UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Carrera de Ingeniería en Sistemas Computacionales

TEMA:

DISEÑO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN INDUSTRIAS KARMAT BAJO LOS LINEAMIENTOS DE LA NORMA ISO 22301 INCORPORANDO UN REPOSITORIO DIGITAL.

Trabajo de Grado previo a la obtención del título de Ingeniero en Sistemas Computacionales.

AUTOR (A):

Yesenia Pamela Coyago Marcalla

DIRECTOR (A):

MSc. Cosme MacArthur Ortega Bustamante

Ibarra, 2023

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003506621		
APELLIDOS Y NOMBRES:	Coyago Marcalla Yesenia Pamela		
DIRECCIÓN:	Alpachaca - Ibarra		
EMAIL:	ypcoyagom@utn.edu.ec		
TELÉFONO FIJO:	062510511	**TELÉFONO MÓVIL:**	0986405422

DATOS DE LA OBRA	
TÍTULO:	DISEÑO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN INDUSTRIAS KARMAT BAJO LOS LINEAMIENTOS DE LA NORMA ISO 22301 INCORPORANDO UN REPOSITORIO DIGITAL.
AUTOR (ES):	COYAGO MARCALLA YESENIA PAMELA
FECHA: DD/MM/AAAA	19/10/2023
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERÍA EN SISTEMAS COMPUTACIONALES
ASESOR /DIRECTOR:	MSC. COSME MACARTHUR ORTEGA BUSTAMANTE

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 19 días del mes de octubre de 2023.

EL AUTOR:

Yesenia Coyago

Nombre: Coyago Marcalla Yesenia Pamela

CERTIFICADO DEL DIRECTOR DE TRABAJO DE GRADO

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR

Por medio del presente yo PhD. MacArthur Ortega, certifico que la Srta. Yesenia Pamela Coyago Marcalla, portadora de la cédula de ciudadanía Nro. 1003506621, ha trabajado en el desarrollo del proyecto de tesis "DISEÑO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN INDUSTRIAS KARMAT BAJO LOS LINEAMIENTOS DE LA NORMA ISO 22301 INCORPORANDO UN REPOSITORIO DIGITAL.", previo a la obtención del título de Ingeniería en Sistemas Computaciones, lo cual ha realizado en su total responsabilidad.

Es todo cuanto puedo certificar en honor a la verdad.

Atentamente,

1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE

Firmado digitalmente por 1001580396 COSME MACARTHUR ORTEGA BUSTAMANTE
Fecha: 2023.10.19 17:07:56 -05'00'

Ing. MacArthur Ortega, MSc.

DIRECTOR DE TESIS

INDUSTRIAS KARMAT

RUC: 1002790358001

Ibarra, 31 de Agosto 2023

Certifica

Me permito informar a Ustedes que la señorita YESENIA PAMELA COYAGO MARCALLA, con cédula de ciudadanía Nro. 1003506621, estudiante de la Universidad Técnica del Norte, ha realizado su Trabajo de Grado con el tema: **"DISEÑO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN INDUSTRIAS KARMAT BAJO LOS LINEAMIENTOS DE LA NORMA ISO 22301 INCORPORANDO UN REPOSITORIO DIGITAL."**
Cumpliendo con todos los requisitos reglamentarios de aprobación de la empresa, con cualidades de responsabilidad y profesionalismo.

Para efecto, se extiende el presente CERTIFICADO DE CULMINACIÓN DEL PLAN, en la ciudad de Ibarra, a los 15 días del mes de agosto de 2023.

Agradezco su atención.

Ing. Gabriela Pilataxi

GERENTE INDUSTRIAS KARMAT

INDUSTRIAS KARMAT pielactive VENTA POR CATÁLOGO

Dirección: MiguelAlbánPaliz1-92entreTobíasMenayRicardoSánchez
Telf.: (065) 001 - 771 **(065)** 001 - 770
Ibarra -Ecuador

DEDICATORIA

Mientras reflexiono sobre el arduo trabajo que ha requerido este proyecto de investigación, no puedo evitar pensar en el papel fundamental que han desempeñado mis padres, hermanos y amigos. Aunque este logro lleva mi nombre, detrás de cada página y noche tardía.

Agradezco de corazón a mis padres, quienes no solo me dieron la vida, sino que también me enseñaron a enfrentar cada desafío con determinación. Su constante presencia, su guía en cada etapa y su inquebrantable apoyo han sido el pilar fundamental que me ha sostenido y permitido llegar a donde estoy hoy.

A mis hermanos, con quienes he compartido innumerables momentos y aprendizajes, les debo gran parte de quien soy.

Y a mis amigos, esos compañeros de vida que elegí y que me eligieron, les agradezco por ser una fuente inagotable de sabiduría, alegría y apoyo. Cada conversación, cada risa compartida y cada consejo han contribuido significativamente a mi crecimiento personal e intelectual. Juntos, hemos construido recuerdos imborrables y han sido, sin lugar a dudas, los compañeros de este éxito que hoy celebro.

Yesenia

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento al equipo de Industrias Karmat. Su confianza en mí y la oportunidad que me brindaron para llevar a cabo todo el proceso han sido fundamentales para mi crecimiento profesional y personal.

Además, deseo destacar la invaluable guía y mentoría de mi tutor, MSc. MacArthur Ortega. Su paciencia, sabiduría y compromiso con mi formación han sido pilares en este viaje. Asimismo, mi sincero reconocimiento a mis asesores: PhD. Daisy Imbaquingo y PhD. Marco Pusdá, quienes con su vasto conocimiento, enseñanzas y disposición a colaborar, no solo enriquecieron este trabajo, sino que también fortalecieron mi formación y visión profesional. Su dirección y consejos han sido cruciales para alcanzar los objetivos propuestos y para el desarrollo exitoso de este proyecto.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Esta investigación se centró en diseñar un plan de continuidad del negocio para la empresa ecuatoriana Industrias Karmat. El objetivo principal fue desarrollar un plan alineado con la norma ISO 22301 para garantizar la continuidad de los procesos de negocio críticos. La metodología empleada fue la Revisión Sistemática de la Literatura (SLR) para analizar las principales fuentes de información e interpretar los resultados. Se utilizó la metodología MAGERIT para la evaluación de riesgos tecnológicos. Los instrumentos de recolección de datos fueron encuestas y entrevistas.

El diagnóstico inicial utilizando las cláusulas ISO 22301 mostró que el nivel de madurez en la gestión de la continuidad del negocio de la empresa era del 23%. Después del diseño e implementación parcial del plan, la madurez aumentó al 73,4%. La acumulación de riesgo de los activos tecnológicos se calificó como crítica (7,2) y la acumulación de impacto en disponibilidad como muy alta (10). Se identificaron seis actividades críticas relacionadas con la infraestructura tecnológica como prioridad máxima para la recuperación. Las estrategias se enfocaron en restaurar primero estas actividades.

El mantenimiento, pruebas y revisión verificaron la viabilidad del plan y establecieron acciones correctivas. Se creó un programa de capacitación para generar conciencia en los empleados. Se incorporó un repositorio digital usando Omeka S para almacenar y categorizar toda la información generada.

Las principales contribuciones fueron aumentar la preparación de continuidad del negocio de la empresa, reducir el impacto de los riesgos tecnológicos, definir procedimientos para garantizar la restauración de actividades críticas y proporcionar un fácil acceso al plan a través del repositorio. Este proyecto sirve como guía para empresas comerciales que buscan continuidad del negocio basada en ISO 22301.

Palabras clave: plan de continuidad del negocio, norma ISO 22301, repositorio digital, riesgos tecnológicos, actividades críticas, estrategias de recuperación, capacitación, Omeka S**.**

ABSTRACT

This research focused on designing a business continuity plan for the Ecuadorian company Industries Karmat. The main objective was to develop a plan aligned with ISO 22301 standard to ensure critical business processes continuity. The methodology employed was Systematic Literature Review (SLR) to analyze main information sources and interpret results. MAGERIT methodology was used for technological risk assessment. Data collection instruments were surveys and interviews.

The initial diagnosis using ISO 22301 clauses showed the company's business continuity management maturity level was 23%. After plan design and partial implementation, maturity increased to 73.4%. Technological asset risk accumulation was rated as critical (7.2), and availability impact accumulation as very high (10). Six critical activities related to tech infrastructure were identified as top priority for recovery. Strategies focused on restoring these activities first.

Maintenance, testing and review verified plan feasibility and established corrective actions. A training program created employee awareness. A digital repository using Omeka S was incorporated to store and categorize all generated information.

The main contributions were increasing the company's business continuity preparedness, reducing technological risks impact, defining procedures to ensure critical activities restoration, and providing easy plan access through the repository. This project serves as a guideline for commercial companies seeking business continuity based on ISO 22301.

Keywords: business continuity plan, ISO 22301 standard, digital repository, technological risks, critical activities, recovery strategies, training, Omeka S

INTRODUCCIÓN

Antecedentes

Al presente el país y el mundo atraviesa una situación compleja producto del aparecimiento del COVID-19, esto obliga a las pequeñas y medianas empresas (pymes) a adaptar su modelo de gestión con herramientas e insumos innovadores.

Las empresas para desarrollar sus actividades dependen de recursos críticos como tecnología de la información, humano, económico, etc. La pérdida de tiempo en la disponibilidad de estos recursos afecta en alto grado la rentabilidad y viabilidad del negocio.

Situación actual

En Ecuador, como en el resto del mundo, las empresas están enfrentando momentos de incertidumbre por la crisis sanitaria, el 84 % de empresas aseguran que las ventas disminuyeron por COVID-19 y el 83 % afirma que su principal preocupación son sus clientes.

En el Ecuador existen riesgos latentes como: terremotos, incendios, inundaciones y últimamente atentados terroristas; y las empresas en su mayoría no están preparadas para estas contingencias, además existen eventos inesperados que no necesariamente se relacionan con desastres naturales, también se relacionan con fallas humanas, interrupción de fluido eléctrico, ciberataques y pérdida de datos (Zapata Vásquez, 2020).

Las pymes deben identificar las principales amenazas de su organización y tener la capacidad de establecer procesos, procedimientos, políticas y estrategias para disminuir el impacto financiero, pérdida de información, credibilidad, reputación y productividad ante un evento crítico inesperado, y poder operar y prestar servicios durante y después de dicho evento.

Prospectiva

Considerando estos posibles fallos que afecten la continuidad de las operaciones en la empresa. Durante la irrupción no se levantará todos los procesos del negocio, pero se deben contar con un mínimo necesario de procesos, que se considerarán críticos en los que se ejecutan cada operación y lograr conservar la imagen corporativa de la empresa, minimizar el impacto y evitar grandes pérdidas monetarias.

Aunque las pérdidas por un desastre informático sean importantes, cada vez son mayores los avances tecnológicos y normas que permiten la recuperación en poco tiempo y en costes razonables, siendo los ciclos de implantación cada vez más cortos (Tumbaco Mieles & Yépez Manosalvas, 2009).

Planteamiento del Problema

Un bajo presupuesto asignado para tecnología cuestiona que los servicios y por ende los procesos que la empresa desarrolle para sus operaciones cuente con los recursos tecnológicos adecuados, siendo de esta manera una limitación de ellos.

Dentro del funcionamiento de la empresa se toma en cuenta el personal, parte esencial de las operaciones por lo que el incumplimiento de las funciones que han sido asignadas a estos provoca un retraso en el cumplimiento de los procesos esenciales.

Una administración inadecuada de los problemas que se presenten en el entorno de la empresa sea cual sea su índole, causa un total desconocimiento de los procesos que se deben ejecutar para la mitigación de dichos problemas.

Figura 1.

Diagrama de planteamiento de problema.

Objetivos

Objetivo General

Diseñar un plan de continuidad del negocio en Industrias Karmat bajo los lineamientos de la norma ISO 22301 incorporando un repositorio digital.

Objetivos Específicos

- Establecer una línea de base de análisis de las políticas de continuidad del negocio de la empresa.
- Realizar una evaluación de riesgos tecnológicos del negocio.
- Diseñar el plan de continuidad del negocio aplicando los lineamientos de la norma ISO 22301.

- Divulgar el plan de continuidad a través de un sistema de gestión de contenidos.

Alcance

El alcance del diseño del Plan de Contingencia en los procesos críticos para la continuidad del negocio, con respecto a las áreas principales de la empresa.

Una vez analizada el estado del arte de continuidad del negocio se genera documentación base en la cual se basa el desarrollo conociendo sus antecedentes.

Dentro del análisis de riesgos tecnológicos del negocio se elabora un mapeo de riesgos tecnológicos.

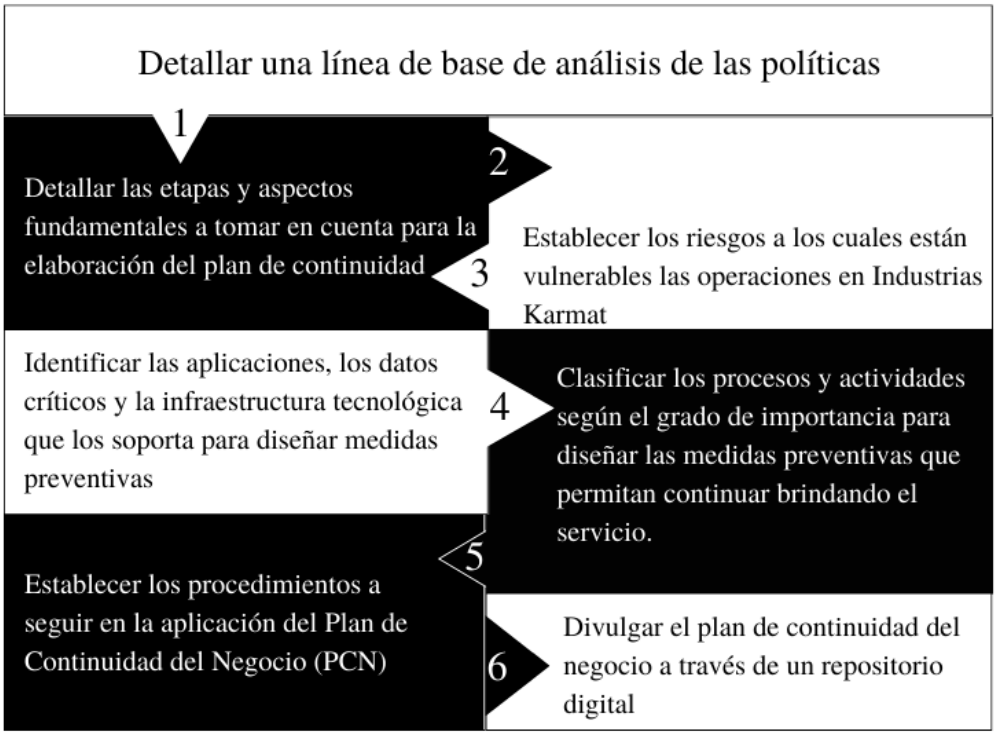
El plan de continuidad se detalla según los requisitos y los posibles riesgos que se puedan presentar en la empresa.

Se incorpora un repositorio digital que está a disposición de los interesados de la organización, que se almacenará de forma cronológica permitiendo un mejor uso del repositorio.

Para el desarrollo de este plan se abordarán los siguientes aspectos. Véase Figura 2

Figura 2.

Flujo del proyecto.



Justificación

Justificación Social

En la Constitución de la República consta que son deberes primordiales del estado ecuatoriano el proteger a las personas, las colectividades y la naturaleza de los efectos negativos causados por los desastres, ya sean estos de origen natural o antrópico.

Se deben elaborar estrategias que prevengan que estas situaciones impacten negativamente en la vida de las personas, para lo que se usan planes de prevención del riesgo, mitigación de desastres, recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, para minimizar la vulnerabilidad.

El propósito de este proyecto es contar con un enfoque integral sobre el impacto que pueden generar eventos antrópicos, así como también analizar el nivel de vulnerabilidad de la empresa

Industrias Karmat. Además, se aprecia una visión integral de los posibles planes de acción de tal manera que se contemple los elementos claves como son el análisis de impacto de recuperación productiva basado en la norma ISO 22301 “Sistema de Gestión de la Continuidad del Negocio - SGCN”, los planes de minimización de impacto en los procesos críticos y el fortalecimiento de la seguridad laboral, para así no solo evitar pérdidas humanas, sino también las materiales y económicas o situaciones que impidan el funcionamiento de la empresa.

Justificación Tecnológica

El impacto tecnológico es innovador, ya que se usa un repositorio digital para resguardar la información recabada del plan de continuidad del negocio, los nombres de los empleados clave para implementar dichos planes y los datos de los clientes, proveedores, distribuidores y red comercial de la empresa, así se logra aplicar un conjunto de acciones, identificando a los responsables de cada acción y los recursos necesarios.

Contexto

Este tema de investigación pretende contextualizar los conocimientos establecidos en los trabajos de investigación de la Tabla 1.

Tabla 1.

Contextualización de trabajos de investigación.

Trabajo de titulación	Enlace	Aporte
Implementación de un Sistema de Gestión de Continuidad de Negocio alineado con la ISO 22301 y la ISO 27031	http://hdl.handle.net/10347/17853	Se usa la versión más actualizada de la norma ISO 22301:2019, en la cual se fija nuevos tipos de documentos.
Desarrollo del plan de continuidad del negocio para la empresa EQUIVIDA S.A. para el período 2012-2015	https://repositorio.espe.edu.ec/bitstream/21000/7421/1/T-ESPE-047538-AC.pdf	Se enfoca en un tipo de actividad diferente referente a la empresa ya que es acerca de una empresa de prestación de comercialización (venta de productos).

Sistema de gestión para la continuidad del negocio que garantice a la Cooperativa de Ahorro y Crédito Atuntaqui Ltda.	http://repositorio.utn.edu.ec/bitstream/123456789/1260/1/PG%20337_PLAN%20DE%20CONTINUIDAD%20DE%20NEGOCIO.pdf	Se aplica una norma de continuidad del negocio bajo la ISO 22301 para cualquier tipo de empresa.
Diseño de un plan de continuidad del negocio en una constructora de la ciudad de Medellín - Colombia bajo la norma ISO 22301:2012	https://repository.uniminuto.edu/bitstream/handle/10656/5687/TEGP_Cata%C3%B1oTurianLuzMarleny_2015.pdf?sequence=1&isAllowed=y	Se utiliza la normativa para cada proceso de la empresa como para cada evento que se pueda presentar en una empresa de comercialización de productos.
Análisis y diseño de un plan de contingencia de las aplicaciones y redes que manejan las pymes en casos de pandemias.	http://repositorio.ug.edu.ec/bitstream/redug/49446/1/B-CINT-PTG-N.559%20Castro%20Guala%20Ronald%20Leonel%20.pdf	Se desarrolla un análisis de toda la infraestructura tecnológica de la empresa, así como la incorporación de los debidos procesos para su verificación.
Diseño de un plan de continuidad del negocio en el área de atención al cliente para la Cooperativa de Ahorro y Crédito San Antonio Ltda. basado en la Norma ISO 22301:2012	http://repositorio.utn.edu.ec/bitstream/123456789/10633/2/04%20IND%20268%20TRABAJO%20GRADO.pdf	Se diseña un plan de continuidad del negocio basado en los principales servicios críticos y tecnológicos que la empresa presente durante el proceso de evaluación.
Políticas de buenas prácticas, relacionadas con la seguridad informática y la continuidad del negocio, en el mall del centro	http://dspace.uniandes.edu.ec/bitstream/123456789/4142/1/PIUAMIE001-2016.pdf	Se aplica la norma ISO 22301 para el desarrollo y ejecución, además de la elaboración de los diferentes planes que conforman el plan de continuidad del negocio.

CAPITULO I

1.1. Marco Teórico

En este capítulo se incluyen definiciones y la línea investigativa en la que se desarrolla la presente investigación obteniendo un conocimiento claro de la continuidad del negocio sus beneficios principales, tipos de planes y fases que lo comprenden, normas que se enfocan en la gestión de la continuidad y herramientas de divulgación para la presentación de resultados.

Para el desarrollo de la investigación, se usó la metodología Revisión Sistemática de la Literatura - SLR para el análisis de las principales fuentes de información del presente estudio e interpretación de los resultados permitiendo la organización efectiva y alineada al punto del estudio.

1.2. Metodología SLR

Una revisión sistemática de la literatura - SLR, es un método para identificar, analizar e interpretar investigaciones relevantes en un campo en particular y ayuda en el proceso de revisión como lo indican (Webster & Watson, 2002) en su artículo "*Analyzing the past to prepare for the future: writing a literature review*". La revisión de información permite la fundamentación teórica del marco conceptual que argumenta sobre la continuidad del negocio.

1.2.1. Preguntas de investigación

Con respecto a la unidad de análisis, se desarrolló preguntas de investigación que son la base para el desarrollo y la formulación de la búsqueda de documentos como se muestra en la Tabla 2.

Tabla 2.

Preguntas de Investigación PI.

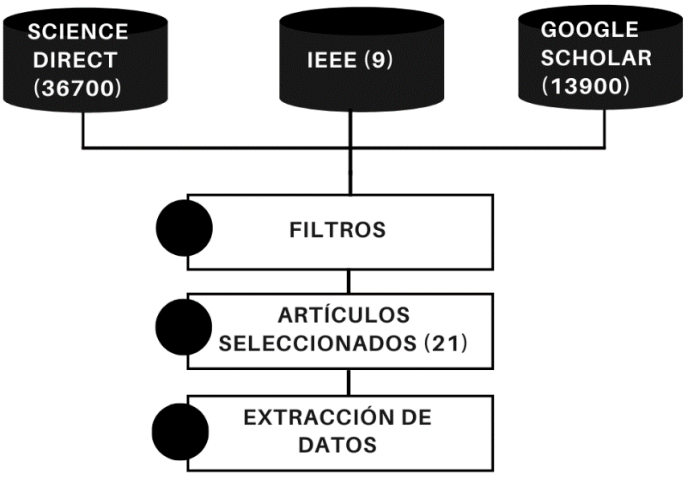
N°	Preguntas de investigación
1	¿Qué es un plan de continuidad del negocio?
2	¿Cuáles son las normas ISO enfocadas en la continuidad del negocio?
3	¿Cuáles son los principales riesgos tecnológicos de la última década en empresas comerciales en Ecuador?

1.2.2. Búsqueda de documentos

Dentro del proceso de búsqueda de documentos se pudo concluir que en su mayoría la información se encuentra en idioma inglés y la información en español es mucho más reducida, por ende, se hizo uso de conectores booleanos (*AND* y *OR*), los términos usados son: *business continuity planning* o su abreviación BCP/PCN y la norma que se estudia es la NORMA ISO 22301, se establecen como principales bases de datos bibliográficos: *ScienceDirect, Institute of Electrical and Electronics Engineers* (IEEE) y *Google Scholar*, definiendo el diagrama de búsqueda así como se puede observar en la Figura 3.

Figura 3

Diagrama de búsqueda.



Los 21 documentos seleccionados se detallan en la Tabla 3.

Tabla 3.

Documentos seleccionados.

Código	Artículo	Autor	Cita
A1	Business Continuity Management Through Stakeholders Collaboration and Participation	Rozova D, Fuchs M	(Rozova & Fuchs, 2021)
A2	Information Management Procedures for Business Continuity Plan Maintenance	Aziz N, Jambari D,	(Aziz & Jambari, 2019)
A3	Why implement continuity plans in Organizations? Approach of a prospective study based on ITIL	Monica R, Henry Q, Estela M, Washington F	(Monica et al., 2020)
A4	Assessing the Business Continuity of a healthcare organization through a data-gathering modality approach	Amara O, Kamissoko D, Fijalkow Y, Benaben F	(Amara et al., 2022)
A5	Business Continuity Plan: Examining of Multi-Usable Framework	Fani S, Subriadi A	(Fani & Subriadi, 2019)
A6	Investigating the influence of governance determinants on reporting cybersecurity incidents to police: Evidence from Canadian organizations' perspectives	Agbodoh-Falschau K, Ravaonorohanta B	(Agbodoh-Falschau & Ravaonorohanta, 2023)
A7	Developing an Enterprise Continuity Program	Petrenko S	(Petrenko, 2021)
A8	Business Continuity Planning: An Effective Strategy During an Electronic Health Record Downtime	Roush K, Opsahl A, Parker K, Davis J	(Roush et al., 2021)
A9	Ecosystem-centric business continuity planning (eco-centric BCP): A post COVID19 new normal	Mukherjee M, Chatterjee R, Khanna B, Dhillon P, Kumar A, Bajwa S, Prakash A, Shaw R	(Mukherjee et al., 2020)
A10	Analysis of workload required for removal of drifting pumice after a volcanic disaster as an aspect of a port business continuity	Asano T, Nagayama A	(Asano & Nagayama, 2021)

	plan: A case study of Kagoshima Port, Japan		
A11	What is business continuity planning?	Phillips B, Landahl M	(Phillips & Landahl, 2021)
A12	Essential tools and resources for business continuity planning	Brenda D. Phillips, Mark Landahl	(Brenda D & Mark, 2021)
A13	FAMMOCN – Demonstration and evaluation of a framework for the multidisciplinary assessment of organizational maturity on business continuity	Russo N, São H, Reis L, Silveira C	(Russo et al., 2022)
A14	Business continuity management of small and medium sized enterprises: Evidence from Thailand	Kato M, Charoenrat T	(Kato & Charoenrat, 2018)
A15	Plan de continuidad del negocio de acuerdo a la norma ISO 22301 de la empresa Formica de Albal (Valencia)	Delfa Baena S	(Delfa Baena, 2022)
A16	Plan de continuidad de negocio en las universidades	Canca Cuenca J	(Canca Cuenca, 2022)
A17	Modelo de Evaluación de Gestión de Continuidad del Negocio basado en la norma ISO 22301:2012	Lojan Granda E	(Lojan Granda, 2017)
A18	Guías para la implementación y auditoría de planes de continuidad de negocio desde la perspectiva de la norma ISO 22301, BS 25999, NTC 5722 y las prácticas profesionales del DRII y de ISACA	Figueroa H, Salamanca M	(Figueroa & Salamanca, 2013)
A19	Business Continuity Planning: Increasing Workplace Resilience to Disasters	Phillips D B, Landahi M	(Phillips D & Landahi, 2021)
A20	Building adaptive business continuity plans: Practical tips on how to inject adaptiveness into continuity planning processes.	Hatton T, Brown C	(Hatton & Brown, 2021)
A21	IT capability and organizational performance: The roles of business process agility and environmental factors	Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S.	(Chen et al., 2014)

1.2.3. Selección de artículos

Para la selección de artículos se aplicaron criterios de inclusión y exclusión para los documentos, para la inclusión se analizan: artículos relacionados con las áreas de ingeniería, tecnología y auditoría, de referencia en idioma inglés; y se excluye todos los artículos relacionados con BCM y aquellos que no sean de revistas o congresos.

Muchos artículos están relacionados con el BCP, por lo que se purgó datos logrando un refinamiento sucesivamente al conjunto de artículos basado en la aplicación de filtros.

Se aplicó el primer filtro, el cual buscó que los títulos se vinculen con BCP de empresas comerciales o departamentos TI, el segundo filtro realizó una eliminación manual por esta razón se consideró todos los artículos que dentro del resumen o *abstract* presenten información relevante acerca de la norma ISO 22301 en su versión del año 2019 y gestión de riesgos en empresas pequeñas y medianas (pymes) obteniendo de este modo la Tabla 3.

Tabla 4.

Listado de fuentes bibliográficas

Fuentes de búsqueda	Artículos encontrados	Filtro 1	Filtro 2	Artículos finales
ScienceDirect	36700	1543	255	10
IEEE	9	7	5	1
Google Scholar	13900	100	42	11
				21

1.3. Continuidad del negocio

Las empresas deben estar preparadas para prevenir, protegerse y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios (Instituto Nacional de Ciberseguridad, 2020).

La continuidad del negocio es aquel nivel la empresa se prepara para solventar y mantener sus funciones críticas durante y después de un evento financiero, legal, tecnológico, de gestión estratégica, accidente o desastre natural.

Considerándose que un evento es aquel suceso imprevisto que se genera de manera fortuita y que causa cierta incidencia para el proceso.

Durante un evento ya sea de tipo: falló de infraestructura o tiempo de inactividad genera pérdidas; todas las pérdidas se deben a oportunidades pérdidas por parte de la organización ya sea que los clientes no pueden acceder a un portal de compras ni los equipos de ventas no pueden interactuar con el público debido a los sistemas de CRM caídos, lo que genera grandes pérdidas anuales que afectar el costo total de la pérdida y al beneficio neto de la empresa (Network Coverage, 2021).

Dentro del estudio de (Hubbard, 2022; Shulmistra, 2022), el coste para este tipo de interrupciones para las pequeñas y medianas empresas (pymes), puede llegar a ser desde los $137 a $427 dólares por minuto, dicho valor afecta o no a la empresa dependiente de factores como: mercado que se desarrolla, tamaño de la empresa y modelo de negocio, siendo estos costes mayores anualmente como se ve en la Figura 4.

Figura 4.

Coste promedio anual.

Fuente: (Xiang et al., 2023)

En el caso de que se suscite un hecho de cualquier índole se debe contar con políticas, estrategias y mecanismos que regulen los procesos a ponerse en marcha, así como establecer los períodos de recuperación mínimo, motivos y retroalimentación acerca del incidente una vez superado.

Hay que valorar los principales servicios, la repercusión en caso de fallo en la organización, y así lograr la consolidación de un plan que se enfoque en recuperar las funcionalidades más esenciales.

1.3.1. Definición del plan de continuidad del negocio

En las organizaciones se ha aprovechado por mucho tiempo, pero en los últimos años ha tenido un mayor impacto en las empresas internacionales, ya que por la aparición del COVID-19 varias de ellas debieron adecuar o modificar sus procesos y considerar cuál de ellos más críticos.

El análisis de los conceptos emitidos por los autores como instituciones se observa en la Tabla 5, una definición más clara sobre el concepto de plan de continuidad del negocio (PCN) en la investigación.

Tabla 5.

Definiciones plan de continuidad del negocio.

Autor	Concepto	Año	País
Superintendencia de Bancos	Es el conjunto de procedimientos que orientan a las entidades a mantener su operatividad si ocurren interrupciones que afecten sus servicios.	2021	Ecuador
Bevan Tony	Procedimientos documentados que guían a una organización para responder, recuperarse, reanudar y restablecerse a un nivel de operación predefinido tras una interrupción.	2019	Reino Unido
Federal Financial Institutions Examination Council IT	Un plan escrito completo para mantener o reanudar el negocio en caso de una interrupción.	2019	Estados Unidos
National Institute of Standards and Technology - U.S. Department of Commerce	La documentación de un conjunto predeterminado de instrucciones o procedimientos que describen cómo se sostendrán los procesos de misión / negocio de una organización durante y después de una interrupción significativa.	2019	Estados Unidos
Martin Juan	Es un documento que consta de la información crítica que necesita una empresa para continuar operando durante un evento no planificado. El BCP debe establecer las funciones esenciales de la empresa, identificar qué sistemas y procesos deben mantenerse y detallar cómo mantenerlos.	2018	España
National Institute of Standards and Technology	El plan de continuidad del negocio se centra en mantener los procesos de misión/negocio de una organización durante y después de una interrupción.	2010	Estados Unidos

Tomando estos conceptos se puede definir el plan de continuidad del negocio como un documento que describe los procesos funcionales y operacionales de la empresa y fundamenta los procedimientos como reglas específicas para cada interrupción, mitigando las afectaciones posibles dentro de la organización; dicho documento describe la información necesaria y actualizada de manera clara y ordenada.

1.3.2. Beneficios de un plan de continuidad del negocio

Identificar los activos y procesos críticos durante la operación y la preparación de medidas preventivas y paliativas para cuando llegue el momento adecuado, garantizando así el uso adecuado de recursos como personal, material y tecnológico; y la continuidad del negocio.

Tabla 6.

Beneficios de un plan de negocio.

