UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

Tema: PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) APLICADO AL DEPARTAMENTO DE TI DE LA EMPRESA DE SOLUCIONES TECNOLÓGICAS TELECOMSEC

Trabajo de Titulación, previo a la obtención del grado académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada

Autora: Ingeniera Paola Alexandra Díaz Parco

Director: Ingeniero Ángel Gabriel Jaramillo Alcázar, Magister.

Ambato – Ecuador

2022

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado. PhD, e integrado por los señores: Ingeniero Mentor Javier Sánchez Guerrero, Magister; Ingeniero Carlos Alberto Martínez Bonilla, Magister, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: *"Plan de Continuidad del Negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC"* elaborado y presentado por la *señora Ingeniera Paola Alexandra Díaz Parco,* para optar por el Grado Académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.

Presidente y Miembro del Tribunal

Ing. Mentor Javier Sánchez Guerrero. Mg.

Miembro del Tribunal

Ing. Carlos Alberto Martínez Bonilla. Mg.

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Plan de Continuidad del Negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC, le corresponde exclusivamente a: Ingeniera Paola Alexandra Díaz Parco, Autora bajo la Dirección del Ingeniero Ángel Gabriel Jaramillo Alcázar, Magister, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniera Paola Alexandra Díaz Parco
c.c.: 1002938056
AUTORA

Ingeniero Ángel Gabriel Jaramillo Alcázar, Magister
c.c.: 1715891964
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniera Paola Alexandra Díaz Parco

c.c.: 1002938056

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

Gracias a Dios por cada día nuevo, por cada alegría, por cada enseñanza, por mi familia, por mis amigos, por permitirme avanzar un paso a la vez.

Mi sincero agradecimiento a los docentes de Posgrado de la Universidad Técnica de Ambato por impartir sus conocimientos y experiencias profesionales, siendo de gran apoyo para culminar con mi meta propuesta.

A mi director de proyecto de titulación, Mg. Ángel Jaramillo, por su valioso aporte y el tiempo dedicado en las tutorías.

A la empresa TELECOMSEC por permitirme desarrollar mi proyecto, de manera especial al Ing. Luis Plasencia por su colaboración y apoyo.

A mis compañeros de clase, por todo el apoyo brindado a lo largo de esta maestría. Fue una linda experiencia.

A todos ustedes, mil gracias

Paola

DEDICATORIA

Este trabajo está dedicado a mi familia:

A mi pequeño príncipe, que es mi fuerza y mi motivación para avanzar cada día. Gracias por tanta felicidad. Eres el amor de mi vida.

A mi esposo, amigo y compañero de vida, gracias por todo lo que compartimos día a día, gracias por tu motivación y apoyo. Somos el mejor equipo. Te amo infinitamente.

A mis padres, que siempre han confiado en mí y han apoyado cada una de mis decisiones. Gracias por toda su ayuda incondicional.

A mis hermanos, gracias por estar cuando los necesito.

Con mucho amor,
Paola

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) APLICADO AL DEPARTAMENTO DE TI DE LA EMPRESA DE SOLUCIONES TECNOLÓGICAS TELECOMSEC

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con componente de investigación aplicada*
AUTOR: *Ingeniera Paola Alexandra Díaz Parco*
DIRECTOR: *Ingeniero Ángel Gabriel Jaramillo Alcázar, Magister*
FECHA: *Veintitrés de agosto de dos mil veintidós*

RESUMEN EJECUTIVO

El Plan de Continuidad del Negocio (BCP) propuesto para el departamento de Tecnologías de la Información (TI) de la empresa TELECOMSEC, está enfocado en describir la manera en la que dicha empresa se mantenga operativa durante la interrupción no planificada de uno o varios de sus servicios. Este BCP constituye una guía de referencia con estrategias planificadas y organizadas que permiten hacerle frente a un incidente materializado en el menor tiempo posible.

Es importante conocer la situación actual de la empresa con respecto a la infraestructura tecnológica, roles del personal técnico y los servicios que ofrece, por lo cual se realizó el levantamiento de información relevante para el desarrollo de este proyecto. El apoyo de los directivos y del personal operativo es fundamental al momento de aplicar los diferentes instrumentos para recolección de información.

Se llevó a cabo el análisis de impacto del negocio BIA (Business Impact Analysis) para determinar los procesos y servicios críticos que deben ser recuperados de manera prioritaria dentro del tiempo máximo tolerable establecido. Posteriormente, se realizó el análisis de riesgos de los activos críticos del departamento de TI de la empresa TELECOMSEC, aplicando la metodología MAGERIT.

En base a los resultados obtenidos en la fase de evaluación de riesgos previa, se estableció las estrategias operacionales y se diseñó el Plan de Continuidad del Negocio considerando diferentes escenarios, tomando como referencias los lineamientos establecidos en la norma internacional ISO 22301:2019. También se definió el plan de pruebas, mantenimiento y revisión de los componentes del BCP.

Finalmente, en la fase de capacitación y concienciación se propuso un temario con varias alternativas para ser impartido al personal técnico. Los temas son seleccionados por el responsable del departamento de TI según la necesidad de la empresa. De igual manera, se sugirió diversas formas en las que se puede socializar el BCP.

DESCRIPTORES: ACTIVO, AMENAZA, ANÁLISIS DE IMPACTO**,** CONFIDENCIALIDAD, CONTINUIDAD DEL NEGOCIO, CRITICIDAD, DISPONIBILIDAD, INTEGRIDAD, NORMA ISO 22301, RIESGO, VULNERABILIDAD.

UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

THEME:

BUSINESS CONTINUITY PLAN (BCP) APPLIED TO THE IT DEPARTMENT OF THE TECHNOLOGICAL SOLUTIONS COMPANY TELECOMSEC

DEGREE MODALITY: *Degree Project with an applied research component*
AUTHOR: *Engineer Paola Alexandra Díaz Parco*
DIRECTED BY: *Engineer Ángel Gabriel Jaramillo Alcázar, Master*
DATE: *August twenty-third, two thousand twenty-two*

EXECUTIVE SUMMARY

The Business Continuity Plan (BCP) proposed for the Information Technology (IT) department of the TELECOMSEC company is focused on describing the way in which said company remains operational during the unplanned interruption of one or more of the its services. This BCP constitutes a reference guide with planned and organized strategies that allow dealing with a materialized incident in the shortest possible time.

It is important to know the current situation of the company with respect to technological infrastructure, roles of technical personnel and the services it offers, for which relevant information was collected for the development of this project. The support of managers and operational staff is essential when applying the different instruments for collecting information.

The business impact analysis (BIA) was carried out to determine the critical processes and services that must be recovered as a priority within the established

maximum tolerable time. Subsequently, the risk analysis of the critical assets of the IT department of the TELECOMSEC Company was carried out, applying the MAGERIT methodology.

Based on the results obtained in the previous risk assessment phase, the operational strategies were established and the Business Continuity Plan was designed considering different scenarios, taking as references the guidelines established in the international standard ISO 22301:2019. The testing, maintenance and review plan for the BCP components was also defined.

Finally, in the training and awareness phase, a syllabus was proposed with several alternatives to be taught to the technical staff. The topics are selected by the person in charge of the IT department according to the need of the company. Similarly, various ways in which the BCP can be socialized were suggested.

KEYWORDS: ASSET, AVAILABILITY, BUSINESS CONTINUITY, CONFIDENTIALITY, CRITICALITY, IMPACT ANALYSIS, INTEGRITY, ISO 22301 STANDARD, RISK, THREAT, VULNERABILITY.

CAPÍTULO I
PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

Existe una alta probabilidad de que un proceso se vea afectado por un incidente, esto se debe a que el riesgo siempre está presente y puede manifestarse de diversas maneras, ya sea como una amenaza natural, fallas humanas o tecnológicas, ataques de ciberseguridad, entre otros.

Con estos riesgos latentes, es importante que cada organización conozca su capacidad de reacción ante una eventualidad no planificada que pueda presentarse ya sea interna o externamente y que puede comprometer el desarrollo de sus actividades.

Una estrategia fundamental es que dentro de la organización se desarrolle una Plan de Continuidad de Negocio (BCP), en el que se incluyan los activos y procesos críticos y que debe ser constantemente revisado y actualizado. El BCP puede ser implementado en pequeñas, medianas y grandes empresas para definir las acciones que se deben ejecutar y los responsables de cada una de ellas.

El BCP está basado en la norma internacional ISO 22301 que contiene los requisitos para llevar a cabo de forma correcta y adecuada, la implementación de un Sistema de Gestión de Continuidad de Negocio, permitiendo entregar productos o servicios a niveles aceptables previamente establecidos luego de un evento de interrupción. Generalmente, se activa en respuesta a eventos que amenazan la viabilidad de una organización.

El objetivo de la norma ISO 22301:2019, se enfoca en dar una respuesta rápida y efectiva a un incidente, definiendo roles y responsabilidades, a diferencia de la revisión anterior publicada en el año 2012, en la que su objetivo principal era cumplir con toda la información documentada que se requería según la norma.

En este proyecto se lleva a cabo el análisis de impacto del negocio BIA y la evaluación de riesgos aplicando la metodología MAGERIT. Con los resultados obtenidos en estos análisis es posible definir las estrategias de recuperación necesarias para la elaboración del BCP.

En el Capítulo I, se describe el problema de investigación que contiene la introducción, justificación, objetivo general y objetivos específicos.

El Capítulo II, contiene una descripción de los antecedentes investigativos relacionados al tema propuesto.

En el Capítulo III, se desarrolla el marco metodológico que contiene varios parámetros sobre la ejecución del proyecto.

En el Capítulo IV, se describen los resultados y discusión en donde se exponen las derivaciones correspondientes de los análisis previos.

El capítulo V, contiene conclusiones, recomendaciones, bibliografía y anexos.

En el capítulo VI, se documenta el BCP propuesto para la empresa TELECOMSEC.

1.2. Justificación

Las organizaciones en general deben tomar medidas de prevención, protección y reacción ante eventos de seguridad que puedan afectar el desarrollo normal de sus operaciones, causando un gran impacto en la entrega de sus servicios.

No obstante, pueden ocurrir sucesos (pandemias, desastres naturales, ataques informáticos, entre otros) que ponen en manifiesto la necesidad de minimizar sus consecuencias, afrontando estos eventos de una manera estratégicamente planificada y organizada.

El presente proyecto se desarrolló con la finalidad de diseñar un BCP tomando como referencia la norma ISO 22301:2019, enfocado en proteger los principales activos de información y procesos críticos del área de TI de la empresa TELECOMSEC, mediante un conjunto de estrategias que permiten prevenir, contener y recuperarse ante la ocurrencia de eventos no deseados, en un determinado tiempo sin comprometer la disponibilidad de sus servicios.

De esta manera se posibilita la ejecución de acciones de manera planificada ante cualquier incidente de seguridad. Esto trascenderá de forma positiva cuidando la imagen y reputación de la empresa en mención, ante sus clientes y partes involucradas.

1.3. Objetivos

1.3.1. General

Elaborar el Plan de Continuidad del Negocio BCP basado en la norma ISO 22301, para el Departamento de TI de la empresa TELECOMSEC, mediante la aplicación de estrategias de prevención, contención y recuperación ante incidentes, reduciendo el tiempo de inoperatividad de los servicios.

1.3.2. Específicos

- Recopilar información de la situación actual referente a infraestructura tecnológica y servicios prestados por la empresa TELECOMSEC.
- Realizar el análisis de impacto del negocio BIA para identificar los procesos críticos de la empresa.
- Realizar el análisis de riesgos, vulnerabilidades y amenazas aplicando la metodología MAGERIT.
- Diseñar un BCP que contenga estrategias de recuperación según el tipo de incidente presentado.

CAPÍTULO II
ANTECEDENTES INVESTIGATIVOS

Un plan de continuidad es un documento que describe los procedimientos que una empresa debe seguir para permitir la continuidad de las operaciones en el caso de presentarse interrupciones en las actividades, independientemente del origen del problema. El objetivo de este plan es reestablecer las funciones principales del negocio en un tiempo aceptable, asegurando los niveles mínimos de servicio, protegiendo la reputación de la empresa y comunicando la crisis de forma adecuada.

Dentro de este plan se define la manera cómo deben actuar las diferentes áreas de la empresa para recuperarse de un incidente y seguir operando. La planificación de la continuidad del negocio trae consigo el análisis del impacto de los procesos críticos y el establecimiento de estrategias de recuperación. Toda esta información debe estar debidamente documentada y probada para lograr una eficacia óptima.

La importancia de un BCP (Business Continuity Plan del español Plan de Continuidad del Negocio) radica en mantener disponibles las funciones prioritarias de las organizaciones durante o después de situaciones de emergencia, protegiendo su imagen empresarial, disminuyendo las pérdidas financieras y minimizando el impacto de esa interrupción sobre el negocio. Es fundamental que cada organización gestione adecuadamente sus riesgos, identificándolos, evaluándolos, controlándolos y que se realice un monitoreo constante para prevenir su materialización o reducir su impacto.

El uso e implementación de diversos estándares o guías referentes a la continuidad del negocio como pueden ser la norma ISO (International Organization for Standardization) 22301, ITIL (Information Technology Infrastructure Library) o COBIT (Control Objetives for Information and Related Technology), en el desarrollo de un BCP es trascendental. Esto se debe al distinto enfoque de cada estándar y dependiendo de la necesidad interna de una organización se debe elegir el que contribuya a lograr los objetivos planteados (Mora, 2019).

El BCP busca mantener en niveles aceptables los procesos críticos del negocio, mediante una adecuada estructuración de procedimientos e información, mismos que son desarrollados, probados y están listos para ser usados en el caso de que ocurra una interrupción inesperada. Se complementa y apoya en otros planes fundamentales como son: Plan de Recuperación ante Desastres, Plan de comunicación de crisis y el Plan de emergencias (Oficina de Sistemas e Informática , 2018).

Un caso particular y reciente, se dio el 11 de marzo de 2020, cuando la Organización Mundial de la Salud (OMS) declaró como pandemia global al COVID-19. Este hecho trajo consigo muchos cambios en la forma de trabajo de innumerables empresas y organizaciones a nivel mundial, así como también se produjo el aumento y aparición de factores críticos de riesgo relacionados con la ciberseguridad. Según el Centro Criptológico Nacional de España (CCN-CERT), el 62% de los incidentes de seguridad informática en el año 2020 corresponden a errores cometidos por el recurso humano de manera involuntaria, mientras que el 14% corresponde al factor humano que ocasionó incidentes de seguridad de manera intencionada. En el año 2019, de manera oficial se reportaron 3172 ciberincidentes calificados con peligrosidad muy alta y ya en 2020 esta cifra se duplicó llegando a reportarse aproximadamente 7000 (CCN-CERT, 2021). En base a los resultados obtenidos en la investigación llevada a cabo por Quituisaca et al. (2021), determinan que es importante que las pequeñas y medianas empresas cuenten con una estrategia de continuidad de negocio para hacerle frente a situaciones que pudieran afectarlas, tomando como ejemplo el confinamiento obligatorio debido al COVID-19 en el Ecuador. Es por ello que se debe tener presente la elaboración de un plan de continuidad de negocios.

Zapata (2020) señala los pasos para el desarrollo del plan de continuidad del negocio, en base a guías de implementación y el estándar ISO 22301. El BCP propuesto en su proyecto, toma como punto inicial al departamento de TI (Tecnologías de la Información) e indica que esta investigación sirve como soporte para elaborar un BCP de manera integral en la organización. El autor justifica la inversión en un BCP,

basado en los resultados positivos de los indicadores financieros y en la mejora del nivel de madurez de la organización con respecto a seguridad informática.

