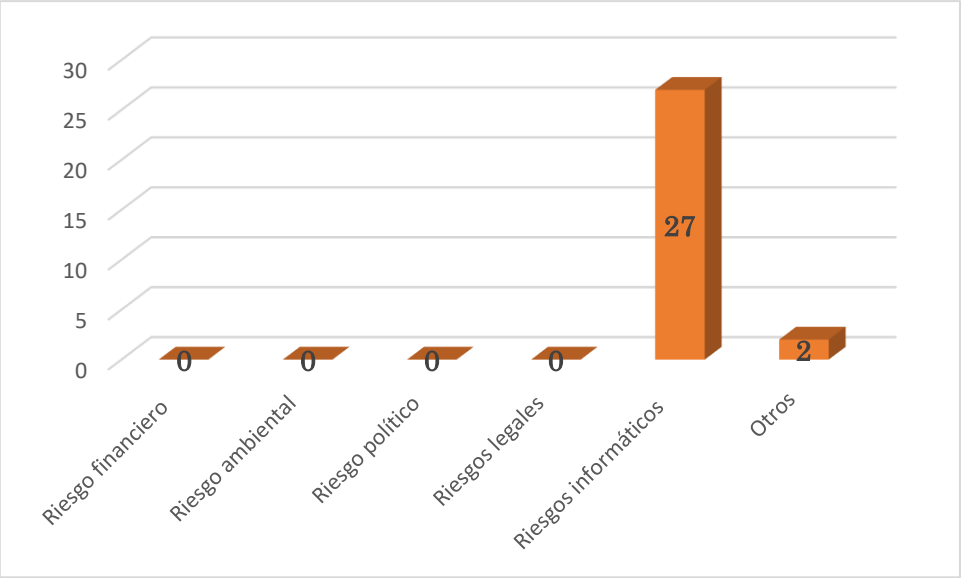


Figura 10. Riesgos presentados en el Gad

Análisis e Interpretación: El 93.1% del total de encuestados ha manifestado que el Qué el riesgo se ha presentado en el GAD Municipal de Bolívar son riesgos informáticos que presenta constantemente, incluso uno de ellos ocasiona la pérdida de un servidor y su información, llevando a esto a la paralización de servicios.

5. **¿Qué tipos de amenazas se ha presentado en el GAD Municipal de Bolívar?**

Tabla 19. Amenazas se ha presentado en el GAD Municipal de Bolívar.

	Cantidad	**Porcentaje**
seguridad informática	**23**	**79,3%**
desastres naturales	**1**	**3,4%**
seguridad física	**5**	**17,2%**
Riesgos legales	**0**	**0%**
Otros	**0**	**0%**
TOTAL	**29**	**100%**

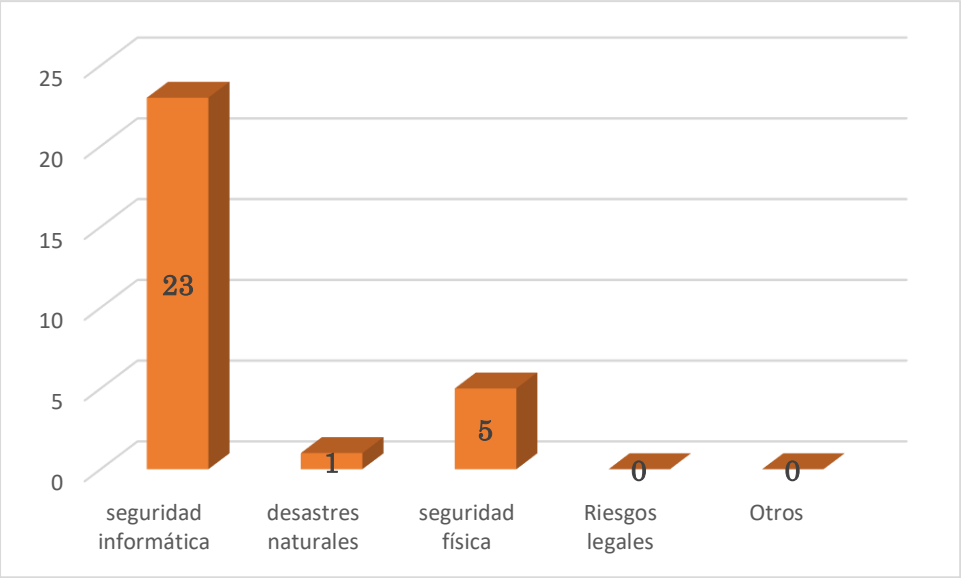


Figura 11. Resultados de amenazas presentadas en el GAD

Análisis e Interpretación: El 79,3% del total de encuestados ha manifestado que el Qué la amenaza se ha presentado en el GAD Municipal de Bolívar son de seguridad informática que presenta constantemente, incluso uno de ellos fue el robo de equipos.

6. **¿Qué tipos de vulnerabilidades en seguridad informática se han presentado en el municipio?**

Tabla 20. Tipos de vulnerabilidades en seguridad informática.

	Cantidad	**Porcentaje**
Mantenimiento de equipos	**27**	**93,1%**
Cableado de instalaciones	**0**	**0%**
Control Interno	**2**	**6,9%**
Otros	**0**	**0%**
TOTAL	**29**	**100%**

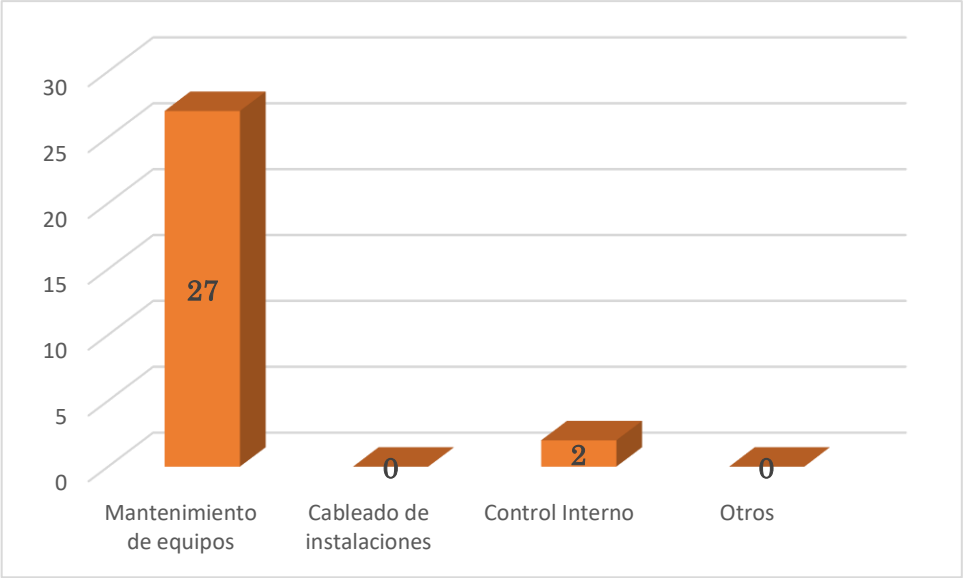


Figura 12. Resultado de vulnerabilidades en seguridad informática

Análisis e Interpretación: El 93,1% del total de los encuestados ha manifestado que el Qué tipos de vulnerabilidades en seguridad informática se han presentado en el municipio son el mantenimiento de equipos que presenta constantemente, incluso uno de ellos fue la falta de medidas preventivas para no tener daños en los equipos.

7. **¿Existe estrategias de recuperación de los procesos críticos frente a una paralización de los activos tecnológicos?**

Tabla 21. Conocimiento del plan de continuidad del negocio.

	Cantidad	Porcentaje
SI	**2**	**6,9%**
NO	**27**	**93,1%**
TOTAL	**29**	**100%**

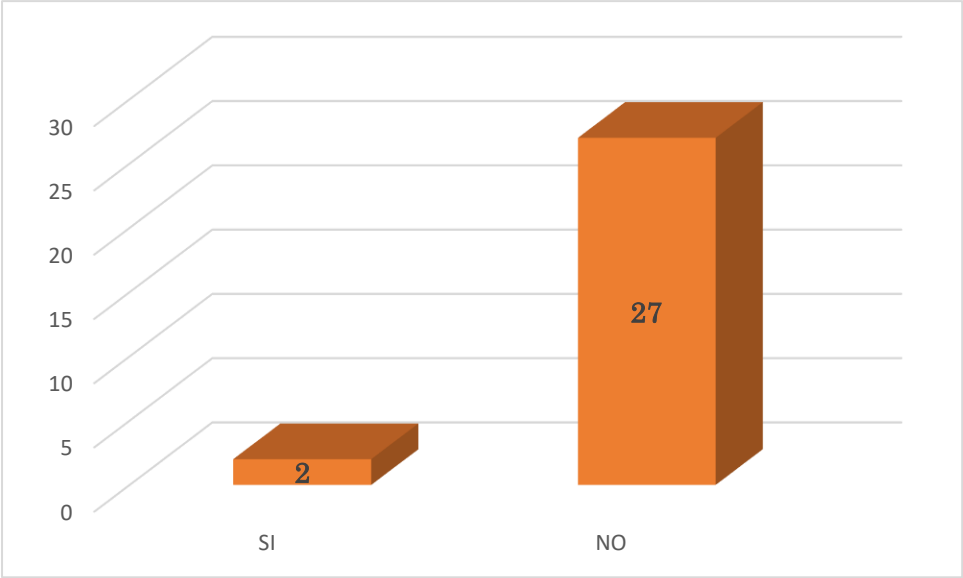


Figura 13. Resultados de recuperación de procesos

8. ¿Durante los últimos 3 años ha existido paralización de los servicios?

Indique las causas por lo que se ha paralizado los servicios

Tabla 22. Paralización de los servicios del municipio.

	Cantidad	Porcentaje
SI	**29**	**100%**
NO	**0**	**0%**
TOTAL	**29**	**100%**

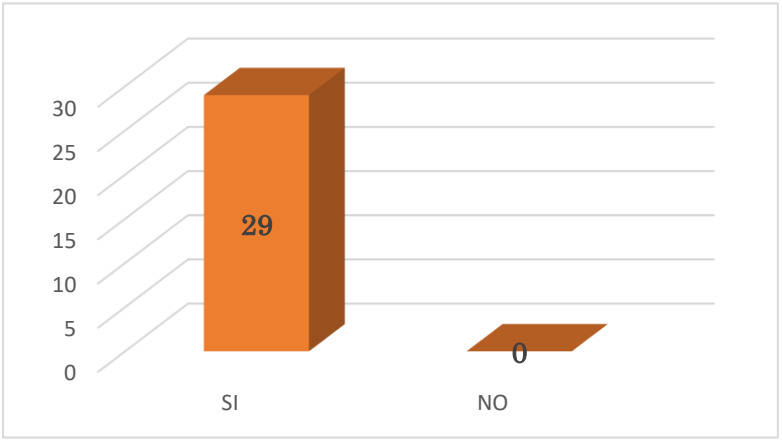


Figura 14. Resultados de recuperación de procesos

Análisis e Interpretación: El 100% del total de encuestados ha manifestado que si existe la paralización de los servicios porque no se encuentra la disponibilidad de cada activo tecnológico.

9. **¿Se realiza simulacros frente a una paralización de activos tecnológicos?**

Cuáles fueron los resultados

Tabla 23. Conocimiento del plan de continuidad del negocio.

	Cantidad	Porcentaje
SI	**29**	**100%**
NO	**0**	**0%**
TOTAL	**29**	**100%**

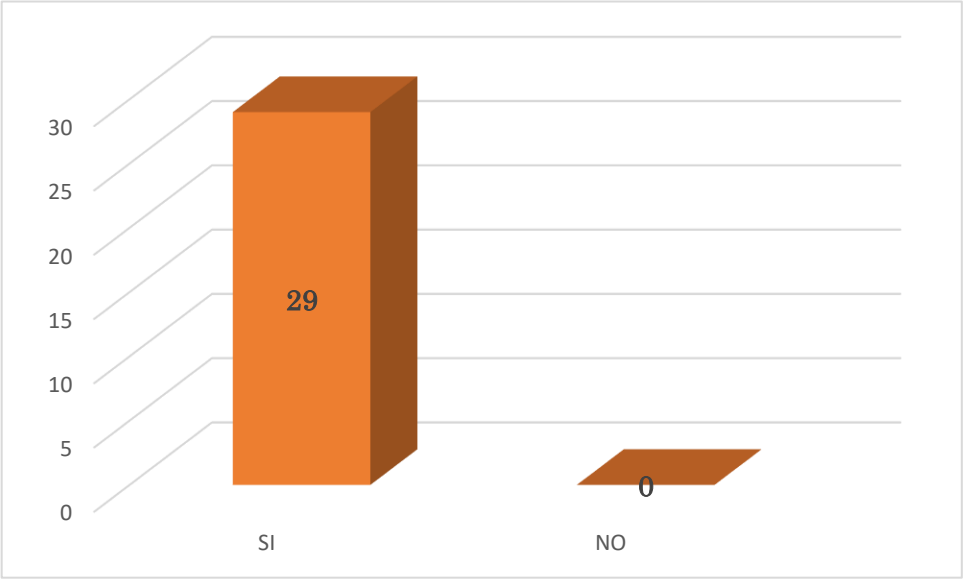


Figura 15. Resultados de la pregunta 8

Análisis e Interpretación: El 100% del total de encuestados ha manifestado que los simulacros se realizan cada 2 años y cada vez que se implementa diferentes activos tecnológicos.

Resultados de la aplicación del plan de continuidad se identificó la siguiente matriz de riesgos

Tabla 24. Tabla de riesgos y el nivel de factor de riesgos

RIESGO	FACTOR DE RIESGO					
	NO	**Muy Bajo**	**Bajo**	**Medio**	**Alto**	**Muy Alto**
Incendio				X		
Deslizamientos	X					
Inundación	X					
Tsunami	X					
Estructuras del Edificio en mal estado	X					
Vientos Fuertes				X		
Robo Común				X		
Vandalismo, daño de equipos y archivos				X		
Faltas, daño de archivos						X
Virus, daño de equipos y archivo				X		
Terremotos, daño de equipos y archivos						X
Acceso no autorizado, filtración de información				X		
Robo de datos						X
Estafa, alteración de información					X	
Otros						

Nota. Elaboración propia de la tabla y el factor de riesgo

4.1.2. Resultados pre, post- propuesta

La norma ISO 22301 provee una herramienta de diagnóstico a modo de cuestionario, que permite llevar a cabo una evaluación inicial para conocer el nivel de gestión de continuidad del negocio dentro de la organización. De esta manera se puede

conocer en qué nivel de madurez se encuentra la empresa en referencia a las acciones tomadas para garantizar la operatividad normal de las actividades.

Los parámetros objeto de la evaluación dentro de la estructura de la norma inician a partir del numeral 4 y finalizan con el numeral 10 y se denominan cláusulas. Cada una de estas cláusulas contiene varios ítems denominados dimensiones que permiten valorar de manera específica los lineamientos establecidos en la norma ISO 22301.

4.1.3. Criterio inicial de cumplimiento de requisitos según ISO 22301

Los valores iniciales obtenidos corresponden al criterio del personal técnico del departamento de TI, en la aplicación del cuestionario.

Tabla 25. Criterios iniciales

CLÁUSULA	CALIFICACIÓN
4. Contexto de la organización	1,31
5. Liderazgo	2,72
6. Planificación	1,89
7. Apoyo	2,06
8. Operación	1,58
9. Evaluación de desempeño 2,02	
10. Mejora	1,83
VALORACIÓN INICIAL GLOBAL	1,92

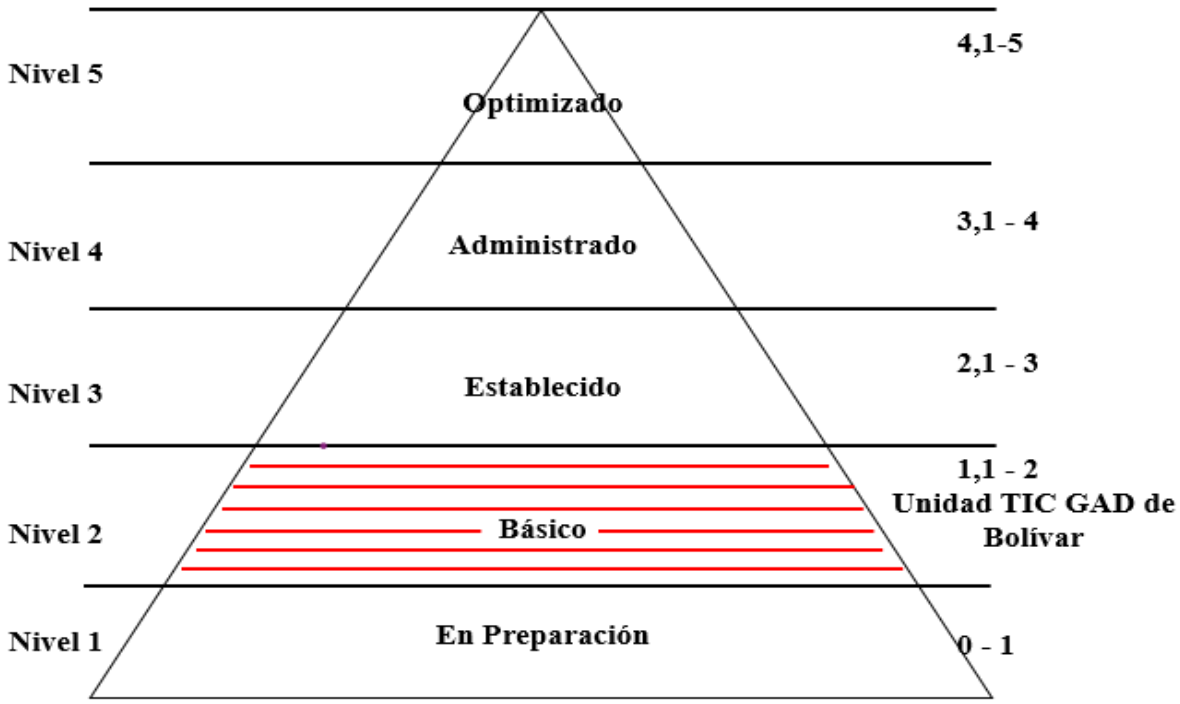
Nota. Elaboración propia. Se muestra la valoración inicial

Para conocer el valor inicial de madurez de la empresa referente a gestión de continuidad del negocio es necesario promediar los valores obtenidos en cada una de las cláusulas correspondientes.

