PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

IMPLEMENTACIÓN DE UN MODELO MULTIDISCIPLINAR PARA EL DISEÑO DE LA CONTINUIDAD DE NEGOCIOS CON UN ENFOQUE EN TIC ORIENTADO A PYMES

Tesis para obtener el título profesional de Ingeniero Informático

AUTOR:

Alexander Emmanuel Flores Barturen

ASESORES:

Dr. Manuel Francisco Tupia Anticona

Dra. Mariuxi Alexandra Bruzza Moncayo

Lima, febrero de 2023

Informe de Similitud

Yo, MANUEL FRANCISCO TUPIA ANTICONA, docente de la Facultad de Ciencias e Ingeniería de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC, orientado a pymes"** del/de la autor(a)/ de los(as) autores(as) Alexander Emmanuel Flores Barturen

dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 27 %. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 29/04/2023.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima 17 de mayo de 2023

Apellidos y nombres del asesor / de la asesora: TUPIA ANTICONA, MANUEL FRANCISCO	
DNI: 10279924	Firma
ORCID: 0000-0001-5260-2829	

Resumen

En la actualidad, el uso de tecnologías de información como soporte de procesos del negocio ha venido en aumento, esto ha generado que las TICs tengan mayor relevancia cuando se habla de continuidad de negocios. Sin embargo, las pymes al contar con recursos limitados, muchas veces se enfocan en asegurar aquellos procesos que le brindan un mayor beneficio económico, olvidando la importancia de la contingencia de TI.

Este enfoque limitado por parte de las pymes también se debe a que no existen modelos que sirvan de guía para el desarrollo e implementación de su continuidad de negocio. Es por esta razón que el presente proyecto de tesis tiene como objetivo implementar un modelo para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes, de manera que estas puedan estar preparadas para reaccionar y recuperarse ante la ocurrencia de un evento disruptivo de TI que afecte el normal funcionamiento de sus operaciones.

Finalmente, este modelo está conformado por cuatro dominios, los cuales a su vez están conformados por procesos, estos últimos cuentan con su respectiva descripción, propósito, documentación relacionada y métricas. Además, se incluye una guía de aplicación práctica del modelo, en donde se indican qué actividades se tienen que realizar en cada proceso y cómo llevarlas a cabo. Para el desarrollo de este modelo se han tomado como referencia principalmente la norma ISO 22301, entre otras.

Dedicatoria

A mis padres Alicia y Alejandro y mi hermana Milagros, por el sacrificio y el esfuerzo realizado para que pueda estudiar y por siempre creer en mí y en mis sueños.

A mi tío Rodolfo, porque en vida me apoyó durante mi educación universitaria.

A mis abuelos Blanca y Horso y mis tíos Gladys, Tito y Juan, por todo el cariño y motivación para seguir adelante.

A mis asesores, por guiarme y apoyarme en el desarrollo de esta tesis.

A mi mascota Giogia, por siempre sacarme una sonrisa con sus ocurrencias.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Capítulo 1. Generalidades

1.1 Problemática

La pandemia del Coronavirus (Covid-19) ha puesto a prueba la continuidad de negocios de empresas de todo tipo y tamaño, dejando en evidencia que no basta con asegurar la continuidad de los procesos operativos, sino que también se debe tomar en cuenta a las TICs, ya que estos procesos son soportados por tecnologías en la mayoría de casos. En el presente capítulo se presentará el contexto de la problemática identificada mediante el uso de la técnica del árbol de problemas, así mismo, se describe el problema central seleccionado, el cual será resuelto a lo largo del presente proyecto de tesis.

1.1.1 Árbol de Problemas

"El árbol de problemas es una técnica que se emplea para identificar una situación negativa (problema central) la cual se intenta solucionar analizando relaciones de tipo causa – efecto. Para ello, se debe formular el problema central de modo tal que permita definir diferentes alternativas de solución en lugar de una solución única" (UNESCO, 2017). En la Tabla 1 se mostrará el árbol de problemas.

1.1.2 Descripción

En los últimos años, la continuidad de negocios ha sido desarrollada e implementada por empresas de distintos rubros y tamaños (grandes, medianas y pequeñas) (Sambo y Bankole, 2016), dándole un enfoque sistemático, tomando como referencia en algunos casos a la ISO 22301 (ISO, 2019), sobre todo en las grandes empresas, lo cual les permite organizar el proceso de implantación en varias fases tales como identificación de riesgos, elaboración de controles, establecimiento y prueba de planes y mejora continua, entre otros. Situaciones como la pandemia que ha venido asolando al planeta los últimos dos años, ha acelerado la necesidad de que las empresas se preparen para interrupciones que afecten las operaciones de negocio, como ya ha venido ocurriendo (Păunescu y Argatu, 2020).

La continuidad del negocio es considerada como un proceso más de gestión, en el cual se identifican los factores que pueden amenazar precisamente a una organización y que provee un marco con el cual se puede desarrollar la resiliencia organizacional y la capacidad de responder efectivamente ante estos eventos (Speight, 2011).

Tabla 1. Árbol de problemas.

PROBLEMAS EFECTOS	Inadecuado o inexistente desarrollo de estrategias, planes y controles de continuidad negocios con enfoque en la contingencia de TI (basado en buenas prácticas) en las pymes.	Detención de los procesos de negocio por un tiempo prolongado ante la ocurrencia de incidentes graves que afecten la continuidad de la operación de las TICs o los servicios de TI (Poca capacidad de reacción y resiliencia).	Ausencia de un papel estratégico de las TICs en la recuperación de las operaciones de las pymes ante incidentes que afecten gravemente la continuidad de los procesos.
PROBLEMA CENTRAL	Inexistencia de modelos o marcos de contingencia de TI relacionados con continuidad de negocios y orientados a pymes.		
PROBLEMAS CAUSAS	Desconocimiento de las buenas prácticas de continuidad de negocios de parte de las pymes.	Visión empresarial sesgada sobre la continuidad de negocios en el sentido que las pymes no consideran ni a la contingencia de TI ni a la resiliencia técnica como elementos base de la operativa de la organización.	Estrategias y planes de continuidad en las pymes que no contemplan aspectos y enfoques sobre contingencia de TI y su importancia en la recuperación de las operaciones del negocio.

Fuente: Elaboración propia.

Si consideramos que la mayoría de las empresas dan soporte a sus procesos de negocio a través del uso intensivo de tecnologías de información y comunicaciones (TIC), cualquier interrupción que afecte a dichas TIC impactará directamente en los procesos a los que están apoyando. La gestión de la contingencia de TI, subproceso de la propia continuidad de negocios, consiste en identificar los riesgos internos y externos que pueden afectar a los activos de TI con la finalidad de crear controles que eviten que esos riesgos se materialicen y afecten el normal funcionamiento de los procesos de negocio empresariales (Filipović et al., 2018).

De acuerdo a la revisión del estado del arte, *la contingencia de TI no es incluida* como parte de la continuidad de negocios como resultado de una visión limitada por parte de las pequeñas y medianas empresas, lo que genera que las empresas sigan experimentando un largo tiempo de inactividad en sus procesos a pesar de tener un plan de continuidad de negocios y que luego, ante incidentes graves -de nuevo, como los de la pandemia, tal como se menciona en la ISO 22313, la cual la cataloga como una interrupción gradual en las actividades (ISO, 2020)- acudan a sus áreas de TI en busca de reactivar la disponibilidad de sus servicios de TI en un orden determinado y con la celeridad del caso (Sambo y Bankole, 2016).

Dentro de los documentos principales que se establecen para implementar la continuidad de negocios y la propia gestión de la contingencia de TI, encontramos a *los planes de contingencia, el plan de continuidad de negocios y el plan de recuperación ante desastres*. El plan de continuidad de negocios (BCP, por sus siglas en inglés) contiene el alcance, los roles, los riesgos identificados y sus respectivos controles para mitigarlos y los procesos y estrategias para hacer frente a los incidentes, la Figura 1 muestra las fases para la construcción del BCP.

Figura 1. Fases para el desarrollo del BCP. Fuente: (ESAP, 2018a).

Las pequeñas y medianas empresas al estar limitadas por la cantidad de recursos que poseen (Tan y Lee, 2021), muchas veces no consideran al área de TI en el desarrollo de los

planes mencionados anteriormente, ya que priorizan aquellos procesos que le generen un mayor beneficio económico (Siciliano y Gaudenzi, 2018); esta decisión ocasiona que no se considere el papel que juegan las TIC tanto para el soporte a los procesos del negocio como en el proceso de recuperación de las operaciones que se han visto interrumpidas, como ya se había mencionado (Sambo y Bankole, 2016).

Cuando una empresa no considera las implicancias de implementar la gestión de la contingencia desde una perspectiva de TI o no incluye buenas prácticas técnicas en la recuperación de sus operaciones y en el desarrollo de la resiliencia organizacional (capacidad para responder y adaptarse ante situaciones imprevistas), Siciliano y Gaudenzi (2018) comentan que ocurre lo siguiente:

- Presentan demoras en la reanudación de sus procesos.
- Pérdida de confianza por parte de los inversionistas y clientes.
- Pérdida de dinero.
- Percepción de que el área de TI no hace bien su trabajo.

En la revisión del estado del arte no se han encontrado modelos basados en componentes para gestionar la contingencia de TI dentro del proceso de continuidad de negocios, ya que estos modelos están mayormente enfocados a la cadena de suministros, lo cual no es de mucha utilidad para las pequeñas y medianas empresas, dado que estas no cuentan con cadenas de suministros complejas. Este vacío hace que las empresas no estén debidamente preparadas para hacer frente a incidentes que amenazan su continuidad de negocios, ya que el solo hecho de contar con documentos, políticas y planes no garantiza una eficiente recuperación de operaciones suspendidas luego de la ocurrencia de algún tipo de desastre.

La propuesta de cualquier marco relacionado con continuidad y haciendo hincapié en contingencia de TI que pueda ser aplicado por pequeñas y medianas empresas de cualquier rubro, tiene que estar formado por componentes y a su vez estar basado en buenas prácticas internacionalmente aceptadas; entendiendo las buenas prácticas como “un conjunto de principios, objetivos y procedimientos que han sido generalmente aceptados o consensuados dentro de un campo específico, ya que han demostrado su eficacia y eficiencia en un determinado contexto”, tal como se puede ver en (Bruzza, 2020).

En consecuencia, a partir de la revisión sistemática del estado del arte, se ha podido identificar que en los últimos años la continuidad de negocios ha venido siendo implementada por las grandes empresas, las cuales han tomado como guía a la ISO 22301. Como se mencionó,

estos planes de continuidad de negocios están mayormente enfocados a la cadena de suministro, dejando de lado la contingencia de TI. Este vacío identificado se debe a que la norma ISO 22301 por su propia naturaleza brinda un enfoque general de la continuidad de negocios, otra razón es que no existe una correcta comunicación entre el área de TI y las gerencias, lo que produce que la alta dirección no tenga conocimiento sobre cómo los riesgos asociados a los activos de TI pueden afectar de manera negativa a los procesos de negocio. Por consiguiente, esta omisión en la contingencia de TI provoca que no se desarrollen estrategias y controles que hagan frente a estos incidentes, lo que puede derivar en pérdidas económicas y de reputación de la marca, siendo las pequeñas y medianas empresas las más afectadas, ya que al poseer recursos limitados les es más difícil poder afrontarlas.

1.1.3 Problema seleccionado

Por lo expuesto previamente, se ha seleccionado como problema central la inexistencia de modelos o marcos de contingencia de TI relacionados con continuidad de negocios y orientados a pymes.

1.2 Objetivos

1.2.1 Objetivo general

Implementar un modelo multidisciplinar para el diseño de la continuidad de negocios con enfoque en la contingencia de TI.

1.2.2 Objetivos específicos

O 1. Identificar las buenas prácticas relacionadas con contingencia de TI y continuidad de negocios que serán componentes del modelo.

O 2. Definir los componentes del modelo con sus respectivas métricas.

O 3. Elaborar la guía de aplicación práctica del modelo orientado al personal de TI.

1.2.3 Resultados esperados

O 1. Identificar las buenas prácticas relacionadas con contingencia de TI y continuidad de negocios que serán componentes del modelo.

R 1. Lista de buenas prácticas identificadas en la literatura mediante una matriz de trazabilidad y relacionadas con los componentes del modelo.

O 2. Definir los componentes del modelo con sus respectivas métricas.

R 2. Estructura a alto nivel del modelo en función de dominios basados en Balanced Scorecard (BSC).

R 3. Lista de componentes organizacionales con sus métricas.

R 4. Lista de componentes de innovación con sus métricas.

R 5. Lista de componentes de gestión de riesgos con sus métricas.

R 6. Lista de componentes estratégicos con sus métricas.

O 3. Elaborar la guía de aplicación práctica del modelo orientado al personal de TI.

R 7. Guía de aplicación práctica del modelo.

1.2.4 Mapeo de objetivos, resultados y verificación

Tabla 2. Resultados esperados del objetivo 1.

Objetivo 1: Identificar las buenas prácticas relacionadas con contingencia de TI y continuidad de negocios que serán componentes del modelo.		
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**
R1. Lista de buenas prácticas identificadas en la literatura mediante una matriz de trazabilidad y relacionadas con los componentes del modelo.	• Matriz de trazabilidad que identifica las buenas prácticas de la literatura y el propósito de su uso en el modelo.	• Matriz con los artículos y estándares identificados de la literatura y el marco conceptual terminada al 100% y verificada por experto en buenas prácticas de continuidad, contingencia de TI y resiliencia organizacional.

Fuente: Elaboración propia.

Tabla 3. Resultados esperados del objetivo 2.

Objetivo 2: Definir los componentes del modelo con sus respectivas métricas.		
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**
R2. Estructura del modelo en función de dominios basados en Balanced Scorecard (BSC).	• Modelo de componentes a alto nivel.	• Documento con el modelo de componentes a alto nivel al 100% y verificado por experto en Balanced Scorecard.

R3. Lista de componentes organizacionales con sus métricas.	• Documento con la hoja de ruta de la creación de los componentes del modelo. • Documentación completa de los componentes del modelo.	• Componentes organizacionales definidos al 100%, verificación y conformidad al 100% por parte de los especialistas en continuidad de negocios y/o contingencia de TI.
R4. Lista de componentes de innovación con sus métricas.	• Documento con la hoja de ruta de la creación de los componentes del modelo. • Documentación completa de los componentes del modelo.	• Componentes de innovación definidos al 100%, verificación y conformidad al 100% por parte de los especialistas en continuidad de negocios y/o contingencia de TI.
R5. Lista de componentes de gestión de riesgos con sus métricas.	• Documento con la hoja de ruta de la creación de los componentes del modelo. • Documentación completa de los componentes del modelo.	• Componentes de gestión de riesgos definidos al 100%, verificación y conformidad al 100% por parte de los especialistas en continuidad de negocios y/o contingencia de TI.
R6. Lista de componentes estratégicos con sus métricas.	• Documento con la hoja de ruta de la creación de los componentes del modelo.	• Componentes estratégicos definidos al 100%, verificación y conformidad al 100% por parte de los

	• Documentación completa de los componentes del modelo.	especialistas en continuidad de negocios y/o contingencia de TI.

Fuente: Elaboración propia.

Tabla 4. Resultados esperados del objetivo 3.

Objetivo 3: Elaborar la guía de aplicación práctica del modelo orientado al personal de TI.		
Resultado	**Medio de verificación**	**Indicador objetivamente verificable**
R7. Guía de aplicación práctica del modelo.	• Documentación con la guía de aplicación práctica del modelo paso a paso.	• Documento con la guía al 100%, informe de revisión y acta de conformidad de la misma por parte del experto en continuidad de negocios.

Fuente: Elaboración propia.

1.3 Métodos y Procedimientos

En esta sección se detallarán tanto las herramientas como las metodologías que se usarán para obtener los resultados esperados.

Tabla 5. Herramientas.

Resultado	Herramienta
Lista de buenas prácticas identificadas en la literatura mediante una matriz de trazabilidad.	No aplica
Estructura del modelo en función de dominios basados en Balanced Scorecard (BSC).	• BSC • COBIT 2019
Lista de componentes organizacionales con sus métricas.	• ISO 22301 • RACI • NIST SP 800-34 • NIST Risk Management Framework
Lista de componentes de innovación con sus métricas.	• ISO 22301 • COBIT 2019 • RACI • NIST SP 800-34

	• NIST Risk Management Framework
Lista de componentes de gestión de riesgos con sus métricas.	• ISO 22301 • COBIT 2019 • RACI • NIST SP 800-34 • NIST Risk Management Framework
Lista de componentes estratégicos con sus métricas.	• ISO 22301 • COBIT 2019 • RACI • NIST SP 800-34 • NIST Risk Management Framework
Guía de aplicación práctica del modelo.	No aplica

Fuente: Elaboración propia.

✓ ISO 22301

La ISO 22301 es una norma que especifica la estructura y los requerimientos para la implementación y el mantenimiento del sistema de gestión de la continuidad de negocios (BCMS, por sus siglas en inglés) en las empresas, con la finalidad de que puedan estar preparadas para hacer frente a incidentes que afecten el desarrollo normal de sus operaciones (ISO, 2019). Esta norma hace énfasis en la importancia que tienen los siguientes cuatro puntos en un BCMS:

- Entender la necesidad que tiene la organización para definir políticas y objetivos relacionados a la continuidad de negocios.
- Operar y mantener procesos, capacidades y estructuras para asegurar que la organización sobreviva a las interrupciones que pueda sufrir.
- Monitorear y revisar la efectividad del BCMS.
- Mejora continua basado en indicadores cuantitativos y cualitativos.

Esta metodología se usará como guía para la construcción del modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque TIC.

✓ Balanced Scorecard

El Balanced Scorecard (BSC) es una herramienta de gestión que permite monitorear todos los elementos importantes en la estrategia de una organización desde cuatro importantes perspectivas (ver Figura 2), interrelacionando objetivos y relacionándolos con acciones concretas para que de esta manera las empresas logren alcanzar la excelencia (Kaplan y Norton, 2005).

Esta herramienta será utilizada para estructurar el modelo en función de dominios que se encuentren relacionados entre sí.

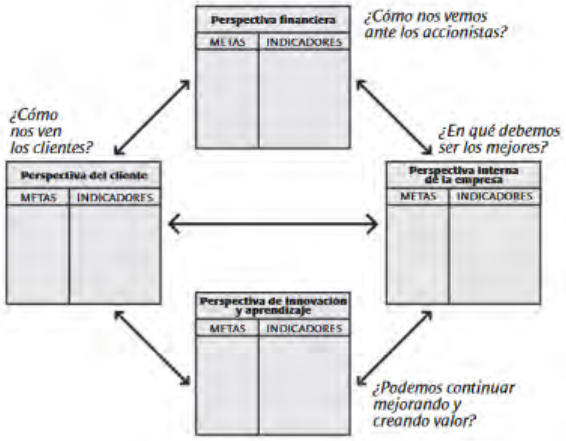


Figura 2. Perspectivas del BSC. Fuente: (Kaplan y Norton, 2005).

- ✓ COBIT 2019

COBIT 2019 es un marco que define los componentes (ver Figura 3) para construir y mantener un sistema de gobierno y gestión de TI a nivel de toda la empresa, el cual incluye: procesos, estructura organizacional, procedimientos y políticas, flujo de información, comportamiento y cultura, habilidades e infraestructura. Así mismo, define los factores de diseño que la empresa debe considerar para construir un sistema de gobierno que se ajuste mejor a sus necesidades (ISACA, 2018a).

Esta herramienta será utilizada como guía para la construcción de los componentes del modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque TIC.

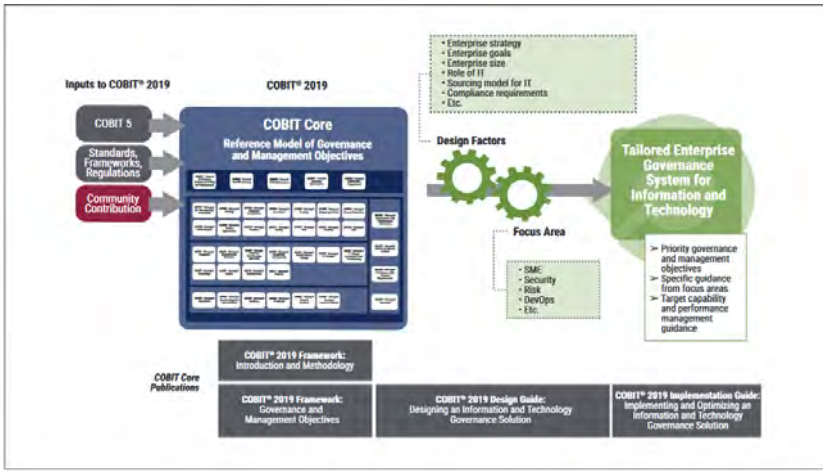


Figura 3. Vista general de COBIT 2019. Fuente: (ISACA, 2018a)

- ✓ Matriz RACI

La matriz RACI es una herramienta básica que permite gestionar responsabilidades y roles de forma simple y clara mediante el mapeo de partes interesadas para cada proyecto y proceso de la empresa (Lee et al., 2021).

Esta herramienta será de utilidad para que se puedan asignar los roles de *Responsable (de ejecutar la tarea/actividad del proceso), Accountable (el cual no tiene una traducción literal al español pero se entiende que es la persona que RESPONDE por los resultados de la actividad/proceso), Consultado e Informado* a cada persona involucrada en la implementación de la continuidad de negocios en la empresa.

- ✓ NIST SP 800-34 – Contingency Planning Guide for Federal Information Systems

La norma NIST SP 800-34 provee una serie de instrucciones, recomendaciones y consideraciones que se deben tomar para desarrollar y mantener un programa de planificación de contingencia viable para los sistemas de información federales. Esta guía define tres fases que muestran las acciones que se deben tomar luego de que ocurra una interrupción del sistema (NIST, 2010), las cuales son:

- Activación: describe el proceso de activación del plan de contingencia en función al impacto de la interrupción.
- Recuperación: detalla un conjunto de acciones que el equipo de recuperación debe seguir para restablecer la operación del sistema.
- Reconstitución: incluye un conjunto de pruebas y validaciones que se deben realizar para comprobar que el sistema funciona con normalidad.

Esta herramienta será utilizada como guía para la construcción de los componentes del modelo.

- ✓ NIST Risk Management Framework

El marco para la gestión de riesgos del NIST proporciona un proceso de siete pasos que pueden ser aplicados por cualquier organización para gestionar la seguridad de la información y riesgos de privacidad (NIST, 2021), estos pasos son:

- Preparar.
- Categorizar.
- Seleccionar.
- Implementar.

- Evaluar.
- Autorizar.
- Monitorear.

Al igual que la norma NIST anterior, esta metodología será utilizada como guía para la construcción de los componentes del modelo.

Capítulo 2. Marco Conceptual

2.1 Introducción

En el presente capítulo se muestran los conceptos relacionados a la continuidad de negocios y contingencia de TI, los cuales son de importancia para entender la problemática y la solución planteada en el presente proyecto de tesis.

2.2 Desarrollo del marco

2.2.1 Buenas prácticas

Es una forma de trabajo que ha demostrado ser exitosa en múltiples organizaciones (ITIL, 2019).

Por otra parte, (Cervera y Hernández, 1999) se refieren a buenas prácticas como un conjunto de principios, objetivos y procedimientos que han sido generalmente aceptados o consensuados dentro de un campo específico, ya que han demostrado su eficacia y eficiencia en un determinado contexto, tal como se puede ver en (Bruzza, 2020).

Algunos ejemplos de buenas prácticas son:

- ITIL (Information Technology Infraestructure Library), es un conjunto de buenas prácticas para la gestión de servicios de tecnologías de la información (TI) (ITIL, 2019).
- COBIT (Control Objectives for Information and Related Technologies), es un conjunto de buenas prácticas para el gobierno y gestión de TI dentro de las empresas (ISACA, 2018a).

2.2.2 Modelo

Es la representación de un sistema, práctica, proceso, servicio u otra entidad que es usada para entender y predecir su comportamiento y relaciones (ITIL, 2019).

Por otro lado, (Notice, 2011) define modelo como un sistema que permite describir de manera aproximada un aspecto específico de la realidad, como se puede apreciar en (Bruzza, 2020).

A manera de ilustración, se presenta el modelo propuesto por (Sambo y Bankole, 2016) para la implementación de un plan de continuidad de negocios (BCP), cuyos pasos son mostrados en la Figura 4.

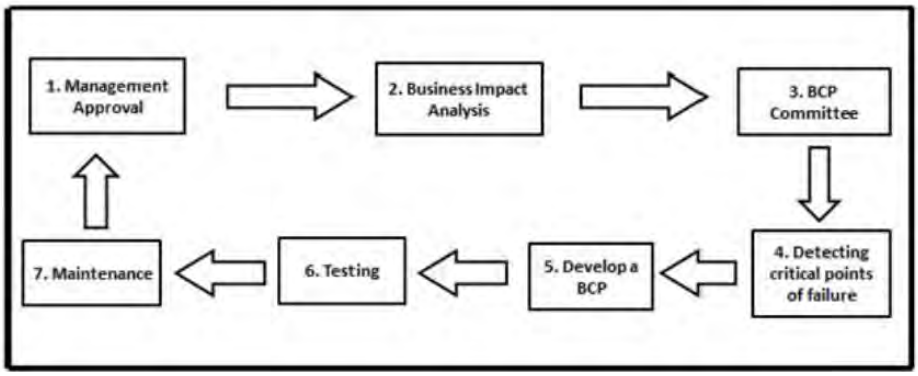


Figura 4. Modelo para la implementación de un BCP. Fuente: (Sambo y Bankole, 2016).

