UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

ESCUELA DE POSGRADO

TRABAJO DE POSGRADO

PROPUESTA DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LAS NORMAS TÉCNICAS PARA LA GESTIÓN DE CONTINUIDAD DE NEGOCIO (EN ESTUDIO) EN LAS ENTIDADES FINANCIERAS

PARA OPTAR AL GRADO DE

MAESTRO EN ADMINISTRACIÓN FINANCIERA

PRESENTADO POR

INGENIERO MARIO ERNESTO DUARTE FIGUEROA

INGENIERO CARLOS MAURICIO MARROQUÍN MONTERROSA

DOCENTE ASESOR

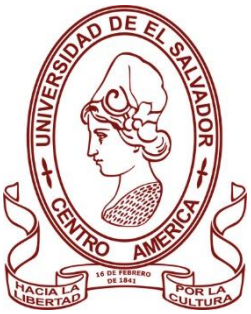
MAESTRO RICARDO JOSÉ FERNÁNDEZ DEL CID

OCTUBRE, 2021

SANTA ANA, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES



M.Sc. ROGER ARMANDO ARIAS ALVARADO

RECTOR

DR. RAÚL ERNESTO AZCÚNAGA LÓPEZ

VICERRECTOR ACADÉMICO

ING. JUAN ROSA QUINTANILLA QUINTANILLA

VICERRECTOR ADMINISTRATIVO

ING. FRANCISCO ANTONIO ALARCÓN SANDOVAL

SECRETARIO GENERAL

LICDO. LUIS ANTONIO MEJÍA LIPE

DEFENSOR DE LOS DERECHOS UNIVERSITARIOS

LICDO. RAFAEL HUMBERTO PEÑA MARÍN

FISCAL GENERAL

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

AUTORIDADES

M.Ed. ROBERTO CARLOS SIGÜENZA CAMPOS

DECANO

M.Ed. RINA CLARIBEL BOLAÑOS DE ZOMETA

VICEDECANA

LICDO. JAIME ERNESTO SERMEÑO DE LA PEÑA

SECRETARIO

M.Ed. JOSE GUILLERMO GARCÍA ACOSTA

DIRECTOR DE LA ESCUELA DE POSGRADO

AGRADECIMIENTOS

A mí Padre Celestial que ha tenido misericordia y gracia para conmigo, a mi esposa Glenda y mi hijo Jefferson que son mis compañeros de aventuras, a mis padres que no dejan de apoyarme en todo lo que hago, a mis hermanos Tony, Marvin y Fabricio por su incondicional apoyo. Gracias a todos por complementar y apoyar mis planes y proyectos.

A Mario mi compañero de tesis por su esfuerzo y dedicación para lograr nuestro objetivo.

Carlos Mauricio Marroquín Monterrosa.

A Dios, por permitirme alcanzar este logro.

A mi madre, por su apoyo incondicional.

A Camila e Isabella, por ser la motivación de mi vida.

A Carlos, mi compañero de tesis por su dedicación y empeño.

Mario Ernesto Duarte Figueroa.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

Uno de los factores estratégicos de toda organización es asegurar la continuidad de sus productos y servicios relevantes frente a un riesgo o incidente de alto impacto, el propósito de este estudio es ofrecer una herramienta que permita a las instituciones financieras del país adoptar e implementar un sistema de gestión de continuidad de negocio, dentro del marco de la gestión integral del riesgo operacional y en cumplimiento a la legislación regulatoria del país.

La investigación se diseñó bajo el enfoque mixto, haciendo uso de instrumentos tanto cuantitativos como cualitativos, como parte de la investigación se analizó la información de aspectos teóricos acerca de estándares, sanas prácticas y metodologías para gestionar la continuidad de negocio. Adicionalmente, se obtuvo información para realizar una valoración del nivel de avance que las entidades financieras poseen en materia de gestión de continuidad de negocio, para ello se determinó como población las entidades que forman parte del Sistema Financiero del país, siendo sujetos obligados del cumplimiento de las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24.

Se empleó como técnica la encuesta, como instrumento de recolección de datos, lo que permitió obtener como resultado que existe en las entidades financieras marcadas brechas de desarrollo en elementos indispensables para una adecuada gestión de continuidad de negocio, evidenciando la necesidad de contar con la metodología propuesta en este estudio.

Partiendo de lo anterior, se recomiendan una serie de directrices y lineamientos para el diseño e implementación de un sistema de gestión de continuidad de negocio para que las entidades financieras desarrollen capacidades de adaptación y respuesta ante circunstancias tan cambiantes que pongan en riesgo su sostenibilidad en el tiempo. La guía metodológica que se propone brinda orientación y pautas a seguir para implementar dicha gestión, tomando como base la normativa regulatoria nacional, así como estándares y buenas prácticas internacionales en la materia.

INTRODUCCIÓN

Las entidades financieras en El Salvador, así como cualquier otra organización, tienen como parte de sus objetivos principales el asegurar la entrega de sus Productos y Servicios de manera continua a sus partes interesadas y fortalecer su capacidad de respuesta ante incidentes de interrupción significativos.

El Salvador es un país que permanentemente se encuentra amenazado por eventos naturales de alto impacto, los cuales han provocado una serie de desastres a lo largo de su historia, como terremotos, erupciones volcánicas, derrumbes, inundaciones, entre otros; así como factores atribuibles a las tecnologías de información, exponen la posible materialización de riesgos, que tienen la capacidad de causar graves interrupciones en la operación normal de una entidad, aumentando el impacto en las pérdidas financieras, de información crítica e imagen, debido a la indisponibilidad de los recursos y servicios de la institución.

La gestión de continuidad de negocio es un proceso de dirección, como parte de la Gestión Integral de Riesgos, que permite identificar los impactos potenciales que amenazan a las entidades y propone un marco adecuado para el desarrollo de la capacidad de responder de forma efectiva, brindar seguridad a las personas, proteger los activos, reducir los tiempos de interrupción y asegurar la reputación de éstas.

Una entidad financiera se vuelve más vulnerable frente a los riesgos y amenazas a medida que:

a. Desconoce el impacto al que se exponen sus funciones al no tener identificados y priorizados los productos, procesos críticos y los elementos de los que depende su continuidad, tanto internos: personal, recursos, tecnología; como externos: proveedores, aspectos contractuales o legales.
b. Carece de estructuras organizativas, roles y responsabilidades en materia de continuidad de negocio.
c. Carece de estrategias de recuperación y planes de continuidad, donde se establezcan los objetivos, prioridades y acciones de recuperación y restauración.

Muchas instituciones toman como referencia el estándar internacional ISO 22301 que orienta sobre la implementación de un Sistema de Gestión de Continuidad de Negocio, no obstante, las entidades financieras se rigen por las normativas que los entes reguladores u organismos internacionales emiten a fin de que éstas se fortalezcan en relación a su gestión de continuidad.

El Banco Central de Reserva, en su función de ente regulador del Sistema Financiero emitió las "Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio – NRP-24". Donde se requiere que los sujetos obligados al cumplimiento de estas normas cuenten con requisitos mínimos para gestionar la continuidad de negocio en sus entidades, de tal modo que se asegure la prestación de los principales procesos de estas entidades en beneficio de las partes interesadas.

A pesar de que el origen de la clasificación de la continuidad del negocio como sistema de gestión es relativamente nuevo (siglo 21), se debe aceptar y reconocer que las acciones de contingencia para recuperar y restablecer la operación en una entidad no es un hecho reciente, lo que si es reciente es la tendencia en aumento de adoptar la continuidad por una gran cantidad de entidades financieras en todo el mundo, lo cual conlleva a plantearse la siguiente pregunta:

¿Cuál ha sido el factor que genera un alto interés en la gestión de la Continuidad de Negocio?

Sin dudar, una de las principales respuestas recae en las grandes pérdidas financieras, que han impactado de forma negativa el patrimonio de las instituciones, cuando han experimentado incidentes disruptivos; sin dejar de lado la afectación en la reputación, y por ende, la disminución en la creación de valor.

Otro factor que impulsa la adopción de una gestión de continuidad, son las condiciones mínimas que una entidad financiera debe poseer para garantizar la capacidad de respuesta ante los riesgos operacionales, establecidos por el Comité de Supervisión Bancaria de Basilea en las Buenas Prácticas para la Gestión y Supervisión del Riesgo Operativo, específicamente en el principio 7: *"Los bancos deberán contar con planes de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad".*

Asimismo, en la regulación del sistema financiero del país, se establece en el artículo 16 de las "Normas Para la Gestión del Riesgo Operacional en las Entidades Financieras (NPB4-50)":

"Las entidades financieras deben implementar un sistema de gestión de continuidad del negocio en caso de interrupciones, que incluyan planes de contingencia, análisis de impacto en el negocio, plan de recuperación de desastres y planes de gestión del incidente, que aseguren la operatividad normal del negocio ante la ocurrencia de eventos adversos."

La gestión del riesgo operacional consiste en minimizar las interrupciones y determinar los impactos de éstas. Involucra la elaboración de planes de continuidad ante desastres que minimicen las pérdidas económicas, disminuyan los tiempos de inactividad, mejoren la reputación, protejan personas y bienes. En este contexto, se propone una guía metodológica para facilitar la implementación de un sistema de gestión de continuidad en las entidades financieras.

El documento comprende los siguientes capítulos:

Capítulo I presenta la problemática planteada, así como los objetivos que se pretende alcanzar, así como la justificación y alcance de la investigación.

Capítulo II comprende el Marco Teórico, se describe de forma general el Sistema Financiero del país, las principales definiciones, así como el marco de referencia para la investigación.

Capítulo III describe la metodología de la investigación, en cuanto al tipo y métodos utilizados.

Capítulo IV presenta tabulación y resultados obtenidos del análisis.

Capítulo V presenta la propuesta y desarrollo metodológico para la gestión de continuidad de negocio, implementa el ciclo de vida y considera mejores prácticas internacionales.