Urquizo (2019) indica que uno de los principales puntos para desarrollar un BCP basado en la norma ISO 22301, es conocer y entender en detalle el giro de negocio de una organización. Esta información permite diseñar una propuesta óptima. Es fundamental pensar en la organización como un conjunto, más no como una subdivisión de áreas. Iza (2021) en su proyecto investigativo menciona que para alcanzar los resultados esperados por el BCP es prioritario que todos los miembros de la organización se comprometan y estén dispuestos a adaptarse a los cambios de mentalidad para culminar con éxito el desarrollo del plan.

Pincay (2021) en su investigación manifiesta que el objetivo es estar prevenido ante posibles interrupciones e incidentes que puedan originarse dentro de la organización independientemente del origen o causa de una amenaza. Determina también que el BCP es una herramienta prioritaria para disminuir riesgos y mantener la continuidad de las actividades. En el desarrollo de su proyecto se definen estrategias en base a los resultados del BIA (Business Impact Analysis) y utiliza KPI (Key Performance Indicator) para medir el desempeño de la empresa.

En el proyecto desarrollado por Correa (2019), recomienda documentar detalladamente la etapa de pruebas del BCP incluyendo observaciones, correcciones y mejoras de las novedades encontradas. Esto con la finalidad de lograr una retroalimentación y obtener los resultados esperados.

2.1. Normas referentes a la continuidad del negocio

En la investigación realizada por Gutiérrez (2018), sobre normas internacionales que tienen relación con la continuidad operativa, describe un listado de normas haciendo énfasis en que esta selección la realiza desde la perspectiva de tecnologías de la información. En la Tabla 1, se muestra un resumen de estas normas.

TABLA 1. NORMAS INTERNACIONALES RELACIONADAS A LA CONTINUIDAD OPERATIVA

NORMA TÉCNICA	DESCRIPCIÓN
ISO 22301	Es una norma que define los conceptos básicos que permiten desarrollar y gestionar la continuidad del negocio. Esta norma de continuidad empresarial es certificable
ITIL	Es un marco para la gestión de servicios de TI que se adecuan a las necesidades del negocio. Dentro de sus procesos se establece la Gestión de la continuidad de los servicios de TI
COBIT	Es un marco de trabajo para gobernanza y gestión de las tecnologías de la información y que en su apartado DSS04 se refiere a objetivos de control encaminados a asegurar la continuidad operativa de una organización
ISO 27031	Esta norma establece directrices para la preparación de TIC para la continuidad del negocio. Recoge los principios y conceptos sobre las TIC con la finalidad de garantizar la continuidad del negocio en cualquier tipo de organización
ISO 22399	Es una guía para desarrollar criterios propios permitiendo a las organizaciones estar preparadas ante incidentes y de esta manera se mantenga la continuidad operacional

Nota. Adaptado de "Estructura de Plan de Continuidad Operativa Bajo el Enfoque de la Gestión de Riesgo de Desastres en Empresas de Saneamiento de Agua", por P. C. Gutiérrez, 2018, *Ciencia & trabajo, 20(63),* p. 172

Para la selección de la norma que sirvió como guía para la implementación del BCP propuesto, se analizaron varios estándares y normas internacionales que tiene relación con la continuidad del negocio. En la Tabla 2, se muestra un cuadro comparativo en base al cumplimiento de parámetros técnicos.

TABLA 2. CUADRO COMPARATIVO DE PARÁMETROS TÉCNICOS DE NORMAS INTERNACIONALES

PARÁMETROS	ISO 22301	ITIL	COBIT	ISO 27031	ISO 22399

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				
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

Nota. Elaboración propia

Según el cuadro comparativo anterior, se puede evidenciar que la norma ISO 22301 cumple con todos los parámetros necesarios para gestión de continuidad del negocio. Esta guía considera todos los servicios, activos y procesos de la organización en relación con ITIL cuyo enfoque es el proceso de gestión de continuidad de los servicios de TI. Por otro lado, COBIT hace énfasis en el cumplimiento regulatorio para agregar valor al área de TI por medio del dominio DSS04 (Deliver, Service and Support). La norma ISO 27031 propone prácticas enfocadas directamente en la continuidad de TIC en caso de eventos disruptivos por lo que se considera un complemento de la ISO 22301. Finalmente, la norma ISO 22399 sirve como guía para que las organizaciones establezcan sus propios criterios de desempeño frente a incidentes y en base a esto seleccionen las alternativas de continuidad de los servicios.

ISO 22300 proporciona un marco de gestión de continuidad operativa alineado con los objetivos de negocio ayudando a optimizar las inversiones realizadas en controles o salvaguardas que protejan los activos (Araujo, 2020). La norma ISO 22301 provee un marco referencial en términos de recuperación ante desastres y se asegura que la organización cuente con los procesos y procedimientos correctos para restaurar los datos críticos de los clientes (British Standards Institution, 2019). Este proceso de gestión holístico identifica amenazas potenciales para la organización y los impactos que puedan causar en las operaciones de negocios, en el supuesto caso de que lleguen a materializarse, proporcionando un marco para la construcción de la resiliencia organizacional (Intedya, 2020).

Flores (2018) sostiene que una organización puede resultar afectada por cualquier amenaza y como resultado sus actividades o servicios quedan inoperativos. Por esta razón es importante tomar las acciones necesarias para reestablecer el servicio. Afirma también que para mantener la continuidad del negocio y de las operaciones a lo largo del tiempo se necesita de una política, que describa los roles de los involucrados y las acciones que tienen a su cargo. La importancia de estar preparados ante cualquier situación crítica y tener como base la norma ISO 22301 y sus recomendaciones con respecto al BCP, son factores relevantes dentro de una organización (Córdova & Solano, 2021).

El objetivo del Sistema de Gestión de Continuidad de negocio (SGCN) descrito en la norma ISO 22301 es brindar un apoyo a las organizaciones para protegerse, mitigar o recuperarse de cualquier evento no planificado (Ángulo et al., 2020). Una gestión adecuada del SGCN, proporciona resiliencia a la organización frente a interrupciones que alteren la operatividad del servicio.

Intedya (2021) señala que la norma ISO 22301 puede ser implementada por organizaciones de cualquier tamaño, tanto para bienes como para servicios, ya que plantea de una forma precisa la preparación, prevención, gestión y recuperación de las empresas ante situaciones que podrían ser muy complejas de manejar. Su

principal beneficio es evitar la improvisación en estos casos. Esto lo reafirma el Instituto Nacional de Ciberseguridad manifestando que es posible creer que la continuidad del negocio es aplicable únicamente en grandes organizaciones, sin embargo, esto no es verdadero, ya que cada organización establece las medidas necesarias y proporcionales a sus necesidades para garantizar su continuidad en caso de desastres (Incibe, 2018).

La estructura de la norma ISO 22301:2019 se basa en 10 puntos prioritarios. Dentro de esta estructura, a partir del numeral 4 se establecen las cláusulas y sus respectivos parámetros de cumplimiento denominados dimensiones, para gestionar la continuidad de las operaciones dentro de una organización. En la Tabla 3 (Olarte, 2016, págs. 38-39), se puede apreciar la forma en la que está organizada la norma.

TABLA 3. ESTRUCTURA DE LA NORMA ISO 22301

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
	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 continua asociada al mantenimiento, actualización y conciencia sobre SGCN

Nota. Adaptado de "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", por A. D. Olarte, 2016, *Signos, 8(1),* p. 31-44

Para evaluar el nivel de gestión de continuidad de las operaciones dentro de una organización, es necesario realizar una evaluación inicial de cumplimiento de las distintas cláusulas establecidas en la norma ISO 22301. En la Tabla 4 (Olarte, 2016, pág. 41), se establecen los criterios de ponderación y su respectiva descripción.

TABLA 4. CRITERIOS DE VALORACIÓN DE NIVEL DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Ponderación	Calificación	Descripción
Entre 0 y 1	En preparación	La organización no cumple con los criterios definidos en la norma ISO 22301. Es necesario definir una metodología de trabajo para iniciar con el SGCN
Entre 1,1 - 2	Básico	La organización acata algunos de los criterios preliminares de un SGCN, sin embargo, aún no cumple con las exigencias mínimas determinadas en la norma ISO 22301
Entre 2,1 - 3	Establecido	La organización ha definido los aspectos y criterios principales de un SGCN, basándose en los requerimientos de la norma ISO 22301. Cuenta con un contingente básico para responder posibles eventualidades
Entre 3,1 - 4	Administrado	El SGCN cumple con los requerimientos de la norma ISO 22301, esto permite iniciar con la certificación a mediano plazo
Entre 4,1 - 5	Optimizado	La organización tiene un SGCN completo, en el que se han considerado los requisitos de la norma ISO 22301 en su totalidad. Se evidencia el apoyo de los directivos por lo que se puede certificar a la empresa a corto plazo

Nota. Adaptado de "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", por A. D. Olarte, 2016, *Signos, 8(1),* p. 31-44

2.2. Normas y metodologías de análisis de riesgos

En el análisis comparativo de metodologías para el desarrollo de Auditorías Informáticas realizado por Cabrera (2021), la autora ratifica que existe un gran número de métodos y normas para analizar riesgos. En este contexto 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), entre otras. Es importante mencionar que cada metodología tiene sus propias características y al momento de elegir una opción, se debe contemplar la utilización de aquella que permita realizar un análisis acorde a la información disponible en la organización. Para llevar de manera correcta el proceso de análisis de riesgos, es fundamental que se realice una socialización sobre la metodología seleccionada a todas las partes interesadas.

En la Tabla 5, se describen algunas metodologías para análisis de riesgo, detallando el cumplimiento de varios parámetros considerados necesarios en el desarrollo de esta fase.

TABLA 5. CUADRO COMPARATIVO DE METODOLOGÍAS DE ANÁLISIS DE RIESGOS

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

Nota. Elaboración propia

Con base en esta comparativa, en este proyecto se utilizó la metodología MAGERIT, debido al alcance completo que ofrece en el análisis y gestión de riesgos. Posee

amplia documentación referente a recursos de información, amenazas y tipos de activos. Permite analizar los riesgos de forma cuantitativa y cualitativa y es de libre uso. Motaki (2016) en la evaluación realizada dentro de su proyecto de investigación, concluye que la metodología MAGERIT es la más adecuada para infraestructuras críticas, además de que ofrece un entorno más amigable para el usuario.

MAGERIT versión 3 fue desarrollada por el Consejo Superior de Administración Electrónica y actualmente es revisada desde la Secretaría General de Administración Digital con la colaboración del Centro Criptológico Nacional en España. Es una metodología de carácter público que puede ser utilizada de forma libre sin autorización previa. Se enfoca en cumplir con el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la relación con las tecnologías de la información para lograr metas, prestar servicios y alcanzar los objetivos de la organización. MAGERIT implementa el Proceso de Gestión de Riesgos basándose en la normativa ISO 31000.

La metodología se centra en conseguir los siguientes objetivos:

- Concienciar a los responsables de las organizaciones de información sobre la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control
- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación

Durante la realización del respectivo análisis de riesgos, el uso de MAGERIT implica una gran ayuda. Inicialmente se identifican los activos, amenazas, detección de las salvaguardas y posteriormente permite desarrollar acciones para controlar y reducir los riesgos encontrados (Cabrejos, 2020).

En la revista científica y tecnológica UPSE (Universidad Estatal Península de Santa Elena), se expone un artículo en el cual se utiliza la metodología MAGERIT para describir el proceso de análisis y gestión de riesgos de los sistemas de información de las organizaciones públicas y privadas de manera general. Aquí se destacan las ventajas y los pasos que deben seguirse previamente a la elaboración de un Plan de Contingencia (Ferruzola et al., 2019).

Santa María (2020), en su trabajo de investigación desarrolló la propuesta de un plan basado en la Metodología MAGERIT cuyo objetivo fue el de reducir los riesgos operativos de tecnologías de la información en la Caja Piura. Para esto llevó a cabo el análisis de los riesgos operativos de TI que existen, el diseño de la propuesta del plan para reducir los riesgos operativos de TI y la validación el modelo propuesto.

Uno de los pasos fundamentales para el desarrollo y creación del BCP es el análisis y evaluación de riesgos. Dentro de este proyecto se ha propuesto utilizar la metodología de análisis y gestión de riesgos MAGERIT V3. El proceso de gestión de riesgos de esta metodología se centra en un marco de trabajo en el cual la toma de decisiones se define considerando los riesgos derivados del uso de tecnologías de la información (Imbaquingo et al., 2016).

2.3. Tipos de amenazas en TI

El Instituto Nacional de Ciberseguridad, define el término amenaza como una circunstancia desfavorable y que una vez que ha ocurrido genera consecuencias negativas sobre los activos como indisponibilidad, mal funcionamiento o pérdida de valor. Las amenazas pueden producirse por causas naturales, accidentales o intencionadas (INCIBE, 2020).

También se considera como amenaza a toda acción que aprovecha una vulnerabilidad para atacar o penetrar un sistema informático. En su mayoría las amenazas provienen en gran medida de ataques externos, aunque también existen amenazas internas como robo de información o uso inadecuado de los sistemas.

Machicao (2019) dentro de su proyecto de investigación define una amenaza como un elemento o acción capaz de atentar contra la seguridad de la información. Una amenaza puede materializarse si existe una vulnerabilidad para explotar. El autor describe 3 tipos de amenazas:

- Actos originados por la criminalidad común y motivación política
- Suceso de origen físico
- Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales

El libro II – Catálogo de elementos (Ministerio de Hacienda y Administraciones Públicas, 2012), de la metodología MAGERIT describe un listado de posibles amenazas, que se resumen en la Tabla 6:

TABLA 6. CLASIFICACIÓN DE AMENAZAS SEGÚN MAGERIT V3

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
	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
Ataques intencionados	Manipulación de los registros de actividad (log)
	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
	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. Adaptado de *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, por Ministerio de Hacienda y Administraciones Públicas, 2012, p. 25-48

CAPITULO III
MARCO METODOLÓGICO

3.1. Ubicación

La empresa de soluciones tecnológicas TELECOMSEC, inició sus actividades en el año 2010 en la ciudad de Quito, donde actualmente se encuentra la oficina matriz. Está conformada por un grupo de expertos en el área de Tecnologías de la Información y fue creada con el objetivo de ofrecer sus servicios a instituciones públicas y privadas, brindando soluciones tecnológicas integrales personalizadas, basadas en el análisis de la situación de cada organización, alineándose a los objetivos y metas del negocio, entregando resultados de manera segura y eficaz.

3.2. Equipos y materiales

Para el desarrollo de este proyecto se requirió de los equipos y materiales que se describen en la Tabla 7.

TABLA 7. EQUIPOS Y MATERIALES UTILIZADOS

ÍTEM	DESCRIPCIÓN	UNIDAD	CANTIDAD	COSTO UNITARIO USD	COSTO TOTAL USD
1	Computador	unidad	1	600	600
2	Servicio de internet	horas	500		50
3	Impresora	unidad	1	300	300
4	Resma de papel	unidad	1	3	3
5	Material bibliográfico	unidad	1	0	0
Costo total					953

Nota. Elaboración propia

3.3. Tipo de investigación

La investigación es de tipo aplicada, ya que en el desarrollo de este proyecto se establecieron estrategias que son empleadas para abordar casos puntuales y que impactan de manera positiva en las actividades diarias de la empresa en estudio.

Se utilizó un enfoque cuali-cuantitativo, debido a que se realizó el análisis de riesgos y el BIA dentro de la fase de evaluación de riesgos.