2.2.3 Continuidad de negocios

Es la capacidad de la organización para continuar con la entrega de productos o servicios a un nivel aceptable (predefinido) durante la ocurrencia de una interrupción (ISO, 2019).

Por otro lado, (ITIL, 2019) define continuidad de negocio como la práctica de asegurar que un servicio esté disponible y que su rendimiento se mantenga en un nivel aceptable en caso de un desastre.

También se le puede definir como un proceso de gestión que tiene como objetivo identificar factores que pueden amenazar a una organización y en base a eso proveer un marco para el desarrollo de la resiliencia organizacional y la capacidad de responder efectivamente ante estos eventos, de tal manera que se protejan los intereses de los stakeholders, así como, la reputación y el valor de la marca de la empresa (Speight, 2011).

Como ejemplo, en la Figura 5, se muestra el marco para la gestión de la continuidad propuesto por la ISO 22301.

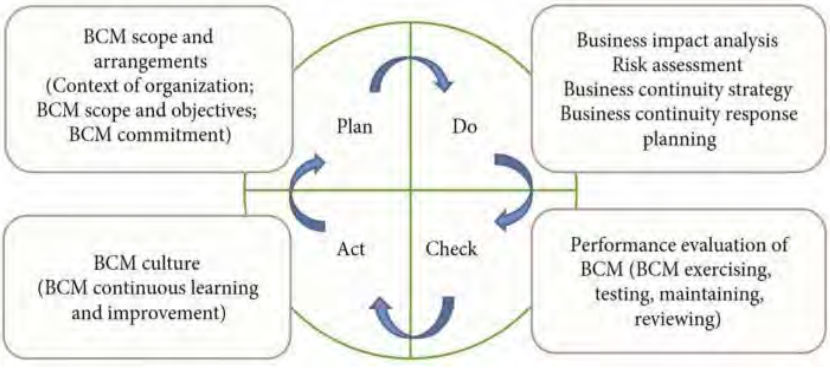
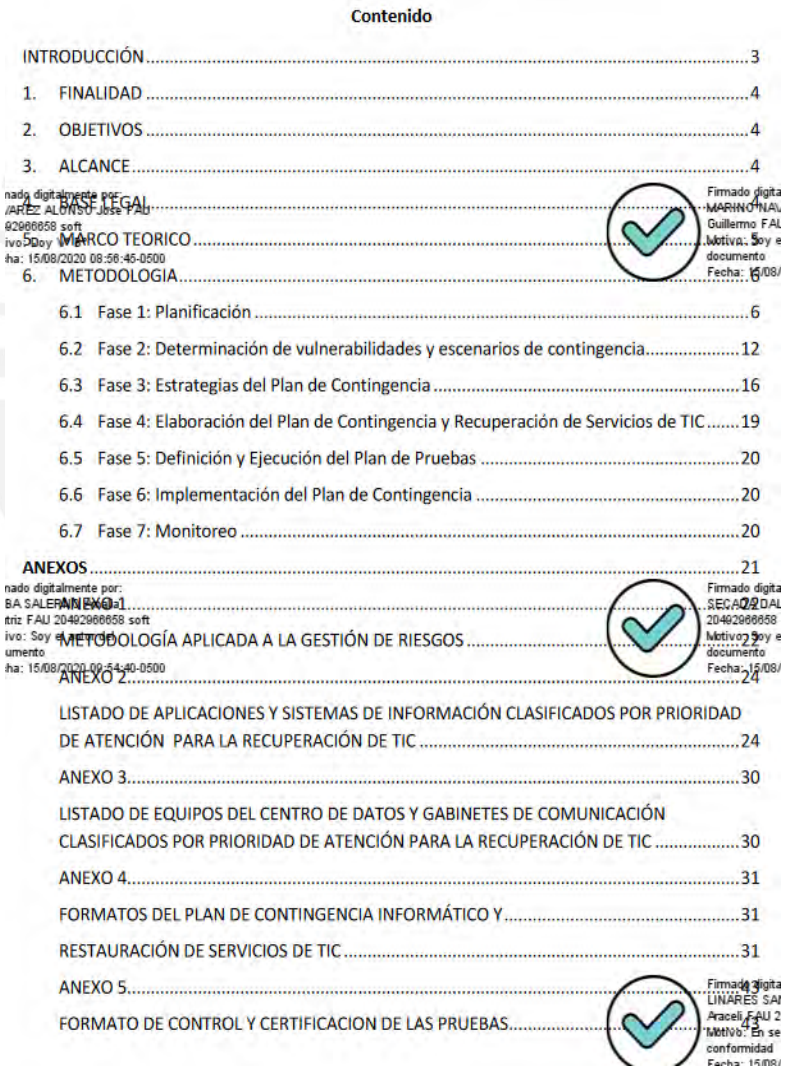


Figura 5. Marco para la gestión de la continuidad de negocios propuesto por la ISO 22301:2019. Fuente: (Păunescu y Argatu, 2020).

2.2.4 Contingencia de TI

Posible futura ocurrencia o cambio de un conjunto particular de circunstancias que pueden representar un riesgo para las TICs (ISO, 2021).

En la Figura 6 se muestra como ejemplo el plan de contingencia informático y recuperación de servicios de tecnología de la información y comunicaciones del Ministerio del Ambiente, el cual tiene como alcance los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal y otros administrados por la Oficina de Tecnologías de Información y Comunicaciones (MINAM, 2020).



Contenido

Figura 6. Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones del Ministerio del Ambiente. Fuente: (MINAM, 2020).

2.2.5 Recuperación ante desastres

Es la capacidad de los elementos de tecnología de la información y las comunicaciones de una organización para respaldar sus funciones comerciales críticas a un nivel aceptable dentro de un periodo predeterminado después de un desastre (ISO, 2018a).

Por ejemplo, una forma de recuperación ante desastres puede ser mediante la redundancia de servidores, es decir una empresa cuenta con dos servidores en distintas ubicaciones geográficas, de tal manera que, si en la ubicación de un servidor ocurre un incidente, las operaciones se pueden reanudar mediante la puesta en marcha del otro equipo. La Figura 7 muestran lo descrito anteriormente.

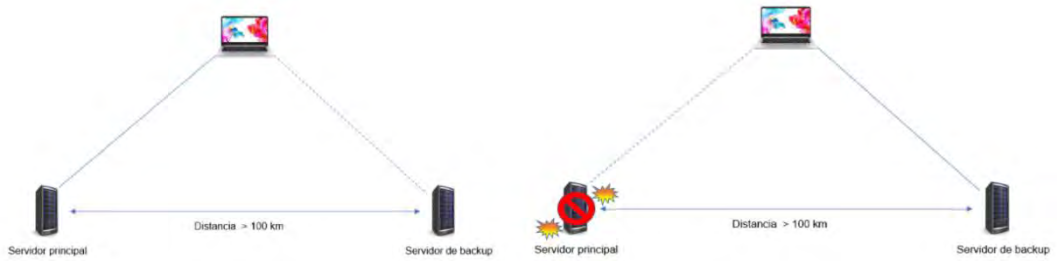


Figura 7. Situación antes y después del desastre. Fuente: Elaboración propia.

2.2.6 Resiliencia organizacional

Es la habilidad que tiene una organización para absorber y adaptarse a un ambiente cambiante (ISO, 2017a).

Así mismo, (ITIL, 2019) define resiliencia organizacional como la habilidad de una organización para anticiparse, prepararse, responder, y adaptarse a influencias externas no planeadas.

La Figura 8 muestra los cinco pasos propuestos por (Siciliano y Gaudenzi, 2018) para que la empresa desarrolle su capacidad de resiliencia, luego de haber identificado los posibles riesgos y el impacto que tendrían si se llegaran a materializar.

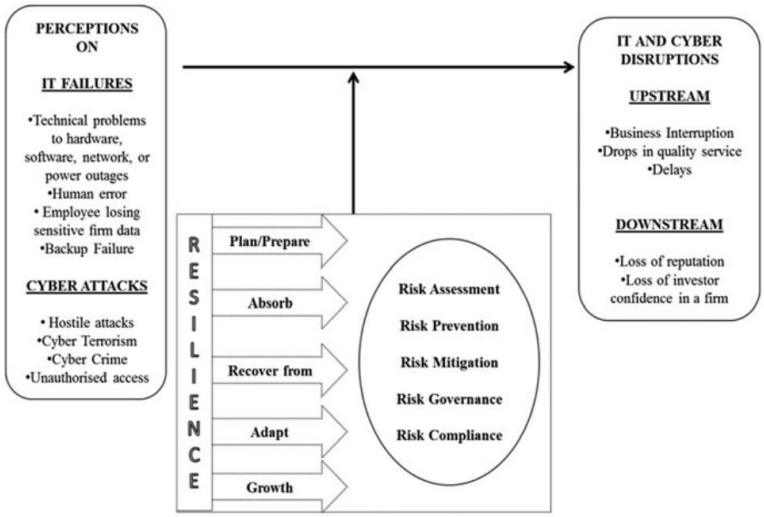


Figura 8. Gestión de riesgos informáticos y cibernéticos en las cadenas de suministro: El papel de la resiliencia. Fuente: (Siciliano y Gaudenzi, 2018).

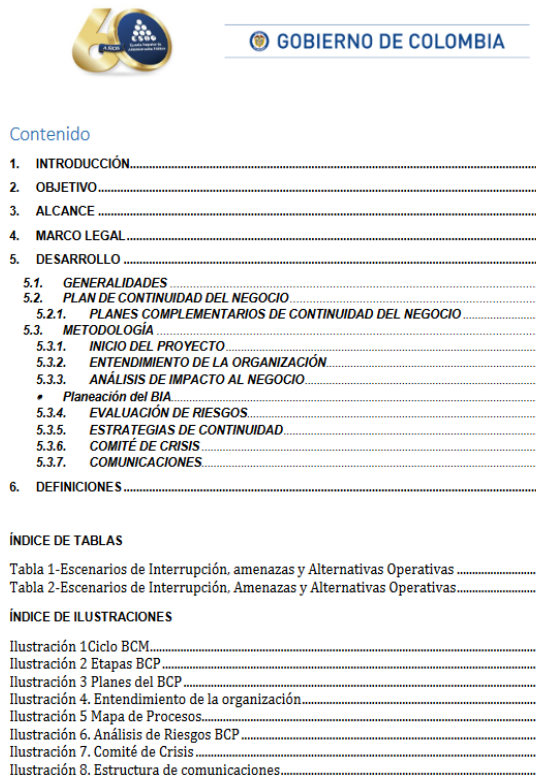
2.2.7 Plan de continuidad de negocios (BCP)

Es la documentación de procesos que sirve de guía a la empresa para responder ante una interrupción y de esta manera recuperar, reanudar y reestablecer la entrega de productos o servicios a un nivel predefinido (ISO, 2019).

A manera de ejemplo, la estructura de un BCP puede ser la siguiente:

- Introducción.
- Objetivo.
- Alcance.
- Marco legal.
- Desarrollo.
- Definiciones.

Tal como se muestra en la Figura 9, la cual muestra el índice del BCP elaborado por la Escuela Superior de Administración Pública de Colombia en el año 2018.



GOBIERNO DE COLOMBIA

Contenido

Figura 9. Índice del BCP. Fuente: (ESAP, 2018a).

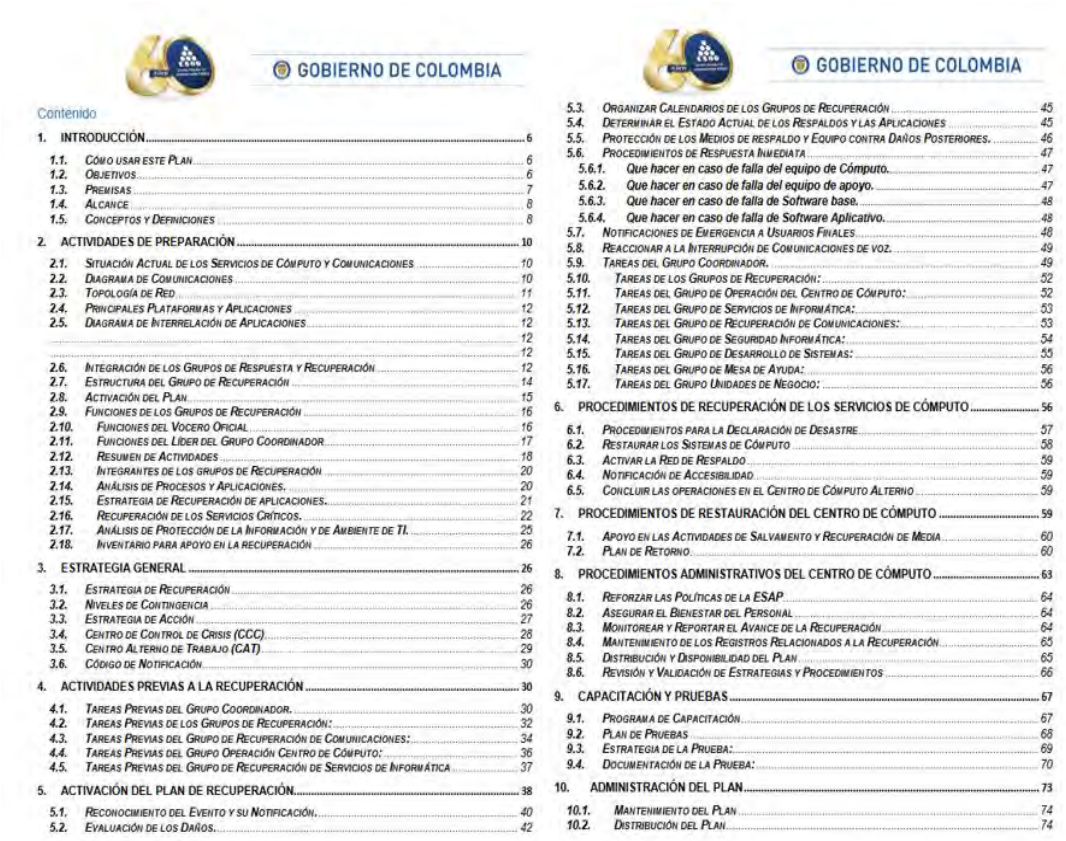
2.2.8 Plan de recuperación ante desastres (DRP)

Un conjunto de procesos claramente definidos relacionados con cómo una organización se recuperará de un desastre, de tal manera que pueda regresar a un estado previo, considerando las cuatro dimensiones de la gestión de servicios (ITIL, 2019).

El DRP puede tener la siguiente estructura:

- Introducción.
- Actividades de preparación.
- Estrategia general.
- Actividades previas a la recuperación.
- Activación del plan de recuperación.
- Procedimientos de recuperación de los servicios de cómputo.
- Procedimientos de restauración del centro de cómputo.
- Procedimientos de administración del centro de cómputo.
- Capacitación y pruebas.
- Administración del plan.

Como se ha encontrado en la Escuela Superior de Administración Pública de Colombia. La Figura 10 muestra el índice de este plan de recuperación ante desastres.



GOBIERNO DE COLOMBIA

Contenido

Figura 10. Índice del DRP. Fuente: (ESAP, 2018b).

2.2.9 Plan de contingencia

Planificación para hacer frente a un factor de riesgo si se convierte en un problema. (ISO, 2017b).

Por otro lado, el (NIST, 2010) define plan de contingencia como la gestión de políticas y procedimientos diseñados para mantener o restaurar las operaciones de negocio, lo cual incluye operaciones computacionales, posiblemente en otra ubicación en caso de eventos de emergencia, fallos en el sistema o desastres.

Como ejemplo, la Figura 11 muestra la plantilla de un plan de contingencia para sistemas de información federales proporcionada por el NIST, el cual consiste en:

- Introducción.
- Concepto de las operaciones.
- Activación y notificación del plan.

- Recuperación.
- Reconstrucción.

TABLE OF CONTENTS

Figura 11. Plan de Contingencia para Sistemas de Información Federales. Fuente: (NIST, 2010).

Capítulo 3. Estado del Arte

3.1 Introducción

En este capítulo se presenta la revisión sistemática del Estado del Arte con respecto a la continuidad de negocios en las empresas con enfoque en TI. Se hará uso de la metodología de revisión propuesta por B. Kitchenham (Kitchenham, 2007) en su estudio "*Guidelines for performing Systematic Literature Review in Software Engineering*", la cual propone una serie de pasos para identificar los artículos relacionados a la investigación que son más relevantes.

3.2 Objetivos de revisión

Esta revisión sistemática de tipo empírica, tiene como objetivo encontrar aquellos estudios y trabajos de investigación que muestran cómo las empresas han logrado hacer frente a incidentes graves que han puesto en riesgo la continuidad de negocios, haciendo especial hincapié precisamente en la continuidad de las operaciones de TI (contingencia de TI), identificando las buenas prácticas internacionalmente aceptadas que han sido usadas. De la misma manera, la revisión busca identificar los riesgos de TI más comunes a los que hacen frente las organizaciones cuando sufren incidentes que afectan gravemente la continuidad del negocio.

3.3 Preguntas de revisión

Se hará uso de los criterios PICOC (Población, Intervención, Comparación, Salida y Contexto) como apoyo para estructurar la búsqueda de información. En la Tabla 6 se muestra la descripción para cada criterio que se usará para esta revisión.

Tabla 6. Criterios PICOC.

Criterio	Descripción
Población	Empresas en general.
Intervención	Buenas prácticas y estándares de continuidad de negocios y contingencia de TI.
Comparación	No aplica.
Salida	Marcos o modelos multidisciplinares para planificar la gestión de la continuidad de negocios y la contingencia de TI.
Contexto	Empresarial con enfoque en TIC.

Fuente: Elaboración propia.

En base a estos criterios, se plantean las siguientes preguntas:

- P1. ¿De qué manera las empresas han hecho frente a incidentes que afectan su continuidad de negocios?
- P2. ¿Cómo se han aplicado las buenas prácticas internacionalmente aceptadas en el manejo de las contingencias de TI, al interior de las empresas?
- P3. ¿Qué marcos o modelos multidisciplinares contribuyen a la gestión de la continuidad de negocios haciendo hincapié en las operaciones de TI y sobre qué tratan?

3.4 Estrategia de búsqueda

Siguiendo la metodología de Kitchenham (Kitchenham, 2007), se procede a definir las siguientes palabras claves en base a las preguntas planteadas en el punto anterior, las cuales están divididas en 3 grupos:

- Continuidad de negocios: business continuity, bcp, IT contingency, business continuity management, bcm, disaster recovery, drp.
- Modelo: model, framework, good practices, best practices.
- Riesgo: risk, risk management.

3.4.1 Motores de búsqueda a usar

Para la presente revisión se emplearán los siguientes motores de búsqueda:

- Scopus
- IEEE Xplore
- ACM Digital Library

3.4.2 Cadenas de búsqueda a usar

Tomando en cuenta el cuadro PICOC y las palabras claves anteriormente definidas, se procede a elaborar la cadena de búsqueda y luego se presenta su respectiva adaptación a cada motor de búsqueda:

- Cadena

  ("business continuity" O "IT contingency" O "business continuity management" O "disaster recovery" O ("IT" Y ("bcp" O "bcm" O "drp"))) Y ("model" O "framework" O "good practices" O "best practices") Y ("risk" O "risk management") Y ("enterprise" O "company" O "organization")

Las respectivas versiones de la cadena en las diferentes bases de datos de artículos se presentan a continuación:

- Scopus

  TITLE-ABS-KEY(("business continuity" OR "IT contingency" OR "business continuity management" OR "disaster recovery" OR ("IT" AND ("bcp" OR "bcm" OR "drp"))) AND ("model" OR "framework" OR "good practices" OR "best practices") AND ("risk" OR "risk management") AND ("enterprise" OR "company" OR "organization"))

- IEEE Xplore

  (("business continuity" OR "IT contingency" OR "business continuity management" OR "disaster recovery" OR ("IT" AND ("bcp" OR "bcm" OR "drp"))) AND ("model" OR "framework" OR "good practices" OR "best practices") AND ("risk" OR "risk management") AND ("enterprise" OR "company" OR "organization"))

- ACM Digital Library

  ((Abstract: "business continuity") OR (Abstract: "it contingency") OR (Abstract: "business continuity management") OR ("disaster recovery") OR (("it") AND (("bcp") OR ("bcm") OR ("drp")))) AND ((Abstract: "model") OR (Abstract: "framework") OR (Abstract: "good practices") OR ("best practices")) AND ((Abstract: "risk") OR (Abstract: "risk management")) AND ((Abstract: "enterprise") OR (Abstract: "company") OR (Abstract: "organization"))

3.4.3 Documentos encontrados

Como resultado de las búsquedas en las tres bases de datos, se obtuvo un total de 423 artículos. La Tabla 7 muestra los resultados por cada motor de búsqueda, así como los artículos repetidos y los que son considerados relevantes luego de haber aplicado los criterios de inclusión y exclusión:

Tabla 7. Resultados de la búsqueda.

Motor de búsqueda	Resultados de la búsqueda	Artículos repetidos	Artículos relevantes
Scopus	361	3[1]	13
IEEE Xplore	50	12	5

[1] Se encontraron versiones repetidas y actualizadas de un mismo artículo en diferentes años.

ACM Digital Library	12	0	0
Total	423	408	18

Fuente: Elaboración propia.

3.4.4 Criterios de inclusión/exclusión

Criterios de inclusión:

- El estudio reporta la forma en que las empresas han enfrentado los incidentes que afectan su continuidad de negocios.
- El estudio describe un modelo o marco de continuidad de negocios enfocado en los procesos/infraestructura de TI.
- El estudio muestra las buenas prácticas aplicadas por las empresas para el manejo de contingencias de TI.
- El estudio muestra casos reales de aplicación de buenas prácticas de continuidad de negocios y contingencia de TI para empresas específicas.

Criterios de exclusión:

- El estudio se ha realizado hace más de 10 años.
- El estudio está redactado en un idioma distinto al español o inglés.
- El estudio utiliza las siglas BCP (plan de continuidad de negocios), DRP (plan de recuperación ante desastres) y BCM (gestión de la continuidad de negocios) en un contexto diferente a la continuidad de negocios y a la contingencia de TI.
- El estudio no muestra marcos, modelos o buenas prácticas orientadas a la continuidad de negocios y a la contingencia de TI.
- El estudio no muestra un caso práctico en el que una empresa específica haya resuelto problemas o incidentes que afecten la contingencia de TI, empleando buenas prácticas.

3.5 Formulario de extracción de datos

La Tabla 8 muestra los artículos considerados relevantes luego de haber realizado la revisión sistemática.

Tabla 8. Lista de artículos considerados relevantes.

ID	Referencia del estudio
T1	Aronis, S., & Stratopoulos, G. (2016). Implementing business continuity management systems and sharing best practices at a European bank.

	Journal of business continuity & emergency planning, 9, 203–217. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84979854549&partnerID=40&md5=f0df27318ed2aa23f3473b122dfb97f9
T2	Filipović, D., Krišto, M., & Podrug, N. (2018). Impact of crisis situations on development of business continuity management in Croatia [Djelovanje kriznih situacija na razvoj upravljanja poslovnim kontinuitetom u Hrvatskoj]. Management (Croatia), 23, 99–122. https://doi.org/10.30924/mjcmi/2018.23.1.99
T3	Gómez, G., Morón, A., & Betancourt, R. (2020). Risk management model, the contribution of phi value in the business continuity plan [Modelo de gestión de riesgos: El aporte del valor phi en el plan de continuidad de negocios]. Revista Venezolana de Gerencia, 25, 112–128. https://doi.org/10.37960/rvg.v25i3.33356
T4	Hersyah, M. H., & Derisma. (2018). A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation. 2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings, 392–397. https://doi.org/10.1109/ICITSI.2018.8696075
T5	Kulkarni, S., Hidding, G. J., & Cicekoglu, S. (2015). A framework for post-crisis business continuity plans. Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, 143–152. https://doi.org/10.1109/HICSS.2015.27
T6	Labus, M., Despotović-Zrakić, M., & Bogdanović, Z. (2017). Introducing adaptive E-business continuity management. Advances in Intelligent Systems and Computing, 569, 628–637. https://doi.org/10.1007/978-3-319-56535-4_62
T7	Lin, C.-S., Kao, S., & Chen, L.-S. (2012). A proactive operational framework for business continuity in the semiconductor industry. Quality and Reliability Engineering International, 28, 307–320. https://doi.org/10.1002/qre.1246
T8	Lindstedt, D. (2017). The capability and constraint model of recoverability: An integrated theory of continuity planning. Journal of business continuity & emergency planning, 11, 52–62. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85037695910&partnerID=40&md5=5a4264f9506e93723021d15d72d3d50c
T9	Margherita, A., & Heikkilä, M. (2021). Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies. Business Horizons, 64, 683–695. https://doi.org/10.1016/j.bushor.2021.02.020

T10	Păunescu, C. (2017). How prepared are small and medium sized companies for business continuity management? Quality - Access to Success, 18, 43–48. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034588398&partnerID=40&md5=1f8bf06d6d9d3f2dac93fc85b39c72b2
T11	Păunescu, C., & Argatu, R. (2020). Critical functions in ensuring effective business continuity management. Evidence from romanian companies. Journal of Business Economics and Management, 21. https://doi.org/10.3846/jbem.2020.12205
T12	Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2021). Framework for designing Business Continuity - Multidisciplinary Evaluation of Organizational Maturity. *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–4. https://doi.org/10.23919/CISTI52073.2021.9476297
T13	Sambo, F., & Bankole, F. O. (2016). A normative process model for ICT business continuity plan for disaster management in small, medium and large enterprises. International Journal of Electrical and Computer Engineering, 6, 2425–2431. https://doi.org/10.11591/ijece.v6i5.11461
T14	Setiawan, A., Wibowo, A., & Susilo, A. H. (2018). Risk analysis on the development of a business continuity plan. Proceedings of the 2017 4th International Conference on Computer Applications and Information Processing Technology, CAIPT 2017, 2018-January, 1–4. https://doi.org/10.1109/CAIPT.2017.8320736
T15	Siciliano, G. G., & Gaudenzi, B. (2018). The role of supply chain resilience on IT and cyber disruptions. Lecture Notes in Information Systems and Organisation, 24, 57–69. https://doi.org/10.1007/978-3-319-62636-9_4
T16	Speight, P. (2011). Business continuity. Journal of Applied Security Research, 6, 529–554. https://doi.org/10.1080/19361610.2011.604021
T17	Suresh, N., Sanders, G. L., & Braunscheidel, M. J. (2020). Business Continuity Management for Supply Chains Facing Catastrophic Events. IEEE Engineering Management Review, 48, 129–138. https://doi.org/10.1109/EMR.2020.3005506
T18	Tan, C., & Lee, S. Z. (2021). Adoption of enterprise risk management (ERM) in small and medium-sized enterprises: evidence from Malaysia. Journal of Accounting and Organizational Change. https://doi.org/10.1108/JAOC-11-2020-0181

Fuente: Elaboración propia.