Finalmente, se presenta las conclusiones y recomendaciones obtenidas de la investigación.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Situación problemática

El Comité de organizaciones patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés) establece un modelo conceptual para de "Gestión de Riesgos Corporativos. Marco Integrado", en el que define la importancia del control interno dentro de las organizaciones y orienta a que las instituciones desarrollen elementos que aseguren la efectividad y eficiencia de las operaciones, la identificación de eventos potenciales y su respuesta, la confiabilidad de la información y el cumplimiento de leyes y regulaciones.

Existen disposiciones emitidas por el Banco Central de Reserva de El Salvador, como ente regulador, donde señalan que las entidades reguladas deben implementar un sistema de gestión de continuidad de negocio, con el objetivo de asegurar su capacidad de operación en forma permanente y minimizar las pérdidas en caso de interrupción de sus actividades.

Las entidades financieras requieren diseñar, implementar y mantener una serie de políticas y procedimientos para responder ante la ocurrencia de eventos de alto impacto que afecten el normal desarrollo de sus operaciones, especialmente en la actualidad donde cada vez más las operaciones del negocio dependen de la tecnología.

Frente a la posible ocurrencia de desastres, interrupciones o contingencias que pueden originar que los negocios y operaciones financieras se suspendan o no se reestablezcan dentro de los plazos requeridos, es necesario que las entidades del sistema financiero cuenten con un sistema de gestión de continuidad que permita, entre otros resultados, formular los planes de continuidad para fortalecer la respuesta, reanudación y recuperación de sus operaciones.

La gestión de riesgos conlleva a identificar los eventos que pueden ocasionar una interrupción, a establecer un determinado nivel de aceptación, a mitigar aquellos que pueden tratarse y a implementar controles, siempre existen situaciones que se pueden desencadenar en un incidente. Entendiendo que un incidente es un evento súbito o calamitoso que conlleva a

un daño, una pérdida o a una destrucción; es una alteración intensa en las personas, los bienes y en el negocio (productos y servicios), causadas por un suceso natural o generado por la actividad humana, que excede la capacidad de respuesta de la entidad afectada.
Existen muchos factores que fuerzan a las instituciones a demostrar la resistencia de las actividades de su negocio ante cualquier incidente: la búsqueda en ser más competitivos, las demandas más exigentes de clientes u otras partes interesadas y la exigencia de requerimientos regulatorios o legales más restrictivos.

Una interrupción del servicio eléctrico, un terremoto, un incendio o una indisponibilidad del centro de procesamiento de información se deben considerar como amenazas reales que merecen un tratamiento preventivo para evitar, en caso de que éstas se materialicen, que las pérdidas sean tan graves que afecten a la viabilidad del negocio.

Son múltiples las instituciones que, independientemente de su tamaño y naturaleza, fracasan o incluso desaparecen por la inexistencia de procesos, estrategias, planes y técnicas que mitiguen los riesgos a los que están expuestos y puedan brindar una garantía de alta disponibilidad en las operaciones de su negocio. De esta manera, se vuelve importante y necesario que las instituciones establezcan una serie de medidas estratégicas, organizativas, técnicas y procedimentales que garanticen la continuidad de los procesos críticos de negocio en caso de tener que afrontar un grave incidente.

Uno de los principales obstáculos o limitantes a las que se enfrenta una institución cuando decide emprender cualquier tipo de iniciativa relacionada con la continuidad de negocio, es la carencia de conocimientos y de instrucciones claras y concisas que muestren por dónde se debe empezar y qué aspectos deben considerarse para tener implementado un adecuado sistema de gestión de continuidad del negocio.

Esta guía metodológica busca solventar estos niveles de desorientación para aquellas instituciones que deseen comprender y conocer los principios y las prácticas del ciclo de vida de todo sistema de gestión de continuidad del negocio.

1.2. Enunciado del problema

Tomando en cuenta la situación problemática, la investigación se orientó con la formulación de la siguiente pregunta: ¿Están las instituciones financieras preparadas para resistir, adaptarse y superar un incidente perturbador?

1.3. Objetivo de la investigación

Objetivo general

Ofrecer una herramienta de consulta que permita resaltar la relevancia y conciencia acerca de la importancia crítica que tiene asegurar la continuidad de las operaciones en una institución financiera, lo que permitirá garantizar la entrega de sus productos/servicios y cumpliendo con la legislación regulatoria del país, que le exige la adopción de un sistema de gestión de continuidad del negocio, dentro del marco de la gestión integral del riesgo operacional.

Objetivos específicos

Que las entidades del sistema financiero puedan:

- Minimizar las pérdidas de un evento disruptivo por medio del fortalecimiento de la resiliencia del negocio.
- Analizar el impacto por la interrupción de los procesos críticos frente a eventos disruptivos.
- Identificar los procesos, sus recursos y dependencias, que permiten la entrega de productos y servicios relevantes.
- Establecer las estrategias de continuidad y recuperación de los procesos críticos.
- Definir la estructura organizativa, sus roles y responsabilidades en materia de continuidad.
- Documentar los planes de continuidad de negocio.
- Fomentar la cultura de continuidad al interior de la institución.
- Mantener y mejorar el sistema de gestión de continuidad de negocio.

1.4. Justificación

Las instituciones no pueden estar completamente preparadas para todos y cada una de las situaciones adversas que pueden sucederle e impactarle en las actividades críticas. Sin embargo, hay unas que logran superar estos eventos debido al nivel preventivo que poseen, poniendo en marcha las medidas necesarias para protegerse. Evidentemente, toda institución posee una dependencia de sus recursos, del personal y de las tareas que día a día ejecuta. A medida que alguno de estos componentes es afectado, la institución puede paralizarse. Cuanto mayor sea el tiempo de inactividad, mayor es el impacto financiero, objetivo y/o reputacional en el negocio.

El objetivo último de cualquier sistema de gestión de continuidad operativa es garantizar que ésta cuenta con una respuesta planificada ante cualquier evento adverso que pueda poner en riesgo su supervivencia. Esta afirmación de por sí, evidencia y explica la necesidad de implantar en las instituciones, acciones y medidas orientadas a la continuidad de sus actividades.

Adicional puede aportar otros beneficios:

- Minimiza o previene las pérdidas de la institución en caso de desastre y permite definir de forma más eficiente el presupuesto en materia de seguridad.
- Disminuye el riesgo de sufrir observaciones y sanciones por entes fiscalizadores.
- Apoya y refuerza la gestión de los riesgos operacionales y fomenta una ventaja competitiva frente a otras instituciones.

1.5. Alcance de la investigación

El trabajo a desarrollar se enmarca en proporcionar al sistema financiero una guía metodológica para que las entidades implementen su sistema de gestión de continuidad y puedan así formular los planes de continuidad respectivos. Dada la complejidad y variabilidad que existe entre una institución y otra, debido a su naturaleza, tamaño y volumen de operaciones, esta guía propone las fases y elementos relevantes que deben considerarse para la implementación de dicho sistema de gestión.

CAPITULO II: MARCO TEÓRICO

2.1. El sistema financiero en El Salvador

El Sistema Financiero se considera parte vital en cualquier sociedad, debido a que en él interactúan diferentes agentes económicos privados y públicos, encargados de producir bienes y servicios en la economía, y los consumidores. Aporta a la producción de un país a través de la generación de productos y servicios de intermediación y de fondos que necesitan las personas para llevar a cabo sus proyectos productivos. Un Sistema Financiero estable, solvente y en desarrollo participa en la estabilidad económica y financiera de un país. La principal función del Sistema Financiero es recibir el ahorro de las personas y empresas, cuidarlo, otorgar préstamos de dinero (créditos) y canalizarlo a negocios (actividades productivas), es decir, a la inversión.

2.1.1. Instituciones que componen el sistema financiero y su rol

De acuerdo a la Ley de Supervisión y Regulación del Sistema Financiero, en el artículo 1, establece que "El Sistema de Supervisión y Regulación Financiera está constituido por la Superintendencia del Sistema Financiero, en adelante denominada "Superintendencia" y por el Banco Central de Reserva. La Supervisión de los integrantes del sistema financiero y demás supervisados de conformidad a esta Ley es responsabilidad de la Superintendencia; la aprobación del Marco Normativo Macro Prudencial necesario para la adecuada aplicación de ésta y las demás leyes que regulan a los integrantes del sistema financiero y demás supervisados, le corresponde al Banco Central. La ejecución y aplicación de la presente Ley se realizará por la Superintendencia y el Banco Central dentro de sus respectivos ámbitos de competencia".

2.1.2. Rol del Banco Central de Reserva de El Salvador (BCR)

El Banco Central tiene, entre otras facultades, las responsabilidades siguientes:

- Regular el sistema Financiero;
- Contribuir para que el país tenga un sistema financiero seguro, eficiente y transparente, que brinde seguridad y confianza a la población y que apoye el crecimiento sostenido de la economía;

- Velar por el buen funcionamiento de los sistemas de pago del país;
- Ofrecer análisis, estudios e investigaciones técnicas para propiciar la toma de mejores decisiones en materia económica y financiera;

Por otra parte, el Banco Central participa activamente en el mercado de valores. En el área de las finanzas públicas, el Banco Central mantiene las funciones de agente financiero del Estado y servicios de asesoría económica y financiera.

2.1.3. Rol de la Superintendencia del Sistema Financiero (SSF)

Según el art. 3 de la Ley de Supervisión y Regulación del Sistema Financiero, inciso primero, la Superintendencia es responsable de supervisar la actividad individual y consolidada de los integrantes del sistema financiero y demás personas, operaciones o entidades que mandan las leyes; para el ejercicio de tales atribuciones contará con independencia operativa, procesos transparentes y recursos adecuados para el despeño de sus funciones. De forma más detallada, la Superintendencia se encarga de:

- Autorizar la constitución, funcionamiento y cierre de los intermediarios financieros, tales como: bancos, conglomerados financieros, intermediarios financieros no bancarios, sociedades de seguro, filiales agencias en el extranjero y demás entidades que las leyes señalan.
- Vigilar y fiscalizar las operaciones de las instituciones supervisadas, con el fin de prevenir situaciones de iliquidez e insolvencia en las instituciones bajo su control.
- Las demás funciones de inspección y vigilancia que le corresponden de acuerdo con las leyes.