De acuerdo con la valoración global y en base a la Tabla 15, el ara de TIC del GAD Municipal de Bolívar inicialmente tiene un nivel básico de gestión de continuidad del

negocio. Esto significa que maneja contingencias básicas para hacer frente a incidentes de seguridad. En la Figura 15, se puede apreciar el resultado

Figura 15. Nivel de madures del área de tics del GAD de Bolívar



Fuente: Elaboración propia

4.1.4. Criterio final de cumplimiento de requisitos según ISO 22301

Posterior a la elaboración de la propuesta del BCP el área TIC del GAD Municipal de Bolívar, se aplicó nuevamente la herramienta de diagnóstico mediante un cuestionario para conocer el nivel de gestión de continuidad alcanzado dentro de la organización. Los valores finales obtenidos corresponden al criterio del personal técnico del departamento de TI, en la aplicación del cuestionario. Estos valores obtenidos del cuestionario por cada ítem tienen una valoración.

Después de haber realizado la resolución de preguntas establecidas en la Norma ISO 22301 lo cual dio como resultado los valores, que nos indican en qué estado se encuentran al inicio, para conocer las preguntas de cada ítem. (Ver anexo N° 6)

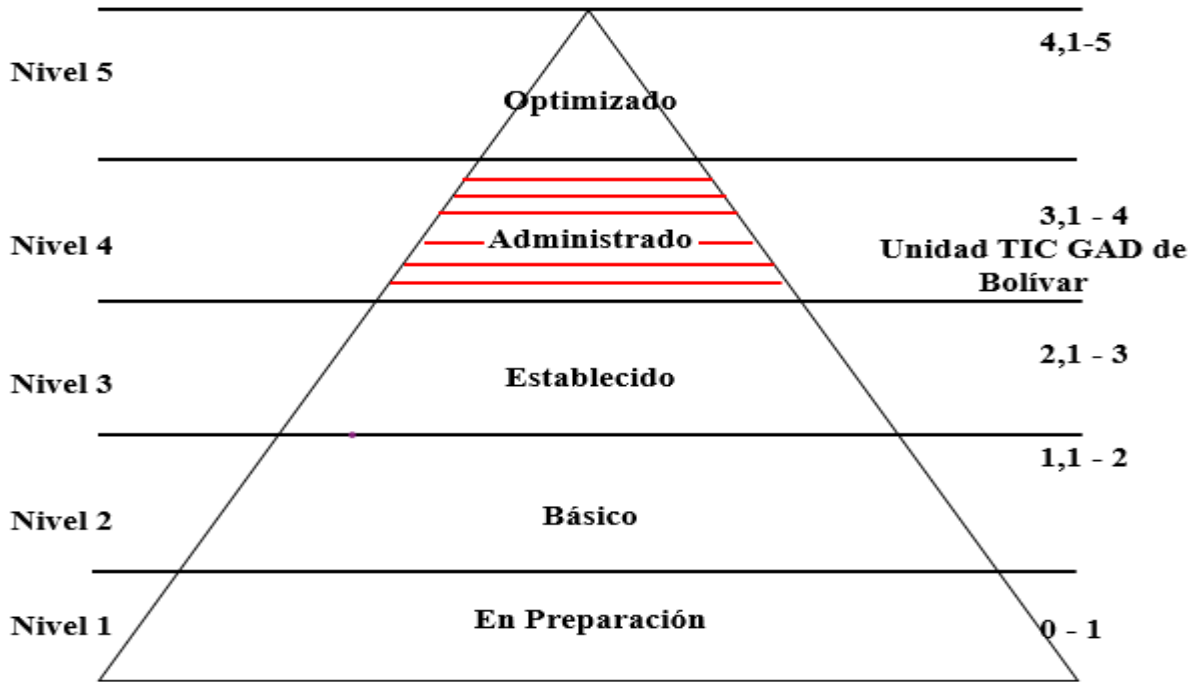
En la Tabla 12, se muestra el resumen de la valoración individual de las cláusulas y el valor final promedio obtenido.

Tabla 26. Clasificación de la valoración individual

CLÁUSULA	CALIFICACIÓN
4. Contexto de la organización	3,94
5. Liderazgo	4,28
6. Planificación	4,17
7. Apoyo	4
8. Operación	4,25
9. Evaluación de desempeño	4,03
10. Mejora	4
VALORACIÓN FINAL GLOBAL	4,09

Nota. Elaboración propia de la tabla de resultados de la valoración individual

Figura 16. Nivel de madurez en el cual se encuentra el GAD de Bolívar



Nota. Elaboración Propia para mostrar a que estado llego el nivel de madures del plan de continuidad de negocios.

4.2. DISCUSIÓN

Iniciando con el problema planteado en esta investigación sobre el actual plan de continuidad del negocio de la Unidad de Tecnología y Comunicación (TIC) es inadecuado con las necesidades de esta, lo que provoca un deficiente manejo de incidentes y desastres dejando en riesgo la disponibilidad de la institución por consiguiente se procedió al desarrollo de un Plan de continuidad del negocio de los activos tecnológicos hardware y software, para ello se detalló un objetivo general y 4 específicos de manera que se concluyó con todas las fases de la investigación. El enfoque que se conservó fue mixto el cual nos permitió levantar información sobre la infraestructura tecnológica, roles y responsabilidades del personal directivo, además se realizó el análisis de riesgos y el BIA que nos ayudaron para determinar activos críticos y el tiempo tolerante máximo, también se pudo detallar las 5 fases correspondientes al BCP de acuerdo con la norma internacional ISO 22301:2019. Finalizando se estableció las estrategias de los activos tecnológicos hardware y software que permitan enfrentar a un incidente y desastres.

Sobre la base de los resultados obtenidos se puede comprobar de la aprobación a la idea defender donde se menciona que si el BCP ayudara a manejar incidentes y desastres para el fortalecimiento de la disponibilidad de los activos tecnológicos hardware y software

Como se ha evidenciado en las tesis elaboradas por (Araujo, 2019) y (Pincay, 2021) el desarrollo de un Plan de continuidad del negocio es importante en una institución porque facilita manejar incidentes y desastres identificando los posibles riesgos proporcionando la disponibilidad de esta, cabe recalcar que Araujo utilizo metodología con la ISO 27005 e ISO 22301:2012 en las 5 fases de su investigación la cual la permitió identificar los principales procesos técnicos, riesgos e interacciones y amenazas que enfrentan la entidad, en el caso de Pincay utilizo la nueva versión con cambios en su estructura, cabe mencionar que se realizó con la aplicación de la norma ISO 22301:2019, como el caso de (Díaz ,2022)la propuesta de un plan de continuidad la cual hace uso de la metodología MAGERIT para el análisis de riesgos tomando en cuenta confidencialidad, disponibilidad e integridad de la seguridad de la información y la norma internacional ISO 22301: 2019, utilizando sus principios y prácticas para la gestión de continuidad, asegurando la disponibilidad con 3 puntos que ofrece el BCP: OPERAR, MANTENER Y RESPONDER.

Pero a diferencia del trabajo mencionado se adaptado el ciclo PDCA (PLAN- DO-CHECK-ACT), donde se apoyó para conocer el nivel de gestión de continuidad del negocio en el municipio, para ello se evidencia el nivel de madurez pre propuesta aplicando las cláusulas de la norma ISO 22301:2019 evaluadas al Jefe de la Unidad de TIC resultante 1,92 encontrándose en un nivel 2(Básico), luego con la propuesta del BCP, se realizó un post propuesta el cual tiene como valor final 4,09 que se encontraría en un nivel 4 (administrado).

Es evidente la aplicación de diferentes metodologías y cada una de ellas aporta para la continuidad del negocio. A diferencia de (Ati, 2018) menciona que el plan de recuperación de desastre y continuidad del negocio está basado en ITIL, COBIT, tomamos en cuenta y realizamos la comparativa con diferentes metodologías para la cual se evidencio que se concuerda con el uso de la norma ISO 22301:2019 y MAGERIT, que para empezar se debe realizar un estudio o el levantamiento de información y se procedió a esta sugerencia para conocer la situación actual de la

Unidad de TIC, identificando toda la infraestructura tecnológica, servicios que presta, roles y responsabilidades del personal directivo.

4.2.1. Establecer los servicios críticos y mantenerlos operativos frente a un evento de vulnerabilidad.

Frente a los activos críticos realizamos un análisis de impacto del negocio (BIA) considerando los tiempos de recuperación o RTO, es decir el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. También revisamos el grado de dependencia de los datos o RPO, es decir el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de respaldos de la organización, para conocer cuáles son los servicios críticos y los tiempos de recuperación (Ver anexo N° 5).

A continuación, se muestra la tabla 17 que indica el nivel de valoración mediante cláusulas las cuales están establecidas en la norma ISO 22301.

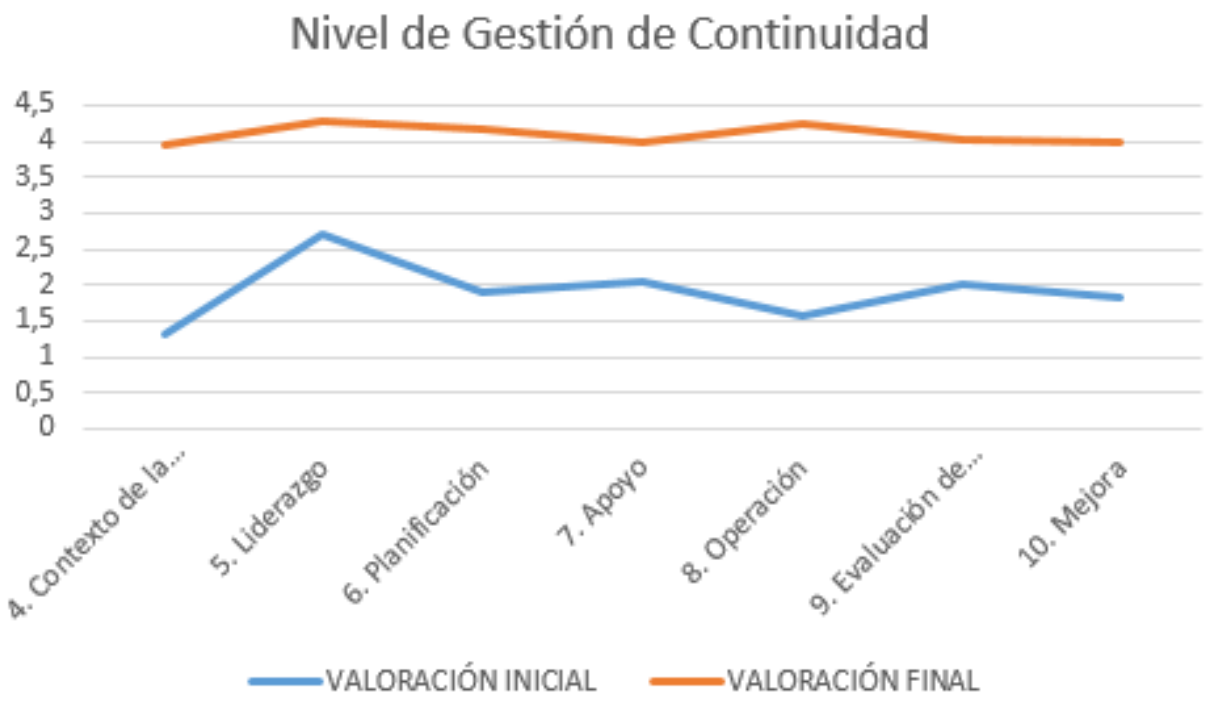
Tabla 27. Nivel de valoración según el plan de continuidad.

CLÁUSULA	VALORACIÓN INICIAL	VALORACIÓN FINAL
4. Contexto de la organización	1,31	3,94
5. Liderazgo	2,72	4,28
6. Planificación	1,89	4,17
7. Apoyo	2,06	4
8. Operación	1,58	4,25
9. Evaluación de desempeño	2,02	4,03
10. Mejora	1,83	4

Nota. Elaboración propia

Estos valores fueron obtenidos después de haber realizado la resolución de preguntas establecidas en la Norma ISO 22301 lo cual dio como resultado los valores de la tabla anterior. (Ver anexo N° 6) para conocer las preguntas de cada ítem.

Figura 17. Apreciación grafica de la valoración del nivel de gestión de continuidad.



Nota. El grafico lineal muestra los resultados de la valoración sobre el nivel de continuidad. Elaboración propia

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se obtuvo cumplimiento del objetivo general referente a la elaboración del plan de continuidad del negocio de los activos tecnológicos hardware y software para el área de Tecnología y Comunicación TIC del GAD Municipal del Cantón Bolívar, usando la norma ISO 22301:2019 la cual que está orientada a la continuidad del negocio y se empleó la metodología Magerit enfocada a la gestión de riesgos de los activos tecnológicos.
- La investigación esta fundamenta bibliográficamente mediante fuentes primarias, libros, revistas, repositorios y medios virtuales incluido la metodología MAGERIT e ISO 22301en sus versiones más actuales las cuales permitieron establecer los procesos de continuidad y gestionar los riesgos que pueden ocurrir de manera imprevista o por error humano entro del área de tecnología y comunicaciones y es de gran importancia, por motivo que la institución estará preparada para cualquier eventualidad en la recuperación de información y así mantener la operatividad de los sistemas y servicios.
- A través de la identificación de factores como riesgos, amenazas y vulnerabilidades que puedan afectar los activos tecnológicos hardware y software es importante determinar varias medidas ante incidentes y posibles desastres que se puedan presentar en la institución de manera que las estrategias establecidas estén acorde a la realidad que presenta la organización y esta sepa responder en los tiempos establecidos.
- En la identificación de los puntos críticos de los activos tecnológicos se conoce cuáles son los activos a los que se debe priorizar la recuperación

- en el menor tiempo posible para evitar paralización de los servicios que presta la institución.
- Mediante la metodología MAGERIT se puede analizar el impacto que puede tener para la empresa, la violación de la seguridad, la identificación de las amenazas que afectan la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.
- Finalmente se realizó una pre y post propuesta aplicando las cláusulas de la normativa ISO 2230 las cuales nos ayudó a identificar el nivel de madurez en el que se encuentra la unidad de TIC del GAD de Bolívar

5.2. RECOMENDACIONES

Finalizado el proceso de investigación, y contando con un conocimiento sobre la estructura y procesos de la empresa, se pone en consideración lo siguiente:

- Es importante tomar en cuenta que la presente investigación está elaborada para un periodo definido y para seguir usándola en otros periodos futuros deberá ser actualizada y comprender las nuevas adquisiciones de los activos tecnológicos hardware y software que posea la institución y de esta manera recuperar la información según lo establecido en el plan.

- Se debe verificar que el plan cuente con buenos procesos de recuperación eficaces para salvaguardar la información de la institución y estar usando las metodologías correctas con las versiones más actuales posibles.

- Tener actualizado la lista de activos que posea la empresa o área en cuestión para así identificar los procesos y acciones a ejecutar para recuperar y salvaguardar la información en tiempos establecidos para evitar interrupciones de los servicios que presta.

- En el plan de continuidad de negocios se debe de tener bien claro los conceptos de riesgos, amenazas y vulnerabilidades que se puedan

presentar en el GAD Municipal de Bolívar para poder identificarlos y actuar de manera precisa en el menor tiempo posible.

- Seguir los lineamientos de la metodología MAGERIT, los cuales son la gestión de riesgos y su clasificación en errores humanos, desastres naturales, desastres de origen industrial, errores intencionados y no intencionados, ataques de diferentes tipos entre otros

VI. REFERENCIAS BIBLIOGRÁFICAS

Araujo, G. (2019*). "Propuesta de un Plan de continuidad del negocio para una entidad pública del Ecuador"*. [Tesis de Maestría, Universidad Técnica de Ambato]. Repositorio Institucional – Universidad Técnica de Ambato.

Ati, T. (2018). *DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO BASADO EN COBIT, ITIL Y DE ACUERDO A LA NORMA ISO 22301, PARA EL CENTRO DE PROCESAMIENTO DE DATOS (CPD) DE LA CARRERA DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO, CAMPUS SUR.* [Tesis de Grado, Universidad Politécnica Salesiana]. Repositorio Institucional de la universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/15904/1/UPS-ST003686.pdf

Blockbit. (2020). ¿Qué es alta disponibilidad? https://www.blockbit.com/es/blog/que-es-alta-disponibilidad/

Cabrejos, R. (2020). *INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC. Perú.* [Tesis de Grado, Universidad Señor de Sipán]. https://repositorio.uss.edu.pe/handle/20.500.12802/7573

Caletec, (2018). Cómo evaluar el nivel de madurez en las empresas. https://www.caletec.com/mejora-continua/como-evaluar-el-nivel-de-madurez-en-las-empresas/

Ciber Seguridad Industrial. (2021). Escenarios de riesgos tecnológicos que pueden afectar a su seguridad operacional. https://www.cci-

es.org/escenarios-de-riesgos-tecnologicos-que-pueden-afectar-a-su-seguridad-operacional/

Conrado G, (2019). *Calidad, gestion de la calidad, gestion de procesos, gestion del cambio, nivel de madurez, pensamiento analitico, pensamiento sistemico, sistemas de gestion, sistemas integrados de gestion*. https://gamontqm.com/2019/01/16/nivel-de-madurez-sg/

Días, P. (2022). *PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) APLICADO AL DEPARTAMENTO DE TI DE LA EMPRESA DE SOLUCIONES TECNOLÓGICAS TELECOMSEC*. [Tesis de Maestría, Universidad Técnica de Ambato]. Repositorio Institucional – Universidad Técnica de Ambato.