AUTOR	**Confianza**	**Responsabilidad**	**Resiliencia**	**Cultura Organizacional**	**Liderazgo**	**Ventaja Competitiva**	**Evitar Pérdidas Financieras**	**Identificación de Riesgos**	**Tranquilidad**	**Mejora de la Ciberseguridad**	**Satisfacción del Cliente**	**Priorización de Recursos**	**Evitar Interrupciones de Servicios**
(Xiang et al., 2023)			x				x		x				
(RESOLUCIÓN Nro. SB-2021-2126, 2021)	x	x		x		x			x		x		
(Cappelo, 2020)	x			x			x	x			x		
(Bevan, 2019)				x		x			x	x			
(Agility Recovery, 2021)			x				x	x			x	x	
(O'Neill, 2017)		x		x		x				x			x
(Federal Financial Institutions Examination Council's (FFIEC), 2023)	x			x		x		x			x	x	
(De La Hoz Suárez et al., 2022)			x					x					x

Dentro del análisis de los beneficios que ofrece un plan de continuidad presentados previamente en la Tabla 6 que enlista varios autores, quienes se enfocan en diferentes aspectos, los más relevantes se detallan a continuación:

- Identificación de riesgos: Conocer y estudiar los eventos que podrían perjudicar la continuidad de las operaciones, considerando los riesgos financieros, humanos o tecnológicos del negocio.
- Cultura organizacional: implementar una cultura de continuidad dentro de la organización permitiendo una mejor gestión de la empresa y aplicar una política de continuidad del negocio.
- Satisfacción del Cliente: Un adecuado manejo de las situaciones de emergencia sin una afectación notable de los servicios permitiendo que la satisfacción del cliente no se vea afectada de esta manera se cuenta con una imagen corporativa confiable.
- Confianza y tranquilidad: La generación de confianza y tranquilidad de la organización y junta directiva permite reforzar el liderazgo en la organización al contar con un plan de continuidad del negocio para resolver problemas, eventos disruptivos o emergencias, por lo que disminuye el estrés bajo presión.
- Ventaja competitiva: Varias empresas no cuentan con medios para el manejo de disrupciones, un PCN[1] es una ventaja competitiva que obtiene beneficios ya sean estos en corto plazo como es la continuidad de las operaciones frente a otra empresa

[1] Plan de continuidad del negocio.

y; largo plazo como la generación de reputación que genera confianza en los clientes y atrae a potenciales clientes.

- Evitar pérdidas financieras: Las pérdidas financieras son el resultado de una interrupción, como los fallos del sistema, la pérdida de energía y las filtraciones de datos, que pueden tener un impacto negativo en el desarrollo de la organización, y esos inconvenientes pueden mitigarse con un correcto proceso de gestión de esta manera evitando o reduciendo el riesgo.

1.3.3. Tipos de plan de continuidad del negocio

Dado que los contextos en los que opera una empresa son muy variados y hay muchas situaciones potenciales que puedan afectar a la continuidad de un negocio, existen diferentes planes de continuidad que permiten preparar más a la empresa. A continuación, se detalla los tres tipos principales en la Tabla 7.

Tabla 7.

Tipos de planes de continuidad

Tipos	Definición
Plan de continuidad del negocio o PCN	Se enfoca en continuar con las operaciones en infraestructura física, tecnológica TIC, personal, enseres, sistemas de producción e industriales; hasta que se logre una recuperación en la empresa; dicho plan contará con información de cada ámbito contemplado.
Plan de continuidad TIC, plan de contingencia TIC o PCTIC	Es parte de plan de continuidad del negocio, su principal diferencia con el PCN es que se enfoca en el área de TIC, permitiendo que se logré un mayor alcance en el ámbito tecnológico al contar con métodos específicos para el espacio definido.
Plan de recuperación ante desastres o PRD	Este plan tiene un menor nivel de profundización al momento del análisis y por ende su enfoque es más técnico, por lo que se enfoca en recuperar las actividades después del desastre

Fuente: (Instituto Nacional de Ciberseguridad, 2020)

1.3.4. Fases de un plan de continuidad del negocio

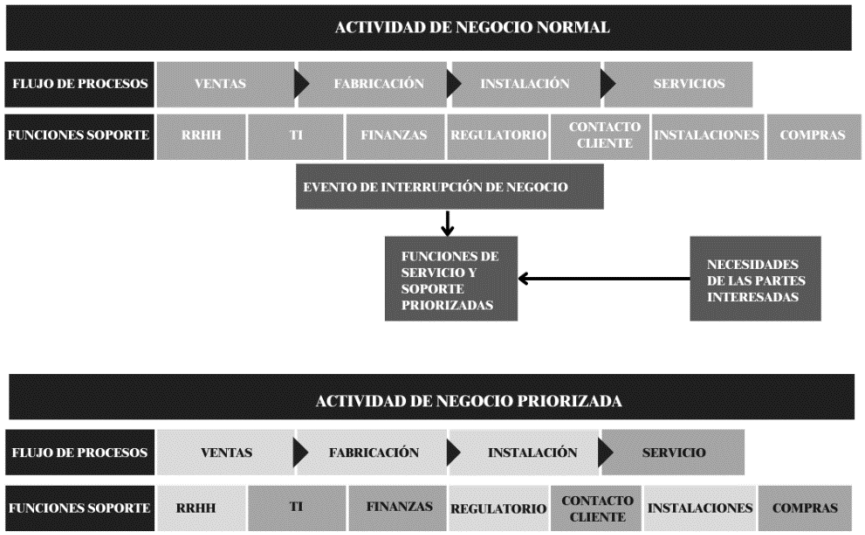
Desde el punto de vista (McFee, 2022), previo al proceso del plan de continuidad se debe tomar en cuenta cuatro principios básicos que son:

- ¿Conoce los productos y servicios clave para el éxito?
- ¿Qué actividades y recursos se necesitan para lograr el éxito? Incluye intangibles como la reputación en las redes sociales.
- ¿Qué podría perturbar su negocio y cuándo? No se debe olvidar las disrupciones provenientes de los clientes.
- ¿Cómo mantener la actividad durante las interrupciones?

Todas estas preguntas ayudan a conocer el desarrollo de la actividad del negocio, permitiendo conocer anticipadamente y enfocada la optimización de recursos de esta, de modo que en la Figura 5 se ve un análisis de una actividad de negocio normal contra una actividad priorizada en la que las actividades se desarrollan de una manera más ordenada y clara.

Figura 5.

Actividad de Negocio Normal vs Actividad de Negocio Priorizada.



Fuente: (Bevan, 2019)

Se establece ciertas estrategias que permiten que el proceso se ejecute correctamente y cumpla con las siguientes cuestiones, las mismas que se contestarán durante el desarrollo del proceso:

- ¿Qué se va a documentar?
- ¿Cuáles serían los tiempos de ejecución?
- ¿Quién aprobará y lo supervisará?
- ¿Quiénes serían los involucrados?
- ¿Qué áreas de la empresa le preocupan?

Para el desarrollo del plan de continuidad del negocio que permita la continuidad de los procesos críticos de la organización se debe tomar en consideración los siguientes pasos:

- Analizar e identificar los recursos críticos en la organización estableciendo prioridades dado el caso que se presente una interrupción.
- Establecer el diseño de una estrategia de continuidad de los servicios según los procesos, buscando reducir los impactos en los servicios críticos para lo que dicha estrategia deber difundirse, aprobarse y respaldarse por los directivos de la organización.
- Elaborar pruebas de continuidad que permitan verificar y asegurar la recuperación segura, atendiendo y mitigando errores que puedan atentar la disponibilidad de las operaciones.
- Comunicar a la organización internamente sobre el plan de continuidad del negocio y del análisis de impacto del negocio para crear sensibilidad a los miembros sobre la importancia de contar con dicho plan y garantizar un normal funcionamiento.

- Capacitar al personal acerca del plan de continuidad y el análisis de impacto del negocio, para que se generen roles y responsabilidades en incidentes y desastres, por lo que hay que verificar y entrenar.
- Generar procedimientos para el control de cambios asegurando que el plan de continuidad este actualizado y listo para afrontar posibles amenazas.

1.4. Normas aplicables

Con el constante cambio que se ha presentado desde el inicio del milenio, *International Organization for Standardization* (ISO) creó un comité técnico el cual se encarga de desarrollar y presentar estándares que se vinculan al área de seguridad social, entre los temas que se tratan son: protección de la sociedad, respuesta a incidentes, emergencias ya sean estás de tipo humano intencional o no intencional, desastres naturales y fallas técnicas.

Durante años el comité técnico ha venido trabajando en varias normas que buscan garantizar que las necesidades de los negocios como es la continuidad del negocio y la funcionalidad de los procesos se puedan restaurar y así evitar la pérdida de tiempo.

En la implementación de normas se tiene la seguridad y fiabilidad de apoyar las políticas públicas y su correcta legislación, la capacidad de trabajar en conjunto a los productos y servicios de la empresa, y una base sólida para las nuevas tecnologías y el mejoramiento de las buenas prácticas. Se han tomado en cuenta, a continuación, analizaremos algunas de ellas:

1.4.1. Norma ISO 22313

Como se indica en (Estruga, 2021), la base del estándar se orienta a las organizaciones para la aplicación de requisitos necesarios para implementar estrategias de continuidad y crear un Sistema de Gestión de la Continuidad del Negocio (SGCN) efectivo. Por consiguiente, está se

adapta a las necesidades de la empresa y sirve para complementar la norma ISO 22301, esta norma es la continuación y evolución del *Standard BS* 25999.

Para el desarrollo de las principales ventajas y desventajas se detalla a continuación la Tabla 8:

Tabla 8.

Ventajas y desventajas de la norma ISO 22313.

Ventajas	Desventajas
Proporciona directrices basadas en buenas prácticas internacionales. Elabora un SGCN[2] basado en las necesidades y requisitos propios de la empresa. Es genérica y aplicable a cualquier tipo de organización.	No evalúa la capacidad de una organización para cumplir las necesidades de continuidad del negocio. No considera las necesidades legales, reglamentarias o necesidades de los clientes o terceros.

Fuente: (Servicio Ecuatoriano de Normalización - INEN, 2017)

Fases. La norma identifica las siguientes fases:

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

[2] Sistema de Gestión de la Continuidad del Negocio

1.4.2. Norma ISO 22317

Esta normativa ISO es una especificación técnica diseñada para orientar, implementar y mantener un BIA o análisis de impacto de negocio. Lo que ayuda a las organizaciones a generar conocimiento sobre todos los procesos e identificar todos los requisitos que aseguren la continuidad frente a cualquier situación como lo indica (Estruga, 2021). La norma no permite que las empresas puedan certificar el BIA, ya que se orienta simplemente a que el proceso se cumpla.

De esta forma se establece métodos, herramientas y técnicas que permiten que el proceso para la generación del BIA se cumpla de acuerdo con la norma establecida, ayudando a que los requisitos tanto legales, regulatorios y contractuales aumenten la capacidad.

Esta norma detalla el proceso de elaboración del BIA de la siguiente forma:

- Pre-requisitos.
- Elaboración del BIA.
- Revisión y seguimiento.

1.4.3. Norma ISO 22318

De acuerdo con (British Standards Institution - BSI Group, 2022b), la norma proporciona información y orientación necesaria para establecer un SGCN enfocado principalmente en el suministro de productos y servicios que una empresa necesita tomando en cuenta el proceso de cadena de suministros, ya que la producción depende directamente de los insumos que disponga la empresa.

Esta normativa ayuda a que las organizaciones tengan buenas prácticas para minimizar el impacto si falla la cadena de suministros y establece las pautas de recuperación de la actividad.

Ventajas y desventajas. Dentro de esta norma se logra un mayor nivel de satisfacción de los clientes y proveedores; lo que beneficia la reducción de riesgos operacionales, y ayuda en el mejoramiento de la gestión de las interrupciones.

Como principal desventaja no analiza otras áreas que no se vinculen a las cadenas de suministro dejando varias áreas sin procedimientos de gestión que se pudiesen aplicar.

Fases.

- Análisis de la cadena de suministro.
- Estrategias de gestión de los riesgos de la cadena de suministro.
- Gestión de la interrupción de la cadena de suministro.

1.4.4. Norma ISO 22320

La norma internacional busca que las empresas, privada o pública, mejoren su capacidad de respuesta ante las posibles emergencias, sin importar la dimensión que se presente; ya sea este local o supranacional, así se garantiza que la gestión de las emergencias se aplique según buenas prácticas.

Además, la aplicación de mando y control dentro de las estructuras organizativas y procedimientos ayuda a la toma de decisiones, trazabilidad y adecuada gestión de la información entre las diferentes organizaciones implicadas el proceso.

Dentro de este ámbito se puede determinar según la Tabla 9.

Tabla 9.

Ventajas y desventajas de la norma ISO 22320.

Ventajas	Desventajas
Establece una estructura, un proceso de mando y control. Define los procesos de gestión de la información operativa. Establece requisitos de cooperación y coordinación de las distintas organizaciones implicadas. Ayuda a garantizar la información oportuna, relevante, precisa y operaciones por procesos.	Tiene como finalidad el ciudadano. Se ejecuta en planes o siniestros naturales.

Fases. Entre las fases que se encuentran en la norma, se ejecutan las siguientes actividades:

- Sistema de comando y control.
- Coordinación interna: Sistema de comando incidente.
- Coordinación interinstitucional: mando conjunto.

1.4.5. Norma ISO 22398

Como lo explica (Estruga, 2021), es un estándar internacional que recoge las buenas prácticas y directrices para la mejora de los programas de ejercicios de cualquier organización. De esta manera se enfoca en identificar las posibles deficiencias y buscar estrategias de mejora y recuperación, asegurando la continuidad del negocio.

Es aplicable a todas las organizaciones, independientemente del tipo, tamaño o naturaleza, ya sea privada o pública. La orientación puede ser adaptada a las necesidades, objetivos, recursos y restricciones de la organización.

Puede ser utilizado por cualquier persona con la responsabilidad de garantizar la competencia del personal de la organización, en particular los líderes de la organización, y aquellos responsables de la gestión de los programas de ejercicios y los planes de ejercicio.

1.4.6. Norma ISO 22399

Esta norma se enfoca en el código de práctica relacionada con la continuidad del negocio para las empresas que desarrollan su propio criterio de desempeño específico, lo que aprueba preparar los incidentes enfocada a la continuidad operacional y medir la capacidad de recuperación que la empresa puede tener.

Se puede determinar según la Tabla 10.

Tabla 10.

Ventajas y desventajas de la norma ISO 22399.

Ventajas	Desventajas
Permite desarrollar sus propios criterios de acción específicos para la preparación de antecedentes tanto en incidentes y continuidad operacional. Diseño de un sistema de gestión de manera adecuado. Provee una base de conocimiento, desarrollo y aplicación de la continuidad de las operaciones lo que permite a la empresa medir una resiliencia de manera consistente y reconocida.	Se enfoca en la prevención o preparación ante una incidencia. Se requiere de mayor esfuerzo en la planificación y en el control de los procesos.

Fases. Las fases que se pueden encontrar dentro de este marco de desarrollo son:

- Definir el marco de trabajo.
- Análisis de impacto de negocio.
- Enfoque de diseño de plan.
- Entrega del plan.
- Pruebas del plan.
- Mantenimiento del plan.

1.4.7. Norma ISO 22301

Es un estándar internacional vinculado a la continuidad del negocio, la cual se basaba en la norma británica BS 25999 proporcionando una línea base que gestionan las operaciones del negocio basándose en el supuesto caso de producirse una irrupción o un desastre, logrando medidas que permitan la continuidad del negocio (Bevan, 2019).

La empresa mantiene medidas o políticas que atenúen las interrupciones, apoyando a la empresa a comprender la magnitud y el tipo de impacto que se genera según la amplitud definida para la necesidad o irrupción.

Entre las principales cláusulas que se pueden tomar en cuenta para el desarrollo del plan de continuidad, se puede observar la Tabla 11:

Tabla 11.

Fases del plan de continuidad del negocio.

Cláusula	Descripción	Observación
Determinación del alcance.	Alcance del BCP.	Definir las áreas.
	Política y objetivos.	Determinar el qué y cómo se desea lograr el cumplimiento de las metas.
Análisis de la organización.	Recopilación de la situación actual.	Información relevante y actualizada.
	Análisis de impacto del negocio (BIA).	Definir los procesos críticos.
	Análisis de riesgo.	Definir los activos críticos.
Determinación de estrategias y planes de continuidad.	Estrategias de continuidad de negocio.	Determinar las estrategias y planes ante incidentes.
Prueba, mantenimiento y revisión.	Planes de prueba y revisión.	Detallar actividades a ejecutarse y responsables.
	Plan de mantenimiento.	Determinar la periodicidad de las revisiones.
Capacitación y concienciación.	Plan de capacitación y concientización.	Describir las necesidades sobre la capacitación al personal.

Fuente: (Zapata Vásquez, 2020)

Una vez descritas varias normas internacionales relacionadas con la continuidad de negocio, en la Tabla 12 se trabajó un cuadro comparativo con parámetros técnicos para seleccionar la norma a trabajarse.

Tabla 12.

Cuadro comparativo de parámetros técnicos de las normas internacionales.

NORMA TÉCNICA/ PARÁMETROS	ISO 22313	ISO 22317	ISO 22318	ISO 22320	ISO 22398	ISO 22399	ISO 22301
Ciclo PDCA	x					x	x
Alcance		x			x	x	x
Referencia	x		x			x	x
Términos y definiciones		x		x	x		x
Sistema de Gestión de Continuidad del negocio	x	x					x
Liderazgo	x		x	x		x	x
Planificación	x	x	x	x		x	x
Riesgo					x	x	x
BIA		x			x	x	x
Soporte	x		x	x			x
Operación	x		x	x		x	x
Identificación de recursos			x	x	x	x	x
Roles y responsabilidades		x				x	x
Plan de Continuidad			x		x		x
Evaluación	x			x		x	x
Pruebas	x	x		x		x	x
Auditoría			x		x	x	x
Mejora Continua	x	x		x		x	x

En base a la tabla anterior, se obtiene que las normas ISO 22399, 22313 y 22398 pueden ser usadas como complementos para la implementación de la norma ISO22301; la norma ISO 22318 y 22320 son aplicables en diferentes campos de acción y la norma ISO 22317 solo trabaja con uno de los elementos considerados dentro de la norma ISO 22301.

La norma ISO 22301 cumple con los parámetros técnicos analizados, permitiendo aplicar cada fase para desarrollar un plan continuidad del negocio, ya que considera todos los servicios, activos y procesos que la organización desarrolla para generar valor de los productos.

Además, provee un marco referencial en términos de recuperación ante desastres y asegura que la organización cuente con los procesos y procedimientos correctos para restaurar los datos críticos de los clientes (British Standards Institution - BSI Group, 2019), en la identificación de amenazas potenciales y sus posibles impactos para la organización (International Dynamic Advisors - INTEDYA, 2020).

Dentro de la norma ISO 22301:2019 se encuentran 10 cláusulas principales, los mismos que instauran condiciones y sus respectivas medidas para su cumplimiento, además de cómo gestionar la continuidad de las operaciones y funciones dentro de la organización.

A continuación, se aprecia cómo está organizada la norma (Bevan, 2019).

- **Alcance:** dentro de la primera cláusula se determina el propósito y requisitos que la organización debe tener para que se encuentre "conforme" la norma y la certificación.
- **Referencias normativas:** se establece antecedentes referentes a normas vinculadas a determinar si la organización cumple o no con la norma ISO 22301:2019.
- **Términos y condiciones:** la cláusula establece cerca de 31 términos y definiciones propias de la norma ISO 22301, de acuerdo con la siguiente tabla, véase Tabla 13:

Tabla 13.

Términos y definiciones de la norma ISO 22301

Términos	Definición
Continuidad de negocio	Capacidad de una organización para continuar la entrega de productos o servicios a niveles predefinidos y aceptables tras una interrupción.
Plan de continuidad del negocio	Procedimientos documentados que guían a una organización para responder, recuperarse, reanudar y restablecerse a un nivel de operación predefinido tras una interrupción.
Periodo máximo tolerable de interrupción (MTPD)	Tiempo para que los impactos adversos, que pueden surgir como resultado de no proporcionar un producto/servicio o realizar una actividad, se vuelvan inaceptables.
Requisitos mínimos de continuidad de negocio (MBCO)	Nivel mínimo de servicios y /o productos aceptables para una organización con el fin de lograr sus objetivos comerciales durante una interrupción.
Objetivo de punto de recuperación (RPO)	Punto en el que la información utilizada por una actividad puede restaurarse para permitir que la actividad se reanude.
Objetivo de tiempo de recuperación (RTO)	Período de tiempo tras un incidente dentro del cual se reanuda un producto, servicio o actividad o se recuperan recursos.

Fuente: (International Organization for Standardization - ISO, 2019)

- **Contexto de la organización:** se realiza un análisis propio del negocio para generar un conocimiento acerca de servicios y productos que la empresa tiene, se aplica la encuesta y entrevista para conocer los siguientes aspectos de la organización.
    - Contexto interno: Para tener una idea sobre los problemas internos se debe considerar: madurez, cultura organizacional, dependencia, gestión, tamaño y madurez de los recursos, coherencia y equipo.
    - Contexto externo: Se debe efectuar un análisis acerca de los aspectos externos con el que se relaciona la empresa como son: propietarios/accionistas, proveedores, reguladores/organismos de control, factores económicos/políticos, dependencias, consideraciones ambientales y clientes.

- Partes interesadas: Se debe considerar a todas las personas afectadas por su SGCN. Dentro del análisis exhaustivo se procesan los problemas internos y externos, pueden extenderse al público y al medioambiente, según su negocio.

- **Legal y regulatorio**: Identificar y mantener actualizado de acuerdo con los requisitos legales y reglamentarios afines con la continuidad de sus productos y servicios, actividades y recursos a implementar y mantener su SGCN.
- **Liderazgo:** se refiere a una participación del proceso de establecimiento, implementación y disposición de los recursos, por lo que la gerencia es la principal implicada dentro de la quinta cláusula.

  Para generar políticas de continuidad de negocio es imprescindible definir roles y responsabilidades alineadas con una dirección estratégica a los procesos comerciales y recursos. De igual manera, se busca que se logren subpolíticas que permitan cubrir procesos y actividades prioritarias.
- **Planificación:** dentro de esta se toma como precedente el contexto de la organización y el alcance del SGCN, buscando determinar los riesgos y oportunidades para lo que se aborda prevenir o reducir los efectos no deseados y lograr una mejora continua.

  Los principales hitos que se pueden encontrar dentro de esta etapa se pueden conocer durante esta fase, véase la Tabla 14.

Tabla 14.

Fases de planificación.

Gestión de riesgos y oportunidades	Objetivos de continuidad de negocio	Consecución de objetivos	Cambios en el SGCN
Identificar acciones para abordar riesgos y oportunidades.	Ser consistentes con la política de continuidad de negocio.	Que debe hacerse Los recursos necesarios	El propósito del cambio y sus posibles consecuencias.
	Ser medibles.		
Implementar las acciones		Quién es responsable	La integridad del SGCN
	Tener en cuenta los requisitos aplicables	La fecha de consecución.	La disponibilidad de recursos.
Evaluar la efectividad de estas acciones	Estar comunicados.	Como se evalúan los resultados	
			La reasignación de responsabilidades y autoridades.
	Estar controlados y actualizados según corresponda.		

Fuente: (Programa de las Naciones Unidas para el Desarrollo - PNUD & Ministerio de Industria Comercio y Mipymes - MICM, 2020)

- **Soporte:** se describe a los recursos de personal, de infraestructura y medioambientales (recursos físicos, materiales, herramientas, etc.), no solamente se toman en cuenta los internos sino también los externos tanto de proveedores como socios.

  Un recurso para ser usado dentro del SGCN debe cumplir con lo siguiente:

  - Ser capaz si este se refiere a equipo o infraestructura.
  - En el caso de ser recurso humano este debe ser competente.
  - Y si el caso fuese referente a suministros deben ser suficientes.

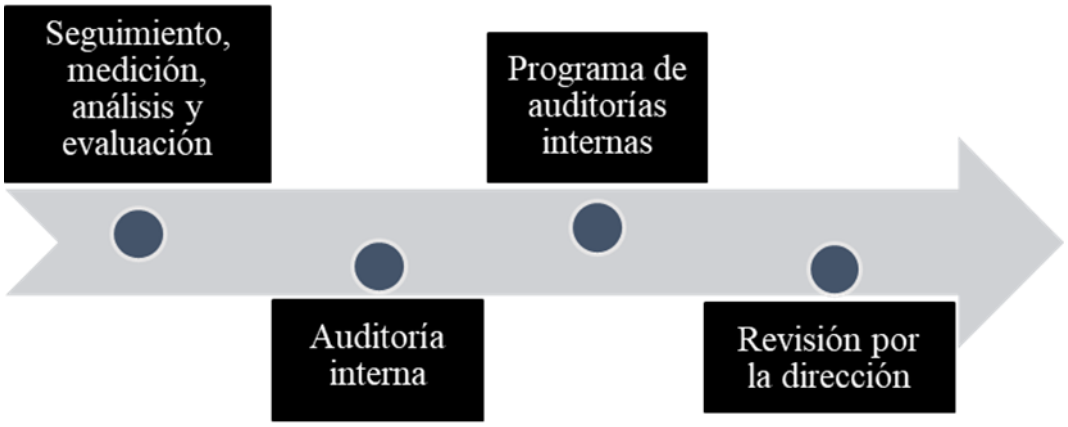
- **Operación:** este paso se debe ejercer una vez finalizado las cláusulas de planificación y evaluación de riesgos, ya que se implementa y se controla las acciones y procesos previamente identificados.

Se definen un responsable que garantizará la identificación sistemática de los riesgos, ejercer una comunicación efectiva del conjunto de actividades para la gestión de riesgos, asignación clara de responsabilidad y de recursos en el momento adecuado y una evaluación rutinaria que colabora con la eficacia de la gestión de los riesgos.

- **Evaluación del desempeño**: toda organización debe establecer parámetros referenciales que le permitan conocer los resultados previstos de los procesos. Dicho proceso se puede representar en la Figura 6.

Figura 6.

Proceso de evaluación del desempeño



Fuente: (Bevan, 2019)

- **Mejora:** el proceso de implementación busca que la organización tenga las herramientas de responder una disrupción de manera oportuna y completamente calificada para los productos y servicios para un nivel definitivo hasta lograr una normalidad operativa. Se determina las oportunidades que permitan la mejora e implementación de acciones.

Para la evaluación de la gestión de continuidad del negocio, se contemplará una evaluación que permita conocer el estado inicial para cumplir las cláusulas en la norma ISO 22301, para lo que se analizan estos puntos a considerarse criterios de valoración. Véase Tabla 15.

Tabla 15.

Criterios de valoración.

Descripción	Ponderación	Calificación
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 0 y 1	En preparación
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 1,1 y 2	Básico
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 2,1 y 3	Establecido
El SGCN cumple con los requerimientos de la norma ISO 22301, esto permite iniciar con la certificación a mediano plazo.	Entre 3,1 y 4	Administrado
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.	Entre 4,1 y 5	Optimizado

1.5. Modelo PDCA (PLAN-DO-CHECK-ACT) o PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR)

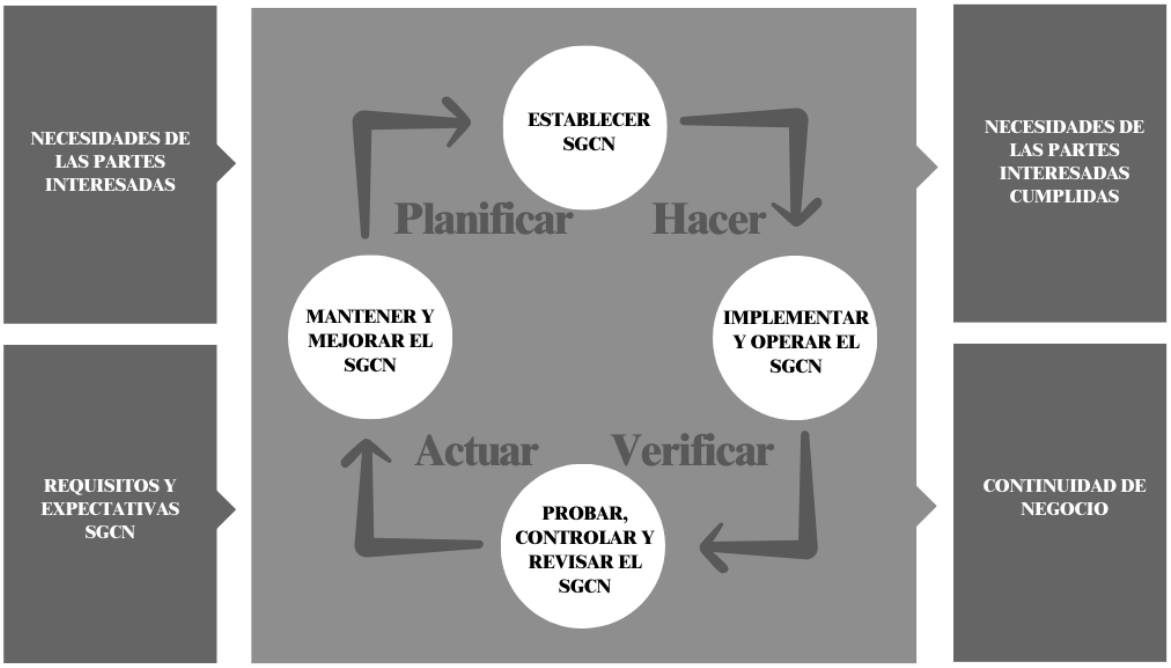
Según (Pinto et al., 2022), la norma ISO 22301 trabaja con el modelo PDCA o también conocido como circulo *Deming* o *Shewhart*, el cual fue diseñado por Walter Shewart; presenta 4 fases muy bien marcadas permitiendo que el ciclo pueda ser aplicado; ya sea a un todo o de manera específica a cada elemento, logrando una mejora continua.

Cuando se aplica el modelo durante la implementación, si los resultados no son los esperados, se realiza una nueva evaluación y se reinicia el ciclo para el proceso, para que se pueda trabajar en el mejoramiento continuo de empresas o proyectos.

El ciclo es circular como se observa en la Figura 7.

Figura 7.

PHVA modelo ISO 22301



Fuente:(International Organization for Standardization - ISO, 2019)

Al tener un desarrollo circular cada fase permite una interacción con la anterior obteniendo resultados que alimenta a la próxima, a continuación, se presenta dentro de la Tabla 16 un análisis de cada una de ellas.

Tabla 16.

Fases del PDCA

Fase	Descripción
I: Plan	Se establecen políticas, objetivos, metas, controles, procesos y procedimientos directamente con los implicados en cada proceso y las personas participan informando sobre los problemas presentados y los retos diarios, así como de esta forma se genera investigación y recopilación de datos enfocados en la búsqueda de una solución.
II: Do	Se trabaja medidas que permitan solventar los problemas anteriormente definidos en la planificación, para dichas soluciones se busca la aplicación de políticas.

III: Check	Análisis de valoración de los resultados obtenidos una vez aplicada la fase anterior obteniendo datos que permitirán conocer la eficiencia de los procesos anteriormente definidos.
IV: Act	Se archivan los resultados obtenidos y se busca ejecutar medidas correctivas con los resultados anteriores y lograr una correcta revisión de la gestión.

Fuente: (Saxena & Srinivas Rao, 2019)

(Lampe, 2020) refiere esto, la norma ISO 22301 nos da una visión particular sobre la gestión de riesgos, caracterizada por su amplio desarrollo en temas como análisis de impacto en el negocio, estrategias de continuidad del negocio, soluciones y evaluación de riesgos.

1.6. Análisis BIA o Business Impact Analysis

Un BIA de acuerdo con (International Organization for Standardization - ISO, 2019), es un proceso de análisis del impacto en el tiempo de una interrupción en la organización, por este motivo es fundamental dentro del PCN.

Como se menciona, se analiza los procesos misionales y servicios de la empresa para garantizar una métrica de la magnitud del impacto operacional o financiero durante la incidencia en el proceso.

Por ende, el análisis de impacto al negocio debe cumplir ciertos requerimientos:

- Conocer las funciones y procesos que permitan la supervivencia de la empresa al momento que se ejecute la interrupción, analizando los procesos claves para que la operación se inicie dándole mayor prioridad posible, frente a aquellos que tenga una menor prioridad.
- Realizar una verificación de los posibles efectos negativos ya sea de operación o económico conociendo lo que una interrupción puede provocar en los procesos de alta prioridad.

- Estimar los tiempos de recuperación considerando las posibles afectaciones que se produzcan en el proceso de alta prioridad para el correcto funcionamiento de la organización.

Por ende, la fase entrega un documento que detallada las funciones y los procesos que se consideren críticos, tomando en cuenta la información básica, recursos requeridos y tiempos de recuperación (Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC & Vive Digital Colombia, 2015).

Figura 8.

Proceso del análisis de impacto del negocio.

Fuente: (Instituto Nacional de Ciberseguridad, 2020)

En la Figura 8 se observan los procesos del análisis de impacto del negocio, así se obtiene un proceso que permite generar un marco de referencia de los principales riesgos que se puedan generar y sus posibles impactos, las operaciones críticas para priorizar los procesos de recuperación, así se usa un esquema de valoración visualizado en la siguiente Tabla 17.

Tabla 17.

Valoración del impacto.