3.6 Resultados de la revisión

A partir de la revisión de los artículos encontrados como resultados de las búsquedas en las bases de datos mencionadas anteriormente, se procede a dar respuestas a las tres preguntas planteadas.

3.6.1 Respuesta a pregunta P1

¿De qué manera las pymes han hecho frente a incidentes que afectan su continuidad de negocios?

Las empresas han organizado su proceso de continuidad de negocio frente a incidentes graves de diversas formas según la literatura:

Por un lado, implementando un sistema de gestión de continuidad de negocio mediante el uso de la norma ISO 22301:2019 (ISO, 2019), la cual organiza las actividades según el ciclo de Deming, el cual consiste de cuatro fases Planear, Hacer, Verificar y Actuar (PDCA, por sus siglas en inglés), como se puede apreciar en la investigación de (Aronis y Stratopoulos, 2016). Este estudio menciona que muchas instituciones financieras y de seguros en Europa son las que destacan en la sofisticación de estos sistemas de gestión haciendo hincapié el caso del grupo Alpha Bank.

Por otro lado, un estudio llevado a cabo por (Filipović et al., 2018) en Croacia, indica que las empresas deben atender cuatro frentes para organizar su continuidad de negocios sin importar su rubro, los cuales son: *desastres naturales, riesgos estratégicos y operacionales, eventos intencionales y eventos accidentales*. Los riesgos tecnológicos están incluidos dentro de las tres últimas categorías.

Así mismo, (Păunescu y Argatu, 2020) mencionan que, para los gerentes de las pequeñas y medianas empresas, los componentes que tienen mayor relevancia al momento de organizar la continuidad de negocios son: evaluación del riesgo, gestión de la continuidad de negocio, elaboración de estrategias y planes, mantenimiento y evaluación del BCP e incluir la continuidad del negocio en la concientización de la cultura organizacional. El estudio se enfocó en pymes en Rumanía.

Otra forma en la que se gestiona la continuidad de negocios es mediante un marco que consta de tres fases, empezando por el equipo de respuesta de emergencia, gestión de crisis y plan de continuidad de negocios, según explica (Lin et al., 2012), estas fases son progresivas, esto quiere decir que ante la ocurrencia de un evento que amenace la continuidad del negocio,

se empieza por la fase del equipo de respuesta de emergencia y dependiendo del impacto que genere, se va escalando a las siguientes fases. Este caso es importante porque el marco que describe el autor fue aplicado por una compañía taiwanesa que forma parte de la industria de semiconductores, sector que ha desempeñado un papel importante en el desarrollo económico de Taiwán y que por esa razón es crucial garantizar la continuidad del negocio para poder satisfacer las necesidades de los clientes

Otra manera que tienen las empresas de gestionar su continuidad de negocios es por medio del desarrollo de la capacidad de resiliencia, como se puede apreciar en la investigación de (Siciliano y Gaudenzi, 2018) a través de la ejecución de un procedimiento de cinco pasos, los cuales son:

- Planear: se identifican sistemáticamente los riesgos y se plantean medidas para prevenirlos y tratarlos cuando se presenten.
- Responder: se enfrentan los riesgos materializados mediante las medidas planificadas en el paso anterior.
- Recuperar: se restauran las operaciones al estado en el que se encontraban antes de que se materialice el riesgo.
- Adaptar: se revisan las medidas actuales y se hacen los ajustes necesarios en base a la experiencia obtenida, esto se realiza como parte del proceso de mejora continua que se desarrolla dentro de la gestión de riesgos.
- Crecer: se vuelve a repetir el ciclo para que de esta manera se siga aumentando la capacidad de resiliencia.

Para el mercado financiero, (Speight, 2011) comenta que la continuidad de negocio se basa principalmente en tres elementos: plan de riesgo operacional, plan de continuidad de negocios y plan de recuperación ante desastres.

En el caso de Sudáfrica, (Sambo y Bankole, 2016) propusieron agregar el procedimiento de detectar puntos críticos de falla al proceso de desarrollo del plan de continuidad de negocios (BCP), ya que al evaluar el por qué las empresas a pesar de contar con un BCP seguían demorando un periodo de tiempo prolongado en recuperarse, notaron que muchas de ellas no consideraban los riesgos asociados al hardware.

Finalmente, en una investigación hecha a pequeñas y medianas empresas en Malasia, se puede apreciar que este tipo de empresas se enfocan en el plan de continuidad de negocios, políticas para la gestión, evaluación y control de riesgos y gestión de incidentes. Así mismo,

señalan que este tipo de empresas muchas veces se ven limitadas por la cantidad de recursos que poseen, lo cual provoca que el desarrollo de la continuidad de negocios no sea tan completo y en consecuencia queden expuestas a incidentes graves que puedan provocar pérdidas significativas (Tan y Lee, 2021).

3.6.2 Respuesta a pregunta P2

¿Cómo se han aplicado las buenas prácticas internacionalmente aceptadas en el manejo de contingencias de TI, al interior de las pymes?

Las siguientes buenas prácticas internacionalmente aceptadas han sido aplicadas en contextos empresariales de continuidad de negocios:

La norma ISO 31000:2018 (ISO, 2018b), el modelo COSO ERM 2017 (COSO, 2017) y el modelo Tres Líneas de Defensa (IIA, 2013) fueron aplicados para gestionar el riesgo de una empresa colombiana dedicada a la producción y distribución de alimentos en el mes de marzo del 2020, como se puede apreciar en el trabajo de (Gómez et al., 2020) esto consistía en ejecutar los siguientes pasos:

- Identificar los factores de riesgo tanto internos como externos que pueden afectar a la organización, así como a las personas que podrían servir de apoyo en el soporte del sistema de gestión de riesgos, tal como lo menciona la ISO 31000 en su cláusula "Entendiendo la organización y su contexto".
- Valorar el riesgo considerando su impacto y probabilidad de ocurrencia, añadiendo a este resultado el valor de una variable llamada "Phi", la cual es usada por los autores para medir la tendencia del riesgo, para finalmente obtener la severidad de los riesgos.
- Se clasifican los riegos en base a su tipo y severidad, se identifican los escenarios bajo los cuales pueden ocurrir y de esta manera poder proponer el tratamiento más adecuado para cada riesgo.
- Finalmente, esto permitía la elaboración de plan de continuidad de negocios acorde a las necesidades de la empresa, de manera que se pueda minimizar el impacto de los incidentes en caso llegaran a ocurrir.

La norma ISO 27002:2005 fue aplicada por (Setiawan, 2018) como guía para identificar la relación de los siguientes cinco aspectos dentro de una organización:

- Inclusión de seguridad de la información dentro del procesos de gestión de continuidad de negocios.

- Continuidad de negocios y evaluación de riesgos.
- Desarrollo e implementación de planes de continuidad incluyendo seguridad de la información.
- Marco de planeamiento de continuidad de negocios.
- Prueba, mantenimiento y evaluación de los planes de continuidad de negocios.

Además, la norma fue utilizada también como herramienta para proponer controles en la fase de tratamiento de riesgos para:

- Contingencia de TI.
- Mantenimiento de las operaciones del negocio.

Por último, se tiene a la norma ISO 22301:2019, la cual ha sido utilizada como ciclo de mejora continua (PDCA, por sus siglas en inglés) con el objetivo de establecer las políticas de continuidad de negocios y contingencia de TI, de manera que puedan ser mejoradas en base a los resultados que se obtengan de las revisiones (Hersyah y Derisma, 2018).

3.6.3 Respuesta a pregunta P3

¿Qué marcos o modelos multidisciplinares contribuyen a la gestión de la continuidad de negocios haciendo hincapié en las operaciones de TI y sobre qué tratan?

Los marcos o modelos multidisciplinares que contribuyen a la gestión de la continuidad de negocios, según los resultados obtenidos luego de haber realizado la revisión sistemática, están principalmente basados en la ISO 22301, estos varían dependiendo de la perspectiva del autor.

Para el caso del grupo Alpha Bank, el modelo consta de 7 hitos, empezando por la gestión del proyecto, análisis de impacto del negocio, evaluación de riesgos, estrategia de continuidad de negocios, desarrollo del plan, práctica y pruebas y por último la gestión del plan desarrollado (Aronis y Stratopoulos, 2016).

Un marco post crisis es el que plantea (Kulkarni et al., 2015), el cual propone tres aspectos que deben ser considerados por la empresa luego de que el daño ha sido causado, los cuales son: gestión de la crisis, recuperación del negocio y renovación del negocio, así mismo, Kulkarni comenta que este marco también puede ser usado para que las empresas evalúen su plan de continuidad de negocios.

El modelo adaptativo de gestión de continuidad de negocio electrónico como se puede apreciar en la investigación de (Labus et al., 2017) está enfocado básicamente a empresas cuyos

procesos principales son altamente dependientes de las TIC para que puedan ser llevados a cabo. Este modelo consiste en 12 parámetros que reflejan las características básicas del entorno en el que se desarrolla la empresa y 4 métodos que son los componentes básicos del sistema de gestión de la continuidad del negocio (BCMS, por sus siglas en inglés), los cuales son: análisis de impacto del negocio, evaluación de riesgos del comercio electrónico, desarrollo del plan de continuidad de negocios y la mejora continua del BCMS.

El modelo de capacidad y restricción de recuperabilidad consiste en definir limitaciones de dos tipos: suaves (tiempo, costo y alcance) y duras (personas, objetos y ambientes físicos), también llamadas restricciones y pérdidas respectivamente. Luego en base a estas limitaciones se elaboran procedimientos, se desarrollan competencias y se asignan recursos, tal como se menciona en el estudio de (Lindstedt, 2017) estos pasos se repiten hasta que se logre tener el balance entre procedimientos, competencias y recursos requerido por la empresa.

En un contexto más reciente como el de la pandemia, (Margherita y Heikkilä, 2021) evaluaron las acciones de contingencia que tomaron 50 empresas líderes a nivel mundial según el ranking publicado por la revista Fortune en el año 2019 y en base a eso los autores propusieron un marco de acciones de respuesta para COVID-19 a nivel empresarial, el cual consta de cinco áreas de actividades organizacionales que a su vez se dividen en trece subáreas.

Otro marco que también ha sido desarrollado en base a la ISO 22301 es el que propone (Păunescu, 2017), el marco para el desarrollo e implementación del sistema de continuidad de negocio consta de siete pasos: entender el contexto de la organización, asegurar el liderazgo y compromiso de la gestión, planificación de la continuidad del negocio, asegurar recursos y soporte, operar, evaluar y mejorar el BCMS. Este marco fue probado en pequeñas y medianas empresas ubicadas en Bucarest, los resultados indicaron que las organizaciones participantes eran conscientes de la importancia del BCMS, sin embargo, solo el 46% evaluaba sus riesgos o amenazas.

Otros modelos como CMMI proponen la planificación de actividades para mitigar interrupciones en las operaciones, marcos como ITIL presentan prácticas para asegurar la disponibilidad del servicio en caso de desastres, COBIT provee un plan que permite a las organizaciones responder y adaptarse rápidamente ante los incidentes (Russo et al., 2021).

Finalmente, el marco para la gestión de la continuidad del negocio en relación a la gestión de riesgos de la cadena de suministro es presentado por (Suresh et al., 2020), este marco no está relacionado a TI, sin embargo, se puede considerar como un ejemplo que demuestra la

manera en que las normas ISO 22301, ISO 22316 y ISO 31000 a pesar de ser generales, pueden ser adaptadas a casos específicos, como es el caso de este trabajo de fin de carrera.

3.7 Discusión

Si bien es cierto que en la revisión del estado del arte se ha podido encontrar que existen normas ISO para sistemas de gestión de continuidad de negocios y muchas otras normas (NIST, DRI) para aspectos específicos de continuidad, ninguna de ellas tiene un enfoque exclusivo hacia las pymes.

Por otro lado, se ha identificado que la mayoría de estudios sobre continuidad de negocios desarrollados durante la pandemia están orientados hacia la continuidad de operaciones de la cadena de suministros, lo cual no es de mucha utilidad para las pymes, ya que no cuentan con cadenas de suministros complejas. Esta situación genera un vacío para las pymes, dado que, no cuentan con estudios que les ofrezcan un modelo para la continuidad de negocios con enfoque en TI.

3.8 Conclusiones

A partir de la revisión realizada se puede concluir lo siguiente:

No existen marcos que aborden el tema de contingencia de TI de manera profunda, ya que en su mayoría tratan de brindar una visión holística de la continuidad de negocios. Tampoco se ha podido encontrar marcos o modelos multidisciplinares de contingencia de TI que estén orientados a las pymes. De igual manera, no se han encontrado estudios situacionales del impacto de no tener estos modelos en las pymes y su afectación durante la pandemia.

Así mismo, se ha podido identificar que distintas normas ISO han sido aplicadas por algunas empresas para el desarrollo de la continuidad de negocios mayormente en relación a sus operaciones de la cadena de suministros.

Finalmente, esta ausencia de marcos y modelos de continuidad de negocios con enfoque en TI y que estén orientados a pymes representa una oportunidad para que el presente proyecto de tesis desarrolle la implementación un modelo multidisciplinar para el diseño de la continuidad de negocios con enfoque en la contingencia de TI que permita cubrir el vacío existente.

Capítulo 4. Resultados esperados del objetivo específico 1

En el presente capítulo se mostrará la matriz de trazabilidad obtenida como resultado del objetivo específico 1.

4.1 Resultado esperado R1

Para el logro de este objetivo se procedió a identificar los temas que serán abordados dentro de cada componente del modelo de continuidad de negocios con enfoque en TIC que se propondrá como resultado del presente trabajo de tesis, los temas fueron seleccionados en base al trabajo de (Russo et al., 2021), el cual muestra las brechas que existen al momento de definir formalmente las actividades de los componentes de la gestión de continuidad de negocios. Luego, se identificaron las normas relacionadas a estos temas y que, además puedan ser de utilidad para el desarrollo del modelo.

En la Figura 12 se muestra una visión general del modelo:

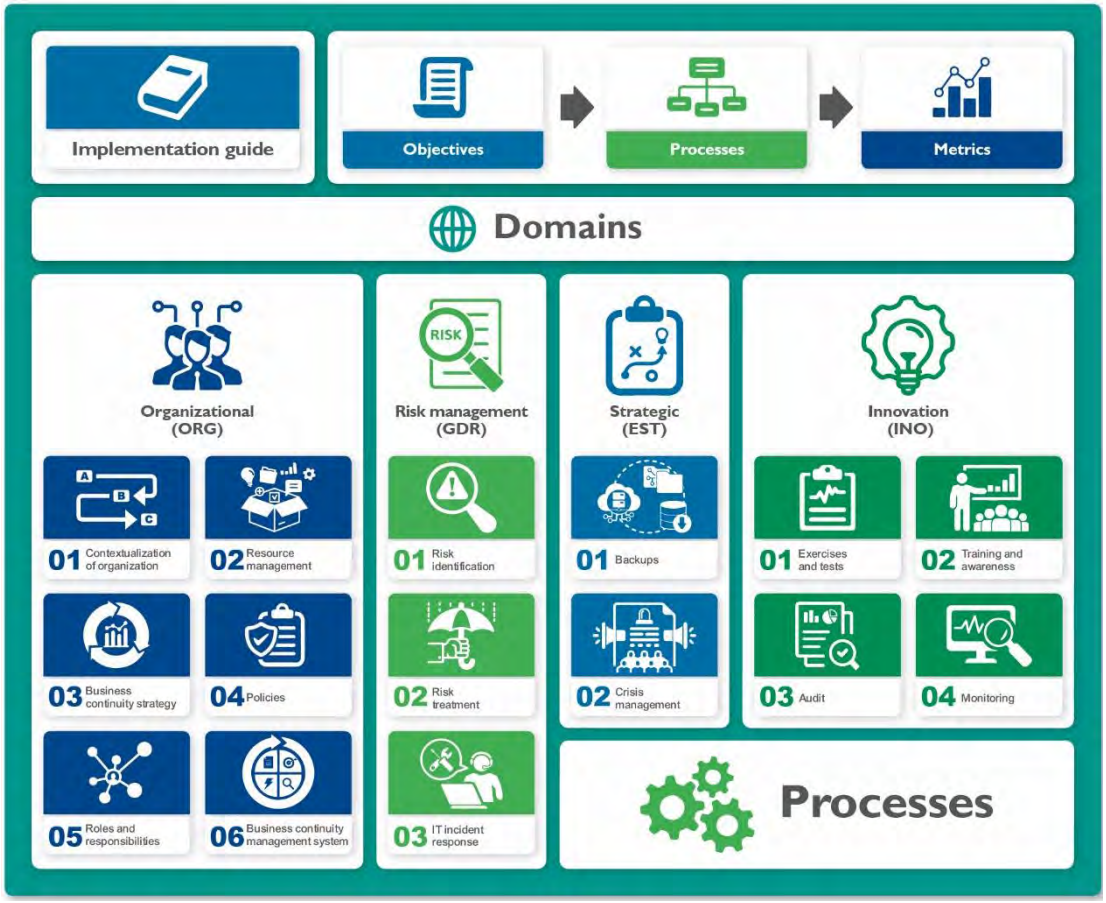


Figura 12. Visión general. Fuente: Elaboración propia.

En la Tabla 9 se muestra la matriz de trazabilidad elaborada para este objetivo.

Tabla 9. Matriz de trazabilidad

ID	Componente	Tema	Norma/Marco	Descripción	Justificación
N1	Todos	- Contextualización de la organización. - Gestión de recursos. - Estrategia de continuidad de negocios. - Políticas. - BCMS. - Identificación de riesgos. - Tratamiento de riesgos. - Respuesta a incidentes de TI. - Ejercicios y pruebas. - Entrenamiento y concientización. - Monitoreo.	ISO 22301: Seguridad y resiliencia - Sistemas de gestión de la continuidad de negocios - Requerimientos	La norma especifica la estructura y los requerimientos para la implementación y mantenimiento de un sistema de continuidad de negocios.	Dado que el modelo a desarrollarse contará con 4 componentes (organizacional, gestión de riesgos, estratégico e innovación), esta norma servirá de guía para determinar lo que se deberá cubrir en cada componente.
N2	Organizacional, Gestión de riesgos e Innovación	- Gestión de recursos. - Políticas. - Roles y responsabilidades. - Tratamiento de riesgos. - Ejercicios y pruebas.	ISO 27031: Tecnologías de la Información - Técnicas de seguridad - Directrices para la preparación de las TIC para la continuidad de negocios	La norma describe los conceptos y principios relacionados a la preparación de las TICs para la continuidad de negocios, también, provee un marco de métodos y procesos para identificar y especificar todos los aspectos para mejorar la preparación de las TICs de una empresa y	Dado que se va a desarrollar un modelo para el diseño de la continuidad de negocios con un enfoque TIC, esta norma servirá para saber que consideraciones relacionadas a las TICs se deben tener en cuenta en el desarrollo de los componentes del modelo.

				asegurar la continuidad de negocios.	
N3	Organizacional	- Roles y responsabilidades.	COBIT 2019	Es un marco de gobierno y gestión de TI dirigido a toda la empresa, que define los componentes para la construcción y mantenimiento de un sistema de gobierno.	Se tomará como referencia las pautas que brinda COBIT para la definición de roles y asignación de responsabilidades.
N4	Gestión de riesgos	- Respuesta a incidentes de TI.	NIST 800-34: Guía de planificación de contingencia para Sistemas de Información Federales	La norma provee instrucciones, recomendaciones y consideraciones para la planificación de contingencia para sistemas de información. La guía define un proceso de planificación de contingencia de siete pasos, el cual puede ser aplicado por cualquier organización para desarrollar y mantener un programa de planificación de contingencia para sus sistemas de información.	Esta norma tiene como anexos un conjunto de plantillas para la elaboración de planes de contingencia, los cuales pueden servir de guía para la elaboración de la documentación que propondrá el modelo dentro del componente de gestión de riesgo.
N5	Gestión de riesgo, Estratégico	- Tratamiento de riesgos. - Backups.	ISO 27002: Tecnologías de la Información - Técnicas de seguridad - Código de	Esta norma brinda pautas para la selección, implementación y gestión de controles relacionados	Las pautas brindadas en esta norma servirán como guía para la elaboración de los controles que ofrecerá el modelo en el

			prácticas para controles de seguridad de información	a la seguridad de la información, considerando el entorno de riesgo al que está expuesta la organización.	componente de gestión de riesgos. Así mismo, ofrece pautas que deben considerarse en el proceso de backup correspondiente al componente estratégico.
N6	Gestión de riesgos	- Identificación de riesgos. - Tratamiento de riesgos. - Respuesta a incidentes de TI.	ISO 31000: Gestión del riesgo - Directrices	Esta norma proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones.	La norma dentro de su proceso considera la evaluación y tratamiento del riesgo, lo cual está dentro del propósito del componente de gestión de riesgos.
N7	Organizacional y Estratégico	- Políticas. - BCMS. - Gestión de crisis.	ISO 22316: Seguridad y resiliencia - Resiliencia organizacional - Principios y atributos	Esta norma proporciona una guía para mejorar la resiliencia organizacional para empresas de cualquier tipo y tamaño.	Los principios y atributos descritos en la norma, servirán de guía para la elaboración de los procesos y actividades que propondrá el modelo dentro del componente organizacional.
N8	Organizacional, Gestión de riesgos y Estratégico	- BCMS. - Identificación de riesgos. - Tratamiento de riesgos. - Respuesta a incidentes de TI. - Gestión de crisis.	ISO 22317: Seguridad y resiliencia - Sistemas de gestión de la continuidad de negocios - Directrices para el análisis de impacto del negocio	Esta norma proporciona una guía para implementar y mantener un proceso de análisis de impacto del negocio (documentado y formal) apropiado a las necesidades de la empresa.	Con el análisis de impacto del negocio se puede conocer que procesos de la empresa son más críticos al momento de que ocurra un incidente, sabiendo esto se pueden priorizar los procesos de acuerdo a su impacto y proponer medidas adecuadas.
N9	Estratégico	- Gestión de crisis.	ISO 22361: Seguridad y resiliencia - Gestión de	Esta norma proporciona una guía para la gestión de la crisis, con la	Se tomará como referencia el proceso de gestión de crisis propuesto por esta norma para el

			crisis - Directivas para una capacidad estratégica	finalidad de ayudar a las organizaciones en la planificación, establecimiento, mantenimiento, revisión y mejora continua de su capacidad estratégica en la gestión de crisis.	desarrollo de las actividades que se propondrán en el modelo.
N10	Innovación	- Auditoría/Revisión.	ISO 19011: Directrices para la auditoría de los sistemas de gestión	Esta norma proporciona una guía sobre la auditoría de sistemas de gestión, incluyendo los principios de auditoría, la gestión de un programa de auditoría y la evaluación de las competencias de las personas involucradas en el proceso de auditoría.	Las pautas brindadas en esta norma servirán para definir los objetivos, criterios, alcance, etc. que deberán considerarse dentro de las actividades de auditoría que se propongan en el modelo.

Fuente: Elaboración propia.

En el Anexo B se muestra el acta de validación del resultado esperado R1.

Capítulo 5. Resultados esperados del objetivo específico 2

En el presente capítulo se mostrarán los cinco resultados esperados del objetivo específico 2.

5.1 Resultado esperado R2

Se tiene como resultado esperado la estructura del modelo en función de dominios. En la Tabla 10 se muestra cada dominio con sus respectivos procesos, la cual ha sido elaborada en base a la lista de componentes y temas presentada en el capítulo anterior.

Tabla 10. Dominios y procesos.

Dominio	Proceso
Organizacional (ORG)	01. Contextualización de la organización.
	02. Gestión de recursos.
	03. Estrategia de continuidad de negocios.
	04. Políticas.
	05. Roles y responsabilidades.
	06. Sistema de gestión de la continuidad de negocios.
Gestión de riesgos (GDR)	01. Identificación de riesgos.
	02. Tratamiento de riesgos.
	03. Respuesta a incidentes de TI.
Estratégico (EST)	01. Backups.
	02. Gestión de crisis.
Innovación (INO)	01. Ejercicios y pruebas.
	02. Entrenamiento y concientización.
	03. Auditoría.
	04. Monitoreo.

Fuente: Elaboración propia.