2.1.4. Instituto de Garantía de Depósitos (IGD)

Es una Institución pública de crédito, autónoma, con personalidad jurídica y patrimonio propio, cuya misión es garantizar los ahorros de los depositantes en cada una de sus instituciones miembros (IMI), hasta el límite establecido en la Ley. Esta protección se da en el caso que la Superintendencia ordene el cierre forzoso de cualquiera de sus Instituciones Miembros (IMIS).

2.1.5. Entidades participantes

Las entidades que participan en el Sistema Financiero son las siguientes:

A. Instituciones captadoras y de crédito

a) Bancos

Se constituyen como sociedades anónimas y tienen por finalidad mediar entre quienes cuentan con dinero y quienes lo necesitan a través de instrumentos que ayudan a administrar y disponer de él con seguridad.

b) Bancos Cooperativos

Son entidades constituidas para captar depósitos del público y prestar servicios financieros. Pueden constituirse en forma de sociedades o asociaciones cooperativas de ahorro y crédito, incluyendo las Cajas de Crédito Rurales y los Bancos de los Trabajadores. Están sometidas a la vigilancia y fiscalización de la Superintendencia del Sistema Financiero.

c) Federaciones de Bancos Cooperativos

Son organizaciones en las que se agrupan Asociaciones o Sociedades Cooperativas de giro financiero o Sociedades de Ahorro y Crédito. Su objetivo es prestar servicios financieros, de asesoría y asistencia técnica.

d) Sociedades de Ahorro y Crédito (SAC)

Son sociedades anónimas que pueden captar y colocar créditos y están sujetas a las disposiciones de la Ley de Bancos y en la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito.

e) Banco de Desarrollo de El Salvador (Bandesal)

Es una institución pública de crédito, autónoma, cuyo principal objetivo es promover, con apoyo financiero y técnico, el desarrollo de proyectos de inversión viables y rentables de los sectores productivos del país, por medio de la concesión de préstamos en condiciones de mercado, a través de las instituciones financieras del sistema o de forma directa.

f) Banco de Fomento Agropecuario (BFA)

Es una institución oficial de crédito, cuyo objetivo es crear, fomentar y mantener facilidades financieras y servicios conexos necesarios para contribuir al fomento agrícola.

g) Instituciones públicas de crédito

i. Fondo Nacional de Vivienda Popular (FONAVIPO)

Institución autónoma cuyo objetivo es facilitar a las familias salvadoreñas de más bajos ingresos, el acceso al crédito que les permita solucionar su problema de vivienda.

ii. Fondo Social para la Vivienda (FSV)

Su objeto es la prestación de servicios financieros para solucionar el problema habitacional de la población empleada en los sectores público y privado.

iii. Corporación Salvadoreña de Inversiones (CORSAIN)

Promueve sociedades y empresas dedicadas a la realización de actividades industriales, especialmente: manufactureras, agroindustriales, extractivas mineras, de pesca e industrialización de productos del mar, así como la promoción del turismo.

iv. Fondo Solidario para la Familia Microempresaria (FOSOFAMILIA)

Su objeto es otorgar créditos, preferentemente y atender las necesidades crediticias de la mujer, en los sectores comerciales, industriales, agropecuarios, artesanales, agroindustriales, de servicios, culturales, y de toda actividad productiva a nivel nacional.

v. Fondo de Saneamiento y Fortalecimiento Financiero (FOSAFFI)

Su finalidad esencial es proceder al saneamiento y fortalecimiento de Bancos Comerciales y Asociaciones de Ahorro y Préstamo, que para tales fines fueran seleccionados por el Banco Central de Reserva, de entre las instituciones financieras cuyas acciones fueron expropiadas mediante la Ley de Nacionalización de las Instituciones de Crédito y Asociaciones de Ahorro y Préstamo.

B. Sistemas de pagos

a) Empresa de transferencia de dinero (Remesadora)

Persona jurídica o extranjera que cumpliendo los requisitos de su país de origen presta el servicio de envío o recepción de dinero, por cualquier medio, sean propios o de terceros.

b) Proveedores de dinero electrónico

Sociedades Proveedoras, bancos, bancos cooperativos y sociedades de ahorro y crédito autorizados para proveer dinero electrónico.

c) Casas de cambio en moneda extranjera

Son sociedades anónimas cuya actividad habitual es la compra y venta de moneda extranjera en billetes, giros bancarios, cheques de viajero y otros instrumentos de pago expresados en divisas.

d) Administradores de sistemas de pagos móviles

Entidad para administrar u operar un sistema de pagos móviles.

C. Previsionales

a) Instituto de Pensiones de los Empleados Públicos (INPEP)

Su objetivo es el manejo e inversión de los recursos destinados al pago de prestaciones, para la cobertura de los riesgos de invalidez, vejez y muerte de los empleados públicos.

b) Instituto Salvadoreño del Seguro Social: Programa de Invalidez, Vejez y Muerte

Se encarga del manejo e inversión de recursos destinados al pago de prestaciones, para la cobertura de riesgos de invalidez, vejez y muerte de los empleados y obreros del sector privado.

c) Instituto de Previsión Social de la Fuerza Armada (IPSFA)

Su función principal es la administración de recursos con fines de previsión y seguridad social, para los elementos de la fuerza armada.

d) Administradoras de Fondos de Pensiones (AFP)

Son instituciones previsionales constituidas como sociedades anónimas que tienen por objeto exclusivo la administración de un fondo de pensiones, así como gestionar y otorgar las prestaciones y beneficios que establece la Ley del Sistema de Ahorro para Pensiones.

D. Seguros y fianzas

a) Sociedades de seguros

Son sociedades anónimas que operan en seguros, reaseguros, fianzas y reafianzamientos. En el contrato de seguro (de acuerdo al Código de Comercio), la empresa aseguradora se obliga, mediante una prima, a resarcir un daño o a pagar una suma de dinero al verificarse la eventualidad prevista en el contrato.

b) Sociedades de garantía recíproca

Sociedades anónimas cuya finalidad exclusiva es otorgar a favor de sus socios partícipes, avales, fianzas y otras garantías financieras aprobadas por la Superintendencia del Sistema Financiero.

E. Mercados bursátiles

a) Bolsas de valores

Sociedades anónimas que tienen por finalidad proveer los medios necesarios para realizar transacciones de valores y que puedan efectuar actividades de intermediación de valores.

b) Casas de corredores de bolsa

Son sociedades anónimas cuya finalidad es intermediar valores. Pueden realizar, además, operaciones de administración de cartera, previa autorización de la Superintendencia de Valores.

c) Sociedades especializadas en el depósito y custodia de valores

Son sociedades anónimas que reciben valores en custodia de intermediarios financieros y público en general, prestando, además, los servicios de cobro de amortizaciones.

d) Organizaciones auxiliares - almacenes generales de depósito

Tienen por objeto principal encargarse de la custodia y conservación de mercancías depositadas a su cuidado, emitiendo certificados de depósito y bono de prenda sobre dichas mercancías.

e) Emisores

Empresas públicas o privadas que emiten valores que se negocian en la Bolsa de Valores. Ponen a disposición de los inversionistas sus bonos y/o acciones para obtener financiamiento.

f) Inversionistas

Personas naturales o empresas que invierten su dinero en valores con el fin de obtener un rendimiento a cambio y hacer crecer su dinero.

g) Calificadoras de riesgo

Empresas dedicadas al análisis profundo del riesgo económico – financiero, emitiendo opinión sobre la calidad crediticia de un emisor y/o sus emisiones.

h) Central de Depósitos de Valores (CEDEVAL)

Entidad especializada que recibe valores para su custodia y administración.

i) Sociedad titularizadora

Entidad que estructura la emisión de titularización, realiza la colocación a través de la Bolsa de Valores y administra el Fondo de Titularización.

j) Representante de los tenedores

Verifica el proceso de administración del fondo de Titularización se desarrolle adecuadamente.

k) Sociedad gestora

Su finalidad principal es administrar fondos de inversión y actividades complementarias a estas.

l) Sociedad especializada en valoración de precios

Es la encargada del proceso de valuación de los valores en que invierten los Fondos.

F. Otros

a) Agencia de información de datos

Toda persona jurídica, pública o privada, exceptuando a la Superintendencia que se dedica a recopilar, almacenar, organizar, comunicar, transferir o transmitir los datos sobre el historial de crédito de los consumidores o clientes, a través de procedimientos técnicos, automatizados o no.

b) Conglomerados financieros

Grupos de entidades que cubren los servicios ofrecidos por los bancos, las compañías de seguros y las sociedades de inversión, o al menos dos de las anteriormente citadas.

c) Auditores externos

Ofrecen una opinión independiente de los estados contables anuales de la organización. Su enfoque es histórico por naturaleza, dado que evalúan si los estados cumplen con principios contables de aceptación general, si presentan adecuadamente la situación financiera, si están representados con precisión, y si los estados contables han sido materialmente manipulados.

d) Peritos

Su función consiste en la valoración de los bienes muebles e inmuebles de los bancos, así como cuando por disposiciones legales sea necesario valorar dichos bienes que reciban en garantía, se requerirá que tales valoraciones se efectúen por peritos inscritos en la Superintendencia.

e) Interventores

Responsable máximo a nivel administrativo de una Oficina o sucursal bancaria de una Entidad Financiera, coordina todos los aspectos administrativos, es decir, el trabajo que se genera como consecuencia de la realización de cualquier tipo de operaciones bancarias por los clientes.

f) Liquidadores

Son administradores y representantes que tienen entre sus facultades construir operaciones sociales que hubieran quedado pendientes al tiempo de la disolución, cobrar lo que se deba a la sociedad y pagar lo que ella deba, así como practicar el balance final de la liquidación.

g) Actuarios

Son profesionales de negocios que abordan la gestión y evaluación del impacto financiero del riesgo y la incertidumbre de una entidad, y que además poseen un profundo conocimiento de los sistemas de seguridad financiera.