Disaster Recovery Journal (2022). El Plan de Continuidad De Negocio. https://drjenespanol.com/recursos/el-plan-de-continuidad-del-negocio/

Egúsquiza Cáceres, H., & Kong Ramos, C. (2017). *Implementación del modelo de gestión de continuidad de servicios TI basado en ITIL v3. Lima: Universidad Ciencias Aplicadas.* [Tesis de Grado, Universidad Peruana de Ciencias Aplicadas (UPC)]. https://repositorioacademico.upc.edu.pe/handle/10757/622506

ESAN Graduate Schoolof Business. (2022). ¿En qué nivel de madurez se encuentra tu organización? https://www.esan.edu.pe/conexion-esan/en-que-nivel-de-madurez-se-encuentra-tu-organizacion

Estacio, J. (2021). Los riesgos tecnológicos en el DMQ: la paradoja del desarrollo urbano y el síndrome de nuevos escenarios de riesgos y desastres. https://www.flacsoandes.edu.ec/web/imagesFTP/1218664438.Ponencia_final_de_Jairo_Estacio.pdf

Ferruzola, E. Duchimaza, J. Ramos, J. y Lindao, Maria. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. CTU Científica Y tecnológica UPSE. https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/429

Garnet. (2019). ¿Por qué medir el nivel de madurez de los procesos en tu empresa? https://www.gb-advisors.com/es/medir-nivel-de-madurez-procesos-empresa/

Ghannam, M. Z. (2017). *Challenges and Opportunities of Having an IT Disaster Recovery Plan. Umeå: Umeå University.* [Tesis de Grado, Umea University]. http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1117263&dswid=-5694

Gutierrez. (2022). DISEÑO DEL PLAN DE CONTINUIDAD DE NEGOCIO APLICADO A SEGURIDAD DE INFORMACIÓN EN PYME INTERVISIÓN DE GUAYAQUIL. [Tesis de Grado Universidad Técnica Salesiana]. https://dspace.ups.edu.ec/bitstream/123456789/22136/1/UPS-GT003667.pdf

Ibukunoluwa Akinbola. (2018). *A Step towards Resilience, Creating a Business Continuity Plan for WhiteRock Finland KY.* [Tesis de Grado, Laurea University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/143538/Thesis%20Deborah%20Akinb%20ola.pdf?sequence=1

*I*mbaquingo, D., Pusdá, M., & Jacomé, J. (2016). *Fundamentos de Auditoría Informática basada en riesgos*. [Tesis de Maestría, Universidad Técnica de Ambato]. Repositorio Institucional – Universidad Técnica de Ambato.

Instituto Distrital de Gestión de Riesgos y Cambio Climático. (2021). Caracterización General del Escenario de Riesgo por Fenómenos de Origen Tecnológico en Bogotá. https://www.idiger.gov.co/rtecnologico

ISOTools. (2019). *Punto de Recuperación Objetivo (RPO). Análisis de partida ante una contingencia de continuidad del negocio.* https://www.isotools.org/2019/07/16/punto-recuperacion-objetivo-rto-analisispartida-ante-una-contingencia-de-continuidad-negocio/

Liñayo, A. (2020). IDENTIFICACIÓN Y TRATAMIENTO DEL RIESGO TECNOLÓGICO URBANO DE LA CIUDAD DE MÉRIDA (VENEZUELA).

https://www.eird.org/plataforma-tematica-riesgo-urbano/recopilacion-de-articulos/alejandro-linayo.pdf

Machicao, S. (2019). *Análisis de riesgo y políticas de seguridad de información de la Oficina de Tecnologías de Información (OTI) – UNA Puno 2018.* [Tesis de Maestría, Universidad Nacional del Altiplano. Escuela de Posgrado]. https://renati.sunedu.gob.pe/handle/sunedu/3223391

Ministerio de Hacienda y Administraciones Públicas, (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

Olarte, A. (2016). Propuesta metodológica para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano bajo el enfoque de la norma ISO 22301:2012. Signos, 8(1), 31 - 44. https://doi.org/10.15332/s2145-1389.2016.0001.02

Orellana, P. (2020). *Control de Calidad. https://economipedia.com/definiciones/control-de-calidad.html*

Ortiz, S. (2019). Hackers lanzaron ofensiv global para atacar webs estatales. Recuperado de https://www.elcomercio.com/actualidad/hackers-ofensiva-globalataqueecuador.html

Patiño, S. (2019). Inteligencia Militar. Recuperado de https://www.eluniverso.com/noticias/2019/04/12/nota/7281890/exjefeinteligenciamilit ar-recomienda-gobierno-fusion-sus-sistemas

Pincay, J. (2021). *TEMA DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO BASADO EN LA NORMA ISO 22301, EN LA EMPRESA "CONSTRUPROYEC S.A.".* [Tesis de Grado, Universidad de Guayaquil]. Repositorio Institucional-Universidad de Guayaquil

QuestionPro. (2020). Madurez y claridad organizacional: Qué es, niveles y cómo impulsarla.

Rázuri, A. (2019). *Desarrollo de un Sistema de Gestión de Continuidad de Negocio en una entidad financiera, basado en la ISO 22301*. [Tesis de Grado, Universidad Nacional Mayor de San Marcos]. Repositorio Institucional–Universidad Nacional Mayor de San Marcos

Sampieri, R. (2018). Metodología de la Investigación: las rutas cuantitativa, cualitativa y mixta. McGRAW-HILL

Santa María, W. (2020). *Plan para reducir los riesgos operativos de Tecnologías de la Información basada en Metodología MAGERIT en la caja Piura de la ciudad de Chiclayo. Chiclayo.* https://repositorio.udl.edu.pe/xmlui/handle/UDL/413

Segovia, F. (2017). *Developing a Framework for Business Continuity Management within Local Government.* [Tesis de Grado, University of Wollongong]. https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1298&context=thesis1

Toro, R. (2021). Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

UNGRD. Unidad Nacional Para la Gestión del riesgo de Desastre Colombia. (2018). https://www.idiger.gov.co/documents/220605/308252/Escenario+de+Riesgo+Tecnológico.pdf/35625b10-f60b-431e-92d1-7eb6951e9cd0

UNGRID, (2021). Caracterización general del escenario de riesgo por eventos de Origen Tecnológico https://rionegro.gov.co/wp-content/uploads/2021/05/Capitulo-6-Caracterizacion-escenario-riesgo-tecnologico.pdf

Unir. (2021). Disponibilidad en seguridad informática: ¿en qué consiste este término? [Universidad Internacional de la Roja].

https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/#:~:text=La%20disponibilidad%20de%20la%20información,los%20individuos%20o%20personas%20autorizadas.

Uxbi. (2022). Niveles de madurez empresarial ¿Sabes en qué etapa está tu empresa? https://www.uxbi.mx/2022/04/04/niveles-de-madurez-empresarial-sabes-en-que-etapa-esta-tu-empresa/#:~:text=Los%20niveles%20de%20madurez%20empresarial,para%20determinar%20esta%20 "Etapa"

Vallery, Z. (2019). *AWARENESS AND IMPORTANCE OF DEVELOPING BUSINESS CONTINUITY PLANS FOR DISASTER RISKS BY COMPANIES AT BAYHEAD*. [Trabajo Final, University of the Free State]. Repositorio Institucional- University of the Free State

Vásquez, S. (2018). Sercop denuncia vulneración del Sistema Nacional de Contratación Pública. Recuperado de https://www.eltelegrafo.com.ec/noticias/informacion/1/sercop-denunciavulneracion- delsistema-nacional-de-contratacion-publica

Yufra, A. (2018). *IMPACTO E IMPLEMENTACIÓN DEL MODELO DE CONTINUIDAD DE SERVICIO DE MESA DE AYUDA EN UN TERMINAL PORTUARIO DEL CALLAO*. [Tesis de Grado, Universidad Usil]. http://repositorio.usil.edu.pe/bitstream/USIL/8841/1/2018_Yufra-Tejerina.pdf

Zapata, C. (2020). *Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A*. [Tesis de Grado, Universidad de la Fuerzas Armadas]. Repositorio Institucional- Universidad de la Fuerzas Armadas (Repositorio DSpace)

VII. ANEXOS

Anexo 1. Acta de sustentación de Predefensa del TIC

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

ACTA

DE LA SUSTENTACIÓN ORAL DE LA PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

ESTUDIANTE:	HURTADO RODRIGUEZ JAZMIN ESTEFANIA	**CÉDULA DE IDENTIDAD:**	0401900485
PERIODO ACADÉMICO:	2022B		
PRESIDENTE TRIBUNAL	MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ	**DOCENTE TUTOR:**	MSC. CARLITOS ALBERTO GUANO CÁRDENAS
DOCENTE:	MSC. JORGE HUMBERTO MIRANDA REALPE		
TEMA DEL TIC:	Plan de continuidad del negocio de los activos tecnológicos hardware y software		

No.	CATEGORÍA	Evaluación cuantitativa	OBSERVACIONES Y RECOMENDACIONES
1	PROBLEMA - OBJETIVOS	8,00	
2	FUNDAMENTACIÓN TEÓRICA	8,00	
3	METODOLOGÍA	8,00	Quitar el muestreo del documento en tal caso colocar censo a las 29 personas
4	RESULTADOS	8,00	
5	DISCUSIÓN	8,00	
6	CONCLUSIONES Y RECOMENDACIONES	8,00	
7	DEFENSA, ARGUMENTACIÓN Y VOCABULARIO PROFESIONAL	8,00	Acoger las recomendaciones del tribunal, acudir a las reuniones con los integrantes del tribunal
8	FORMATO, ORGANIZACIÓN Y CALIDAD DE LA INFORMACIÓN	8,00	Revisar el documento, formatos, errores ortográficos y otros relacionados

Obteniendo una nota de: 8,00 Por lo tanto, **APRUEBA** ; debiendo el o los investigadores acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el miércoles, 15 de febrero de 2023

MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
PRESIDENTE TRIBUNAL

MSC. CARLITOS ALBERTO GUANO CÁRDENAS
DOCENTE TUTOR

MSC. JORGE HUMBERTO MIRANDA REALPE
DOCENTE

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

ACTA

DE LA SUSTENTACIÓN ORAL DE LA PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

ESTUDIANTE:	PASPUEL PUSDA LUPE FERNANDA	**CÉDULA DE IDENTIDAD:**	0450026323
PERIODO ACADÉMICO:	2022B		
PRESIDENTE TRIBUNAL	MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ	**DOCENTE TUTOR:**	MSC. CARLITOS ALBERTO GUANO CÁRDENAS
DOCENTE:	MSC. JORGE HUMBERTO MIRANDA REALPE		
TEMA DEL TIC:	Plan de continuidad del negocio de los activos tecnológicos hardware y software		

No.	CATEGORÍA	Evaluación cuantitativa	OBSERVACIONES Y RECOMENDACIONES
1	PROBLEMA - OBJETIVOS	8,00	
2	FUNDAMENTACIÓN TEÓRICA	8,00	
3	METODOLOGÍA	8,00	Quitar el muestreo del documento en tal caso colocar censo a las 29 personas
4	RESULTADOS	8,00	
5	DISCUSIÓN	8,00	
6	CONCLUSIONES Y RECOMENDACIONES	8,00	
7	DEFENSA, ARGUMENTACIÓN Y VOCABULARIO PROFESIONAL	8,00	Acoger las recomendaciones del tribunal, acudir a las reuniones con los integrantes del tribunal
8	FORMATO, ORGANIZACIÓN Y CALIDAD DE LA INFORMACIÓN	8,00	Revisar el documento, formatos, errores ortográficos y otros relacionados

Obteniendo una nota de: 8,00 Por lo tanto, **APRUEBA** : debiendo el o los investigadores acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el miércoles, 15 de febrero de 2023

MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
PRESIDENTE TRIBUNAL

MSC. CARLITOS ALBERTO GUANO CÁRDENAS
DOCENTE TUTOR

MSC. JORGE HUMBERTO MIRANDA REALPE
DOCENTE

Anexo 2. Certificado de abstract por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Hurtado Rodriguez Jazmin Estefania y Paspuel Pusda Lupe Fernanda

DATE: 23 de febrero de 2023

TOPIC: "Plan de continuidad del negocio de los activos tecnológicos hardware y software"

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ■	GOOD: 1Vera Játiva Edwin Andrés,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: **Hurtado Rodríguez Jazmín Estefanía** y **Paspuel Pusda Lupe Fernanda**
Fecha de recepción del abstract: 23 de febrero de 2023

Fecha de entrega del informe: 23 de febrero de 2023

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9, por lo cual se validad dicho trabajo.

Atentamente

EDISON BOANERGES PEÑAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3. Informe de anti-plagio (Turnitin)

Plan de Continuidad del negocio Hurtado - Paspuel

INFORME DE ORIGINALIDAD

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

FUENTES PRIMARIAS

1	repositorio.umb.edu.pe:8080 Fuente de Internet	2%

Excluir citas	Activo	Excluir coincidencias	< 2%
Excluir bibliografía	Activo		

Anexo 4. Documento que acredita que el municipio dará la información

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN BOLÍVAR
Administración 2019 - 2023

Oficio No.150-2021-GAD-BOLIVAR-SISTEMAS

Bolívar, 12 de julio de 2021

Srtas. Jazmín Hurtado y Fernanda Paspuel.
Estudiantes de la carreta de computación de laUPEC
Presente.-

Según a la sumilla de parte del Sr. Alcalde con fecha de 08 de julio de 2021 en el documento entregado por parte de las estudiantes de la UPEC mencionadas anteriormente con respecto a que solicitan desarrollar su Trabajo de Integración Curricular con el tema: Plan de Continuidad de Operaciones de los activos tecnológicos hardware y software. En donde solicitan la información necesaria para completar su trabajo curricular.

Por tal motivo, en calidad de Jefe de la Unidad de Tecnología de la Información y Comunicación facilitare toda la información necesaria para que las Srtas. cumplan con este requisito indispensable para su titulación.

Sin más que referir, les deseo un excelente día.

Atentamente

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN BOLÍVAR CARCHI - ECUADOR
SISTEMAS

Ing. Andrés Villarruel
JEFE DE LA UNIDAD DE TECNOLOGIA Y COMUNICACIÓN

Dirección García Moreno y Egas esq.
(06) 2 287384 / 119 / 218
www.municipiobolivar.gob.ec
Bolívar - Carchi - Ecuador

Anexo 5. Aceptación del Municipio para realizar el plan de continuidad

Educamos para transformar el mundo

Tulcán, 08 de julio de 2021

Ing.

Livardo Benalcázar

ALCALDE DEL CANTÓN BOLÍVAR

Presente. -

GADM. DEL CANTÓN Bolívar

USD. 0.50

De mi consideración:

Reciba un atento y cordial saludo a la vez que les deseamos éxitos en las funciones que usted acertadamente desempeña.

Por medio del presente me permito solicitar información necesaria correspondiente al área de sistemas para el desarrollo del Trabajo de Integración Curricular con el Tema: Plan de Continuidad de operaciones de los activos tecnológicos hardware y software. La investigación será desarrollada por estudiantes de la Universidad Politécnica Estatal del Carchi del Octavo semestre de la carrera de Computación: Jazmín Estefanía Hurtado Rodríguez, C.I.040190048-5, y Lupe Fernanda Paspuel Pusda, C.I. 0450026323.

En la cual se desarrollará en el Municipio de Bolívar periodo de Julio- Diciembre 2021, por otra parte me permito poner en su conocimiento sobre el Trabajo de Integración Curricular Jazmín Hurtado - estudiante de la Carrera (Correo electrónico jazmin.hurtado@upec.edu.ec, contacto 0997804846).

Por la atención que se digne al presente anticipo mis agradecimientos.

Atentamente,

Jazmín Hurtado. Fernanda Paspuel.

AUTORES DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Anexo: Resumen del Plan de Continuidad de Operaciones de los Activos Tecnológicos hardware y software.

08-07-21
16:02

Anexo 6. Encuesta 1

ENCUESTA APLICADA AL PERSONAL DE COORDINACIÓN DE INNOVACIÓN

MUNICIPIO DE BOLÍVAR

Instrucciones: Marque con una X la alternativa que considere más adecuada.

1. ¿Al no contar con un plan de continuidad de negocios afecta negativamente al área de Sistemas?

Si Y No_____

2. ¿Existen políticas para la gestión de continuidad de negocios?

Si X No_____ Desactualizado

3. ¿Existe estrategias de recuperación de los servicios críticos frente a una caída de los sistemas de información y comunicación?

Si X No_____ No Documentada

4. ¿Se realiza simulacros frente a una caída de los sistemas de información y comunicación?

Si_____ No X

5. ¿Se realiza tareas de monitoreo a los sistemas de información y comunicación?

Si X No_____

6. ¿Se realiza el control de los procesos críticos de los sistemas de información y comunicación?

Si X No_____

7. ¿Un plan de continuidad de negocio mejorará la disponibilidad de los sistemas de información de la

entidad?