En los próximos subcapítulos se presentará un resultado específico por cada dominio, en el cual se detallará cada proceso indicando descripción, propósito, actividades, documentación (marcos, normas) relacionada tomada como referencia, actividades de implementación y métricas.

En el Anexo C se muestra el acta de validación del resultado esperado R2.

5.2 Resultado esperado R3

A continuación, se presenta el componente organizacional del modelo.

5.2.1 Contextualización de la organización (ORG01)

Tabla 11. ORG01 - Contextualización de organización.

Dominio: ORGANIZACIONAL **ORG01 – Contextualización de la organización**	
Descripción	
Determinar los aspectos internos y externos que pueden afectar a la pyme, en lo concerniente a su continuidad de negocios y al manejo de la contingencia de TI. Los responsables de llevar a cabo esto deberían ser los miembros de la alta dirección de la organización.	
Propósito	
Tener claro el contexto en el que se desarrolla la pyme, de manera que sirva de input para los siguientes procesos y se puedan tomar decisiones estratégicas efectivas con respecto a su resiliencia organizacional.	
Actividades del proceso	
1. Identificar la misión, visión y objetivos estratégicos de la pyme.	
2. Identificar e involucrar a los interesados tanto internos como externos a la pyme.	
3. Realizar el análisis PESTLE para identificar aquellos factores externos que representen una amenaza a la continuidad de negocios y contingencia de TI de la pyme.	
4. Elaborar la matriz FODA para identificar aquellos factores internos que representen una amenaza a la continuidad de negocios y contingencia de TI de la pyme.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 4.1
ISO 22316	Cláusula 5.3

Actividades de implementación	Actividad de proceso
Identificar la misión, visión y objetivos estratégicos de la pyme.	1
Elaborar modelos de simulación empresarial.	1
Identificar a las partes interesadas internas y externas.	2
Fortalecer las relaciones con las partes interesadas.	2
Involucrar activamente a las partes interesadas.	2
Definir un equipo de trabajo multidisciplinar	3
Identificar el marco regulatorio al que está expuesta la pyme.	3
Elaborar una plantilla para el análisis PESTLE.	3
Establecer la frecuencia con la que se actualizará el análisis PESTLE.	3
Elaborar una plantilla de la matriz FODA.	4
Identificar las debilidades de la pyme mediante un análisis de impacto del negocio (BIA).	4
Identificar las amenazas que podrían provocar un incidente grave que afecte la continuidad de negocios de la pyme.	4
Identificar las fortalezas de la pyme para luego proponer controles y estrategias que puedan hacer frente a las amenazas.	4
Planificar simulacros para probar las estrategias de continuidad de negocios y de esa manera tener la oportunidad de mejorar las mismas.	4
Establecer la frecuencia con la que se actualizará la matriz FODA.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se revisa anualmente la matriz FODA.	Numérico sin unidades
Número de veces que se revisa anualmente el análisis PESTLE.	Numérico sin unidades

Fuente: Elaboración propia.

5.2.2 Gestión de recursos (ORG02)

Tabla 12. ORG02 - Gestión de recursos.

Dominio: ORGANIZACIONAL **ORG02 – Gestión de recursos**	
Descripción	
Gestionar aquellos recursos humanos, materiales, tecnológicos y financieros con los que cuenta la pyme y que van a ser utilizados con la finalidad de preservar la continuidad del negocio y la contingencia de TI en caso se requiera. Los responsables de llevar a cabo esto deberían ser la alta dirección y los responsables de las tecnologías de información.	
Propósito	
Gestionar los recursos de la pyme para garantizar el establecimiento, implementación, mantención y mejora de su continuidad de negocios y la contingencia de TI.	
Actividades del proceso	
1. Gestionar los recursos humanos necesarios para las funciones de continuidad de negocios y contingencia de TI.	
2. Gestionar los recursos materiales necesarios para las funciones de continuidad de negocios y contingencia de TI.	
3. Gestionar los recursos tecnológicos necesarios para las funciones de continuidad de negocios y contingencia de TI.	
4. Gestionar los recursos financieros necesarios para las funciones de continuidad de negocios y contingencia de TI.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 7.1
Actividades de implementación	**Actividad de proceso**
Determinar las competencias necesarias con las que debe contar el personal.	1
Evaluar las aptitudes y actitudes del personal.	1
Realizar un inventario de los recursos materiales con los que se cuenta para las funciones de contingencia de TI.	2

Establecer la frecuencia con la que se actualizará el inventario.	2
Realizar un inventario de los recursos tecnológicos con los que se cuenta para las funciones de contingencia de TI.	3
Evaluar si los servicios tecnológicos brindados por terceros cumplen con la política de continuidad de negocios de la pyme.	3
Elaborar un reporte con el presupuesto que cuenta la pyme para el desarrollo de su continuidad de negocios.	4
Métricas e indicadores	**Rango de valores de la métrica**
Cantidad de personas que cuentan con las competencias necesarias para el desarrollo de la continuidad de negocios y la contingencia de TI de la pyme.	Numérico (Unidad: persona)
Porcentaje anual utilizado del presupuesto asignado para los recursos humanos, materiales y tecnológicos necesarios para las funciones de continuidad de negocios y contingencia de TI.	Numérico sin unidades

Fuente: Elaboración propia.

5.2.3 Estrategia de continuidad de negocios (ORG03)

Tabla 13. ORG03 - Estrategia de continuidad de negocios.

Dominio: ORGANIZACIONAL **ORG03 – Estrategia de continuidad de negocios**	
Descripción	
Definir, gestionar y monitorear la estrategia de continuidad de negocios que seguirá la pyme, de manera que se garantice el cumplimiento de todas las condiciones necesarias para la reanudación de las actividades, en el caso de que se materialice una amenaza. Los responsables de llevar a cabo esto deberían ser los miembros de la alta dirección y el gerente de TI.	
Propósito	
Tener definida una estrategia de continuidad de negocios, de manera que más adelante se puedan elaborar políticas de continuidad de negocios y contingencia de TI acordes a esta.	
Actividades del proceso	
1. Definir la estrategia de continuidad de negocios.	
2. Gestionar la estrategia de continuidad de negocios.	
3. Monitorear y evaluar la estrategia de continuidad de negocios.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 8.3
Actividades de implementación	**Actividad de proceso**
Evaluar la situación actual de la pyme con respecto a la continuidad de negocios y contingencia de TI.	1
Definir el objetivo y el alcance de la estrategia de continuidad de negocios en base a la evaluación realizada previamente.	1

Establecer la fecha límite en la que se deberá cumplir con el objetivo de la estrategia de continuidad de negocios.	1
Asignar al encargado de la gestión de la estrategia de continuidad de negocios.	2
Establecer la frecuencia con la que se actualizará la estrategia de continuidad de negocios.	2
Comunicar a los involucrados la estrategia de continuidad de negocios que seguirá la pyme.	2
Definir los indicadores con los cuales se medirá la efectividad de la estrategia de continuidad de negocios.	3
Evaluar el cumplimiento de la estrategia de continuidad de negocios.	3
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se evalúa anualmente el cumplimiento de la estrategia de continuidad de negocios.	Numérico sin unidades
Cantidad de incumplimientos de la estrategia de continuidad de negocios detectados anualmente.	Numérico sin unidades

Fuente: Elaboración propia.

5.2.4 Políticas (ORG04)

Tabla 14. ORG04 - Políticas.

Dominio: ORGANIZACIONAL **ORG04 – Políticas**	
Descripción	
Establecer, implementar, mejorar de manera continua y documentar la política de continuidad de negocios y todas aquellas políticas que seguirá la pyme para el desarrollo de su resiliencia organizacional. Los responsables de llevar a cabo esto deberían ser los miembros de la alta dirección.	
Propósito	
Obtener un documento que especifique las directrices de continuidad de negocios que seguirá la pyme; así como, la difusión y concientización en toda la pyme.	
Actividades del proceso	
1. Establecer el compromiso de la alta dirección con respecto a la política.	
2. Elaborar y documentar la política.	
3. Gestionar el cumplimiento de la política.	
4. Difundir la política.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 5.2
ISO/IEC 27031	Cláusula 5.7.2
ISO 22316	Cláusula 5.5
Actividades de implementación	**Actividad de proceso**
Mostrar de qué manera la política beneficiará a la pyme.	1
Elaborar un acta de compromiso.	1

Identificar los objetivos de continuidad de negocios de la pyme.	2
Definir el alcance de la política.	2
Definir la fecha desde la cual la política será vigente.	2
Documentar y publicar la política.	2
Asignar al encargado de la gestión de la política.	3
Establecer la frecuencia con la que se revisará y/o actualizará la política.	3
Evaluar que lo establecido en la política aún este acorde con los objetivos de la pyme.	3
Compartir la política con todos los trabajadores de la pyme.	4
Adecuar la cultura organizacional de tal manera que se incluya lo establecido en la política.	4
Organizar talleres de concientización de la política.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se revisa anualmente la política.	Numérico sin unidades
Cantidad de incumplimientos de la política detectados anualmente.	Numérico sin unidades
Perdidas monetarias que ha tenido la pyme debido al incumplimiento de la política.	Numérico (Unidad: Monetaria)
Pérdidas humanas que ha tenido la pyme debido al incumplimiento de la política.	Numérico (Unidad: Persona)
Pérdidas materiales que ha tenido la pyme debido al incumplimiento de la política.	Numérico sin unidades

Fuente: Elaboración propia.

5.2.5 Roles y responsabilidades (ORG05)

Tabla 15. ORG05 - Roles y responsabilidades.

Dominio: ORGANIZACIONAL **ORG05 – Roles y responsabilidades**	
Descripción	
Definir, monitorear y supervisar los roles y responsabilidades asignados al personal, de tal manera que estén acorde a las políticas y procedimientos de continuidad de negocios de la pyme. Los responsables de llevar a cabo esto deberían ser los miembros de la alta dirección y el gerente de TI.	
Propósito	
Asegurar que se asignen las responsabilidades y los encargados para cada rol definido; así como, la difusión en toda la pyme y la supervisión de su cumplimiento.	
Actividades del proceso	
1. Definir los roles y sus respectivas responsabilidades.	
2. Definir los perfiles adecuados para cada rol.	
3. Asignar los roles de tal manera que se evite tener dependencia en individuos clave.	
4. Difundir y supervisar los roles y responsabilidades asignados.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
COBIT 2019	APO07
ISO 22301	Cláusula 5.3
Actividades de implementación	**Actividad de proceso**
Definir los roles y responsabilidades necesarios para cada proceso de tal manera que se cumpla con las políticas de la pyme.	1
Elaborar un documento en el que se especifiquen los roles con sus responsabilidades.	1

Establecer la frecuencia con la que se revisará el documento definido en el punto anterior.	1
Definir las aptitudes y actitudes necesarias para cada rol.	2
Identificar el perfil de cada trabajador que participará en los procesos de continuidad de negocios.	3
Elaborar la matriz RACI de manera que se utilice a todo el personal involucrado y se minimice la dependencia.	3
Establecer la frecuencia con la que se actualizará la matriz RACI.	3
Comunicar a todo el personal sobre los roles asignados.	4
Capacitar al personal de acuerdo a su rol asignado.	4
Elaborar un documento para cada rol en el que se especifiquen sus objetivos y responsabilidades.	4
Definir las métricas con las que se evaluará el cumplimiento de los objetivos de cada rol.	4
Establecer la frecuencia con la que se medirá el logro de los objetivos de cada rol.	4
Realizar informes de las evaluaciones y mostrarlos a la alta dirección.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se revisa anualmente la matriz RACI.	Numérico sin unidades
Número de incumplimientos de la matriz RACI.	Numérico sin unidades
Número de capacitaciones que se brindan anualmente al personal.	Numérico sin unidades

Fuente: Elaboración propia.

5.2.6 Sistema de gestión de continuidad de negocios (ORG06)

Tabla 16. ORG06 - Sistema de gestión de continuidad de negocios.

Dominio: ORGANIZACIONAL **ORG06 – Sistema de gestión de continuidad de negocios**	
Descripción	
Definir, implementar y mejorar de manera continua el sistema de gestión de continuidad de negocios (BCMS) de la pyme, de manera que incluya todos los procesos necesarios para el manejo de la contingencia de TI. El responsable de llevar a cabo esto debería ser el gerente de TI.	
Propósito	
Contar con un BCMS que ayude a la pyme a estar preparada antes, durante y después de que ocurra un evento disruptivo.	
Actividades del proceso	
1. Definir el BCMS.	
2. Implementar el BCMS.	
3. Evaluar el BCMS.	
4. Mejorar el BCMS.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusulas del 4 al 10
Actividades de implementación	**Actividad de proceso**
Identificar los requerimientos legales y regulatorios a los que está sujeta la pyme.	1
Definir el alcance que tendrá el BCMS.	1
Definir políticas de contingencia de TI y continuidad de negocios.	1
Identificar los riesgos que pueden afectar la continuidad de negocios de la pyme.	1
Realizar el análisis de impacto del negocio (BIA).	2

Evaluar los riesgos identificados anteriormente.	2
Definir las estrategias y soluciones de continuidad de negocios.	2
Elaborar los planes de continuidad de negocios y contingencia de TI.	2
Capacitar al personal sobre la gestión de continuidad de negocios.	2
Definir qué aspectos del BCMS se medirán y cómo se medirán.	3
Definir y ejecutar escenarios de prueba para medir la efectividad de las estrategias planteadas.	3
Elaborar un plan de auditoría.	3
Identificar los puntos débiles del BCMS en base a las pruebas ejecutadas anteriormente.	4
Desarrollar mejoras que cubran los puntos débiles identificados.	4
Evaluar el contexto organizacional para adecuar el BCMS en caso sea necesario.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se realiza anualmente la evaluación de riesgos.	Numérico sin unidades
Número de pruebas que se realizan anualmente al BCMS.	Numérico sin unidades
Número de veces al año que la alta dirección revisa el BCMS.	Numérico sin unidades
Número de veces que se audita anualmente el BCMS.	Numérico sin unidades

Fuente: Elaboración propia.

En el Anexo D se muestra el acta de validación del resultado esperado R3.

5.3 Resultado esperado R4

A continuación, se presenta el componente de innovación del modelo.

5.3.1 Ejercicios y pruebas (INO01)

Tabla 17. INO01 - Ejercicios y pruebas.

Dominio: INNOVACIÓN **INO01 – Ejercicios y pruebas**	
Descripción	
Planificar, ejecutar y mejorar las pruebas mediante las cuales se entrenará al personal involucrado en las funciones de continuidad de negocios y contingencia de TI de la pyme. El encargado de llevar a cabo esto debería ser el gerente de TI en conjunto con los subgerentes o jefes del área de TI y del área de recursos humanos.	
Propósito	
Definir y llevar a cabo las pruebas mediante las cuales se validarán las estrategias de continuidad de negocios y contingencia de TI que ha implementado la pyme.	
Actividades del proceso	
1. Planificar las pruebas.	
2. Ejecutar las pruebas.	
3. Evaluar los resultados de las pruebas.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 8.5
ISO/IEC 27031	Cláusula 8.1.3
Actividades de implementación	**Actividad de proceso**

Definir el alcance del plan de pruebas.	1
Definir las pruebas indicando descripción, objetivos, alcance, roles y responsabilidades de los involucrados y criterios de éxito.	1
Elaborar el calendario de ejecución de las pruebas.	1
Definir los resultados esperados de las pruebas.	1
Documentar todas las pruebas dentro del plan de pruebas.	1
Comunicar el plan de pruebas a la alta dirección y los involucrados.	1
Ejecutar las pruebas de acuerdo al calendario establecido.	2
Documentar los resultados de la ejecución de las pruebas.	2
Analizar los resultados de las pruebas.	3
Calificar los resultados de las pruebas.	3
Identificar aspectos de mejora de las pruebas, así como de los recursos humanos y tecnológicos.	3
Documentar el proceso de mejora como resultado de la ejecución de las pruebas.	3
Métricas e indicadores	**Rango de valores de la métrica**
Número de mejoras introducidas en el proceso de contingencia de TI como resultado de la ejecución del plan de pruebas.	Numérico sin unidades
Número de veces que se ejecuta anualmente el plan de pruebas.	Numérico sin unidades

Fuente: Elaboración propia.

5.3.2 Entrenamiento y concientización (INO02)

Tabla 18. INO02 - Entrenamiento y concientización.

Dominio: INNOVACIÓN **INO02 – Entrenamiento y concientización**	
Descripción	
Definir e implementar las estrategias mediante las cuales se capacita y concientiza a todos los trabajadores de la pyme con respecto a continuidad de negocios y contingencia de TI, de acuerdo a su cargo y sus funciones. El encargado de llevar a cabo esto debería ser el gerente de TI en conjunto con el gerente de recursos humanos.	
Propósito	
Establecer una cultura de continuidad de negocios y contingencia de TI a todo nivel en la pyme.	
Actividades del proceso	
1. Definir la estrategia de capacitación y concientización sobre continuidad de negocios y contingencia de TI.	
2. Implementar la estrategia de capacitación y concientización sobre continuidad de negocios y contingencia de TI.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 8.5
Actividades de implementación	**Actividad de proceso**
Definir la estrategia de capacitación y concientización.	1
Agrupar a los trabajadores de acuerdo al nivel de capacitación y concientización que requieran en base a sus roles y responsabilidades.	1
Elaborar un calendario para las capacitaciones y concientizaciones de todos los grupos.	1
Definir los criterios de éxito de la capacitación y concientización de cada grupo.	1
Brindar las capacitaciones y concientizaciones respetando el alcance y fechas definidas para cada grupo.	2

Evaluar el resultado de las capacitaciones y concientizaciones según los criterios de éxito definidos en la estrategia.	2
Solicitar feedback sobre los procesos de capacitación y concientización.	2
Identificar e implementar aspectos de mejora para las capacitaciones y concientizaciones.	2
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se capacita y concientiza anualmente a los trabajadores en temas de continuidad de negocios y contingencia de TI.	Numérico sin unidades
Cantidad de personas que participan de las capacitaciones y concientizaciones.	Numérico (Unidad: Persona)

Fuente: Elaboración propia.

5.3.3 Auditoría (INO03)

Tabla 19. INO03 - Auditoría.

Dominio: INNOVACIÓN **INO03 – Auditoría**	
Descripción	
Definir y ejecutar un plan de auditoría, de manera que la pyme cuente con un procedimiento definido para la evaluación de sus estrategias de continuidad de negocios, los planes de contingencia de TI y los recursos involucrados en ambos. El encargado de llevar a cabo esto debería ser el auditor de TI.	
Propósito	
Evaluar el cumplimiento de los objetivos establecidos en la estrategia de continuidad de negocios y contingencia de TI, así como la eficiencia y efectividad de las acciones llevadas a cabo.	
Actividades del proceso	
1. Definir el plan de auditoría.	
2. Ejecutar el plan de auditoría.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 19011	Cláusulas 5 y 6
Actividades de implementación	**Actividad de proceso**
Establecer los objetivos del plan de auditoría.	1
Identificar los elementos (p. ej. planes, controles, recursos, etc.) concernientes a continuidad de negocios y contingencia de TI que serán evaluados, así como, sus responsables e involucrados.	1
Definir los métodos y criterios de evaluación que serán usados durante la auditoría.	1
Documentar el plan de auditoría y planificar su ejecución.	1

Recolectar y verificar información sobre cada elemento en evaluación.	2
Evaluar la información recolectada.	2
Elaborar un reporte con las conclusiones de la auditoría.	2
Identificar oportunidades de mejora en base a los resultados de la auditoría.	2
Métricas e indicadores	**Rango de valores de la métrica**
Número de mejoras introducidas en el proceso de contingencia de TI como resultado de la auditoría a la estrategia, los planes y los recursos involucrados.	Numérico sin unidades
Cantidad de elementos que cumplen satisfactoriamente con los criterios de evaluación de la auditoría.	Numérico sin unidades

Fuente: Elaboración propia.

5.3.4 Monitoreo (INO04)

Tabla 20. INO04 - Monitoreo.

Dominio: INNOVACIÓN **INO04 – Monitoreo**	
Descripción	
Definir e implementar un procedimiento mediante el cual se monitoree y mida el desempeño de las estrategias de continuidad de negocios y contingencia de TI implementadas en la pyme. El encargado de llevar a cabo esto debería ser el gerente de TI.	
Propósito	
Asegurar y mejorar el desempeño de las estrategias de continuidad de negocios y contingencia de TI.	
Actividades del proceso	
1. Definir el procedimiento de monitoreo.	
2. Implementar el procedimiento de monitoreo.	
3. Reportar el monitoreo.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 22301	Cláusula 9.1
ISO/IEC 27031	Cláusula 8.1.2
ISO 31000	Cláusula 6.6
Actividades de implementación	**Actividad de proceso**
Identificar los elementos (p. ej. planes, controles, recursos, etc.) concernientes a continuidad de negocios y contingencia de TI que serán monitoreados.	1
Definir las métricas e indicadores mediante los cuales se medirá el desempeño de cada elemento identificado.	1

Definir el nivel mínimo de desempeño aceptable para cada elemento identificado.	1
Definir el método mediante el cual se monitoreará cada elemento identificado.	1
Definir la frecuencia con la que se monitoreará cada elemento identificado.	1
Asignar a los responsables del monitoreo de cada elemento identificado.	1
Documentar los resultados del procedimiento de monitoreo.	1
Ejecutar el procedimiento de monitoreo.	2
Analizar y evaluar la información recolectada del procedimiento de monitoreo.	3
Elaborar un informe con el análisis realizado y los puntos de mejora identificados.	3
Métricas e indicadores	**Rango de valores de la métrica**
Número de elementos que no tienen el desempeño esperado y generar interrupciones en la continuidad de negocios.	Numérico sin unidades
Porcentaje de elementos que cumplen con el desempeño esperado.	Numérico sin unidades

Fuente: Elaboración propia.

En el Anexo E se muestra el acta de validación del resultado esperado R4.

5.4 Resultado esperado R5

A continuación, se presenta el componente de gestión de riesgos del modelo.

5.4.1 Identificación de riesgos (GDR01)

Tabla 21. GDR01 - Identificación de riesgos.

Dominio: GESTIÓN DE RIESGOS **GDR01 – Identificación de riesgos**	
Descripción	
Identificar, analizar y evaluar aquellos riesgos de TI a los que está expuesta la pyme y que pueden tener un impacto negativo sobre su continuidad de negocios, en caso lleguen a ocurrir. Este proceso deberá incluirse dentro de la gestión de riesgos que la pyme ejecute para otras áreas. El responsable de llevar a cabo esto debería ser el gerente de TI en conjunto con los subgerentes o jefes del área de TI.	
Propósito	
Identificar los riesgos de TI de pueden afectar a la pyme, de manera que más adelante puedan ser tratados.	
Actividades del proceso	
1. Determinación del contexto.	
2. Inventariar y valorizar los activos de TI.	
3. Analizar los riesgos de TI.	
4. Evaluar los riesgos de TI, de manera que se determine el impacto y la probabilidad de ocurrencia.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 31000	Cláusula 6.4
Actividades de implementación	**Actividad de proceso**
Contextualizar el entorno tanto interno como externo en el que se desarrolla la pyme.	1

Identificar los activos de TI que serán considerandos dentro de la gestión de riesgos.	2
Valorizar los activos de TI identificados.	2
Priorizar los activos de TI identificados.	2
Documentar el inventario de los activos de TI y su valorización.	2
Identificar las vulnerabilidades de cada activo de TI.	3
Identificar las amenazas que pueden afectar a los activos de TI.	3
Identificar los riesgos asociados a cada activo de TI.	3
Identificar los escenarios bajo los cuales podrían presentarse los riesgos de TI.	3
Determinar el impacto que generaría sobre la pyme la ocurrencia de los riesgos de TI.	4
Calcular la probabilidad de ocurrencia de cada riesgo de TI.	4
Valorizar los riesgos de TI en base a su probabilidad de ocurrencia e impacto.	4
Documentar el análisis y evaluación de los riesgos de TI.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se actualiza anualmente el contexto interno y externo.	Conjunto numérico sin unidades
Número de veces que se analizan y evalúan anualmente los riesgos de TI.	Numérico sin unidades

Fuente: Elaboración propia.

5.4.2 Tratamiento de riesgos (GDR02)

Tabla 22. GDR02 - Tratamiento de riesgos.

Dominio: GESTIÓN DE RIESGOS **GDR02 – Tratamiento de riesgos**	
Descripción	
Elegir el tratamiento más adecuado para cada riesgo de TI que puede afectar negativamente la continuidad de negocios de la pyme, así como el diseño e implementación de controles para hacerles frente. El responsable de llevar a cabo esto debería ser el gerente de TI en conjunto con los subgerentes o jefes del área de TI.	
Propósito	
Identificar y definir de qué manera la pyme afrontará los riesgos de TI.	
Actividades del proceso	
1. Elegir el tratamiento de riesgo más adecuado.	
2. Diseñar controles para hacer frente a los riesgos de TI, según el tratamiento seleccionado.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO 31000	Cláusula 6.5
ISO/IEC 27002	Cláusula 4.3
Actividades de implementación	**Actividad de proceso**
Consultar con el responsable del activo de TI si el(los) riesgo(s) asociado debe ser eliminado, transferido, mitigado o tolerado.	1
Evaluar el costo beneficio de cada tipo de tratamiento para todos los riesgos.	1
Definir el tipo de tratamiento que se le dará al riesgo.	1
Definir de qué trata el control.	2

Definir cuál es el propósito del control, clasificándolo como preventivo, detectivo o correctivo.	2
Definir cómo el control debe ser implementado.	2
Definir quién es el responsable del control.	2
Implementar los controles definidos.	2
Establecer las métricas con las que se evaluarán los controles.	2
Documentar todos los controles diseñados.	2
Establecer la frecuencia con la que se revisarán los controles.	2
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se revisan anualmente el diseño y desempeño de los controles definidos para los riesgos de TI.	Numérico sin unidades

Fuente: Elaboración propia.