2.1.6. Estructura del sistema financiero, siglas y acrónimos

a) Regulación y supervisión

- Banco Central de Reserva de El Salvador (BCR)
- Superintendencia del Sistema Financiero (SSF)

b) Mercados Financieros

- Administradoras de Fondos de Pensiones (AFP's)
- Automatic Clearing House o cámara de compensación automatizada (ACH)
- Banco de Desarrollo de El Salvador (BANDESAL)
- Fondo de Desarrollo Económico (FDE)
- Fondo de Saneamiento y Fortalecimiento Financiero (FOSAFFI)
- Fondo Nacional de Vivienda Popular (FONAVIPO)
- Fondo Salvadoreño de Garantías (FSG)
- Fondo Social para la Vivienda (FSV)
- Fondo Solidario para la Familia Microempresaria (FOSOFAMILIA)
- Instituto de Garantía de Depósitos (IGD)
- Instituto de Previsión Social de la Fuerza Armada (IPSFA)

- Instituto Nacional Pensiones de los Empleados Públicos (INPEP)
- Instituto Salvadoreño del Seguro Social (ISSS)

La figura 1 presenta la estructura del Sistema Financiero con todas las instituciones participantes.

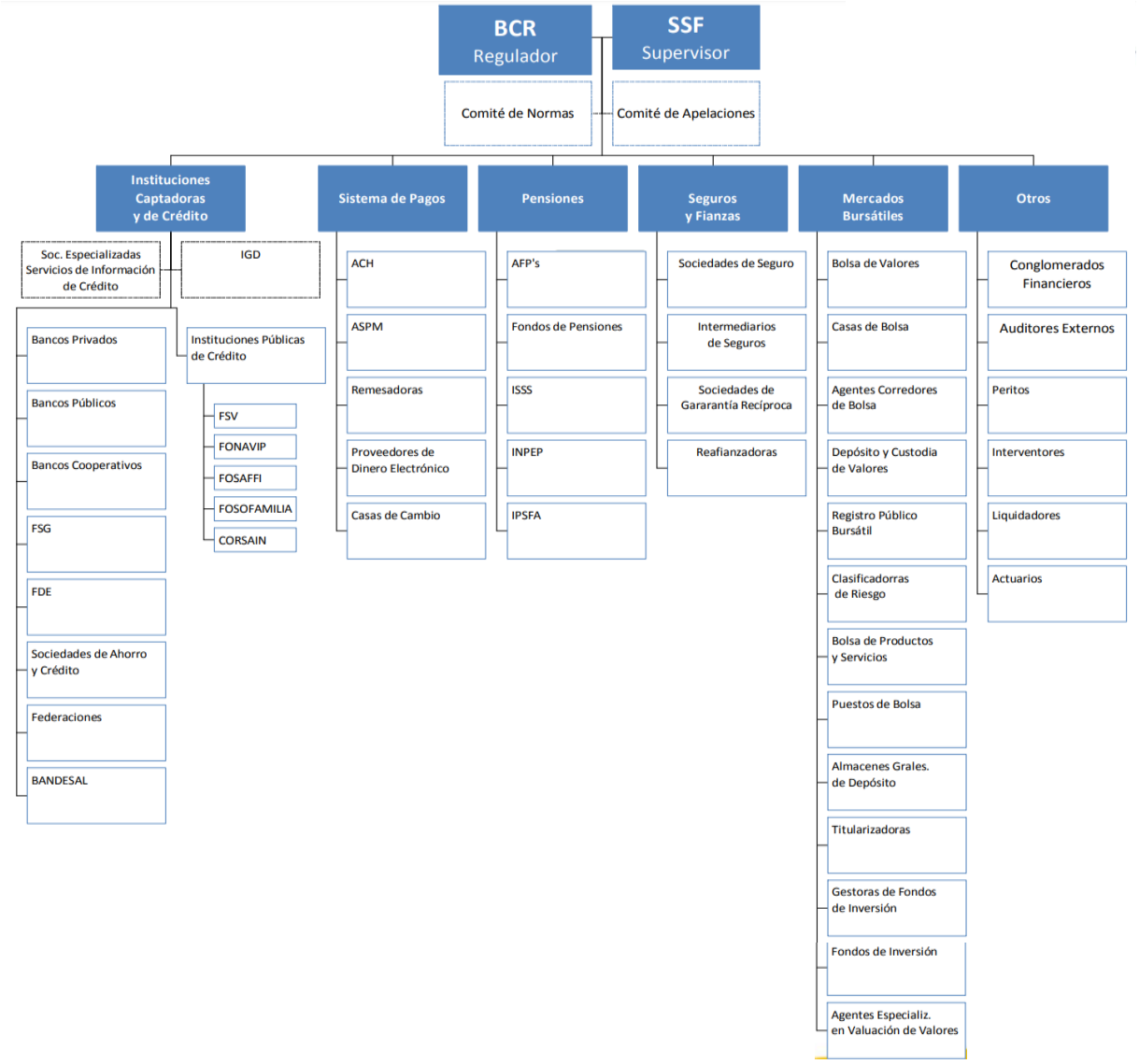


Figura 1. Estructura del Sistema Financiero en El Salvador

2.2. Definición de riesgo

2.2.1. Riesgo

Generalmente, cuando se hace alusión al termino riesgo, se asocia a "aquellos sucesos que impactan de forma adversa los objetivos estratégicos y operativos de toda entidad". La premisa fundamental en materia de riesgos, para el logro de objetivos, es que toda entidad no puede ni debe perder de vista a que se enfrenta, que puede salir mal, que puede generar variación en los resultados esperados, esto conlleva a prever y conocer los posibles eventos que pueden impedir o modificar estos resultados.

Esta apreciación del riesgo contempla su identificación, análisis y evaluación. El tratamiento de éste se basa en potenciar los riesgos positivos (oportunidades) y disminuir aquellos que se consideran negativos.

Una definición de riesgos es: "*Amenazas originadas por circunstancias, que tienen la posibilidad de afectar de forma adversa la capacidad de la organización para cumplir sus objetivos y ejecutar sus estrategias*" (ISO 31000, 2018).

Las fuentes que originan los riesgos pueden ser internas o externas, se parte del concepto que no es posible estar exento de riesgos, más sí es posible, para ciertos tipos, evitarlos, reducirlos, eliminarlos y/o transferirlos. Los de fuente interna son aquellos relacionados con el ambiente de control: los procesos, las personas que participan o deciden sobre estos y los recursos, tanto físicos, tecnológicos y financieros. Son de fuente externa los relacionados al contexto y que son atribuibles al giro del negocio o a otros factores que se escapan de su control (factores económicos, ambientales, sociales, políticos y tecnológicos).

2.2.2. Clasificación de los riesgos

Según distintos profesionales, los riesgos pueden clasificarse en cuatro categorías: Riesgos Estratégicos, Operacionales, Financieros y de Cumplimiento (Sadgrove, 2005; Deloitte, 2013; Ernst & Young, 2011).

a) Riesgos estratégicos

Son riesgos que afectan o son creados por la estrategia comercial y los objetivos estratégicos de una organización (Deloitte, 2013). Incluyen entre otros los daños a la reputación de la empresa (por ejemplo, erosión de marca, fraude y publicidad desfavorable), competencia, deseos del cliente, tendencias demográficas y socioculturales, innovación tecnológica, disponibilidad de capital y tendencias normativas y políticas (Casualty Actuarial Society, 2003).

b) Riesgos operacionales

Afectan a los procesos, sistemas, personas y a la cadena de valor general de un negocio (Ernst & Young, 2011) y son los principales riesgos que influyen sobre la capacidad de una organización para ejecutar su plan estratégico. Comprenden operaciones comerciales (por ejemplo, recursos humanos, desarrollo de productos, capacidad, eficiencia, falla de productos/ servicios, gestión de canales, gestión de la cadena de suministro y ciclos comerciales), tecnología de la información, informes de negocios (por ejemplo, elaboración de presupuestos y planificación, información contable, fondo de pensiones, evaluación de inversiones e impuestos) (Casualty Actuarial Society, 2003).

c) Riesgos financieros

Surgen por la volatilidad en los mercados y de la economía real (Ernst &Young, 2011) e incluyen áreas tales como informes financieros, valoración, mercado, liquidez y riesgos crediticios (Deloitte, 2013). Los riesgos financieros surgen del efecto de las fuerzas del mercado sobre los activos o pasivos financieros e incluyen el riesgo de crédito, el riesgo de mercado y el riesgo de liquidez.

i. Riesgo de crédito

El riesgo de crédito se entiende como la posibilidad de pérdida, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte, entendida esta última como un prestatario o un emisor de deuda (Superintendencia del Sistema Financiero, 2011).

ii. Riesgo de mercado:

Es la posibilidad de pérdida, producto de movimientos en los precios de mercado que generan un deterioro de valor en las posiciones dentro y fuera del balance o en los resultados financieros de la entidad (Superintendencia del Sistema Financiero, 2011).

iii. Riesgo de liquidez

Es la posibilidad de incurrir en pérdidas por no disponer de los recursos suficientes para cumplir con las obligaciones asumidas, incurrir en costos excesivos y no poder desarrollar el negocio en las condiciones previstas (Superintendencia del Sistema Financiero, 2011).

iv. Riesgos de cumplimiento

Se relacionan con el cumplimiento legal y regulatorio (Deloitte, 2013) y se originan por situaciones de política, leyes, reglamentación o del gobierno corporativo (Ernst & Young, 2011).

2.2.3. Gestión del riesgo

El Comité de organizaciones de la Comisión Treadway (COSO, por sus siglas en inglés) define a la gestión de riesgos como " proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos" (COSO, 2004, pág. 2).

La función primordial de la gestión de riesgos es crear una estructura que posibilite que directivos y administradores incorporen sus decisiones cotidianas en aspectos relacionados al manejo de los riesgos. Cuando una institución tiene una cultura de riesgo, genera una ventaja competitiva; asume riesgos más conscientemente, se anticipa a los cambios adversos, se protege de eventos inesperados y logra una mejor administración o manejo de los mismos.

Por el contrario, una entidad que no tiene cultura de riesgos posiblemente no esté consciente de las pérdidas que incurre o de las ganancias que dejan de percibir, por no prestar la debida atención a los riesgos inherentes a sus actividades (Escobar León, 2011).