Si X No_____

Anexo 7. Clasificación de amenazas según MAGERIT versión 3

TIPO DE AMENAZA	CLASIFICACIÓN
Desastres naturales	Fuego
	Daños por agua
	Desastres naturales
De origen industrial	Fuego
	Daños por agua
	Desastres industriales
	Contaminación mecánica
	Contaminación electromagnética
	Avería de origen físico o lógico
	Corte del suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Fallo de servicios de comunicaciones
	Interrupción de otros servicios y suministros esenciales
	Degradación de los soportes de almacenamiento de la información
	Emanaciones electromagnéticas
Errores y fallos no intencionados	Errores de los usuarios
	Errores del administrador
	Errores de monitorización (log)
	Errores de configuración
	Deficiencias en la organización

Errores y fallos no intencionados	Difusión de software dañino
	Errores de [re-]encaminamiento
	Errores de secuencia
	Escapes de información
	Destrucción de información
	Fugas de información
	Vulnerabilidades de los programas (software)
	Errores de mantenimiento / actualización de programas (software)
	Errores de mantenimiento / actualización de equipos (hardware)
	Caída del sistema por agotamiento de recursos
	Pérdida de equipos
	Indisponibilidad del personal
	Manipulación de los registros de actividad (log)
Ataques intencionados	Manipulación de la configuración
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Uso no previsto
	Difusión de software dañino
	[Re-]encaminamiento de mensajes
	Alteración de secuencia
	Acceso no autorizado
	Análisis de tráfico

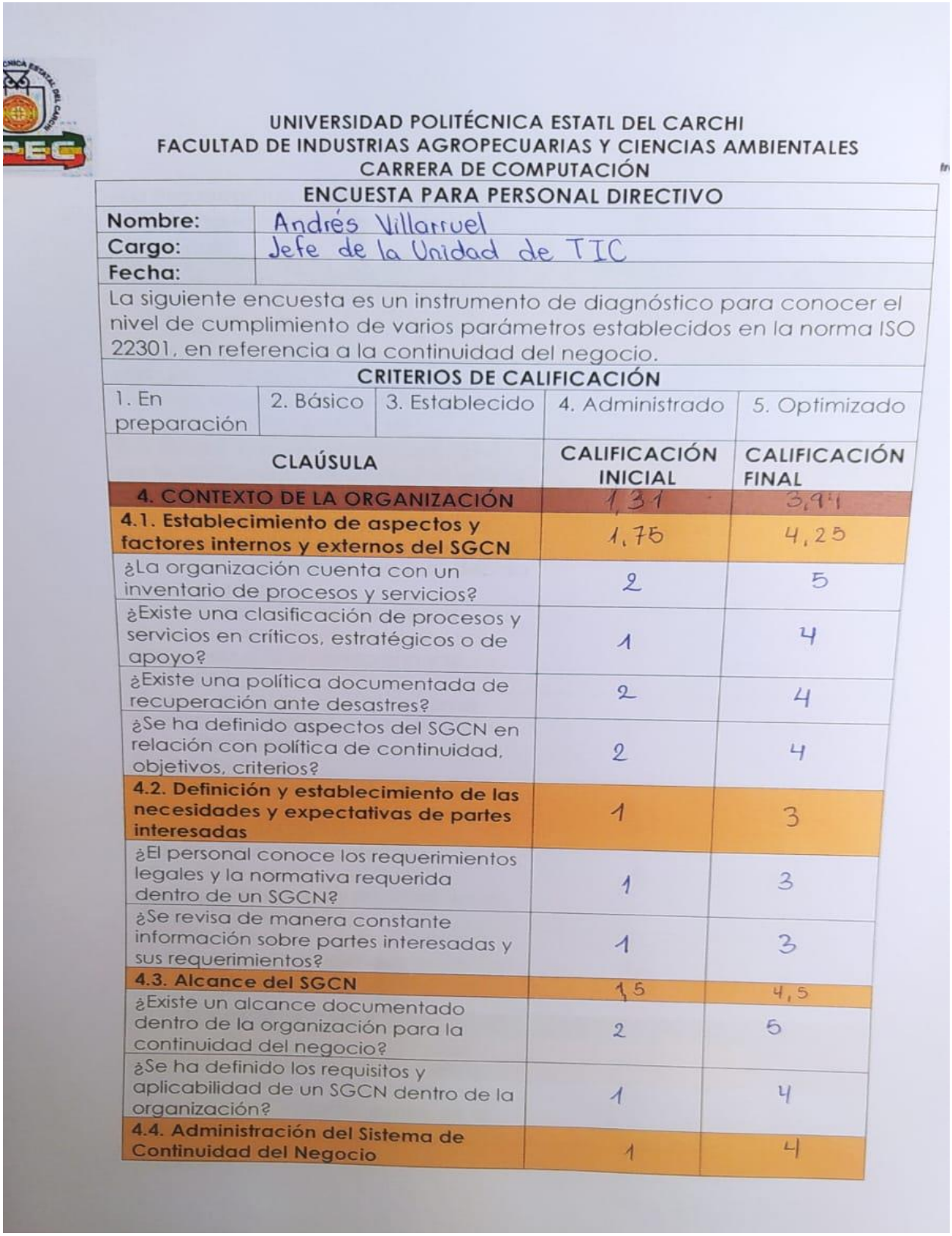
Ataques intencionados	Repudio
	Interceptación de información (escucha)
	Modificación deliberada de la información
	Destrucción de información
	Divulgación de información
	Manipulación de programas
	Manipulación de los equipos
	Denegación de servicio
	Robo
	Ataque destructivo
	Ocupación enemiga
	Indisponibilidad del personal
	Extorsión
	Ingeniería social (picaresca)

Nota. En la tabla anterior se muestra una clasificación de diferentes amenazas, de varios tipos esta categorización de inminencias son las que Margerit en su versión tres menciona. Adaptado de MAGERIT versión 3.0

Anexo 8. Tiempos de recuperación

Tiempo de Recuperación	Descripción
RPO (Recobery Point Obcjetive)	Punto de Recuperación Objetivo Cantidad máxima aceptable de pérdida de datos que la empresa puede tolerar
RTO (Recovery Time Objetive)	Tiempo de Recuperación Objetivo Cantidad máxima aceptable necesario para que todos los sistemas vuelvan a operar
WRT (Work Recovery Time)	Tiempo de Recuperación del trabajo Cantidad máxima de tiempo tolerable necesario para verificar los procesos y la integridad de los datos.
MTD (Maximun Tolerable Downtime)	Tiempo Máximo de Inactividad Tolerable Periodo máximo de inoperatividad que puede tolerar la empresa sin causar consecuencias graves.

Anexo 9. Encuesta 2



UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

ENCUESTA PARA PERSONAL DIRECTIVO	
Nombre:	Andrés Villarruel
Cargo:	Jefe de la Unidad de TIC
Fecha:	

La siguiente encuesta es un instrumento de diagnóstico para conocer el nivel de cumplimiento de varios parámetros establecidos en la norma ISO 22301, en referencia a la continuidad del negocio.

CRITERIOS DE CALIFICACIÓN

1. En preparación	2. Básico	3. Establecido	4. Administrado	5. Optimizado

CLAÚSULA	CALIFICACIÓN INICIAL	CALIFICACIÓN FINAL
4. CONTEXTO DE LA ORGANIZACIÓN	1,31	3,91
4.1. Establecimiento de aspectos y factores internos y externos del SGCN	1,75	4,25
¿La organización cuenta con un inventario de procesos y servicios?	2	5
¿Existe una clasificación de procesos y servicios en críticos, estratégicos o de apoyo?	1	4
¿Existe una política documentada de recuperación ante desastres?	2	4
¿Se ha definido aspectos del SGCN en relación con política de continuidad, objetivos, criterios?	2	4
4.2. Definición y establecimiento de las necesidades y expectativas de partes interesadas	1	3
¿El personal conoce los requerimientos legales y la normativa requerida dentro de un SGCN?	1	3
¿Se revisa de manera constante información sobre partes interesadas y sus requerimientos?	1	3
4.3. Alcance del SGCN	1,5	4,5
¿Existe un alcance documentado dentro de la organización para la continuidad del negocio?	2	5
¿Se ha definido los requisitos y aplicabilidad de un SGCN dentro de la organización?	1	4
4.4. Administración del Sistema de Continuidad del Negocio	1	4

UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

¿La organización ha establecido un SGCN y ha realizado las revisiones periódicas?	1	4
5. LIDERAZGO	2,72	4,28
5.1. Compromiso, apoyo, patrocinio y gestión, por parte de los ejecutivos y la alta gerencia al SGCN	3	4
¿La alta dirección ha mostrado interés y apoyo en el establecimiento e implementación del SGCN?	3	4
5.2. Establecimiento y comunicación de la política de continuidad al interior de toda la organización	2,66	4,33
¿La alta dirección ha establecido y comunicado políticas, normativa legal y el reglamento interno para su debido cumplimiento?	3	4
¿La alta dirección ha establecido una política de continuidad del negocio apropiada a la organización y su contexto?	2	5
¿Existen acuerdos que permitan el acceso del personal a la red interna de la organización generados desde la alta dirección?	3	4
5.3. Asegurar la definición de roles, responsabilidad, autoridad y rendición de cuentas del SGCN	2,5	4,5
¿La alta dirección ha designado roles y ha definido de manera clara las responsabilidades del personal dentro de la organización?	2	5
¿La alta dirección ha documentado los planes de contingencias existentes y ha designado responsables de su ejecución?	3	4
6. PLANIFICACIÓN	1,89	4,17
6.1. Identificación y determinación oportuna de riesgos y oportunidades	1,67	4,33
¿Se han identificado los posibles riesgos y oportunidades dentro de la organización?	2	5

UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

¿Existe planes para reducir o prevenir la materialización de los riesgos?	2	4
¿Existe un plan para tratamiento del riesgo?	1	4
6.2. Alineación estratégica para prevenir efectos y evaluar acciones	2	3,67
¿Existe planificación previa para la realización de cambios?	2	4
¿Se emiten informes posteriores a los cambios realizados?	2	4
¿Se realizan evaluaciones periódicas a los cambios realizados?	2	3
6.3. Definición de los objetivos del SGCN alineados a los planes y estrategias	2	4,5
¿Dentro de la organización, se han establecido objetivos que garanticen la continuidad del negocio?	2	5
¿Existen procesos enfocados en mantener operativas las actividades?	2	4
7. APOYO	2,06	4
7.1. Determinar y proporcionar los recursos necesarios para atender el SGCN	2,5	3,5
¿Existen los recursos necesarios para implementar un SGCN?	3	3
¿Se ha considerado las capacidades y limitantes de los recursos dentro de la organización?	2	4
7.2. Recursos que cuentan con competencia, habilidades, experiencia y toma de conciencia para el SGCN	1,5	4
¿Existe un proceso definido que determine las competencias del personal en relación con la continuidad del negocio?	1	5
¿Se realiza evaluaciones al personal para determinar sus capacidades profesionales?	2	4
¿Se ha realizado el proceso de concienciación al personal sobre la	1	3

UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

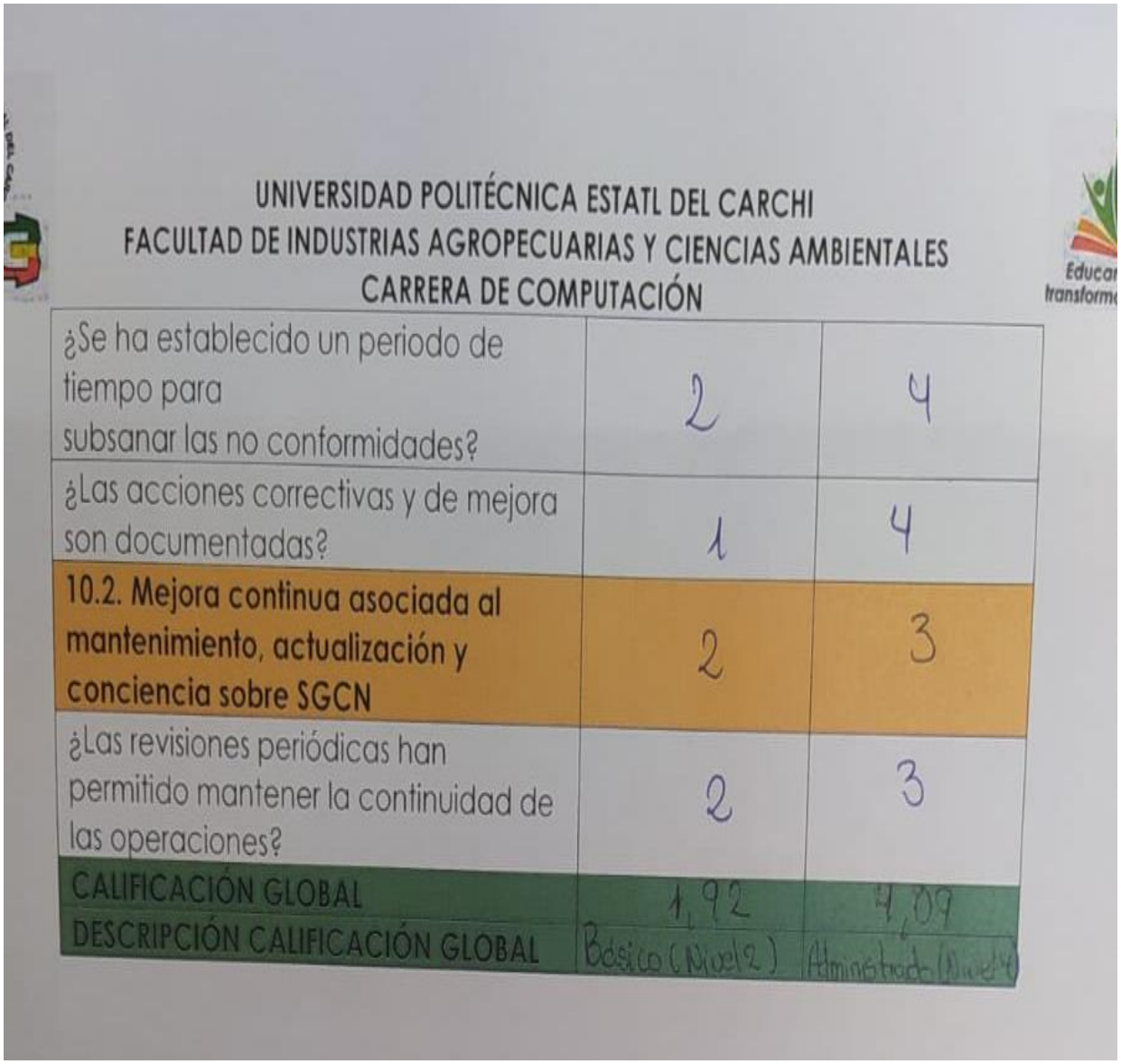
importancia de la continuidad del negocio?	2	4
¿El personal comprende de manera clara las implicaciones de la interrupción de las actividades?	2	4
7.3. Dispone de mecanismos de comunicación interna y externa, quién, cuándo, dónde y procedimientos	2,5	4,5
¿La organización ha definido procedimientos para garantizar la disponibilidad de los medios de comunicación durante la ocurrencia de incidentes que alteren la operatividad de las actividades ?	3	5
¿Se realizan pruebas de validación al proceso que permite la comunicación durante la interrupción de las actividades dentro de la organización?	2	4
7.4. Información documentada del SGCN(creación, actualización, control)	1,75	4
¿La organización mantiene la información documentada siguiendo un estándar?	1	4
¿La información documentada tiene identificación, descripción, fecha, autor, control de cambios?	2	5
¿Existe control de acceso a la información confidencial?	2	3
¿La información documentada se mantiene como evidencia de la conformidad y protegida contra modificaciones no autorizadas?	2	4
8. OPERACIÓN	1,58	4,25
8.1. Definición, evaluación y administración de riesgos y análisis de impacto al negocio BIA	1,25	4,25
¿Dentro de la organización existe un procedimiento para realizar el análisis de impacto y la evaluación de riesgos?	1	5

UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

¿Los resultados obtenidos en la evaluación de riesgos, son comunicados al personal?	1	5
¿Se han establecido planes para el tratamiento de los riesgos?	2	4
¿Se monitorean y evalúan periódicamente el plan de tratamiento de riesgos?	1	3
8.2. Diseño, determinación y administración de estrategias DRP y BCP para todo el SGCN	1,33	4
¿La organización ha definido estrategias para la continuidad del negocio?	1	4
¿Se han adoptado medidas para reducir interrupciones ocasionadas por amenazas materializadas?	2	4
¿Se han definido los tiempos máximos de inoperatividad a causa de un incidente?	1	4
8.3. Procedimientos del SGCN, administración y respuesta a incidentes	2	5
¿La organización ha establecido procedimientos para asegurar la continuidad del negocio ante un incidente?	2	5
¿La organización ha definido planes de recuperación de desastres o de contingencia?	2	5
8.4. Definición, ejecución y evaluación de ejercicios y pruebas al SGCN	1,75	3,75
¿Dentro de la organización se realizan planes de pruebas y verificación?	2	4
¿Se han definido los distintos escenarios de incidentes?	1	4
¿La alta dirección forma parte en la realización de pruebas y verificaciones?	2	4
¿Se documenta el resultado de pruebas para posteriormente socializarlo?	2	3
9. EVALUACIÓN DE DESEMPEÑO	2,02	4,03

UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

9.1. Evaluación y medición de todo el procedimiento de continuidad del negocio	1,67	4
¿Se realiza el monitoreo y evaluación a los diferentes procesos?	2	4
¿Se documenta los resultados del monitoreo y evaluaciones de los procesos?	1	4
¿Se ha establecido un periodo de tiempo en la evaluación de los procesos?	2	4
9.2. Realización y cumplimiento de auditorías internas planificadas	2,4	3,6
¿Dentro de la organización se llevan a cabo auditorías programadas?	2	3
¿Previo a una auditoría se definen los criterios y el alcance?	2	4
¿Se garantiza la imparcialidad de los auditores seleccionados?	3	4
¿Los resultados posteriores a la auditoría son comunicados a los responsables de los procesos?	2	3
¿La organización toma en consideración las recomendaciones que surgen posterior a la auditoría?	3	4
9.3. Revisión y evaluación de los ejecutivos y gerencia al SGCN	2	4,50
¿Se revisa periódicamente los procesos, procedimientos para garantizar la continuidad de las operaciones dentro de la organización?	2	4
¿La alta dirección revisa constantemente el cumplimiento de los objetivos de la organización?	2	5
10. MEJORA	1,83	4
10.1. Identificación, monitoreo y solución de no conformidades y acciones correctivas	1,67	3,5
¿Se comunican las no conformidades al personal responsable para determinar mejorar las estrategias definidas?	2	4



UNIVERSIDAD POLITÉCNICA ESTATL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACIÓN

¿Se ha establecido un periodo de tiempo para subsanar las no conformidades?	2	4
¿Las acciones correctivas y de mejora son documentadas?	1	4
10.2. Mejora continua asociada al mantenimiento, actualización y conciencia sobre SGCN	2	3
¿Las revisiones periódicas han permitido mantener la continuidad de las operaciones?	2	3
CALIFICACIÓN GLOBAL	1,92	4,09
DESCRIPCIÓN CALIFICACIÓN GLOBAL	Básico (Nivel 2)	Administrado (Nivel 4)

Anexo 10: Certificado de culminación del trabajo de TIC

Alcaldía Bolívar
Reescribiendo su Historia..!