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

En el análisis se considera la priorización en la recuperación de los procesos, en los que se desarrolla el análisis BIA, que pueden evaluarse según la Tabla 18.

Tabla 18.

Valoración priorización de recuperación de procesos.

Prioridad de recuperación	MTD en días	MTD en horas
1	0.5 – 1	12 – 24
2	1 – 2	24 – 48
3	2 – 3	48 – 72
4	3 – 4	72 – 96

1.7. Metodología de Análisis y Gestión de Riesgos

La parte esencial dentro del proceso de seguridad es aplicar el análisis y la gestión de riesgos por esta razón se debe mantener actualizado, ya que permite tener un mantenimiento controlando, una reducción en el nivel de los riesgos aceptados, estableciendo un equilibrio entre los datos y los tratamientos (Maldonado Mariño, 2013).

Por lo que el estudio de una metodología de análisis y gestión de riesgos permite que se aplique un proceso sistemático, estableciendo procedimientos que ayudan a estimar la magnitud de riesgos que la organización puede tener, de esta manera se selecciona e implanta el salvaguardar y controlar riesgos identificados.

1.7.1. Metodología MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información) es una metodología que toma como referencia los criterios del *Information Technologies Security Evaluation Criteria* (ITSEC), la metodología se relaciona con la generalización del uso de las tecnologías de la información, por ende, analiza el impacto que se puede presentar en la organización (Allaico Chimborazo, 2021).

Fases. La metodología como se observa en la Figura 9 se divide en cinco pasos, los cuales son: determinación de activos donde se realiza un reconocimiento de los insumos y personal; determinación de las amenazas conoce las dimensiones de la organización como son: confidencialidad, trazabilidad, integridad, autenticidad y disponibilidad, así como el realizar la determinación de riesgo y salvaguardas de esta manera se logra determinar el riesgo residual.

Figura 9.

Fases metodología MAGERIT.

Fuente: (Avila Torres & Cuenca Tapia, 2021)

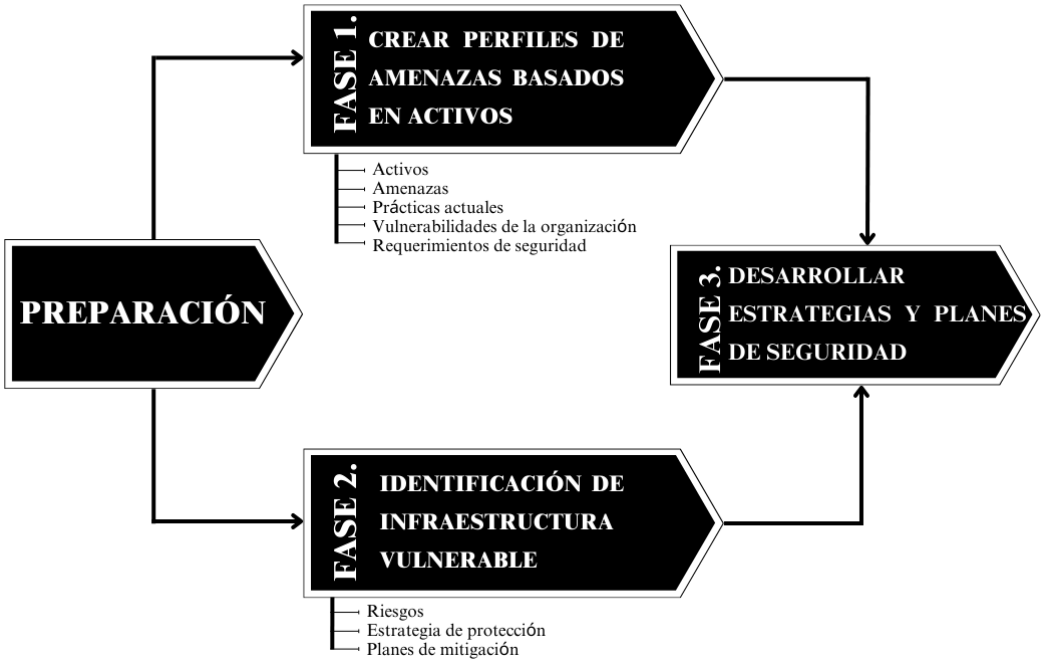
1.7.2. Metodología OCTAVE

Según (Pacheco Fernández et al., 2021), OCTAVE (*Operationally Critical Threat Asset, and Vulnerability Evaluation*) es una metodología de evaluación de riesgos desarrollada por el *Software Engineering Institute (SEI*) en Estados Unidos, que busca cubrir los riesgos operacionales y prácticas de seguridad. Se implementa para organizaciones que superan los 300 empleados.

Fases. Los procesos y actividades elaboran una vista detallada de las necesidades de seguridad de una organización. Su objetivo se enfoca al riesgo y no se basa en la tecnología, las cuatro fases ayudan en el desarrollo de la metodología se representa en la Figura 10.

Figura 10.

Fases metodología OCTAVE.



Fuente: (Pacheco Fernández et al., 2021)

En la preparación se organiza los detalles que se van a trabajar, en la fase 1 permite desarrollar los perfiles de las amenazas que se basan en los activos: identificando bienes, amenazas,

prácticas, vulnerabilidades y recursos de seguridad. La fase 2 identifica las vulnerabilidades en la infraestructura, busca los principales componentes y con ello sus vulnerabilidades técnicas y, finalmente la fase 3 ayuda a desarrollar estrategias y planes de seguridad que se basan en los riesgos, la estrategia de la protección y los planes de mitigación.

1.7.3. Metodología CRAMM

De acuerdo con la opinión de (Crespo Martínez & Cordero Torres, 2015), CRAMM (*CCTA Risk Analysis and Management Method*) es una metodología destinada a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y sus activos; además busca el análisis y la gestión de riesgos la cual puede ser aplicable en todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad; donde el alto nivel del riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones.

Fases. Durante la fase 1 se busca recoger y definir los objetivos de seguridad, en la fase 2 se realiza análisis de riesgos y su identificación y en la fase 3 se realiza una identificación y selección de medidas de seguridad para lo cual CRAMM proporciona una librería con acerca 3000 medidas de seguridad, se puede ver todo este proceso en la Figura 11.

Figura 11.

Fases metodología CRAMM.

Fuente: (Sánchez Contreras, 2015)

1.7.4. Metodología MEHARI

La metodología de análisis y gestión de riesgos MEHARI (Método Armonizado de Análisis de Riesgos) desarrollada por *Club de la Sécurité de l'Information Français* (CLUSIF) en 1995 y deriva de las metodologías previas Melissa y Marion (Huerta, 2012), proporciona una guía de implantación de la seguridad de la entidad en el área de seguridad informática.

Fases. La metodología consta de tres fases: valoración de los riesgos en la que se identifican se estima y evalúa los riesgos; tratamiento de los riesgos descritos y gestión de los riesgos para lo que se aplican planes de acción, implementación y monitoreo y revisión, véase la Figura 12.

Figura 12.

Fases metodología MEHARI

Fuente: (Cardinault, 2018; Marcillo Baque, 2017)

Dentro del proceso de investigación de las metodologías de Análisis y Gestión de Riesgos se elabora una tabla comparativa que contiene parámetros de evaluación que permitió la selección de la metodología a trabajarse, como se detalla en la Tabla 19.

Tabla 19.

Tabla comparativa de los parámetros de las metodologías para el Análisis y Gestión de Riesgos.

Metodología	Tipo de análisis		Activo			Amenaza			Vulnerabilidad			Salvaguarda			Riesgos
	Cualitativo	Cuantitativo	Forma de caracterizar	Valoración	Procedimiento	Forma de caracterizar	Valoración	Procedimiento	Forma de caracterizar	Valoración	Procedimiento	Forma de caracterizar	Valoración	Procedimiento	
MAGERIT	x	x	x	x		x	x					x	x		Los riesgos se estiman e interpretan los resultados
OCTAVE	x	x	x			x			x						Se desarrolla estrategias, planes y una

									lista de acciones
CRAMM	Opcional		x	x		x		x	No se analiza
MEHARI	x	x		x		x		x	Retención, reducción de riesgos, así como evitar y transferir el mismo

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), es una metodología de carácter público, es decir, su uso es libre y no se requiere autorización previa del mismo, está enfocado en el análisis y gestión de los riesgos permitiendo adaptarse a cualquier tipo de organización, sistemas informáticos y servicios tecnológicos.

Dentro de las etapas que se desarrollan para el proceso de metodología de MAGERIT tenemos:

- Análisis de riesgos.
- Caracterización de los activos.
- Caracterización de las amenazas.
- Caracterización de salvaguardas.
- Estimación del estado del riesgo.
- Gestión de los riesgos.

Para la correcta implementación se debe considerar el manejo de una herramienta que permite automatizar el proceso de análisis de riesgos como es el Entorno de Análisis de Riesgos/Procedimiento Informático – Lógico para el Análisis de Riesgos o sus siglas EAR/PILAR.

Como lo indica (Ministerio de Hacienda y Administración Públicas, 2012) es una herramienta que apoya el proceso de gestión de riesgos de los sistemas de información en largos

periodos para lo cual se basa en la metodología MAGERIT RA/RM, permitiendo que esta vaya cambiando de acuerdo con la mejora de las salvaguardas que se implementen como son:

- Análisis y gestión de riesgos tanto cuantitativa o cualitativamente.
- Análisis cuantitativo o cualitativo de impacto en la organización, así como la continuidad de las operaciones.

Entre los beneficios que se podrían detallar seria:

- Es intuitivo.
- Proporciona la ejecución de cálculos rápidos.
- Genera reportes de texto y gráficos.

1.8. Riesgos Tecnológicos

De acuerdo con la (Real Academia Española - RAE, 2023), se considera como riesgo a toda contingencia o proximidad de un daño, de esta manera se podría definir que es todo aquello que puede producir ciertos fallos o problemas y que genere una vulnerabilidad.

Tomando en cuenta que el término tecnológico hace referencia a todo el ámbito de tecnología, para dicho proceso se analiza todas las operaciones que tienen una automatización en parte de sus actividades o toda la actividad al aplicar medios tecnológicos ayudando a la reducción de costos de recursos físicos, estructurales y humanos (Agbodoh-Falschau & Ravaonorohanta, 2023).

Todos los sistemas actualmente tecnológicos permiten que se realicen consultas en tiempo real de información, la gestión de actividades y tareas, además de manejar la información financiera e interacciones con entidades públicas (IESS, SRI, etc.), como privadas (bancos) asociados a la misma.

Debe considerarse que todo uso de tecnología es ventajoso, ya que aprovecha la mayor capacidad que pueda ofrecer la empresa, y una incorrecta implementación pueden provocar que esta sea considerada una pérdida y no contribuya a la continuidad del negocio.

Para lo cual se definirán dos tipos de riesgos que son:

- Riesgos internos: ponen en peligro la conservación de la información y la comunicación entre las áreas de la empresa a nivel interno, para lo que se evaluarán los activos y se definirán claramente si esa información se mantendrá en la empresa o se necesitarán medios digitales externos para conservarlo.
- Riesgos externos: se considera externos a los servicios suministrados por proveedores externos a la empresa, como servicio de internet, gestión de información, etc. Su nivel de criticidad será mayor y se deberá llevar de otra manera, ya que varios de estos continúan a otros servicios.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves y el ciberterrorismo han mostrado la necesidad de incorporar nuevas amenazas en la continuidad de negocio. Para garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en el tipo de riesgos al que se expone.

Según (British Standards Institution - BSI Group, 2022b), las fallas debido a problemas derivados del nuevo modo de trabajo se encuentran en el primer lugar, le siguen los incidentes de seguridad; en el 2021, las interrupciones de TI y telecomunicaciones se encuentran en tercer lugar, se puede tener más información, en la Tabla. 20, se presentan los resultados completos de la encuesta tanto para el año 2021.

Tabla 20.

Frecuencia que se han producido los sucesos y niveles de impacto año 2021.

Evento	Frecuencia	Impacto	Índice de riesgo
(Problemas derivados del) trabajo a distancia/nuevo entorno de trabajo	11.4	2.1	24.3
Incidente de seguridad (daños personales, víctimas mortales, daños peligrosos, incidente notificable)	7.8	1.9	14.5
Interrupción de TI y telecomunicaciones	6.1	2	12.3
Ciberataque y violación de datos	6	2	11.7
Cambios reglamentarios	5.2	2.1	10.9
Introducción de nuevas tecnologías (*IoT, IA, Big data*)	4.4	1.9	8.4

Fuente: (British Standards Institution - BSI Group, 2022a)

En la Tabla 21, se puede observar que hubo ciertos cambios con respecto a los eventos durante el año 2022, en la cual los eventos referentes al ciberataque y violación de datos se encuentran en primer lugar, en segunda posición se encuentra los problemas derivados del trabajo a distancia/nuevo entorno de trabajo y en tercer lugar se encuentra las interrupciones de TI y telecomunicaciones.

Tabla 21.

Frecuencia que se han producido los sucesos y niveles de impacto año 2022.

Evento	Probabilidad	Impacto	Puntuación de riesgo
Ciberataque y violación de datos	3.1	2.2	6.9
(Problemas derivados del) trabajo a distancia/nuevo entorno de trabajo	3.6	1.4	5
Interrupción de TI y telecomunicaciones	2.9	1.7	4.9
Introducción de nuevas tecnologías (IoT, IA, Big data)	2.7	1.5	4.1
Incidente de seguridad (daños personales, víctimas mortales, daños peligrosos, incidente notificable	2.4	1.6	3.8
Cambios reglamentarios	2.5	1.4	3.5

Fuente: (British Standards Institution - BSI Group, 2022a)

1.9. Repositorios Digitales

Un repositorio digital, de acuerdo con (Rivera Gómez, 2009) señala que “los repositorios son sitios en donde se almacena y resguarda información de forma centralizada y son accedidos principalmente desde redes informáticas o de internet”, dicha definición anterior es un poco general.

Como lo define (Fierro Saltos et al., 2018) definen a los repositorios digitales como “un depósito de documentos digitales, cuyo propósito es gestionar, organizar, almacenar, preservar y difundir en acceso abierto la producción administrativa, científica y/o académica resultante de las actividades de una institución u organización”.

De acuerdo con el contexto anteriormente tratado se podría definir que un repositorio digital es aquella plataforma digital en la que se centra toda la información generada ya sea académica, científica o de carácter legal por parte de una institución, pueden ser agrupados de acuerdo con el contenido siendo estos: institucionales, temáticos, de datos, de eprints, de objetos de aprendizaje, huérfanos y agregados/recolectores creando colecciones.

Los repositorios digitales dentro de su almacenamiento pueden tener diferentes tipos de documentos o información, los cuales pueden ser:

- Científicos: en este segmento se consideran los documentos generados de investigaciones de pregrado y posgrado, usados por instituciones educativas o publicas vinculadas a la educación.
- Institucionales y/o Administrativas: se clasifican las revistas, reglamentos, normas, documentos de trabajo, informes técnicos y todo aquel material que se haya generado en las instituciones.

- Objetos de aprendizaje: referencia a las guías de estudio, ejercicios, material audiovisual, así como a simuladores, presentaciones académicas, pruebas en línea y laboratorio, todo lo que se pueda usar como material para actividades académicas.

A continuación, se describe un listado de repositorios digitales haciendo énfasis en la perspectiva de manejo de la información. En la Tabla 22, se muestra un resumen de estos repositorios.

Tabla 22.

Tipos de repositorios digitales.

Repositorio Digital	Definición
Dspace	Es un software de código abierto que provee herramientas para la administración de colecciones digitales, el uso más común es la creación de repositorios institucionales.
Eprints	Es utilizado para la creación de repositorios y es compatible con el protocolo *Open Archives Initiative* (OAI) para la recolección de metadatos.
WordPress	Es un código abierto que se puede utilizar como plataforma para un repositorio de objetos de aprendizaje (LOR) para crear un índice público de contenido alojado en un servidor crea un registro para cada objeto de aprendizaje que contiene metadatos sobre el formato, el contenido y la accesibilidad del objeto.
Drupal	Es un sistema de gestión de contenido dinámico en lugar de almacenar sus contenidos en archivos estáticos en el sistema de ficheros del servidor de forma fija, el contenido textual de las páginas y otras configuraciones son almacenados en una base de datos y se editan utilizando un entorno Web.
Omeka	Es un software libre, flexible y de código abierto pensado para la publicación en web de colecciones de bibliotecas digitales, archivos, museos o cualquier otra institución que desee difundir su patrimonio cultural.

Fuente: (Alcaraz Martínez, 2021; González Mendoza & Aguilar Juárez, 2015; Rodríguez Gairín & Sulé Duesa, 2008)

Para la selección del repositorio como gestor de contenido, se analizaron varios parámetros que tiene relación con los aspectos técnicos. En la Tabla 23, se muestra un cuadro comparativo en base al cumplimiento de ciertos parámetros.

Tabla 23.

Cuadro comparativo de tipos de repositorios digitales.

Repositorio	Dspace	Eprints	WordPress	Drupal	Omeka
Tipo	Gestor de repositorios	Gestor de repositorios	CMS	CMS	Gestor de colecciones
Servidor Propio	Si	Si	Si	Si	Si
Modo de explotación	Repositorio	Repositorio	Portal o sede web	Portal o sede web	Galerías
Metadatos	Dublin Core	Dublin Core	No	No	Dublin Core
Licencia GNU	Si	No	No	Si	Si
Curva de aprendizaje	Alta	Alta	Media	Alta	Baja
Multiplataforma	Si	Si	Si	No	Si

Según el cuadro comparativo anterior, se puede evidenciar que Omeka cumple con todos los parámetros necesarios para la gestión del contenido. Esta a su vez es la más apta ya que los usuarios aportarán el material a la colección, catalogando y describiendo los documentos que se almacenarán. Así se establecen relaciones entre cada documento de la colección.

1.9.1. Omeka

De acuerdo con (Peña F, 2019), una plataforma de publicación web libre, flexible y de código abierto, que permite realizar colecciones digitales y exposiciones virtuales de bibliotecas, archivos, museos o cualquier otro tipo de información. Se encuentra bajo la licencia de software libre (*GPLv3*), con lo cual su distribución, uso y modificación son libres.

Dentro de los beneficios e inconvenientes que se pueden presentar de la plataforma se puede describir en la Tabla 24.

Tabla 24.

Beneficios e inconvenientes en Omeka.

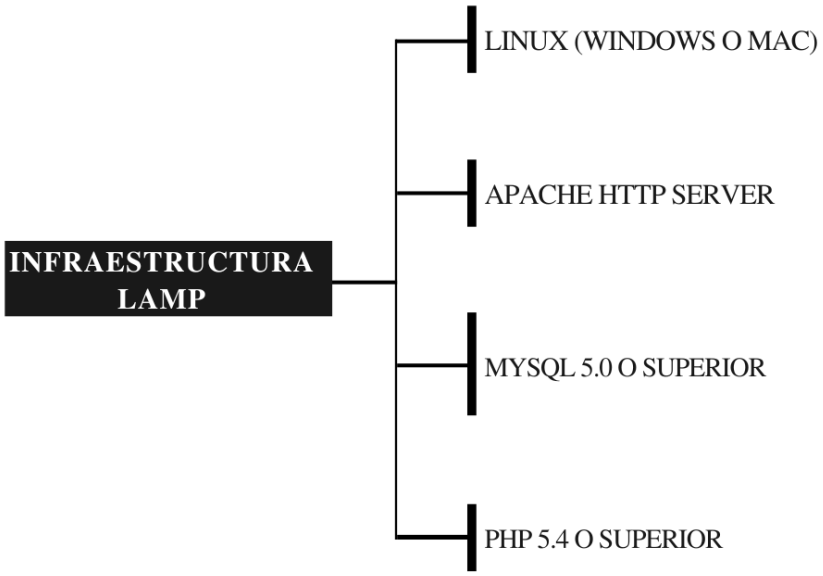
Beneficios	Inconvenientes
Galerías: se presenta la información de manera interactiva. Los tipos de ficheros son variados. Permite un trabajo de múltiples plataformas. Se puede realizar presentaciones personalizadas.	Tiene un almacenamiento limitado debido al costo. Se tiene una comunidad sesgada con desarrollos para fines muy concretos. Se tiene una capacidad limitada en la búsqueda y recuperación. No se tiene un dominio o servidor propio.

Fuente: (Aguillo, 2017)

Arquitectura de Omeka. La infraestructura que maneja es LAMP la misma que se representa de acuerdo con la Figura 13.

Figura 13.

Arquitectura de Omeka.



Fuente: (Alcaraz Martínez, 2021)

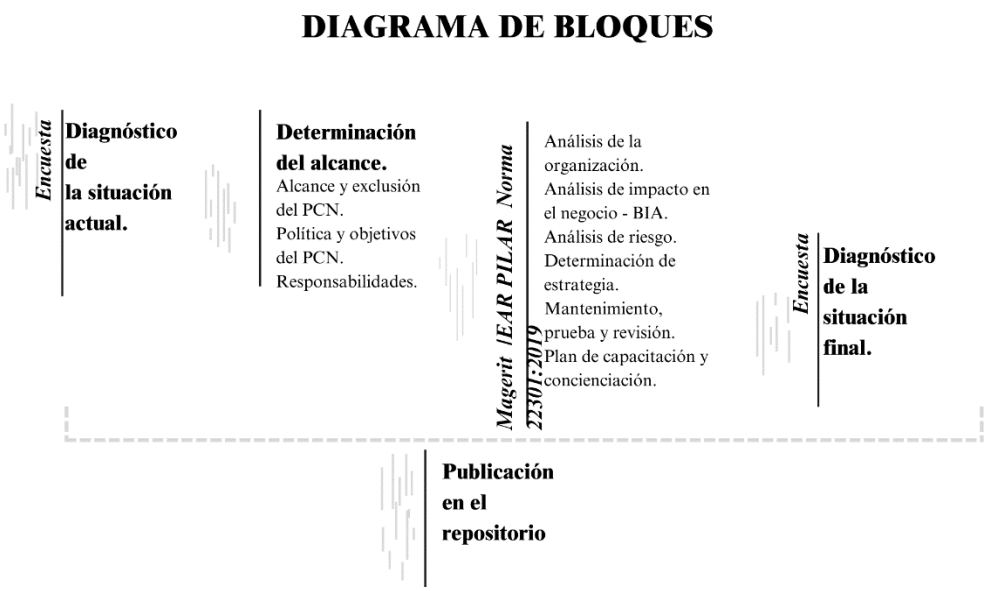
Dublin Core. (Biblioteca Universidad de Sevilla, 2017) se refiere al conjunto de metadatos que se usan para el registro de los elementos, archivos y colecciones. Cada uno de estos puede contener una o varias entradas según los siguientes parámetros: título, materia,

descripción, autor, fuente, editor, fecha, colaboración, derechos, relación, formato, idioma, tipo, identificador y cobertura.

Tras el análisis, se estructura una guía de trabajo en la que se basa el proyecto, se trabaja en cada fase para desarrollar y obtener resultados.

Figura 14.

Diagrama de bloques.



En la Figura 14 se conoce el proceso en el que se basa esta investigación. Este inicia con una evaluación de la situación actual antes de iniciar el proceso, en la determinación del alcance se definen 3 áreas importantes como: alcance - exclusión, políticas - objetivos y responsabilidades; como metodología se usa MAGERIT, la norma ISO 22301:2019 y para la recolección de datos se usan instrumentos como: encuesta y/o entrevista.

Toda la información que se genera se divulga dentro de un repositorio digital de Industrias Karmat, esto a su vez permite que se genere planes de capacitación y concientización para el personal que labora en la empresa. Y como punto final se realiza un análisis una vez implementado y evalúa uno de los procesos a desarrollarse.

CAPÍTULO II

En este capítulo se muestra la situación en que la que se encuentra actualmente la empresa Industrias Karmat, los antecedentes y demás se hace uso de herramientas que permitan conocer el impacto y las vulnerabilidades potenciales.

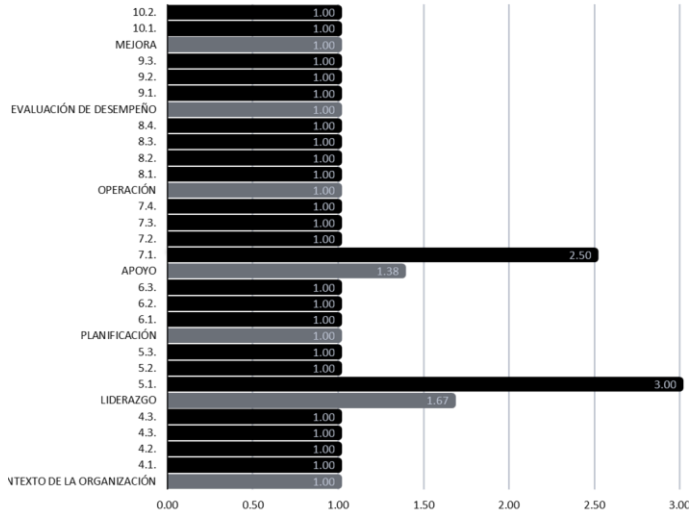
2.1. Diagnóstico de la situación actual norma ISO 22301

En el desarrollo de la norma ISO 22301 se elabora un diagnóstico, que se ejecuta según la encuesta (Anexo A), que busca analizar el nivel de gestión conforme a la continuidad del negocio para conocer la madurez de la empresa respecto a las acciones tomadas en caso de riesgos.

Para dicho proceso de evaluación se tomaron las cláusulas que conforman la norma a partir del contexto de la organización hasta mejora, se analizó cada una de las dimensiones asignándoles un valor que inicia en 1 como en preparación hasta 5 optimizado. En dicho análisis se estiman resultados promedios para lo que se representa en la Figura 15.

Figura 15.

Diagnóstico inicial según la norma ISO 22301.



Así se puede conocer el valor inicial de la madurez de la organización según la continuidad del negocio, se promedian esos valores para conocer la valoración global y esta a su vez nos sirve como punto de partida.

Tabla 25.

Valoración inicial cláusulas norma ISO 22301.

CLÁUSULA	PROMEDIO
Contexto de la organización	1.00
Liderazgo	1.67
Planificación	1.00
Apoyo	1.38
Operación	1.00
Evaluación de desempeño	1.00
Mejora	1.00
VALORACIÓN INICIAL GLOBAL	*1.15*

De acuerdo con la valoración global y en base a la Figura 15 y Tabla 25, Industrias Karmat obtiene una valoración de 1.15, el cual se representa como un nivel de preparación con respecto a la gestión de la continuidad del negocio, es decir, la empresa no cuenta con procesos de contingencias ya sean estos básicos para el manejo de los incidentes de seguridad.

De igual manera se obtuvo los comentarios de parte de la gerente general de la organización, la cual manifiesta su interés y predisposición para la implementación de un plan de continuidad y de esta manera el proyecto será de gran ayuda para el proceso de implementación del PCN para Industrias Karmat.

2.2. Determinación del alcance

En la fase uno se definirá el alcance - exclusiones, políticas - objetivos y responsabilidad que se manejarán en el plan de continuidad del negocio.

2.2.1. Alcance y exclusión del plan de continuidad del negocio

El alcance del plan de continuidad del negocio está enfocado en el desarrollo de un plan de continuidad para Industrias Karmat vinculando a todo el personal, procesos y activos críticos que conforma la organización, lo que permite una alta capacidad de reacción para los incidentes que afecten las operaciones.

El enfoque principal del plan son los servicios tecnológicos de Industrias Karmat, sin embargo, en el futuro se puede extender a los demás recursos que cuenta la organización.

2.2.2. Política y objetivos del plan de continuidad del negocio

La Gerencia de Industrias Karmat, siempre en la búsqueda de satisfacer las necesidades de los clientes y proveedores busca brindar un servicio de calidad y con esto lograr la continuidad de los principales servicios de esta, está siendo su principal razón decide contar con un plan de continuidad del negocio, el cual se adapta a las necesidades y estructura de la misma, para lo cual dicho plan debe ser correctamente documentado y socializado, así como, su alcance está relacionado a los responsables de la tarea encomendada.

La estructura del PCN se compone según la norma ISO 22301:2019, reestructurada según los requerimientos de la organización, ya que si se da o presenta un incidente que comprometa la seguridad, infraestructura o falla de aplicaciones, la aplicación del plan será obligatoria y cumpliendo los procedimientos para las tareas mencionadas.

Para mantener el PCN actualizado, se establece que los periodos de revisión se los realicen semestralmente para lo que se debe contar con todo el personal involucrado en el plan, tómese en cuenta que todas las modificaciones constan en el repositorio de la organización.

Entre los objetivos que se plantea con la implementación, la empresa busca:

- Disminuir las amenazas presentes dentro de la organización que pueden causar interrupciones operativas.
- Garantizar la continuidad en los procesos.
- Coordinar el cumplimiento de las estrategias de recuperación en los procesos críticos de Industrias Karmat.
- Entregar un servicio de calidad a los clientes cumpliendo los tiempos aceptables de recuperación.

2.2.3. Responsabilidades

Entre las responsabilidades generales se encuentran:

- El personal de la empresa es el responsable de la implementación según la política y así proporciona los recursos necesarios para su aplicación.
- Se define al Comité de Crisis con el encargado de declarar la situación de la crisis e iniciar con la ejecución del plan de continuidad.
- La gerencia general juntamente con la presidencia del comité de crisis es quienes coordinan, revisan, realizan y aprueban dichos cambios.

2.3. Análisis de la organización

Se describe los aspectos referentes a los servicios y productos de acuerdo con el análisis del negocio para lo cual se representará el contexto interno, externo y partes interesadas de la organización

Se mantienen reuniones con el personal de la organización para el levantamiento de la información, así como los activos y los procesos críticos que apoyan el desarrollo de Industrias Karmat (Anexo B). Además, se realiza una recolección de información de las aplicaciones, dependencias y recursos que se trabajan dentro de la organización.

La documentación que se utiliza se encuentra en la intranet de la empresa, además de la página web corporativa a través de la encuesta y entrevistas al personal.

2.3.1. Situación actual

Industrias Karmat es una organización que tiene como objetivo prestar los servicios de venta de productos, la matriz principal se encuentra en la ciudad de Ibarra-Ecuador, ubicada Miguel Alban Paliz 1-92 entre Ricardo Sánchez y Tobías Mena, contando con 8 trabajadores con contrato de tiempo completo y 10 con contrato de medio tiempo, siendo 18 en total.

2.3.2. Misión

Brindar una amplia gama de productos de calidad, con diseños variados, innovadores y de temporada, de acuerdo con las necesidades de los clientes a precios convenientes, a través de un grupo humano excelente, comprometidos a elaborar y entregar los productos de manera eficiente y oportuna además de generar excelentes oportunidades para personas activas, emprendedoras que

2.3.3. Visión

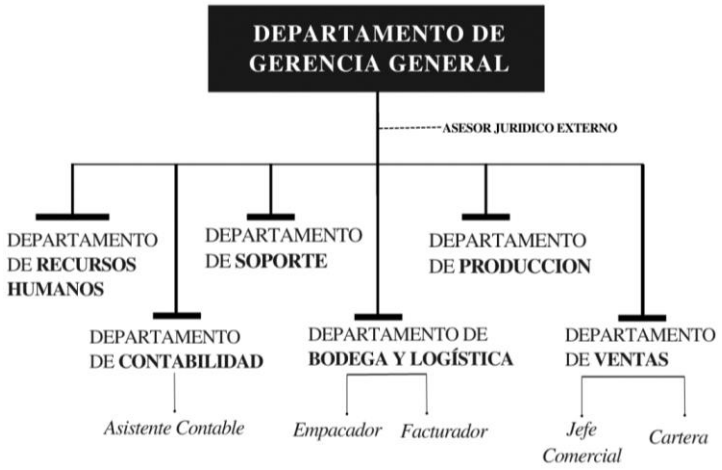
Ser una empresa líder a nivel nacional y reconocida en el mercado de la venta de productos, lograr también extendernos y crear puntos de ventas, proporcionando un servicio de calidad a nuestros clientes, compitiendo en el mercado nacional con los mejores precios.

2.3.4. Personal, equipos y servicios tecnológicos

Para el desarrollo de dicho plan de continuidad se manejará un amplio conocimiento concerniente al personal que labora en la empresa, equipos y todos aquellos servicios tecnológicos que permiten que la organización pueda ejecutar sus procesos, dicho esto dentro del personal a continuación se detalla en la Figura 16.

Figura 16.

Organigrama Industrias Karmat.



Cada departamento tiene actividades diferentes definidas durante el proceso de satisfacción del cliente, destacando que cada uno trabaja coordinadamente con la gerencia general para aprovechar al máximo los recursos.