2.2.4. Etapas de gestión del riesgo

Las Normas para la Gestión Integral de Riesgos de Las Entidades Financieras NPB4-47 (2011), así como las sanas y buenas prácticas internacionales, reconocen para la gestión de riesgos un proceso integrado y documentado que contenga al menos las siguientes etapas:

a) Identificación

Es la etapa en la que se reconocen y se entienden los riesgos existentes en cada operación, producto, procesos y líneas de negocios que desarrolla la entidad y de aquéllos que se produzcan en las nuevas líneas de negocio.

b) Medición

Es la etapa en la que los riesgos deberán ser cuantificados con el objeto de determinar el cumplimiento o adecuación de las políticas, los límites fijados y medir el posible impacto económico en los resultados financieros de la entidad. Las metodologías y herramientas para medir el riesgo deben estar de conformidad con el tamaño, la naturaleza de sus operaciones y los niveles de riesgos asumidos por la entidad.

c) Control y mitigación

Es la etapa que busca asegurar que las políticas, límites y procedimientos establecidos para el tratamiento y mitigación de los riesgos son apropiadamente tomados y ejecutados.

d) Monitoreo y comunicación

Es la etapa que da seguimiento sistemático y permanente a las exposiciones de riesgo y de los resultados de las acciones adoptadas.

Estos sistemas deberán asegurar una revisión periódica y objetiva de las posiciones de riesgos y la generación de información suficiente, para apoyar los procesos de toma de decisiones.

2.2.5. Riesgo operacional

El riesgo operativo se define como el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal y los sistemas internos o bien de acontecimientos externos. Esta definición incluye el riesgo legal (jurídico), pero excluye el riesgo estratégico y el riesgo de reputación. (Basilea, 2003).

En los recientes años, la globalización de los servicios financieros, el desarrollo tecnológico relacionado, así como el crecimiento de los servicios bancarios por medio de internet, sugieren que las pérdidas por riesgos operacionales pueden generarse cada vez con mayor frecuencia e impacto.

El sector financiero enfrenta uno de los retos más importantes en cuanto a la identificación, medición y control del Riesgo Operativo, la adopción de modelos, la falta de información y de datos históricos respecto a las pérdidas originadas por personas, sistemas, factores externos, así como la aplicación incorrecta o mala interpretación de la regulación, vuelve aún más complejo e importante reconocer e incorporar este riesgo en el perfil del riesgo de toda institución financiera.

2.2.6. Factores de riesgo operacional

Los principales factores que constituyen el origen del riesgo operacional, y que por ende deben ser gestionados por toda entidad financiera, son los siguientes:

a) Procesos

Las entidades financieras, a fin de garantizar el uso eficiente de los recursos y procurar la estandarización de las actividades, la deben establecer procesos bien definidos, documentados y actualizados de forma permanente, tanto de nivel estratégico, de negocio y de soporte.

Deben gestionar apropiadamente los riesgos asociados a dichos procesos, con énfasis en las fallas o debilidades que presenten, dado que éstas pueden tener como consecuencia el desarrollo deficiente de las operaciones.

b) Personas

Siendo las personas la parte más importante en la gestión del riesgo operacional, las entidades deben establecer políticas, procesos y procedimientos que procuren una adecuada planificación del capital humano. Estableciendo mecanismos preventivos que permitan identificar y gestionar fallas, insuficiencias, negligencia, sabotaje, robo, inadecuada capacitación, apropiación indebida de información, entre otros, asociadas al personal, vinculado directa o indirectamente a la entidad.

c) Tecnología de información

Las entidades deben gestionar los riesgos asociados a la tecnología de información, entre otros, los relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como la calidad de la información y una adecuada inversión en tecnología.

d) Acontecimientos externos

Las entidades deben gestionar los riesgos asociados a acontecimientos externos ajenos al control de la entidad que pudiesen alterar el desarrollo normal de sus actividades, relacionados a fallas en los servicios críticos provistos por terceros, contingencias legales, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

2.3. Definición de continuidad de negocio

2.3.1. Continuidad de negocio

En un mundo tan globalizado, las organizaciones, en su objetivo de entregar sus productos y servicios a sus clientes, enfrentan un entorno complejo, con múltiples interdependencias y

conexiones con compañías que son tanto sus clientes como sus proveedores de bienes y servicios. En este entorno existen muchas amenazas que, al materializarse, podrían afectar no sólo la sostenibilidad y supervivencia de la organización que lo sufre, sino también a todo el entramado con el que se relaciona directa o indirectamente con ella.

Comprender la organización, sus interrelaciones y los impactos adversos que, a lo largo del tiempo, tendría una interrupción de la entrega de esos productos, y por ende de las actividades y recursos que los respaldan, se vuelve cada vez más importante y hace necesarios procesos que analicen de forma sistemática los impactos al negocio y se evalúen los riesgos de interrupción a lo largo y ancho de la entidad, ver figura 2.

Figura 2. Comprensión de la organización y sus interrelaciones

Los desastres han generado que las organizaciones sientan la necesidad no sólo de proteger y garantizar la tecnología, como siempre se ha hecho, sino también la continuidad del negocio, es decir, sus procesos y recursos que lo soportan, infraestructuras, equipos, localidades de trabajo, el personal y red de proveedores.

La norma ISO 22301, define la continuidad como la **capacidad** de una organización para continuar con la entrega de sus productos y servicios, en un tiempo y nivel aceptable, luego de un incidente disruptivo. En los últimos años la continuidad ha venido tomando mayor auge y esto se debe al aumento de eventos como los desastres naturales, las pandemias o atentados terroristas, entre otros, que tienen la potencialidad de afectar tanto a personas como el ámbito reputacional, operativo y económico. (ISO 22301, 2019).

2.3.2. Objetivos de la continuidad de negocio

Generalmente, cuando una entidad se enmarca en implementar un proyecto de continuidad de negocio busca cumplir los objetivos que se muestran a continuación:

a) Costo

- **Minimizar las pérdidas originadas por un incidente disruptivo.** Las entidades invierten con la intención de que, si ocurre algo, serán capaces de garantizar la entrega y prestación de productos.
- **Optimizar el rendimiento de la inversión.** Las entidades intentan ajustar el presupuesto al mínimo para garantizar la continuidad de sus funciones más críticas en desastres o contingencia.

b) Cobertura de riesgos

- **Cubrir los riesgos que se consideren de mayor impacto para la organización.** Bajo la concepción que la cobertura de todos los riesgos de una entidad es imposible y tendría unos costos inalcanzables, las entidades evalúan los riesgos que pueden tener un mayor impacto en la misma e intentan mitigarlos de la forma más económica y eficiente posible.
- **Asumir riesgos residuales con menor probabilidad e impacto.** Orientan sus inversiones para tratar de mitigar los riesgos de mayor probabilidad e impacto. Los de menor probabilidad e impacto son aceptados o transferidos a terceros.
- **Administración de actividades tercerizadas.** Deben considerar e incluir revisiones de la Continuidad de empresas que ofrecen servicios o productos tercerizados, principalmente cuando son críticos y de tecnología de la información.

- **Minimizar incumplimientos legales/regulatorios**. Las entidades están obligadas a implementar la continuidad de negocio para garantizar un adecuado nivel de servicio y cumplir con requisitos y disposiciones normativas.
- **Proteger la reputación y la confianza de la entidad.** Cuando se afronta uno o varios eventos de gran magnitud, aparte de afectaciones financieras y operacionales, puede tener impactos en la reputación y partes interesadas, frente a sus clientes, usuarios o al público en general.

c) Tiempo de recuperación de procesos críticos

- **Minimizar el tiempo de recuperación**. Las entidades buscan minimizar el tiempo de interrupción de los productos y servicios afectados por la materialización de un incidente disruptivo.
- **Proteger y recuperar las actividades más urgentes.** Las entidades buscan asegurar la continuidad de las funciones y actividades más urgentes. Preparar planes para todos los procesos y servicios de la entidad es costoso, por lo que es recomendable una priorización por niveles de criticidad.
- **Reducir la improvisación**. Implementar la continuidad de negocio permite definir las acciones que se deberían seguir para restaurar la operativa del negocio.

d) Cultura de continuidad de negocio

- **Fomentar una cultura en la entidad.** Involucrar a toda la entidad es uno de los retos y objetivos clave del éxito. Es necesario formar y concientizar a todo el personal para alcanzar los objetivos.
- **Tranquilizar**. La gestión de continuidad busca dar tranquilidad a la propia entidad. Es una ventaja el poder pensar que se está preparado frente a desastres y que se dispone de mecanismos para afrontar incidentes disruptivos que podrían poner en peligro la sostenibilidad de la entidad.

La figura 3 resume los objetivos que una entidad busca al implementar un plan de continuidad.

Figura 3. Objetivos al implementar la continuidad de negocio

2.3.3. Gestión de continuidad de negocio

La gestión de continuidad de negocio es un **proceso** de dirección holístico que identifica las amenazas potenciales contra una organización y los impactos en las operaciones del negocio si se presentaran esas amenazas, ofrece un marco de trabajo para construir la resiliencia organizacional con capacidad de dar una respuesta efectiva que permita proteger los intereses de sus grupos de interés clave, reputación, marca, y actividades que crean valor (BCI, 2013).

El Banco de España, considera que: « (…) la gestión de la continuidad de negocio debe formar parte de la gestión del riesgo operacional de una entidad. Como ocurre con la gestión de cualquier riesgo, es necesario un marco global que incluya políticas, estrategias y procedimientos que aseguren que determinadas operaciones – en especial, las de carácter más crítico – puedan mantenerse o recuperarse lo antes posible en caso de un desastre» (Banco de España, 2006. Pag. 2).

De lo anterior, es recomendable que la gestión de continuidad de negocio sea considerada y gestionada en función de los riesgos operacionales a fin de facilitar y complementar la definición de políticas y procedimientos necesarios para asegurar el funcionamiento aceptable de las operaciones de la entidad.