5.4.3 Respuesta a incidentes de TI (GDR03)

Tabla 23. GDR03 - Respuesta a incidentes de TI.

Dominio: GESTIÓN DE RIESGOS **GDR03 – Respuesta a incidentes de TI**	
Descripción	
Definir y elaborar los planes de contingencia de TI y recuperación ante desastres, de manera que, se garantice la continuidad de negocios de la pyme por lo menos a un nivel mínimo aceptable. El responsable de llevar a cabo esto debería ser el gerente de TI en conjunto con los subgerentes o jefes del área de TI.	
Propósito	
Contar con procedimientos definidos para actuar durante y después de la ocurrencia de un evento disruptivo.	
Actividades del proceso	
1. Elaborar el plan de contingencia de TI.	
2. Elaborar el plan de recuperación ante desastres enfocado a TI.	
3. Gestionar los planes de contingencia de TI y recuperación ante desastres.	
4. Conformar y gestionar los equipos de respuesta a incidentes.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
NIST 800-34	Capítulos 3 y 4
ISO/IEC 27031	Cláusula 6.3.2
Actividades de implementación	**Actividad de proceso**
Definir el objetivo del plan de contingencia.	1
Listar las tareas relacionadas con el uso y aplicación de los controles detectivos y correctivos diseñados en la gestión de riesgos.	1

Definir los roles y responsabilidades mediante una matriz RACI.	1
Establecer una estrategia de contingencia de TI.	1
Definir las estrategias de contingencia.	1
Definir los procedimientos para llevar a cabo cada estrategia.	1
Documentar y difundir el plan de contingencia de TI.	1
Definir el alcance del plan de recuperación ante desastres.	2
Definir las estrategias de recuperación para cada escenario.	2
Definir el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO).	2
Definir los procedimientos para llevar a cabo cada estrategia.	2
Definir los roles y responsabilidades mediante una matriz RACI.	2
Documentar el plan de recuperación ante desastres.	2
Definir las pruebas y el mantenimiento que se le dará a ambos planes.	3
Informar sobre los planes a cada uno de los miembros involucrados.	3
Seleccionar al personal con el perfil adecuado.	4
Definir y asignar las responsabilidades de cada miembro del equipo.	4
Entrenar y motivar al equipo.	4
Evaluar el cumplimiento de las responsabilidades de cada miembro del equipo.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se revisa anualmente el plan de contingencia de TI.	Numérico sin unidades
Número de veces que se revisa anualmente el plan de recuperación ante desastres.	Numérico sin unidades
Número de procedimientos ejecutados satisfactoriamente.	Numérico (Unidad: Procedimiento)

Número de incidentes de TI resueltos mediante la aplicación del plan de contingencia.	Numérico sin unidades
Número de incidentes de TI que requirieron de la activación del plan de recuperación.	Numérico sin unidades
Número de incidentes de TI que fueron resueltos mediante la participación de personal externo a los equipos de respuesta a incidentes.	Numérico sin unidades
Costo anualizado de resolución de incidentes y desastres de TI por externos.	Numérico (Unidad: Monetaria)

Fuente: Elaboración propia.

En el Anexo F se muestra el acta de validación del resultado esperado R5.

5.5 Resultado esperado R6

A continuación, se presenta el componente estratégico del modelo.

5.5.1 Backups (EST01)

Tabla 24. EST01 - Backups.

Dominio: ESTRATÉGICO **EST01 – Backups**	
Descripción	
Gestionar las copias de información, software y sistemas que servirán de respaldo de acuerdo a la política y estrategia de recuperación ante desastres de la pyme, de manera que se asegure su integridad, disponibilidad y confidencialidad. El responsable de llevar a cabo esto debería ser el jefe de infraestructura en conjunto con el gerente de TI.	
Propósito	
Permitir la recuperación ante la perdida de datos o sistemas.	
Actividades del proceso	
1. Gestionar los proveedores de respaldo y recuperación.	
2. Gestionar los backups.	
3. Gestionar la restauración de los respaldos.	
4. Probar los backups.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO/IEC 27002	Cláusula 8.13
COBIT 2019	DSS04

Actividades de implementación	Actividad de proceso
Identificar y evaluar a los proveedores de respaldo y recuperación.	1
Seleccionar al proveedor de respaldo y recuperación más conveniente para la pyme.	1
Definir el acuerdo de nivel de servicio que ofrecerá el proveedor.	1
Establecer las vías de comunicación que se utilizarán para contactar al proveedor en el momento que se requiera hacer uso de los respaldos.	1
Definir la estrategia de backup.	2
Identificar la información, software y sistemas a los que se le generará un respaldo.	2
Definir a los responsables (internos y externos) de los procesos y del acceso según el tipo de backup para cada activo de TI.	2
Definir la tecnología (software y hardware) que se usará para realizar y guardar los respaldos.	2
Generar los respaldos de cada activo de TI identificado.	2
Almacenar y proveer los respaldos realizados para cada activo de TI identificado.	2
Identificar que datos y aplicaciones se van a restaurar.	3
Verificar que la orden de restauración sea dada por personal autorizado.	3
Ejecutar la restauración de los respaldos.	3
Elaborar el acta de restauración.	3
Planificar las pruebas que se le realizarán a los respaldos para validar su integridad y correcto funcionamiento.	4
Definir a los responsables de ejecutar las pruebas.	4
Ejecutar las pruebas definidas.	4
Documentar el plan de pruebas de los respaldos.	4

Métricas e indicadores	Rango de valores de la métrica
Número de veces en el año que la recuperación mediante el uso de los backups no ha cumplido con el RPO definido.	Numérico sin unidades
Número de veces que se evalúa anualmente la integridad y correcto funcionamiento de los backups.	Numérico sin unidades

Fuente: Elaboración propia.

5.5.2 Gestión de crisis (EST02)

Tabla 25. EST02 - Gestión de crisis.

Dominio: ESTRATÉGICO **EST02 – Gestión de crisis**	
Descripción	
Definir el proceso de gestión de crisis que seguirá la pyme, de manera que, pueda estar preparada antes, durante y después de la ocurrencia de una situación crítica que pueda afectar gravemente su continuidad de negocios. El encargado de llevar a cabo esto debería ser el gerente de TI en conjunto con los subgerentes o jefes del área de TI.	
Propósito	
Desarrollar la capacidad de gestión de crisis de la pyme.	
Actividades del proceso	
1. Definir la estrategia de gestión de crisis.	
2. Hacer frente a la crisis.	
3. Recuperarse de la crisis.	
4. Evaluar y entrenar.	
Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
ISO/DIS 22361	Cláusulas 5, 6, 8 y 9
Actividades de implementación	**Actividad de proceso**
Identificar los escenarios bajo los cuales se puede presentar una crisis.	1
Definir los roles y responsabilidades del equipo de gestión de crisis.	1
Conformar el equipo de gestión de crisis (CMT).	1
Definir de qué manera se informará a los interesados sobre la situación de crisis.	1

Elaborar una plantilla del discurso que se usará para comunicar la situación de crisis.	1
Elaborar el plan de gestión de crisis.	1
Activar al equipo de gestión de crisis.	2
Identificar las condiciones de la situación actual.	2
Liderar la ejecución del plan de gestión de crisis por parte del CMT.	2
Informar sobre la situación actual a los interesados internos y externos.	2
Evaluar los efectos negativos que ha generado la crisis.	3
Ejecutar las actividades de recuperación definidas en el plan de gestión de crisis.	3
Entrenar al equipo de gestión de crisis.	4
Planificar escenarios para probar la estrategia de gestión de crisis.	4
Evaluar la estrategia de gestión de crisis.	4
Métricas e indicadores	**Rango de valores de la métrica**
Número de veces que se revisa anualmente la estrategia de gestión de crisis.	Numérico sin unidades
Número de veces que se capacita anualmente al equipo de gestión de crisis.	Numérico sin unidades

Fuente: Elaboración propia.

En el Anexo G se muestra el acta de validación del resultado esperado R6.

Capítulo 6. Resultado esperado del objetivo específico 3

En el presente capítulo se mostrará la guía de aplicación práctica del modelo como resultado del objetivo específico 3.

6.1 Resultado esperado R7

A continuación, se detalla la guía de aplicación práctica del modelo orientado al personal de TI. Para cada proceso se indicarán las actividades que se deben seguir para poder lograr el propósito.

Guía de aplicación del modelo

1. Componente Organizacional (ORG)

1.1. Contextualización del entorno organizacional (ORG01)

En la Figura 13, se muestran las actividades que se tienen que seguir para poder identificar los factores internos y externos que pueden afectar a la pyme en cuanto a continuidad de negocios se refiere.

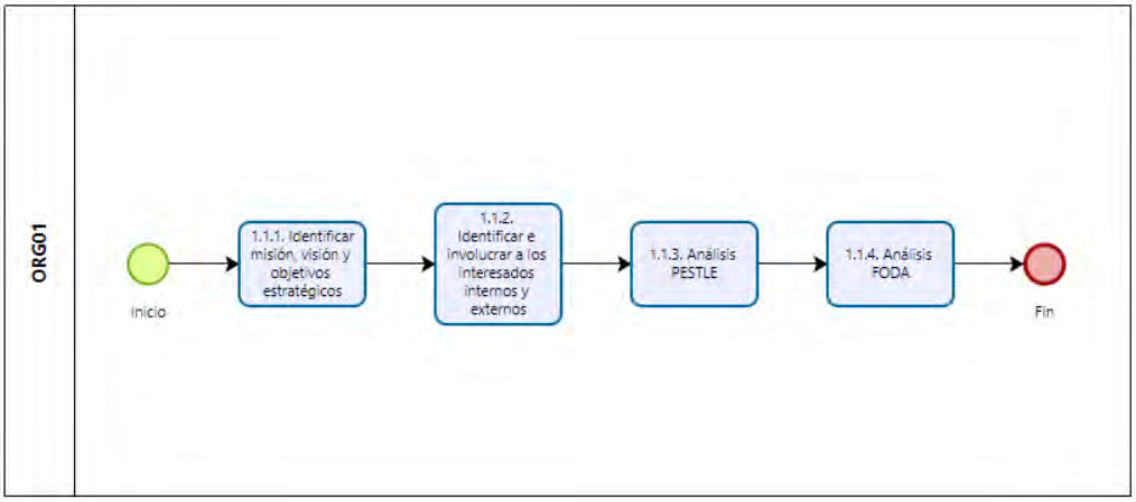


Figura 13. Flujo del proceso ORG01. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 13.

1.1.1. Identificar misión, visión y objetivos estratégicos

- Identificar la misión, visión y objetivos estratégicos de la pyme, los cuales ya debieron ser definidos como parte del planeamiento estratégico de la empresa.
- Elaborar y ejecutar modelos de simulación empresarial.

1.1.2. Identificar e involucrar a los interesados tanto internos como externos

- Identificar a las partes interesadas internas y externas.
- Fortalecer las relaciones con las partes interesadas.
- Involucrar activamente a las partes interesadas.

1.1.3. Análisis PESTLE

- Definir un equipo de trabajo multidisciplinar.
- Identificar el marco regulatorio al que está expuesta la pyme.
- Elaborar una plantilla para el análisis PESTLE.
- Establecer la frecuencia con la que se actualizará el análisis PESTLE.

Tener en cuenta que para el desarrollo del análisis PESTLE se tiene que identificar los siguientes 6 factores externos:

✓ Político

Indican de qué manera las acciones y medidas tomadas por el gobierno pueden influir sobre la pyme.

✓ Económico

Son aspectos que afectan al mercado en el que se desarrolla la pyme.

✓ Social

Son aspectos como cultura, religión, etc. que influyen sobre las personas que integran el mercado en el que se desarrolla la pyme.

✓ Tecnológico

Son aspectos relacionados a la evolución de la tecnología y el impacto que tienen sobre la pyme.

✓ Legal:

Son aspectos relacionados a las normas y regulación vigente que tiene que cumplir la pyme.

✓ Ambiental:

Son aspectos relacionados con la conservación del medio ambiente.

1.1.4. Análisis FODA.

En la Tabla 26 se muestra el enfoque con el que se debe desarrollar la matriz FODA.

Tabla 26. Matriz FODA.

Fortalezas	Debilidades
Identificar las **fortalezas** de la pyme para luego proponer controles y estrategias que puedan hacer frente a las amenazas.	Identificar las **debilidades** de la pyme mediante un análisis de impacto del negocio (BIA).
Oportunidades	**Amenazas**
Planificar simulacros para probar las estrategias de continuidad de negocios, de manera que se tenga la **oportunidad** de poder mejorarlas.	Identificar las **amenazas** que podrían provocar un incidente grave que afecte la continuidad de negocios de la pyme.

Fuente: Elaboración propia.

1.2. Gestión de recursos (ORG02)

En la Figura 14, se muestran las actividades que se tienen que seguir para poder gestionar los recursos necesarios para las funciones de continuidad de negocios y contingencia de TI.

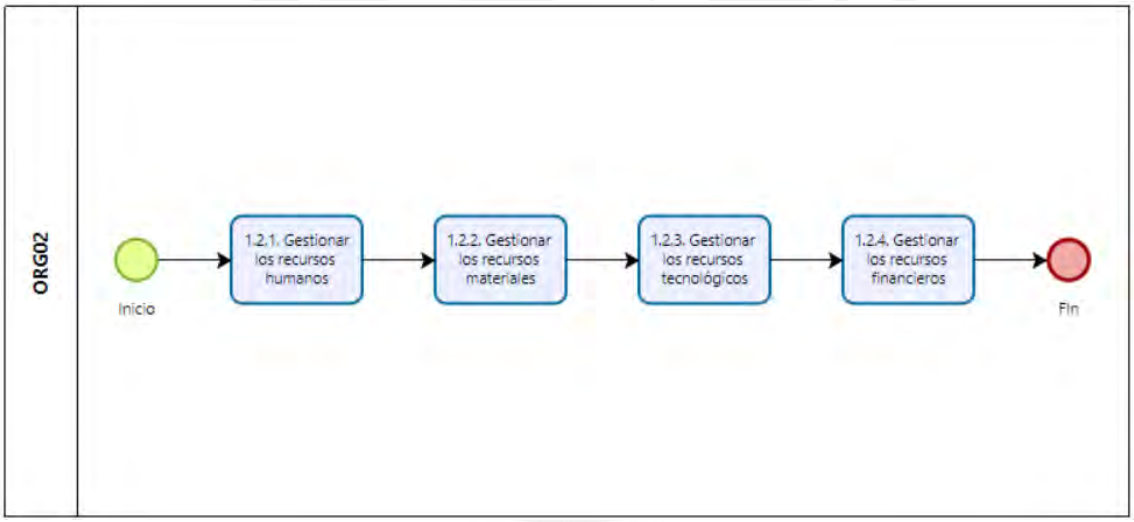


Figura 14. Flujo del proceso ORG02. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 14.

1.2.1. Gestionar los recursos humanos

- Determinar las competencias necesarias con las que debe contar el personal que participará en las funciones de contingencia de TI.
- Evaluar las aptitudes y actitudes del personal que formará parte de las funciones de contingencia de TI.

1.2.2. Gestionar los recursos materiales

- Realizar un inventario de los recursos materiales con los que se cuenta para las funciones de contingencia de TI.
- Establecer la frecuencia con la que se actualizará el inventario.

1.2.3. Gestionar los recursos tecnológicos

- Realizar un inventario de los recursos tecnológicos con los que se cuenta para las funciones de contingencia de TI.
- Evaluar si los servicios tecnológicos brindados por terceros cumplen con la política de continuidad de negocios de la pyme.

1.2.4. Gestionar los recursos financieros

- Elaborar un reporte con el presupuesto que cuenta la pyme para el desarrollo de su continuidad de negocios.

1.3. Estrategia de continuidad de negocios (ORG03)

En la Figura 15, se muestran las actividades que se tienen que seguir para poder definir, gestionar y monitorear la estrategia de continuidad de negocios que seguirá la pyme.

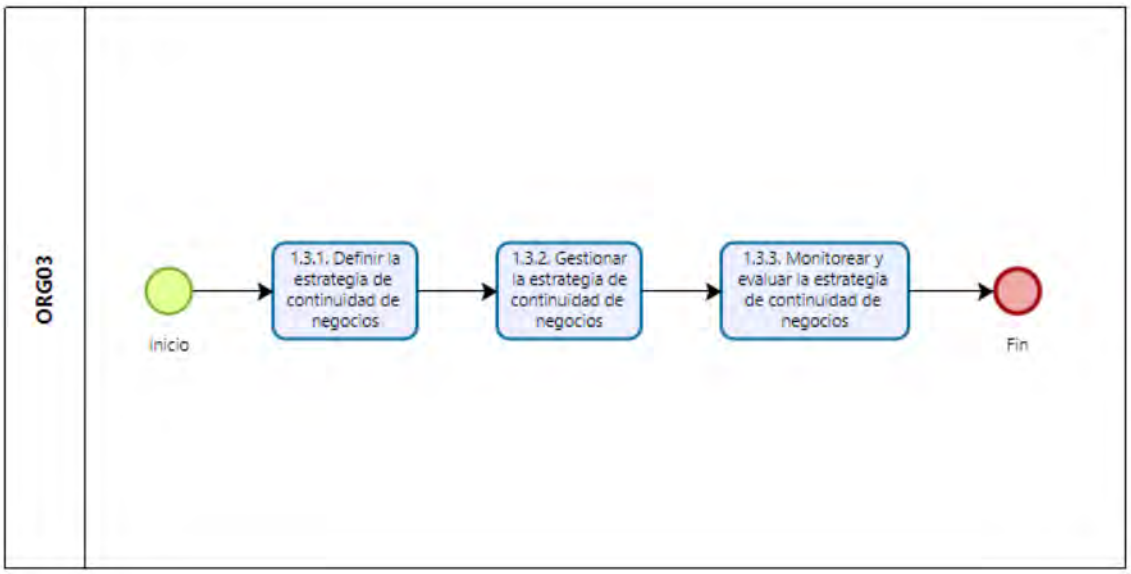


Figura 15. Flujo del proceso ORG03. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 15.

1.3.1. Definir la estrategia de continuidad de negocios

- Evaluar la situación actual de la pyme con respecto a la continuidad de negocios y contingencia de TI.
- Definir el objetivo y el alcance de la estrategia de continuidad de negocios en base a la evaluación realizada previamente.
- Establecer la fecha límite en la que se deberá cumplir con el objetivo de la estrategia de continuidad de negocios.

1.3.2. Gestionar la estrategia de continuidad de negocios

- Asignar al encargado de la gestión de la estrategia de continuidad de negocios.
- Establecer la frecuencia con la que se actualizará la estrategia de continuidad de negocios.
- Comunicar a los involucrados la estrategia de continuidad de negocios que seguirá la pyme.

1.3.3. Monitorear y evaluar la estrategia de continuidad de negocios

- Definir los indicadores con los cuales se medirá la efectividad de la estrategia de continuidad de negocios.
- Evaluar el cumplimiento de la estrategia de continuidad de negocios.

1.4. Políticas (ORG04)

En la Figura 16, se muestran las actividades que se tienen que seguir para establecer, implementar, mejorar de manera continua y documentar la política de continuidad de negocios y todas aquellas políticas que seguirá la pyme para el desarrollo de su resiliencia organizacional.

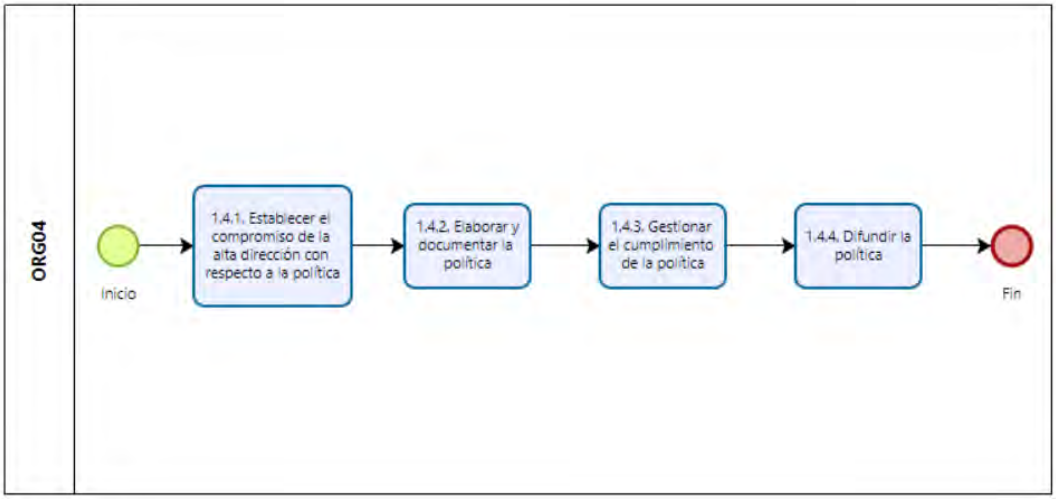


Figura 16. Flujo del proceso ORG04. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 16.

1.4.1. Establecer el compromiso de la alta dirección con respecto a la política

- Mostrar de qué manera la política beneficiará a la pyme.
- Elaborar un acta de compromiso.

1.4.2. Elaborar y documentar la política

- Identificar los objetivos de continuidad de negocios de la pyme.
- Definir el alcance de la política.
- Definir la fecha desde la cual la política será vigente.
- Documentar y publicar la política.

1.4.3. Gestionar el cumplimiento de la política

- Asignar al encargado de la gestión de la política.
- Establecer la frecuencia con la que se revisará la política.
- Evaluar que lo establecido en la política aún esté acorde con los objetivos de la pyme.

1.4.4. Difundir la política

- Compartir la política con todos los trabajadores de la pyme.
- Adecuar la cultura organizacional de tal manera que se incluya lo establecido en la política.

- Organizar talleres de concientización de la política.

Como parte de las políticas a desarrollar, se tiene que considerar a la política de seguridad de la información, la cual puede tener la siguiente estructura:

- ✓ Objetivo
- ✓ Alcance
- ✓ Vigencia
- ✓ Base legal
- ✓ Roles y responsabilidades
- ✓ Políticas
- ✓ Sanciones por incumplimiento

1.5. Roles y responsabilidades (ORG05)

En la Figura 17, se muestran las actividades que se tienen que seguir para definir, monitorear y supervisar los roles y responsabilidades asignados al personal, de tal manera que estén acorde a las políticas y procedimientos de continuidad de negocios de la pyme.

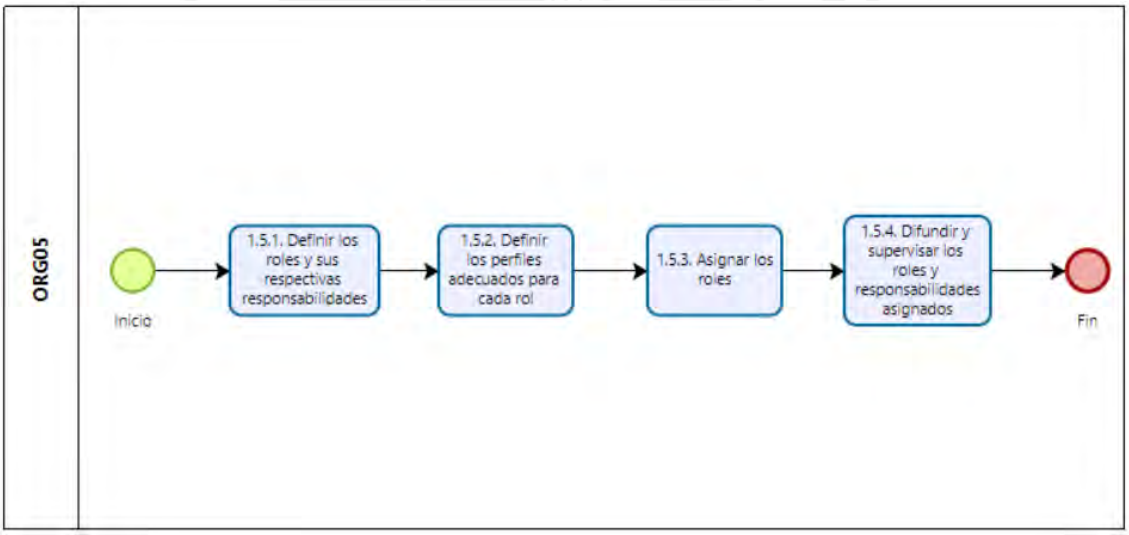


Figura 17. Flujo del proceso ORG05. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 17.

1.5.1. Definir los roles y sus respectivas responsabilidades

- Definir los roles y responsabilidades necesarios para cada proceso de tal manera que se cumpla con las políticas de la pyme.

- Elaborar un documento en el que se especifiquen los roles con sus responsabilidades.
- Establecer la frecuencia con la que se revisará el documento definido en el punto anterior.

1.5.2. Definir los perfiles adecuados para cada rol

- Definir las aptitudes y actitudes necesarias para cada rol.

1.5.3. Asignar los roles

- Identificar el perfil y actitudes necesarias para cada rol.
- Identificar el perfil de cada trabajador que participará en los procesos de continuidad de negocios.
- Elaborar la matriz RACI de manera que se utilice a todo el personal involucrado y se minimice la dependencia en individuos clave.