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN BOLÍVAR
Administración 2019 - 2023

Bolívar, 25 de enero de 2023

CERTIFICA:

Que, las señoritas HURTADO RODRIGUEZ JAZMIN ESTEFANIA CI: 0401900485 y PASPUEL PUSDA LUPE FERNANDA CI: 0450026323 han cumplido con su trabajo investigativo denominado "PLAN DE CONTINUADAD DEL NEGOCIO DE LOS ACTIVOS TECNOLÓGICOS HARDWARE Y SOFTWARE", Cabe indicar que han realizado un excelente trabajo el cual ha culminado con éxito.

Reescribiendo su Historia..!

Lo que certifico en honor a la verdad, facultando al interesado hacer uso del presente en lo que estimare conveniente.

Atentamente,

SISTEMAS

Ing. Andrés Villarruel
JEFE DE LA UNIDAD DE TECNOLOGIA Y COMUNICACIÓN

Dirección García Moreno y Egas esq.
(06) 2 287384 / 119 / 218
www.municipiobolivar.gob.ec
Bolívar - Carchi - Ecuador

Anexo 11. Validación de pregunta por parte de expertos

Juicio de expertos para validación de instrumentos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento del Tema Integración Curricular: "Plan de continuidad del negocio de los activos tecnológicos hardware y software"

Con la validación de instrumentos se pretende conseguir resultados óptimos al tema de investigación, posteriormente siendo los mismos usados de manera adecuada para beneficio del proyecto a desarrollar.

Agradecemos su valiosa colaboración.

1. **DATOS DEL EXPERTO**

Nombres: Marco Antonio	**Apellidos:** Yandún Velastegui
Formación Académica: Magíster en Auditoría de Tecnologías de la Información	
Cargo Actual: Docente	
Institución: UPEC	

2. **OBJETIVOS**

2.1.OBJETIVO GENERAL: Desarrollar un plan de continuidad del negocio de los activos tecnológicos hardware y software para la Unidad de Tecnología y Comunicación TIC del GAD Municipal del Cantón Bolívar.

3. **INDICACIONES GENERALES**

3.1. Con el objetivo de aplicar los términos de manera adecuada, a continuación, se muestran las definiciones de las dimensiones del instrumento a evaluar:

Construcción Teórica	Ítems	Definición
Plan de Continuidad del Negocio	1 al 4	Hace referencia al conocimiento de un plan de continuidad del negocio.
Riesgos, amenazas y vulnerabilidades	5 al 7	Riesgos, amenazas y vulnerabilidades que han

		presentado en los activos tecnológicos hardware y software del GAD Municipal de Bolívar.
Paralización, simulacros, monitoreo de los activos tecnológicos.	8 al 14	Paralización de los servicios, frecuencia de los simulacros, actividades que se llevan acabó para el monitoreo de los activos tecnológicos en el GAD Municipal de Bolívar.

Indicaciones para evaluar la validez de contenido del instrumento

1. Para la correcta evaluación de los instrumentos se evalúa las siguientes categorías: **Suficiencia, Claridad, Coherencia y Relevancia.**

2. Lea cada ítem y seleccione la opción que refleja su opinión respecto a los siguientes indicadores.

CATEGORÍA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los ítems que cumplan con la dimensión bastan para obtener la medida de ésta.	1. No cumple con el criterio	Los ítems no son capaces para medir la dimensión
	2. Bajo Nivel	Los ítems miden escasos aspectos de la dimensión, pero no cumplen la medición total.
	3. Moderado nivel	Se deben incluir más ítems para poder medir la dimensión totalmente
	4. Alto nivel	Los ítems son suficientes
CLARIDAD El ítem se entiende fácilmente, su sintáctica y semántica son adecuadas y suficientes.	1. No cumple con el criterio	El ítem no es claro
	2. Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras.
	3. Moderado nivel	Se requiere una modificación específica de ciertos términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo nivel	El ítem tiene una relación baja con la dimensión que se está midiendo.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.

	4. Alto nivel	El ítem se encuentra completamente Relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, para la dimensión por ende debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la dimensión
	2. Bajo nivel	El ítem tiene cierta relevancia, pero otro ítem está incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es limitadamente importante
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Evaluación de la validez de contenido

N°	Ítem	Suficiencia	Claridad	Coherencia	Relevancia	Observaciones
1	**¿Qué es para usted un plan de continuidad del negocio?**	1	3	2	1	Colocar un breve texto explicativo de continuidad de negocio y la ISO que aplica.
2	**¿Usted considera que es útil desarrollar un plan de continuidad de negocio?** SI ☐ NO ☐ **Porque**	1	3	1	3	Resultado esperado es SI
3	**¿Al no contar con un plan de continuidad de negocio afecta negativamente a la disponibilidad de los activos tecnológicos de hardware y software de la Unidad Tecnológica y Comunicación TIC?** SI ☐ NO ☐ **Porque.....**	1	1	2	2	Es contradictoria la pregunta doble negación
4	**¿Existen políticas para la gestión de continuidad de negocio?** SI ☐ **¿Cuáles?.....** NO ☐ **Porque.....**	1	3	2	3	Detallar las políticas

5	**¿Qué riesgos se han presentado en el GAD Municipal de Bolívar, que puedan afectar a las diferentes operaciones y/o servicios que esta entidad presta?** *(Puede elegir más de una opción)* Riesgo financiero ☐ Riesgo ambiental ☐ Riesgo político ☐ Riesgos legales ☐ Riesgos informáticos ☐ Otros.....	3	1	1	3	-Que Riesgos se ha identificado -Que incidentes ha ocurrido
6	**¿Qué tipos de amenazas se han presentado en el GAD Municipal de Bolívar, que logren afectar los servicios y operaciones?** ☐ Amenaza de seguridad informática Amenaza de desastres naturales ☐ Amenaza de seguridad física ☐ Amenazas producidas por el hombre ☐ Otros.....	3	1	1	3	* que amenazas esta expuesto el GAD. que amenazas se ha identificado
7	**¿Qué tipos de vulnerabilidades en seguridad informática se han identificado en el municipio, que puedan afectar las operaciones y/o servicios?** Mantenimiento de equipos ☐ Cableado de instalaciones ☐ Control interno ☐ Actualización de Antivirus ☐ Otros.....	3	2	2	4	-Equipos sin mantenimto Caducados, obsoletos -Cableado sin certificado - Explique control
8	**¿Existen estrategias de recuperación de los procesos críticos frente a una paralización de los activos tecnológicos?** SI ☐ **¿Cuáles?**_____ NO ☐ **Porque**_____	3	1	1	3	Detalle ~~procesos~~ estrategias
9	**¿Durante los últimos 3 años ha existido paralización de los servicios?** SI ☐ NO ☐ **En caso de que su respuesta sea afirmativa mencione cuales:**	1	1	2	3	Indique los causas por las que se ha paralizado los servicios

10	¿Se realizan simulacros frente a una potencial paralización de activos tecnológicos? SI ☐ NO ☐ Porque.....	1	1	1	3	Resultados de último simulacro
11	¿Cada que tiempo se realiza un simulacro frente a una paralización de activos tecnológicos dentro de la institución?	3	3	3	4	
12	¿Se realiza tareas de monitoreo a los activos tecnológicos hardware y software críticos? SI ☐ NO ☐ Porque.....	2	2	3	3	Indique o liste, Activos – Monitoreo
13	¿Con que frecuencia se realiza el monitoreo a los activos tecnológicos hardware y software? _____	3	3	3	4	Escalas de tiempo 3 meses 6 meses 9 mese.
14	¿Cómo considera usted que se podrá mejorar la disponibilidad de la información con la aplicación de un plan de continuidad del negocio? _____	1	1	1	1	No aplica.

FIRMA DEL EXPERTO

Anexo 12. Plan de Continuidad del Negocio

PLAN DE CONTINUIDAD DEL NEGOCIO DE LA UNIDAD DE TECNOLOGÍA Y COMUNICACIÓN (TIC) DEL GAD MUNICIPAL DEL CANTÓN BOLÍVAR

DATOS INFORMATIVOS

Título	Plan de Continuidad del Negocio (BCP)aplicado a la Unidad de Tecnología y Comunicación (TIC) de GAD Municipal del Cantón Bolívar.
Área	Unidad de Tecnología y Comunicación (TIC) del GAD Municipal del Cantón Bolívar.
Beneficiarios	Alcalde Unidad de TIC Servidores Públicos Ciudadanía del Cantón Bolívar Procesos de GAD Municipal del Cantón Bolívar.
Ubicación	Bolívar – Carchi
Responsables	Hurtado Jazmín y Paspuel Fernanda
Tutor Encargado	Ing. Guano Carlos MSc.

PRESENTACIÓN

La importancia de la disponibilidad de los servicios y activos tecnológicos del Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar, son muy relevantes los cuales mantienen información, por lo cual se debe tomar en cuenta medidas que permitan estar preparados para vulnerabilidades y desastres de diferente tipo.

La Unidad de Tecnología y Comunicación TIC del GAD Municipal del Cantón Bolívar, su misión es permitir la continuidad de los recursos informáticos que permitan seguridad, eficacia, eficiencia y oportunidad. En consecuencia, se presenta el Plan de Continuidad del Negocio del Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar; el cual tiene beneficios que permitirán advertir sobre desastres o diferentes circunstancias con los servicios y hardware, software de los activos tecnológicos.

Los responsables de la tecnología y comunicación del GAD Municipal del Cantón Bolívar tienen como obligación comunicar las medidas de seguridad, tiempos de recuperación, responsables de los equipos y el correcto manejo de estos; de esta manera se identifica riesgos, amenazas y vulnerabilidades actuales de cada uno de los activos disponibles, evitando pérdidas y desastres de mayor escala.

INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar es evidente que tiene paralizaciones de servicios y es vulnerable a distintas fallas poniendo en riesgo la disponibilidad de la institución y su figura pública frente a la ciudadana para cumplir el correcto funcionamiento. En caso del Municipio se origina estos problemas por falta de prevención y estudio de diferentes riesgos, al igual por la falta de ejecución y actualización del Plan de Continuidad.

GENERALIDADES

Objetivos

- **Objetivo General**

Desarrollar con un Plan de continuidad del negocio conveniente a la Unidad de TIC del GAD Municipal del Cantón Bolívar, el que permita la continuidad de los procesos enfrentando a fallas, eventos o riesgos inesperados asegurando la disponibilidad de los servicios, con el fin de prevenir, contener, recuperar y transferir de manera rápida los equipos o información en menor tiempo, al igual la mejora de la prestación de servicios de la institución.

- **Objetivos Específicos**

Detallar con documentación que permita al Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar, la disponibilidad de los activos tecnológicos, servicios o procesos sin contar con la paralización y pérdidas mayores.

Identificar y analizar los riesgos, vulnerabilidades y amenazas que están expuestos los servicios, activos tecnológicos y procesos de la institución.

Establecer estrategias, procedimientos y lineamientos puntuales de recuperación ante los diferentes problemas asegurando la continuidad.

Base Legal

Norma Internacional 22301:2019 Norma internacional para sistemas de gestión de la continuidad de negocio (SGCN) y metodología MAGERIT para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas.

Fases Del Plan De Continuidad

FASE	DESCRIPCIÓN	OBSERVACIONES
Fase 0: Determinación del alcance	Alcance del BCP	Define las áreas donde se va a desarrollar el BCP
	Política y objetivos de la continuidad del negocio	Documentación de lo que se quiere lograr con el BCP y cómo controlar
Fase 1: Análisis de la Organización	Determinación de la situación actual de la organización	Información de cómo se encuentra la organización, organigrama, inventario de recursos tecnológicos.
	Análisis de impacto de la organización (BIA)	Identificación de procesos críticos
	Análisis de riesgos	Determinar los activos tecnológicos críticos
Fase 2: Determinación de estrategias de continuidad del negocio	Estrategias de continuidad del negocio	Documentación que contiene estrategias de respuesta frente a un incidente.
Fase 3: Respuesta a la contingencia	Plan de contingencia	Se debe definir como se debe registrar los riesgos
	Comité de crisis	
Fase 4: Prueba, mantenimiento, revisión	Planes de prueba y revisión	Se debe definir los escenarios y objetivos que se deben cumplir
	Plan de mantenimiento del BCP	Documentación que debe contar cuando y quien va a realizar el mantenimiento.

Fase 5: Capacitación y concienciación	Plan de capacitación y concienciación	Las necesidades de temas de capacitación del personal.

Fase 0: Determinación del alcance

Alcance del Plan de Continuidad del Negocio (BCP)

El desarrollo de este Plan de Continuidad está enfocado en la Unidad de tecnología y comunicación TIC del GAD Municipal de Bolívar con la realidad y necesidades que presenta la institución pública. Se toma en cuenta todo el personal que labora en la unidad de TIC, así como Jefe de la Unidad de TIC, y diferentes unidades que conforman el recurso humano involucrado dentro de este Plan, al igual se toma en consideración todos los procesos y activos que forman parte de la cadena de valor del Unidad de TICC de esta institución para desarrollar medidas que permitan la continuidad del negocio.

Política de continuidad del negocio

La Gerencia General del GAD Municipal de Bolívar, consciente de la importancia de brindar un servicio de calidad y mantener su infraestructura operativa, ha considerado de vital importancia contar con Plan de Continuidad del Negocio para la Unidad de Tecnología y Comunicación TIC, debidamente documentado, socializado y al alcance de los responsables designados en cada tarea. El contenido del BCP, está basado en la norma internacional ISO 22301:2019 y ha sido adaptado a las necesidades propias de esta organización, por lo que de presentarse algún incidente de seguridad informático o fallo en la infraestructura, su aplicación es de carácter obligatorio y se debe seguir los procedimientos mencionados ejecutando las tareas descritas según corresponda. Con la finalidad de mantener actualizado el Plan de Continuidad, se establece una revisión semestral del documento en el que actuarán las partes interesadas, pudiendo añadir o mejorar las estrategias y planes propuestos en dicho documento. Es importante recalcar que previo a cualquier modificación en los planes de contingencia y recuperación de desastres, es necesaria la

realización de pruebas en ambiente de preproducción y posteriormente el paso a producción debe ser autorizado por el Jefe de la Unidad de TIC.

Fase 1: Análisis de la Organización

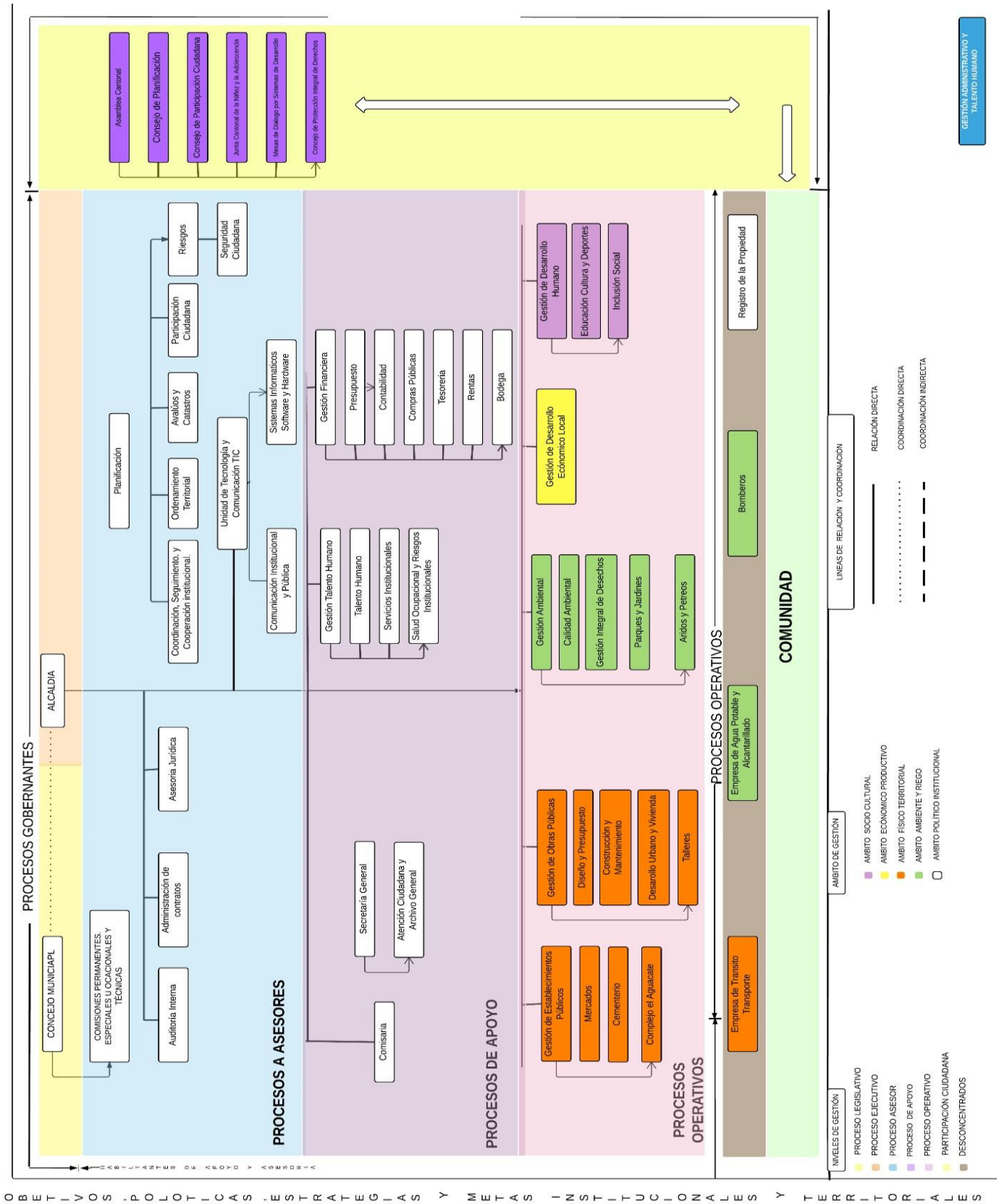
Situación Actual

El Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar, es primordial un Plan de continuidad de negocio de los activos tecnológicos, que tenga políticas de seguridad, prevención y contención. Para poder realizar dicho plan es necesario realizar un análisis del estado actual de la institución o entidad a la cual se le ejecutara revisiones de control.