2.3.4. Gestión de riesgos, continuidad de negocio y resiliencia corporativa

La práctica de Gestión de Riesgos y Continuidad de Negocio son disciplinas complementarias que deben implementarse y mantenerse de forma coordinada, a fin de fortalecer la resiliencia de cualquier organización, para ello se deben establecer procesos periódicos para la valoración de riesgos que identifique, analice, evalúe y monitoree sistemáticamente el riesgo de interrupción de las actividades críticas y priorizadas de la organización, y de los procesos, sistemas, información, personas, activos, proveedores y otros recursos que les brindan soporte (ISO 22313, 2020).

Valorar los riesgos de interrupción de esta manera, permite a las organizaciones implementar un proceso estructurado que analiza los riesgos en términos de las consecuencias y probabilidad previo a determinar las medidas de mitigación o tratamiento que se pueden necesitar.

El alcance de esta valoración debe comprender las amenazas y vulnerabilidades de los recursos requeridos para los productos, servicios y actividades, y en particular aquellos que son necesarios para actividades con mayor prioridad o que tienen un tiempo significativo para su reemplazo.

La gestión de continuidad de negocio debe ser vista como una parte de la gestión integral de riesgos en una organización, debe ser reconocida como una práctica profesional y como parte de un buen gobierno corporativo. Se considera una actividad estratégica y no debe tomarse únicamente como algo operativo o un proyecto con un plazo de finalización definido.

Al comprender que la gestión de continuidad de negocio se enmarca en la gestión general de la organización, específicamente en la gestión integral de riesgos y que tiene áreas superpuestas con otras gestiones como el riesgo operacional, la seguridad de la información, las tecnologías de la información, la Ciberseguridad, ver Figura 4, se logra un incremento en la capacidad de recuperación de las actividades más críticas de una organización y a la vez, contribuye a un mejor desempeño corporativo.

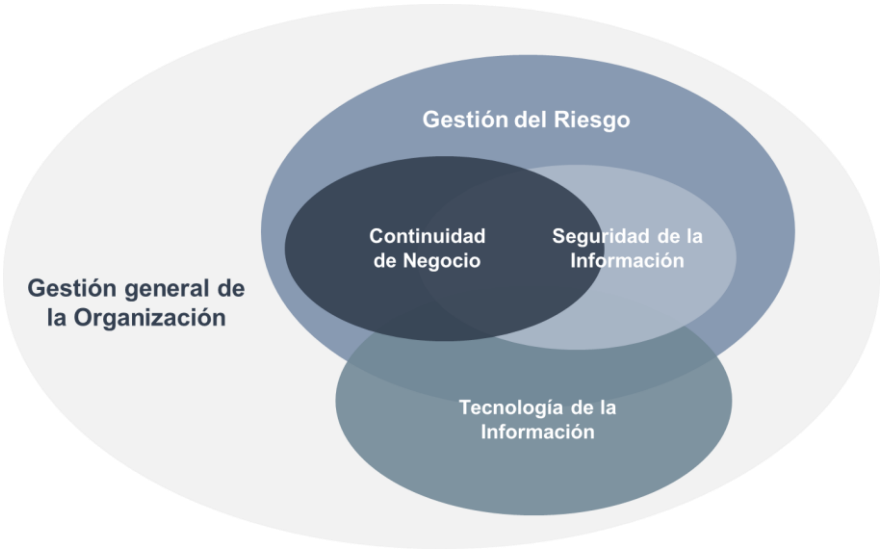


Figura 4. Continuidad de negocio en la gestión general de la organización

Si bien es cierto, que tanto la gestión de continuidad de negocio como la gestión de riesgos son disciplinas complementarias, los enfoques y métodos empleados en cada gestión son muy diferentes.

La Tabla 1 destaca las diferencias entre ambas gestiones.

	Gestión de riesgos	Gestión de continuidad de negocio
Método clave	Análisis de riesgo	Análisis de impacto sobre el negocio
Parámetros clave	Impacto y Probabilidad	Impacto y Tiempo
Tipo de incidente	Todo tipo de eventualidades	Eventos de alto impacto para el negocio
Magnitud del incidente	Toda magnitud (coste)	sólo los incidentes que afectan al negocio
Alcance	Objetivos del negocio	Incidentes en su mayor parte externos
Intensidad	Todas, desde graduales hasta súbitos	Eventos súbitos o de rápida evolución

Tabla 1. Comparación entre la gestión de riesgos y gestión de continuidad de negocio

Es conocido que la continuidad de negocio puede mejorar la resiliencia organizacional como parte del desarrollo normal de la actividad. Su aplicación exitosa incrementa la capacidad de recuperación de una organización y a la vez, contribuye a un mejor desempeño corporativo. La resiliencia se define ampliamente como la capacidad que tiene una organización para absorber, responder a y recuperarse de las alteraciones.

Proporciona el marco para entender cómo se crea y mantiene el valor dentro de una organización, y establece una relación directa con las dependencias y vulnerabilidades inherentes a la entrega de ese valor.

El objetivo del análisis de riesgo en continuidad es identificar nuevas opciones de prevención o mejorar las medidas ya existentes para cada uno de los eventos de riesgo considerados. El riesgo de continuidad se estima combinando probabilidad e impacto, abordando generalmente aquellos eventos de gran impacto y poca probabilidad de ocurrencia (ver Figura 5), pudiendo ser por métodos cualitativos o cuantitativos.

Figura 5. Abordaje de la continuidad de negocio en la gestión de riesgos

El problema de los métodos cuantitativos es que necesitan data histórica además de complejas formulas estadísticas de proyección de la ocurrencia de incidentes disruptivos. Y en muchos casos se confunde que el objetivo de la continuidad es proponer medidas preventivas y no necesariamente la estimación de la probabilidad y riesgo de manera exacta. Debido a esto, es preferible estimar el nivel de riesgo cualitativo.

2.3.5. Sistema de gestión de continuidad de negocio

Un Sistema de Gestión de Continuidad de Negocio (SGCN) ayuda a mantener los procesos empresariales críticos y mantener los efectos de los eventos adversos en la organización lo más bajos posible. Para ello, hay que tomar decisiones estratégicas, establecer estructuras organizativas y aplicar salvaguardias, es un elemento estratégico que no debe tomarse únicamente como un aspecto operativo.

Esto implica que un Sistema de Gestión de Continuidad de Negocio tenga como mínimo:

- Un marco de trabajo documentado que establezca la política, objetivos y alcance de SGCN y que identifique los resultados esperados en términos que se puedan medir. Este marco de trabajo también deberá definir personas con responsabilidades claras;
- Una revisión formal del desempeño de SGCN que compare los resultados acordados y la evaluación de factores internos y externos que puedan requerir cambios en el SGCN; y
- La implementación de los resultados de la revisión, incluidas las acciones correctivas para eliminar la no-conformidad y las medidas para mejorar la efectividad o eficiencia de SGCN.

Al igual que otros sistemas de gestión, el SGCN utiliza el ciclo Planear-Hacer-Verificar-Actuar (PDCA), la Tabla 2 muestra el modelo PDCA aplicado a los procesos de continuidad de negocio.

Planear (establecer)	Establecer la política de la Continuidad del Negocio al igual que los objetivos, metas, controles, procesos y procedimientos relevantes para mejorar la gestión, para brindar resultados acordes con las políticas y los objetivos generales de la organización.
Hacer (implementar y operar)	Implementar y operar la política de Continuidad del Negocio mediante controles, procesos y procedimientos.

Verificar (monitorear y revisar)	Monitorear y revisar el desempeño comparado con la política y objetivos de la Continuidad del Negocio, informe los resultados a la gerencia para su revisión, y determinar y autorice acciones para remediar y mejorar.
Actuar (mantener y mejorar)	Mantener y mejorar el SGCN tomando acciones correctivas con base en los resultados de la revisión de la Gerencia, y revalúar el ámbito de aplicación del SGCN como también la política y objetivos de la Continuidad de Negocio.

Tabla 2. Modelo PDCA aplicado a los procesos de continuidad de negocio

2.3.6. Plan de continuidad de negocio

La norma ISO 22301:2019, define al Plan de Continuidad de Negocio (PCN) como "Procedimientos documentados que orientan a las organizaciones para responder, recuperar, reanudar y restablecer hasta un nivel predeterminado las operaciones luego de una disrupción." Posee procesos documentados para que las entidades puedan reanudar su prestación de productos dentro del tiempo de recuperación definidos.

Estos planes de continuidad formalizan las estrategias en un documento que busca ser consultado y utilizado durante un evento de alto impacto, es decir en situaciones de mucha presión y estrés. Por lo tanto, debe diseñarse un documento focalizado, especifico y fácil de usar. Su alcance puede cubrir cualquiera o todas las fases de respuesta a un evento, desde la respuesta inicial hasta la reanudación de las operaciones normales. (SELA, 2013).

Tienen como objetivo principal asegurar que la entidad siga funcionando antes, a lo largo y después de experimentar un desastre. Busca que los procesos y servicios críticos que la entidad presta aún se lleve a cabo, tanto durante la interrupción como después.

Para ello la entidad debe tomar en cuenta las amenazas comunes para sus funciones esenciales, así como las vulnerabilidades asociadas que podrían afectar el normal funcionamiento en determinado momento. Proporciona una estrategia a largo plazo para asegurar que la operación continua con éxito, a pesar de los hechos y desastres inevitables (Eric Conrad, 2010).

Este plan establece medidas para evitar que las entidades se queden sin disponibilidad de sus servicios ante un evento disruptivo, es decir ante los diversos escenarios de pérdida total o parcial de uno o más factores necesarios para la prestación de los procesos críticos. La figura 6 ilustra algunos ejemplos de situaciones que pueden afectar los procesos críticos de una institución.