1.5.4. Difundir y supervisar los roles y responsabilidades asignados

- Comunicar a todo el personal involucrado sobre sus roles.
- Capacitar al personal de acuerdo a su rol asignado.
- Elaborar un documento para cada rol en el que se especifiquen sus objetivos y responsabilidades.
- Definir las métricas con las que se evaluará el cumplimiento de los objetivos de cada rol.
- Establecer la frecuencia con la que se medirá el logro de los objetivos de cada rol.
- Realizar informes de las evaluaciones y mostrarlos a la alta dirección.

1.6. Sistema de Gestión de Continuidad de Negocios (ORG06)

En la Figura 18, se muestran las actividades que se tienen que seguir para definir, implementar y mejorar de manera continua el sistema de gestión de continuidad de negocios (BCMS) de la pyme, de manera que incluya todos los procesos necesarios para el manejo de la contingencia de TI.

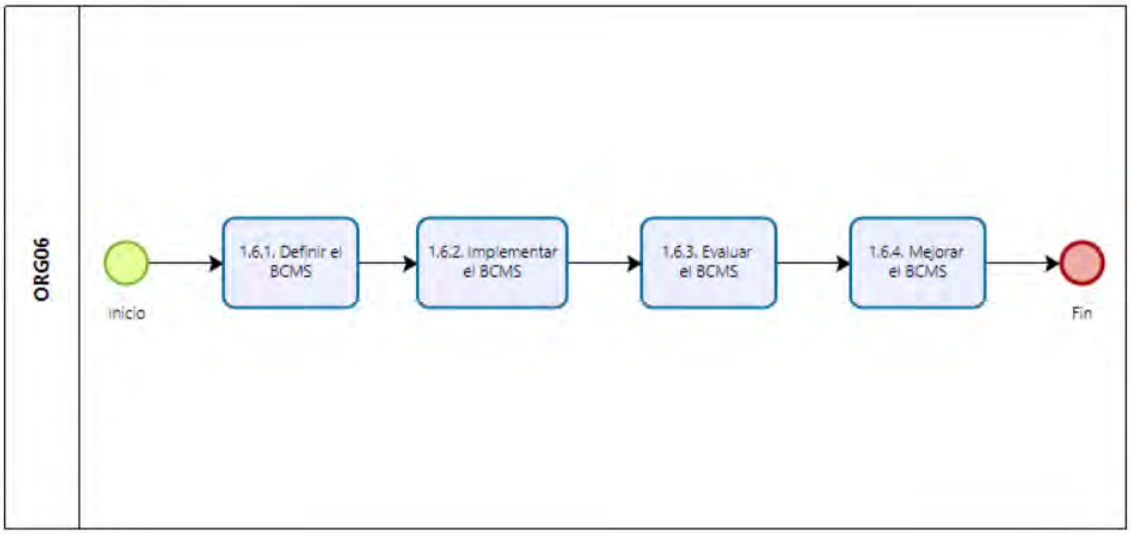


Figura 18. Flujo del proceso ORG06. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 18.

1.6.1. Definir el BCMS

- Identificar los requerimientos legales y regulatorios a los que está sujeta la pyme.
- Definir el alcance que tendrá el BCMS.
- Definir políticas de contingencia de TI y continuidad de negocios.
- Identificar los riesgos que pueden afectar la continuidad de negocios de la pyme.

1.6.2. Implementar el BCMS

- Realizar el análisis de impacto del negocio (BIA).
- Evaluar los riesgos identificados anteriormente.
- Definir las estrategias y soluciones de continuidad de negocios.
- Elaborar los planes de continuidad de negocios y contingencia de TI.
- Capacitar al personal sobre la gestión de continuidad de negocios.

1.6.3. Evaluar el BCMS

- Definir qué aspectos del BCMS se medirán y cómo se medirán.
- Definir y ejecutar escenarios de prueba para medir la efectividad de las estrategias planteadas.
- Elaborar un plan de auditoría.

1.6.4. Mejorar el BCMS

- Identificar los puntos débiles del BCMS en base a las pruebas ejecutadas anteriormente.
- Desarrollar mejoras que cubran los puntos débiles identificados.
- Evaluar el contexto organizacional para adecuar el BCMS en caso sea necesario.

2. Componente de Gestión de riesgos (GDR)

2.1. Identificación de riesgos (GDR01)

En la Figura 19, se muestran las actividades que se tienen que seguir para identificar, analizar y evaluar aquellos riesgos de TI a los que está expuesta la pyme y que pueden tener un impacto negativo sobre su continuidad de negocios, en caso lleguen a ocurrir.

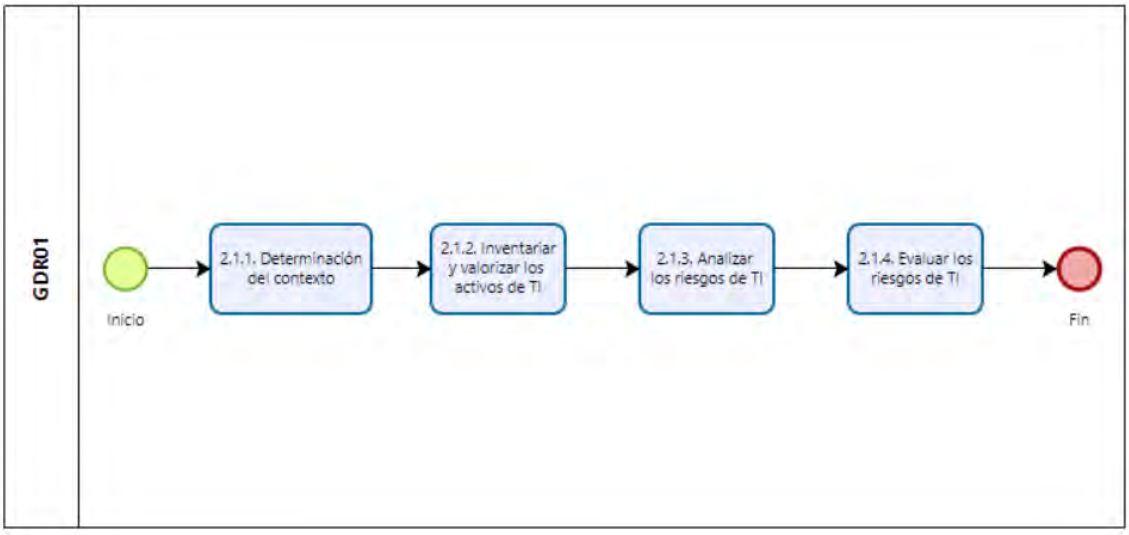


Figura 19. Flujo del proceso GDR01. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 19.

2.1.1. Determinación del contexto

- Contextualizar el entorno tanto interno como externo en el que se desarrolla la pyme.

2.1.2. Inventariar y valorizar los activos de TI

- Identificar los activos de TI que serán considerados dentro de la gestión de riesgos.
- Valorizar los activos de TI identificados considerando lo siguiente:
  - ❖ Factores cuantitativos.
  - ❖ Factores cualitativos.
- Priorizar los activos de TI identificados en base a dos criterios:

- ❖ Criticidad de su participación en los procesos de la pyme.
- ❖ Nivel de exposición del activo.

- Documentar el inventario de los activos de TI y su valorización.

2.1.3. Analizar los riesgos de TI

- Identificar las vulnerabilidades de cada activo de TI.
- Identificar las amenazas que pueden afectar a los activos de TI.
- Identificar los riesgos asociados a cada activo de TI.
- Identificar los escenarios bajo los cuales podrían presentarse los riesgos de TI.

Se recomienda elaborar un cuadro con las siguientes columnas:

- ✓ Activo.
- ✓ Vulnerabilidad.
- ✓ Amenaza.
- ✓ Riesgos.
- ✓ Escenarios.

2.1.4. Evaluar los riesgos de TI

- Determinar el **impacto** que generaría sobre la pyme la ocurrencia de los riesgos de TI.
  Se recomienda usar una escala de 3 o 5 niveles para medir el impacto, definiendo para cada nivel lo siguiente:
  - ❖ Impacto.
  - ❖ Descripción.
  - ❖ Valor numérico.
- Calcular la **probabilidad de ocurrencia** de cada riesgo de TI.
  Se recomienda usar la misma cantidad de niveles que se usaron para medir el impacto, definiendo para cada nivel lo siguiente:
  - ❖ Probabilidad.
  - ❖ Descripción.
  - ❖ Valor numérico.
- Valorizar los riesgos de TI en base a su probabilidad de ocurrencia e impacto.
  Calcular el riesgo en base a la siguiente fórmula:

  Riesgo = Impacto * Probabilidad

  Agrupar los riesgos según su valoración en:

- ❖ Alto: aquellos riesgos cuyo valor está en el rango [c;d]
- ❖ Medio: aquellos riesgos cuyo valor está en el rango [b;c[
- ❖ Bajo: aquellos riesgos cuyo valor está en el rango [a;b[

- Documentar el análisis y evaluación de los riesgos de TI.

2.2. Tratamiento de riesgos (GDR02)

En la Figura 20, se muestran las actividades que se tienen que seguir para elegir el tratamiento más adecuado para cada riesgo de TI que puede afectar negativamente la continuidad de negocios de la pyme, así como el diseño e implementación de controles para hacerles frente.

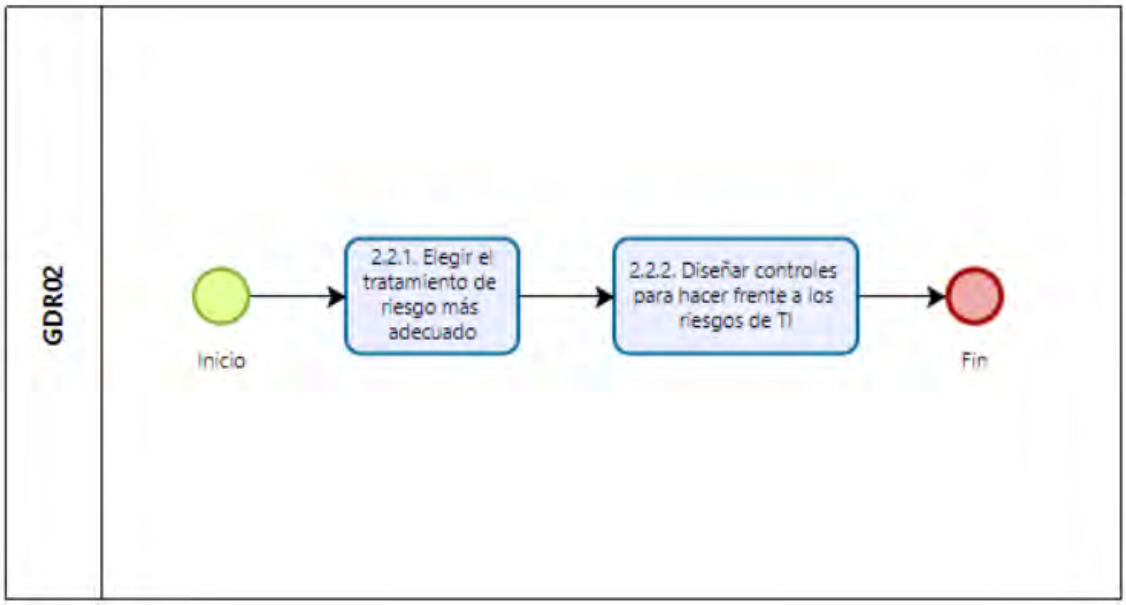


Figura 20. Flujo del proceso GDR02. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 20.

2.2.1 Elegir el tratamiento de riesgo más adecuado

- Consultar con el responsable del activo de TI si el(los) riesgo(s) asociado deben ser eliminado, transferido, mitigado o tolerado.
- Evaluar el costo beneficio de cada tipo de tratamiento para todos los riesgos.
- Definir el tipo de tratamiento que se le dará al riesgo.

2.2.2. Definir controles para hacer frente a los riesgos de TI

- Definir de qué trata el control.

- Definir cuál es el propósito del control, clasificándolo como preventivo, detectivo o correctivo.
- Definir cómo el control debe ser implementado.
- Definir quién es el responsable del control.
- Implementar los controles definidos.
- Establece las métricas con las que se evaluarán los controles.
- Documentar todos los controles diseñados,
- Establecer la frecuencia con la que se revisarán los controles.

Para la elaboración de cada control se puede hacer uso del formato mostrado en la Tabla 27.

Tabla 27. Formato para la elaboración del control.

Código del control	*Nombre del control*
***Descripción**: de qué trata el control.*	
***Propósito**: qué se busca lograr con el control.*	
***Tipo de control**: preventivo, detectivo o correctivo.*	
***Responsable**: nombre, cargo, área a la que pertenece, etc.*	
***Implementación**: pasos para implementar el control.*	
***Métricas e indicadores**: cómo se medirá el desempeño del control.*	

Fuente: Elaboración propia.

2.3. Respuesta a incidentes de TI (GDR03)

En la Figura 21, se muestran las actividades que se tienen que seguir para definir y elaborar los planes de contingencia de TI y recuperación ante desastres, de manera que, se garantice la continuidad de negocios de la pyme por lo menos a un nivel mínimo aceptable.

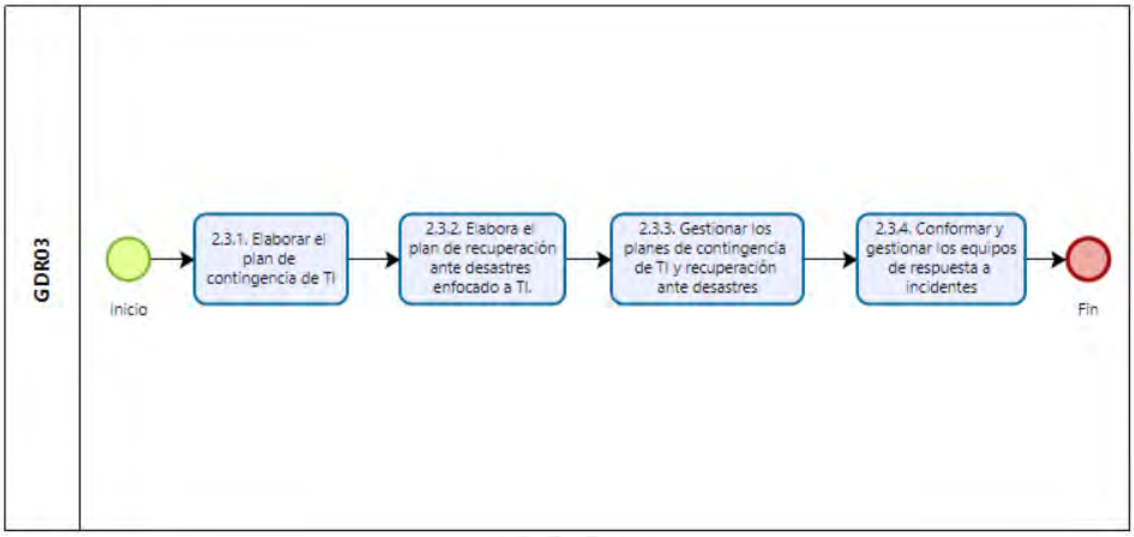


Figura 21. Flujo del proceso GDR03. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 21.

2.3.1. Elaborar el plan de contingencia de TI

- Definir el objetivo del plan de contingencia.
- Listar las tareas relacionadas con el uso y aplicación de los controles detectivos y correctivos diseñados en la gestión de riesgos.
- Definir los roles y responsabilidades mediante una matriz RACI.
- Establecer una estrategia de contingencia de TI.
- Definir las estrategias de contingencia.
- Definir los procedimientos para llevar a cabo cada estrategia.
- Documentar y difundir el plan de contingencia de TI.

2.3.2. Elaborar el plan de recuperación ante desastres enfocado a TI

- Definir el alcance del plan de recuperación ante desastres.
- Definir las estrategias de recuperación para cada escenario.
- Definir el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO).
- Definir los procedimientos para llevar a cabo cada estrategia.
- Definir los roles y responsabilidades mediante una matriz RACI.
- Documentar el plan de recuperación ante desastres.

2.3.3. Gestionar los planes de contingencia de TI y recuperación ante desastres

- Definir las pruebas y el mantenimiento que se le dará a ambos planes.
- Informar sobre los planes a cada uno de los miembros involucrados.

2.3.4. Conformar y gestionar los equipos de respuesta a incidentes

- Seleccionar al personal con el perfil adecuado.
- Definir y asignar las responsabilidades de cada miembro del equipo.
- Entrenar y motivar al equipo.
- Evaluar el cumplimiento de las responsabilidades de cada miembro del equipo.

3. Componente Estratégico (EST)

3.1. Backup (EST01)

En la Figura 22, se muestran las actividades que se tienen que seguir para gestionar las copias de información, software y sistemas que servirán de respaldo, de acuerdo a la política y estrategia de recuperación ante desastres de la pyme, de manera que se asegure su integridad, disponibilidad y confidencialidad.

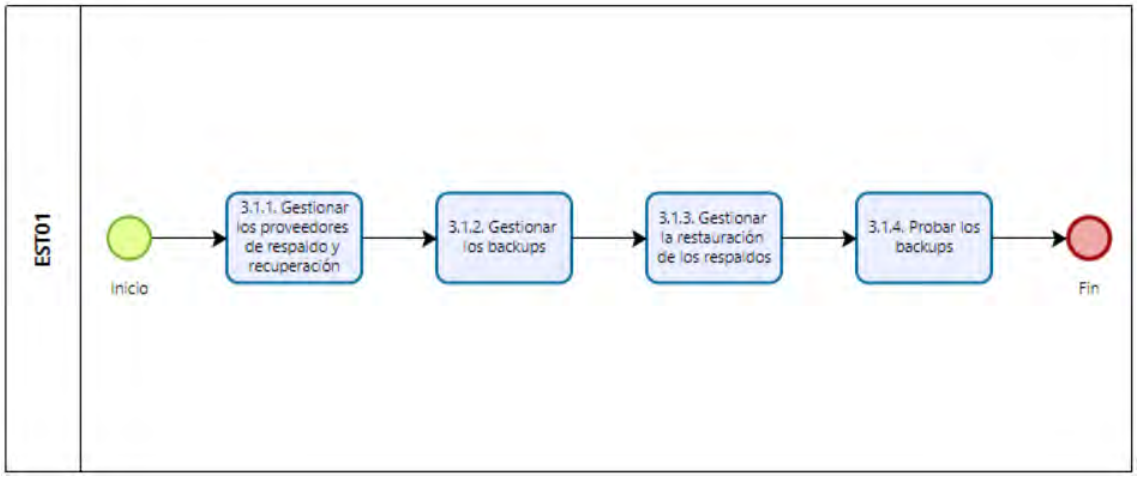


Figura 22. Flujo del proceso EST01. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 22.

3.1.1. Gestionar los proveedores de respaldo y recuperación

- Identificar y evaluar los proveedores de respaldo y recuperación.
- Seleccionar al proveedor de respaldo y recuperación más conveniente para la pyme.
- Definir el acuerdo de nivel de servicio que ofrecerá el proveedor.

- Establecer las vías de comunicación que se utilizarán para contactar al proveedor en el momento que se requiera hacer uso de los respaldos.

3.1.2. Gestionar los backups

- Definir la estrategia de backup.
- Identificar la información, software y sistemas a los que se le generará un respaldo.
- Definir a los responsables (internos y externos) de los procesos y del acceso según el tipo de backup para cada activo de TI.
- Definir la tecnología (software y hardware) que se usará para realizar y guardar los respaldos.
- Generar los respaldos de cada activo de TI identificado.
- Almacenar y proveer los respaldos realizados para cada activo de TI identificado.

3.1.3. Gestionar la restauración de los respaldos

- Identificar que datos y aplicaciones se van a restaurar.
- Verificar que la orden de restauración sea dada por personal autorizado.
- Ejecutar la restauración de los respaldos.
- Elaborar el acta de restauración.

3.1.4. Probar los backups

- Planificar las pruebas que se le realizarán a los respaldos para validar su integridad y correcto funcionamiento.
- Definir a los responsables de ejecutar las pruebas.
- Ejecutar las pruebas definidas.
- Documentar el plan de pruebas de los respaldos.

3.2. Gestión de crisis (EST02)

En la Figura 23, se muestran las actividades que se tienen que seguir para definir el proceso de gestión de crisis que seguirá la pyme, de manera que, pueda estar preparada antes, durante y después de la ocurrencia de una situación crítica que pueda afectar gravemente su continuidad de negocios.

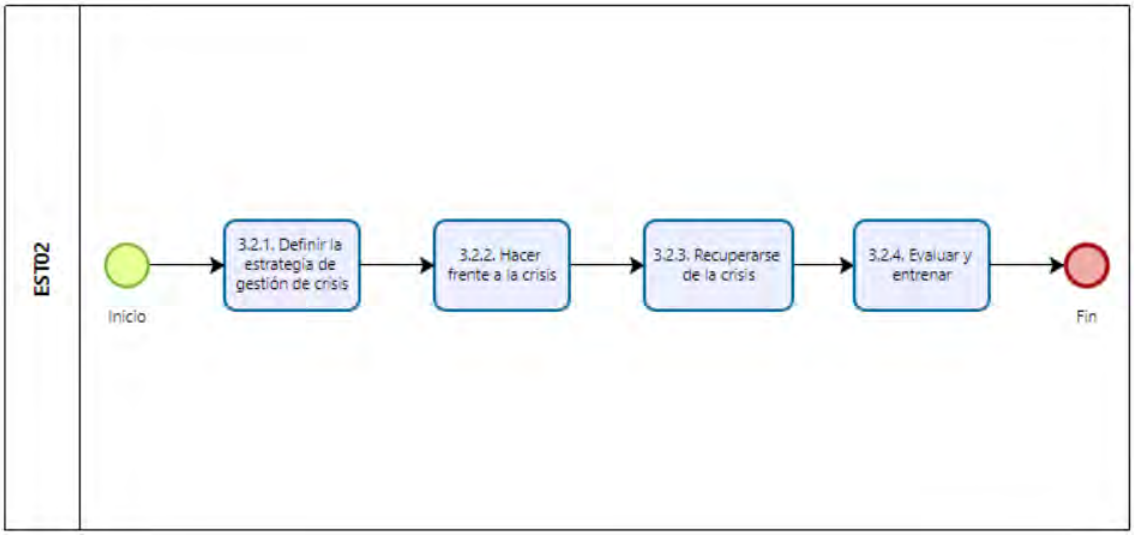


Figura 23. Flujo del proceso EST02. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 23.

3.2.1. Definir la estrategia de gestión de crisis

- Identificar los escenarios bajo los cuales se puede presentar una crisis.
- Definir los roles y responsabilidades del equipo de gestión de crisis.
- Conformar el equipo de gestión de crisis (CMT).
- Definir de qué manera se informará a los interesados sobre la situación de crisis.
- Elaborar una plantilla del discurso que se usará para comunicar la situación de crisis.
- Elaborar el plan de gestión de crisis.

3.2.2. Hacer frente a la crisis

- Activar al equipo de gestión de crisis.
- Identificar las condiciones de la situación actual.
- Liderar la ejecución del plan de gestión de crisis por parte del CMT.
- Informar sobre la situación actual a los interesados internos y externos.

3.2.3. Recuperarse de la crisis

- Evaluar los efectos negativos que ha generado la crisis.
- Ejecutar las actividades de recuperación definidas en el plan de gestión de crisis.

3.2.4. Evaluar y entrenar

- Entrenar al equipo de gestión de crisis.

- Planificar escenarios para probar la estrategia de gestión de crisis.
- Evaluar la estrategia de gestión de crisis.

4. Componente de Innovación (INO)

4.1. Ejercicios y pruebas (INO01)

En la Figura 24, se muestran las actividades que se tienen que seguir para planificar, ejecutar y mejorar las pruebas mediante las cuales se entrenará al personal involucrado en las funciones de continuidad de negocios y contingencia de TI de la pyme.

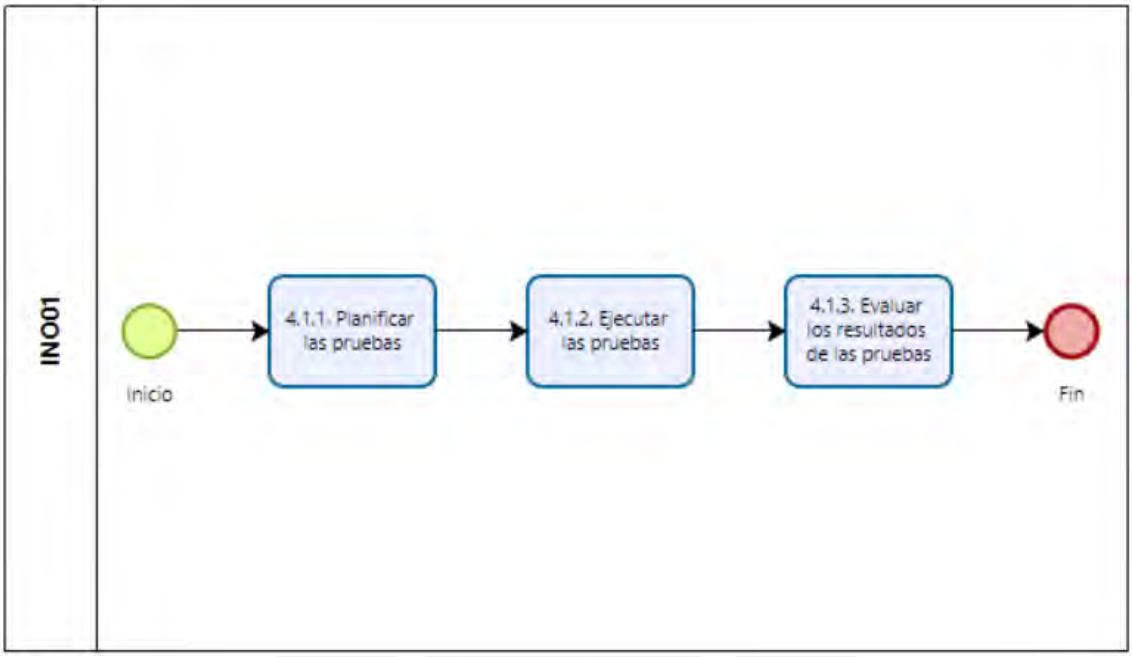


Figura 24. Flujo del proceso INO01. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 24.