También es del tipo explicativa, ya que finalmente se desarrolla un documento que contiene el Plan de Continuidad del Negocio en el que se describe de manera detallada las acciones que se deben tomar frente a incidentes presentados y los responsables de poner en marcha las medidas establecidas.

3.4. Prueba de Hipótesis

El Plan de Continuidad del negocio BCP aplicado al Departamento de TI de la empresa TELECOMSEC, influye en la disponibilidad de los servicios y sistemas de dicha empresa.

3.5. Población

Carrillo (2015) describe a la población como un conjunto de individuos, elementos o fenómenos que pueden presentar determinadas características sujetas a estudios.

La población accesible considerada dentro de este proyecto es la que conforma el departamento de TI y el Gerente General de la empresa TELECOMSEC. En la Tabla 8, se detalla la población.

TABLA 8. DETERMINACIÓN DE LA POBLACIÓN

PERSONAL	**NÚMERO DE PERSONAL**
Gerente General	1

Jefe del Departamento de Tecnologías de la Información	1
Técnico de redes	2
Técnico en seguridad informática	2
Desarrollador	2
Técnico de soporte	2
TOTAL	10

Nota. Elaboración propia

3.6. Recolección de información:

Para la recolección de información se utilizó la técnica de encuestas a través de la aplicación de cuestionarios al personal técnico de TI, ya que se buscaba conocer la capacidad de reacción de la empresa ante incidentes, así como su capacidad de recuperación y el nivel de madurez como organización para afrontar eventos no deseados.

Para determinar el nivel de criticidad de procesos y activos de TI, se utilizó la técnica de la entrevista de tipo estructurada a través del instrumento de entrevista grupal al responsable del Departamento de TI y al Gerente General, esto permitió tener una visión clara del grado de importancia de estos activos para la empresa.

Escobar y Cuervo (2008) en su publicación, definen la validación de expertos como:

> El juicio de expertos se define como una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones. (pág. 29)

La confiabilidad de los instrumentos de recolección de datos se determinó mediante la validación de expertos en reuniones llevadas a cabo con personal del área de TI y previa revisión del director de este proyecto de titulación. (Ver Anexo 5.4.2)

3.7. Procesamiento de la información y análisis estadístico

Para el procesamiento de la información se utilizó la técnica de la estadística descriptiva, que según López (2019) es una rama que permite recolectar datos y realizar los cálculos de parámetros varios, para presentarlos mediante tablas o gráficos.

El análisis de datos fue realizado con la prueba estadística T de Student para muestras emparejadas, utilizando el programa Excel.

3.8. Variables respuesta o resultados alcanzados

En la Tabla 9, se describe los resultados obtenidos, posterior a la aplicación de las técnicas de recolección de información empleadas.

TABLA 9. RESULTADOS POSTERIORES ALCANZADOS

VARIABLE	DEFINICIÓN	DIMENSIÓN	INDICADOR	TÉCNICA / INSTRUMENTO
Cumplimiento de requisitos de SGCN	El cumplimiento de requisitos del Sistema de Gestión de Continuidad del Negocio según la norma ISO 22301, ayuda a determinar el nivel inicial de madurez de la empresa en referencia a gestión de la continuidad	Valoración de las cláusulas establecidas dentro de la norma	Cumplimiento total o parcial de requisitos para la continuidad del negocio	Encuesta / Cuestionario
Análisis de Impacto del Negocio (BIA)	El BIA permite determinar los procesos críticos de la empresa y los tiempos de	Identificación de procesos Establecimiento de tiempos de	Nivel de criticidad de los procesos identificados Prioridad de recuperación de	Entrevista / Entrevista estructurada

	interrupción máximos tolerables	recuperación	los procesos	
Análisis de riesgos	El análisis de riesgos permite determinar los activos críticos de los procesos identificados en el BIA	Identificación de activos Identificación de vulnerabilidades y amenazas	Determinación del impacto y del riesgo asociado	Entrevista / Entrevista estructurada

Nota. Elaboración propia

CAPITULO IV
RESULTADOS Y DISCUSIÓN

4.1. Resultados pre-propuesta

4.1.1. Criterio inicial de cumplimiento de requisitos según ISO 22301

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.

En la Figura 1, se puede observar la valoración promedio de cada una de las dimensiones definidas dentro de cada cláusula y que se representan en las barras de color azul. Las barras de color rojo representan el valor promedio de las cláusulas, obtenido luego de promediar el valor de cada dimensión. La descripción de la nomenclatura utilizada en la Figura 1, se puede visualizar en la Tabla 3.

Los valores iniciales obtenidos corresponden al criterio del personal técnico del departamento de TI, en la aplicación del cuestionario. (Ver Anexo 5.4.1)

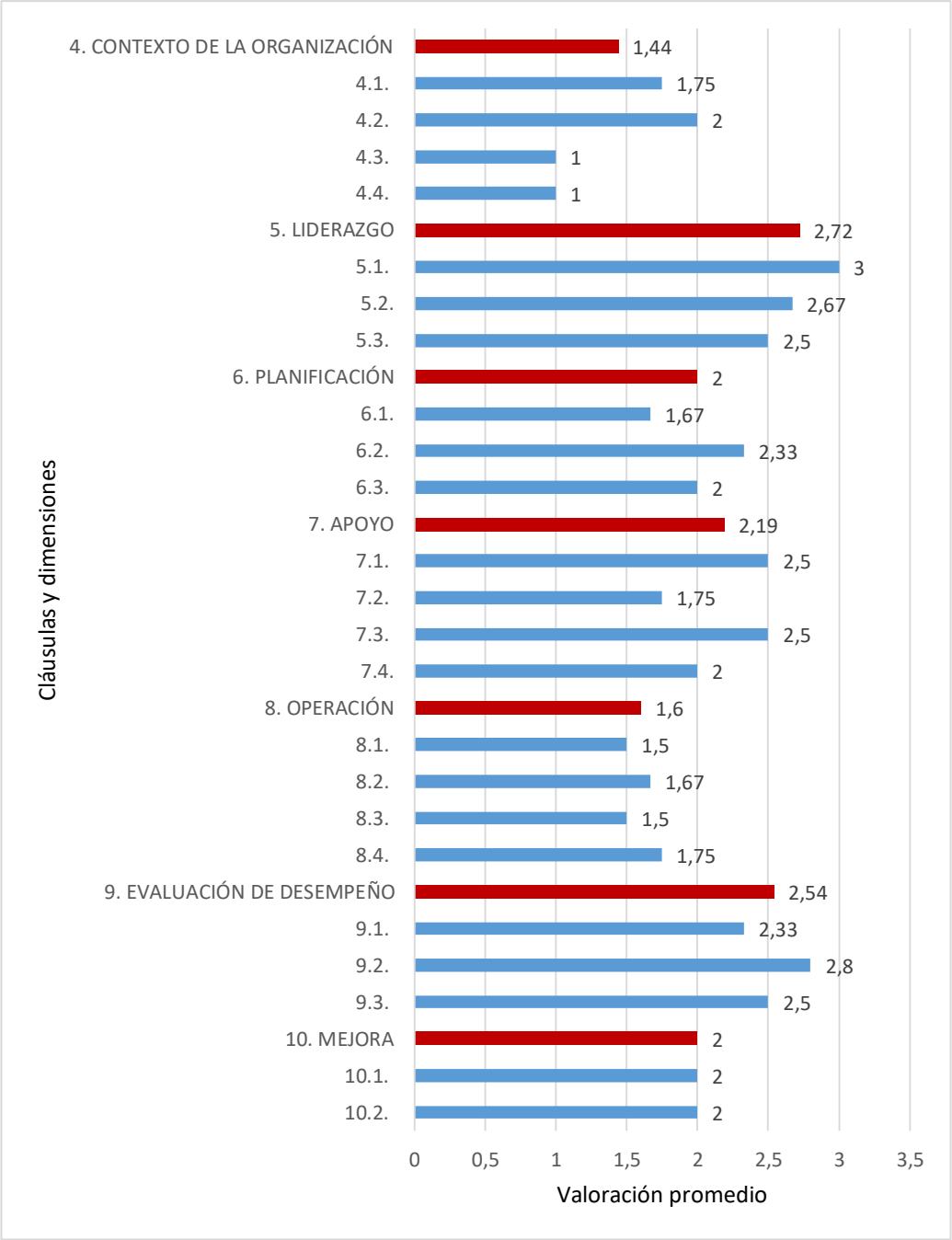

Figura 1. Promedio inicial de cumplimiento de cláusulas y sus respectivas dimensiones
Nota. Elaboración propia

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.

TABLA 10. CUADRO RESUMEN DE VALORACIÓN INICIAL DE CLÁUSULAS

CLÁUSULA	VALORACIÓN PROMEDIO
4. Contexto de la organización	1,44
5. Liderazgo	2,72
6. Planificación	2
7. Apoyo	2,19
8. Operación	1,6
9. Evaluación de desempeño	2,54
10. Mejora	2
VALORACIÓN INICIAL GLOBAL	**2,07**

Nota. Elaboración propia

De acuerdo con la valoración global y en base a la Tabla 4, la empresa TELECOMSEC 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 2, se puede apreciar el resultado.

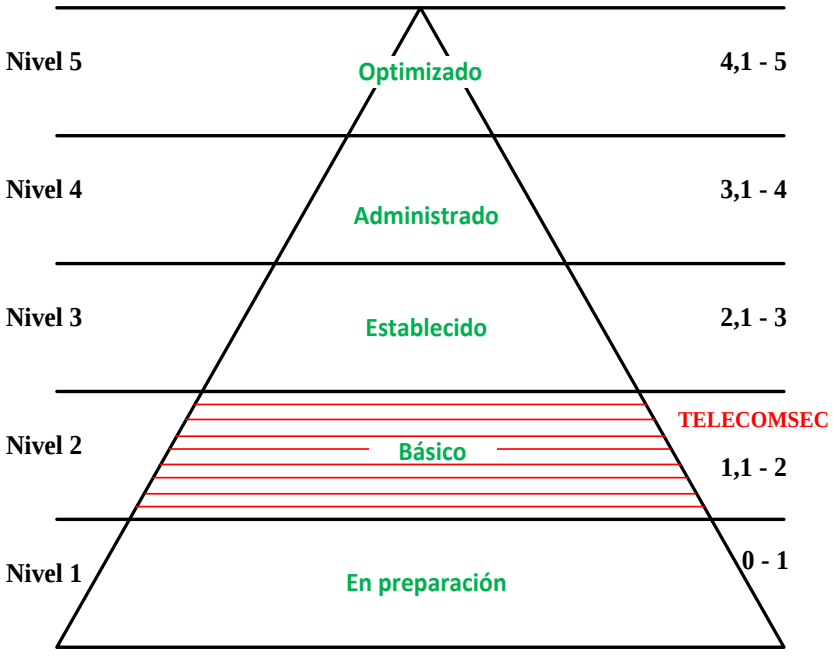

Figura 2. Nivel de gestión inicial de continuidad del negocio
Nota. Adaptado de Olarte (2016)

4.2. Resultados post-propuesta

4.2.1. Criterio final de cumplimiento de requisitos según ISO 22301

Posterior a la elaboración de la propuesta del BCP de la empresa TELECOMSEC, se aplicó nuevamente la herramienta de diagnóstico mediante un cuestionario para conocer el nivel de gestión de continuidad alcanzado dentro de la organización.

En la Figura 3, se puede observar la valoración promedio de cada una de las dimensiones definidas dentro de cada cláusula y que se representan en las barras de color azul. Las barras de color verde representan el valor promedio de las cláusulas, obtenido luego de promediar el valor de cada dimensión.

Los valores finales obtenidos corresponden al criterio del personal técnico del departamento de TI, en la aplicación del cuestionario. (Ver Anexo 5.4.1)

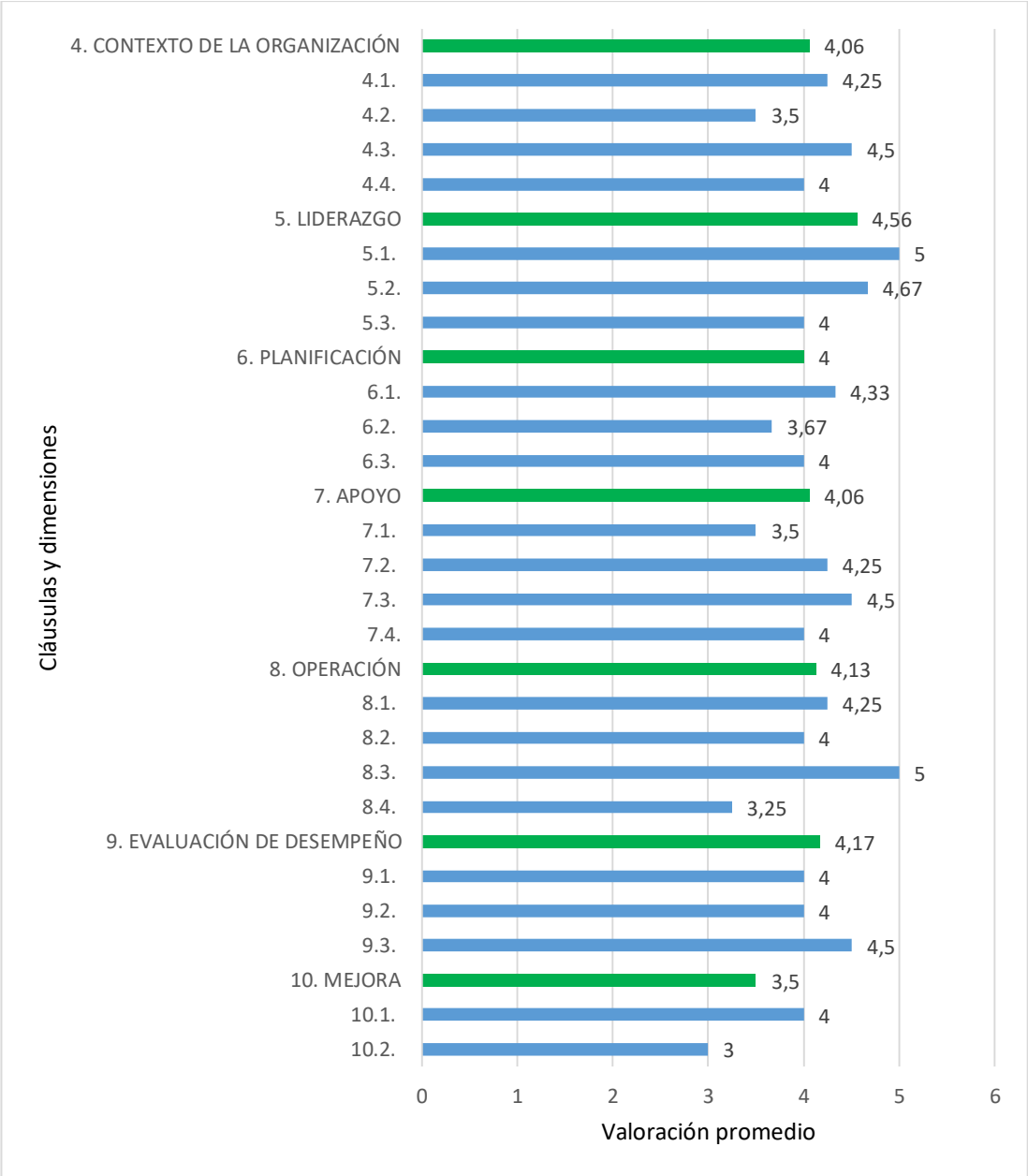

Figura 3. Promedio final de cumplimiento de cláusulas y sus respectivas dimensiones
Nota. Elaboración propia

En la Tabla 11, se muestra el resumen de la valoración individual de las cláusulas y el valor final promedio obtenido.