Los equipos tecnológicos dentro de la empresa permiten la ejecución de varias de sus actividades, para lo cual el uso de los equipos es necesario para lograr la interacción, dentro de la Tabla 26, se detalla a grandes rasgos los equipos.

Tabla 26.

Equipos tecnológicos.

Cant	Descripción	Departamento
1	Central Telefónica	Producción
1	Computador Asus (Monitor, teclado, CPU)	Recursos Humanos
5	Computador Dell (Monitor, teclado, CPU)	Contabilidad - Asistente Contable - Ventas - jefe Comercial - Producción
1	Computador HP (Monitor, teclado, CPU)	Producción

7	Computador Intel (Monitor, teclado, CPU)	Soporte - Bodega y Logística - Ventas - Cartera - Producción - Facturación
1	Firewall HP	Producción
5	Impresora Matricial	Facturador
5	Impresoras Epson	Contabilidad – Soporte – Bodega y Logística – Ventas – Recursos Humanos
1	Portátil Asus	Producción
1	Portátil HP	Gerencia
1	Portátil Toshiba	Gerencia
4	Routers	Producción
1	Servidor HP	Producción
1	Switches	Producción
10	Teléfono IP Granstream	Contabilidad – Soporte – Bodega y Logística – Ventas – Recursos Humanos - jefe Comercial - Asistente Contable - Producción
2	UPS SMART	Producción

En la Tabla 27 se muestra los servicios tecnológicos que brinda Industrias Karmat por medio de su infraestructura tecnológica lo que permite el desarrollo de las actividades en las diferentes áreas de trabajo.

Tabla 27.

Servicios tecnológicos y sistemas/módulos.

Servicio Tecnológico	Descripción	Sistema/módulos
Administración de base de datos	Gestor y administrador de base de datos y procesos de extracción, transformación y carga (ETL).	Oracle
Aplicaciones empresariales	Aplicaciones propias para el apoyo del negocio.	NEGYSERT - Sistema Contable, Semiya ERP
Bot-Auto respuestas	Software de envió de mensajería masiva	Whatsappiando
Configuración de equipos de usuarios	Equipo de cómputo, desktops y laptops marca con sistema operativo	Hardware HP - Asus - Dell - Intel - Toshiba, Windows 10 – 8

Correo electrónico	Envió y recepción de mensajes de correo.	Hostinger, Hotmail
Datacenter	Centro de cómputo donde se concentran los diferentes sistemas de comunicación y servidores.	UPS, equipos de comunicaciones, servidores y firewall.
Firewall	Servidor proxy de filtrado de navegación	Linux
Gestión Hipervisor vCenter	Plataforma para control de virtualización	VMware
Infraestructura de red	Redes LAN	Cisco
Instalación de aplicaciones de proveedor	Aplicaciones de empresas externas para el apoyo al negocio	Anydesk, TeamViewer
Internet y navegación web	Navegación para acceso a internet y varias aplicaciones en línea.	Web IESS, Banco Pichincha, Banco de Guayaquil, SRI, TuFactura, Laarcourier, Servientrega, Registro Civil, Canva
Intranet	Sitio web empresarial que contiene información y acceso a varios módulos.	Semiya ERP
Nube	Repositorio de archivos digitales.	OneDrive, Drive
Ofimática	Herramientas de procesamiento de texto, hojas de cálculo.	Microsoft Office, Adobe Reader
Página web	Gestor de contenidos. Alojamiento página web	WordPress Hostinger
Servicio de cámaras	Cámaras IP desplegadas en puntos estratégicos	iVMS
Servicio de internet	Enlace de internet	NETLIFE
Servicio de telefonía IP	Telefonía por el protocolo IP que conecta a todas las oficinas.	PBX Panasonic
Servicios de aplicaciones	Aplicaciones de terceros que ayudan a la gestión de las actividades en las áreas.	WhatsApp
Servidor de archivos	Transferencia de archivos de un equipo local a un remoto	WinSCP
Servidor de dominio	Servicio de libretas de direcciones, DNS	Hostinger
Transferencia de archivos	Transferencia para subida de archivos para terceros.	WeTransfer

Además, Industrias Karmat cuenta con documentación propia para la configuración de dispositivos tanto nuevos como después de un procedimiento de formateo, toda la documentación es considerada como confidencial por lo cual no es posible su publicación, sin embargo, esta se usa de manera adecuada al proceso en el cual se requiera.

2.4. Análisis de Impacto del Negocio – BIA

Dentro del análisis de impacto del negocio se determinan los procesos prioritarios de la organización, evaluando la criticidad del impacto que se podría generar si se produce un incidente.

2.4.1. Identificación de actividades y procesos de negocio

En esta instancia se analizan las áreas, las actividades de negocio y los procesos dentro de la organización para cumplir los objetivos; se consideran todas las áreas de la empresa como se ve en la Tabla 28.

Tabla 28.

Identificación de áreas, actividades de negocio y procesos.

Área	Actividad de Negocio	Procesos
Ventas	Comercialización de productos	Pedidos de productos.
	Diseño de políticas de comercialización	Información de ventas por distribuidores. Relacionamiento con los clientes y proveedores. Consulta de comisiones e informe mensual.
Gerencia General	Dirección	Gestión de información de nuevas colecciones. Coordinación de actividades técnicas de control de calidad. Renovación anual de permisos de funcionamiento.
	Comunicación	Aseguramiento de la Calidad. Responsabilidad social. Comunicación externa con proveedores externos.
	Contraloría y auditoria	Creación de formatos de documentación para procedimientos.

Recursos humanos	Administración de personal	Identificación de procesos existentes y faltantes en los procesos de la organización. Liquidación y control de cuentas. Ingreso de nuevo personal. Control de asistencia. Notificación de cambios del personal.
	Nómina	Remuneraciones y beneficios de los empleados. Control de nómina (pago sueldos y beneficios sociales). Reportes a organismos de control.
	Comunicación interna	Manejo de información interna para el personal.
Soporte	Financiero	Cierre mensual de cartera y cobranza. Elaboración y despacho de pedidos.
	Sistemas	Gestión de creación de usuarios y asignación de permisos a sistemas.
Bodega y logística	Financiero	Baja de productos por fallas de fábrica.
	Compras y logística	Gestión de proveedor. Codificación en barra de los productos. Ingreso a productos a bodega. Control de inventarios, despachos, ingresos y devoluciones.
Producción	Administración	Facturación, notas de crédito a clientes. Control y análisis de flujo de caja. Planes telefonía celular.
	Diseño gráfico	Creación de representaciones gráficas para colección actual.
	Desarrollo de estrategias de marketing	Lanzamiento de nuevas colecciones y material promocional. Planificación mensual de material digital para redes sociales.
	Comunicación	Administración y actualización de página web. Comunicación con proveedores de servicios tecnológicos.
	Sistemas (IT)	Gestión del correcto uso de infraestructura física, virtual y servidores (Intranet, aplicaciones web, firewall, equipos de personal, Página web, archivos, correo electrónico, dominio)

		Gestión de respaldo de servidores virtuales. Administración de página web. Administración de la infraestructura de red cableada e inalámbrica. Administración de la intranet. Supervisión de sistemas de respaldo de energía eléctrica. Supervisión y mantenimiento de Data Center. Conexión de enlaces de datos, telefónico o internet. Correo electrónico. Central telefónica IP. Cámaras IP.
Contabilidad	Financiero	Elaboración y presentación de información contable para Organismos de Control. Revisión y envió de comprobantes de retención en la fuente. Realización y preparación de declaraciones de impuestos y anexos tributarios. Cierre mensual de ventas. Generación de proveedores. Altas y bajas de activos fijos. Gestión de inventarios. Análisis y contabilización de facturas. Registro contable de mercadería y notas de créditos. Gestión de compras locales.

Tras finalizar la identificación de las actividades y procesos, que se sustentan en recursos y activos tecnológicos, y se valorarán los impactos que se generarían en caso de interrupción.

2.4.2. Evaluación de impactos operacionales

Para lo cual se presenta la clasificación del impacto operacional, el cual nos ayuda a determinar los procesos más críticos de la organización clasificado en la Tabla 29.

Así se observa el proceso o la actividad del negocio y su relación con el servicio tecnológico y el módulo o sistema que soporta.

Tabla 29.

Procesos, servicios tecnológicos y nivel de impacto.

Procesos Críticos	Servicio Tecnológico	Sistema/módulos	Nivel de impacto
Administración de la infraestructura de red cableada e inalámbrica.	Software de monitoreo	Cisco	A
Administración de la intranet.	Servidor intranet	Oracle	A
Administración de página web.	Servidor página web, Gestor de contenidos	WordPress	A
Administración y actualización de página web.	Gestor de contenidos	WordPress	B
Altas y bajas de activos fijos.	Intranet, Ofimática	Semiya, Microsoft Office	C
Análisis y contabilización de facturas.	ERP	Cuentas por pagar facturas de proveedores, notas de créditos	B
Aseguramiento de la Calidad.	Ofimática, correo electrónico	Microsoft Office, Hostinger	A
Baja de productos por fallas de fábrica.	ERP	Semiya, inventario	B
Cámaras IP.	Servicio de cámaras	iVMS	B
Central telefónica IP.	Servicio de telefonía IP	PBX Panasonic	C
Cierre mensual de cartera y cobranza.	ERP, Ofimática e Intranet	Semiya, Microsoft Office, TuFactura	A
Cierre mensual de ventas.	ERP, Ofimática e Intranet	Semiya, Microsoft Office, TuFactura	B
Codificación en barra de los productos.	Ofimática, ERP	Microsoft Office, Semiya	B
Comunicación con proveedores de servicios tecnológicos.	Correo electrónico, Servicios de aplicaciones	WhatsApp	C
Comunicación externa con proveedores externos.	Ofimática, correo electrónico	Microsoft Office, Hostinger	C

Conexión de enlaces de datos, telefónico o internet.	Consola web (Data Center)	PBX Panasonic	B
Consulta de comisiones e informe mensual.	Intranet	Semiya	C
Control de asistencia.	Intranet	Semiya	C
Control de inventarios, despachos, ingresos y devoluciones.	Ofimática, Correo electrónico	Microsoft Office, Hostinger	B
Control de nómina (pago sueldos y beneficios sociales).	Ofimática, correo electrónico e intranet	Microsoft Office, Hostinger y reportes	B
Control y análisis de flujo de caja.	Ofimática	Microsoft Office	B
Coordinación de actividades técnicas de control de calidad.	Ofimática, correo electrónico	Microsoft office, Hostinger	C
Correo electrónico.	Correo electrónico	Hostinger, Hotmail	B
Creación de formatos de documentación para procedimientos.	Ofimática, correo electrónico	Microsoft Office, Hostinger	C
Creación de representaciones gráficas para colección actual.	Ofimática, Aplicación web	Microsoft Office, Canva	C
Elaboración y despacho de pedidos.	Ofimática, correo electrónico, Internet	Microsoft Office, Hostinger, Web servicio de mensajería	B
Elaboración y presentación de información contable para Organismos de Control.	Ofimática y reportes	Ofimática y Semiya ERP	A
Facturación, notas de crédito a clientes.	Intranet, ERP	TuFactura, Semiya	A
Generación de proveedores.	ERP	Semiya	C
Gestión de compras locales.	ERP, Ofimática y correo electrónico	Semiya, Microsoft Office y Hostinger	C
Gestión de creación de usuarios y asignación de permisos a sistemas.	Aplicaciones empresariales	Semiya	A
Gestión de información de nuevas colecciones.	Gestor de contenidos	WordPress	A
Gestión de inventarios.	ERP, Ofimática e Intranet	Semiya, Microsoft Office	B
Gestión de proveedor.	ERP	Semiya	B

Gestión de respaldo de servidores virtuales.	Gestión Hipervisor vCenter	VMware	A
Gestión del correcto uso de infraestructura física, virtual y servidores (Intranet, aplicaciones web, firewall, equipos de personal, Página web, archivos, correo electrónico, dominio)	Data Center	SSH	A
Identificación de procesos existentes y faltantes en los procesos de la organización.	Ofimática, correo electrónico	Microsoft Office, Hostinger	C
Información de ventas por distribuidores.	Intranet	Semiya	A
Ingreso a productos a bodega.	ERP	Semiya	A
Ingreso de nuevo personal.	Aplicaciones empresariales, aplicaciones web	Semiya, IESS	C
Lanzamiento de nuevas colecciones y material promocional.	Ofimática, correo electrónico, redes sociales	Microsoft Office, Hostinger, Facebook, Instagram, TikTok, Página Web	A
Liquidación y control de cuentas.	Ofimática, correo electrónico	Microsoft Office, Hostinger	C
Manejo de información interna para el personal.	Ofimática, correo electrónico y navegador	Microsoft Office, Hostinger y Canva	C
Notificación de cambios del personal.	Ofimática, correo electrónico	Microsoft Office, Hostinger	C
Pedidos de productos.	Instalación de aplicaciones de proveedor	Semiya	A
Planes telefonía celular.	Ofimática, Correo electrónico	Microsoft Office, Hostinger	C
Planificación mensual de material digital para redes sociales.	Ofimática	Microsoft Office	C
Realización y preparación de declaraciones de impuestos y anexos tributarios.	Ofimática, DIMM	Microsoft Office, SRI software	A
Registro contable de mercadería y notas de créditos.	Ofimática, correo electrónico y ERP	Microsoft Office, Hostinger, Semiya	A

Relacionamiento con los clientes y proveedores.	Ofimática, correo electrónico	Microsoft Office, Hostinger	A
Remuneraciones y beneficios de los empleados.	Ofimática, correo electrónico	Microsoft Office, Hostinger	B
Renovación anual de permisos de funcionamiento.	Navegador, Ofimática, Correo electrónico	Portal entidades públicas, Microsoft Office, Hostinger	B
Reportes a organismos de control.	Navegador e intranet	IESS Web, Web SRI y reportes	C
Responsabilidad social.	Ofimática, correo electrónico	Microsoft Office, Hostinger	C
Revisión y envió de comprobantes de retención en la fuente.	Ofimática, correo electrónico	Microsoft Office, Hostinger y TuFactura	A
Supervisión de sistemas de respaldo de energía eléctrica.	UPS (Data Center)	UPS	A
Supervisión y mantenimiento de Data Center.	Control de acceso	Oracle	A

Como medio para la recolección de la información pertinente para la asignación del nivel de impacto de cada uno de los procesos identificados dentro de la empresa se aplicó una entrevista la cual se realizó al personal que se encuentra dentro de la empresa, tomando como base el criterio de cada uno de los usuarios, experiencia en el proceso y en el medio tecnológico como se detalla en el (Anexo B), siendo la calificación de A considerada como la más esencial dentro del desarrollo de los procesos en Industrias Karmat.

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

Una vez analizado los procesos que se tiene en Industrias Karmat, se toma en cuenta todos los procesos que de acuerdo con las reuniones mantenidas con el personal han calificado con un nivel de impacto tipo A, para lo cual se define el tiempo máximo de inactividad (MTD), así como también la prioridad de recuperación según la Tabla 16, donde 1 es equivalente al nivel alto de

prioridad y 4 es el nivel más bajo, es decir, cual proceso debe ser restaurado con mayor rapidez. A continuación, se detalla en la Tabla 30, la información recopilada.

Tabla 30.

Procesos críticos y establecimiento de tiempos de recuperación.

Procesos Críticos	Servicio Tecnológico	Sistema/ módulos	Nivel de impacto	MTD (días)	ROL
Administración de la infraestructura de red cableada e inalámbrica.	Software de monitoreo	Cisco	A	2	2
Administración de la intranet.	Servidor intranet.	Oracle	A	2	1
Administración de página web.	Servidor página web, Gestor de contenidos	WordPress	A	1	2
Aseguramiento de la Calidad.	Ofimática, correo electrónico	Microsoft Office, Hostinger	A	1	3
Cierre mensual de cartera y cobranza.	ERP, Ofimática e Intranet	Semiya, Microsoft Office, TuFactura	A	2	3
Elaboración y presentación de información contable para Organismos de Control.	Ofimática y reportes	Ofimática y Semiya ERP	A	2	2
Facturación, notas de crédito a clientes.	Intranet, ERP	TuFactura, Semiya	A	0.5	1
Gestión de creación de usuarios y asignación de permisos a sistemas.	Aplicaciones empresariales	Semiya	A	2	1
Gestión de información de nuevas colecciones.	Gestor de contenidos	WordPress	A	2	3
Gestión de respaldo de servidores virtuales.	Gestión Hipervisor vCenter	VMware	A	0.5	1
Información de ventas por distribuidores.	Intranet	Semiya	A	3	4
Ingreso a productos a bodega.	ERP	Semiya	A	2	1

Gestión del correcto uso de infraestructura física, virtual y servidores (Intranet, aplicaciones web, firewall, equipos de personal, Página web, archivos, correo electrónico, dominio)	Data Center	SSH	A	2	3
Lanzamiento de nuevas colecciones y material promocional.	Ofimática, correo electrónico, redes sociales	Microsoft Office, Hostinger, Facebook, Instagram, TikTok, Página Web	A	1	1
Pedidos de productos.	Instalación de aplicaciones de proveedor	Semiya	A	0.5	1
Realización y preparación de declaraciones de impuestos y anexos tributarios.	Ofimática, DIMM	Microsoft Office, SRI software	A	2	4
Registro contable de mercadería y notas de créditos.	Ofimática, correo electrónico y ERP	Microsoft Office, Hostinger, Semiya	A	1	2
Relacionamiento con los clientes y proveedores.	Ofimática, correo electrónico	Microsoft Office, Hostinger	A	2	3
Revisión y envió de comprobantes de retención en la fuente.	Ofimática, correo electrónico	Microsoft Office, Hostinger y TuFactura	A	2	4
Supervisión de sistemas de respaldo de energía eléctrica.	UPS (Data Center)	UPS	A	2	1
Supervisión y mantenimiento de Data Center.	Control de acceso	Oracle	A	1	1

Dentro de la Tabla 29 se define los tiempos mínimos siendo de 0.5 a 3 días que es el tiempo en el cual el proceso se podría recuperar sin provocar problemas a Industrias Karmat, además se pudo establecer la prioridad de cada uno de los procesos para conocer y adecuar los planes de contingencia para el levantamiento del proceso, siendo los principales procesos los siguientes: Facturación, notas de crédito a clientes, gestión de respaldo de servidores virtuales, pedidos de productos, gestión del correcto uso de infraestructura física, virtual y servidores (intranet, aplicaciones web, firewall, equipos de personal, página web, archivos, correo electrónico, dominio). Los cuales obtuvieron un tiempo de máximo tolerable de caída de 0.5(medio día) este valor es representado en días.

2.4.4. Identificación de recursos tecnológicos

Se analiza los recursos que son claves para la continuidad de las actividades desarrolladas por Industrias Karmat, para lo cual se considera los servicios, activos, aplicaciones, módulos o sistemas que pudiesen presentar problemas relacionados a la tecnología, como se puede observar en la Tabla 31.

Tabla 31.

Servicios tecnológicos Industrias Karmat.

Servicio Tecnológico	Descripción	Sistema/ módulos	Nivel de impacto	MTD (días)	Prioridad de recuperación
Aplicación web	Aplicaciones que se usan para el apoyo del negocio.	Semiya ERP, NEGYSERT, TuFactura	A	0.5	1
Configuración de equipos para usuarios	Computadores, sistemas operativos.	Hardware, Windows 7/10	B	1	2

Correo electrónico	Servicio de envío y recepción de mensajes.	Hostinger	B	1	2
Data Center	Centro de cómputo donde se encuentra los dispositivos y servicios de comunicaciones.	Servicio de alimentación eléctrica, equipos de comunicación, servidores y backups.	A	0.5	1
DIMM	Software utilizado para el desarrollo de documentación tributaria.	SRI Software	B	2	3
ERP	Sistema informático para la gestión de procesos (financieros, contables y recursos).	Semiya ERP	A	0.5	1
Firewall	Servidor proxy que funciona para el filtrado de navegación.	Oracle Linux Firewall	A	0.5	1
Gestión Hipervisor vCenter	Plataforma de control y virtualización.	VMware	A	0.5	1
Gestor de contenidos	Programa informático que permite crear un entorno de trabajo para la creación y	WordPress	B	2	2

	administración de contenidos.				
Instalación de aplicaciones de proveedor	Aplicaciones de proveedores externos que permiten el apoyo al negocio.	Canva, IESS, Banco Pichincha, Banco Guayaquil	B	1	1
Intranet	Sitio web corporativo que brinda la información del negocio y desarrollo de procesos.	NEGYSERT, Semiya ERP	A	0.5	1
Navegación web	Acceso a la navegación de internet a varias aplicaciones en línea.	IESS Web, Web SRI, Portales entidades públicas	B	1	3
Ofimática	Herramientas usadas para el procesamiento de texto u hojas de cálculo.	Microsoft Office	C	2	3
Página web	Alojamiento y gestión de contenidos de la página web.	WordPress, Hostinger	B	0.5	2
Redes sociales	Software comercial usado para la distribución de contenido multimedia.	Facebook, Instagram, Tik Tok	C	2	3
Reportes	Desarrollo de reportes	Semiya ERP	B	2	2

	requeridos por los departamentos.				
Servicio de cámaras	Cámaras IP colocadas en puntos de acceso e interiores de la infraestructura física.	iVMS	C	2	4
Servicio de telefonía IP	Servicio de telefonía bajo el protocolo IP que conecta a todos los departamentos.	PBX Panasonic	B	1	2
Servicios de aplicaciones	Aplicaciones externas que permiten el desarrollo de CMS.	Whatsappiando	C	2	3
Software de monitoreo	Sistema de monitoreo de red (software y hardware) que da detalle de los diversos aspectos de la red y su funcionamiento.	Cisco	B	1	2
UPS (Data Center)	Dispositivos que permiten la continuidad de los equipos operantes dentro de la empresa	UPS	B	0.5	1

De igual manera como se realizó el análisis de los procesos críticos, elaboramos el análisis de los recursos tecnológicos para lo cual asignamos valores para el nivel de impacto, el MTD (días) y una prioridad de recuperación, lo cual permite conocer que va desde el 0.5 a 2 días para el restablecimiento de los servicios.

Algunos de los servicios tecnológicos dependen directamente de proveedores externos, mismos que no se pueden considerar como críticos para la empresa obteniendo un nivel de impacto tipo B.

2.4.5. Asignación de RTO y RPO de servicios tecnológicos prioritarios

Una vez concluido con la categorización de los servicios tecnológicos con la designación del MTD y la prioridad de recuperación de estos, se realiza un análisis de los tiempos de recuperación objetivo (RTO) y se define el punto de recuperación objetivo (RPO) los mismos que se definen en valor de horas de los servicios tecnológicos de nivel de impacto A, como se puede ver en la Tabla 32.

Tabla 32.

Servicios tecnológicos nivel de impacto A.

Servicio Tecnológico	Descripción	Sistema/ módulos	Nivel de impacto	MTD (días)	Prioridad de recuperación	RTO (h)	RPO (h)
Aplicación web	Aplicaciones que se usan para el apoyo del negocio.	Semiya ERP, NEGYSERT, TuFactura	A	0.5	1	4	8
Data Center	Centro de cómputo donde se encuentra los dispositivos y servicios de comunicaciones.	Servicio de alimentación eléctrica, equipos de comunicación, servidores y backups.	A	0.5	1	4	8
ERP	Sistema informático para la gestión de procesos	Semiya ERP	A	0.5	1	4	8

	(financieros, contables y recursos).						
Firewall	Servidor proxy que funciona para el filtrado de navegación.	Oracle Linux Firewall	A	0.5	1	2	12
Gestión Hipervisor vCenter	Plataforma de control y virtualización.	VMware	A	0.5	1	5	8
Intranet	Sitio web corporativo que brinda la información del negocio y desarrollo de procesos.	NEGYSERT, Semiya ERP	A	0.5	1	4	12

Dentro del proceso de recuperación del negocio se debe restaurar cinco servicios tecnológicos, los mismos que están relacionadas con los procesos que son considerados los más críticos para Industrias Karmat, por esta razón un correcto mantenimiento de servicios ayuda a gestionar la continuidad del negocio.

El servicio más crítico es la gestión de hipervisor vCenter (Plataforma de control y virtualización) con un tiempo de RTO de 5 horas y su RPO es de 8 horas, una vez pasado estos tiempos se pueden presentar pérdidas muy importantes para la empresa.

2.5. Análisis de Riesgo

2.5.1. Identificación de activos

Dentro de este proceso se toma como ayuda al equipo responsable de cada uno de los departamentos de la empresa y de los conceptos a considerar de la metodología MAGERIT para generar los activos de Industrias Karmat como se define en la Tabla 33.

Tabla 33.

Activos de la empresa Industrias Karmat.

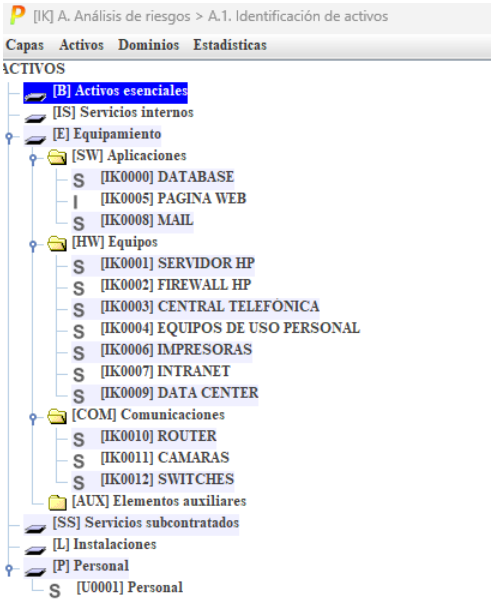
Código	Nombre	Tipo	Descripción y servicios	Responsable	Ubicación
IK0000	DATABASE	Virtual	Servidor de base de datos.	INDUSTRIAS KARMAT	OFICINAS
IK0001	SERVIDOR HP	Virtual	Gestor de máquinas virtuales.	INDUSTRIAS KARMAT	OFICINAS
IK0002	FIREWALL HP	Físico	Dispositivo para la distribución de internet.	INDUSTRIAS KARMAT	OFICINAS
IK0003	CENTRAL TELEFÓNICA	Físico	Central telefónica IP.	INDUSTRIAS KARMAT	OFICINAS
IK0004	EQUIPOS DE USO PERSONAL	Físico	Equipos de computadora para usuarios finales.	INDUSTRIAS KARMAT	OFICINAS
IK0005	PAGINAWEB	Virtual	Servidor de página web CMS WordPress.	INDUSTRIAS KARMAT	OFICINAS
IK0006	IMPRESORAS	Físico	Dispositivos de impresión.	INDUSTRIAS KARMAT	OFICINAS
IK0007	INTRANET	Virtual	Servidor corporativo.	INDUSTRIAS KARMAT	OFICINAS
IK0008	MAIL	Virtual	Servidor de correos electrónicos.	INDUSTRIAS KARMAT	OFICINAS
IK0009	DATA CENTER	Físico	Centro de cómputo.	INDUSTRIAS KARMAT	OFICINAS
IK0010	ROUTER	Físico	Conexión de redes.	INDUSTRIAS KARMAT	OFICINAS
IK0011	CAMARAS	Físico	Programa para el monitoreo de cámaras IP.	INDUSTRIAS KARMAT	OFICINAS
IK0012	SWITCHES	Físico	Dispositivo para comunicación.	INDUSTRIAS KARMAT	OFICINAS

Dentro de la identificación de los activos se considera al recurso humano de la empresa para lo cual se asigna el código U0001 para el correspondiente análisis.

En la Figura 17 se presenta la identificación de los activos de acuerdo con la herramienta PILAR.

Figura 17.

Identificación de activos de Industrias Karmat en la herramienta PILAR.



2.5.2. Valoración de activos

En EAR/PILAR se establecen 7 dimensiones en las que se puede valorar un activo para lo que se considera el impacto que tiene para el negocio, o sea, la importancia que tienen para el desarrollo de un proceso, analizaremos la Tabla 34.

Tabla 34.

Dimensiones de valoración de activos de acuerdo con MAGERIT.

Dimensión	Definición
Confidencialidad	La información no está disponible, ni se puede acceder ni por parte de usuarios, entidades no autorizadas. *¿Qué daño causaría que lo conociera quien no debe?*
Integridad	La información se mantendrá sin modificaciones sin que esta se haya autorizado. *¿Qué perjuicio causaría que estuviera dañado o corrupto?*
Disponibilidad	El activo puede ser accedido ya sea a un proceso o entidad con sus debidos accesos.

	¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?
Autenticidad	La entidad es la responsable de que la fuente de la cual proceda el activo sea garantizada.
	¿Qué perjuicio causaría que fuese suplantado o falsificado?
Trazabilidad	Las actuaciones que genera la entidad son imputables a la entidad.
	¿Qué daño causaría no saber quién accede a qué datos?

Fuente: (Centro Criptológico Nacional - CCN, 2023)

En cada una de estas dimensiones de los activos se puede generar una valoración que permita una evaluación de las posibles consecuencias en caso de suscitarse una amenaza dentro de la organización, para dicha valoración se analiza la escala de criterios los cuales se puede observar en la Tabla 35.

Tabla 35.

Criterios de valoración de activos.

Criterio	Valor
Daño extremadamente grave	Extremo (10)
Daño muy grave	Muy alto (9)
Daño grave	Alto (6-8)
Daño importante	Medio (3-5)
Daño menor	Bajo (1-2)
Irrelevante a efectos prácticos	Depreciable (0)

Fuente: (Centro Criptológico Nacional - CCN, 2023)

Los valores que reciben de esta tabla se refieren a la medida de perjuicio para la organización si el activo se daña en esa dimensión.

Junto con el personal de Industrias Karmat se respondió las preguntas propuestas por MAGERIT con la asignación de valores (Tabla 35 – Anexo B) para cada dimensión.

Figura 18.

Valoración de activos por dimensiones Industrias Karmat.

[IK] A.1. Activos > A.1.4. valoración de los dominios

Editar Exportar Importar

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[IK] Gestión de riesgos							
[essential] Activos esenciales	[10]	[9]	[9]	[9]	[8]	[10]	[9]
[IK0000] DATABASE	[9]	[9]	[6]	[9]	[8]	[8]	[3]
[IK0005] PAGINA WEB	[8]	[7]	[5]	[5]	[5]	[5]	[1]
[IK0008] MAIL	[5]	[8]	[8]	[8]	[4]	[3]	[6]
[IK0001] SERVIDOR HP	[10]	[7]	[7]	[8]	[2]	[5]	[1]
[IK0002] FIREWALL HP	[10]	[9]	[8]	[7]	[5]	[1]	[2]
[IK0003] CENTRAL TELEFÓNICA	[9]	[7]	[6]	[4]	[1]	[5]	[1]
[IK0004] EQUIPOS DE USO PERSONAL	[10]	[8]	[9]	[9]	[2]	[5]	[9]
[IK0006] IMPRESORAS	[8]	[6]	[6]	[6]	[1]	[4]	[4]
[IK0007] INTRANET	[10]	[9]	[7]	[9]	[6]	[8]	[4]
[IK0009] DATA CENTER	[10]	[8]	[7]	[9]	[2]	[7]	[1]
[IK0010] ROUTER	[10]	[7]	[5]	[7]	[5]	[2]	[1]
[IK0011] CAMARAS	[0]	[1]	[6]	[6]	[7]	[6]	[2]
[IK0012] SWITCHES	[9]	[8]	[7]	[7]	[5]	[4]	[2]
[U0001] PERSONAL	[7]			[7]		[10]	[8]
Dominios de seguridad							
[base] Red Corporativa	[10]	[9]	[9]	[9]	[8]	[10]	[9]

Dentro de la Figura 18 en cada dimensión se puede observar la valoración que tiene cada uno de los activos, por lo que se puede definir que los activos más críticos en relación de Disponibilidad (D) son: IK000, IK0001, IK0002, IK0004, IK0007, IK0009, IK0010 para los cuales se obtuvo una ponderación de 10, mientras que en el activo U0001 se considera como el activo más valioso en relación con el Valor (V).

2.5.3. Identificación de amenazas

Una vez establecidos los activos más críticos para el desarrollo de la actividad de la empresa, se debe continuar identificando amenazas para lo que se analizan los sucesos que se pueden presentar para dicho activo.

De acuerdo con el tipo y naturaleza del activo, EAR/PILAR asigna de manera automática la amenaza ya sea esta de tipo: NATURAL [n], INDUSTRIAL [i], HUMANO errores no intencionados[e], ATAQUES errores intencionados[a] y RIESGOS DE PRIVACIDAD [pr].

Debido a estas amenazas detectadas también se presentan diferentes escalas de valoración de cada uno de estos, en referencias a las dimensiones anteriormente definidas en la Tabla 32, de esta manera se expresa la frecuencia y las consecuencias en caso de materializarse la amenaza como se describe en la Tabla 36 y 37.