4.1.1. Planificar las pruebas

- Definir el alcance del plan de pruebas.
- Definir las pruebas indicando descripción, objetivos, alcance, roles y responsabilidades de los involucrados y criterios de éxito.
- Elaborar el calendario de ejecución de las pruebas.
- Definir los resultados esperados de las pruebas.
- Documentar todas las pruebas dentro del plan de pruebas.
- Comunicar el plan de pruebas a la alta dirección y los involucrados.

Para la elaboración de cada prueba se puede hacer uso del formato mostrado en la Tabla 28.

Tabla 28. Formato para la elaboración de una prueba.

Código de la prueba	*Nombre de la prueba*
***Descripción**: de qué trata la prueba.*	
***Alcance:** qué se está cubriendo con la prueba.*	
***Objetivos**: qué se busca verificar mediante la ejecución de la prueba.*	
***Responsable**: nombre, cargo, área a la que pertenece, etc.*	
***Implementación**: pasos para la ejecución de la prueba.*	
***Criterios de éxito**: cómo se evaluarán los resultados de la prueba.*	

Fuente: Elaboración propia

4.1.2. Ejecutar la prueba

- Ejecutar las pruebas de acuerdo al calendario establecido.
- Documentar los resultados de la ejecución de las pruebas.

4.1.3. Evaluar los resultados de las pruebas

- Analizar los resultados de las pruebas.
- Calificar los resultados de las pruebas.
- Identificar aspectos de mejora de las pruebas, así como de los recursos humanos y tecnológicos.
- Documentar el proceso de mejora como resultado de la ejecución de las pruebas.

4.2. Entrenamiento y concientización (INO02)

En la Figura 25, se muestran las actividades que se tienen que seguir para definir e implementar las estrategias mediante las cuales se capacita y concientiza a todos los trabajadores de la pyme con respecto a continuidad de negocios y contingencia de TI, de acuerdo a su cargo y sus funciones.

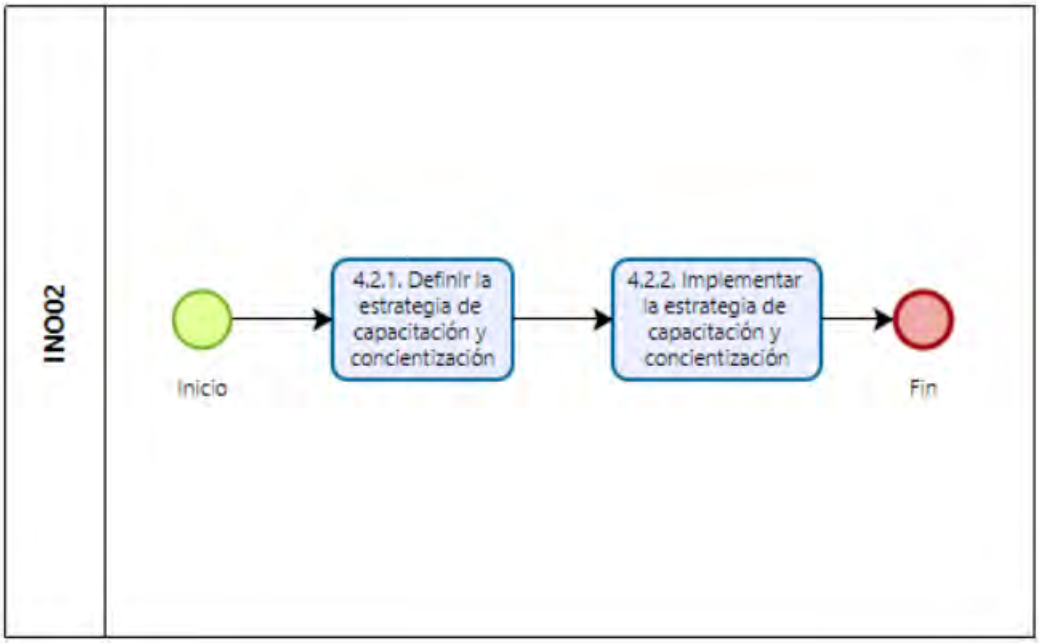


Figura 25. Flujo del proceso INO02. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 25.

4.2.1. Definir la estrategia de capacitación y concientización

- Definir la estrategia de capacitación y concientización sobre continuidad de negocios y contingencia de TI.
- Agrupar a los trabajadores de acuerdo al nivel de capacitación y concientización que requiera en base a sus roles y responsabilidades.
- Elaborar un calendario para las capacitaciones y concientizaciones de todos los grupos.
- Definir los criterios de éxito de la capacitación y concientización de cada grupo.

4.2.2. Implementar la estrategia de capacitación y concientización

- Brindar las capacitaciones y concientizaciones respetando el alcance y las fechas definidas para cada grupo.
- Evaluar el resultado de las capacitaciones y concientizaciones según los criterios de éxito definidos en la estrategia.
- Solicitar feedback sobre los procesos de capacitación y concientización.
- Identificar e implementar aspectos de mejora para las capacitaciones y concientizaciones.

4.3. Auditoría (INO03)

En la Figura 26, se muestran las actividades que se tienen que seguir para definir y ejecutar un plan de auditoría, de manera que la pyme cuente con un procedimiento definido para la evaluación de sus estrategias de continuidad de negocios, los planes de contingencia de TI y los recursos involucrados en ambos.

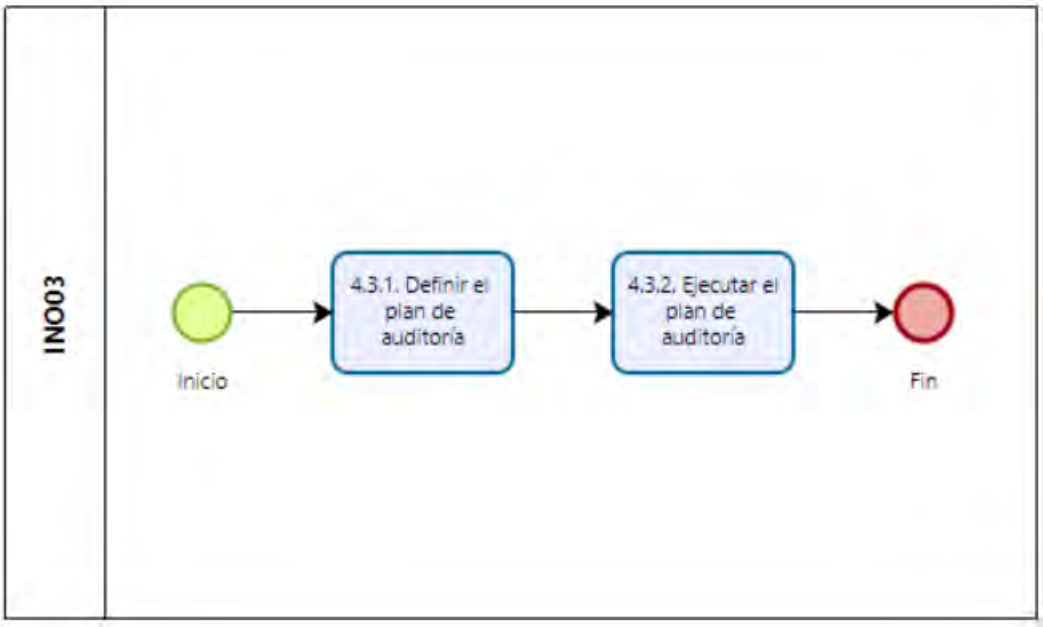


Figura 26. Flujo del proceso INO03. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 26.

4.3.1. Definir el plan de auditoría

- Establecer los objetivos del plan de auditoría.
- Identificar los elementos (p. ej. planes, controles, recursos, etc.) concernientes a continuidad de negocios y contingencia de TI que serán evaluados, así como, sus responsables.
- Definir los métodos y criterios de evaluación que serán usados durante la auditoría.
- Documentar el plan de auditoría sobre cada elemento en evaluación.

4.3.2. Ejecutar el plan de auditoría

- Recolectar y verificar información sobre cada elemento en evaluación.
- Evaluar la información recolectada.
- Elaborar un reporte con las conclusiones de la auditoría.

- Identificar oportunidades de mejora en base a los resultados de la auditoría.

4.4. Monitoreo (INO04)

En la Figura 27, se muestran las actividades que se tienen que seguir para definir e implementar un procedimiento mediante el cual se monitoreé y mida el desempeño de las estrategias de continuidad de negocios y contingencia de TI implementadas en la pyme.

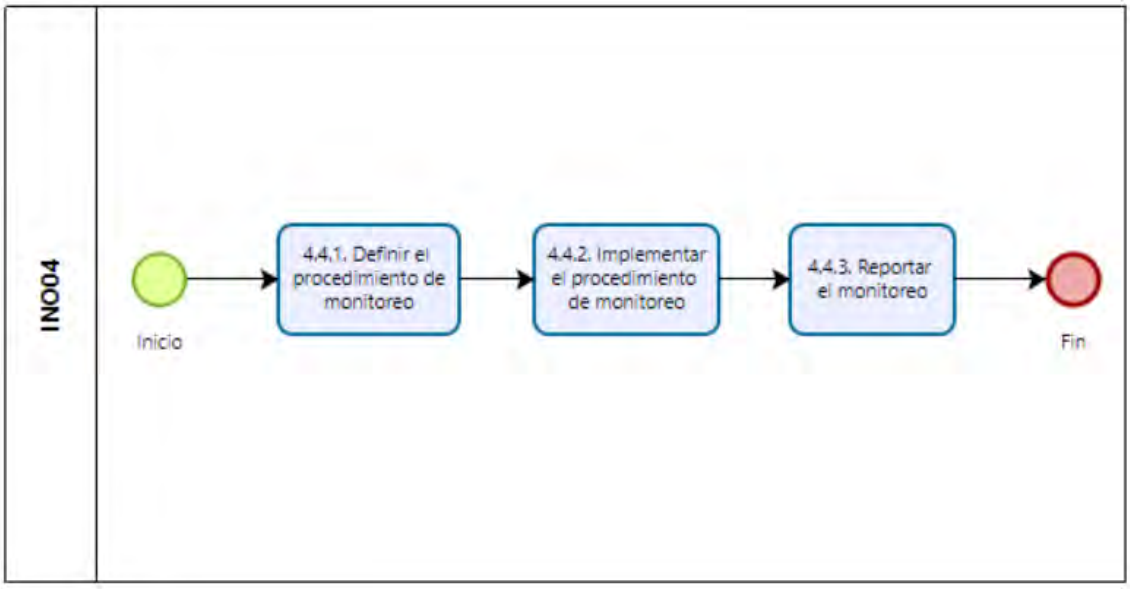


Figura 27. Flujo del proceso INO04. Fuente: Elaboración propia.

A continuación, se indica de qué manera deben llevarse a cabo las actividades mostradas en la Figura 27.

4.4.1. Definir el procedimiento de monitoreo

- Identificar los elementos (p. ej. planes, controles, recursos, etc.) concernientes a continuidad de negocios y contingencia de TI que serán monitoreados.
- Definir las métricas e indicadores mediante los cuales se medirá el desempeño de cada elemento identificado.
- Definir el nivel mínimo de desempeño aceptable para cada elemento identificado.
- Definir el método mediante el cual se monitoreará cada elemento identificado.
- Definir la frecuencia con la que se monitoreará cada elemento identificado.
- Asignar a los responsables del monitoreo de cada elemento identificado.
- Documentar los resultados del procedimiento de monitoreo.

4.4.2. Implementar el procedimiento de monitoreo

- Ejecutar el procedimiento de monitoreo.

4.4.3. Reportar el monitoreo

- Analizar y evaluar la información recolectada del procedimiento del monitoreo.
- Elaborar un informe con el análisis realizado y los puntos de mejora identificados.

Finalmente, en la Tabla 29 se muestra la matriz RACI para la aplicación del modelo. Los 12 roles propuestos han sido tomados en base a la estructura organizacional que propone COBIT 2019 Framework: Governance and Management Objectives (ISACA, 2018b).

Cabe resaltar que los roles y responsabilidades son referenciales y pueden ser adaptados a la estructura de la pyme; p. ej. si la pyme solo cuenta con un responsable de TI, entonces esa persona asumiría el papel de gerente de TI y jefe de TI.

Tabla 29. Matriz RACI.

	Gerente general	Gerente de finanzas	Gerente de operaciones	Gerente de riesgos	Gerente de TI	Gerente (Oficial) de seguridad de la información	Jefe de finanzas	Jefe de operaciones	Jefe de TI	Jefe de proyectos	Jefe de recursos humanos	Auditor
ORG01	A	R	R	R	R	C	C	C	C	C	C	C
ORG02	A	R	I	I	R	I	C	I	C		R	C
ORG03	A	I	R	R	R	C	I	I	I			C
ORG04	A	I	I	R	R	R	I	I	I	I	I	C
ORG05	A	I	I	R	R	R	C	C	C	I	I	C
ORG06	A	I	I	R	R	R	C	C	C	I	I	C
GDR01	I	I	I	A	R	C	C	C	R	C	C	R
GDR02	I	I	I	A	R	C	C	C	R			R
GDR03	I	I	I	A	R	C	I	C	R			I
EST01	I	I	I	C	A	R	C	C	R	I		
EST02	I	I	I	A	R	C	I	C	R	I	I	C
INO01	I	I	I	C	A	C	C	I	R	I	R	C
INO02	I	I	I	C	A	I	I	I	R	I	R	
INO03	I	I	I	C	R	C	I	I	R	I	I	R
INO04	I	I	I	I	A	C	I	C	R			I

Fuente: Elaboración propia

En el Anexo H se muestra el acta de validación del resultado esperado R7.

Capítulo 7. Conclusiones y trabajo futuro

En este capítulo se presentarán las conclusiones obtenidas para cada uno de los objetivos específicos del proyecto; así como el trabajo futuro que se puede realizar sobre el mismo.

7.1 Conclusiones

Con respecto al objetivo específico 1 se puede concluir que no existen marcos de aplicación exclusiva para pymes con una orientación hacia contingencia de TI y que presenten medidas genéricas que les permitan reaccionar ante un incidente de TI y posteriormente recuperarse.

Debido a las características de este tipo de empresas, no resulta posible la implementación de un sistema de gestión de continuidad de negocios, siguiendo por ejemplo la norma ISO 22301, ya que para eso se necesita:

- Contar con una determinada cantidad de recursos humanos, tecnológicos y económicos.
- Tener un determinado nivel de madurez con respecto a contingencia de TI.

Es por esto que la pyme busca ser reactiva con respecto a su contingencia de TI. Sin embargo, cuando la reactividad ya no es suficiente para hacer frente a los incidentes de TI, la organización debe contar con otras medidas de control y realizar cambios en su estructura (p. ej. responsabilidades, capacidades, etc.), de manera que pueda asegurar la continuidad del negocio. Esas otras medidas adicionales están propuestas en el modelo que se ha elaborado.

Con respecto al objetivo específico 2 se puede concluir que ha sido posible identificar 4 dominios generales basados en Balanced Scorecard que permiten agrupar todos los aspectos que debería considerar una pyme para hacer frente de manera reactiva a los incidentes que afectan la contingencia de TI, basando los dominios y los procesos propuestos en buenas prácticas internacionalmente aceptadas.

Con respecto al objetivo específico 3 se puede concluir que la guía de aplicación es válida teóricamente según la opinión de los expertos, así mismo, cubre todas las actividades necesarias para implementar los procesos que forman parte de los dominios y que contempla las métricas adecuadas para la medición de los mismos.

7.2 Trabajo futuro

Como parte del trabajo futuro a realizarse para este modelo, se tiene planificado lo siguiente:

- Probar el modelo desarrollado por lo menos en una pyme, con la finalidad de identificar oportunidades de mejora sustanciales que se pudieran plantear en el modelo.
- Profundizar en la explicación sobre las métricas que forman parte de los componentes para aquella empresa que vaya a aplicar el modelo, considerando los siguientes aspectos:
    - ❖ Instrumentos de medición.
    - ❖ Mecanismos de medición.
    - ❖ Frecuencia de medición.
    - ❖ Responsables de la medición.
    - ❖ Análisis de los resultados de las métricas.
- Modificar el modelo manteniendo la orientación hacia las pymes, con la finalidad de que se cubran otros aspectos diferentes, por ejemplo, profundizar en gestión de riesgos (incluyendo riesgos operacionales), de manera que se pueda ofrecer una herramienta más completa.

Referencias

ACM. (2020). Paradigms for Global Computing Education. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf

Aronis, S., & Stratopoulos, G. (2016). Implementing business continuity management systems and sharing best practices at a European bank. Journal of business continuity & emergency planning, 9, 203–217. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84979854549&partnerID=40&md5=f0df27318ed2aa23f3473b122dfb97f9

Asociación de Auditoría y Control de Sistemas de Información (ISACA). (2018a). COBIT 2019 Framework: Introduction and Methodology.

Asociación de Auditoría y Control de Sistemas de Información (ISACA). (2018b). COBIT 2019 Framework: Governance and Management Objectives.

Bruzza, M. (2020). Diseño de un modelo para la implementación de gobierno electrónico en instituciones estatales. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/17147

Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO). (2017). Gestión de riesgos empresariales: marco integrado https://www.coso.org/Pages/default.aspx

Cervera, J & Hernández, A. (1999). Las Buenas Prácticas: ¿Propaganda institucional o difusión de ejemplos para la mejora de la realidad? http://habitat.aq.upm.es/boletin/n10/ajcer.html

Escuela Superior de Administración Pública de Colombia (ESAP) (2018a). Plan de continuidad de negocios. https://www.esap.edu.co/portal//wp-content/uploads/2019/03/Plan-de-continuidad-del-negocio-v1.pdf

Escuela Superior de Administración Pública de Colombia (ESAP) (2018b). Plan de recuperación ante desastres. https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Recuperaci%C3%B3n-de-Desastres-v1.pdf

Filipović, D., Krišto, M., & Podrug, N. (2018). Impact of crisis situations on development of business continuity management in Croatia [Djelovanje kriznih situacija na razvoj upravljanja poslovnim kontinuitetom u Hrvatskoj]. Management (Croatia), 23, 99–122. https://doi.org/10.30924/mjcmi/2018.23.1.99

Gómez, G., Morón, A., & Betancourt, R. (2020). Risk management model, the contribution of phi value in the business continuity plan [Modelo de gestión de riesgos: El aporte del valor phi en el plan de continuidad de negocios]. *Revista Venezolana de Gerencia*, *25*, 112–128. https://doi.org/10.37960/rvg.v25i3.33356

Hersyah, M. H., & Derisma. (2018). A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation. 2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings, 392–397. https://doi.org/10.1109/ICITSI.2018.8696075

Instituto de Auditores Internos (IIA). (2013). Las tres líneas de defensa para una efectiva gestión de riesgos y control. https://na.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Spanish.pdf

Information Technology Infraestructure Library (ITIL) (2019). ITIL v4 Foundation.

Instituto Nacional de Estándares y Tecnología (NIST) (2010). Contingency Planning Guide for Federal Informaction Systems. https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

Instituto Nacional de Estándares y Tecnología (NIST) (2021). NIST RIsk Management Framework (RMF). https://csrc.nist.gov/projects/risk-management

Kaplan R. & Norton D. (2005). El Balanced Scorecard: Mediciones que impulsan el desempeño.

Kitchenham, B. (2007). Guidelines for performing systematic literature reviews in software engineering.

Kulkarni, S., Hidding, G. J., & Cicekoglu, S. (2015). A framework for post-crisis business continuity plans. Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, 143–152. https://doi.org/10.1109/HICSS.2015.27

Labus, M., Despotović-Zrakić, M., & Bogdanović, Z. (2017). Introducing adaptive E-business continuity management. Advances in Intelligent Systems and Computing, 569, 628–637. https://doi.org/10.1007/978-3-319-56535-4_62

Lee, W.-Y., Lee, S.-H., Jin, C., & Hyun, C.-T. (2021). Development of the RACI model for processes of the closure phase in construction programs. *Sustainability (Switzerland)*, *1806*, 1–26. https://doi.org/10.3390/su13041806

Lin, C.-S., Kao, S., & Chen, L.-S. (2012). A proactive operational framework for business continuity in the semiconductor industry. Quality and Reliability Engineering International, 28, 307–320. https://doi.org/10.1002/qre.1246

Lindstedt, D. (2017). The capability and constraint model of recoverability: An integrated theory of continuity planning. Journal of business continuity & emergency planning, 11, 52–62. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85037695910&partnerID=40&md5=5a4264f9506e93723021d15d72d3d50c

Margherita, A., & Heikkilä, M. (2021). Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies. Business Horizons, 64, 683–695. https://doi.org/10.1016/j.bushor.2021.02.020

Ministerio del Ambiente (MINAM). (2020). Plan de contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones del Ministerio del Ambiente. https://cdn.www.gob.pe/uploads/document/file/1250398/ANEXO%201%20PCO%20-%20Plan%20de%20Contingencia%20Inform%C3%A1tico%20y%20Recuperaci%C3%B3n%20de%20Servicios%20de%20Tecnolog%C3%ADa%20de%20la%20Informaci%C3%B3n%20y%20Comunicaciones%20del%20Ministerio%20del%20Ambiente.pdf

Notice, C. (2011). Standard glossary of terms used in Requirements Engineering. Requirements Engineering Qualifications Board, 1, 1–24.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2017). Guía para Políticas. http://www.unesco.org/new/es/culture/themes/%20cultural-diversity/diversity-of-cultural%20expressions/tools/policy-guide/planificar/diagnosticar/arbol-de-problemas/

Organización Internacional de Normalización (ISO). (2013). Tecnología de información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información (ISO 27002). https://www.iso.org/standard/54533.html

Organización Internacional de Normalización (ISO). (2017a). Seguridad y resiliencia – Resiliencia organizacional – Principios y atributos (ISO 22316). https://www.iso.org/standard/50053.html

Organización Internacional de Normalización (ISO). (2017b). Sistemas e Ingeniería de Software - Vocabulario (ISO 24765). https://www.iso.org/standard/71952.html

Organización Internacional de Normalización (ISO). (2018a). Sistemas e Ingeniería de Software – Requerimientos para gerentes de información, usuarios de sistemas, software y servicios. (ISO 26511). https://www.iso.org/standard/70879.html

Organización Internacional de Normalización (ISO). (2018b). Gestión de riesgos (ISO 31000). https://www.iso.org/standard/65694.html

Organización Internacional de Normalización (ISO). (2019). Seguridad y resiliencia: Sistemas de gestión de la continuidad del negocio (ISO 22301). https://www.iso.org/standard/75106.html

Organización Internacional de Normalización (ISO). (2020). Seguridad y resiliencia – Sistema de gestión de la continuidad del negocio – Guía para el uso de la ISO 22301. (ISO 22313). https://www.iso.org/standard/75107.html

Organización Internacional de Normalización (ISO). (2021). Seguridad y resiliencia: Vocabulario (ISO 22300). https://www.iso.org/standard/77008.html

Păunescu, C. (2017). How prepared are small and medium sized companies for business continuity management? Quality - Access to Success, 18, 43–48. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034588398&partnerID=40&md5=1f8bf06d6d9d3f2dac93fc85b39c72b2

Păunescu, C., & Argatu, R. (2020). Critical functions in ensuring effective business continuity management. Evidence from romanian companies. Journal of Business Economics and Management, 21. https://doi.org/10.3846/jbem.2020.12205

Russo, N., Reis, L., Silveria, C. & Sao Mamede, H. (2021). Framework for designing Business Continuity – Multidisciplinary Evaluation of Organizational Maturity (pp. 1-4). Recuperado de

https://ieeexplore-ieee-org.ezproxybib.pucp.edu.pe/document/9476297

Sambo, F., & Bankole, F. O. (2016). A normative process model for ICT business continuity plan for disaster management in small, medium and large enterprises. International Journal of Electrical and Computer Engineering, 6, 2425–2431. https://doi.org/10.11591/ijece.v6i5.11461

Setiawan, A., Wibowo, A., & Susilo, A. H. (2018). Risk analysis on the development of a business continuity plan. Proceedings of the 2017 4th International Conference on Computer Applications and Information Processing Technology, CAIPT 2017, 2018-January, 1–4. https://doi.org/10.1109/CAIPT.2017.8320736

Siciliano, G. G., & Gaudenzi, B. (2018). The role of supply chain resilience on IT and cyber disruptions. Lecture Notes in Information Systems and Organisation, 24, 57–69. https://doi.org/10.1007/978-3-319-62636-9_4

Speight, P. (2011). Business continuity. Journal of Applied Security Research, 6, 529–554. https://doi.org/10.1080/19361610.2011.604021

Suresh, N., Sanders, G. L., & Braunscheidel, M. J. (2020). Business Continuity Management for Supply Chains Facing Catastrophic Events. IEEE Engineering Management Review, 48, 129–138. https://doi.org/10.1109/EMR.2020.3005506

Tan, C., & Lee, S. Z. (2021). Adoption of enterprise risk management (ERM) in small and medium-sized enterprises: evidence from Malaysia. Journal of Accounting and Organizational Change. https://doi.org/10.1108/JAOC-11-2020-0181

Anexos

Anexo A: Plan de proyecto.