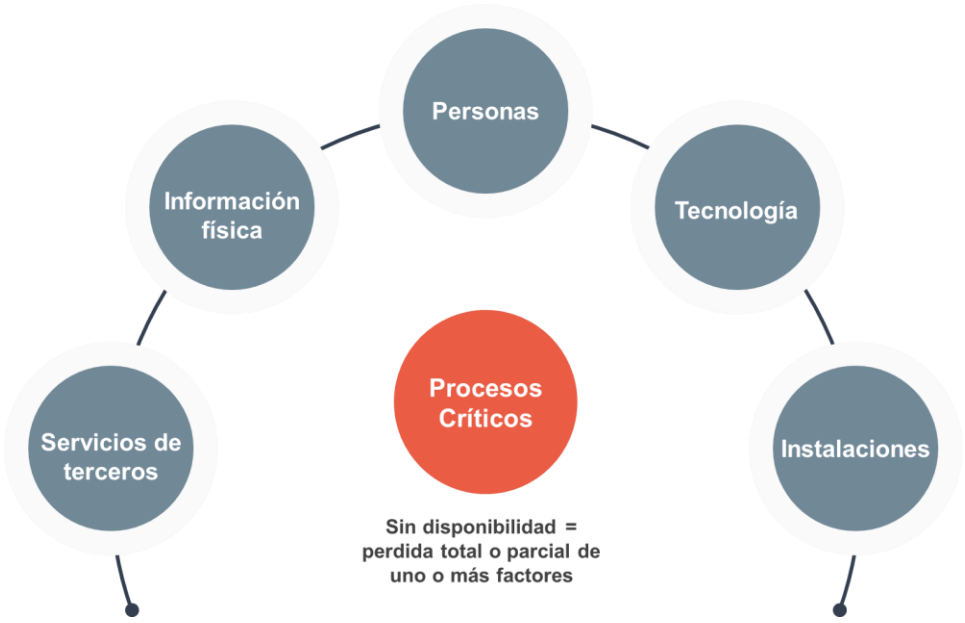


Figura 6. Escenarios que afectan los procesos críticos

Según la norma británica para la gestión de continuidad de negocio (BSI Group, BS 25999-1, 2006), el Plan de Continuidad de Negocio debería contener:

1. **Generalidades**.

   a) **Propósito y alcance.** Debe estar definido, acordado por la Alta Dirección y entendido por los que pondrán el plan en ejecución.

Asimismo, debe referenciarse toda relación que se tenga con otros planes o documentos orientados a la continuidad de las operaciones. Cada plan debe establecer:

- Los Productos y Servicios críticos que deben recuperarse,
- Los plazos o tiempos en que deben recuperarse,
- Los niveles de recuperación necesarios para cada producto y servicio, y
- Las situaciones en que debe utilizarse el plan.

b) **Funciones y responsabilidades.** Deben estar claramente documentadas las funciones y responsabilidades del personal y equipos que tengan autoridad (tanto a nivel de toma de decisiones y de gastos emergentes) y que ejecutan actividades durante y después de un incidente.

c) **Propietario y responsable del mantenimiento del plan.** Debe estar documentado quién es el responsable de la revisión, modificación y actualización del plan a intervalos regulares.

d) **Información de contacto.** El plan debe contener o proporcionar una referencia a los datos de contacto esenciales correspondientes a todos los grupos de interés fundamentales.

2. Planes de acción / lista de tareas

a) La activación del plan, documentando directrices claras y criterios referentes a qué personas tienen la autoridad necesaria para activar y desactivar el plan y bajo qué circunstancias.

b) Procedimientos claros que cada persona debe adoptar al tomar la decisión de activar el plan.

c) Cómo se deben tomar las decisiones.

d) Directrices claras sobre quién va adónde, y cuándo.

e) Procedimientos de recuperación de las actividades

f) Qué servicios están disponibles, dónde, y cuando; movilización de recursos.

g) Informar estatus a instancias correspondientes.

3. **Requisitos de recursos**

   Deben identificarse los recursos necesarios para la continuidad y recuperación, pudiendo incluir:

   a) Personal, instalaciones y necesidades de espacios de trabajo.

   b) Tecnología, comunicaciones y datos.

   c) Seguridad, transporte y logística.

   d) Necesidades básicas y suministros

Evolución del plan de continuidad de negocio

El Plan de Continuidad de Negocio ha ido evolucionando en el tiempo haciéndose más preciso en definir algunos ámbitos sobre los cuales se implementa. Al inicio, el termino de continuidad estaba muy asociado a acciones específicas de contingencia informática. Luego se identificó que uno de los escenarios de mayor impacto es la caída de un Centro de Datos completo, entonces se fue cambiando el concepto de ser específico a escenarios o contingencias puntuales. Acá se comenzó a hablar de "Plan de Recuperación ante Desastres". Posteriormente este abarcaba la posibilidad de que no solo el Centro de Datos se caiga, sino también las operaciones del negocio por otras razones como: afectación de instalaciones, proveedores críticos, ausencia de personal clave, entre otros. En este punto se comienza a usar el término "Continuidad del Negocio".

Es así que el objetivo inicial que era formular el documento, es decir "el plan", pasó a ser un proceso permanente, cuyos objetivos, entregables y resultados debían ser actualizados constantemente y es acá donde se comienza a hablar de "Programa de Continuidad de Negocio" como un conjunto de planes y luego un conjunto de fases. Finalmente, este programa que requiere ser gestionado de acuerdo a un sistema de mejora continua, se convierte en un "Sistema de Gestión de Continuidad del Negocio", esta evolución se presenta en la figura 7.

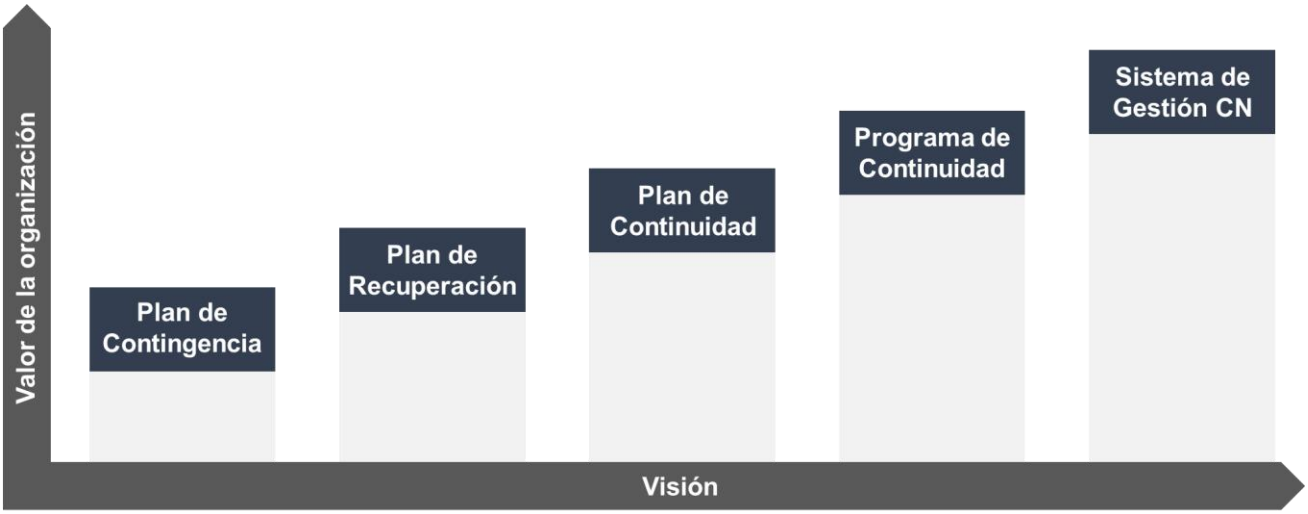


Figura 7. Evolución del plan de continuidad de negocio

En la actualidad, la Gestión de Continuidad de Negocio es un proceso holístico, que no solo "identifica amenazas potenciales para la organización y el impacto que su materialización podría ocasionar en las operaciones corporativas, sino que también proporciona un marco para crear **resistencia corporativa** de modo que pueda dar una **respuesta eficaz**, que **proteja los intereses de sus grupos de interés**, **reputación**, **marcas** y **actividades de creación de valor** fundamentales.

En sus inicios el Plan de Continuidad de Negocio era un documento de gran tamaño que contenía información diversa y estaba enfocado en la respuesta, pero también en las causas de por qué esa respuesta era importante. Con lo cual el plan contenía las principales amenazas y riesgos que enfrentaba la organización y las prioridades de recuperación. También definía las estrategias de recuperación, los roles necesarios para esas respuestas, los protocolos de actuación y las responsabilidades de mantenimiento, capacitación y pruebas del plan. El objetivo principal era compendiar toda esta información en un solo documento.

Hoy en día, el plan ha cambiado el sentido y está enfocado principalmente a responder al incidente, es decir, ya no está orientado a tener volúmenes de información, más bien a que su contenido sea muy ligero, fácil de recordar y trasladar.

El plan de continuidad de negocio actual hace énfasis en los **protocolos de respuesta por rol**. Se podría tener incluso pequeños planes de continuidad o secciones por cada rol, aunque el plan como concepto más amplio sería el conjunto o compilación de todos estos pequeños planes. Sin embargo, de cara al que va a responder, solo le corresponde conocer y administrar su propio plan para afrontar algún incidente particular.

Las demás informaciones y elementos que ya no se documentan en el Plan de Continuidad de Negocio tales como el Análisis de Impacto al Negocio (BIA por sus siglas en ingles), la Evaluación de Amenazas y Riesgos, las Estrategias de Recuperación y Continuidad, son documentos independientes que pueden consultarse pero ya forman parte del Programa o Sistema de Gestión, más no del Plan de Continuidad del Negocio, ver figura 8.

Lo mismo en el caso del mantenimiento o ejercicios y pruebas que no se circunscriben al plan si no a todas las demás actividades del programa a fin de crear conciencia, mantener el estado de alerta y las capacidades activas a nivel de estrategias, así como de ejercitar y validar los protocolos o los planes correspondientes.