Cabe recalcar que se realizó un diagnóstico de la situación actual de la entidad, contando con un plan sostenible para prevenir y menguar cualquier problema o desastre informático interno o externo de manera que natural o externo de los servicios tecnológicos que presta la institución.

Sin embargo, estas políticas no permiten asegurar, restaurar los equipos con menores pérdidas posibles en forma rápida eficiente y oportuna en caso de detectar amenazas, riesgos y vulnerabilidades, certificando la integridad, disponibilidad y confidencialidad de la información de la Municipalidad y servicios prestados a los usuarios.

Organigrama del GAD Municipal del Cantón Bolívar



Unidad de Tecnología y Comunicación TIC

Misión:

Administrar y gestionar eficientemente los recursos informáticos y de comunicación, mediante la utilización y aplicación de las tecnologías de información TIC.

Funciones de los procesos a ejecutar

- ✓ Brindar soluciones informáticas de hardware y software a la Institución.
- ✓ Realizar servicios de mantenimiento preventivo de equipos de computación y telecomunicaciones.
- ✓ Desarrollar Planes informáticos que permitan la disponibilidad de los recursos tecnológicos.

Orgánico Funcional de la Unidad de Tecnología y Comunicación TIC

La Estructura está conformada por:

Detalle de funciones de cada ente que conforma el orgánico funcional de la Unidad de TIC

Unidad de Tecnología y Comunicación
• Plan de mantenimiento de hardware y software del parque informático. • Informe de ejecución del plan de mantenimientos de hardware y software. • Administración de la página web. • Administración de correos electrónicos. • Auditoría informática de hardware y software. • Plan de contingencia del centro de cómputo. • Administración de la Biblioteca Virtual. • Administración de la central telefónica. • Administración del servidor de impresiones.

Comunicación Institucional y Pública
• Producción audiovisual • Spots publicitarios • Cuñas publicitarias • Jingles • Trípticos • Revistas • Folletos • Dípticos • Grabaciones en OFF • Retoque fotográfico • Diseño de logotipos • Diseño de afiches • Diseño de banners • Diseño de rótulos

Comunicación Institucional y Pública
• Producción audiovisual • Spots publicitarios • Cuñas publicitarias • Jingles • Trípticos • Revistas • Folletos • Dípticos • Grabaciones en OFF • Retoque fotográfico • Diseño de logotipos • Diseño de afiches • Diseño de banners • Diseño de rótulos

Inventario de Recursos Informáticos

El inventario de recursos hardware y software debe ser actual de los cuales posee el Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar. **(Anexo 1)**

Para el inventario de los activos tecnológicos se tendrá en cuenta las siguientes características:

- Especificación de hardware y software
- Ubicación
- Dirección IP
- Marca
- Sistema operativo
- Tipo de activo

El etiquetado de cada activo debe ser de diferente color en caso de vulnerabilidades para tener en cuenta su importancia. Ejemplo: activos críticos (rojo), los activos fijos, pero no contienen información representativa(amarillo).

Análisis de Impacto del negocio (BIA)

El análisis de impacto del negocio (BIA) ha permitido determinar los principales procesos del GAD Municipal del Cantón Bolívar, valorar el nivel de criticidad para determinar el impacto operacional.

Para ellos se debe identificar los procesos y funciones que presta el GAD Municipal del Cantón Bolívar, posterior clasificar o evaluar el impacto en diferentes aspectos identificando los procesos críticos de la institución.

CLASIFICACIÓN DEL IMPACTO OPERACIONAL

Descripción	Valoración
Proceso crítico para la institución, no es posible realizar la función señalada	**A**
Proceso no crítico para la institución, pero forma parte integral de esta	**B**
Proceso no crítico y no forma parte integral de la institución	**C**

Identificación de funciones y procesos del Gobierno Autónomo Descentralizado Municipal del Cantón Bolívar

Función Interna/externa	Proceso	Nivel	Descripción
Tecnología y Comunicación, Comunicación Institucional y Pública, Sistemas Informáticos y Software y Hardware	Plan de mantenimiento de hardware y software	**B**	Personal encargado
	Informe de ejecución del plan de mantenimientos de hardware y software.	**B**	Personal encargado
	Administración de la página web.	**C**	Unidad de TIC
	Administración de correos electrónicos.	**B**	Correo institucional
	Soporte Técnico de hardware y software.	**B**	Soporte Técnico
	Plan de continuidad del negocio	**B**	Unidad encargada
	Servicio de internet	**A**	Enlace de Internet
	Administración de la central telefónica.	**C**	Telefonía IP
	Administración del servidor	**A**	Data Center
	Seguridad Informática (Firewall)	**A**	Seguridad Perimetral
	Respaldos de información	**A**	Servidores
	Recurso humano	**B**	Personal de TIC

Identificación de procesos críticos y establecimientos de tiempos de recuperación

Es preciso detallar los procesos críticos y establecer los tiempos de recuperación de acuerdo con el nivel de prioridad de cada proceso.

Función interna/externa	Proceso	Nivel	Tiempo en Horas				Prioridad de recuperación
			RPO	RTO	WRT	MTD	
Tecnología y Comunicación , Comunicación Institucional y Pública, Sistemas Informáticos y Software y Hardware	Plan de mantenimiento de hardware y software	B	1	1	2	3	2
	Informe de ejecución del plan de mantenimientos de hardware y software.	B	2	2	2	4	2
	Administración de la página web.	C	4	3	4	7	3
	Administración de correos electrónicos.	B	3	4	2	6	3
	Soporte Técnico de hardware y software.	B	2	2	2	4	2
	Plan de continuidad del negocio	B	1	2	4	6	2
	Servicio de internet	A	1	1	1	2	1
	Administración de la central telefónica.	C	4	4	4	8	3
	Administración del servidor	A	1	1	1	2	1
	Seguridad Informática(Firewall)	A	1	1	1	2	1
	Respaldos de información	A	1	1	2	3	1
	Recurso humano	B	1	1	2	3	2

Análisis de riesgos

La valoración de criticidad se muestra la identificación y valoración de activos críticos del GAD Municipal de Bolívar, para la cual se toma en cuenta la valoración en las 3 dimensiones: disponibilidad, integridad y confidencialidad.

Valoración de criticidad de los activos

IDENTIFICACIÓN DE ACTIVOS		VALORACIÓN DE ACTIVOS						
N°	Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	Servidor de virtualización	Alta(A)	3	Alta(A)	3	Alta(A)	3	3
2	Firewall	Alta(A)	3	Media(M)	2	Alta(A)	3	3
3	Servidor (Backups)	Alta(A)	3	Alta(A)	3	Alta(A)	3	3
4	Servidor de red	Alta(A)	3	Alta(A)	3	Media(M)	2	3

El análisis de riesgos de la Unidad de TIC del GAD Municipal del Cantón Bolívar permite determinar las amenazas relacionadas con cada activo para la cual se detalla a continuación:

Identificación de activos	**Amenazas**
Activo	**Descripción**
Servidor de virtualización	Daños ocasionados por fuego
	Daños ocasionados por agua
	Daños ocasionados por corte de suministro eléctrico
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
	Desconexión deliberada o accidental del equipo
	Falta de actualizaciones de versión de sistema operativo
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo
	Degradación por saturación de recursos del equipo
	Imposibilidad de recuperar el equipo por falta de planes de contingencia
	Daño en el equipo por falta de mantenimiento
Firewall	Daños ocasionados por fuego

	Daños ocasionados por agua
	Daños ocasionados por corte de suministro eléctrico
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
	Desconexión deliberada o accidental del equipo
	Falta de actualizaciones de versión de sistema operativo
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo
	Degradación por saturación de recursos del equipo
	Imposibilidad de recuperar el equipo por falta de planes de contingencia
	Daño en el equipo por falta de mantenimiento
Servidor (Backups)	Daños ocasionados por fuego
	Daños ocasionados por agua
	Daños ocasionados por corte de suministro eléctrico
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
	Desconexión deliberada o accidental del equipo
	Falta de actualizaciones de versión de sistema operativo

	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo
	Degradación por saturación de recursos del equipo
	Imposibilidad de recuperar el equipo por falta de planes de contingencia
	Daño en el equipo por falta de mantenimiento
Servidor de red	Daños ocasionados por fuego
	Daños ocasionados por agua
	Daños ocasionados por corte de suministro eléctrico
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
	Desconexión deliberada o accidental del equipo
	Falta de actualizaciones de versión de sistema operativo
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo
	Degradación por saturación de recursos del equipo
	Imposibilidad de recuperar el equipo por falta de planes de contingencia
	Daño en el equipo por falta de mantenimiento

El cálculo de la valoración del impacto de las amenazas sobre los activos se basa en las 3 dimensiones, juntamente con el porcentaje de daño que ocasiona cada una de estas en su degradación **(Anexo2).**

La valoración del riesgo se toma en cuenta por la probabilidad de incidencia de un evento y el impacto sobre los activos tecnológicos.

Fase 2: Determinación de estrategias de continuidad del negocio

Estrategias de Continuidad del negocio

PROCESO	RESPONSABLE	RTO	ESTRATEGIA DE RECUPERACIÓN	ACCIONES	RECURSOS
Servicio de internet	Jefe de la Unidad de TIC	1 hora	Actualización de contacto de proveedores	Contactar a proveedor del servicio	Contactos de proveedor
	Jefe de la Unidad de TIC	1 hora	Repetición del servicio de internet	Contar con enlace backups de internet	Infraestructura de red
Administracion del servidor	Jefe de la Unidad de TIC	1 hora	Levantar un servidor alterno o tener en cuenta los backups	Acceder a los servicios contratados para hacer uso de los recursos de red	IaaS (Infraestructura como Servicio) en la nube
Seguridad informatica firewall	Jefe de la Unidad de TIC	1 hora	Disponibilidad	Conexión automática del equipo secundario	Equipos secundarios
Respaldos de informacion	Jefe de la Unidad de TIC	1 hora	Sitios de copias de seguridad por duplicado	Contar con servidor alterno de duplicado	Servidor, Soporte de Red
	Jefe de la Unidad de TIC	1 hora	Actualización de respaldos		
	Jefe de la Unidad de TIC	1 hora	Registro y control de backups		
	Jefe de la Unidad de TIC	1 hora	Dispositivos físicos de almacenamiento	Correcto funcionamiento	Discos de almacenamiento
	Jefe de la Unidad de TIC	1 hora	Sitio de almacenamiento en la nube	Verificar almacenamiento	Servicio de almacenamiento en la nube

Fase 3: Respuesta a la contingencia

Plan de Contingencia

El plan de contingencia se compone del plan de prevención de riesgos, plan de gestión de emergencias y el plan de recuperación de desastres.

PLAN DE PREVENCIÓN DE RIESGOS

El proceso de recuperación de los activos debe realizarse en el menor tiempo posible y con el menor costo posible del GAD Municipal del Cantón Bolívar.

Para ello se debe tomar en cuenta lo siguiente:

- Los sistemas de información
- Equipos de cómputo
- Respaldos de información

PROCEDIMIENTOS DE CONTINGENCIA DEL NEGOCIO EN CASO DE FALLA DE FIREWALL

Objetivo

Definir las acciones, procedimientos y recurso humano para garantizar la recuperación de los servicios a través del Firewall de contingencia de la unidad de TIC.

Responsable	Actividades por realizar
Jefe de la unidad de Tecnología de la Información y Comunicación	• Realizar respaldos de la de las reglas del Firewall (Revisar **la tabla N. ª 1**) • Subir las reglas al ordenador central (Revisar Tabla **N.º 2**)
	• Dar mantenimientos preventivos y correctivos cada 6 meses al servidor de Firewall (Revisar la tabla **N. ª 3**) • En caso de fallar el firewall dar aviso al jefe de tecnología y comunicaciones (Revisar el apéndice **N.º 4**)
	• Contar con un equipo firewall de contingencia en el Sitio principal y alterno • Restablecer el servicio (Revisar la tabla **N.º 5**) • Encender máquina virtual (mirar la tabla **N. ª 6**) • Instalar reglas en el servidor de contingencia (Revisar la tabla **N. ª 7**) • Instructivo para reiniciar el SIC del firewall (Revisar la tabla N. ª **8**)

Procesos afectados: Todos los procesos de la unidad de TIC

Tiempo estimado de activación: Se estima 60 minutos en la ejecución de las actividades descritas a continuación

Nivel o estado: Por la afectación a todos los procesos de la unidad de TIC se considera de nivel crítico que corresponde al más alto y de pronta recuperación

ACCIONES PREVIAS AL EVENTO

TABLA N. ª 1

ACTIVIDAD: Realizar respaldos de la de las reglas del Firewall	**RESPONSABLE**
1. Tener un dispositivo de almacenamiento	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel
2. Conectar el dispositivo al firewall para obtener el respaldo	
3. Realizar una copia de seguridad de las reglas con su versión más actualizada	
4. Retirar el dispositivo de almacenamiento	
5. Etiquetar con la fecha del día de realización	
6. Guardar el dispositivo de almacenamiento en el estante de respaldos	

TABLA N. ª 2

ACTIVIDAD: Subir las reglas al ordenador central	**RESPONSABLE**
1. Tener el dispositivo de almacenamiento con las reglas nuevas (en caso de colocar nuevas restricciones)	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel
2. Conectar el dispositivo al firewall para colocar las reglas	
3. Conectarse Management Principal utilizando la dirección IP que se encuentra en el formato de inventario de servidores que reposa en la oficina del jefe de unidad.	
4. Logearse al sistema operativo con el usuario y contraseña propio de cada usuario.	
5. Conectarse por FTP al servidor de Respaldos a la dirección IP y con las credenciales que se encuentra en el formato de inventario de servidores que reposa en el departamento	
6. Realizar el traspaso de las reglas al firewall en el área central	

7. Finalizar la acción de traspaso	
8. Retirar el dispositivo de almacenamiento de las reglas del firewall	
9. Guardar el dispositivo de almacenamiento en el estante de respaldos	

ACCIONES DURANTE EL EVENTO

TABLA N. ª 3

• **ACTIVIDAD:** Dar mantenimientos preventivos y correctivos cada 6 meses al servidor de Firewall	**RESPONSABLE**
1. Estar al día con las actualizaciones de tu antivirus.	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel
2. Asegurar la configuración del firewall (previniendo las entradas no autorizadas).	
3. Preservar el rendimiento de las máquinas virtuales.	
4. Realizar un backup automatizado y periódico de los elementos guardados en el servidor, para que, en caso de fallo y pérdida de datos, estos puedan recuperarse o restaurarse de forma rápida	
5. Estar al día con las actualizaciones de tu antivirus.	
6. Asegurar la configuración del firewall (previniendo las entradas no autorizadas).	
7. Preservar el rendimiento de las máquinas virtuales.	
En el caso de correctivos contactar al técnico el cual realizará una serie de procesos correctivos y dará un diagnostico	
8. Posterior al diagnóstico recibido el jefe de la unidad dará la orden de realizar la corrección	
9. Comprobar si el área ya tiene el servicio	
10. Finalización del mantenimiento	

TABLA N. ª 4

• **ACTIVIDAD:** En caso de fallar el firewall dar aviso al jefe de tecnología y comunicaciones	**RESPONSABLE**
1. Revisar conexiones de electricidad	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel
2. Comunicar el Inicio de la Incidencia de Firewall de acuerdo al Plan de Comunicaciones	
3. Verificar que exista electricidad en el tomacorriente con un cargador de celular, lampara u oro objeto que disponga de comprobación inmediata,	
4. Reiniciar el firewall	
5. Si los pasos anteriores no solucionan el problema realizar un diagnóstico del problema	
6. Dar aviso en modo sunami a todo el personal que usa el firewall	
7. Comunicar que se restablecerá el servicio dentro de una hora	
8. Si el firewall no responde, pasar de inmediato al firewall de respaldo,	
9. Conectarlo y encenderlo. En el nuevo firewall subir las reglas (ver apéndice N° 2)	
10. Reactivar el servicio	

ACCIONES DESPUÉS DEL EVENTO

TABLA N. ª 5

• **ACTIVIDAD:** Contar con un equipo firewall de contingencia en el Sitio principal y alterno	**RESPONSABLE**
1. Conectar el firewall de respaldo	Jefe de la unidad de Tecnología de la Información y Comunicación
2. Comunicar el Inicio de la Incidencia de Firewall	
3. Tener los dispositivos con las reglas actualizadas y subirlos al nuevo firewall	