Tabla 36.

Consecuencias de la materialización de amenazas.

Nivel	Abreviación	Porcentaje
Total	T	100%
Muy alta	MA	90%
Alta	A	50%
Media	M	10%
Baja	B	1%

Fuente: (Pilar, 2021)

En la Tabla 37 se detalla la escala de frecuencia de ocurrencia que se puede presentar dentro de la probabilidad de materialización de las amenazas en el cual podemos definir como:

Tabla 37.

Probabilidad de materialización de amenazas.

Potencial	Probabilidad	Frecuencia	
XL	Muy probable	100	Todos los días
L	Probable	10	Todos los meses
M	Poco probable	1	Todos los años
S	Improbable	0.1	Cada 10 años

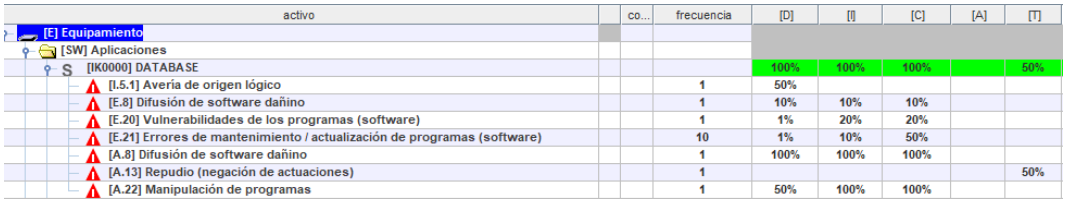
Fuente: (Quintero Villarroya, 2012)

Se presenta los resultados obtenidos una vez que se valoraron las amenazas para los activos de Industrias Karmat, para todos aquellos activos que tienen un nivel alto de disponibilidad, la misma que fue calificada como 10 e igualmente valor con una calificación de 10.

En la Figura 19 se muestra las amenazas que se presentan en el activo IK0000 DATABASE de tipo [E] Equipamiento respecto a Aplicaciones [SW]

Figura 19.

Amenazas asociadas a Equipamiento en Aplicaciones activo IK0000.



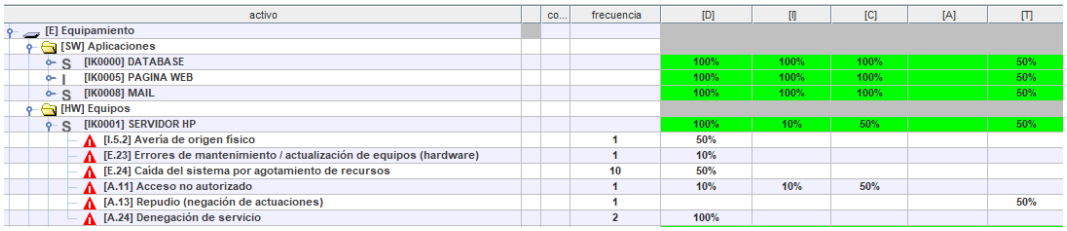
activo		co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento								
[SW] Aplicaciones								
S [IK0000] DATABASE				100%	100%	100%		50%
[I.5.1] Avería de origen lógico			1	50%				
[E.8] Difusión de software dañino			1	10%	10%	10%		
[E.20] Vulnerabilidades de los programas (software)			1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)			10	1%	10%	50%		
[A.8] Difusión de software dañino			1	100%	100%	100%		
[A.13] Repudio (negación de actuaciones)			1					50%
[A.22] Manipulación de programas			1	50%	100%	100%		

La amenaza más frecuente que se presenta es la difusión de software dañino de tipo A.

En la Figura 20 se muestra las amenazas que se presentan en el activo IK0001 SERVIDOR HP de tipo [E] Equipamiento respecto a Equipos [HW].

Figura 20.

Amenazas asociadas a Equipamiento en Equipos activo IK0001.



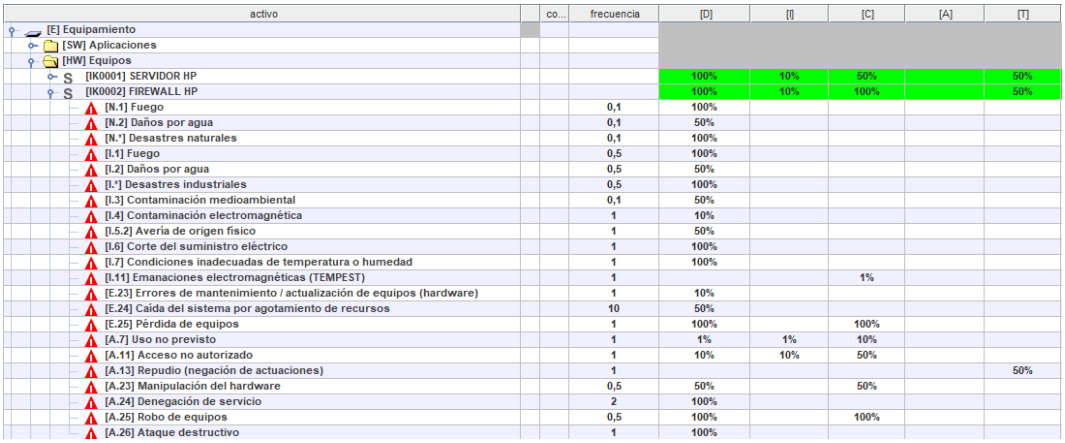
activo		co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento								
[SW] Aplicaciones								
S [IK0000] DATABASE				100%	100%	100%		50%
I [IK0005] PAGINA WEB				100%	100%	100%		50%
S [IK0008] MAIL				100%	100%	100%		50%
[HW] Equipos								
S [IK0001] SERVIDOR HP				100%	10%	50%		50%
[I.5.2] Avería de origen físico			1	50%				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)			1	10%				
[E.24] Caída del sistema por agotamiento de recursos			10	50%				
[A.11] Acceso no autorizado			1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)			1					50%
[A.24] Denegación de servicio			2	100%				

La principal amenaza que se presenta con el activo es la denegación de servicio de tipo A (ataques).

En la Figura 21 se muestra las amenazas que se presentan en el activo IK0002 FIREWALL HP de tipo [E] Equipamiento respecto a Equipos [HW].

Figura 21.

Amenazas asociadas a Equipamiento en Equipos activo IK0002.



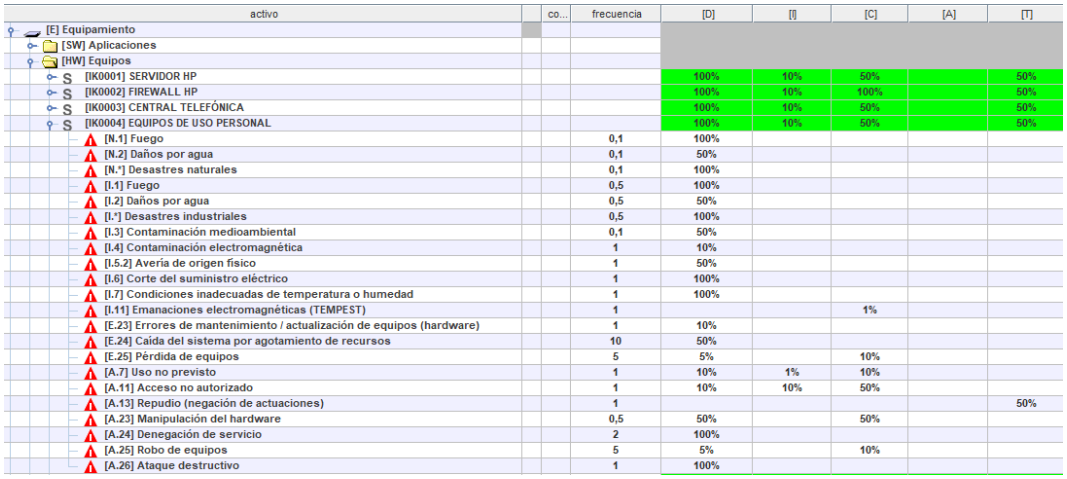
activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento							
[SW] Aplicaciones							
[HW] Equipos							
[IK0001] SERVIDOR HP			100%	10%	50%		50%
[IK0002] FIREWALL HP			100%	10%	100%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	100%		100%		
[A.7] Uso no previsto		1	1%	1%	10%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	100%		100%		
[A.26] Ataque destructivo		1	100%				

La principal amenaza que se presenta con el activo son corte de suministro eléctrico de, condiciones inadecuadas de temperatura o humedad siendo estas de tipo I (industrial), pérdida de equipos de tipo E (humano - errores no intencionados), denegación de servicios, robo de equipos y ataque destructivo de tipo A (ataque).

En la Figura 22 se muestra las amenazas que se presentan en el activo IK0004 EQUIPOS DE USO PERSONAL de tipo [E] Equipamiento respecto a Equipos [HW].

Figura 22.

Amenazas asociadas a Equipamiento en Equipos activo IK0004.



activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento							
[SW] Aplicaciones							
[HW] Equipos							
[IK0001] SERVIDOR HP			100%	10%	50%		50%
[IK0002] FIREWALL HP			100%	10%	100%		50%
[IK0003] CENTRAL TELEFÓNICA			100%	10%	50%		50%
[IK0004] EQUIPOS DE USO PERSONAL			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		5	5%		10%		
[A.7] Uso no previsto		1	10%	1%	10%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		5	5%		10%		
[A.26] Ataque destructivo		1	100%				

La principal amenaza que se presenta con el activo son corte de suministro eléctrico de, condiciones inadecuadas de temperatura o humedad siendo estas de tipo I (industrial).

En la Figura 23 se muestra las amenazas que se presentan en el activo IK0007 INTRANET de tipo [E] Equipamiento respecto a Equipos [HW].

Figura 23.

Amenazas asociadas a Equipamiento en Equipos activo IK0007.

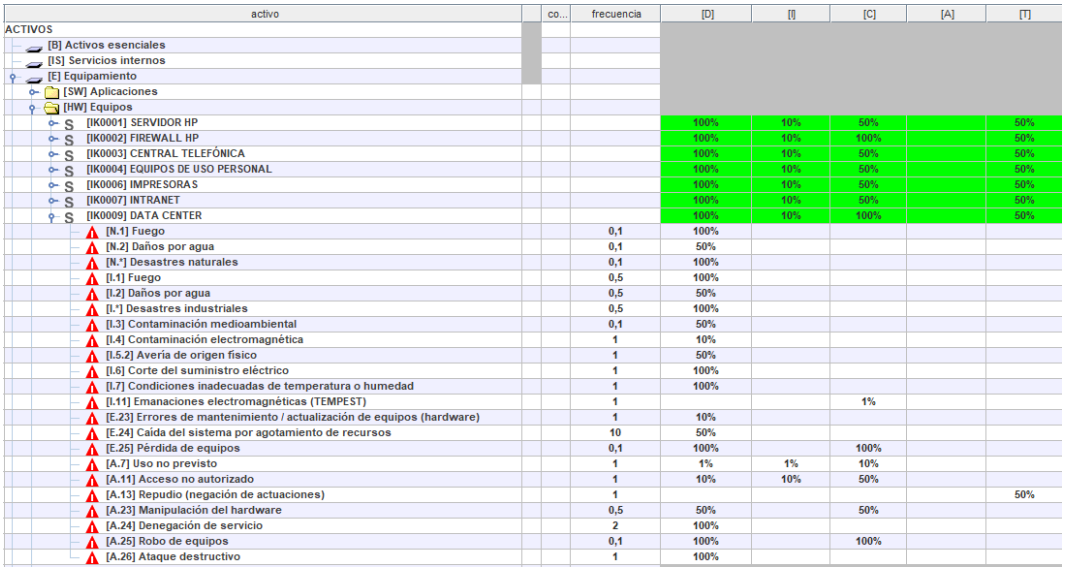
activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[HW] Equipos							
[IK0001] SERVIDOR HP			100%	10%	50%		50%
[IK0002] FIREWALL HP			100%	10%	100%		50%
[IK0003] CENTRAL TELEFÓNICA			100%	10%	50%		50%
[IK0004] EQUIPOS DE USO PERSONAL			100%	10%	50%		50%
[IK0006] IMPRESORAS			100%	10%	50%		50%
[IK0007] INTRANET			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	100%		50%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	100%		50%		
[A.26] Ataque destructivo		1	100%				

La principal amenaza que se presenta con el activo son corte de suministro eléctrico de, condiciones inadecuadas de temperatura o humedad siendo estas de tipo I (industrial), pérdida de equipos de tipo E (humano - errores no intencionados), denegación de servicios, robo de equipos y ataque destructivo de tipo A (ataque).

En la Figura 24 se muestra las amenazas que se presentan en el activo IK0009 DATA CENTER de tipo [E] Equipamiento respecto a Equipos [HW].

Figura 24.

Amenazas asociadas a Equipamiento en Equipos activo IK0009.



activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
[HW] Equipos							
[IK0001] SERVIDOR HP			100%	10%	50%		50%
[IK0002] FIREWALL HP			100%	10%	100%		50%
[IK0003] CENTRAL TELEFÓNICA			100%	10%	50%		50%
[IK0004] EQUIPOS DE USO PERSONAL			100%	10%	50%		50%
[IK0006] IMPRESORAS			100%	10%	50%		50%
[IK0007] INTRANET			100%	10%	50%		50%
[IK0009] DATA CENTER			100%	10%	100%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		0,1	100%		100%		
[A.7] Uso no previsto		1	1%	1%	10%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,1	100%		100%		
[A.26] Ataque destructivo		1	100%				

La principal amenaza que se presenta con el activo son corte de suministro eléctrico de, condiciones inadecuadas de temperatura o humedad siendo estas de tipo I (industrial), pérdida de equipos de tipo E (humano - errores no intencionados), denegación de servicios, robo de equipos y ataque destructivo de tipo A (ataque).

En la Figura 25 se muestra las amenazas que se presentan en el activo IK0010 ROUTER de tipo [E] Equipamiento respecto a Comunicaciones [COM].

Figura 25.

Amenazas asociadas a Equipamiento en Equipos activo IK0010.

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[E] Equipamiento							
[SW] Aplicaciones							
[HW] Equipos							
[COM] Comunicaciones							
[IK0010] ROUTER			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	20%		50%		
[A.7] Uso no previsto		1	10%		10%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	100%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	20%		50%		
[A.26] Ataque destructivo		1	100%				

La principal amenaza que se presenta con el activo son corte de suministro eléctrico de, condiciones inadecuadas de temperatura o humedad siendo estas de tipo I (industrial), pérdida de equipos de tipo E (humano - errores no intencionados), denegación de servicios, robo de equipos y ataque destructivo de tipo A (ataque).

En la Figura 26 se muestra las amenazas que se presentan en el activo U0001 USUARIOS de tipo [P] Personal.

Figura 26.

Amenazas asociadas a Equipamiento en Equipos activo U0001.

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SS] Servicios subcontratados							
[L] Instalaciones							
[P] Personal							
[U0001] PERSONAL			10%	50%	10%		50%
[E.15] Alteración de la información		1		10%			
[E.18] Destrucción de la información		1	1%				
[E.19] Fugas de información		1			10%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.15] Modificación de la información		1		50%			
[A.18] Destrucción de la información		1	10%				
[A.19] Revelación de información		5			10%		
[A.28] Indisponibilidad del personal		0,1	10%				
[A.29] Extorsión		0,9	10%	10%	10%		
[A.30] Ingeniería social (picaresca)		1	10%	10%	10%		

Según lo analizado a través de la herramienta EAR/PILAR, las amenazas más presentadas son fallas en el suministro de energía, denegación de servicios, condiciones inadecuadas del

humedad y ataques destructivos para los activos según el catálogo de información de la herramienta.

En el proceso de investigación se definió que la empresa sufrió problemas en el suministro de energía al no estar conectada directamente a la red eléctrica publica, y en varias ocasiones ha sido un problema para la prestación de servicios digitales para la empresa, personal y usuarios.

2.5.4. Impacto y riesgo

Para esta etapa se analiza los resultados obtenidos del impacto y el riesgo acumulado que pueden afectar a los grupos de activos anteriormente presentados.

Impacto Acumulado: Para este se debe tomar en cuenta que impacto es la medida de daño probable que se puede producir sobre un activo o sistema. Según la Tabla 38, se puede definir una escala nominal de valores.

Tabla 38.

Escala nominal de impacto.

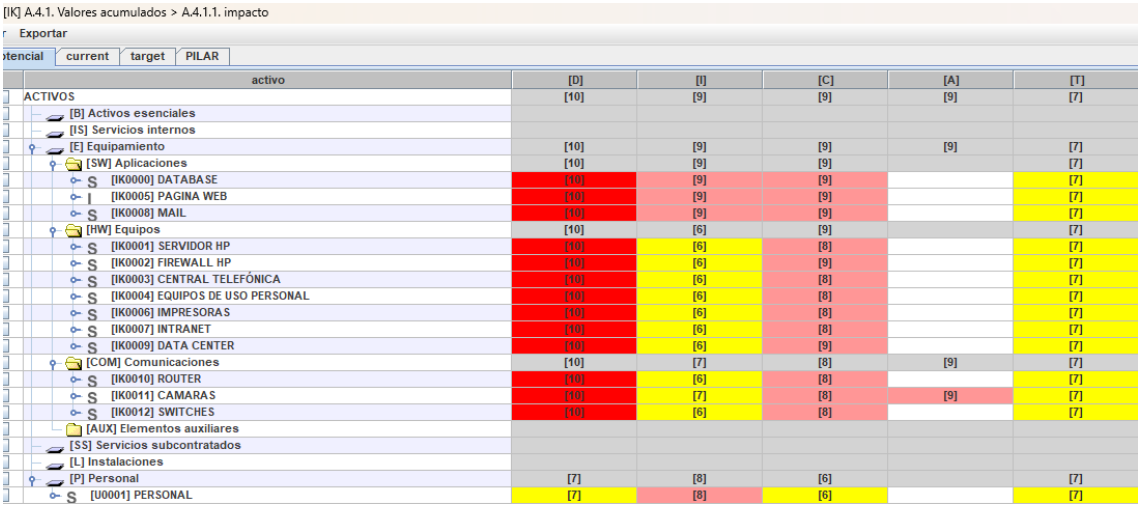
Valor	Descripción
10	Nivel 10
9	Nivel 9
8	Alto +
7	Alto
6	Alto -
5	Medio +
4	Medio
3	Medio -
2	Bajo +
1	Bajo
0	Despreciable

Fuente: (Pilar, 2021)

Como se puede observar en la Figura 27 se muestra los resultados obtenidos de la herramienta EAR/PILAR a los activos y personal de Industrias Karmat.

Figura 27.

Impacto acumulado de los activos y personal de Industrias Karmat.



[IK] A.4.1. Valores acumulados > A.4.1.1. impacto

Exportar

otencial | current | target | PILAR

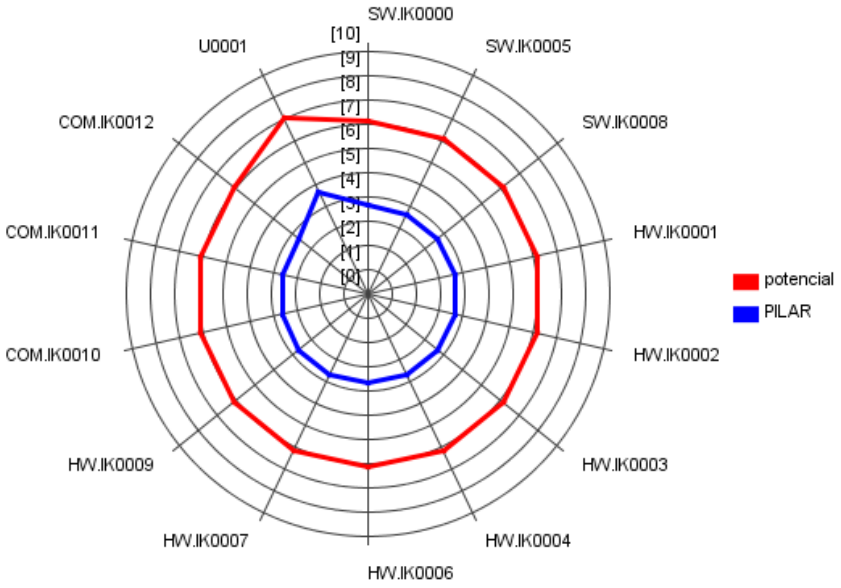
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[10]	[9]	[9]	[9]	[7]
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento	[10]	[9]	[9]	[9]	[7]
[SW] Aplicaciones	[10]	[9]	[9]		[7]
[IK0000] DATABASE	[10]	[9]	[9]		[7]
[IK0005] PAGINA WEB	[10]	[9]	[9]		[7]
[IK0008] MAIL	[10]	[9]	[9]		[7]
[HW] Equipos	[10]	[6]	[9]		[7]
[IK0001] SERVIDOR HP	[10]	[6]	[8]		[7]
[IK0002] FIREWALL HP	[10]	[6]	[9]		[7]
[IK0003] CENTRAL TELEFÓNICA	[10]	[6]	[8]		[7]
[IK0004] EQUIPOS DE USO PERSONAL	[10]	[6]	[8]		[7]
[IK0006] IMPRESORAS	[10]	[6]	[8]		[7]
[IK0007] INTRANET	[10]	[6]	[8]		[7]
[IK0009] DATA CENTER	[10]	[6]	[9]		[7]
[COM] Comunicaciones	[10]	[7]	[8]	[9]	[7]
[IK0010] ROUTER	[10]	[6]	[8]		[7]
[IK0011] CAMARAS	[10]	[7]	[8]	[9]	[7]
[IK0012] SWITCHES	[10]	[6]	[8]		[7]
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal	[7]	[8]	[6]		[7]
[U0001] PERSONAL	[7]	[8]	[6]		[7]

Como resultado de dicho análisis se puede observar que el nivel de impacto predominante es de 10, lo que nos quiere decir que el nivel que se presenta es muy alto en caso de presentarse una amenaza.

En la Figura 28 se presenta el impacto potencial para cada activo de Industrias Karmat, tomando como referencia que la línea roja representa aquellos valores de impacto acumulado potencial y la línea azul representa los valores recomendados por PILAR.

Figura 28.

Valores de impacto potencial acumulado de afectación de activos de Industrias Karmat.



Riesgo acumulado: Es calculado de acuerdo con el activo para lo cual se debe analizar el impacto acumulado que reciba este en base a la amenaza y su probabilidad de suceder. Como se observa en la Figura 29.

Figura 29.

Riesgo acumulado de los activos y personal de Industrias Karmat.

[IK] A.4.1. Valores acumulados > A.4.1.2. riesgo

/er Exportar

potencial | current | target | PILAR

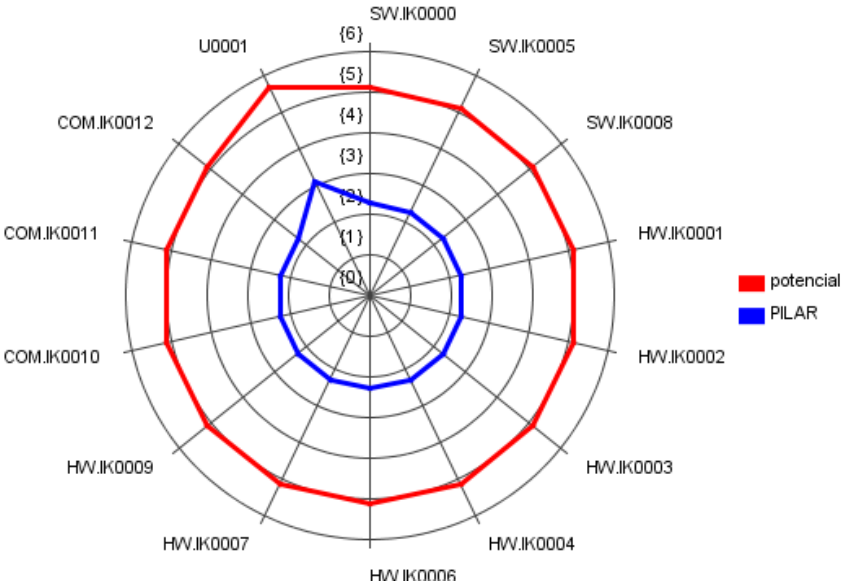
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{7,7}	{6,2}	{6,6}	{6,2}	{5,1}
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento	{7,7}	{6,2}	{6,6}	{6,2}	{5,1}
[SW] Aplicaciones	{6,8}	{6,2}	{6,6}		{5,1}
S [IK0000] DATABASE	{6,8}	{6,2}	{6,6}		{5,1}
I [IK0005] PAGINA WEB	{6,8}	{6,2}	{6,6}		{5,1}
S [IK0008] MAIL	{6,8}	{6,2}	{6,6}		{5,1}
[HW] Equipos	{7,2}	{4,5}	{6,2}		{5,1}
S [IK0001] SERVIDOR HP	{7,2}	{4,5}	{5,7}		{5,1}
S [IK0002] FIREWALL HP	{7,2}	{4,5}	{6,2}		{5,1}
S [IK0003] CENTRAL TELEFÓNICA	{7,2}	{4,5}	{5,7}		{5,1}
S [IK0004] EQUIPOS DE USO PERSONAL	{7,2}	{4,5}	{5,7}		{5,1}
S [IK0006] IMPRESORAS	{7,2}	{4,5}	{5,7}		{5,1}
S [IK0007] INTRANET	{7,2}	{4,5}	{5,7}		{5,1}
S [IK0009] DATA CENTER	{7,2}	{4,5}	{5,7}		{5,1}
[COM] Comunicaciones	{7,7}	{5,0}	{5,7}	{6,2}	{5,1}
S [IK0010] ROUTER	{7,2}	{4,5}	{5,7}		{5,1}
S [IK0011] CAMARAS	{7,7}	{5,0}	{5,7}	{6,2}	{5,1}
S [IK0012] SWITCHES	{7,2}	{4,5}	{5,7}		{5,1}
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal	{5,1}	{5,7}	{5,1}		{5,1}
S [U0001] PERSONAL	{5,1}	{5,7}	{5,1}		{5,1}

En base a la dimensión de Disponibilidad se puede analizar que el valor esta entre 5,1 (crítico) a 7,2 (extremadamente crítico).

En la Figura 30 se presenta el riesgo potencial para cada activo de Industrias Karmat, tomando como referencia que la línea roja representa aquellos valores de impacto acumulado potencial y la línea azul representa los valores recomendados por PILAR.

Figura 30.

Valores de riesgo acumulado de afectación de los activos de Industrias Karmat.



2.6. Determinación de estrategia

En esta fase se fijarán las estrategias para una correcta recuperación de las actividades del negocio definidas como críticas, asociadas a los principales recursos o servicios tecnológicos. Dicha asignación se definió durante la fase de elaboración del BIA y dentro del análisis de riesgos a los activos críticos.

2.6.1. Objetivo, alcance y usuarios

Delimitar como Industrias Karmat aplica las debidas estrategias que garantice una pronta reanudación de las actividades del negocio.

En este documento se aplica el alcance del plan de continuidad del negocio, como se define la Política de Gestión de la Continuidad del Negocio, por lo que sus principales usuarios del mencionado documento será la gerencia, jefes de departamentos y personal que ha trabajado en el diseño del plan de continuidad del negocio.

En caso de suscitarse problemas o amenazas de desastres físicos en Industrias Karmat las reuniones del Comité de Crisis se desarrollan a través de medios digitales, buscando de esta manera optimizar el tiempo y gestionarse el traslado del personal que ayude a la recuperación de los procesos.

2.6.2. Plan de recuperación de desastres

Análisis de impacto en el negocio – BIA: Dentro del BIA realizado, se pudo observar que 6 actividades son las que presentan nivel de impacto tipo A y tienen una prioridad de recuperación 1 referente a los servicios tecnológicos de Industrias Karmat.

Tabla 39.

Listado de actividades críticas.

Actividades	Servicio Tecnológico	Sistema/ módulos	Activos	MTD (días)	RTO(h)	RPO(h)
Sistemas para el ingreso de pedidos y facturación.	Aplicación web	Semiya ERP, NEGYSERT, TuFactura	U0001 - PERSONAL IK0004 – EQUIPO DE USO PERSONAL	0.5	4	8
Gestión de funcionamiento de la	Data Center	Servicio de alimentación eléctrica,	IK009 – DATA CENTER	0.5	4	8

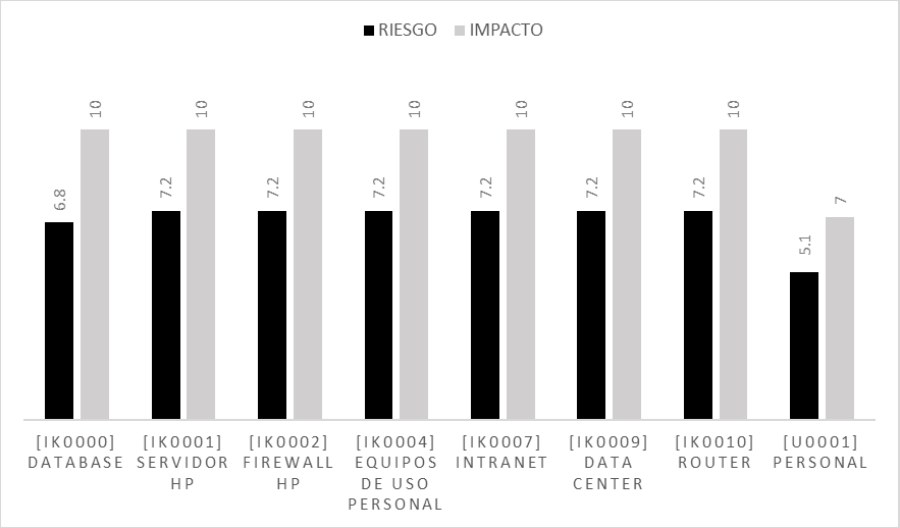
infraestructura física y virtual de servidores		equipos de comunicación, servidores y backups.				
Administración de actividades y procesos administrativos	ERP	Semiya ERP	IK0000 – DATABASE IK0002 – FIREWALL HP	0.5	4	8
Infraestructura de red	Firewall	Oracle Linux Firewall	IK0002 – FIREWALL HP IK0010 - ROUTER	0.5	2	12
Supervisión de la infraestructura de red	Gestión Hipervisor vCenter	VMware	IK0009 – DATA CENTER IK000 – DATABASE	0.5	5	8
Administración de la intranet	Intranet	NEGYSERT, Semiya ERP	IK0007 – INTRANET IK0004 – EQUIPO DE USO PERSONAL U0001 - PERSONAL	0.5	4	12

Como se puede observamos en la Tabla 39, ante un evento disruptivo dentro de Industrias Karmat tiene como prioridad restaurar las actividades críticas relacionadas a su infraestructura tecnológica para luego así, dar soporte a las actividades principales del negocio de la organización y que esta siga operando.

Evaluación de riesgos: A continuación, se presentan los resultados obtenidos de la evaluación de riesgos como son el impacto y el riesgo al que se enfrentan los activos críticos de Industrias Karmat, dichos valores fueron resultantes una vez aplicada la herramienta EAR/PILAR, por lo que en la Figura 31 se detalla dichos valores.

Figura 31.

Riesgo e impacto acumulado a los principales activos de Industrias Karmat.



El valor en la mayoría de los activos es de 10, significa que es muy alto y el riesgo acumulado es de 7,8, según la escala nominal estaría en estado crítico.

Comité de Crisis: Ante un evento disruptivo, el encargado de activar el plan de continuidad del negocio y dirigir las acciones durante la contingencia es el Comité de Crisis, dentro de Industrias Karmat se ha conformado un Comité Paritario el mismo que está conformado por representantes tanto del empleador como de los empleados quedando de la siguiente manera:

- Responsable de Seguridad.
- Presidente.
- Secretario.
- Primer Vocal Empleados.
- Segundo Vocal Empleados.
- Primer Vocal Empleador.
- Segundo Vocal Empleador.

Como miembros de apoyo del Comité de Crisis estará, el personal de tecnología que es la persona encargada de analizar y delimitar el impacto de la incidencia además realiza el papel de gerente de recuperación del proceso a cargo, el responsable de Seguridad estará a cargo de la logística en caso de ir a un sitio alterno, la presidenta se encarga de las adquisiciones y la secretaria se encarga de informar a los clientes, proveedores y usuarios sobre la situación.

El Comité de Crisis es dirigido por el presidente del Comité Paritario, dicha función es llamar a reunión al comité y notificar la materialización de un evento presentado.

Estrategias de recuperación: A continuación, se establecen estrategias de acuerdo con los procedimientos internos que se deban aplicar para cada actividad considera como crítica. Por lo cual se trabaja con la información de la Tabla 39 en la cual se determinan las actividades críticas para Industrias Karmat.