TABLA 11. CUADRO RESUMEN DE VALORACIÓN FINAL DE CLÁUSULAS

CLÁUSULA	VALORACIÓN PROMEDIO
4. Contexto de la organización	4,06
5. Liderazgo	4,56
6. Planificación	4

7. Apoyo	4,06
8. Operación	4,13
9. Evaluación de desempeño	4,17
10. Mejora	3,50
VALORACIÓN FINAL GLOBAL	**4,07**

Nota. Elaboración propia

De acuerdo a la valoración final global, posterior a la propuesta del BCP la empresa TELECOMSEC ha alcanzado un nivel administrado de gestión de continuidad del negocio, según la Tabla 4. Esto significa que ya cuenta con estrategias planificadas para hacer frente a incidentes de seguridad y cumple con los requisitos de la norma ISO 22301. En la Figura 4, se puede apreciar este resultado.

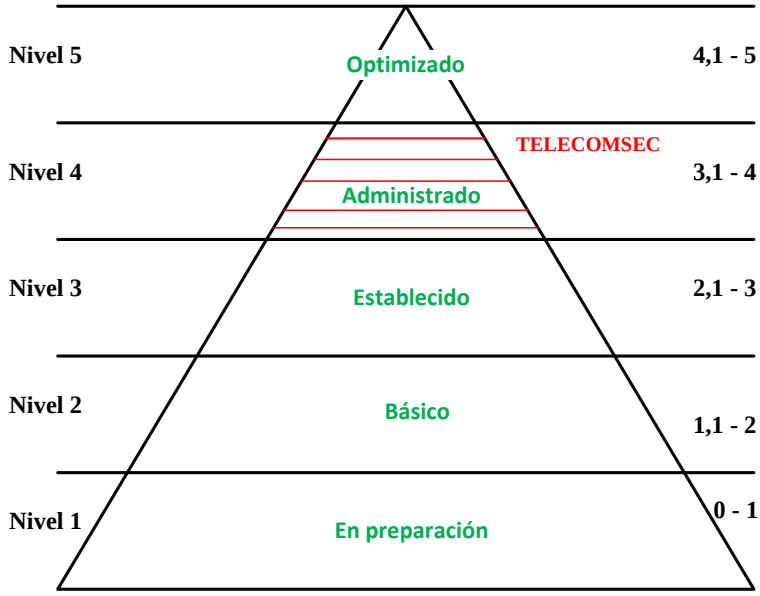

Figura 4. Nivel de gestión final de continuidad del negocio
Nota. Adaptado de Olarte (2016)

4.3. Discusión

Mediante la herramienta de análisis de datos del programa Excel, se evaluaron los valores obtenidos utilizando la función T de Student, con un valor de confianza del 99% y un margen de error del 1% (0.01). En la Tabla 12, se muestran los valores obtenidos en la evaluación inicial y final.

TABLA 12. COMPARACION DE VALORES INICIALES Y FINALES

Cláusula	Valoración inicial	Valoración final
4. Contexto de la organización	1,44	4,06
5. Liderazgo	2,72	4,56
6. Planificación	2	4
7. Apoyo	2,19	4,06
8. Operación	1,6	4,13
9. Evaluación de desempeño	2,54	4,17
10. Mejora	2	3,50

Nota. Elaboración propia

En la Figura 5, se muestra la variación del resultado inicial del nivel de gestión de continuidad con respecto al resultado final, obtenidos mediante la aplicación de la herramienta de diagnóstico de la norma ISO 22301.

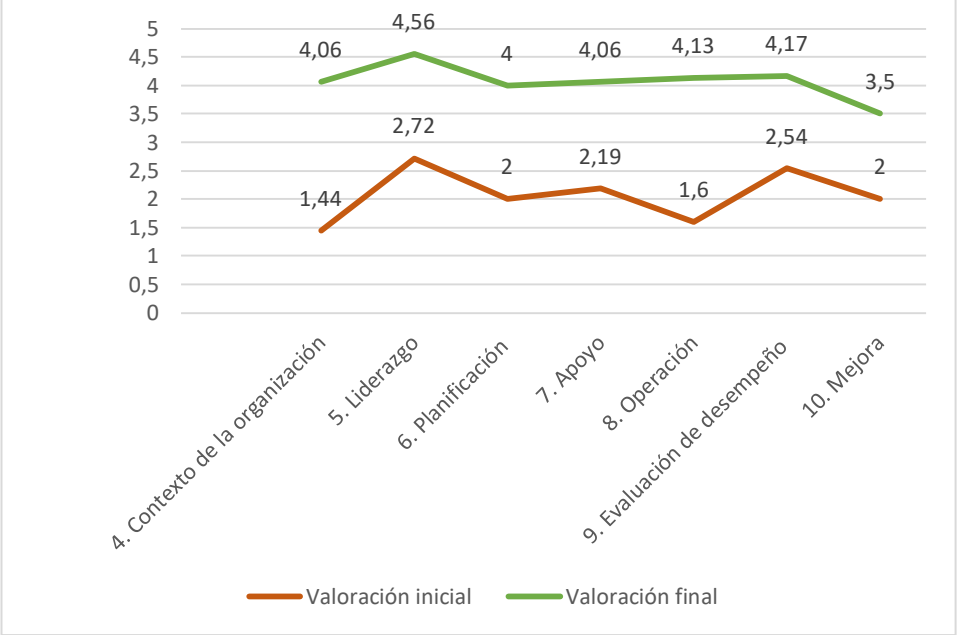

Figura 5. Gráfica comparativa de nivel de gestión de continuidad inicial y final
Nota. Elaboración propia

En la Tabla 13, se muestran los resultados posteriores a la aplicación de la T de Student para medias de dos muestras emparejadas

TABLA 13. T DE STUDENT PARA MEDIAS DE DOS MUESTRAS EMPAREJADAS

	Valoración inicial	**Valoración final**
Media	2,07	4,068571429
Varianza	0,214233333	0,097280952
Observaciones	7	7
Coeficiente de correlación de Pearson	0,447019706	
Diferencia hipotética de las medias	0	
Grados de libertad	6	
Estadístico t	-12,37939996	
P(T<=t) una cola	0,0000084776	
Valor crítico de t (una cola)	1,943180281	
P(T<=t) dos colas	1,69552E-05	
Valor crítico de t (dos colas)	2,446911851	

Nota. Análisis de datos mediante Microsoft Excel

El P valor resultante del proceso estadístico con los valores calculados para las categorías pre propuesta y post propuesta con un 99 % de confianza da un P valor igual a 0,0000084 para una cola y este valor es menor que el P valor para un margen de error del 1% que corresponde a 0,01, por lo que se rechaza la hipótesis nula y se acepta la hipótesis de investigación.

- **Hi:** El Plan de Continuidad del negocio BCP aplicado al Departamento de TI de la empresa TELECOMSEC, influye en la disponibilidad de los servicios y sistemas de dicha empresa.

- **Ho:** El Plan de Continuidad del negocio BCP aplicado al Departamento de TI de la empresa TELECOMSEC, no influye en la disponibilidad de los servicios y sistemas de dicha empresa.

CAPÍTULO V
CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1. Conclusiones

Debido a la importancia de mantener operativos los servicios y sistemas de información, en el presente proyecto se elabora un BCP que establece estrategias para prevención, contención y recuperación ante eventos disruptivos.

La herramienta de diagnóstico proporcionada por la norma ISO 22301 sirve de instrumento de evaluación inicial y final para determinar el cumplimiento de diferentes parámetros internos y externos de la empresa relacionados con la continuidad operativa.

Durante el proceso de recolección de información y posterior análisis se determina el nivel de madurez inicial de la empresa en referencia al nivel de gestión de continuidad del negocio, así como también se identifican los procesos y activos críticos que deben ser recuperados de manera prioritaria en el caso de ocurrencia de un incidente de seguridad.

Gracias al profesionalismo de los directivos y del personal técnico en la aplicación de la encuesta y entrevista, la información obtenida permitió realizar un análisis completo de impacto y riesgo de los servicios y activos críticos dentro de la empresa. De igual manera, las estrategias fueron establecidas acorde a la realidad de la organización.

Posterior a la elaboración de la propuesta del BCP para la empresa TELECOMSEC, en base a los resultados obtenidos se pudo evidenciar una mejora en el nivel de gestión de continuidad del negocio.

Una de las falencias internas es la falta de capacitación y socialización al personal técnico en temas relacionados con la recuperación de servicios y continuidad del negocio. Esto genera un mayor tiempo de resolución de problemas y las acciones tomadas no siguen un orden adecuado. Sin embargo, es un tema que ya está en análisis para reducir tiempos de inoperatividad.

5.2. Recomendaciones

Se recomienda que desde el inicio del proyecto se involucre a la alta dirección para que participe de manera activa y contribuya con su apreciación y conocimiento en la determinación de los diferentes parámetros necesarios para el desarrollo de la investigación.

Para identificar los procesos que son críticos dentro de la empresa, es fundamental aplicar la técnica de recolección de datos al personal que trabaja directamente con el proceso, de esta manera se puede obtener una estimación real de la importancia de mantener disponible un servicio o sistema.

Es necesario planificar las capacitaciones al personal para que se mantengan actualizados en temas de interés para la empresa, de esta manera se contribuye con la resolución de problemas presentes o futuros.

Es importante socializar los cambios con el personal involucrado para que todos manejen la misma información y así evitar ambigüedades.

Se recomienda revisar el BCP según la frecuencia establecida y de ser necesario se debe actualizarlo. Todos los cambios deben ser documentados.

Se recomienda revisar el perfil profesional del personal técnico y socializar de manera clara las responsabilidades que tiene cada uno a su cargo. En el caso del personal nuevo, es necesario que se imparta una inducción previa para que familiarice con la empresa.

5.3. Bibliografía

Ángulo, N., Cárdenas , J., & Bolaños, F. (2020). La continuidad de negocio en las instituciones de educación superior del Ecuador. Caso de estudio. *Revista Científica Multidisciplinaria Arbitrada YACHASUN*.

Birner, K. (06 de Septiembre de 2022). *¿Qué es un plan de continuidad de la actividad?* https://safetyculture.com/es/temas/plan-de-continiudad-del-negocio/

British Standards Institution. (2019). *Gestión de continuidad de negocio ISO 22301*. España.

Cabrejos, R. (2020). *INFLUENCIA DE LA METODOLOGÍA MAGERIT V3 EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA DECO INTERIORS SAC.* Perú.

Cabrera, K. (2021). *Análisis Comparativo de Metodologías para el desarrollo de Auditorías Informáticas para organizaciones en el Ecuador considerando: Análisis de Riesgos, Minería de Datos, Marcos de Referencia y Estándares y Normas Internacionales de Estandarización.*

Carrillo Flores, A. L. (2015). *Población y muestra*. México.

CCN-CERT. (2021). *Ciber_Amenazas y Tendencias.* Ministerio de Defensa, España.

Córdova, M., & Solano, G. (2021). *Desarrollar una metodología para el despliegue de un sitio alterno aplicando la norma ISO 22301 a un centro de datos usando la aplicación VEEAM.* Cuenca.

Correa, R. (2019). *Diseño de un Plan de Continuidad para los servicios críticos del área de Tecnologías de la Información de la empresa JJC Contratistas Generales S.A., basado principalmente en la norma ISO/IEC 27031:2011*. Lima.

Del Amor, A. (10 de Junio de 2020). *Claves para un plan de continuidad de negocio (BCP)*. https://nae.global/es/

Escobar, J., & Cuervo, Á. (2008). VALIDEZ DE CONTENIDO Y JUICIO DE EXPERTOS: UNA APROXIMACIÓN A SU UTILIZACIÓN. *Avances en Medición*(6), 27-36.

Ferruzola, E., Duchimaza, J., Ramos, J., & Alejandro, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. *Revista Científica y Tecnológica UPSE*, 34-41.

Flores, C. (2018). *ISO 22301 Sistema de Continuidad del Negocio.* Perú.

Groucutt, P. (2020). *Data Health Check 2020.*

Groucutt, P. (2021). *Data Health Check 2021.*

Gutiérrez Falcón, P. C. (2018). Estructura de Plan de Continuidad Operativa Bajo el Enfoque de la Gestión de Riesgo de Desastres en Empresas de Saneamiento de agua. *Ciencia & Trabajo*(63), 169-177.

Imbaquingo, D., Pusdá , M., & Jacomé, J. (2016). *Fundamentos de auditoría informática basada en riesgos.* Ibarra: UTN.

Incibe. (2018). *Plan de Contingencia y Continuidad del negocio.* España.

INCIBE. (2020). *Glosario de términos de ciberseguridad.*

Intedya. (2020). *Introducción a ISO 22301:2019.*

Intedya. (2021). *ISO 22301 Sistema de Gestión de Continuidad de Negocio.*

Iza, L. (2021). *Diseño del Plan de Continuidad de Negocio basado en la norma ISO 22301 para la empresa AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. (PLUS Servicios Tecnológicos) de la ciudad de Ibarra.* Ibarra.

LISA Institute. (15 de Septiembre de 2021). *¿Qué es la continuidad de negocio y por qué es importante?* https://www.lisainstitute.com/blogs/blog/que-es-continuidad-negocio-importante

López, J. F. (15 de Noviembre de 2019). *Estadística descriptiva*. Economipedia.com: https://economipedia.com/definiciones/estadistica-descriptiva.html

Machicao, S. (2019). *ANÁLISIS DE RIESGO Y POLÍTICAS DE SEGURIDAD DE INFORMACIÓN DE LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN (OTI) – UNA PUNO 2018.*

Meruvia, S. (2021). *Evaluación de riesgos y amenazas informáticas en repositorio institucional mediante metodología magerit.* Bolivia.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. (2015). *Guía para realizar el Análisis de Impacto de Negocios BIA.*

Mora, D. (2019). *Plan de Continuidad de Negocio como base del éxito organizacional.* Bogotá.

Motaki, K. (2016). *Risk Analysis and Risk Management in Critical Infrastructures.*

NQA. (2019). *ISO 22301:2019 IMPLEMENTATION GUIDE*.

Oficina de Sistemas e Informática . (2018). *Plan de Continuidad del Negocio BCP.* Colombia.

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

Ortiz, Á. (28 de Abril de 2020). *¿Qué es BCP (Business Continuity Plan, Plan de continuidad comercial)?* https://blog.hostdime.com.co/que-es-bcp-business-continuity-plan-plan-de-continuidad-comercial/

Pincay, J. (2021). *Desarrollo de un plan de continuidad del negocio basado en la norma ISO 22301, en la empresa "CONSTRUPROYEC S.A.".* Guayaquil.

Quituisaca, A., Ruilova, E., & Araujo, G. (2021). Continuidad de las MiPymes bajo la norma ISO 22301. Caso Cuenca – Azuay. *593 Digital Publisher CEIT*, 30-42.

Rodríguez , C. (2020). *La importancia de un Plan de Continuidad del Negocio*.

Rubén, R. (13 de Junio de 2020). *Conceptos básicos de Plan de Continuidad de Negocio (RPO, RTO, WRT, MTD)*. https://ciberseguridad.blog/conceptos-basicos-de-plan-de-continuidad-de-negocio-rpo-rto-wrt-mtd/

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.

Universidad Adventista de Chile. (2018). *Guía para validar instrumentos de investigación.*

Urquizo, D. (2019). *PLAN DE CONTINUIDAD DEL NEGOCIO*.