<table>
<tr><td>4. Contactar con el proveedor de acuerdo al siguiente cuadro para reportar el incidente:
<table><tr><td colspan="2">Proveedor de internet</td></tr><tr><td>SOPORTE</td><td>09[redacted]</td></tr><tr><td>GERENTE TECNICO</td><td></td></tr><tr><td>Email:</td><td>[redacted]@gmail.com</td></tr></table></td><td>Proveedor</td></tr>
<tr><td>5. Encender la Máquina Virtual de respaldo ubicada en la portátil del jefe de la unidad (CentOS Recuperación) que se encuentra en la oficina.</td><td rowspan="6">Jefe de la unidad de TIC
Andrés Villarruel</td></tr>
<tr><td>6. Configurar la tarjeta Ethernet de la Laptop de Contingencia con los siguientes parámetros:
IP: 192.[redacted]
Mascara: 255.[redacted]</td></tr>
<tr><td>7. Conectar la interfaz 1 del Firewall al puerto Ethernet de la portátil de contingencia.</td></tr>
<tr><td>8. Iniciar el proceso de Re-inicialización del SIC.</td></tr>
<tr><td>9. Conectar las interfaces de red en el Firewall de respaldo.</td></tr>
<tr><td>10. Comprobar las conexiones entre redes y verificar las reglas de Firewall, ejecutando comandos ping a distintas direcciones en la Red</td></tr>
<tr><td>11. Comunicar disponibilidad de servicios</td></tr>
</table>

PLAN DE COMUNICACIÓN DE LA UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

SITUACIÓN	MEDIO	INFORMACIÓN RELEVANTE	RESPONSABLE DE ENVÍO
INICIO DE LA INCIDENCIA	Correo electrónico WhatsApp	Tipo de daño Servicios Afectados Tiempo estimado de restablecimiento del servicio	Director de Tecnología de la Información y Comunicaciones

ACTIVACIÓN DE PLAN DE CONTINGENCIA		Condiciones de funcionalidad de los equipos de contingencias Servicios restaurados	
RESTAURACIÓN DE OPERACIONES NORMALES		Fecha y hora de inicio de operaciones normales	

TABLA N. ª 6

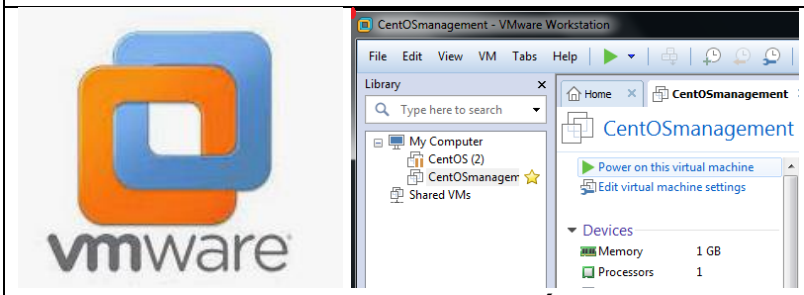
ACTIVIDAD: Encender máquina virtual	**RESPONSABLE**
1. En la barra de herramientas del escritorio de Windows escoger el icono del software de virtualización y dar doble click, escoger la Maquina CEntos Manager y dar click en el botón play  **Icono del software de virtualización, Pantalla de inicio de CentOS** 2. Una vez levantada la máquina virtual probar la conectividad haciendo ping a la IP [redacted] en caso de responder revisar las configuraciones de red de la Laptop para Contingencias y de la Máquina Virtual.	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel

TABLA N. ª 7

ACTIVIDAD: Instalar reglas en el servidor de contingencia Instructivo para instalar reglas en el servidor management de contingencia	**RESPONSABLE**

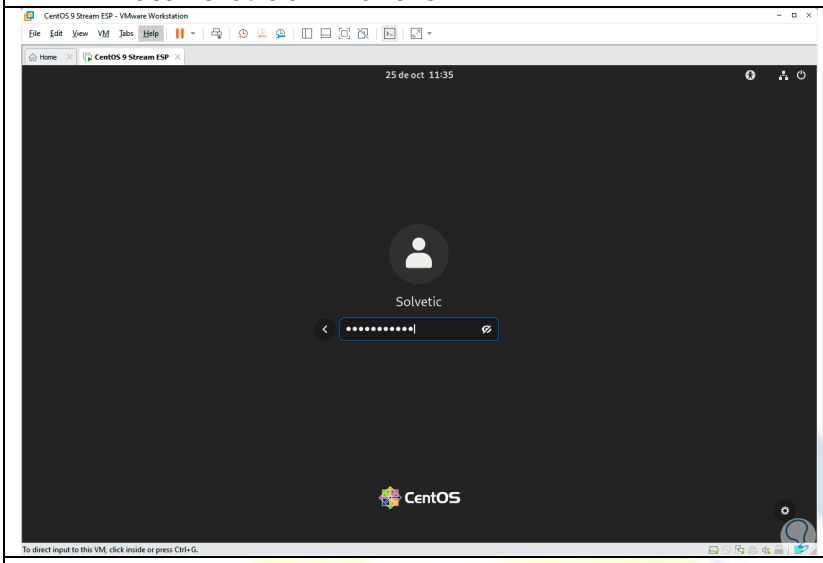
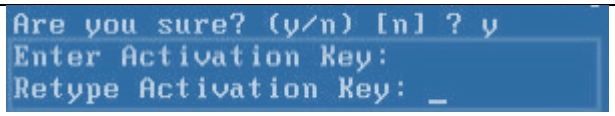
1. Conectarse al Security Management (Contingencia)	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel
2. Logearse al sistema operativo con las credenciales **Usuario:** administrator **Password:** administrator	
	
3. Ejecutar los comandos requeridos (solo el personal autorizado tiene conocimiento a seguir)	
4. Ingresamos a la aplicación, SmartDashboard ingresando el usuario y la clave de contingencia que reposa en los documentos de la unidad del documento de Políticas y Procedimiento del subproceso Seguridad y control de la información de los recursos tecnológicos.	
5. Verificar que se muestren las políticas del Firewall en la pestaña *"Firewall"* opción "Policy"	
6. En caso de no visualizar las reglas, contactar al proveedor para repetir el procedimiento.	

TABLA N. ª 7

ACTIVIDAD: Instructivo para reiniciar el SIC del firewall	**RESPONSABLE**
1. Conectarse al Security Management	Jefe de la unidad de Tecnología de la Información y Comunicación Andrés Villarruel
1. Logearse al Sistema operativo **Usuario:** administrator **Password:** administrator	
2. Ejecutar los commandos **[Expert@HostName]# cpconfig** Escoger la opción cinco "SecureInternalCommunication" ingresando el número cinco desde el teclado.	

3. Se le preguntará si desea reiniciar la comunicación. Pulsar la tecla "Y" y dar "Enter": se le pedirá de nuevo si desea reinicializar la comunicación, pulsar la tecla "**y**" y dar "Enter":

4. Se pedirá que introduzca una nueva clave "SIC". Asegúrese de introducir la misma clave en ambos campos. Una vez que termine de escribirlo, dar "Enter":



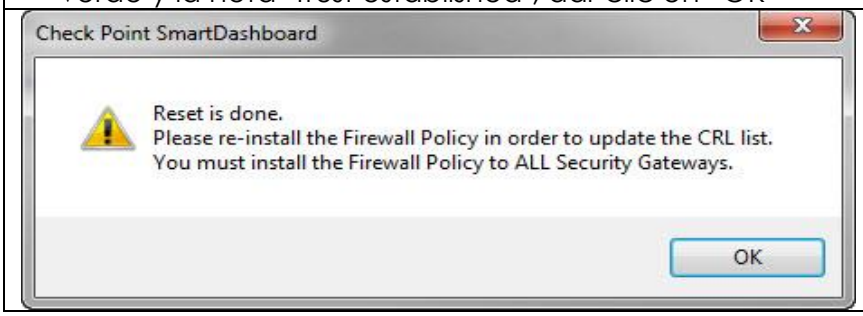
5. Esperar hasta que se despliegue el mensaje de que la Comunicación, interna segura se reinició satisfactoriamente y escoger la opción de salir.

6. En el escritorio ingresamos a la aplicación, SmartDashboard que se encuentra instalada en los equipos del personal de Infraestructura, en la carpeta "CheckpointSmartConsole R77.30" e ingresamos a la aplicación, SmartDashboard ingresando el usuario y la clave de contingencia

7. En caso de no visualizar las reglas, contactar al proveedor para repetir el procedimiento.

8. Abrir el Objeto del Firewall, clic en communication, clic en el botón "Reset" Y le preguntará si está seguro de que desea restablecer, dar clic en "Yes": Se desplegará una notificación. dar clic en Aceptar"

9. Introduzca la nueva clave del SIC, una vez que el SIC se ha inicializado, verá el icono de estado de certificado de color verde y la nota "Trust established"; dar clic en "OK"

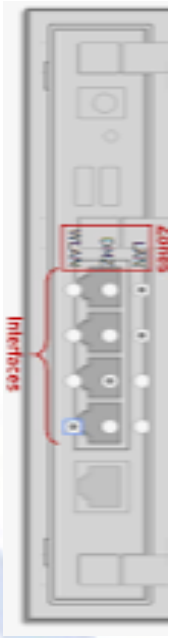


INSTRUCTIVO PARA CONECTAR LAS INTERFACES DEL FIREWALL

Firewall Principal

Distribución de interfaces y Conexiones físicas

SERVIDOR DL 380 G8 (PRINCIPAL)			
Red	**PUERTO**		**Etiqueta cable**
192.xxx.xx.x	ETH1	**INTERFACES MAINBOARD**	1
192.xxx.xx.x	ETH2		2
192.xxx.xx.xxx	ETH3		3
190.xxx.xxx.xx	ETH4		4
200.xxx.xx.xx	ETH1	**INTERFACES TARJETA PCI**	5
132.xxx.xx.xx	ETH2		6
192.xxx.xx.xxx	ETH3		7
192.xxx.xx.xxx	ETH4		8



GLOSARIO

FIREWALL: Un cortafuegos (*firewall*) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Reglas de Red: Reglas de Red son aquellas reglas que se aplican en un equipo de seguridad de datos como Firewall para indicar los accesos y bloqueos que ha determinado la Institución para asegurar la información

Interfaces de Red: Son dispositivos que permiten la conexión de elementos pasivo de red como cables UTP, Fibra o Coaxial según el tipo de Interfaz, con el fin de poder conectar un dispositivo o servidor a una red de datos

Procedimiento de contingencia: Son los procedimientos de aplicación para activar la infraestructura de contingencia de tecnología.

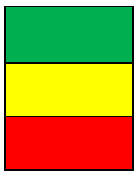
Procedimiento de Restauración: Son los procedimientos de aplicación que permiten regresar desde los procedimientos de contingencia a la infraestructura principal

PROCEDIMIENTOS DE CONTINGENCIA DEL NEGOCIO EN CASO DE FALLA DEL SERVIDOR DE RED

Objetivo

Definir las acciones, procedimientos y recurso humano para garantizar la recuperación de los servicios a través del servidor de red.

Según cada caso de amenaza existen diferentes actividades a realizar las cuales se muestran a continuación en las respectivas tablas con los identificadores:



Verde: seguir con las actividades de manera habitual

Amarillo: tomar acciones de prevención y asegurar respaldos

Rojo: ejecutar el plan de continuidad (recuperar los procesos)

AMENAZAS QUE SE PODRÍAN PRESENTAR	**RESPONSABLE**
Daños ocasionados por agua (**mirar las tablas 1,2 y 3 en la amenaza correspondiente**)	JEFE ENCARGADO DE LA UNIDAD DE TIC
Daños ocasionados por fuego (**mirar las tablas 1,2 y 3 en la amenaza correspondiente**)	
Daños ocasionados por corte de suministro eléctrico (**mirar las tablas 1,2 y 3 en la amenaza correspondiente**)	
Daños ocasionados por condiciones inadecuadas de temperatura y humedad (**mirar las tablas 1,2 y 3 en la amenaza correspondiente**)	
Desconexión deliberada o accidental del equipo (**mirar las tablas 1,2 y 3 en la amenaza correspondiente**)	
Falta de actualizaciones de versión de sistema operativo (**mirar las tablas 1,2 y 3 en la amenaza correspondiente**)	

Para conocer cuáles son las acciones a realizar antes, durante y después de haber ocurrido cada amenaza revisar las **siguientes tres tablas** las cuales poseen la información detallada de acciones a realizar.

Tabla N° 1: En el caso de presentarse daños previos a el incidente

CASO AMENAZA	ACTIVIDADES POR REALIZAR	Responsable
Daños ocasionados por agua	1. Revisar la existencia de filtraciones 2. Informar al personal respectivo en caso de hallar daños físicos en paredes	JEFE ENCARGADO DE LA UNIDAD DE TIC
Daños ocasionados por fuego	1. Extintores en excelente estado 2. Mantas apropiadas 3. Procurar no almacenar productos inflamables	
Daños ocasionados por corte de suministro eléctrico	1. Tener conectado el UPS 2. Sacar respaldos en tiempos establecidos 3. Revisar las conexiones periódicamente	
Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1. Adecuar el lugar 2. Conexiones seguras 3. Ventilación adecuada 4. Impermeabilidad de piso, techo y paredes	
Desconexión deliberada o accidental del equipo	1. Colocar canaletas 2. Conexión de cableado adecuado 3. Espacio correcto de conectores	
Falta de actualizaciones de versión de sistema operativo	1. Realizar mantenimiento 2. Adquirir licencias de sistemas operativos 3. Tener antivirus activos	

Tabla N° 2: Se detallan las acciones ya actividades a realizar en el caso de presentarse daños durante el incidente de:

CASO AMENAZA	ACCIONES	Responsable
Daños ocasionados por agua	1. Secar el agua de inmediato con mantas o material absorbente. 2. Cubrir con mantas a prueba de agua	JEFE ENCARGADO DE LA UNIDAD DE TIC
Daños ocasionados por fuego	1. Conserve la calma 2. Hacer uso de los extintores en el área incendiada 3. Si el fuego es de origen eléctrico no intente apagarlo con agua 4. Retirar elementos de acción rápida al fuego 5. Al momento de abrir una puerta, verifique que la chapa no esté	

	caliente antes de abrirla; sí lo está, lo más probable es que haya fuego al otro lado de ella, no la abra. 6. Si se incendia su ropa, no corra: tírese al piso y ruede lentamente. De ser posible cúbrase con una manta para apagar el fuego. 7. Alejar los elementos que están cerca	
Daños ocasionados por corte de suministro eléctrico	1. Evitar que los cables en mal estado choquen entre si 2. Verificar el tiempo de duración del UPS 3. Asegurar respaldo 4. Guardar información sensible	
Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1. Realizar respaldos de información de manera inmediata 2. Impermeabilidad pronta del lugar y/o adecuación de ventiladores.	
Desconexión deliberada o accidental del equipo	1. Volver a conectar de manera inmediata 2. Volver a encender el equipo 3. Comprobar su funcionamiento 4. Evitar la entrada a personal no autorizado	
Falta de actualizaciones de versión de sistema operativo	1. Comprobar la falla del equipo (acciones correctivas) 2. Realizar la actualización de inmediato 3. Revisar si los antivirus están activados	

Evaluación de daños

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo.

Tabla N° 3: En el caso de presentarse daños después del incidente de:

CASO AMENAZA	ACCIONES	Responsable

Daños ocasionados por agua	1. Secar los equipos que hayan sido afectados por el agua 2. Revisar los equipos para ver si funcionan 3. Realizar un inventario de los equipos funcionales y de los que se debe dar de baja	JEFE ENCARGADO DE LA UNIDAD DE TIC
Daños ocasionados por fuego	1. Comprobar que el fuego se haya extinguido en su totalidad 2. Retirar los restos dejados por el fuego 3. Comprobar el funcionamiento de los artefactos y equipos 4. Ventilar el área afectada	
Daños ocasionados por corte de suministro eléctrico	1. Revisar las conexiones 2. Recargar el UPS 3. Revisar los respaldos 4. Brindar de inmediato el servicio de internet	
Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1. Adecuar el lugar 2. Asegurar las conexiones (mantenimiento) 3. Adecuar la ventilación del lugar 4. Revisar y adecuar la impermeabilidad de piso, techo y paredes	
Desconexión deliberada o accidental del equipo	1. Colocar de manera correcta las conexiones y los cables en canaletas 2. Adecuar el espacio para movilizarse y evitar estos accidentes 3. Verificar estado del cableado.	
Falta de actualizaciones de versión de sistema operativo	1. Verificar el tiempo de vigencia de las licencias de los sistemas operativos 2. Revisión de antivirus (que estén activados)	

GLOSARIO DE TERMINOS

Para el propósito de este documento, los siguientes términos y definiciones

Activo de Información: Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento

Amenaza: Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.

Aplicaciones: Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la Entidad.

Control: Control: Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cortafuego (Firewall): El Cortafuegos, es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.

Datos: en general se consideran datos a todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.

Impacto: Es el resultado o efecto de un evento, el impacto de un evento quede ser positivo o negativo sobre los objetivos relacionado de la institución.

Incidente: En este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático.

Probabilidad: Posibilidad que un evento determinado ocurra en un período de tiempo dado.

Anexo: Plan de continuidad de los activos tecnológicos– Backups

Descripción de Evento

Evento:	Falla del servidor de backups
Descripción del evento:	Procedimientos relativos a sistemas de información, equipo de cómputo, obtención, almacenamiento de los respaldos de información (backups) y políticas (normas y procedimientos de backups).
Objetivo:	Garantizar la continuidad de las actividades que presenta la institución, manejando correctamente estrategias que permitan la seguridad de la información.
Entorno:	Instalaciones de la Unidad de TIC.
Personal encargado:	Personal de la Unidad de TIC
Procesos afectados	Todos los procesos del Municipio

Tiempo estimado de activación	
Nivel de afectación	

Acciones periódicas antes del evento

Personal	Actividades a realizarse
Jefe de la Unidad de Tecnología y comunicación	Respaldo diario de la información crítica (Backups de sistema operativo, aplicativo, de datos, passwords, y archivos que contengan información de la institución)
Jefe de la Unidad de Tecnología y comunicación	Validación del backups de la información, uso de formularios para registro de los backups.
Jefe de la Unidad de Tecnología y comunicación	Realizar periódicamente los backups de la información de los equipos tecnológicos de cada Unidad.