La estrategia busca precautelar ante todo la integridad física del personal, durante y después de presentarse un evento sea cual sea su tipo.

Tabla 40.

Estrategia para el Sistema para el ingreso de pedidos y facturación.

1. Sistema para el ingreso de pedidos y facturación		
Objetivo: Desarrollar el proceso de ingreso de pedidos y facturación a través de la infraestructura. El RTO para esta actividad es de 4 horas.		
Recursos: La persona responsable para la recuperación de esta actividad es el Personal de TI.		
Servicios: Aplicación Web		
Activos: U0001 - PERSONAL	**Riesgo:** 5,1	**Impacto:** 7
IK0004 – EQUIPO DE USO PERSONAL	**Riesgo:** 7,2	**Impacto:** 10
Recuperación:		
• En el caso de la presentación de la denegación de servicio, se procede a revisar la documentación del Proceso A1: Denegación de servicio		
• En el caso de presentarse una difusión de software dañino, aplicar el Proceso A2: difusión de software dañino		

Tabla 41.

Estrategia para la gestión de funcionamiento de la infraestructura física y virtual de servidores.

2. Gestión de funcionamiento de la infraestructura física y virtual de servidores		
Objetivo: Comprender el entorno tecnológico de los servidores virtuales y físicos que soportan los procesos dentro de Industrias Karmat y lograr que dicha infraestructura tenga la capacidad de recuperarse de un evento. El RTO para esta actividad es de 4 horas.		
Recursos: La persona responsable para la recuperación de esta actividad es el Personal de TI.		
Servicios: Data Center		
Activos: IK0009 – DATA CENTER	**Riesgo:** 7,2	**Impacto:** 10
Recuperación:		
• Si se presenta la denegación de servicio o ataques destructivos, se revisará Proceso A1 y Proceso A3.		
• En el caso de presentarse corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad, se procede a revisar el Proceso A4 y A5		

Tabla 42.

Estrategia para la administración de actividades y procesos administrativos.

3. Administración de actividades y procesos administrativos		
Objetivo: Garantizar la correcta ejecución de las actividades y procesos de tipo administrativo que se ejecutan en Industrias Karmat para su operación. El RTO para esta actividad es de 4 horas.		
Recursos: La persona responsable para la recuperación de esta actividad es el Personal de TI.		
Servicios: ERP		
Activos: IK0000 – DATABASE	**Riesgo:** 6,8	**Impacto:** 10
IK0002 – FIREWALL	**Riesgo:** 7,2	**Impacto:** 10
Recuperación:		
• En el caso de la presentación de difusión de software dañino se debe recurrir al Proceso A2.		
• En el caso de presentarse corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad y pérdida de equipos se revisa los Procesos A4, A5 y A6.		

Tabla 43.

Estrategia de infraestructura de red.

4. Infraestructura de red		
Objetivo: Garantizar la correcta conectividad de equipos tanto en red WAN como LAN. El RTO para esta actividad es de 2 horas.		
Recursos: La persona responsable para la recuperación de esta actividad es el Personal de TI.		
Servicios: Firewall		
Activos: IK0010 – ROUTER	**Riesgo:** 7,2	**Impacto:** 10
IK0002 – FIREWALL	**Riesgo:** 7,2	**Impacto:** 10
Recuperación:		
• En el caso de presentarse corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad y pérdida de equipos se debe revisar los Proceso A4, A5 y A6.		
• Si se presenta denegación de servicios o ataque destructivo el Proceso A1 o A3.		

Tabla 44.

Estrategia de supervisión de la infraestructura de red.

5. Supervisión de la infraestructura de red		
Objetivo: Reducir el impacto que podría generarse en caso de un incorrecto funcionamiento de la infraestructura de red. El RTO para esta actividad es de 5 horas.		
Recursos: La persona responsable para la recuperación de esta actividad es el Personal de TI.		
Servicios: Gestión Hipervisor vCenter		
Activos: IK0009 – DATA CENTER	**Riesgo:** 7,2	**Impacto:** 10
IK0000 – DATABASE	**Riesgo:** 6,8	**Impacto:** 10
Recuperación:		
• Si se presenta la denegación de servicio o ataques destructivos, se revisará Proceso A1 y Proceso A3.		
• En el caso de presentarse corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad, se procede a revisar el Proceso A4 y A5		
• En el caso de la presentación de difusión de software dañino se debe recurrir al Proceso A2.		

Tabla 45.

Estrategia para la administración de la intranet.

6. Administración de la intranet		
Objetivo: Recuperar los servicios que brinda la intranet a los procesos del negocio. El RTO para esta actividad es de 4 horas.		
Recursos: La persona responsable para la recuperación de esta actividad es el Personal de TI.		
Servicios: Intranet		
Activos: IK0007 – INTRANET	**Riesgo:** 7,2	**Impacto:** 10
IK0004 – EQUIPO DE USO PERSONAL	**Riesgo:** 7,2	**Impacto:** 10
U0001 - PERSONAL	**Riesgo:** 5,1	**Impacto:** 7
Recuperación:		
• En el caso de presentarse corte del suministro eléctrico, condiciones inadecuadas de temperatura o humedad y pérdida de equipos se debe revisar los Proceso A4, A5 y A6.		
• En el caso de la presentación de la denegación de servicio, se procede a revisar la documentación del Proceso A1: Denegación de servicio		
• En el caso de presentarse una difusión de software dañino, aplicar el Proceso A2: difusión de software dañino		

A continuación, en la Tabla 46, se detalla los procedimientos que se aplican en caso de presentarse una amenaza.

Tabla 46.

Procedimientos antes, durante y después de amenazas.

Proceso	Actividades antes	Actividades durante	Actividades después
A1: denegación de servicio	Verificar que la conexión y configuración entre los routers de la red interna con los Proveedores de Servicio de Internet se encuentre correcta. Utilizar un equipo o software específico para firewall. Poseer equipos para redundancia y balanceo de carga, ya que, si un equipo se cae, el otro asumirá el trabajo. Mantener el software actualizado de todos los equipos, para evitar cualquier tipo de ataque que vulnere las actividades de la empresa. Mantener el antivirus actualizado en todos los equipos. Contar con un plan de pruebas de las aplicaciones expuestas a la red. Capacitar a todo el personal sobre ataques informáticos, mediante charlas o reuniones para que se encuentren preparados ante cualquier tipo de ataque. Realizar copias de seguridad de información relevante como: bases de datos, aplicaciones, entre otros.	Monitorear el software de antivirus y firewall permitiendo detectar ataques que puedan afectar las actividades de la empresa. Identificar los equipos afectados por este ataque, aislándolos para un breve análisis. En caso de reemplazo o adquisición de equipos informático se deberá seguir los siguientes pasos: - Adquirir el equipo con características similares para lo cual se debe llenar el Formato Adquisición de equipos informáticos. - Instalar el sistema operativo y controladores. Se debe verificar que el firewall se encuentre activo, para evitar que intrusos puedan acceder a la red y así vulnerar a los servidores. Examinar los equipos infectados y eliminar dichas infecciones mediante un software de seguridad que: - Realice un seguimiento a las direcciones IP de toda la red - Gestione los picos de tráfico en toda la red. - Analice las IP de destino y puertos que se encuentren abiertos. Reforzar el tráfico de la red mediante subredes y reglas de firewall que permita proteger de las conexiones de tráfico no deseado.	Una vez detectado el ataque, realizar un bloqueo de las IP que muestren un comportamiento anormal. Restringir el acceso a los sitios web. Mantener habilitadas las aplicaciones más importantes. Importar las copias de seguridad que se efectúo anteriormente. Restaurar los archivos necesarios para el normal funcionamiento de los servicios. Presentar un informe detallado (Formato **Reporte de incidentes)** de los incidentes e informar al Comité de Crisis. Evaluar periódicamente todos los incidentes de seguridad de la información. Realizar mejoras en la seguridad de la información. Establecer políticas y procedimientos para la reparación, mantenimiento o reemplazo, para mantener a los equipos en buenas condiciones. Cumplir con todas las responsabilidades asignadas ante un evento inesperado. Registrar en la bitácora los acontecimientos sucedidos (Formato **Bitácora de incidencias**).

A2: difusión de software dañino	Tener software actualizado, para evitar ataques de software dañinos. Utilizar un software antivirus y mantenerlo actualizado para proteger a los equipos frente a software dañinos y evitar su distribución. Acceder solo a sitios seguros para realizar descargar de software o programas. Realizar copias diarias de seguridad, de base de datos e información realizada internamente para salvaguardar la información manejada por la institución y registrar (Formato Copias de seguridad). Analizar dispositivos de almacenamiento como USB mediante el software antivirus antes de su uso. Verificar que el firewall se encuentre activo para proteger los equipos de accesos no deseados. Restricciones de acceso físico a las instalaciones donde se albergan el *Data Center*, para resguardar la información que se almacena en esta. Mantener inventarios documentados y actualizados de los equipos informáticos (Formato **Inventario de equipos informáticos/software**) y relacionados, en donde conste: - Lista de todos los activos. - Etiquetas para identificación de manera única. Establecer horarios para realizar copias de seguridad regulares en medios de almacenamiento externos, los mismo que se encuentra en un Data Center alterno y registrar (Formato **Copias de seguridad**). Respaldar toda la información en los principales activos en un Data Center alterno que posee la institución, mediante: - Creación de imágenes de los sistemas operativos. - Creación de puntos de restauración.	Una vez identificados los equipos infectados por un software dañino, se recomienda desconectar de la red los equipos que no se han infectado, ya que si están conectados la posibilidad de infectarse es mayor. Mantener el software de antivirus actualizado para realizar un análisis a los equipos para: - Escanear en tiempo real todos los archivos, aplicaciones y servicios. - Escanear los dispositivos de almacenamiento como USB o discos duros externos, pues estos pueden ser portadores de virus. - Analizar los tipos de virus. El personal no debe ingresar a enlaces o sitios no seguros, es recomendable pasar el ratón por encima del enlace y verificar si es confiable y seguro. Comprobar si la amenaza tuvo origen interno o externo, si resulta ser interno identificar a los responsables y llenar el reporte correspondiente (Formato **Registro de incidentes**)	Realizar informes con el siguiente formato (Formato **Informe de difusión de software dañino**). Se debe tener la capacidad para descubrir el ataque, solucionarlo y recuperar la información que se encuentra involucrada. Tener un control de acceso de los usuarios con el siguiente procedimiento: - La información que maneja la institución no puede ser revelada a otra institución. - El control de acceso lógico es responsable del personal de cada departamento. Se deberá anotar en la bitácora los acontecimientos sucedidos (Formato **bitácora de incidencias**).

A3: ataques destructivos	- Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo. Brindar capacitaciones al personal nuevo que ingrese a la empresa. Contar con un control de acceso, asignando para cada empleado un usuario y contraseña dependiendo el cargo que desempeña en la empresa. Se recomienda que la contraseña sea fuerte y difícil de descifrar, además no se debe almacenar en lugares visibles o de fácil acceso. El uso del equipo informático es para el ámbito laboral, más no personal. Revisar la configuración del firewall. Tener un control de copias de seguridad. (Formatos **Copia de seguridad**) Para mantener la integridad y confidencialidad de los datos que maneja la empresa, se realiza copias de seguridad diarias, almacenándolas en los servidores ubicados en un Data Center alterno y registrarlas (Formato **Copias de seguridad**) Definir políticas donde el personal de la empresa tenga claro cuáles son actividades que desempeña. (Formato **Funciones y roles de seguridad al personal).**	Se maneja mucha información, así que se debe hacer reuniones con el personal para comprobar la cantidad de información afectada, además de identificar las causas, de origen humano o técnico, identificar a los responsables del ataque, de los sistemas o servicios afectados (Formato Registro de incidentes). Durante un desastre o falla, el personal de TI tiene acceso las 24 horas del día. La información que maneja la empresa no debe ser accesible para otra empresa, a menos que esta lo autorice, la información debe encontrarse resguardada en sitios seguros como: Data Center alternos para respaldos.	Detección de todos los incidentes de seguridad de la información. Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información. Registrar las acciones preventivas y correctivas. Evaluar periódicamente todos los incidentes de seguridad de la información. Realizar mejoras en la seguridad de la información.

A4: corte del suministro eléctrico	El ambiente de las instalaciones debe ser estable para el normal funcionamiento de los equipos del Data Center. Contar con UPS para el Data Center y lugares que así lo requieran para evitar la interrupción del funcionamiento de servidores y equipos relacionados por falta de energía. Contar con equipos de redundancia para continuar las actividades con normalidad. Respaldar toda la información en los principales activos del Data Center alterno que posee la empresa, mediante: - Creación de imágenes de los sistemas operativos. - Creación de puntos de restauración. - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.	Guardar toda la información que se está manejando en el momento del corte de suministro eléctrico, luego se procederá a apagar los equipos como servidores, equipos de red, etc., mientras retorna la energía eléctrica o se ha regulado los daños. Seguir el procedimiento adecuado de apagado para cada uno de los servidores mediante el emulador de terminal Putty o VMware, dando prioridad a los equipos de alta disponibilidad. Asegurarse de contar con fuentes de alimentación alternas en caso de que falle las fuentes normales: - Disponer del número necesario de generadores de energía, los cuales deben contar con los mínimos estándares de seguridad, confiabilidad y calidad. - Los generadores deben ubicarse, por lo general en el suelo. - Los UPS deben estar ubicados a una distancia segura de los equipos informáticos de alta disponibilidad.	Realizar reuniones con el personal para notificar los daños en los equipos, y proceder al reemplazo o recuperación de la información de estos, emitiendo informes (Formato **Informe corte de suministro eléctrico**). Todo el personal debe revisar su área y posteriormente conectar todos los equipos. El personal debe reanudar todos los servicios para uso del cliente. Se deberá anotar en la bitácora los acontecimientos sucedidos (Formato **Bitácora de incidencias**).

A5: condiciones inadecuadas de temperatura o humedad	Contar con sensores para detectar presencia de temperatura o humedad. Verificar las conexiones de agua del servicio higiénico. Contar con un sistema de sellado en tuberías para impedir fugas de agua o rompimientos en las conexiones. Tener precaución con los desagües ubicados en el piso, donde también se encuentran conexiones eléctricas. Tener precaución en los meses que en donde se presenta abundantes lluvias en el cantón. Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante: - Creación de imágenes de los sistemas operativos. - Creación de puntos de restauración. - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la empresa en equipos de respaldo.	Los sistemas de alarma y detección física deben proporcionar alertas tempranas de ocurrencia al personal, todas las alarmas deben tener vínculos con la policía nacional y los bomberos. Verificar los daños físicos que se han presentado en los equipos informáticos, y si necesita reemplazo de algún componente contactarse con los proveedores pertinentes tomando en cuenta los siguientes aspectos (Formato **Adquisición de equipos informáticos**): - Estimar los tiempos de entrega de equipos y repuestos. - Garantía en caso de desperfectos. - Soporte en instalación y capacitación.	Verificar que el nivel de humedad sea el adecuado para evitar filtración de agua en equipos informáticos. Incluir diseño de protección, como rociadores de tubería seca y detectores automáticos. Reportar los incidentes mediante el siguiente procedimiento para hacer frente a estos, en el cual debe abarcar (Formato **Reporte de incidentes definido**): - Detección de todos los incidentes de seguridad de la información. - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información. - Registrar las acciones preventivas y correctivas. - Evaluación periódica de todos los incidentes de seguridad de la información. - Realizar mejoras en la seguridad de la información

A6: pérdida de equipos	Disponer con proveedores para cambios, mantenimiento o alquiler de equipos informáticos. Se debe asignar funciones y roles de seguridad al personal, que abarque (Formato **Funciones y roles de seguridad al personal**): Deben asegurarse de mantener inventarios actualizados de sus dispositivos físicos y artículos de equipamiento. (Formato **Inventario de equipos informáticos/software**): - Lista de todos los activos. - Etiquetas para identificación de manera única. En caso de subcontratación: - No se puede poner el nombre de la institución como etiqueta. - Se informa a la institución cuando los activos están siendo reubicados. - Los activos se devuelven dentro del plazo determinado y acordado.	Cualquier evento que se presente, se debe informar al responsable del Comité de Crisis. Verificar que las instalaciones cuenten con buenas medidas de seguridad física, como: - Todas las puertas deben estar protegidas con cerraduras. Si el equipo fue reemplazado el personal responsable deberá realizar el siguiente proceso para dar continuidad a los servicios que brinda la empresa al cliente: - Adquirir el equipo con características similares. - Instalar el sistema operativo. - Instalar controladores. - Reiniciar el equipo	Mantener la redundancia en los equipos para que los servicios se encuentren disponibles y el cliente tenga acceso, mediante: - La información de respaldo debe ser enviar al sitio alterno seguro. Los equipos puestos nuevamente en servicio deben revisarse y probarse para verificar su configuración y normal funcionamiento, además debe apagarse y reiniciarse antes de ponerlos en servicio. El personal de cada departamento debe reportar el incidente y seguir el procedimiento para hacer frente a estos casos e informar al Comité de Crisis, en el cual debe abarcar (Formato **Reporte de incidentes definido**): - Detección del incidente de seguridad. - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad. - Registrar las acciones preventivas y correctivas. - Evaluación periódica de todos los incidentes de seguridad. El personal deberá anotar en la bitácora los acontecimientos sucedidos (Formato **Bitácora de incidencias**).

2.7. Mantenimiento, prueba y revisión

2.7.1. Objetivo, alcance y usuario

El objetivo del plan durante esta etapa de la continuidad del negocio es determinar la viabilidad de las medidas y establecer las acciones correctivas.

Se aplicará a los elementos del alcance del plan de continuidad del negocio.

2.7.2. Plan de mantenimiento del plan de continuidad del negocio

Dentro de este plan se contempla los siguientes elementos del plan de continuidad del negocio:

- Análisis de Impacto sobre el Negocio (BIA).
- Análisis de Riesgo.
- Cambios organizativos o de negocio: se debe realizar revisiones periódicas sobre la estructura organización, cambios de personal (nuevas contrataciones, despidos o renuncias), cambios en el desarrollo de los procesos y cambios tecnológicos.
- Responsabilidades: se debe actualizar las responsabilidades del personal en caso de tener cambios de personal o de funciones.
- Capacitaciones: Comité de Crisis debe estar consciente y formado sobre cada concepto definido dentro del plan de continuidad del negocio.
- Comunicaciones: Motivar al personal de Industrias Karmat la cultura de continuidad del negocio dentro de la empresa.
- Auditorias: se debe continuar con un plan de auditoría a los componentes que conforman el plan de continuidad del negocio.
- Pruebas de estrategias de recuperación: Se procede a realizar una revisión de los resultados de las pruebas ejecutadas, así como de las mejoras aplicadas.

- Actualización del BCP: se debe contar con información clara y concreta del personal involucrado en el proceso de manera actualizada si hay crisis, así al contar con información exacta y fiable permitirá tener una correcta revisión y actualización, como se indica en la Tabla 47.

Tabla 47.

Cronograma de mantenimiento de los elementos del plan de continuidad del negocio.

ELEMENTOS DEL BCP	TIEMPO EN MESES											
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**
Análisis de Impacto sobre el Negocio (BIA).	x											
Análisis de Riesgo.	x											
Cambios organizativos o de negocio	x						x					
Responsabilidades	x			x			x			x		
Capacitaciones	x			x			x			x		
Comunicaciones	x		x		x		x		x		x	
Auditorias	x						x					
Pruebas de estrategias de recuperación											x	
Actualización del BCP						x						x

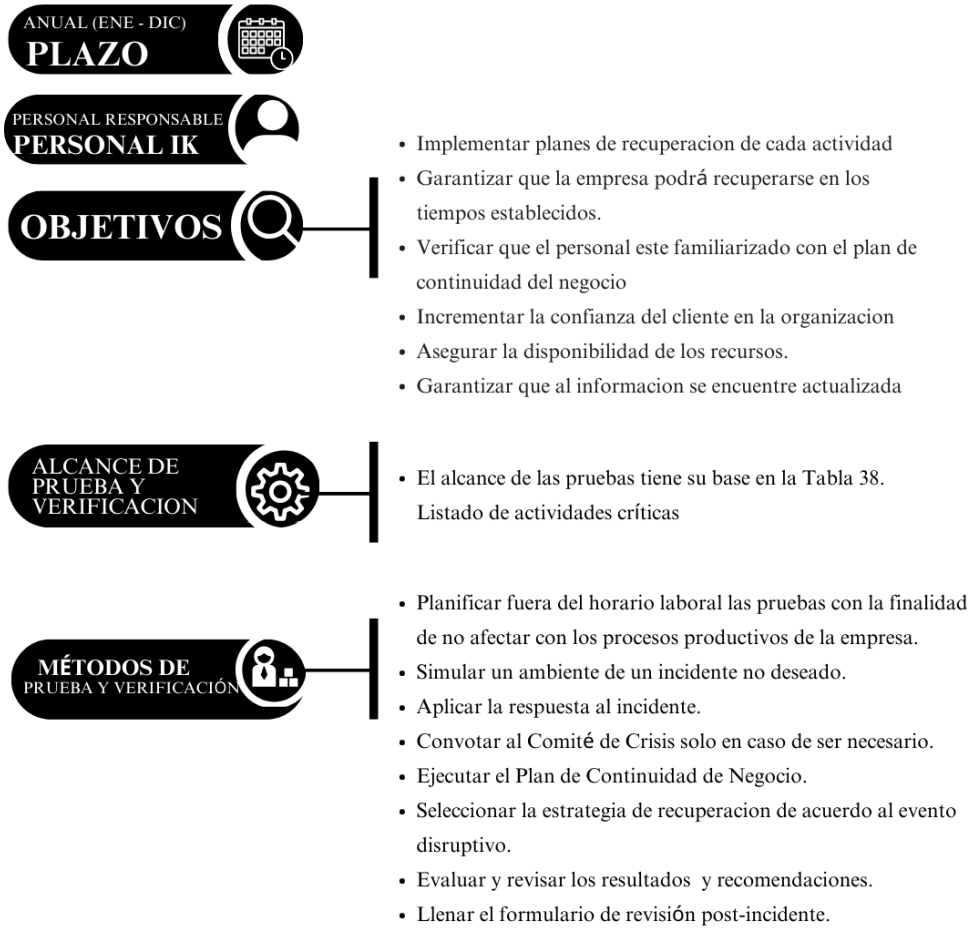
El presidente del Comité de Crisis será el responsable de la ejecución el cronograma de mantenimiento, además de hacer cumplir con cada una de las tareas indicadas, aunque en caso fortuito puede designar a un responsable para cada actividad e ir supervisando que se realice una correcta actualización de estos, la vigencia de dicho plan es anual.

2.7.3. Prueba y revisión

Este plan busca realizar una prueba y verificar la continuidad del negocio que se implanta en Industrias Karmat, de acuerdo con la Figura 32:

Figura 32.

Plan de prueba y revisión.



Informes de pruebas y verificación: A continuación, se presenta un informe de la prueba realizada a Industrias Karmat para la actividad del proceso Gestión de funcionamiento de la infraestructura física y virtual de servidores se realizó en un ambiente controlado en el que se simuló un corte de energía eléctrica, el tiempo en el que se generó dicha prueba fue después del horario de oficina y teniendo en cuenta la estrategia de continuidad Proceso A4: corte del suministro eléctrico.

Para lo cual se aplicó el siguiente esquema:

- Fecha: 15 de junio 2023

- Persona responsable de la prueba: Personal IK
- Alcance de la prueba y verificación: con esta prueba se obtuvo los tiempos de respuesta por parte del personal y de entrada en funcionamiento de los equipos UPS.
- Proceso:
    - Primer Paso: Se notificó al personal de Industrias Karmat a través del correo empresarial acerca de la actividad, tomando en cuenta que en caso de suscitarse un caso real este paso no es necesario.
    - Luego, se procede con la simulación para lo cual se bajó el breaker de energía del edificio donde se ubica Industrias Karmat.
    - Se procede a tomar los tiempos de respuesta o de funcionamiento tanto del UPS como del generador eléctrico.
    - Declarar la situación de crisis, apoyados en la guía.
    - Registro del cumplimiento de los objetivos de la prueba
    - Mencionar acciones o medidas correctivas y recomendaciones.
- Datos recolectados
    - Tiempo de respuesta del UPS: Menos de un segundo
    - Tiempo de respuesta del generador eléctrico: 10 min

Tabla 48.

Logros de objetivos para el proceso Gestión de funcionamiento de la infraestructura física y virtual de servidores.

Objetivo: Conocer los tiempos de respuesta y el funcionamiento de UPS y generador eléctrico para un incidente		
Criterios de Valoración		
1: No alcanzado	2: Alcanzado Parcialmente	3: Alcanzado
Proceso: Gestión de funcionamiento de la infraestructura física y virtual de servidores		
Objetivo de la prueba	**Logro del objetivo**	
Simular un ambiente controlado de corte de suministro eléctrico		3
Verificar y tomar tiempos de respuesta		3
Comprobar el funcionamiento de UPS		3
Comprobar el funcionamiento del generador eléctrico		3
	TOTAL	**12**

Con base a los resultados obtenidos en la Tabla 48, se concluye lo siguiente:

- La prueba cumplió con el RTO de 4 horas por lo que no se consideró situación de crisis.
- Recomendaciones:
    - Si el objetivo es menor a 3 se debe aplicar correcciones a la estrategia aplicada.
    - Se debe considerar para el correcto funcionamiento del generador eléctrico la realización de un mantenimiento preventivo, así como la compra del combustible para el mismo.

2.8. Plan de capacitación y concienciación

Dentro de la fase final el público objetivo será el personal de Industrias Karmat y el Comité de Crisis para lo cual se tratan temas que ayuden a la continuidad del negocio.

2.8.1. Capacitación y concienciación

Como medio de capacitación se ha habilitado para Industrias Karmat un repositorio en el cual se encuentra la información presentada en el proyecto (BIA, estrategias y formatos) con el fin de lograr una comunicación asertiva con cada uno de los involucrados.

Además, se envían emails y se planificaron charlas enfocadas en la concientización sobre la continuidad del negocio, esto busca que el personal asimile y adopten los conceptos que se desean transmitir y así lograr un aporte por parte de ellos.

Se aplicará el siguiente plan de concienciación como se detalla en la Tabla 49.

Tabla 49.

Plan de capacitación y concienciación de Industrias Karmat.

ACCIÓN	TIEMPO EN MESES											
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**
Dia informativo	x											
Capacitaciones		x						x				
Informes en el repositorio		x		x		x		x		x		x
Reuniones conjuntas	x	x	x	x	x	x	x	x	x	x	x	x
Emails	x		x		x		x		x		x	
Encuestas de satisfacción						x						x

El cronograma que se presenta puede estar sujeto a cambios o como le convenga a la empresa para no afectar su correcto funcionamiento.

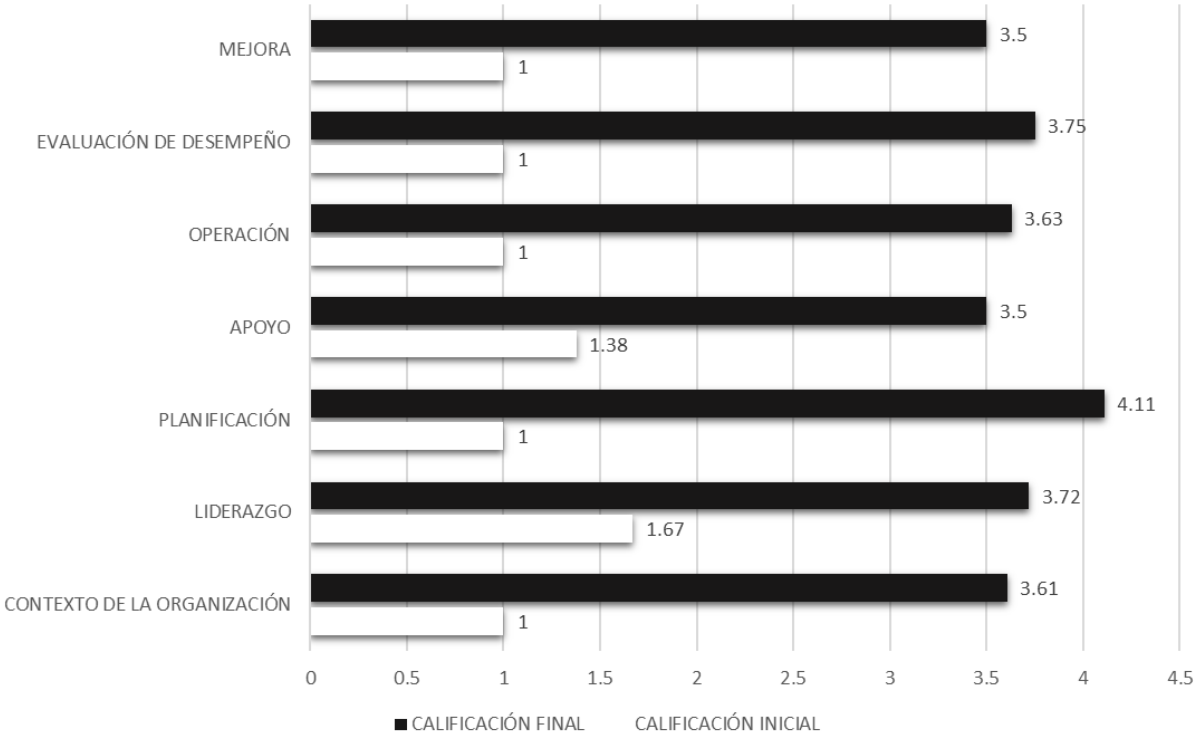
2.9. Diagnóstico de la situación final

En el desarrollo de la norma ISO 22301 se elabora un diagnóstico final, según la encuesta aplicada al personal de la empresa (Anexo D), que busca definir la madurez de la empresa respecto a las acciones tomadas en cuenta.

Para dicho proceso de evaluación se enfoca en el contexto de la organización hasta mejora, para lo cual se asignó un valor que inicia en 1 como en preparación hasta 5 optimizado. En dicho análisis se procede a realizar una estimación de resultados promedios como se representa en la Figura 33.

Figura 33.

Situación Inicial vs Situación Final.



Se puede visualizar un aumento significativo de la actual situación de Industrias Karmat con respecto a su preparación y desarrollo del plan de continuidad del negocio como se puede visualizar en la Tabla 50.

Tabla 50.

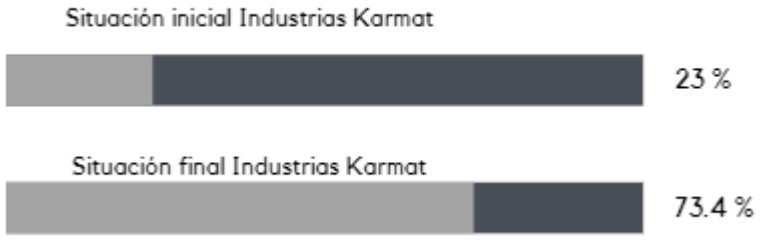
Valor Inicial vs Valor Final.

VALORES	CALIFICACIÓN INICIAL	CALIFICACIÓN FINAL
CALIFICACIÓN GLOBAL	1.15	3.69
PORCENTAJE	23%	73.40%

En la Figura 34, al iniciar el desarrollo del proyecto Industrias Karmat se presenta un 23% de preparación con respecto a la continuidad del negocio mientras una vez aplicado una parte del plan se tiene un valor porcentual del 73.4%.

Figura 34.

Porcentaje calificación inicial vs calificación final.



2.10. Análisis costo – beneficio

Se presenta un presupuesto referencial para la implementación del plan de continuidad del negocio para Industrias Karmat, para la implementación del presente proyecto se analiza los recursos humanos, técnicos materiales y financieros que se relacionen con la ejecución de las estrategias descritas.

2.10.1. Recursos humanos

Para la implementación habrá personal externo a la empresa, ya que se necesita personal competente en Sistemas, para lo que se considerará una referencia de un sueldo mensual de una persona en el área de TIC.

Tabla 51.

Recursos humanos del proyecto.

Cargo	Etapa	Horas de participación	Salario Mensual	Salario Anual
Personal de TI	Implementación AÑO 0[3]	4 horas /día	750.00	4500.00

El salario anual por participación se calcula tomando el salario mensual por los 12 meses y dividiendo por el tiempo de horas de participación. Este valor se considerará en el presupuesto total de recursos humanos como se observa en la Tabla 51.

2.10.2. Recursos técnicos – materiales

Se describirán los recursos necesarios para la implementación, para lo que se considera: pago de licencias, honorarios por asesoría y equipos necesarios.