Zapata, C. (2020). *Plan de Continuidad de Negocio BCP aplicado al Departamento de Tecnología de Laboratorios Bagó del Ecuador S.A.* Quito.

5.4. Anexos

5.4.1. Encuesta inicial para valoración de cumplimiento según requisitos de la norma ISO 22301

TABLA 14. VALORACIÓN DE CUMPLIMIENTO DE REQUISITOS SEGÚN LA NORMA ISO 22301

ENCUESTA PARA PERSONAL DIRECTIVO				
Nombre:				
Cargo:				
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
CLÁUSULA			**CALIFICACIÓN INICIAL**	**CALIFICACIÓN FINAL**
4. CONTEXTO DE LA ORGANIZACIÓN			**1,44**	**4,06**
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			**2**	**3,5**
¿El personal conoce los requerimientos legales y la normativa requerida dentro de un SGCN?			1	4
¿Se revisa de manera constante información sobre partes interesadas y sus requerimientos?			3	3
4.3. Alcance del SGCN			**1**	**4,5**
¿Existe un alcance documentado dentro de la organización para la continuidad del negocio?			1	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**
¿La organización ha establecido un SGCN y ha realizado las revisiones periódicas?			1	4

5. LIDERAZGO	**2,72**	**4,56**
5.1. Compromiso, apoyo, patrocinio y gestión, por parte de los ejecutivos y la alta gerencia al SGCN	**3**	**5**
¿La alta dirección ha mostrado interés y apoyo en el establecimiento e implementación del SGCN?	3	5
5.2. Establecimiento y comunicación de la política de continuidad al interior de toda la organización	**2,67**	**4,67**
¿La alta dirección ha establecido y comunicado políticas, normativa legal y el reglamento interno para su debido cumplimiento?	3	5
¿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**
¿La alta dirección ha designado roles y ha definido de manera clara las responsabilidades del personal dentro de la organización?	3	5
¿La alta dirección ha documentado los planes de contingencia existentes y ha designado responsables de su ejecución?	2	3
6. PLANIFICACIÓN	**2**	**4,00**
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
¿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	**2,33**	**3,67**
¿Existe planificación previa para la realización de cambios?	3	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**
¿Dentro de la organización, se han establecido objetivos que garanticen la continuidad del negocio?	2	4
¿Existen procesos enfocados en mantener operativas las actividades?	2	4
7. APOYO	**2,19**	**4,06**

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	**1,75**	**4,25**
¿Existe un proceso definido que determine las competencias del personal en relación con la continuidad del negocio?	2	5
¿Se realiza evaluaciones al personal para determinar sus capacidades profesionales?	2	4
¿Se ha realizado el proceso de concienciación al personal sobre la importancia de la continuidad del negocio?	1	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)	**2**	**4**
¿La organización mantiene la información documentada siguiendo un estándar?	2	4
¿La información documentada tiene identificación, descripción, fecha, autor, control de cambios?	2	4
¿Existe control de acceso a la información confidencial?	2	4
¿La información documentada se mantiene como evidencia de la conformidad y protegida contra modificaciones no autorizadas?	2	4
8. OPERACIÓN	**1,6**	**4,13**
8.1. Definición, evaluación y administración de riesgos y análisis de impacto al negocio BIA	**1,5**	**4,25**
¿Dentro de la organización existe un procedimiento para realizar el análisis de impacto y la evaluación de riesgos?	2	5
¿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	**1,67**	**4**

estrategias DRP y BCP para todo el SGCN		
¿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?	2	4
8.3. Procedimientos del SGCN, administración y respuesta a incidentes	**1,5**	**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?	1	5
8.4. Definición, ejecución y evaluación de ejercicios y pruebas al SGCN	**1,75**	**3,25**
¿Dentro de la organización se realizan planes de pruebas y verificación?	2	3
¿Se han definido los distintos escenarios de incidentes?	1	3
¿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	**2,54**	**4,17**
9.1. Evaluación y medición de todo el procedimiento de continuidad del negocio	**2,33**	**4,00**
¿Se realiza el monitoreo y evaluación a los diferentes procesos?	2	4
¿Se documenta los resultados del monitoreo y evaluaciones de los procesos?	2	4
¿Se ha establecido un periodo de tiempo en la evaluación de los procesos?	3	4
9.2. Realización y cumplimiento de auditorías internas planificadas	**2,8**	**4**
¿Dentro de la organización se llevan a cabo auditorías programadas?	3	4
¿Previo a una auditoría se definen los criterios y el alcance?	3	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	4
¿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	**2,5**	**4,5**
¿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?	3	5
10. MEJORA	**2**	**3,50**
10.1. Identificación, monitoreo y solución de no conformidades y acciones correctivas	**2**	**4,00**
¿Se comunican las no conformidades al personal responsable para determinar mejorar las estrategias definidas?	2	4
¿Se ha establecido un periodo de tiempo para subsanar las no conformidades?	2	4
¿Las acciones correctivas y de mejora son documentadas?	2	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	**2,07**	**4,07**
DESCRIPCIÓN CALIFICACIÓN GLOBAL	**Básico**	**Administrado**

Nota. Adaptado de (Olarte, 2016)

5.4.2. Confiabilidad de los instrumentos de recolección de datos

Para determinar la confiabilidad de los instrumentos de recolección de datos, se requirió de la validación de expertos, haciendo uso del siguiente formulario:

1. La puntuación se asigna entre 1 (muy en desacuerdo) a 6 (totalmente de acuerdo), se calcula el promedio de adecuación y el promedio de pertinencia de cada pregunta.
2. Si el promedio de puntuaciones de los expertos para adecuación, así como para pertinencia es igual o superior a 4, la pregunta se considera validada.

TABLA 15. FORMULARIO PARA VALIDACIÓN DE EXPERTOS

PREGUNTA		**PUNTUACIÓN EXPERTOS**					**VALIDACIÓN** pregunta (SÍ/NO
n.º	**Evaluación**	**1**	**2**	**3**	**SUMA** puntuaciones	**PROMEDIO** puntuaciones	
1	Adecuación						
	Pertinencia						
2	Adecuación						

	Pertinencia						
3	Adecuación						
	Pertinencia						
n	Adecuación						
	Pertinencia						

Nota. (Universidad Adventista de Chile, 2018)

5.4.3. Entrevista al personal directivo del departamento de TI

TABLA 16. PLANTILLA PARA ENTREVISTA AL PERSONAL DIRECTIVO

ENTREVISTA AL PERSONAL DIRECTIVO	
Nombre del entrevistador	
Ciudad	
Fecha	
Estimado entrevistado: El motivo de la siguiente entrevista es conocer sobre los procesos y recursos críticos dentro de la empresa que forman parte de la cadena de valor.	
Nombre del entrevistado	
Edad	
Cargo	
1. ¿Se dispone de un inventario de procesos, servicios o recurso tecnológico?	
2. ¿Qué servicios son prioritarios para la empresa?	
3. ¿Dentro de la empresa se manejan SLA?	
4. ¿Conoce los riesgos a los que pueden estar expuesto su empresa?	
5. ¿Se ha identificado los factores determinantes de riesgo?	
6. ¿Se realizan pruebas a los diferentes sistemas para detectar vulnerabilidades?	
7. ¿Conoce sobre la probabilidad de ocurrencia de un incidente dentro de la empresa?	
8. ¿Se ha estimado el impacto que ocasionaría un incidente dentro de la empresa?	
9. ¿Qué servicios o procesos se consideran críticos?	
10. ¿Se toman medidas para garantizar la operatividad de los procesos críticos?	
11. ¿Qué tipo de afectaciones trae consigo la suspensión de servicios críticos?	
12. ¿Se ha estimado el tiempo máximo tolerable de inoperatividad de los servicios críticos?	

13. ¿El personal conoce cómo actuar en caso de materializarse una amenaza?
14. ¿El personal está capacitado para responder en caso de un incidente de seguridad?

Nota. Elaboración propia

CAPÍTULO VI
PROPUESTA

6.1. Datos Informativos

Título:	Plan de Continuidad del Negocio (BCP) aplicado al departamento de TI de la empresa de soluciones tecnológicas TELECOMSEC.
Institución:	Departamento de TI de la empresa TELECOMSEC.
Beneficiarios:	Gerencia General Departamento de TI Usuarios internos Clientes
Ubicación:	Quito – Pichincha
Responsable:	Ing. Paola Alexandra Díaz Parco
Director:	Ing. Ángel Gabriel Jaramillo Alcázar, Mg.

6.2. Antecedentes de la propuesta

Hace varios años atrás, las amenazas de TI se asociaban mayormente a incidentes de carácter natural y tecnológico, sin embargo, hoy en día se han mostrado otros escenarios como ciberataques, terrorismo, guerras, paralización de actividades y una de las amenazas más recientes fue la pandemia debido al COVID-19. Debido a estas múltiples amenazas, las organizaciones se han visto en la necesidad de plantearse estrategias que garanticen la continuidad de las actividades ante eventualidades que pueden impactar de diversas maneras a sus negocios.

TELECOMSEC es una empresa del sector privado que brinda soluciones integrales de tecnología, por esta razón es fundamental que los servicios y sistemas de

información se mantengan operativos tanto para el personal como para el cliente final. Las acciones realizadas dentro de la empresa para asegurar la disponibilidad de sus servicios son básicas, no están documentadas y de presentarse un incidente de seguridad que interrumpa las actividades normales podría ser perjudicial para la imagen de la organización, ocasionando pérdidas económicas e incluso problemas legales.

6.3. Justificación

A pesar de que no es posible garantizar la seguridad total, las empresas si pueden y deben estar preparadas para resguardarse ante un posible desastre que paralice sus actividades. La continuidad de negocio requiere de una planificación y preparación previa para garantizar que una organización sea capaz de mantenerse operativa durante eventos emergentes o disruptivos (LISA Institute, 2021).

Rodríguez (2020) señala que el objetivo de un BCP es evitar cualquier impacto significativo en la marca, la imagen y la reputación de la organización, a la vez que garantiza la continuidad de las operaciones. Desde el punto de vista del cliente esto es un factor prioritario a la hora de contratar un servicio.

Según el último estudio realizado en el año 2021 por Data Health Check, organización conformada en Reino Unido para desarrollar e implementar estrategias de resiliencia de TI, se ve un aumento en el porcentaje de empresas que ya han implementado un BCP con respecto a años anteriores (Groucutt, 2021). En la Figura 6, se puede apreciar los resultados de este estudio.

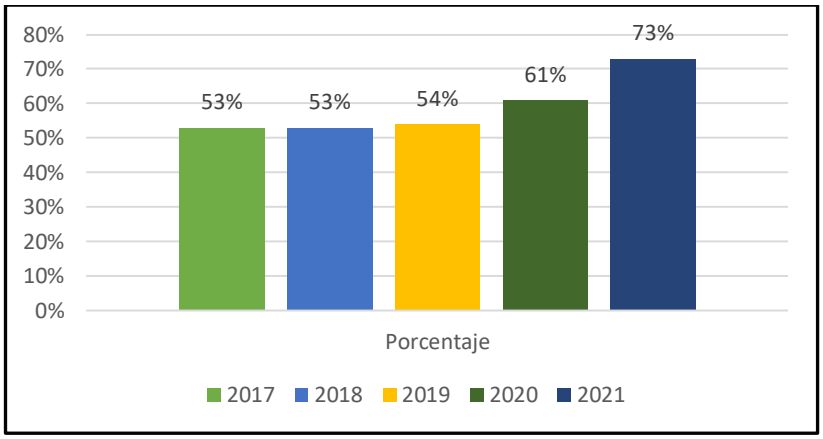

Figura 6. Porcentaje de implementación de BCP en organizaciones según Data Health Check
Nota. (Groucutt, 2020)

6.4. Objetivos

6.4.1. General

Elaborar el Plan de Continuidad del Negocio BCP basado en la norma ISO 22301, para el Departamento de TI de la empresa TELECOMSEC, mediante la aplicación de estrategias de prevención, contención y recuperación ante incidentes, reduciendo el tiempo de inoperatividad de los servicios.

6.4.2. Específicos

- Recopilar información de la situación actual referente a infraestructura tecnológica y servicios prestados por la empresa TELECOMSEC.
- Realizar el análisis de impacto del negocio BIA para identificar los procesos críticos de la empresa.
- Realizar el análisis de riesgos, vulnerabilidades y amenazas aplicando la metodología MAGERIT.
- Diseñar un BCP que contenga estrategias de recuperación según el tipo de incidente presentado.

6.5. Análisis de factibilidad

6.5.1. Factibilidad operacional

Este proyecto es factible operacionalmente ya que se cuenta con el apoyo de la Gerencia General y el personal que conforma el departamento de TI de la empresa, quienes han mostrado su interés y colaboración en el desarrollo de este.

6.5.2. Factibilidad técnica

La realización de este proyecto es técnicamente factible ya que se cuenta con el acceso necesario a la infraestructura tecnológica, así como a la información relevante para su documentación.

6.5.3. Factibilidad económica

La elaboración del BCP para el departamento de TI no representa un gasto adicional para la empresa. Los recursos económicos necesarios para el desarrollo de la propuesta corren a cargo de la investigadora.

6.6. Fundamentación

Un BCP es un proceso previamente planificado que ayuda a prevenir y recuperar las actividades frente a amenazas dentro de la organización, siguiendo los pasos establecidos y documentados, reduciendo el tiempo de inactividad de los procesos (Ortiz, 2020). El BCP debe ser considerado como una herramienta de análisis que permita tomar decisiones que respondan a contingencias, emergencias o desastres, asegurando la excelencia operativa ante cualquier escenario adverso (Del Amor, 2020).

6.7. Metodología, modelo operativo

La metodología utilizada para determinar el nivel de madurez, en lo referente a gestión de la continuidad del negocio en la empresa, está basada en la verificación del cumplimiento de las cláusulas establecidas en la norma ISO 22301, descritas en la Tabla 3. De la misma forma, esta norma determina las fases para el diseño del BCP.

Para el análisis de impacto se realizó el BIA correspondiente y en lo referente al análisis de riesgos se tomó como referencia la metodología MAGERIT.

6.7.1. ISO 22301, fases del BCP

Las fases del Plan de Continuidad del Negocio según la norma ISO 22301:2019, se resumen en la Tabla 17.

TABLA 17. FASES DEL BCP

FASE	DESCRIPCIÓN	OBSERVACIONES
Fase 1: Determinación del alcance	Alcance del BCP	Definir las áreas consideradas para el diseño del BCP
	Política y objetivos de la continuidad del negocio	Determinar qué es lo que se quiere lograr y de qué manera hacerlo
Fase 2: Análisis de la organización	Recopilación de la situación actual de la organización	Información relevante y actual sobre la organización
	Análisis de impacto de la organización (BIA)	Determinar los procesos críticos de la organización
	Análisis de riesgos	Determinar los activos críticos de la organización
Fase 3: Determinación de estrategias y	Estrategias de continuidad del negocio	Definir las estrategias y planes de respuesta frente a incidentes.

planes de continuidad		
Fase 4: Prueba, mantenimiento y revisión	Planes de prueba y revisión	Detallar las actividades a ejecutarse y los responsables en cada escenario
	Plan de mantenimiento del BCP	Definir la periodicidad de revisión del BCP
Fase 5: Capacitación y concienciación	Plan de capacitación y concienciación	Describir las necesidades de capacitación del personal

Nota. Adaptado de (Zapata, 2020)

6.7.2. Análisis de impacto del Negocio (BIA)

El presente análisis de impacto ha permitido identificar los procesos prioritarios de la empresa, evaluando su nivel de criticidad para determinar el impacto que ocasionaría su interrupción si se presenta un incidente o la ocurrencia de un desastre.