Acciones periódicas durante del evento

ACTIVIDAD	RESPONSABLE
7. Dar aviso del incidente al jefe de la Unidad Tecnología de la Información y Comunicaciones	Jefe de la unidad de Tecnología de la Información y Comunicación
8. Comunicar el Inicio de la Incidencia con el incidente de backup	
9. Analizar la unidad e información importante que se guardaba como respaldo	Jefe de la unidad de Tecnología de la Información y Comunicación
10. Ejecutar el proceso de backup en horas nocturnas	Jefe de la unidad de TIC Ing. Andrés Villarruel
11. Verificar las formas de realizar backup	
12. Verificar tamaño de archivos	
13. Iniciar proceso de backup	
14. Comprobar si se realiza la copia de seguridad de archivos	

15. Comunicar disponibilidad de servicios de backup	

Plan de comunicación de la Unidad de Tecnología y Comunicación (TIC)

SITUACIÓN	MEDIO	INFORMACIÓN RELEVANTE	RESPONSABLE DE ENVÍO
INICIO DE LA INCIDENCIA	Correo electrónico WhatsApp	Tipo de daño Servicios Afectados Tiempo estimado de restablecimiento del servicio	Director de la Unidad de Tecnología de la Información y Comunicaciones
ACTIVACIÓN DE PLAN DE CONTINGENCIA		Condiciones de funcionalidad de los equipos de contingencias Servicios restaurados	
RESTAURACIÓN DE OPERACIONES NORMALES		Fecha y hora de inicio de operaciones normales	

Instructivo de Respaldos de reglas de Backups

INSTRUCCIONES DE PROCESO DE BACKUP

1. La Unidad de TIC debe verificar que los backups deben realizarse de manera automática, al final del día llevándose a cabo en horas nocturnas para lo cual se debe tomar en cuenta:
    - Backup de base de datos
    - Backup de copias que se ejecutaran en el servidor
    - Backup de imágenes

    Para la verificación de los backup se debe realizar de dos formas:

    - Fecha de creación de backup y modificación de archivo

      Se debe verificar en la carpeta de ubicación en este caso "Backups BasedeDatos" las cuales al abrir saldrá de manera

PROCESO_Fr0012022.backup y Copia_Fr012022, tomar en cuenta que se crea con la fecha del día de creación o modificación.

- Tamaño de archivos

  Para el tamaño de las imágenes se verificará su tamaño y se almacenan de manera externa de forma diferencial.

  Backups BasedeDatos verificando el tamaño del archivo en este caso como ejemplo: PROCESO_23092022.BACKUP "size" 459.102 KB
- Los backups de realizaran al finalizar el día por programación de estas y se almacenaran en el disco duro de manera automática.
- Para verificación del backups se verifica fecha de creación en las carpetas del disco duro y visualizar el tamaño se da clic en propiedades
- Llevar una bitácora de los controles de backups con sus respectivos fechas y nombres.

Definiciones

Backup:	Copia de seguridad de aplicaciones. Base de datos, imágenes disponibles en unidades de almacenamiento, las cuales nos permiten guardar información en caso de daños, robos, etc.
Base de datos:	Conjunto de datos y archivos de un mismo grupo de datos.
Copias de seguridad:	Copias de un grupo de información en un método o instrumento de resguardo.

Anexo: Plan de continuidad de los activos tecnológicos– Base de datos

Descripción de Evento

Evento:	Falla del servidor de base de datos
Descripción del evento:	
Objetivo:	Garantizar la continuidad de las actividades que presenta la institución, manejando correctamente

	estrategias que permitan la seguridad de la información.
Entorno:	Instalaciones de la Unidad de TIC.
Personal encargado:	Personal de la Unidad de TIC
Procesos afectados	Todos los procesos del Municipio
Tiempo estimado de activación	
Nivel de afectación	

Accioness periódicas antes del evento

Personal	**Actividades a realizarse**
Jefe de la Unidad de Tecnologia y comunicación	Respaldo diario de la información crítica (de datos, passwords, y archivos que contengan información de la institución)
Jefe de la Unidad de Tecnologia y comunicación	Validación de información de base de datos de la información, uso de formularios para registro de la información.
Jefe de la Unidad de Tecnologia y comunicación	Realizar periódicamente la revisión de base de datos de la información de los equipos tecnológicos de cada Unidad.

Acciones periódicas durante del evento

ACTIVIDAD	**RESPONSABLE**
16. Dar aviso del incidente al jefe de la Unidad Tecnología de la Información y Comunicaciones	Jefe de la unidad de Tecnología de la Información y Comunicación
17. Comunicar el Inicio de la Incidencia con el incidente de base de datos	
18. Analizar la unidad e información importante que se guardaba en la base de datos	Jefe de la unidad de Tecnología de la Información y Comunicación

19. Ejecutar el proceso de base de datos	Jefe de la unidad de TIC Ing. Andrés Villarruel
20. Verificar las formas de realizar el resguardo de base de datos	
21. Verificar tamaño de archivos	
22. Iniciar proceso de verificación de base de datos	
23. Comprobar si se realiza el proceso de base de datos de los archivos	
24. Comunicar disponibilidad de servicios de base de datos	

Plan de comunicación de la Unidad de Tecnologia y Comunicación (TIC)

SITUACIÓN	**MEDIO**	**INFORMACIÓN RELEVANTE**	**RESPONSABLE DE ENVÍO**
INICIO DE LA INCIDENCIA	Correo electrónico WhatsApp	Tipo de daño Servicios Afectados Tiempo estimado de restablecimiento del servicio	Director de la Unidad de Tecnología de la Información y Comunicaciones
ACTIVACIÓN DE PLAN DE CONTINGENCIA		Condiciones de funcionalidad de los equipos de contingencias Servicios restaurados	
RESTAURACIÓN DE OPERACIONES NORMALES		Fecha y hora de inicio de operaciones normales	

Instructivo de resguardo de base de datos

INSTRUCCIONES DE PROCESO DE RESGUARDO DE BASE DE DATOS

Establecer los lineamientos para guardar la base de datos de manera que la información se encuentre en caso de una contingencia o desastre.

Es importante guardar información del municipio se encuentre almacenada en las computadoras de manera que sea confiable.

1. Se analiza la información más importante para resguardar.
2. Se define el periodo de conservación de la información.
3. Se realiza una solicitud para asignar una unidad y acceso del usuario.
4. Se verifica información y se verifica en caso de respaldo sea de manera exitosa.
5. Cada usuario es responsable de información en cada unidad para luego respaldar, la cual se debe crear un directorio de respaldo.
6. La cual se debe establecer tiempo de prioridad que pueden ser semanal o mensual.
7. Se debe establecer que métodos se va a utilizar para generarse una base de datos de información para ello se debe mantener si es una copia norma, diaria o incremental.
8. La información debe ser confidencial, integral y se debe asegurar de su disponibilidad.
9. Para lo cual se debe realizar actividades antes de tener en cuenta una base de datos:
    - Analizar las carpetas para el respaldo
    - Actualizar los datos de cada tabla de cada respaldo
    - Verificar en el sistema si se encuentra la base de respaldos.

Definiciones

Base de datos:	Conjunto de datos y archivos de un mismo grupo de datos.
Copias de seguridad:	Copias de un grupo de información en un método o instrumento de resguardo.

Comité De Crisis

Este grupo conformado por personal de la institución se encarga de activar y dirigir el plan de continuidad del negocio ante la presencia de una

eventualidad. Frente a una situación de crisis se debe tomar en cuenta el tiempo máximo tolerable de inactividad de cada proceso crítico para determinar si es necesario que este se active o no este comité.

Los miembros que conforman el comité de crisis son:

CONFORMACIÓN DEL COMITÉ DE CRISIS		
Responsable del comité de crisis	Jefe de la Unidad de TIC	Es la persona encargada de dirigirse a los miembros el cual tiene como deber de comunicarse, notificar de diferentes eventos.
Miembros del comité de crisis	Alcalde Personal de la Unidad de TIC Directores de las diferentes Unidades	Son personas que ayudan a dar solución, contribuir con información verídica de diferentes hechos.
Lugar de Reunión	Sala de reuniones de Alcaldía	

Fase 4: Prueba, mantenimiento, revisión

En esta fase se determina la frecuencia y las actividades a realizarse para llevar a cabo las pruebas necesarias de los diferentes componentes del BCP.

Plan De Prueba Y Revisión

PLAN DE PRUEBAS DE LOS COMPONENTES DEL BCP

Objetivo	Establecer la periodicidad y las acciones a ejecutarse para validar las estrategias determinadas en el proceso de continuidad del negocio y en el caso de requerirlo utilizar las mejoras necesarias.
Alcance	El plan de pruebas se aplica a todos los componentes que conforman el BCP

Componentes	Roles y responsabilidades
	BIA
	Análisis de riesgos
	Estrategias de recuperación
	Auditoría interna
	Capacitaciones
	Comunicación del BCP
	Actualización del BCP

Plan de mantenimiento del BCP

FRECUENCIA DE MANTENIMIENTO DEL BCP

Componente	**Método**	**Frecuencia**
Roles y responsabilidades	Revisión de roles y responsabilidades por parte del área de recursos humanos	Anual
	Actualización de perfiles	
	Actualización de movimiento de personal o funciones	
BIA	Revisión y actualización de procesos críticos y tiempos máximos tolerables de inactividad	Anual

Análisis de riesgos	Exploración y actualización de activos críticos y nivel de riesgo determinado	Anual
Estrategias de recuperación	Simulación de eventos disruptivos de manera planificada y fuera de horario laboral	e Semestral
Auditoría interna	Planificación para auditar internamente los procesos de TI	Anual
Capacitaciones	Planificación de capacitaciones para el personal en temas relacionados con tecnología	Trimestral
Comunicación del BCP	Socialización del BCP mediante correo electrónico o reuniones de área	Semestral
Actualización del BCP	Con base en todos los componentes y pruebas realizadas, el BCP se mantendrá actualizado y con las mejoras sugeridas en cada escenario	Semestral

Fase 5: Capacitación y concienciación

Dentro de esta fase se proponen, de manera tentativa, los temas de capacitación y los medios a emplearse para socializar el BCP.

Plan de capacitación y concienciación

Inicialmente, el plan de capacitación y concienciación está dirigido al personal de la Unidad de TIC. En la, se puede visualizar de manera general los temarios

tentativos que están relacionados con la continuidad del negocio y que servirán para reforzar o actualizar los conocimientos del personal técnico.

El responsable de la Unidad de TIC definirá los temas prioritarios para la capacitación y lo comunicará mediante correo electrónico. Los horarios y participantes serán establecidos de manera que no afecte a la continuidad operativa

TEMARIO GENERAL DE CAPACITACIÓN

Temario	**Duración (horas)**
Normas y estándares de seguridad de la información	40
Fundamentos de Ciberseguridad	30
Metodologías de análisis de riesgos	30
Hacking ético	40
Gestión y respuesta de riesgos	30
Gestión de continuidad del negocio	40

Con el fin de lograr una comunicación efectiva, la socialización del plan de continuidad del negocio se realizará mediante mensajes por correo electrónico, videos explicativos y charlas.

Anexos

Anexo 1. Inventario de Recursos Tecnológicos

PRIMER PISO					
DESCRIPCIÓN	**IP**	**MARCA**	**SISTEMA OPERATIVO**	**TIPO-ACTIVO**	**DEPARTAMENTO**
ESCRITORIO	[redacted]	LENOVO	Windows 7 Profesional	FIJO	RECAUDACIÓN
ESCRITORIO		LENOVO	Windows 10 Profesional	FIJO	RECAUDACIÓN
IMPRESORA		EPSON		FIJO	RECAUDACIÓN
IMPRESORA		EPSON LX350		FIJO	RECAUDACIÓN
IMPRESORA		EPSON LX 300 + II		FIJO	RECAUDACIÓN
IMPRESORA		SAMSUNG		FIJO	RECAUDACIÓN
ESCRITORIO		PRIMA	Windows 7 Ultimate	FIJO	AVALUOS
ESCRITORIO		PRIMA	Windows 7 Profesional	FIJO	AVALUOS

LAPTOP	[redacted]	HP	windows 10 Pro	FIJO	AVALUOS
IMPRESORA		EPSON L55		FIJO	AVALUOS
FOTOCOPIADORA		RICOH Aficio MPC5000		FIJO	AVALUOS
ESCRITORIO		SAMSUNG	Windows 10 Pro	FIJO	TALENTO HUMANO
ESCRITORIO		SAMSUNG	Windows 10 Pro	FIJO	TALENTO HUMANO
ESCRITORIO		LENOVO	Windows 10 Pro	FIJO	TALENTO HUMANO
IMPRESORA		EPSON L575		FIJO	TALENTO HUMANO
ESCRITORIO		LG- CPU QUASAD		FIJO	ASISTENTE REGISTRO DE LA PROPIEDAD
IMPRESORA		EPSON L575		FIJO	ASISTENTE REGISTRO DE LA PROPIEDAD
ESCRITORIO		AOC		FIJO	ANALISTA DEL REGISTRO DE LA PROPIE
ESCRITORIO		LG		FIJO	ANALISTA DEL REGISTRO DE LA PROPIE

ROUTER	[redacted]	DLINK		FIJO	ANALISTA DEL REGISTRO DE LA PROPIE
IMPRESORA		RICOH MP C401SR		FIJO	REGISTRO DE LA PROPIEDAD
ESCRITORIO		LG		FIJO	ASISTENTE TÉCNICO
IMPRESORA		HP LASER JET P1102W		FIJO	ASISTENTE TÉCNICO
ESCRITORIO		LG		FIJO	BODEGA
ESCRITORIO		LG- CPU Altekpe		FIJO	TESORERIA
ESCRITORIO		AOC - cpu LG		FIJO	TESORERIA
IMPRESORA		LEXMARK MX410		FIJO	TESORERIA
LAPTOP		TOSHIBA	Windows 7	FIJO	COMPRAS PÚBLICAS
IMPRESORA		EPSON L575		FIJO	COMPRAS PÚBLICAS
[redacted]					
ESCRITORIO		LG	Windows 7 Ultimate	FIJO	CONTABILIDAD

ESCRITORIO	[redacted]	LENOVO	Windows 10 Pro	FIJO	CONTABILIDAD
ESCRITORIO		LENOVO	Windows 10 Pro	FIJO	CONTABILIDAD
ESCRITORIO		LENOVO	Windows 10 Pro	FIJO	CONTABILIDAD
ESCRITORIO		LENOVO	Windows 8	FIJO	CONTABILIDAD
PORTATIL		DELL	Windows 10 Pro	FIJO	DEPARTAMENTO FINANCIERO
ESCRITORIO		SAMSUNG	Windows 7 Ultimate	FIJO	OBRAS PUBLICAS
ESCRITORIO		LG	Windows 7 Ultimate	FIJO	OBRAS PUBLICAS
ESCRITORIO		LG	Windows 10 Pro	FIJO	OBRAS PUBLICAS
ESCRITORIO		LG	Windows 10 Pro	FIJO	OBRAS PUBLICAS
ESCRITORIO		SAMSUNG	Windows 10 Home	FIJO	OBRAS PUBLICAS
IMPRESORA		EPSON Workforce WF-7720		FIJO	OBRAS PUBLICAS
IMPRESORA		SCX-430		FIJO	OBRAS PUBLICAS

IMPRESORA	[redacted]	SAMSUNG ML-2010		FIJO	OBRAS PUBLICAS
IMPRESORA		HP		FIJO	OBRAS PUBLICAS
IMPRESORA		HP Desinger T1100		FIJO	OBRAS PUBLICAS
Consola de audio				FIJO	OBRAS PUBLICAS
Parlante				FIJO	OBRAS PUBLICAS
Dron		FIMI X82020		FIJO	OBRAS PUBLICAS
ESCRITORIO		HP	Windows 10	FIJO	COMUNICACIÓN
ESCRITORIO		HP	Windows 10	FIJO	COMUNICACIÓN
IMPRESORA		L575		FIJO	COMUNICACIÓN
ESCRITORIO		LENOVO	Windows 7 Pro	FIJO	SISTEMAS
ESCRITORIO		LENOVO	Windows 7 Pro	FIJO	SISTEMAS
LAPTOP		DELL	Windows 10	FIJO	SISTEMAS
LAPTOP		TOSHIBA	Windows 10	FIJO	SISTEMAS
Swith 24 puertos				FIJO	SISTEMAS
Router		T-Plink ac-1200		FIJO	SISTEMAS
Impresora		L20		FIJO	SISTEMAS
Infocus		Lw		FIJO	SISTEMAS
Infocus		EPSON			

ESCRITORIO	[redacted]	AOC			PLANFICACIÓN
LAPTOP			Windows 7 Pro	FIJO	PLANFICACIÓN
ESCANER		HP	ScanJetPro 2500	FIJO	PLANFICACIÓN
LAPTOP		DELL		FIJO	PLANFICACIÓN
IMPRESORA		EPSON WORKFORCE 7720		FIJO	PLANFICACIÓN
ESCRITORIO		SAMSUNG		FIJO	PLANFICACIÓN
ESCRITORIO		LG		FIJO	PLANFICACIÓN
2 PRPYECTORES		EPSON-INFOCUS		FIJO	PLANFICACIÓN
LAPTOP		TOSHIBA	WINDOWS 10	FIJO	PLANFICACIÓN
ESCRITORIO		LG		FIJO	PLANFICACIÓN
ESCRITORIO		LENOVO		FIJO	AMBIIENTAL
IMPRESORA		EPSON L555		FIJO	AMBIIENTAL
IMPRESORA		HP Laser Jet 3555		FIJO	AMBIIENTAL
ESCRITORIO		LG		FIJO	AMBIIENTAL
IMPRESORA		EPSON L555		FIJO	AMBIIENTAL
ESCRITORIO		Delux	Windows 7 Pro	FIJO	SECRETARIA GENERAL
IMPPRESORA		EPSON 14160		FIJO	SECRETARIA GENERAL

IMPRESORA	[redacted]	EPSON L555		FIJO	PROCADURÍA
ESCRITORIO		LG		FIJO	RECEPCIÓN
IMPRESORA		EPSON 3110		FIJO	RECEPCIÓN
ESCRITORIO		LENOVO		FIJO	ALCALDIA