Los recursos escogidos fueron Database, Servidor Hp, Firewall Hp, Equipos De Uso Personal, Intranet, Data Center, Router los mismos que son considerados como activos críticos para dar continuidad a los procesos de la empresa.

La Tabla 52 se muestra los recursos técnicos materiales necesarios para la implementación del plan de continuidad del negocio.

[3] Año 0: momento en el tiempo donde se realizan las inversiones fijas.

Tabla 52.

Recursos técnicos-materiales.

Recursos necesarios	Costo mensual	Costo año 0	Costo anual
Implementación de equipos (un solo pago)	800.00	800.00	0.00
Adquisición nuevos equipos (un solo pago)	18027.33	18027.33	0.00
Configuración de equipos (un solo pago)	950.00	950.00	0.00
Licencia Database	1200.00	0.00	14400.00
Sitio alterno de almacenamiento	12.50	0.00	150.00
	TOTAL	**19777.33**	**14550.00**

2.10.3. Presupuesto estimado del proyecto

El presupuesto estima un tiempo de 3 años, para lo cual se toma en cuenta los valores de los recursos humanos externos como los recursos técnico-materiales.

Tabla 53.

Proyección de la inversión de recursos.

Elementos de gastos	**Año 0**	**Año 1**	**Año 2**	**Total**
Recursos Humanos Externos	4500.00	4500.00	4500.00	13500.00
Recursos técnico-materiales	19777.33	14550.00	14550.00	48877.33
Total costos BCP Industrias Karmat	**24277.33**	**19050.00**	**19050.00**	**62377.33**

Como se puede apreciar en la Tabla 53, se proyecta una inversión fuerte para el año 0 ya que durante este año se adquirirá equipo por una única vez. La inversión se justificará a continuación.

2.10.4. Relación costo – beneficio

Según (GlobalSuite Solutions, 2023) para realizar la relación costo - beneficio para la implementación del plan de continuidad del negocio, se calculará el Retorno de Inversión (ROI), el cual es un indicador financiero para conocer los resultados de inversión de la empresa, lo que permite conocer las posibles consecuencias financieras, igualmente se calculan los siguientes indicadores financieros como son: flujo de fondos, valor presente neto y tasa interna de retorno.

Para lo cual, en el año 0, se toma en cuenta los costos de sueldos, mercadería y comisiones de 4 meses, tiempo que se demorará la implantación de las estrategias del plan de continuidad del negocio tomando en cuenta los valores correspondientes del año 1 dividido para los 4 meses en los años siguientes se consideró la inflación de 2021 que fue de 3.74%[4]

Con respecto a los sueldos, la empresa tiene 18 empleados, 8 empleados pertenecen al área administrativa y 10 del área de logística, este rubro se cancela 95000.00; los sueldos tienen un aumento anual según la inflación del año anterior (3.74 %).

Con referencia a la adquisición de mercadería para la venta de los artículos se adquirió un valor de 225000.00 por año, para lo cual se aplica una tasa de inflación para los años siguientes.

Se cuenta con un equipo de 152 directoras las cuales reciben una comisión de venta de acuerdo con rangos de venta de su red comercial, este valor anual sería de 15000,00; también se aplica la misma inflación.

La información fue proporcionada por el departamento de contabilidad, no se muestran datos exactos ya que se tiene un acuerdo de confidencialidad, en la Tabla 53 se representan los

[4] Instituto Nacional de Estadística y Censos (INEC). inflación correspondiente del 2021 es de 3.74% según publicación del INEC: https://www.swissinfo.ch/spa/ecuador-inflaci%C3%B3n_ecuador-cerr%C3%B3-diciembre-de-2022-con-una-inflaci%C3%B3n-acumulada-de-3-74--/48186160

valores de costos, ingresos y flujo de fondo de la empresa en los próximos 2 años para lo cual se incluye el costo BCP Industrias Karmat, los ingresos se toman las ventas anuales de ventas en el año 2020 y 2021.

Tabla 54.

Flujo de fondos de Industrias Karmat.

Elementos	Año 0	Año 1	Año 2
Sueldos	23750.00	95000.00	98553.00
Mercadería	56250.00	225000.00	233415.00
Comisiones	3750.00	15000.00	15561.00
BCP Industrias Karmat	24277.33	19050.00	19050.00
Total Costos	108027.33	354050.00	366579.00
Total, Ingresos		500000.00	500000.00
Flujo de fondo (FNE)	**-108027.33**	**145950.00**	**133421.00**

En la Tabla 55 se muestra los indicadores financieros que ayuden a la gerencia en la toma de decisiones para saber si se procede con la implementación del proyecto.

Tabla 55.

Indicadores financieros de rentabilidad.

Indicador	Sigla	Valor
Valor Presente Neto	VPN	171343.67
Tasa Interna de Retorno	TIR	98%
Beneficio	B	1000000.00
Costo	C	828656.33
Relación Costo-Beneficio	B/C	1.21
Retorno de Inversión	ROI	21%

Según la tabla anterior se observa que el TIR que se obtiene es de 98% lo que indica que nos conviene realizar la implementación, y la relación Costo-Beneficio es sumamente aceptable con el 1.21 y al finalizar el ROI demuestra una rentabilidad del 21%.

2.10.5. Análisis de beneficios

Para la implementación del plan de continuidad del negocio se requiere una inversión considerable, dicha implementación es considerada como justificable ya que se evitarían pérdidas económicas por la falta del plan.

Como ejemplo en caso de interrupción de alguno de los activos críticos que generarían perdidas monetarias y por ende la afectación de la imagen corporativa. En 2020 la empresa facturo 500000.00, se divide para el número de días laborables al año (260), obteniendo que la factura diaria es de 1923.08, este valor por hora laborada es de 240.38.

Así se obtiene el valor en caso de interrupción de operaciones si se suscita un evento inesperado si se presenta una interrupción de 5 horas, el valor puede llegar a 1201.92, como se aprecia al contar con un plan de continuidad del negocio se pueden evitar pérdidas monetarias representativas para la empresa.

CAPÍTULO III

3.1. Análisis de requerimientos

Dentro de la visualización de los documentos que formaron parte del plan de continuidad del negocio se busca que se cumpla con los requerimientos que permitan una búsqueda dentro de los documentos almacenados a continuación, se especifican requerimientos:

A continuación, se busca identificar las necesidades del usuario en referencia a las funcionalidades mediante historias de usuario en la Tabla 56.

Tabla 56.

Descripción de historias de usuario.

ID	ROL	DESCRIPCIÓN	PRUEBAS DE ACEPTACIÓN
1	Administrador	Puede cargar y descargar documentos.	Ingresar al repositorio con su cuenta de administración y cargar un archivo en la base de datos. Ingresar al repositorio con su cuenta de administración y descargar un archivo en la base de datos.
2	Administrador	Puede modificar los metadatos asociados a los documentos.	Ingresar al repositorio con su cuenta de administración y modificar los datos como: Titulo, Autor, Fecha, Tema y demás metadatos asociados a los documentos que se encuentren en la base de datos.
3	Usuario	Se debe registrar en el repositorio para el acceso al contenido.	Ingresar al repositorio sin registrarse y comprobar que no cuenta con el acceso para visualizar los documentos. Registrar sus datos como usuario y comprobar su acceso al repositorio.
4	Usuario	Puede consultar todos los documentos que se encuentran en el repositorio.	Ingresar al repositorio con su cuenta de usuario y realizar una consulta.
5	Usuario	Puede ver todo el contenido de los documentos.	Ingresar al repositorio con su cuenta de usuario y comprobar la visualización de los documentos.

6	Usuario	Puede hacer consultas por cualquiera de los metadatos asociados a los documentos.	Ingresar con su cuenta de usuario y realizar consultas por ítems específicos.

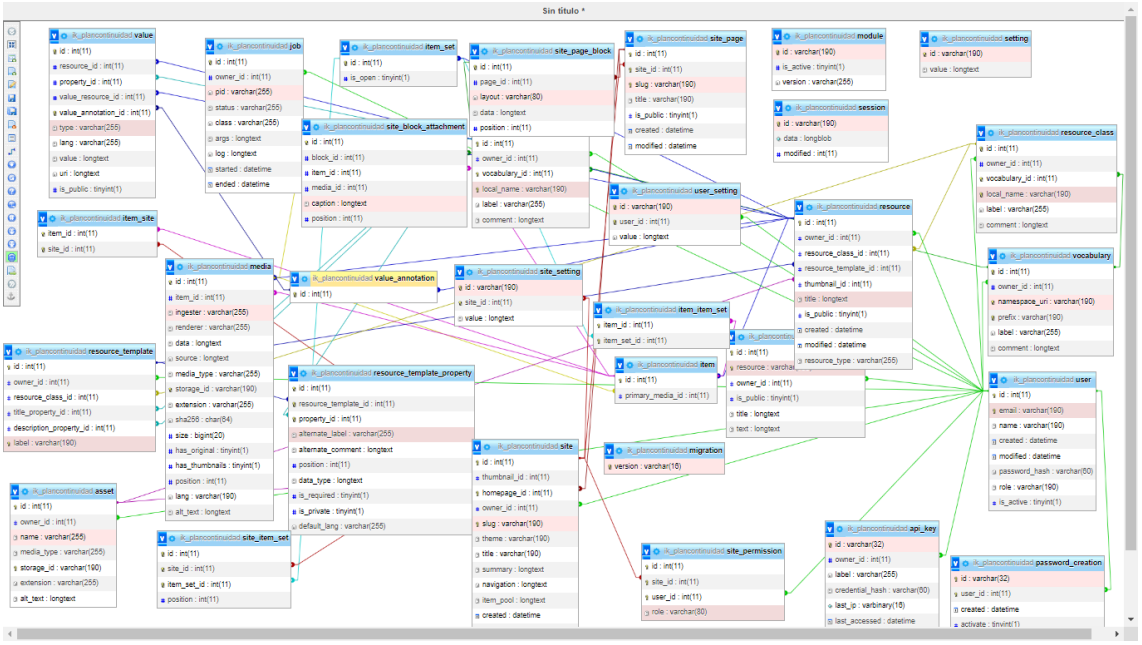
3.2. Diagrama entidad – relación

De acuerdo con (Universidad Autónoma del Estado de Hidalgo, 2020) es un modelo de datos representa la estructura global lógica de la base de datos empleando los tres conceptos básicos: conjuntos de entidades, conjuntos de relaciones y atributos.

En la Figura 35 se observa los elementos anteriormente mencionados, los mismos que conforman la base de datos de la aplicación.

Figura 35.

Diagrama e-r Omeka.

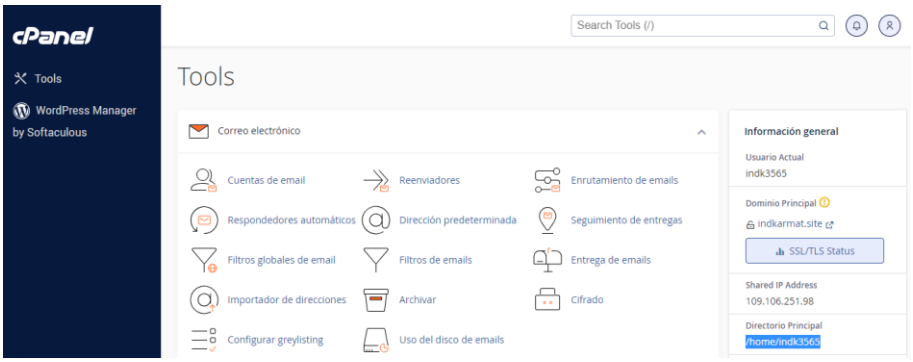


3.3. Configuración de Omeka S

Dentro del panel de control del hosting cargar la base de datos y un archivo tipo .zip del programa como se muestra en la Figura 36.

Figura 36.

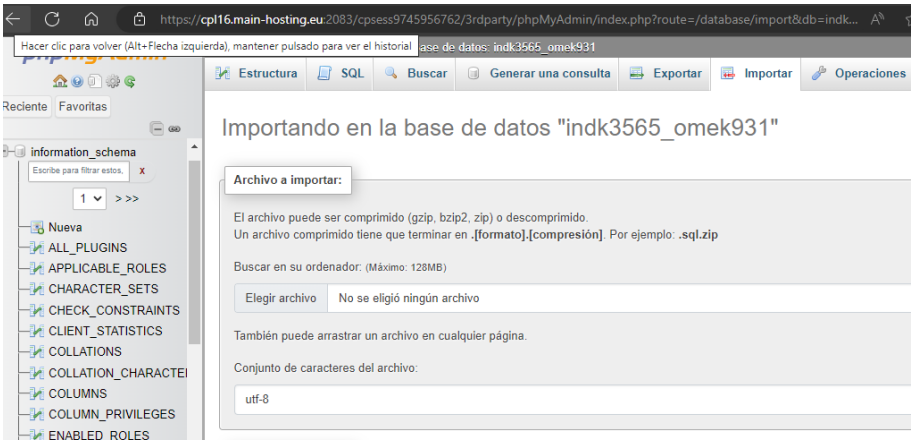
Configuración del entorno cPanel.



Se realiza la importación de la base de datos a través de *phpMyAdmin*, para ello se tiene listo un script con la información de la base de datos como se puede ver en la Figura 37.

Figura 37.

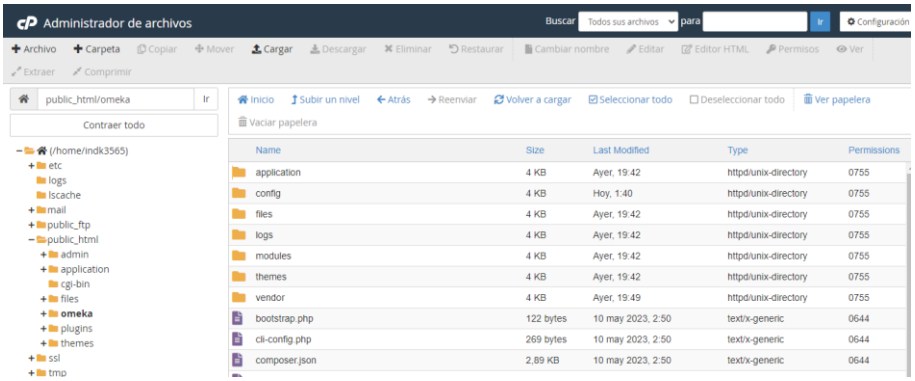
Importación Base de Datos



Una vez subido el archivo se procede a descomprimir el archivo y configurar el archivo de conexión de la base de datos con la información de usuario y base de datos generado por el hosting, como se indica en la Figura 38.

Figura 38.

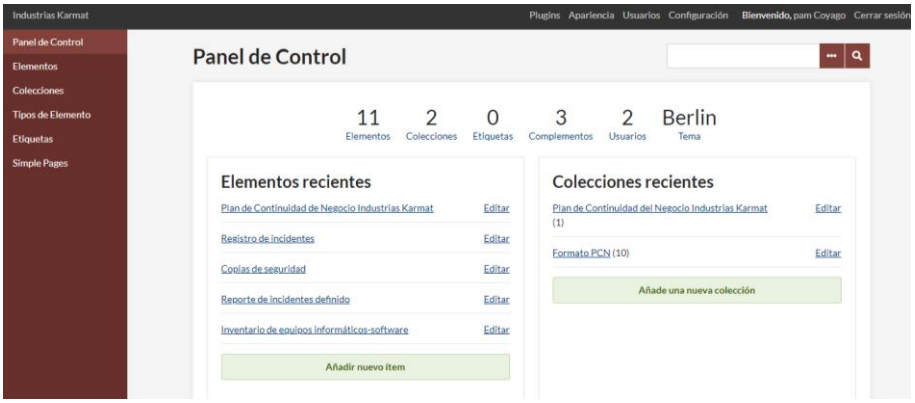
Vista administrador de archivos.



Configuramos nuestro panel de control para lo cual se configura el tema, las colecciones y recursos gráficos de la página como se muestra en la Figura 39 estas opciones solo se encuentran activadas para el Administrador.

Figura 39.

Panel de Control Omeka - Administrador



Se crea las diferentes colecciones en las cuales se van a agrupar cada uno de los elementos que sean añadidos ya sea por el administrador o los otros roles. Ver Figura 40.

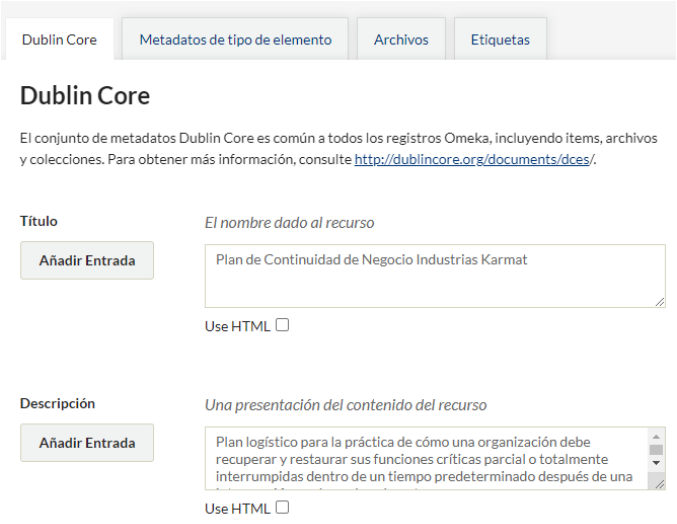
Figura 40.

Creación de colecciones.

Para crear elementos el procedimiento es similar para el administrador y los otros roles, los principales campos que se llenan son: título, descripción corta, autor, fecha y formato, se selecciona la colección a la que pertenece y se guarda. Como se muestra en la Figura 41.

Figura 41.

Creación de un elemento.




Autor
Añadir Entrada
Entidad responsable de la creación del recurso.
Yesenia Coyago
Use HTML
Fecha
Añadir Entrada
Un punto o período de tiempo asociado con un evento en el ciclo de vida del recurso
22/06/2023
Use HTML
Formato
Añadir Entrada
El formato de archivo, medio físico, o dimensiones del recurso
application/pdf
Use HTML
Guardar
Ver la página pública
Eliminar
Público:
Destacado:
Colección
Plan de Continuidad del Negoci

CONCLUSIONES

Este trabajo de investigación desarrolló un marco conceptual referencial para aplicar normas y procesos lo que permitió la generación de una guía para la implementación del plan de continuidad del negocio para Industrias Karmat.

El riesgo acumulado de los activos críticos como son: Database, Servidor Hp, Firewall Hp, Equipos De Uso Personal, Intranet, Data Center y Router de Industrias Karmat es considerado como crítico (7,2); así como el impacto acumulado en calificación de la dimensión de disponibilidad es muy alto obteniendo como calificación 10.

Al inicio la empresa no tenía ningún plan de gestión de riesgos, por lo que su situación inicial fue del 23 %; una vez diseñado y probado el plan de continuidad del negocio se obtiene una mejora del 73,4% en referencia al inicio.

La implementación del plan de continuidad del negocio es un cimiento importante que ayuda a la empresa con la mejora en su plan de negocio y apoya a la visión empresarial que tiene con los diferentes proveedores y entidades bancarias.

Se obtuvo una muy buena experiencia con el uso de la norma ISO22301:2019, sus fases se adaptan a cualquier organización, además de acoplarse muy fácilmente a la Metodología MAGERIT, de esta manera se optimizó el uso del tiempo y recursos; además de permitir que el trabajo conjunto con el personal de Industrias Karmat se pueda analizar correctamente con la herramienta de software EAR/PILAR.

RECOMENDACIONES

Dada las condiciones favorables del entorno, y el hecho de tener una idea del plan de continuidad del negocio clara, se recomienda implementar adicional a este un plan de contingencia TIC o PCTIC y un plan de recuperación ante desastres o PRD.

Se recomienda que además de servicios tecnológicos se analicen las amenazas que se pueden presentar en la empresa como: desastres naturales y desastres financieros sin clasificarse por su nivel de impacto.

El desarrollo del plan de continuidad del negocio no está fuera del alcance de las empresas, no importa el giro del negocio o mercado, el contar con el permite un servicio estable y garantiza mayor confiabilidad en la empresa.

BIBLIOGRAFÍA

Agbodoh-Falschau, K. R., & Ravaonorohanta, B. H. (2023). Investigating the influence of governance determinants on reporting cybersecurity incidents to police: Evidence from Canadian organizations' perspectives. *Technology in Society*, 102309. https://doi.org/10.1016/j.techsoc.2023.102309

Agility Recovery. (2021). *ROI of Business Continuity*. https://www.agilityrecovery.com/webinars/roi-business-continuity

Aguillo, I. F. (2017). *Propuesta de repositorio RECIDA con OMEKA*. https://www.miteco.gob.es/es/ceneam/grupos-de-trabajo-y-seminarios/centros-de-documentacion-ambiental-y-espacios-naturales-protegidos/aguillo-isidro-repositorio-recida-omeka_tcm30-428632.pdf

Alcaraz Martínez, R. (2021). *Construyendo un repositorio digital con Omeka y mucho más: teoría y práctica*.

Allaico Chimborazo, M. M. (2021). *Diseño de un plan de continuidad del negocio en la empresa Cañar Net* [Universidad Católica de Cuenca]. https://dspace.ucacue.edu.ec/bitstream/ucacue/12763/1/ORIGINAL_TESIS_MIRIAN%20Final.pdf

Amara, O. Ben, Kamissoko, D., Fijalkow, Y., & Benaben, F. (2022). Assessing the Business Continuity of a healthcare organization through a data-gathering modality approach. *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2215–2222. https://doi.org/10.1109/SMC53654.2022.9945437

Asano, T., & Nagayama, A. (2021). Analysis of workload required for removal of drifting pumice after a volcanic disaster as an aspect of a port business continuity plan: A case study

of Kagoshima Port, Japan. *International Journal of Disaster Risk Reduction*, *64*, 102511. https://doi.org/10.1016/j.ijdrr.2021.102511

Avila Torres, R. A., & Cuenca Tapia, J. P. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. *Universidad Católica de Cuenca*. https://doi.org/http://dx.doi.org/10.23857/dc.v7i4.2425

Aziz, N. M. A. A., & Jambari, D. I. (2019). Information Management Procedures for Business Continuity Plan Maintenance. *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, 489–495. https://doi.org/10.1109/ICEEI47359.2019.8988804

Bevan, T. (2019). *ISO 22301:2019 Guía de implantación de la continuidad de negocio*.

Biblioteca Universidad de Sevilla. (2017). *Omeka - Manual Básico*. https://bib.us.es/sites/bib3.us.es/files/omeka_manual_usuario.pdf

Brenda D, P., & Mark, L. (2021). Essential tools and resources for business continuity planning. In *Business Continuity Planning* (pp. 179–180). Elsevier. https://doi.org/10.1016/B978-0-12-813844-1.09995-4

British Standards Institution - BSI Group. (2019). *Gestión de continuidad de negocio ISO 22301*. https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

British Standards Institution - BSI Group. (2022a). *BCI Horizon Scan Report 2022*. https://www.bsigroup.com/globalassets/localfiles/en-th/iso-22301/bci-horizon-scan-report/bci-horizon-scan-report-2022-th.pdf

British Standards Institution - BSI Group. (2022b). *Curso de Directrices para la continuidad de la cadena de suministro (ISO/TS 22318:2015)*. https://www.bsigroup.com/globalassets/localfiles/es-es/training/iso-22301/ficha-del-curso-directrices-para-la-continuidad-de-la-cadena---es.pdf

Canca Cuenca, J. (2022). *Plan de continuidad de negocio en las universidades*. Universidad de Castilla.

Cappelo, R. (2020). *Situación Empresarial Ecuador frente al Covid-19*. https://www.andeanecuador.com.ec/dc/es/pages/fas/situacion-empresarial-ecuador.html

Cardinault, C. (2018). *Metodologias usadas en el análisis de riesgos - Curso de Auditoría en Informática*. https://sites.google.com/site/avauditoriaeninformatica/home/modulo-3-tecnicas-y-herramientas-de-la-auditoria-de-sistemas/descripcin-de-las-fases-del-ciclo-de-anlisis-de-riesgos

Centro Criptológico Nacional - CCN. (2023, May 25). *PILAR - Implementación*. Implementación. https://pilar.ccn-cert.cni.es/index.php/metodologia/implementacion

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S. (2014). IT capability and organizational performance: the roles of business process agility and environmental factors. *European Journal of Information Systems*, *23*(3), 326–342. https://doi.org/10.1057/ejis.2013.4

Crespo Martínez, E., & Cordero Torres, G. (2015). *Estudio comparativo entre las metodologías CRAMM y MAGERIT para la gestión de riesgos de ti en las MPYMES.* https://revistas.uazuay.edu.ec/index.php/udaakadem/article/view/129/126

De La Hoz Suárez, B. A., De La Hoz Suárez, A. I., Pérez Suescún, L. F., & Jiménez Sierra, D. (2022). Planes de continuidad de negocios ante el evento disruptivo Covid-19. *Revista Publicando*, *9*(35), 1–18. https://doi.org/10.51528/rp.vol9.id2331

Delfa Baena, S. (2022). *Plan de continuidad del negocio de acuerdo a la norma ISO 22301 de la empresa Formica de Albal (Valencia)*. https://riunet.upv.es:443/handle/10251/185635

Estruga, N. (2021, April 5). *10 normas ISO para la continuidad de negocio*. EALDE Businees School. https://www.ealde.es/normas-iso-continuidad-de-negocio/

Fani, S. V., & Subriadi, A. P. (2019). Business Continuity Plan: Examining of Multi-Usable Framework. *Procedia Computer Science*, *161*, 275–282. https://doi.org/10.1016/j.procs.2019.11.124

Federal Financial Institutions Examination Council's (FFIEC). (2023). *FFIEC IT Examination Handbook InfoBase - Appendix B: Glossary*. https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/appendix-b-glossary.aspx

Fierro Saltos, W. R., Bosquez Barcenes, V. A., & Cárdenas Benavides, J. P. (2018). *Una mirada a los repositorios digitales en Ecuador*. *2*(1), 836–863. https://doi.org/10.26820/reciamuc/2.1.2018.836-863

Figueroa, H., & Salamanca, M. (2013). *Guías para la implementación y auditoría de planes de continuidad de negocio desde la perspectiva de la norma ISO 22301, BS 25999, NTC 5722 y las prácticas profesionales del DRII y de ISACA*. Universidad Piloto de Colombia.

GlobalSuite Solutions. (2023). *ROI en proyectos de Continuidad de Negocio*. Delgado Gallego, Alejandro. https://www.globalsuitesolutions.com/es/roi-proyectos-continuidad-negocio/

González Mendoza, A. M., & Aguilar Juárez, I. (2015). *Situación Actual de los Repositorios Abiertos en México*. www.europeana.eu

Hatton, T., & Brown, C. (2021). Building adaptive business continuity plans: Practical tips on how to inject adaptiveness into continuity planning processes. *Henry Stewart Ublications*, *15*, 1–104.

Hubbard, B. (2022, October 14). *Coste del tiempo de inactividad de servicios: ¿cuánto le cuesta a tu empresa una interrupción informática?* https://blog.invgate.com/es/coste-del-tiempo-de-inactividad-de-servicios

Instituto Nacional de Ciberseguridad, M. de A. E. y T. D. (2020). *Plan de contingencia y continuidad del negocio*. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

International Dynamic Advisors - INTEDYA. (2020). *Introducción a ISO 22301:2019*. 10–11. https://www.intedya.com/productos/IntroduccionISO22301PIC.pdf

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

Kato, M., & Charoenrat, T. (2018). Business continuity management of small and medium sized enterprises: Evidence from Thailand. *International Journal of Disaster Risk Reduction*, *27*, 577–587. https://doi.org/10.1016/j.ijdrr.2017.10.002

Lampe, G. M. M. S. I. I. R. C. (2020). Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis. *6th BASIQ International Conference on New Trends in Sustainable Business and Consumption*, 942–949.

Lojan Granda, E. (2017). Modelo de Evaluación de Gestión de Continuidad del Negocio basado en la norma ISO 22301:2012. *Universidad de Especialidades Espíritu Santo*, 1–22. http://201.159.223.2/handle/123456789/1433

Maldonado Mariño, D. C. (2013). *Gestión de riesgos informáticos para la protección de los sistemas de información en la Cooperativa de Ahorro y Crédito Campesina COOPAC*

[Universidad Regional Autónoma de los Andes “UNIANDES”]. https://dspace.uniandes.edu.ec/handle/123456789/4522

Marcillo Baque, A. G. (2017). *Propuesta para el desarrollo de un SGSI basado en la norma ISO 27001*. https://docplayer.es/85952413-Universidad-de-guayaquil-facultad-de-ingenieria-industrial.html

Ministerio de Hacienda y Administración Públicas. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. https://www.pilar-tools.com/doc/magerit/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, & Vive Digital Colombia. (2015). *Guía para realizar al Análisis de Impacto de Negocios BIA*.

Monica, R., Henry, Q., Estela, M., & Washington, F. (2020). Why implement continuity plans in Organizations? Approach of a prospective study based on ITIL. *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*, 1–5. https://doi.org/10.1109/ISCV49265.2020.9204335

Mukherjee, M., Chatterjee, R., Khanna, B. K., Dhillon, P. P. S., Kumar, A., Bajwa, S., Prakash, A., & Shaw, R. (2020). Ecosystem-centric business continuity planning (eco-centric BCP): A post COVID19 new normal. *Progress in Disaster Science*, *7*, 100117. https://doi.org/10.1016/j.pdisas.2020.100117

Network Coverage. (2021). *Average Cost of Data Loss & Data Center Outages*.

O’Neill, J. L. (2017). Deploying a WordPress-based learning object repository to scale up instruction and effect a culture of sharing. *Reference Services Review*, *45*(1), 131–140. https://doi.org/10.1108/RSR-10-2016-0059

Pacheco Fernández, A. E., Suarez Santamaría, L. I., & González Chacón, J. H. (2021). *Aplicar la Metodología OCTAVE de identificación de amenazas y vulnerabilidades en una entidad bancaria*. https://proyectosmaestrias.virtual.uniandes.edu.co/images/mlC4bCJ5XSVNmWQUD6uN4V2gJFMiZDbyVCkn22QE.pdf

Peña F, L. M. (2019). *Omeka: un gestor de contenido para bibliotecas digitales muy fácil de instalar y utilizar*. https://www.apachefriends.org/es/download.html

Petrenko, S. (2021). Developing an Enterprise Continuity Program. *Developing an Enterprise Continuity Program*.

Phillips, B. D., & Landahl, M. (2021). What is business continuity planning? In *Business Continuity Planning* (pp. 1–24). Elsevier. https://doi.org/10.1016/B978-0-12-813844-1.00009-9

Phillips D, B., & Landahi, M. (2021). *Business Continuity Planning: Increasing Workplace Resilience to Disasters*.

Pilar. (2021). *PILAR - Manual de Usuario (2021.1)*. http://java.com]

Pinto, D., Fernandes, A., da Silva, M. M., & Pereira, R. (2022). Maturity Models for Business Continuity-A Systematic Literature Review. *International Journal of Safety and Security Engineering*, *12*(1), 123–136. https://doi.org/10.18280/ijsse.120115

Programa de las Naciones Unidas para el Desarrollo - PNUD, & Ministerio de Industria Comercio y Mipymes - MICM. (2020). *Plan de continuidad del negocio - PCN Documento Conceptual*.

Quintero Villarroya, J. L. (2012). *Análisis y gestión de riesgos - Herramienta Pilar*. https://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128

Real Academia Española - RAE. (2023). *Diccionario de la lengua española | RAE - ASALE*. https://dle.rae.es/riesgo?m=form

Rivera Gómez, A. C. (2009). *Creación de un repositorio digital con la producción intelectual de la Dra. María Eugenia Bozzoli Vargas, en el laboratorio de etnología de la Universidad de Costa Rica*. Universidad de Costa Rica.

Rodríguez Gairín, J. M., & Sulé Duesa, A. (2008). *DSpace: un manual específico para gestores de la información y la documentación*. https://bid.ub.edu/20rodri2.htm

Roush, K., Opsahl, A., Parker, K., & Davis, J. (2021). Business Continuity Planning: An Effective Strategy During an Electronic Health Record Downtime. *Nurse Leader*, *19*(5), 525–531. https://doi.org/10.1016/j.mnl.2021.01.003

Rozova, D., & Fuchs, M. (2021). Business Continuity Management Through Stakeholders Collaboration and Participation. *2021 New Trends in Aviation Development (NTAD)*, 146–149. https://doi.org/10.1109/NTAD54074.2021.9746265

Russo, N., São Mamede, H., Reis, L., & Silveira, C. (2022). FAMMOCN – Demonstration and evaluation of a framework for the multidisciplinary assessment of organizational maturity on business continuity. *Heliyon*, *8*(9), e10566. https://doi.org/10.1016/j.heliyon.2022.e10566

Sánchez Contreras, A. (2015). *Metodología o herramientas para el análisis y gestión de riesgos CRAMM*. https://slideplayer.es/slide/5503051/

Saxena, M. M., & Srinivas Rao, K. (2019). Quality Management, Total Quality Management and Six Sigma. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, *8*. www.ijstr.org

Servicio Ecuatoriano de Normalización - INEN. (2017). *Protección y Seguridad de la Ciudadanía - Sistema de Gestión de Continuidad del Negocio - Directrices (ISO 22313:2012, IDT)*.