La Tabla 18, muestra la clasificación del impacto operacional, que permite identificar los procesos críticos del negocio.

TABLA 18. CLASIFICACIÓN DEL IMPACTO OPERACIONAL

Valoración	Descripción
A	Proceso crítico para el negocio, no es posible realizar la función señalada
B	Proceso no crítico para el negocio, pero forma parte integral de este.
C	Proceso no crítico y no forma parte integral del negocio

Nota. Adaptado de (Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, 2015)

6.7.2.1. Identificación de funciones y procesos de la empresa TELECOMSEC

La Tabla 19, describe los principales procesos del departamento de TI de la empresa.

TABLA 19. FUNCIONES Y PROCESOS PROPIOS DE LA EMPRESA

Función interna / externa	Proceso (Servicios)	Nivel	Descripción
Proveedor externo de internet	Servicio de internet	A	Enlace de internet
Aplicaciones	Servicio de monitoreo	B	Nagios, Zabbix
Aplicaciones	Sistema de respaldo de archivos	A	FREENAS
Aplicaciones	Entorno de pruebas de software	C	Servidor WEB, BDD
Seguridad informática	Firewall	A	Seguridad Perimetral
Sistema de almacenamiento	NAS	A	Backup de VM
Soporte técnico	Help Desk	B	Soporte Clientes
Área de TI	Datacenter	A	Centro de datos
Comunicaciones	Correo electrónico	B	Correo institucional
Comunicaciones	Telefonía IP	C	Central telefónica
Web empresarial	Venta de hardware	C	Página WEB
Recurso humano	Personal de TI	B	Personal encargado de administrar la infraestructura tecnológica

Nota. Elaboración propia

6.7.2.2. Identificación de procesos críticos y establecimiento de tiempos de recuperación

Es necesario definir los procesos críticos y establecer los tiempos de recuperación de acuerdo con el nivel de prioridad de cada uno de ellos. En la Figura 7, se puede

apreciar la escala de tiempos definida y las fases a la que pertenecen cada uno de ellos.

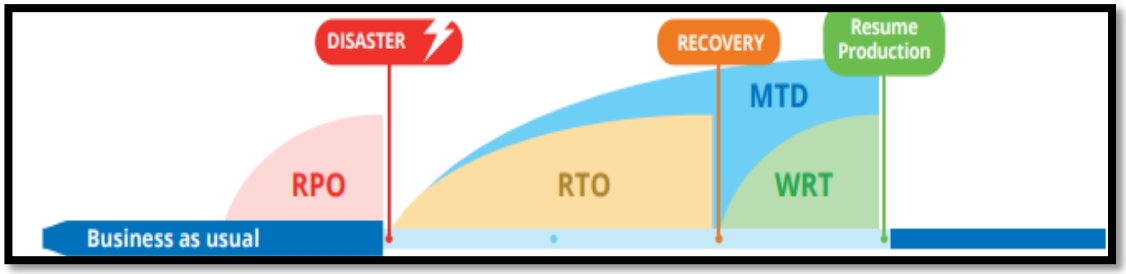

Figura 7. Escala de tiempos de recuperación
Nota. (Rubén, 2020)

En la Tabla 20, se listan los tiempos de recuperación empleados dentro de este análisis y su respectiva descripción.

TABLA 20. DESCRIPCIÓN DE TIEMPOS DE RECUPERACIÓN

Tiempo de Recuperación	Descripción
RPO (Recovery Point Objective)	Punto de Recuperación Objetivo. Cantidad máxima aceptable de pérdida de datos que la empresa puede tolerar.
RTO (Recovery Time Objective)	Tiempo de Recuperación Objetivo. Cantidad máxima de tiempo aceptable necesario para que todos los sistemas críticos 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.

Nota. (Rubén, 2020)

En la Tabla 21, se establecen los tiempos de recuperación de los procesos críticos de la empresa y su prioridad de recuperación.

TABLA 21. IDENTIFICACIÓN DE PROCESOS CRÍTICOS

COMPONENTES CRÍTICOS DEL PROCESO			TEMPORALIDAD (Horas)				Prioridad de recuperación
Función interna / externa	**Servicios**	**Nivel**	**RPO**	**RTO**	**WRT**	**MTD**	
Proveedor externo de internet	Servicio de internet	A	1	1	1	2	1
Aplicaciones	Servicio de monitoreo	B	1	2	4	6	2
Aplicaciones	Sistema de respaldo de archivos	A	1	1	2	3	1
Aplicaciones	Entorno de pruebas de software	C	8	24	8	32	3
Seguridad informática	Firewall	A	1	1	1	2	1
Sistema de almacenamiento	NAS (Backup VM)	A	1	1	1	2	1
Soporte técnico	Help Desk	B	2	2	2	4	2
Área de TI	Datacenter	A	1	1	1	2	1
Comunicaciones	Correo electrónico	B	3	4	2	6	3
Comunicaciones	Telefonía IP	C	4	4	4	8	3
Web empresarial	Venta de hardware	C	4	3	4	7	3
Recurso humano	Personal de TI	B	1	1	2	3	2

Nota. Elaboración propia

6.7.3. Análisis de riesgos

El análisis de riesgos se llevó a cabo utilizando la metodología MAGERIT, que toma en consideración tres dimensiones de valoración:

- Disponibilidad: Característica de los activos que consiste en que las organizaciones autorizadas puedan acceder a los mismos en cualquier momento.
- Integridad: Característica que consiste en conservar la información sin modificaciones no autorizadas.
- Confidencialidad: Característica que consiste en mantener la privacidad de la información, previniendo la divulgación no autorizada de la misma**.**

6.7.3.1. Valoración de criticidad

Para determinar el nivel de criticidad es necesario valorar las tres características arriba mencionadas. En las Tablas 22, 23, 24 y 25 se describen los criterios de valoración utilizados para el correspondiente análisis de riesgos.

El valor de criticidad se determina tomando el valor máximo obtenido en los criterios de Disponibilidad, Integridad y confidencialidad de cada uno de los activos.

TABLA 22. CRITERIO DE VALORACIÓN DE 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

Nota. Elaboración propia

TABLA 23. CRITERIO DE VALORACIÓN DE DISPONIBILIDAD

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

Nota. Elaboración propia

TABLA 24. CRITERIO DE VALORACIÓN DE INTEGRIDAD

Criterio de valoración INTEGRIDAD		
Alta (A)	3	Información cuya modificación no autorizada no 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

Nota. Elaboración propia

TABLA 25. CRITERIO DE VALORACIÓN DE 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 solo puede ser conocida y utilizada por determinado personal dentro de la 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

Nota. Elaboración propia

En la Tabla 26, se muestra la identificación y valoración de activos críticos de la empresa TELECOMSEC.

TABLA 26. VALORACIÓN DE CRITICIDAD DE ACTIVOS

IDENTIFICACIÓN DE ACTIVOS		VALORACIÓN DE ACTIVOS						
#	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 NAS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
4	Switch capa 3	Alta (A)	3	Alta (A)	3	Media (M)	2	3
5	Switch capa 2	Alta (A)	3	Alta (A)	3	Media (M)	2	3
6	Servidor de red	Alta (A)	3	Alta (A)	3	Media (M)	2	3
7	Aire acondicionado	Media (M)	2	Media (M)	2	Media (M)	2	2
8	UPS	Alta (A)	3	Media (M)	2	Media (M)	2	3
9	Sistema de video vigilancia	Media (M)	2	Alta (A)	3	Alta (A)	3	3
10	Freenas	Media (M)	2	Alta (A)	3	Alta (A)	3	3

Nota. Elaboración propia

6.7.3.2. Identificación de amenazas

En la Tabla 27, se muestran las posibles amenazas relacionadas con cada uno de los activos críticos de la empresa.

TABLA 27. IDENTIFICACIÓN DE AMENAZAS

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 NAS	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
Switch capa 3	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
Switch capa 2	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
Aire acondicionado	Daños ocasionados por fuego
	Daños ocasionados por agua
	Daños ocasionados por corte de suministro eléctrico
	Daño de componentes del equipo
	Error en la instalación del equipo
	Imposibilidad de recuperar el equipo por falta de planes de contingencia
	Equipo sin mantenimientos
	Desconexión deliberada o accidental del equipo
UPS	Daños ocasionados por fuego
	Daños ocasionados por agua
	Daños ocasionados por corte de suministro eléctrico

	Daño de componentes del equipo
	Errores de usuario en la administración, configuración y monitorización del equipo
	Error en la instalación del equipo
	Imposibilidad de recuperar el equipo por falta de planes de contingencia
	Equipo sin mantenimientos
	Desconexión deliberada o accidental del equipo
Sistema de video vigilancia	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
Freenas	Problemas de disponibilidad del sistema
	Sistema desactualizado
	Uso indebido de credenciales de acceso por funcionarios no autorizados
	Posible acceso indebido al servidor remotamente
	Posibilidad de pérdida de información alojada en el servidor
	Posibilidad de errores de usuario en la administración, configuración del sistema

Nota. Elaboración propia

6.7.3.3.Valoración del impacto

El impacto se calcula tomando el máximo valor de degradación que la amenaza produce sobre el activo por su nivel de criticidad. En la Tabla 28, se muestra un ejemplo de cálculo del impacto de una amenaza sobre un activo.

TABLA 28. EJEMPLO DE CÁLCULO DE IMPACTO DE UNA AMENAZA SOBRE UN ACTIVO

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	D	I	C	TOTAL
X	3	Daños ocasionados por fuego	100%	60%	50%	3x100%=3

Nota. Elaboración propia

Por cada activo y amenaza se estima la degradación para cada una de las características de disponibilidad, integridad y confidencialidad, estableciendo el porcentaje de daño que está entre 0% (no hay daño) y el 100% (daño total).

En la Tabla 29, se muestra la escala de valoración del Impacto.

TABLA 29. CRITERIO DE VALORACIÓN DEL IMPACTO

Valoración IMPACTO	
Criticidad por degradación (D.I.C)	
Alto (A)	3
Medio (M)	2
Bajo (B)	1

Nota. Elaboración propia

En la Tabla 30, se muestra el cálculo del impacto sobre los activos de la empresa.

TABLA 30. VALORACIÓN DEL IMPACTO SOBRE LOS ACTIVOS

ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	**Criticidad**	**Descripción**	**D**	**I**	**C**	**TOTAL**
Servidor de virtualización	3	Daños ocasionados por fuego	100%	60%	20%	3
		Daños ocasionados por agua	100%	60%	20%	3
		Daños ocasionados por corte de suministro eléctrico	50%	25%	20%	1,5
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	70%	30%	20%	2,1
		Desconexión deliberada o accidental del equipo	100%	20%	20%	3
		Falta de actualizaciones de versión de sistema operativo	30%	15%	20%	0,9
		Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	40%	100%	20%	3
		Degradación por saturación de recursos del equipo	60%	80%	20%	2,4
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	20%	3
		Daño en el equipo por falta de mantenimiento	100%	50%	20%	3
Firewall	3	Daños ocasionados por fuego	100%	60%	10%	3
		Daños ocasionados por agua	100%	60%	10%	3
		Daños ocasionados por corte de suministro eléctrico	50%	35%	10%	1,5
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	70%	25%	10%	2,1
		Desconexión deliberada o accidental del equipo	50%	50%	10%	1,5
		Falta de actualizaciones de versión de sistema operativo	80%	25%	10%	2,4
		Posibilidad de error de usuario en administración, configuración y monitorización del equipo	70%	100%	50%	3
		Degradación por saturación de recursos del equipo	70%	65%	25%	2,1
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	90%	80%	30%	2,7
		Daño en el equipo por falta de mantenimiento	95%	45%	50%	2,85
Servidor NAS	3	Daños ocasionados por fuego	100%	100%	30%	3

		Daños ocasionados por agua	100%	100%	30%	3
		Daños ocasionados por corte de suministro eléctrico	40%	50%	30%	1,5
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	50%	30%	1,5
		Desconexión deliberada o accidental del equipo	50%	50%	30%	1,5
		Falta de actualizaciones de versión de sistema operativo	40%	50%	30%	1,5
		Posibilidad de error de usuario en administración, configuración y monitoreo del equipo	60%	100%	90%	3
		Degradación por saturación de recursos del equipo	90%	100%	30%	3
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	70%	3
		Daño en el equipo por falta de mantenimiento	80%	40%	30%	2,4
Switch capa 3	3	Daños ocasionados por fuego	100%	30%	10%	3
		Daños ocasionados por agua	100%	30%	10%	3
		Daños ocasionados por corte de suministro eléctrico	100%	20%	10%	3
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	20%	10%	3
		Desconexión deliberada o accidental del equipo	100%	50%	10%	3
		Falta de actualizaciones de versión de sistema operativo	45%	10%	10%	1,35
		Posibilidad de error de usuario en administración, configuración y monitorización del equipo	100%	50%	10%	3
		Degradación por saturación de recursos del equipo	75%	30%	10%	2,25
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	30%	10%	3
		Daño en el equipo por falta de mantenimiento	100%	30%	10%	3
Switch capa 2	3	Daños ocasionados por fuego	100%	30%	10%	3
		Daños ocasionados por agua	100%	30%	10%	3
		Daños ocasionados por corte de suministro eléctrico	100%	20%	10%	3
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	20%	10%	3
		Desconexión deliberada o accidental del equipo	100%	50%	10%	3

		Falta de actualizaciones de versión de sistema operativo	45%	10%	10%	1,35
		Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	50%	10%	3
		Degradación por saturación de recursos del equipo	75%	30%	10%	2,25
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	30%	10%	3
		Daño en el equipo por falta de mantenimiento	100%	30%	10%	3
Servidor de red	3	Daños ocasionados por fuego	100%	60%	20%	3
		Daños ocasionados por agua	100%	60%	20%	3
		Daños ocasionados por corte de suministro eléctrico	50%	25%	20%	1,5
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	70%	30%	20%	2,1
		Desconexión deliberada o accidental del equipo	100%	20%	20%	3
		Falta de actualizaciones de versión de sistema operativo	30%	15%	20%	0,9
		Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	40%	100%	20%	3
		Degradación por saturación de recursos del equipo	60%	80%	20%	2,4
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	20%	3
		Daño en el equipo por falta de mantenimiento	100%	50%	20%	3
Aire acondicionado	2	Daños ocasionados por fuego	100%	30%	5%	2
		Daños ocasionados por agua	100%	30%	5%	2
		Daños ocasionados por corte de suministro eléctrico	60%	30%	5%	1,2
		Daño de componentes del equipo	100%	30%	5%	2
		Error en la instalación del equipo	100%	30%	5%	2
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	30%	5%	2
		Equipo sin mantenimientos	80%	30%	5%	1,6
		Desconexión deliberada o accidental del equipo	100%	30%	5%	2
UPS	3	Daños ocasionados por fuego	100%	15%	5%	3

		Daños ocasionados por agua	100%	15%	5%	3
		Daños ocasionados por corte de suministro eléctrico	25%	15%	5%	0,75
		Daño de componentes del equipo	70%	15%	5%	2,1
		Error de usuario en administración, configuración y monitorización del equipo	5%	15%	5%	0,45
		Error en la instalación del equipo	15%	15%	5%	0,45
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	65%	15%	5%	1,95
		Equipo sin mantenimientos	80%	15%	5%	2,4
		Desconexión deliberada o accidental del equipo	25%	15%	5%	0,75
Sistema de video vigilancia	3	Daños ocasionados por fuego	100%	50%	60%	3
		Daños ocasionados por agua	100%	50%	60%	3
		Daños ocasionados por corte de suministro eléctrico	65%	50%	30%	1,95
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	50%	60%	1,8
		Desconexión deliberada o accidental del equipo	100%	50%	30%	3
		Falta de actualizaciones de versión de sistema operativo	45%	50%	30%	1,5
		Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	35%	50%	40%	1,5
		Degradación por saturación de recursos del equipo	50%	50%	50%	1,5
		Imposibilidad de recuperar el equipo por falta de planes de contingencia	90%	50%	50%	2,7
		Daño en el equipo por falta de mantenimiento	35%	50%	20%	1,5
Freenas	3	Problemas de disponibilidad del sistema	100%	50%	50%	3
		Sistema desactualizado	20%	20%	20%	0,6
		Uso indebido de credenciales de acceso por funcionarios no autorizados	20%	70%	30%	2,1
		Posible acceso indebido al servidor remotamente	50%	50%	30%	1,5
		Posibilidad de pérdida de información alojada en el servidor	50%	60%	90%	2,7
		Posibilidad de error de usuario en administración, configuración del sistema	80%	40%	70%	2,4

Nota. Elaboración propia

6.7.3.4. Valoración del riesgo

Para la valoración del riesgo se toma en consideración la probabilidad de ocurrencia de un evento y el impacto que este produce sobre los activos.