Anexo B: Acta de validación del resultado esperado R1.

Anexo C: Acta de validación del resultado esperado R2.

Anexo D: Acta de validación del resultado esperado R3.

Anexo E: Acta de validación del resultado esperado R4.

Anexo F: Acta de validación del resultado esperado R5.

Anexo G: Acta de validación del resultado esperado R6.

Anexo H: Acta de validación del resultado esperado R7.

Anexo A: Plan de proyecto

- ✓ Justificación

Desde los primeros meses del 2020, la pandemia del Coronavirus (Covid-19) ha representado una gran amenaza para la continuidad de negocios de empresas de todo tipo y tamaño alrededor del mundo (Margherita y Heikkilä, 2021), siendo las más afectadas las pymes, dado que, al estar limitadas por la cantidad de recursos que poseen (Tan y Lee, 2021), muchas veces no consideran al área de TI en el desarrollo de las estrategias de continuidad de negocios, ya que priorizan aquellos procesos que les genere un mayor beneficio económico (Siciliano y Gaudenzi, 2018). El tener una visión sesgada en el desarrollo de la continuidad de negocios, ha provocado que las pymes experimenten largos tiempos de inactividad en sus procesos a pesar de contar con un plan de continuidad de negocios (Sambo y Bankole, 2016), lo que genera pérdida de dinero, pérdida de confianza en la marca y una percepción de que el área de TI no hace bien su trabajo (Siciliano y Gaudenzi, 2018).

Según la revisión empírica realizada, se ha podido identificar que las empresas -en su mayoría grandes empresas- usan la ISO 22301 o modelos basados en esta norma como guía para la implementación y mantenimiento de su sistema de continuidad de negocios (Hersyah y Derisma, 2018); el punto débil de estos modelos es que están enfocados solamente a la continuidad de negocios en la cadena de suministros, lo cual no termina siendo de mucha utilidad para las pymes, ya que muchas de estas no cuentan con cadenas de suministros complejas. Así mismo, se pudo encontrar que algunas empresas si consideran la contingencia de TI dentro de sus planes de continuidad de negocios, sin embargo, estas medidas no llegan a ser del todo efectivas, ya que no se cuenta con una participación activa por parte del área de TI (Siciliano y Gaudenzi, 2018).

Por lo expuesto, el presente proyecto de fin carrera tiene como objetivo la implementación de un modelo multidisciplinar – basado en buenas prácticas sobre gestión de contingencia de TI – que permita a las pymes desarrollar los procedimientos, métricas y planes de contingencia que debe tener y mantener para poder hacer frente a incidentes que afecten la continuidad de sus operaciones.

- ✓ Viabilidad
  - ➢ Viabilidad temporal

El presente trabajo de fin de carrera tendrá una duración equivalente a 11 semanas, a partir del 21 de marzo del 2022 hasta el 5 de junio del 2022 (semana 11 del ciclo 2022-1 aproximadamente).

- Viabilidad técnica

  El presente proyecto de fin de carrera se considera técnicamente viable, debido a que se cuenta con conocimientos en gestión y gobierno de TI, continuidad de negocios y riesgos; además, se cuenta con el apoyo de los asesores de tesis en caso exista alguna duda o desconocimiento teórico sobre algún tema. Así mismo, se cuenta con acceso a la documentación de las distintas normas, marcos y estándares que serán de utilidad para el desarrollo del proyecto.

- Viabilidad económica

  El presente proyecto de fin de carrera se considera económicamente viable, ya que no se requiere de una inversión considerable dado que, ya se cuenta con una laptop para el desarrollo del proyecto y el acceso a la documentación de las normas, marcos y estándares se puede conseguir gratuitamente mediante la universidad y en algunos casos puede ser facilitada por el asesor.

✓ Alcance

El presente proyecto de tesis implica el desarrollo de un modelo multidisciplinar para la continuidad de negocios con enfoque en TIC que pueda ser aplicado por cualquier tipo de pyme. El proceso iniciará con la elaboración de una matriz de trazabilidad en la cual se asociarán las buenas prácticas identificadas en la revisión del estado del arte con sus respectivos propósitos en el modelo a desarrollar.

Luego se procederá a dividir el modelo en componentes, los cuales tendrán una estructura similar a la de COBIT 2019, es decir, cada componente tendrá:

- Un propósito.
- Una descripción.
- Un conjunto de procesos y actividades.
- Un conjunto de métricas.
- Un conjunto de indicadores.

- Una breve guía para su implementación.

Finalmente, se elaborarán plantillas para los planes de continuidad y contingencia, con la finalidad de que pueda servir de guía para las pymes en el proceso de documentación. Una guía del alcance que puede tener el presente proyecto se muestra en la Figura 28.

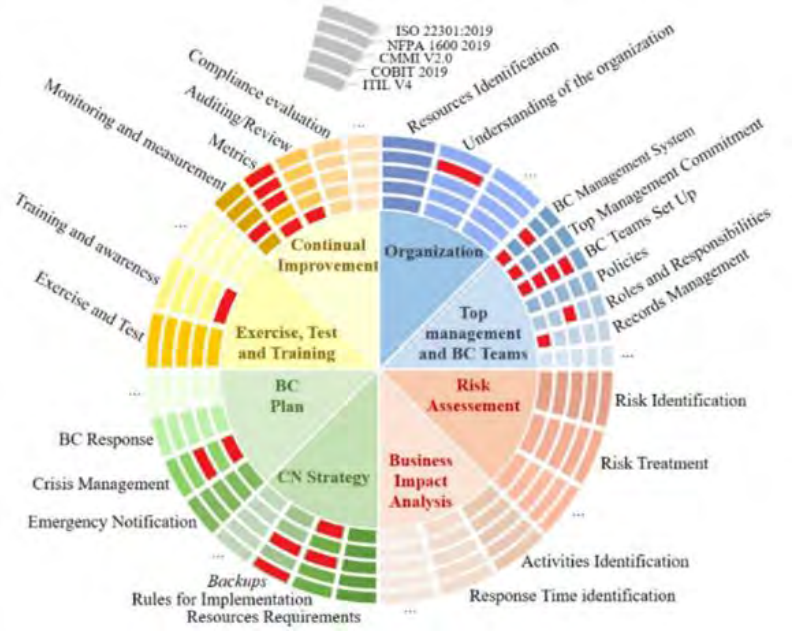


Figura 28. Componentes y actividades del BCMS. Fuente: (Russo et al., 2021).

✓ Limitaciones

El presente proyecto no está enfocado al desarrollo de un plan de continuidad de negocios ni un plan de recuperación ante desastres u ofrecer solamente un compendio de planes de continuidad para una empresa en particular; así mismo, tampoco se pretende ofrecer un planeamiento estratégico para la continuidad de negocios en las pymes, menos aún desarrollar una norma como la ISO 22301.

✓ Riesgos

En la presente sección se muestra la Tabla 30 con los riesgos identificados en el proyecto, la forma en que podría manifestarse el riesgo, su probabilidad de ocurrencia, el impacto que generaría en caso llegara a materializarse. Para medir la probabilidad y el impacto se usará una escala cualitativa de cinco niveles: muy alto, alto, medio, bajo y muy bajo.

Tabla 30. Riesgos.

Descripción	Manifestación	Probabilidad	Impacto	Mitigación
Problemas generados por la pandemia.	El tesista o alguien de la familia del tesista se enferma.	Alta	Muy alto	Tomar las medidas de bioseguridad necesarias para evitar contagios.
Falta de acceso a los diferentes especialistas para realizar la validación de los medios de verificación	Las personas encargadas de las validaciones no cuentan con disponibilidad y/o no se comunican con los asesores o el tesista	Alto	Muy alto	Contactar a los especialistas y agendar las reuniones virtuales con anticipación
Deterioro de equipos	La laptop con la que se realizará el desarrollo del proyecto presenta alguna falla	Media	Alta	Contar con copias de seguridad en el drive, así como, enviar los avances periódicamente a los asesores
Conectividad a internet	Fallas en la conexión a internet	Media	Media	Tener datos móviles de respaldo siempre que se tenga alguna actividad programada que requiera de conexión a internet.

Fuente: Elaboración propia.

✓ Estructura de descomposición del trabajo

En la Figura 29, se presenta la estructura de descomposición del trabajo para el presente proyecto

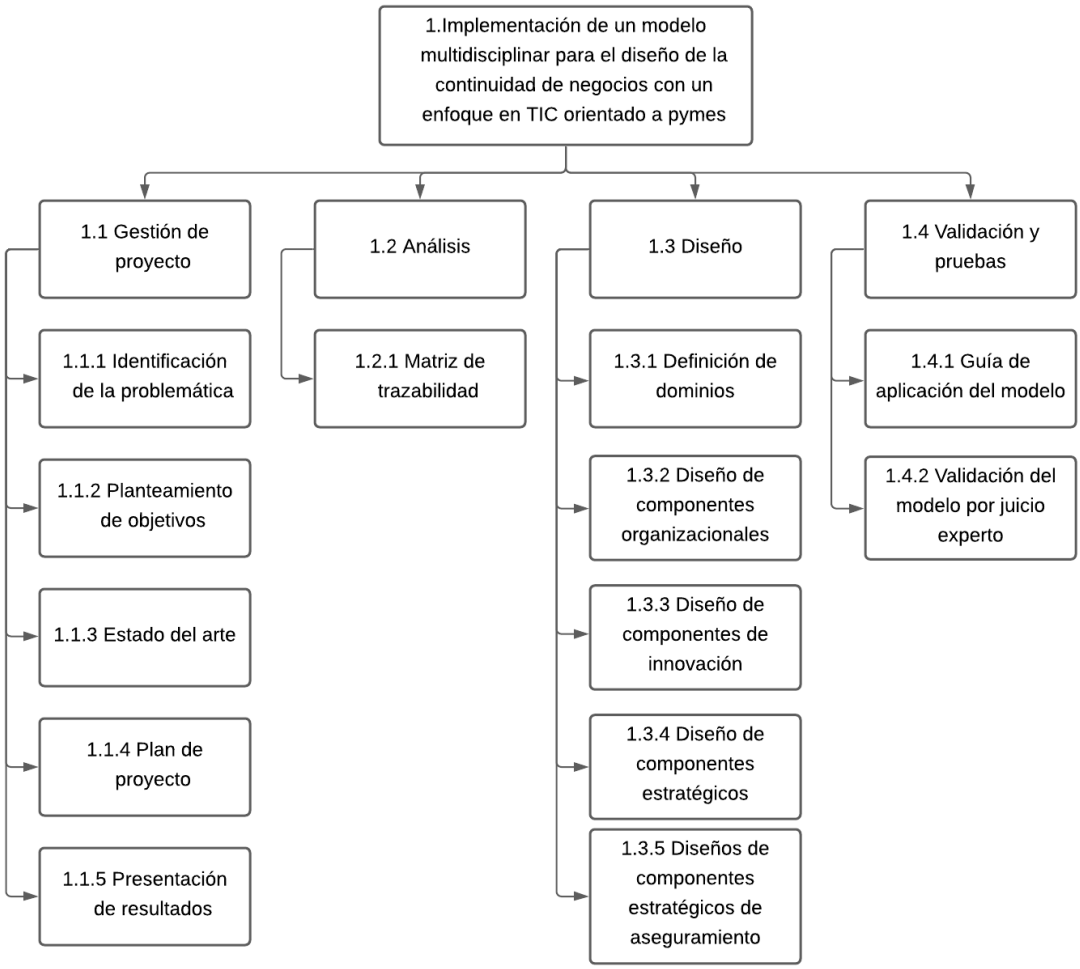


Figura 29. EDT. Fuente: Elaboración propia.

✓ Lista de tareas

En la Tabla 31 se muestran las actividades que se realizarán a lo largo del proyecto de tesis, indicando los días estimados de duración, el esfuerzo total y el costo.

Tabla 31. Lista de tareas.

Ítem	Actividad	Duración estimada (días)	Esfuerzo (hora - persona)	Costo (S/.)
1.1	**Gestión de proyecto**	**69**	**89**	**1157.0**
1.1.1	Desarrollar ficha de registro	4	4	52.0
1.1.2	Definir preguntas de revisión	1	1	13.0
1.1.3	Definir motores de búsqueda	1	1	13.0
1.1.4	Elaborar formulario de extracción	14	7	91.0
1.1.5	Revisión de la literatura	18	36	468.0
1.1.6	Desarrollar marco conceptual	3	3	39.0

1.1.7	Describir la problemática	3	3	39.0
1.1.8	Definir los objetivos del proyecto	3	3	39.0
1.1.9	Definir los resultados esperados	3	3	39.0
1.1.10	Definir métodos y procedimientos	4	4	52.0
1.1.11	Definir justificación del proyecto	1	2	26.0
1.1.12	Definir alcance del proyecto	1	1.5	19.5
1.1.13	Definir limitaciones del proyecto	1	1.5	19.5
1.1.14	Definir riesgos del proyecto	1	1	13.0
1.1.15	Definir EDT	1	2	26.0
1.1.16	Definir lista de tareas	2	3	39.0
1.1.17	Definir cronograma del proyecto	2	3	39.0
1.1.18	Definir costeo del proyecto	1	2	26.0
1.1.19	Presentar resultados	4	8	104.0
1.2	**Análisis**	**4**	**8**	**104.0**
1.2.1	Desarrollar matriz de trazabilidad	4	8	104.0
1.3	**Diseño**	**65**	**130**	**1690.0**
1.3.1	Definir dominios del modelo	6	12	156.0
1.3.2	Validar los dominios definidos con un experto en BSC	7	14	182.0
1.3.3	Definir los componentes organizacionales	6	12	156.0
1.3.4	Validar los componentes organizacionales con un experto en continuidad de negocios	7	14	182.0
1.3.5	Definir los componentes de innovación	6	12	156.0
1.3.6	Validar los componentes de innovación con un experto en continuidad de negocios	7	14	182.0
1.3.7	Definir los componentes de gestión de riesgos	6	12	156.0
1.3.8	Validar los componentes de gestión de riesgos con un experto en continuidad de negocios	7	14	182.0
1.3.9	Definir los componentes estratégicos	6	12	156.0
1.3.10	Validar los componentes estratégicos con un experto en continuidad de negocios	7	14	182.0
1.4	**Validación y pruebas**	19	38	494.0
1.4.1	Elaborar guía de aplicación del modelo	12	24	312.0
1.4.2	Validar la guía de aplicación con un experto en continuidad de negocios	7	14	182.0

Fuente: Elaboración propia.

- ✓ Cronograma del proyecto

A continuación, la Tabla 32 muestra el cronograma para el desarrollo del proyecto de tesis, indicando los días estimados de duración y las fechas aproximadas de inicio y fin para cada actividad. Para mayor detalle ingrese al siguiente enlace:

https://docs.google.com/spreadsheets/d/1JNcWbe5oeMMSKPmt2QsPdq6aLqV9pmGQ/edit?usp=sharing&ouid=113446393740774420678&rtpof=true&sd=true

Tabla 32. Cronograma del proyecto.

Ítem	Actividad	Duración (días)	Inicio	Fin
1.1 Gestión de proyecto				
1.1.1	Desarrollar ficha de registro	4	23/08/2021	27/08/2021
1.1.2	Definir preguntas de revisión	1	30/08/2021	31/08/2021
1.1.3	Definir motores de búsqueda	1	31/08/2021	31/08/2021
1.1.4	Elaborar formulario de extracción	14	01/09/2021	15/09/2021
1.1.5	Revisión de la literatura	18	02/09/2021	20/09/2021
1.1.6	Desarrollar marco conceptual	3	26/09/2021	29/09/2021
1.1.7	Describir la problemática	3	03/10/2021	06/10/2021
1.1.8	Definir los objetivos del proyecto	3	25/10/2021	28/10/2021
1.1.9	Definir los resultados esperados	3	25/10/2021	28/10/2021
1.1.10	Definir métodos y procedimientos	4	02/11/2021	06/11/2021
1.1.11	Definir justificación del proyecto	1	08/11/2021	08/11/2021
1.1.12	Definir alcance del proyecto	1	09/11/2021	09/11/2021
1.1.13	Definir limitaciones del proyecto	1	09/11/2021	09/11/2021
1.1.14	Definir riesgos del proyecto	1	10/11/2021	10/11/2021
1.1.15	Definir EDT	1	15/11/2021	15/11/2021
1.1.16	Definir lista de tareas	2	16/11/2021	17/11/2021
1.1.17	Definir cronograma del proyecto	2	16/11/2021	17/11/2021
1.1.18	Definir costeo del proyecto	1	17/11/2021	17/11/2021
1.1.19	Presentar resultados	4	18/11/2021	22/11/2021
Publicar cronograma de trabajo		4	21/03/2022	25/03/2022
1.2 Análisis				
1.2.1	Desarrollar matriz de trazabilidad	6	21/03/2022	27/03/2022
1.3 Diseño				
1.3.1	Definir dominios del modelo	6	28/03/2022	03/04/2022

Exposición 1		1	29/03/2022	29/03/2022
1.3.2	Definir los componentes organizacionales	6	04/04/2022	10/04/2022
Exposición 2		1	05/03/2022	05/03/2022
1.3.3	Validar los dominios definidos con un experto en BSC	6	11/04/2022	17/04/2022
1.3.4	Definir los componentes de gestión de riesgos	13	11/04/2022	24/04/2022
Exposición 3		1	12/04/2022	12/04/2022
1.3.5	Definir los componentes estratégicos	20	18/04/2022	08/05/2022
Exposición 4		1	19/04/2022	19/04/2022
1.3.6	Validar los componentes organizacionales con un experto en continuidad de negocios	6	25/04/2022	01/05/2022
Entrega avance parcial		6	02/05/2022	08/05/2022
1.3.7	Validar los componentes de gestión de riesgos con un experto en continuidad de negocios	6	02/05/2022	08/05/2022
1.3.8	Definir los componentes innovación	13	09/05/2022	22/05/2022
1.3.9	Validar los componentes estratégicos con un experto en continuidad de negocios	6	16/05/2022	22/05/2022
Exposición 5		1	24/05/2022	24/05/2022
1.3.10	Validar los componentes de innovación con un experto en continuidad de negocios	5	30/05/2022	05/06/2022
1.4 Validación y pruebas				
1.4.1	Elaborar guía de aplicación del modelo	13	16/05/2022	29/05/2022
1.4.2	Validar la guía de aplicación con un experto en continuidad de negocios	5	30/05/2022	05/06/2022
Exposición 6		1	31/05/2022	31/05/2022
Entregable final		6	06/06/2022	12/06/2022
Levantamiento de observaciones		6	27/06/2022	03/07/2022
Exposición final		1	05/07/2022	05/07/2022

Fuente: Elaboración propia.

- ✓ Lista de recursos

  En esta sección se muestran los recursos necesarios para el desarrollo del proyecto de tesis.

  - ➢ Personas involucradas y necesidades de capacitación
    - ▪ Un tesista para el desarrollo de todo el proyecto.

- Dos asesores de tesis para el seguimiento de todo el proyecto.
- Un especialista en continuidad de negocios para la validación de los componentes y el modelo en general.

➢ Estándares, normas y marcos utilizados en el proyecto

- El estándar ISO 22301 para ser utilizada como guía en el desarrollo del modelo.
- El marco COBIT para ser utilizado como guía en la definición y construcción de los componentes del modelo.
- La norma NIST SP 800-34 para ser utilizada como guía en la construcción de los componentes del modelo.
- El marco para la gestión de riesgos del NIST para ser utilizado como guía en la construcción de los componentes del modelo.

➢ Equipamiento requerido

- Una laptop para el desarrollo de todo el proyecto.
- Un smartphone con datos móviles como respaldo para cuando no se tenga internet disponible.

✓ Costeo del proyecto

En la Tabla 33 se muestran los costos estimados en los que se incurrirá para el desarrollo del proyecto de tesis.

Tabla 33. Costo del proyecto.

Ítem	Descripción	Unidad	Cantidad	Valor unitario (S/.)	Monto parcial (S/.)	Subtotal (S/.)
1	**Tesistas**					**265.0**
1.1	Tesista	Horas	265	10.0	265.0	
2.	**Otros participantes**					**4400.0**
2.1	Asesor	Horas	40	50.0	2000.0	
2.2	Asesora	Horas	40	50.0	2000.0	
2.3	Experto en continuidad de negocios	Horas	10	40.0	400.0	
3.	**Materiales**					**29.0**
3.1	Hojas bond	Millar	1	21.0	21.0	

3.2	Lapicero, resaltador	Unidad	4	2.0	8.0	
4.	**Bienes y equipos**					**2079.6**
4.1	Laptop	Unidad	1	400.0	400.0	
4.2	Internet	Mes	12	75.9	910.8	
4.3	Licencia Office 365	Año	1	290	290.0	
4.4	Plan de datos	Mes	12	39.9	478.8	
					Total	**6773.6**

Fuente: Elaboración propia.

Anexo B: Acta de validación del resultado esperado R1

Lima, 5 de abril del 2022

Validación de las buenas prácticas elegidas para la adaptación de los componentes del modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Por medio de la presente acta se hace constar que **Manuel Francisco Tupia Anticona** , identificado con DNI 10279924, ha revisado el proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión de las buenas prácticas seleccionadas y su relación con cada componente del modelo, correspondiente al resultado R1 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

Anexo C: Acta de validación del resultado esperado R2

Lima, 5 de abril del 2022

Validación de la estructura a alto nivel del modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Por medio de la presente acta se hace constar que **Manuel Francisco Tupia Anticona** ha revisado el proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión de la estructura en función de dominios que tendrá el modelo, correspondiente al resultado R2 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

Anexo D: Acta de validación del resultado esperado R3

Lima, 09 de mayo del 2022

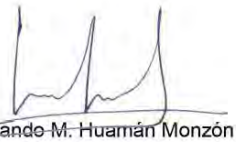
ACTA DE REVISIÓN Y VALIDACIÓN

Modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Validación del Componente Organizacional

Por medio de la presente acta se hace constar que **Fernando Miguel Huamán Monzón** ha revisado y validado el Componente Organizacional que formará parte del modelo correspondiente al resultado R3 del proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú.

Atentamente,



Ing. Fernando M. Huamán Monzón

Anexo E: Acta de validación del resultado esperado R4

Lima, 23 de mayo del 2022

Validación del componente de Innovación del modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Por medio de la presente acta se hace constar que **Jorge Herrera Tapia** ha revisado el proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del componente de Innovación que formará parte del modelo, correspondiente al resultado R4 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

JORGE SERGIO HERRERA TAPIA
Firmado digitalmente por JORGE SERGIO HERRERA TAPIA
Fecha: 2022.05.30 20:17:05 -05'00'

Ing. Jorge Herrera Tapia, PhD
Profesor Principal Universidad Laica Eloy Alfaro de Manabí
Manta - Ecuador
Email: jorge.herrera@uleam.edu.ec
Telf. +593 993 951 006

Anexo F: Acta de validación del resultado esperado R5

Lima, 23 de mayo del 2022

Validación del componente de Gestión de riesgos del modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Por medio de la presente acta se hace constar que **Jorge Herrera Tapia** ha revisado el proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a PYMES"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del componente de Gestión de riesgos que formará parte del modelo, correspondiente al resultado R5 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

JORGE SERGIO HERRERA TAPIA
Firmado digitalmente por JORGE SERGIO HERRERA TAPIA
Fecha: 2022.05.30 20:16:30 -05'00'

Ing. Jorge Herrera Tapia, PhD
Profesor Principal Universidad Laica Eloy Alfaro de Manabí
Manta - Ecuador
Email: jorge.herrera@uleam.edu.ec
Telf. +593 993 951 006

Anexo G: Acta de validación del resultado esperado R6

Lima, 23 de mayo del 2022

Validación del componente Estratégico del modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Por medio de la presente acta se hace constar que **Jorge Herrera Tapia** ha revisado el proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión del componente Estratégico que formará parte del modelo, correspondiente al resultado R6 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

JORGE SERGIO HERRERA TAPIA
Firmado digitalmente por JORGE SERGIO HERRERA TAPIA
Fecha: 2022.05.30 20:15:55 -05'00'

Ing. Jorge Herrera Tapia, PhD
Profesor Principal Universidad Laica Eloy Alfaro de Manabí
Manta - Ecuador
Email: jorge.herrera@uleam.edu.ec
Telf. +593 993 951 006

Anexo H: Acta de validación del resultado esperado R7

Lima, 06 de junio del 2022

Validación de la guía de aplicación del modelo de continuidad de negocios con enfoque en TIC orientado a pymes

Por medio de la presente acta se hace constar que **Jorge Herrera Tapia** ha revisado el proyecto de tesis titulado **"Implementación de un modelo multidisciplinar para el diseño de la continuidad de negocios con un enfoque en TIC orientado a pymes"** del alumno **Alexander Emmanuel Flores Barturen**, alumno de la especialidad de Ingeniería Informática en la Pontificia Universidad Católica del Perú. Se realizó la validación y revisión de la guía de aplicación del modelo, correspondiente al resultado R7 con el compromiso por parte del tesista de corregir y mejorar las observaciones hechas por el especialista.

Atentamente,

JORGE SERGIO HERRERA TAPIA
Firmado digitalmente por JORGE SERGIO HERRERA TAPIA
Fecha: 2022.06.05 16:15:03 -05'00'

Ing. Jorge Herrera Tapia, Ph.D
PROFESOR PRINCIPAL
E-mail: jorge.herrera@uleam.edu.ec
UNIVERSIDAD LAICA ELOY ALAFARO DE MANABÍ
MANTA - ECUADOR