Shulmistra, D. (2022, June 13). *The Ultimate: Business Continuity Plan, Guide Template & FAQ [2022]*. https://invenioit.com/continuity/business-continuity-plan-guide-template-faq/

RESOLUCIÓN Nro. SB-2021-2126, 1 (2021).

Universidad Autónoma del Estado de Hidalgo. (2020). *Diseño de Base de Datos*. Instituto de Ciencias Básicas e Ingeniería. http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro14/index.html

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a review literature. In *MIS Quarterly* (Vol. 26, Issue 2). http://www.misq.org/misreview/announce.html

Xiang, W., Wang, Y., & Zhang, Z. (2023). *The Research on Business Continuity Planning of E-government Based on Information Security Risk Management*.

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

ANEXOS

Anexo A. Valoración inicial del plan de continuidad del negocio ISO 22301.

Diagnóstico de la situación actual de la gestión de la continuidad de negocio ISO 22301.

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:

A. Cumple del todo con la cláusula enunciada (5.00 puntos: Optimizado);

B. Cumple relativamente con la cláusula enunciada (4.00 puntos: Administrado);

C. Cumple con el mínimo de la cláusula enunciada (3.00 puntos: Establecido);

D. Cumple parcialmente con la cláusula enunciada (2.00 puntos: Básico).

E. No cumple con la cláusula enunciada (1.00 puntos: En preparación

CLÁUSULA	CALIFICACIÓN INICIAL
CONTEXTO DE LA ORGANIZACIÓN	1.00
Establecimiento de aspectos y factores internos y externos del SGCN	1.00
¿La organización cuenta con un listado de procesos y servicios?	1.00
¿Existe una clasificación de procesos y servicios en críticos, estratégicos o de apoyo?	1.00
¿Existe una política documentada de recuperación ante desastres?	1.00
¿Se ha definido aspectos del SGCN en relación con política de continuidad, objetivos y criterios?	1.00
Definición y establecimiento de las necesidades y expectativas de las partes interesadas	1.00
¿El personal conoce los requerimientos legales y la normativa requerida dentro de un SGCN?	1.00
¿Se revisa de manera constante información sobre las partes interesadas y sus requerimientos?	1.00
Alcance del SGCN	1.00
¿Existe un alcance documentado dentro de la organización para la continuidad del negocio?	1.00

¿Se ha definido los requisitos y aplicabilidad de un SGCN dentro de la organización?	1.00
Administración del Sistema de Continuidad del Negocio	1.00
¿La organización ha establecido un SGCN y ha realizado las revisiones periódicas?	1.00
LIDERAZGO	1.67
Compromiso, apoyo, patrocinio y gestión por parte de los ejecutivos y la alta gerencia al SGCN	3.00
¿La alta dirección ha mostrado interés y apoyo en el establecimiento e implementación del SGCN?	3.00
Establecimiento y comunicación de la política de continuidad al interior de toda la organización	1.00
¿La alta dirección ha establecido y comunicado políticas, normativa legal y el reglamento interno para su debido cumplimiento?	1.00
¿La alta dirección ha establecido una política de continuidad del negocio apropiada a la organización y su contexto?	1.00
¿Existen acuerdos que permitan el acceso del personal a la red interna de la organización generados desde la alta dirección?	1.00
Asegurar la definición de roles, responsabilidad, autoridad y rendición de cuentas del SGCN	1.00
¿La alta dirección ha designado roles y ha definido de manera clara las responsabilidades del personal dentro de la organización?	1.00
¿La alta dirección ha documentado los planes de contingencia existentes y ha designado responsables de su ejecución?	1.00
PLANIFICACIÓN	1.00
Identificación y determinación oportuna de riesgos y oportunidades	1.00
¿Se han identificado los posibles riesgos y oportunidades dentro de la organización?	1.00
¿Existe planes para reducir o prevenir la materialización de los riesgos?	1.00
¿Existe un plan para el tratamiento de riegos?	1.00

Alineación estratégica para prevenir efectos y evaluar acciones	1.00
¿Existe planificación previa para la realización de cambios?	1.00
¿Se emiten informes posteriores a los cambios realizados?	1.00
¿Se realizan evaluaciones periódicas a los cambios realizados?	1.00
Definición de los objetivos del SGCN alineados a los planes y estrategias	1.00
¿Dentro de la organización, se han establecido objetivos que garanticen la continuidad del negocio?	1.00
¿Existen procesos enfocados en mantener operativas las actividades?	1.00
APOYO	1.38
Determinar y proporcionar los recursos necesarios para atender el SGCN	2.50
¿Existen los recursos necesarios para implementar un SGCN?	4.00
¿Se ha considerado las capacidades y limitantes de los recursos dentro de la organización?	1.00
Recursos que cuentan con competencia, habilidades, experiencia y toma de conciencia para el SGCN	1.00
¿Existe un proceso definido que determine las competencias del personal en relación con la continuidad del negocio?	1.00
¿Se realiza evaluaciones al personal para determinar sus capacidades profesionales?	1.00
¿Se ha realizado el proceso de concienciación al personal sobre la importancia de la continuidad del negocio?	1.00
¿El personal comprende de manera clara las implicaciones de la interrupción de las actividades?	1.00
Dispone de mecanismos de comunicación interna y externa, quien, cuándo, dónde y procedimientos	1.00
¿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?	1.00
¿Se realizan pruebas de validación al proceso que permite la comunicación durante la interrupción de las actividades dentro de la organización?	1.00
Información documentada del SGCN (creación, actualización, control)	1.00

¿La organización mantiene la información documentada siguiendo un estándar?	1.00
¿La información documentada tiene identificación, descripción, fecha, autor, control de cambios?	1.00
¿Existe control de acceso a la información confidencial?	1.00
¿La información documentada se mantiene como evidencia de la conformidad y protegida contra modificaciones no autorizadas?	1.00
OPERACIÓN	1.00
Definición, evaluación y administración de riesgos y análisis de impacto al negocio BIA	1.00
¿Dentro de la organización existe un procedimiento para realizar el análisis de impacto y la evaluación de riesgos?	1.00
¿Los resultados obtenidos en la evaluación de riesgos, son comunicados al personal?	1.00
¿Se han establecido planes para el tratamiento de los riesgos?	1.00
¿Se monitorean y evalúan periódicamente el plan de tratamiento de riesgos?	1.00
Diseño, determinación y administración de estrategias DRP y BCP para todo el SGCN	1.00
¿La organización ha definido estrategias para la continuidad del negocio?	1.00
¿Se han adoptado medidas para reducir interrupciones ocasionadas por amenazas materializadas?	1.00
¿Se han definido los tiempos máximos de inoperatividad a causa de un incidente?	1.00
Procedimientos del SGCN, administración y respuesta a incidentes	1.00
¿La organización ha establecido procedimientos para asegurar la continuidad del negocio ante un incidente?	1.00
¿La organización ha definido planes de recuperación de desastres o de contingencia?	1.00
Definición, ejecución y evaluación de ejercicios y pruebas al SGCN	1.00
¿Dentro de la organización se realizan planes de pruebas y verificación?	1.00

¿Se han definido los distintos escenarios de incidentes?	1.00
¿La alta dirección forma parte en la realización de pruebas y verificaciones?	1.00
¿Se documenta el resultado de pruebas para posteriormente socializarlo?	1.00
EVALUACIÓN DE DESEMPEÑO	1.00
Evaluación y medición de todo el procedimiento de continuidad del negocio	1.00
¿Se realiza el monitoreo y evaluación a los diferentes procesos?	1.00
¿Se documenta los resultados del monitoreo y evaluaciones de los procesos?	1.00
¿Se ha establecido un periodo de tiempo en la evaluación de los procesos?	1.00
Realización y cumplimiento de auditorías internas planificadas	1.00
¿Dentro de la organización se llevan a cabo auditorías programadas?	1.00
¿Previo a una auditoría se definen los criterios y el alcance?	1.00
¿Los resultados posteriores a la auditoria son comunicados a los responsables de los procesos?	1.00
¿La organización toma en consideración las recomendaciones que surgen posterior a la auditoría?	1.00
Revisión y evaluación de la gerencia al SGCN	1.00
¿Se revisa periódicamente los procesos, procedimientos para garantizar la continuidad de las operaciones dentro de la organización?	1.00
¿La alta dirección revisa constantemente el cumplimiento de los objetivos de la organización?	1.00
MEJORA	1.00
Identificación, monitoreo y solución de no conformidades y acciones correctivas	1.00
¿Se comunican las no conformidades al personal responsable para determinar mejorar las estrategias definidas?	1.00
¿Se ha establecido un periodo de tiempo para subsanar las no conformidades?	1.00

¿Las acciones correctivas y de mejora con documentadas?	1.00
Mejora continua asociada al mantenimiento, actualización y conciencia sobre SGCN	1.00
¿Las revisiones periódicas han permitido mantener la continuidad de las operaciones?	1.00
CALIFICACIÓN GLOBAL	1.15
DESCRIPCIÓN CALIFICACIÓN GLOBAL	En preparación

Anexo B. Mesa de trabajo

MESA DE TRABAJO

INDUSTRIAS KARMAT

CRITERIOS Y VALORACIÓN PARA LOS ACTIVOS

Fecha: 17 de mayo de 2023 **Lugar:** Miguel Alban Paliz 1-92

Hora de inicio: 9:00am **Hora de finalización:** 12:00pm

Objetivos:

- Definir los criterios de valoración para los activos de acuerdo con la metodología Magerit.
- Definir el valor de cada activo en base a los criterios anteriormente definidos.

Criterios de valoración:

Para el desarrollo del presente estudio, se definirá como valoración al tipo cualitativo ya que este permite la asignación de un valor a los activos, de esta manera se puede definir una escala de acuerdo con el siguiente detalle:

Por favor responda a las siguientes preguntas, tomando en cuenta los siguientes parámetros:

Despreciable	Bajo	Medio	Alto	Muy alto	Extremo
0	1-2	3-5	6-8	9	10

¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

- **DISPONIBILIDAD**

Información que no se encuentre accesible durante **un periodo de tiempo mínimo (30 min)** podría impedir el desarrollo de las actividades de Industrias Karmat.	10
Información que no se encuentre accesible durante un **periodo de tiempo prolongado (60 min)** podría impedir el desarrollo de las actividades de Industrias Karmat.	9

Información que no se encuentre accesible durante **una jornada laboral** podría impedir el desarrollo de las actividades de Industrias Karmat.	6-8
Información que no se encuentre accesible durante **días (2 – 4 días)** podría impedir el desarrollo de las actividades de Industrias Karmat.	3-5
Información que no se encuentre accesible durante **una semana (5 días laborables)** podría impedir el desarrollo de las actividades de Industrias Karmat.	1-2
Información que no se encuentre accesible no afecte a las actividades de Industrias Karmat.	0

¿Qué daño causaría que lo conociera quien no debe?

- **CONFIDENCIALIDAD**

Información puede ser conocida **por pocas personas** y en caso de divulgación esta podría causar prejuicios en el desarrollo de las actividades de Industrias Karmat.	10
Información puede ser conocida **por un grupo de personas muy reducido** y en caso de divulgación esta podría causar prejuicios en el desarrollo de las actividades de Industrias Karmat.	9
Información puede ser conocida **por los usuarios** y en caso de divulgación o mal uso esta podría causar inconvenientes en el desarrollo de las actividades de Industrias Karmat.	6-8
Información que puede **ser conocida por los usuarios** de Industrias Karmat.	3-5
Información **que puede ser conocida y maneja por los usuarios o personal** de Industrias Karmat.	1-2

Información que puede **ser conocida y usada sin ningún tipo de autorización** de Industrias Karmat tanto internamente como externamente.	0

¿Qué perjuicio causaría que estuviera dañado o corrupto?

- **INTEGRIDAD**

Información que se encuentre modificada sin la debida autorización que **no podría repararse** lo que impediría el desarrollo de las actividades de Industrias Karmat.	10
Información que se encuentre modificada sin la debida autorización que **sea muy difícil de recuperarse** lo que impediría el desarrollo de las actividades de Industrias Karmat.	9
Información que se encuentre modificada sin la debida autorización que **sea difícil de recuperarse** lo que impediría el desarrollo de las actividades de Industrias Karmat.	6-8
Información que se encuentre modificada sin la debida autorización **que no permita el desarrollo** correcto de las actividades de Industrias Karmat.	3-5
Información que se encuentre modificada sin la debida autorización que **se pueda recuperar** lo que impediría el desarrollo de las actividades durante un corto periodo dentro de Industrias Karmat.	1-2
Información que se encuentre modificada sin la debida autorización **sea de fácil recuperación o que no afecte** en el correcto desarrollo de las actividades de Industrias Karmat.	0

¿Qué perjuicio causaría que fuese suplantado o falsificado?

- **AUTENTICIDAD**

Información que pueda **accederse a otras personas sin permisos** impidiendo las actividades de Industrias Karmat.	10
Información que pueda **accederse a otras personas sin permisos** causando prejuicio sobre las actividades de Industrias Karmat.	9
Información que pueda **accederse a otras personas sin permisos** conociendo información que cause prejuicio sobre las actividades de Industrias Karmat.	6-8
Información que pueda **accederse a otras personas sin permisos** conociendo información que cause daños sobre Industrias Karmat.	3-5
Información que pueda **accederse a otras personas sin permisos** conociendo información que cause un daño mejor sobre Industrias Karmat.	1-2
Información que pueda **accederse a otras personas sin permisos** conociendo información que no cause un daño sobre Industrias Karmat.	0

¿Qué daño causaría no saber quién accede a qué datos?

- **TRAZABILIDAD**

Registro deficiente de usuarios que **han accedido a información y no sé conoce a cuál de ella accedió o que información manipulo** sin permisos impidiendo las actividades de Industrias Karmat.	10
Registro deficiente de usuarios que **han accedido a información y no sé conoce a cuál de ella accedió o que información manipulo** sin permisos impidiendo las actividades de Industrias Karmat.	9

Registro deficiente de usuarios que **han accedido a información y sé conoce a cuál de ella accedió o que información** sin permisos impidiendo las actividades de Industrias Karmat.	6-8
Registro parcial de usuarios que **han accedido a información y registro de información manipulada** de Industrias Karmat.	3-5
Registro completo de usuarios que **han accedido a información** de Industrias Karmat.	1-2
Registro completo de usuarios que **han accedido a información y registro de información manipulada** de Industrias Karmat.	0

Valoración de activos

De acuerdo con la mesa de trabajo se pudo valor los activos que son de propiedad de la empresa para lo cual se analizó cada propiedad de la seguridad tomando en cuenta el análisis de sus funciones y su importancia, de acuerdo con los criterios anteriormente analizados obteniendo de esta manera la siguiente tabla:

ACTIVOS INDUSTRIAS KARMAT							
CÓDIGO	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	VALOR	DATOS PERSONALES
Aplicaciones							
IK000 DATABASE	9	9	6	9	8	8	3

IK0005 PAGINA WEB	8	7	5	5	5	5	1
IK0008	5	8	8	8	4	3	6
Equipos							
IK 0001 SERVIDOR HP	10	7	7	8	2	5	1
IK0002 FIREWALL HP	10	9	8	7	5	1	2
IK0003 CENTRAL TELEFÓNICA	9	7	6	4	1	5	1
IK0004 EQUIPOS DE USO PERSONAL	9	7	6	4	1	5	1
IK0006 IMPRESORAS	8	6	6	6	1	4	4
IK0007 INTRANET	10	9	7	09	6	8	4

Damos conocer el acta firmada de la mesa de trabajo del miércoles, 17 de abril de 2023, en la cual se llevó a cabo:

- Definición de los criterios de valoración para los activos de acuerdo con la metodología Magerit.

Definición del valor de cada activo en base a los criterios **DISPONIBILIDAD, CONFIDENCIALIDAD, INTEGRIDAD, AUTENTICIDAD, TRAZABILIDAD**

Siendo parte de esta mesa de trabajo Ing. Gabriela Pilataxi Gerente General de Industrias Karmat y Srta. Yesenia Coyago autor del presente proyecto de trabajo de grado.

Ing. Gabriela Pilataxi
Gerente General Industrias Karmat

Srta. Yesenia Coyago
Tesista

INDUSTRIAS KARMAT
pielactive
VENTA POR CATALOGO

Anexo C. Valoración de amenazas

[IK] A.2. Amenazas > A.2.3. valoración

itar Exportar Importar TSV

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS							
[B] Activos esenciales							
[IS] Servicios internos							
[E] Equipamiento							
[SW] Aplicaciones							
S [IK0000] DATABASE			100%	100%	100%		50%
[I.5.1] Avería de origen lógico		1	50%				
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	10%	50%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.22] Manipulación de programas		1	50%	100%	100%		
I [IK0005] PAGINA WEB			100%	100%	100%		50%
[I.5.1] Avería de origen lógico		1	50%				
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	10%	50%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.22] Manipulación de programas		1	50%	100%	100%		
S [IK0008] MAIL			100%	100%	100%		50%
[I.5.1] Avería de origen lógico		1	50%				
[E.8] Difusión de software dañino		1	10%	10%	10%		
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%		
[E.21] Errores de mantenimiento / actualización de programas (software)		10	1%	10%	50%		
[A.8] Difusión de software dañino		1	100%	100%	100%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.22] Manipulación de programas		1	50%	100%	100%		
[HW] Equipos							
S [IK0001] SERVIDOR HP			100%	10%	50%		50%
[I.5.2] Avería de origen físico		1	50%				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.24] Denegación de servicio		2	100%				

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
S [IK0002] FIREWALL HP			100%	10%	100%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	100%		100%		
[A.7] Uso no previsto		1	1%	1%	10%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	100%		100%		
[A.26] Ataque destructivo		1	100%				

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
S [IK0003] CENTRAL TELEFÓNICA			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	100%		50%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	100%		50%		
[A.26] Ataque destructivo		1	100%				

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]
S [IK0004] EQUIPOS DE USO PERSONAL			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		5	5%		10%		
[A.7] Uso no previsto		1	10%	1%	10%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		5	5%		10%		
[A.26] Ataque destructivo		1	100%				
S [IK0006] IMPRESORAS			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.25] Pérdida de equipos		1	100%		50%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	100%		50%		
[A.26] Ataque destructivo		1	100%				
S [IK0007] INTRANET			100%	10%	50%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				
[I.5.2] Avería de origen físico		1	50%				
[I.6] Corte del suministro eléctrico		1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)		1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)		1	10%				
[E.24] Caída del sistema por agotamiento de recursos		10	50%				
[E.25] Pérdida de equipos		1	100%		50%		
[A.11] Acceso no autorizado		1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)		1					50%
[A.23] Manipulación del hardware		0,5	50%		50%		
[A.24] Denegación de servicio		2	100%				
[A.25] Robo de equipos		0,5	100%		50%		
[A.26] Ataque destructivo		1	100%				
S [IK0009] DATA CENTER			100%	10%	100%		50%
[N.1] Fuego		0,1	100%				
[N.2] Daños por agua		0,1	50%				
[N.*] Desastres naturales		0,1	100%				
[I.1] Fuego		0,5	100%				
[I.2] Daños por agua		0,5	50%				
[I.*] Desastres industriales		0,5	100%				
[I.3] Contaminación medioambiental		0,1	50%				
[I.4] Contaminación electromagnética		1	10%				

[I.5.2] Avería de origen físico	1	50%					
[I.6] Corte del suministro eléctrico	1	100%					
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%					
[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					
[E.24] Caída del sistema por agotamiento de recursos	10	50%					
[E.25] Pérdida de equipos	0,1	100%		100%			
[A.7] Uso no previsto	1	1%	1%	10%			
[A.11] Acceso no autorizado	1	10%	10%	50%			
[A.13] Repudio (negación de actuaciones)	1					50%	
[A.23] Manipulación del hardware	0,5	50%		50%			
[A.24] Denegación de servicio	2	100%					
[A.25] Robo de equipos	0,1	100%		100%			
[A.26] Ataque destructivo	1	100%					
[COM] Comunicaciones							
[IK0010] ROUTER		100%	10%	50%		50%	
[N.1] Fuego	0,1	100%					
[N.2] Daños por agua	0,1	50%					
[N.*] Desastres naturales	0,1	100%					
[I.1] Fuego	0,5	100%					
[I.2] Daños por agua	0,5	50%					
[I.*] Desastres industriales	0,5	100%					
[I.3] Contaminación medioambiental	0,1	50%					
[I.4] Contaminación electromagnética	1	10%					
[I.5.2] Avería de origen físico	1	50%					
[I.6] Corte del suministro eléctrico	1	100%					
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%					
[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					
[E.24] Caída del sistema por agotamiento de recursos	10	50%					
[E.25] Pérdida de equipos	1	20%		50%			
[A.7] Uso no previsto	1	10%		10%			
[A.11] Acceso no autorizado	1	10%	10%	50%			
[A.13] Repudio (negación de actuaciones)	1					50%	
[A.23] Manipulación del hardware	0,5	100%		50%			
[A.24] Denegación de servicio	2	100%					
[A.25] Robo de equipos	0,5	20%		50%			
[A.26] Ataque destructivo	1	100%					
[IK0011] CAMARAS		100%	20%	50%	100%	50%	
[N.1] Fuego	0,1	100%					
[N.2] Daños por agua	0,1	50%					
[N.*] Desastres naturales	0,1	100%					
[I.1] Fuego	0,5	100%					
[I.2] Daños por agua	0,5	50%					
[I.*] Desastres industriales	0,5	100%					
[I.3] Contaminación medioambiental	0,1	50%					
[I.4] Contaminación electromagnética	1	10%					
[I.5.2] Avería de origen físico	1	50%					
[I.6] Corte del suministro eléctrico	1	100%					
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%					
[I.8] Fallo de servicios de comunicaciones	1	50%					
[I.11] Emanaciones electromagnéticas (TEMPEST)	1			1%			
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%			
[E.9] Errores de [re-]encaminamiento	1			10%			
[E.10] Errores de secuencia	1		10%				
[E.15] Alteración de la información	1		1%				
[E.19] Fugas de información	1			10%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%					
[E.24] Caída del sistema por agotamiento de recursos	10	50%					
[E.25] Pérdida de equipos	1	20%		50%			
[A.5] Suplantación de la identidad	1		10%	50%	100%		
[A.7] Uso no previsto	1	10%	10%	10%			
[A.9] [Re-]encaminamiento de mensajes	1			10%			
[A.10] Alteración de secuencia	1		10%				
[A.11] Acceso no autorizado	1	10%	10%	50%	100%		
[A.12] Análisis de tráfico	1			2%			
[A.13] Repudio (negación de actuaciones)	1					50%	
[A.14] Interceptación de información (escucha)	1			10%			
[A.15] Modificación de la información	1		10%				
[A.18] Destrucción de la información	1	50%					
[A.23] Manipulación del hardware	0,5	100%		50%			
[A.24] Denegación de servicio	10	100%					
[A.25] Robo de equipos	0,5	20%		50%			
[A.26] Ataque destructivo	1	100%					

activo		co...	frecuencia	[D]	[I]	[C]	[A]	[T]
[IK0012] SWITCHES				100%	10%	50%		50%
[N.1] Fuego			0,1	100%				
[N.2] Daños por agua			0,1	50%				
[N.*] Desastres naturales			0,1	100%				
[I.1] Fuego			0,5	100%				
[I.2] Daños por agua			0,5	50%				
[I.*] Desastres industriales			0,5	100%				
[I.3] Contaminación medioambiental			0,1	50%				
[I.4] Contaminación electromagnética			1	10%				
[I.5.2] Avería de origen físico			1	50%				
[I.6] Corte del suministro eléctrico			1	100%				
[I.7] Condiciones inadecuadas de temperatura o humedad			1	100%				
[I.11] Emanaciones electromagnéticas (TEMPEST)			1			1%		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)			1	10%				
[E.24] Caída del sistema por agotamiento de recursos			10	50%				
[E.25] Pérdida de equipos			1	20%		50%		
[A.7] Uso no previsto			1	10%		10%		
[A.11] Acceso no autorizado			1	10%	10%	50%		
[A.13] Repudio (negación de actuaciones)			1					50%
[A.23] Manipulación del hardware			0,5	100%		50%		
[A.24] Denegación de servicio			2	100%				
[A.25] Robo de equipos			0,5	20%		50%		
[A.26] Ataque destructivo			1	100%				
[AUX] Elementos auxiliares								
[SS] Servicios subcontratados								
[L] Instalaciones								
[P] Personal								
[U0001] PERSONAL				10%	50%	10%		50%
[E.15] Alteración de la información			1		10%			
[E.18] Destrucción de la información			1	1%				
[E.19] Fugas de información			1			10%		
[A.13] Repudio (negación de actuaciones)			1					50%
[A.15] Modificación de la información			1		50%			
[A.18] Destrucción de la información			1	10%				
[A.19] Revelación de información			5			10%		
[A.28] Indisponibilidad del personal			0,1	10%				
[A.29] Extorsión			0,9	10%	10%	10%		
[A.30] Ingeniería social (picaresca)			1	10%	10%	10%		

Anexo D. Valoración final del plan de continuidad del negocio ISO 22301.

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	
CLÁUSULA	**CALIFICACIÓN FINAL**
CONTEXTO DE LA ORGANIZACIÓN	3.61
Comprensión de la organización y de su contexto	4.00
¿La organización ha identificado cuales pueden ser los problemas internos y externos que alterarían la operatividad del negocio?	4.00
¿La organización ha identificado cuanto nivel de riesgo podría hacerse cargo ante un posible evento adverso?	4.00
Comprensión de las necesidades y expectativas de las partes interesadas	3.50
¿La organización ha identificado a las stakeholder(partes interesadas) significativas que influyen directamente en la Continuidad del Negocio?	4.00
¿La empresa ha identificado los requisitos relevantes de las partes interesadas?	3.00
¿Cuentan con un proceso que tenga la finalidad de reconocer, permitir y examinar las condiciones legales y reglamentarias que tengan que ver con la Continuidad de Negocio?	4.00
¿Se encuentra documentado el procedimiento, las condiciones legales y reglamentarias concernientes?	3.00
Determinación del alcance del sistema de gestión de la continuidad de negocio	3.33
¿Los servicios ofertados por la organización se encuentran disponibles en la documentación para las partes de la organización que tienen que ver con la Continuidad de Negocio?	3.00
¿Fueron documentadas y aprobadas por las partes (personal) de la organización que no tienen que ver con la Continuidad de Negocio?	4.00
¿El alcance de la Continuidad de Negocio se encuentra claramente definido y documentado?	3.00
LIDERAZGO	3.72

Liderazgo y compromiso de la Gerencia	3.50
¿Existe un compromiso y liderazgo notorio de parte de la empresa con respecto a la Continuidad de Negocio?	3.00
¿Cuenta con un programa o política que permitan demostrar cuan comprometida se encuentra la alta dirección hacia la Continuidad de Negocio?	4.00
Política	3.67
¿Existe una política de Continuidad de Negocio?	3.00
¿La política de Continuidad de Negocio se encuentra socializada por parte de los directivos dentro de la empresa?	4.00
¿El personal de la empresa y las partes interesadas tiene a disposición la política de Continuidad de Negocio?	4.00
Roles, responsabilidades y autoridades	4.00
¿Cuenta con roles y responsabilidades definidas para cumplir con el Plan de Continuidad de Negocio?	4.00
PLANIFICACIÓN	4.11
Riesgos y oportunidades del PCN	4.33
¿La organización ha reconocido los riesgos?	5.00
¿La empresa ha tomado medidas para minimizar el riesgo de las operaciones en el negocio?	4.00
¿La organización ha reconocido las oportunidades de como minimizar el impacto que un evento adverso puede tener sobre la operatividad de la empresa?	4.00
Objetivos de Continuidad de Negocio	4.00
¿Se ajustan los objetivos a la política de continuidad?	4.00
¿Los objetivos de Continuidad de Negocio son medibles y fueron implantados, socializados y documentados en la empresa?	4.00
¿La organización ha reconocido las actividades, responsables e insumos para cada uno de los objetivos de Continuidad de Negocio?	4.00
Planificación de cambios en la Continuidad de Negocio	4.00
¿Cuenta con una planificación de cambios y sus posibles consecuencias?	4.00
APOYO	3.50
Recursos	3.00

¿La organización ha reconocido los insumos para implantar, poner en marcha, conversar y renovar la Continuidad de Negocio constantemente?	3.00
Competencia	3.00
¿Las responsabilidades del personal que está encargado de la Continuidad de Negocio fueron determinadas y examinadas para un correcto funcionamiento de la Continuidad de Negocio?	3.00
Concientización	4.00
¿Los trabajadores de la organización conocen como deben actuar antes, durante y después de un evento adverso?	4.00
¿Los trabajadores de la organización conocen cómo colaborar al correcto funcionamiento de la Continuidad de Negocio y cómo se ajusta a los objetivos estratégicos de la organización?	4.00
Información documentada	4.00
¿Se encuentran establecidos los procedimientos de los planes que se necesita para obtener un SGCN efectivo para la organización?	4.00
¿La organización ha puesto a disposición los documentos para utilizarlos cuando exista un evento adverso, tomando en cuenta toda la información importante para la organización?	4.00
OPERACIÓN	3.63
Planificación y control operacional	3.50
¿Se encuentran controlados los procesos externos para garantizar que estén disponibles antes, durante y después de un evento adverso?	3.00
¿Se han establecido los criterios para el control de los procesos?	4.00
Análisis de impacto empresarial y evaluación de riesgos	3.67
¿La organización cuenta con un registro del BIA y formatos para el análisis de riesgos?	4.00
¿El BIA y el análisis de riesgos cumplen con los requisitos establecidos por la norma ISO 22301 en todos los procesos?	4.00
¿Se ha definido los tipos de impacto y los criterios relevantes para la organización?	3.00
Estrategia de Continuidad de Negocio	3.73

¿Las estrategias de continuidad de negocio se determinaron y documentaron según el BIA y el análisis de riesgos?	4.00
¿Se encuentran establecidos los tiempos de reactivación de actividades según la prioridad de cada proceso de la organización?	4.00
¿La empresa ha reconocido cuáles son los insumos necesarios para iniciar estrategias de continuidad de negocio?	4.00
¿La organización ha desarrollado un plan preventivo para las amenazas potenciales, con el fin de minimizar el impacto a los procesos y aminorar el tiempo de suspensión de actividades?	3.00
¿Los procedimientos son tolerables y adaptables ante cualquier suceso imprevisto ya sea interno o externo?	4.00
¿La organización ha asignado funciones a los trabajadores y a equipos de emergencia para que sean capaces de responder antes, durante y después de un percance?	3.00
¿La organización ha especificado el tiempo y el modo en el cual se reactivarán las actividades críticas?	4.00
¿La organización ha efectuado simulacros y capacitaciones para saber cómo responder ante un suceso adverso?	4.00
¿La organización ha llevado a cabo ensayos para restaurar el servicio?	4.00
¿La organización cuenta con ensayos basados en posibles sucesos?	3.00
¿La organización ha determinado metas a cumplirse en cada simulacro y capacitación?	4.00
EVALUACIÓN DE DESEMPEÑO	3.75
Supervisión, Medición, análisis y evaluación	3.75
¿La organización cuenta con un documento establecido para dar seguimiento al Plan de Continuidad de Negocio?	4.00
¿La organización inspecciona cada cierto tiempo sobre las modificaciones para garantizar la efectividad de la Continuidad de Negocio?	4.00
¿Se documenta las inspecciones después de una interrupción?	4.00
¿Existe personal y tiempo asignado para realizar el seguimiento y control del Plan de Continuidad de Negocio?	3.00
¿La organización cuenta con una planificación de auditorías internas en intervalos de tiempo determinado?	4.00
MEJORA	3.50

No conformidad y acción correctiva	3.50
¿La organización ha reconocido cuales son las no conformidades con respecto a los requisitos del SGCN y que acciones correctivas se debe realizar?	3.00
¿La organización cuenta con un método que permita administrar las no conformidades, acciones correctivas que lleven a la mejora continua de la organización?	4.00
CALIFICACIÓN GLOBAL	3.69
DESCRIPCIÓN CALIFICACIÓN GLOBAL	En preparación