TABLA 31. CRITERIO DE VALORACIÓN DE LA PROBABILIDAD DE OCURRENCIA

Criterio de valoración PROBABILIDAD		
Probabilidad de ocurrencia de un evento		
Alta (A)	3	Diariamente
Media (M)	2	Mensualmente
Baja (B)	1	1 vez al año
Nula (N)	0,1	Más de 1 año

Nota. Elaboración propia

En la Tabla 32, se muestra un ejemplo de cálculo del riesgo en base a los valores de la probabilidad de ocurrencia y el impacto.

TABLA 32. EJEMPLO DE CÁLCULO DE RIESGO

ACTIVO	**AMENAZAS**	**CÁLCULOS**		
Activo	Descripción	PROBABILIDAD	IMPACTO	RIESGO
X	Daños ocasionados por fuego	1	3.00	1*3=3

Nota. Elaboración propia

En la Tabla 33, se muestra los criterios de valoración del nivel de riesgo.

TABLA 33. CRITERIOS DE VALORACIÓN DEL NIVEL DE RIESGO

	Niveles de riesgo	
6	Riesgo Extremo (E)	Requiere respuesta y atención inmediata
4	Riesgo Alto (A)	Requiere atención a corto plazo
2	Riesgo Medio (M)	Revisión constante, atención a mediano plazo
0	Riesgo Bajo (B)	Revisión de rutina

Nota. Elaboración propia

En la Tabla 34, se muestra la valoración del nivel de riesgo de los activos de la empresa.

TABLA 34. VALORACIÓN DEL NIVEL DE RIESGO DE LOS ACTIVOS

ACTIVOS	AMENAZAS	CÁLCULOS		
Activo	**Descripción**	**Probabilidad**	**Impacto**	**Riesgo**
Servidor de virtualización	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	1	1,5	1,5
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	2,1	0,21
	Desconexión deliberada o accidental del equipo	1	3	3
	Falta de actualizaciones de versión de sistema operativo	1	0,9	0,9
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	2	3	6
	Degradación por saturación de recursos del equipo	1	2,4	2,4
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	2	3	6
	Daño en el equipo por falta de mantenimiento	2	3	6
Firewall	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	1	1,5	1,5
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	2,1	0,21
	Desconexión deliberada o accidental del equipo	1	1,5	1,5
	Falta de actualizaciones de versión de sistema operativo	1	2,4	2,4
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	1	3	3
	Degradación por saturación de recursos del equipo	1	2,1	2,1
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	2	2,7	5,4
	Daño en el equipo por falta de mantenimiento	1	2,85	2,85
Servidor NAS	Daños ocasionados por fuego	0,1	3	0,3

	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	1	1,5	1,5
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	1,5	0,15
	Desconexión deliberada o accidental del equipo	1	1,5	1,5
	Falta de actualizaciones de versión de sistema operativo	0,1	1,5	0,15
	Posibilidad de error de usuario en administración, configuración y monitorización del equipo	1	3	3
	Degradación por saturación de recursos del equipo	1	3	3
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	1	3	3
	Daño en el equipo por falta de mantenimiento	1	2,4	2,4
Switch capa 3	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	1	3	3
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3	0,3
	Desconexión deliberada o accidental del equipo	1	3	3
	Falta de actualizaciones de versión de sistema operativo	0,1	1,35	0,14
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	1	3	3
	Degradación por saturación de recursos del equipo	0,1	2,25	0,23
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	1	3	3
	Daño en el equipo por falta de mantenimiento	1	3	3
Switch capa 2	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	1	3	3
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3	0,3
	Desconexión deliberada o accidental del equipo	1	3	3
	Falta de actualizaciones de versión de sistema operativo	0,1	1,35	0,135

	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	1	3	3
	Degradación por saturación de recursos del equipo	0,1	2,25	0,225
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	1	3	3
	Daño en el equipo por falta de mantenimiento	1	3	3
Servidor de red	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	1	1,5	1,5
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	2,1	0,21
	Desconexión deliberada o accidental del equipo	1	3	3
	Falta de actualizaciones de versión de sistema operativo	0,1	0,9	0,09
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	1	3	3
	Degradación por saturación de recursos del equipo	0,1	2,4	0,24
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	1	3	3
	Daño en el equipo por falta de mantenimiento	1	3	3
Aire acondicionado	Daños ocasionados por fuego	0,1	2	0,2
	Daños ocasionados por agua	0,1	2	0,2
	Daños ocasionados por corte de suministro eléctrico	0,1	1,2	0,12
	Daño de componentes del equipo	1	2	2
	Error en la instalación del equipo	0,1	2	0,2
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	0,1	2	0,2
	Equipo sin mantenimientos	0,1	1,6	0,16
	Desconexión deliberada o accidental del equipo	1	2	2
UPS	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	0,1	0,75	0,075

	Daño de componentes del equipo	1	2,1	2,1
	Errores de usuario en la administración, configuración y monitorización del equipo	0,1	0,45	0,045
	Error en la instalación del equipo	0,1	0,45	0,045
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	0,1	1,95	0,195
	Equipo sin mantenimientos	1	2,4	2,4
	Desconexión deliberada o accidental del equipo	1	0,75	0,75
Sistema de video vigilancia	Daños ocasionados por fuego	0,1	3	0,3
	Daños ocasionados por agua	0,1	3	0,3
	Daños ocasionados por corte de suministro eléctrico	0,1	1,95	0,195
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	1,8	0,18
	Desconexión deliberada o accidental del equipo	1	3	3
	Falta de actualizaciones de versión de sistema operativo	1	1,5	1,5
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	1	1,5	1,5
	Degradación por saturación de recursos del equipo	1	1,5	1,5
	Imposibilidad de recuperar el equipo por falta de planes de contingencia	0,1	2,7	0,27
	Daño en el equipo por falta de mantenimiento	1	1,5	1,5
Freenas	Problemas de disponibilidad del sistema	2	3	6
	Sistema desactualizado	1	0,6	0,6
	Uso indebido de credenciales de acceso por funcionarios no autorizados	1	2,1	2,1
	Posible acceso indebido al servidor remotamente	0,1	1,5	0,15
	Posibilidad de pérdida de información alojada en el servidor	1	2,7	2,7
	Posibilidad de errores de usuario en la administración, configuración del sistema	1	2,4	2,4

Nota. Elaboración propia

6.7.3.5. Riesgo actual y riesgo objetivo

En la Tabla 35, se resume los valores correspondientes al riesgo actual, el riesgo objetivo y el límite del nivel de riesgo, según lo detallado a continuación:

- Valor actual: Promedio de todos los riesgos asociados a un activo
- Valor objetivo: Recomendación de reducción de riesgo (30%)
- Valor límite: Valor máximo de riesgo, del cual no se deberá sobrepasar

TABLA 35. RIESGO ACTUAL Y RIESGO OBJETIVO

Activo	Riesgo actual	Riesgo objetivo	Límite
Servidor de virtualización	2,66	1,86	4
Firewall	1,96	1,37	4
Servidor NAS	1,53	1,07	4
Switch capa 3	1,63	1,14	4
Switch capa 2	1,63	1,14	4
Servidor de red	1,46	1,02	4
Aire acondicionado	0,64	0,45	4
UPS	0,69	0,48	4
Sistema de video vigilancia	1,02	0,71	4
Freenas	2,33	1,63	4

Nota. Elaboración propia

En la Figura 8, se puede apreciar los valores detallados en la Tabla 35.

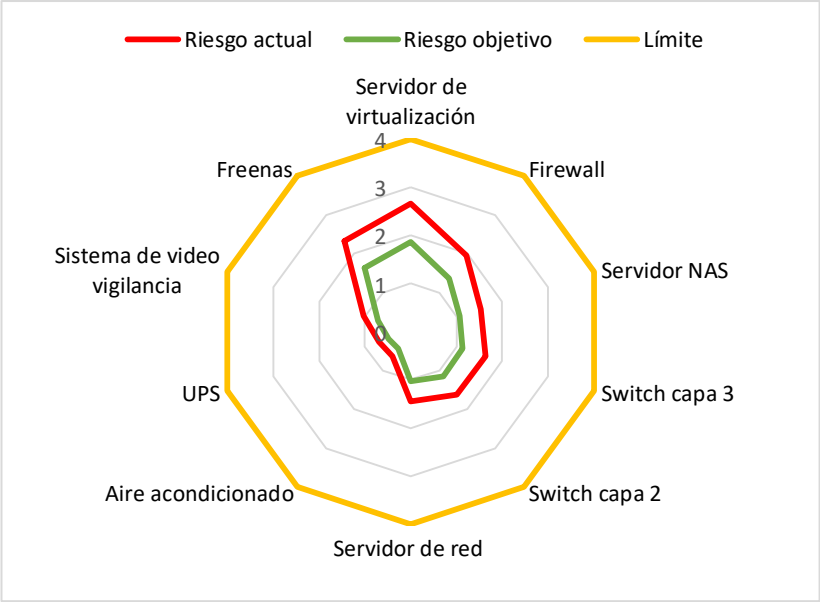

Figura 8. Gráfico de radar del riesgo actual y riesgo objetivo
Nota. Elaboración propia

6.8. Plan de Continuidad del negocio para la empresa TELECOMSEC

Dentro del BCP se desarrollan las siguientes fases:

- Fase 1: Determinación del alcance
- Fase 2: Análisis de la organización
- Fase 3: Determinación de estrategias y planes de continuidad
- Fase 4: Prueba, mantenimiento y revisión
- Fase 5: Capacitación y concienciación

6.8.1. Fase 1: Determinación del alcance

En esta fase se define el alcance, la política de continuidad del negocio y los objetivos del BCP.

6.8.1.1. Alcance del BCP

El desarrollo de este BCP está enfocado en el departamento de Tecnologías de la Información de la empresa de soluciones tecnológicas TELECOMSEC. Todo el personal que labora en el área de TI, así como el Gerente General, conforman el recurso humano involucrado dentro de este proyecto.

Dentro de este plan se toma en consideración todos los procesos y activos que forman parte de la cadena de valor del departamento de TI de esta empresa.

6.8.1.2. Política de continuidad del negocio

La Gerencia General de la empresa TELECOMSEC, 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 el departamento de TI, 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 y ha sido adaptado a las necesidades propias de esta empresa, 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 Gerente General.

6.8.1.3. Objetivos del BCP

Los objetivos que persigue la empresa con la elaboración del Plan de Continuidad son:

- Mitigar amenazas que puedan causar interrupciones en la operatividad y entrega de servicios a usuarios finales.
- Garantizar la continuidad de los procesos críticos de la empresa.
- Asegurar el cumplimiento coordinado de las estrategias de recuperación propuestas, para las funciones críticas del negocio.
- Mantener tiempos aceptables de recuperación en los procesos agregadores de valor

6.8.2. Fase 2: Análisis de la organización

Dentro de esta fase se describen los aspectos relevantes de la empresa, sus principales actividades, así como las responsabilidades asignadas al personal técnico del departamento de TI.

6.8.2.1. Situación actual

La empresa de soluciones tecnológicas TELECOMSEC, inició sus actividades en el año 2010 en la ciudad de Quito, donde actualmente se encuentra la oficina matriz. Está conformada por un grupo de expertos en el área de Tecnologías de la Información y fue creada con el objetivo de ofrecer sus servicios a instituciones públicas y privadas, brindando soluciones tecnológicas integrales personalizadas, basadas en el análisis de la situación de cada organización, alineándose a los objetivos y metas del negocio, entregando resultados de manera segura y eficaz.

Actualmente, la empresa cuenta con cuatro áreas funcionales:

- Gerencia General
- Departamento de TI
- Departamento administrativo
- Departamento comercial

Cada una de estas áreas tiene una persona responsable que se encarga de llevar a cabo los procesos correspondientes y del manejo del recurso humano a su cargo.

Entre los principales servicios que brinda la empresa, se listan los siguientes:

- Diseño y reingeniería de redes de comunicación
- Implementación de soluciones de seguridad perimetral
- Soporte técnico especializado en sistemas operativos, bases de datos, desarrollo de software
- Soporte técnico especializado en hardware (servidores, computadores, almacenamiento, conectividad, entre otros)
- Consultoría en seguridad de la información
- Auditoría informática basada en normas y estándares internacionales
- Venta de hardware y software

- Monitoreo, análisis y respuesta a incidentes de ciberseguridad
- Implementación de soluciones empresariales basadas en software libre
- Mantenimiento de Datacenter e infraestructura de hardware y software

6.8.2.2. Responsables y roles (Departamento de TI)

TABLA 36. RESPONSABLES Y ROLES DEL PERSONAL

CARGO	ROL
Gerente General	Se encarga de planificar las diferentes actividades que se desarrollan dentro de la empresa, organiza los recursos, define los objetivos y metas a alcanzar en un determinado período de tiempo, define estrategias de captación de posibles clientes, impulsa al equipo de trabajo a cumplir con las tareas encomendadas, entre otras actividades.
Jefe del Departamento de Tecnologías de la Información	Es el encargado de organizar y gestionar el área de tecnologías de la información, lidera los procesos de tecnología verificando el uso correcto y eficiente de recursos, asigna tareas al personal a su cargo, mantiene operativa la infraestructura tecnológica.
Técnico de redes	Se encarga de la instalación de redes informáticas, verifica el correcto funcionamiento de las conexiones y cableado, propone soluciones a los problemas y fallos del sistema, configura y realiza pruebas del software, mantenimiento preventivo y correctivo del hardware y de los dispositivos periféricos.
Técnico en seguridad informática	Su principal función es garantizar la seguridad de los sistemas informáticos de la empresa, evitar intrusiones externas o fugas de datos. Constantemente se actualiza en temas relacionados con nuevas formas de amenazas y sus posibles soluciones.
Desarrollador	Se encarga de diseñar aplicaciones a medida, mantiene y

	evalúa software existente o nuevo, corrige errores en aplicativos.
Técnico de soporte	Se encarga de dar atención a los requerimientos generados por los clientes en el sitio o de manera remota. Brinda soporte técnico dentro de la empresa.

Nota. Elaboración propia

6.8.3. Fase 3: Determinación de estrategias y planes de continuidad

En esta fase se establecen las estrategias y planes necesarios para mantener la continuidad operativa. Se define también el personal que conforma el comité de crisis.

6.8.3.1. Estrategias de continuidad del negocio

En la Tabla 37, se listan las estrategias de continuidad de los procesos críticos.

TABLA 37. ESTRATEGIAS DE CONTINUIDAD DE PROCESOS CRÍTICOS

Proceso	Responsable	RTO	Estrategia de recuperación	Acciones	Recursos
Servicio de internet	Jefe de TI	1 hora	Redundancia del servicio de internet	Disponer de un enlace de internet principal y un enlace de internet de backup para garantizar la continuidad del servicio.	Infraestructura de red
	Jefe de TI	1 hora	Mantener actualizado el directorio de contacto de los proveedores	Contactar al proveedor para revisión del daño y pronta solución	Contactos telefónicos y correo electrónico del proveedor
	Jefe de TI	1 hora	Revisión y aplicación de SLA (Acuerdo de Nivel de Servicio)	Coordinar con el proveedor de servicios las acciones a seguir según lo establecido en el SLA	Contrato en donde se detalle los Niveles de Acuerdo de Servicios
Sistema de respaldo de archivos	Técnico de redes	1 hora	Sitio alterno duplicado	Levantar un servidor alterno de respaldo de archivos	Infraestructura de red
Seguridad informática / Firewall	Técnico de seguridad informática	1 hora	Alta disponibilidad	Conexión automática del equipo secundario	Equipo secundario
Sistema de	Técnico de seguridad	1 hora	Servicio de	Almacenamiento en la nube	Servicio de

almacenamiento / NAS (Backup VM)	informática		almacenamiento en la nube		almacenamiento en la nube
	Técnico de seguridad informática	1 hora	Servidor alterno de almacenamiento	Levantar un servidor alterno para almacenamiento	Hardware
	Técnico de seguridad informática	1 hora	Dispositivos físicos de almacenamiento	Verificar el correcto funcionamiento de los dispositivos físicos de almacenamiento	Discos de almacenamiento externo, cintas
Datacenter	Técnico de redes	1 hora	Sitio alterno equipado	Levantar servidores principales	Hardware, software, respaldos
	Técnico de redes	1 hora	Servicios en la nube	Acceder a los servicios contratados para hacer uso de los recursos de red	IaaS (Infraestructura como Servicio) en la nube

Nota. Elaboración propia

6.8.3.2. 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**

TABLA 38. PLAN DE PREVENCIÓN DE RIESGOS ANTE EVENTOS DE FALLO FÍSICO O LÓGICO

Evento: Falla en hardware o software
Descripción del evento:
Interrupción de los servicios ocasionado por falla en hardware o software, daño en enlaces de internet o datos u otro tipo de incidente que ocasione la suspensión temporal o total del servicio
Objetivo:
Garantizar la continuidad de las actividades operativas, empleando mecanismos que ayuden a prevenir la ocurrencia de amenazas o incidentes de seguridad dentro de la empresa
Entorno:
Los daños pueden producirse dentro o fuera de las instalaciones de la empresa
Personal encargado:
- Personal del área de TI - Proveedores externos
Prevención de riesgo:
- Revisión periódica de enlaces físicos de datos e internet - Monitoreo de disponibilidad de enlaces - Mantenimiento preventivo y correctivo de equipamiento de servidores - Respaldo diario de la información crítica - Validación del backup de la información - Mantenimiento preventivo y correctivo de UPS, aire acondicionado, sistema de control de acceso al Datacenter, sistema de video vigilancia.

- Actualización de versiones y parches de seguridad de Sistemas Operativos y aplicativos en general
Acciones por tomar:
- Determinar, planificar, ejecutar y supervisar procedimientos de respaldo y restauración de información - Mantenimientos preventivos planificados a la infraestructura tecnológica - Documentar hardware y software existente - Monitoreo periódico de servicios y recursos - Listar equipos y servicios con garantía vigente - Capacitar al personal en temas de seguridad informática

Nota. Elaboración propia

TABLA 39. PLAN DE PREVENCIÓN DE RIESGOS ANTE DESASTRES NATURALES

Escenario: Desastres naturales
Descripción del evento:
Interrupción de los servicios ocasionado por desastres naturales como terremotos, inundaciones, temblores, entre otros.
Objetivo:
Establecer acciones previas ante la ocurrencia de eventos no anticipados, que permitan al personal estar preparados para actuar de manera organizada frente a la ocurrencia de cualquier desastre natural.
Entorno:
Los daños pueden producirse dentro o fuera de las instalaciones de la empresa.
Personal encargado:
Comité de crisis
Preparación ante el riesgo:
- Señalizar adecuadamente las salidas de emergencia, puntos de encuentro, sitios de alto riesgo. - El cuarto de equipos debe tener instalado sistemas de monitoreo que detecten la variación en la temperatura y emitan alarmas en el caso de que sobrepase los umbrales establecidos.

- Se debe socializar al personal el procedimiento interno para actuar en caso de ocurrencia de desastres naturales.
- Revisar el estado de la tubería.
- Revisar el estado de las conexiones eléctricas.
- El responsable del comité de crisis debe realizar simulacros para que todo el personal esté preparado ante esta eventualidad.
- Elaboración de la cadena de llamadas

Acciones por tomar:

- Señalización clara dentro de la empresa
- Implementación de sistemas de detección de temperatura, humo dentro del cuarto de equipos.
- Instalación de extintores.
- Revisiones de la parte eléctrica, tuberías
- Socialización al personal
- Planificación de simulacros

Nota. Elaboración propia

TABLA 40. PLAN DE PREVENCIÓN DE RIESGOS ANTE EVENTOS FORTUITOS

Escenario: Casos fortuitos (Pandemia, manifestaciones)

Descripción del evento:

Suspensión temporal del servicio provocado por fallos a nivel de hardware o software y que dependen de la intervención humana para su solución.

Objetivo:

Determinar las acciones necesarias para garantizar la continuidad operativa en el caso de ocurrencia de eventos fortuitos.

Entorno:

Las afectaciones inciden directamente en el personal de la empresa

Personal encargado:

- Personal del área de TI
- Proveedores externos
- Comité de crisis

Prevención de riesgo:

- En el caso de pandemia, se debe comunicar al personal las medidas de bioseguridad establecidas por la autoridad competente. - En el caso de manifestaciones, se debe establecer una jornada reducida para que el personal pueda movilizarse. - Adoptar el sistema de teletrabajo. - Probar los mecanismos para la realización de teletrabajo. - En el caso de requerir la presencia específica del personal, se debe establecer las medidas de seguridad respectivas. - Determinar el personal de backup - Elaboración de la cadena de llamadas
Acciones por tomar:
- Socialización de medidas de bioseguridad - Capacitación en el uso de herramientas para conexión remota segura - Acceso mediante red privada virtual (VPN) del personal autorizado y a la información necesaria - Realizar pruebas previas de acceso con las respectivas credenciales - Capacitar al personal de backup - Formar grupos de trabajo para evitar el contacto o la movilización del personal

Nota. Elaboración propia

- **Plan de gestión de emergencias**

TABLA 41. PLAN DE EMERGENCIAS ANTE INDISPONIBILIDAD DE LOS SERVICIOS

Eventos que activan la Contingencia:
Indisponibilidad en los servicios
Procesos Relacionados:
Disponibilidad de respaldos de información
Disponibilidad de enlaces de internet
Disponibilidad de recursos tecnológicos para contingencia
Personal que autoriza la contingencia:
Jefe del departamento de TI

Actividades por realizarse:
- Activación de la cadena de llamadas - Revisión física de los posibles daños - Revisión de posibles cambios al código - Verificación de garantía vigente de equipos - Verificación de SLA de servicios brindados por proveedores externos - Aplicación de estrategias de continuidad del negocio - Sustitución física de partes o piezas dañadas - Restauración de versiones estables anteriores
Duración:
Tiempo máximo de la contingencia no debe ser superior a las dos (2) horas.

Nota. Elaboración propia

TABLA 42. PLAN DE EMERGENCIAS ANTE DESASTRES NATURALES

Eventos que activan la Contingencia:
Ocurrencia de un desastre natural
Procesos Relacionados:
Disponibilidad de respaldos de información
Disponibilidad de recursos tecnológicos para contingencia
Seguridad del recurso humano
Personal que autoriza la contingencia:
Responsable del comité de crisis
Actividades por realizarse:
- Detener las actividades del personal - Activación de la cadena de llamadas - En lo posible, apagar los equipos de trabajo y desconectar de la energía eléctrica - El personal capacitado debe poner en práctica lo aprendido en los simulacros - Evacuación del personal a un sitio seguro
Duración:
Tiempo máximo de la contingencia no debe ser superior a las dos (2) horas.

Nota. Elaboración propia

TABLA 43. PLAN DE EMERGENCIAS FRENTE A CASOS FORTUITOS

Eventos que activan la Contingencia:
Ocurrencia de casos fortuitos
Procesos Relacionados:
Disponibilidad de respaldos de información
Disponibilidad de enlaces de internet
Acceso remoto autorizado por medios seguros
Seguridad del recurso humano
Personal que autoriza la contingencia:
Jefe del departamento de TI
Comité de crisis
Actividades por realizarse:
- Activación de la cadena de llamadas - Aplicación de medidas de bioseguridad - Conformación de grupos de trabajo para laborar en jornadas diferentes - Aplicación de teletrabajo
Duración:
Tiempo máximo de la contingencia no debe ser superior a las cuatro (4) horas.

Nota. Elaboración propia

- **Plan de recuperación de desastres**

TABLA 44. DRP ANTE FALLAS A NIVEL FÍSICO O LÓGICO

Evento: Falla en hardware o software
Personal encargado:
Personal del departamento de TI
Actividades:
Activación de la cadena de llamadas
Verificación de garantía vigente de equipos
Instalación y configuración de equipos de contingencia
Aplicación de acuerdos de nivel de servicio (SLA)

Restauración de copias de respaldo
Validación de funcionamiento de servicios
Mecanismos de comprobación:
Realización de pruebas pertinentes posteriores al reemplazo de partes, piezas o equipos de contingencia. Validación de copias de seguridad
Registro del incidente en una bitácora que incluya las acciones realizadas para su solución
El personal técnico responsable del activo o servicio debe elaborar un informe explicando de manera detallada la causa que originó la afectación de las actividades. Debe incluir el tiempo total de interrupción, la contingencia aplicada, las pruebas de restablecimiento del servicio, entre otros parámetros que considere relevantes
Desactivación del DRP
Una vez que se ha solucionado el incidente, el Jefe del departamento de TI es el encargado de desactivar el plan de recuperación y de comunicar al resto del personal
Proceso de Actualización
Basado en el informe emitido por el personal técnico responsable posterior a un incidente, se deberá analizar y evaluar las acciones tomadas en la solución de este y de ser necesario se actualizará el plan de prevención para mitigar futuros riesgos
Actualizar el stock de partes, piezas y recurso tecnológico disponible

Nota. Elaboración propia

TABLA 45. DRP ANTE DESASTRES NATURALES

Evento: Desastres naturales
Personal encargado:
Personal del departamento de TI
Comité de crisis
Actividades:
Activación de la cadena de llamadas
Revisión de la infraestructura, tuberías o posibles daños en las instalaciones

eléctricas
Evaluar la condición física del recurso humano
Si no existen daños en la infraestructura, levantar y verificar el correcto funcionamiento de los diferentes servicios
Verificación de garantía vigente de equipos
Monitoreo continuo de las acciones de recuperación
Mecanismos de comprobación:
Registrar en la bitácora el proceso de recuperación, documentando cualquier cambio o modificación en el proceso normal de operación
Documentar el tiempo empleado en el proceso de recuperación tanto del personal interno, como del proveedor externo de servicios
En el caso de daño de equipos con garantía, iniciar la comunicación con el proveedor
En el caso de existir, se debe determinar de manera aproximada los gastos incurridos durante el proceso de recuperación
El comité de crisis debe elaborar un informe que detalle la aplicación del plan de recuperación, la evaluación de los daños y la afectación económica producida
Desactivación del DRP
Una vez que se ha solucionado el incidente y se ha determinado que es seguro regresar al sitio de trabajo, el comité de crisis y el Jefe del departamento de TI son los encargado de desactivar el plan de recuperación y de comunicar al resto del personal
Proceso de Actualización
En base al informe emitido por el comité de crisis, se debe evaluar si las acciones empleadas son suficientes para recuperar la operatividad dentro de la empresa. Bajo este criterio es posible analizar otras acciones que deben ser incluidas o que pueden complementar a las ya existentes

Nota. Elaboración propia

TABLA 46. DRP FRENTE A CASOS FORTUITOS

Evento: Casos fortuitos

Personal encargado:
Personal del departamento de TI
Comité de crisis
Actividades:
Activación de la cadena de llamadas
Activación de mecanismos para teletrabajo
Soporte remoto para usuario final
Grupos de trabajo en horarios diferentes
Mecanismos de comprobación:
En caso de contagio en pandemia, el personal involucrado debe reportar al área de recursos humanos su condición de salud para determinar si es factible que realice o no teletrabajo
En el caso de cierre de vías por manifestaciones, el personal afectado debe informar al jefe inmediato para la autorización de teletrabajo
En cualquier caso fortuito se activa el personal de backup para garantizar la continuidad de las operaciones, así como el soporte al cliente final
Socializar por los medios autorizados, los grupos de trabajo conformados
Desactivación del DRP
El comité de crisis es el encargado de desactivar el plan de recuperación y de comunicar al resto del personal las acciones que se mantendrán mientras duren este tipo de incidentes
Proceso de Actualización
De manera semanal el responsable del comité de crisis actualizará la información sobre las medidas adoptadas en base al desarrollo de los acontecimientos.

Nota. Elaboración propia

6.8.3.3. Comité de crisis

Este grupo conformado por varios directivos y personal de la empresa 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:

TABLA 47. CONFORMACIÓN DEL COMITÉ DE CRISIS

Responsable del comité de crisis	Jefe del departamento de TI	Es el encargado de convocar a reuniones, notificar las eventualidades, dirigir las reuniones y designar el personal de reemplazo en el caso de ausencia de alguno de los miembros
Miembros del comité de crisis	Gerente General	Son los encargados de aportar con la información requerida de acuerdo con su área
	Jefe administrativo	
	Analista de recursos humanos	
	Técnico en seguridad informática	
	Desarrollador	
Lugar de reunión	Sala de reuniones de gerencia	

Nota. Elaboración propia

6.8.4. 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.

6.8.4.1. Plan de prueba y revisión

TABLA 48. PLAN DE PRUEBAS DE LOS COMPONENTES DEL BCP

Objetivo	Determinar la periodicidad y las acciones a ejecutarse para validar las estrategias establecidas en el proceso de continuidad del negocio y en el caso de requerirlo aplicar las mejoras necesarias.
Alcance	El plan de pruebas se aplica a todos los componentes que conforman el BCP
Componentes	Stakeholders
	Roles y responsabilidades
	BIA
	Análisis de riesgos
	Estrategias de recuperación
	Auditoría interna
	Capacitaciones
	Comunicación del BCP
	Actualización del BCP

Nota. Elaboración propia

6.8.4.2. Plan de mantenimiento del BCP

TABLA 49. 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	Revisión y actualización de activos críticos y nivel de riesgo	Anual

	determinado	
Estrategias de recuperación	Simulación de eventos disruptivos de manera planificada y fuera de horario laboral	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

Nota. Elaboración propia

6.8.5. 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.

6.8.5.1. Plan de capacitación y concienciación

Inicialmente, el plan de capacitación y concienciación está dirigido al personal del departamento de TI. En la Tabla 50, 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 del área de TI 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.

TABLA 50. 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 incidentes	30
Gestión de continuidad del negocio	40

Nota. Elaboración propia

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 informativas.