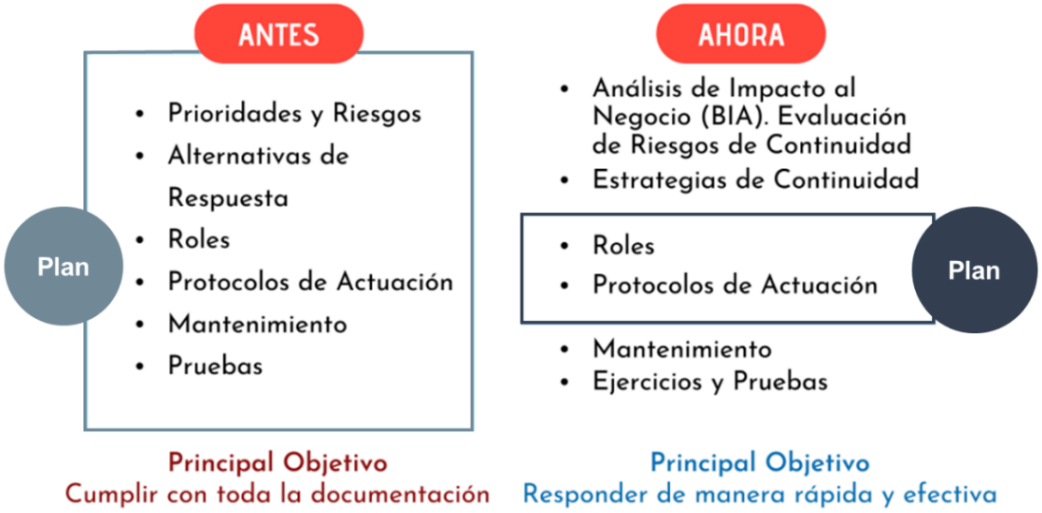


Figura 8. Enfoque del plan de continuidad de negocio en la actualidad

2.3.7. El plan de continuidad de negocio y la gestión de incidentes

Un sólido proceso de gestión de riesgos anticipa y evalúa los riesgos para la entidad, estableciendo medidas preventivas para su mitigación. Asimismo, las entidades deben estar preparadas para responder y recuperarse de una interrupción del negocio, independientemente de su causa.

Hay varias fases en una respuesta que se resumen en la figura 9, donde se presenta las principales que existen durante la materialización de un incidente disruptivo, muestra además la relación entre las disciplinas de Continuidad de Negocio, Manejo de Emergencia y Gestión de Incidentes.

Figura 9. Cronograma de un incidente disruptivo

Respuesta de emergencia: se ocupa de los impactos inmediatos de un incidente, una fase relativamente a corto plazo que se centra en garantizar que las personas y el medio ambiente sean seguros.

Gestión de incidentes: describe cómo la organización gestionará las consecuencias de la interrupción del negocio. Cubre quién está a cargo, cómo mantener informadas a las partes interesadas, los procesos de escalamiento, la coordinación de recursos, etc.

Gestión de crisis: se ocupa de la gestión de acciones estratégicas y complejas, donde se requiere la integración con otras disciplinas.

Continuidad del negocio: describe las acciones definidas para mantener las actividades comerciales críticas/urgentes a un nivel predeterminado, es decir, lo que se hará. La fase de análisis establece el objetivo de tiempo de recuperación, la interrupción máxima aceptable y el objetivo mínimo de continuidad del negocio (es decir, el nivel de servicio) para cada actividad crítica.

Recuperación: es de mayor duración e implica una mayor participación de las partes interesadas. Detalla las prioridades para la recuperación, es decir, qué, cómo y en qué orden se producirá la recuperación a la nueva normalidad después de una interrupción.

2.3.8. Tiempos críticos de recuperación en continuidad de negocio

El análisis del impacto de las interrupciones permite definir prioridades y requisitos de continuidad de negocio, esto incluye la definición de criterios de evaluación del impacto y los plazos que hay que tener en cuenta. El tiempo que un impacto tarda en volverse inaceptable puede oscilar entre unos segundos o varios meses. Esto dependerá de la sensibilidad al paso del tiempo de los productos y servicios de la entidad.

La interrupción de las actividades afecta directamente a la entrega de productos y servicios. Por ejemplo, la pérdida de la capacidad de pagar a los proveedores puede dañar la reputación de la organización y dar lugar a que estos se nieguen a suministrar bienes. A menudo existen variaciones estacionales y mayores niveles de actividad asociados con plazos semanales, mensuales o anuales o con las fechas de entrega de los proyectos. Tener en cuenta estas consecuencias y dar por hecho que las disrupciones se producen en el peor momento posible, garantiza que se evalúen los máximos impactos posibles y sus plazos.

Es importante determinar los umbrales temporales de impacto que son inaceptables para la organización:

Plazo máximo tolerable de disrupción (MTPD, por sus siglas en inglés): Es el tiempo que se tardaría en que los impactos se vuelvan inaceptables, también se le conoce como “periodo máximo tolerable” o “tiempo de inactividad máximo aceptable”.

Objetivo mínimo de continuidad del negocio (MBCO, por sus siglas en inglés): Es el nivel mínimo de productos o servicios que es aceptable para la organización. Es un nivel reducido de los productos o servicios que la organización ofrece, ya que considera como premisa que ante un incidente de alto impacto, se deben enfocar esfuerzos y priorizar recursos a las funciones más relevantes de la institución.

Tiempo objetivo de recuperación (RTO, por sus siglas en inglés): Plazo para reanudar una actividad, por definición este parámetro de tiempo, deber menor que el Máximo tiempo permitido de interrupción.

Punto de recuperación objetivo (RPO, por sus siglas en inglés): Punto hasta el cual se podrán restaurar la información y los datos que se usan en una actividad de tal forma que esta última opere al reanudarla.

En la figura 10, se presenta la relación de estos tiempos en la línea temporal de un incidente disruptivo.

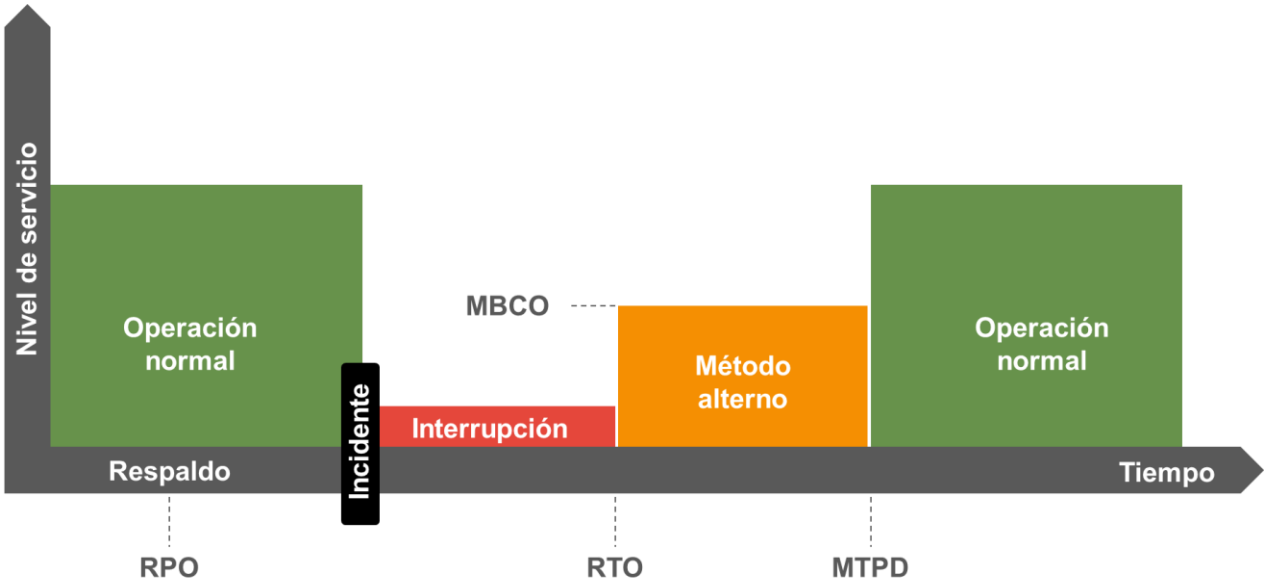


Figura 10. Los tiempos críticos en la continuidad de negocio

2.3.9. Fases del ciclo de vida de continuidad de negocio

Según la **Guía de Buenas Prácticas** (GPG, 2013) del BCI, el ciclo de vida de la Gestión de Continuidad del Negocio se compone por 6 fases, las cuales se presentan en la Figura 11.

Figura 11.fases de la continuidad de negocio

a) Política y Gestión del Programa. Establece la política institucional en relación a la Continuidad de Negocio. Define cómo se implementa la política a través de un ciclo continuo de actividades.

b) Incorporación. En esta etapa se busca constantemente integrar, por medio de la sensibilización y capacitación, la continuidad del negocio en las actividades cotidianas y en la cultura organizacional.

c) Análisis. En esta etapa se identifica cuáles los procesos y servicios críticos de la entidad, los recursos clave que soportan estos procesos y los riesgos o amenazas a las cuales la institución está expuesta.

d) Diseño. Se identifican y seleccionan soluciones para lograr la continuidad de las operaciones ante un evento mayor. Estas soluciones deben satisfacer los requisitos identificados en la etapa de análisis.

e) **Implementación:** Se implementan las soluciones establecidas en la etapa de diseño. Esta implementación se logra a través de "planes de continuidad" que cumplan con los requerimientos y soluciones previamente identificados y definidos en las etapas de análisis y diseño.

f) **Validación.** Se asegura que las estrategias de continuidad respondan al tamaño, complejidad y tipo de entidad, y que los planes sean precisos, efectivos, probados y actualizados oportunamente. Debe crearse un proceso continuo de mejora del programa.

2.4. Marco de referencia

2.4.1. Marco nacional normativo relacionado a la continuidad de negocio

a) Normas gestión del riesgo operacional en las entidades financieras NPB4-50

Es una norma emitida por la Superintendencia del Sistema Financiero que abarca principalmente aspectos de Riesgo Operacional, incluyendo disposiciones para la Continuidad de Negocio. El objeto de estas normas es proporcionar lineamientos mínimos para una adecuada gestión del riesgo operacional y criterios para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías para la gestión del riesgo, acordes con la naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones.

En materia de Continuidad de Negocio, en el art. 16 establece que las entidades deben implementar un sistema de gestión de continuidad del negocio en caso de interrupciones que incluya planes de contingencia, análisis de impacto en el negocio, plan de recuperación de desastres y planes de gestión del incidente, que aseguren la operatividad normal del negocio ante la ocurrencia de eventos adversos.

b) Normas técnicas para el sistema de gestión de continuidad de negocio NRP-24

Es una norma emitida por el Banco Central de Reserva de El Salvador, que regula específicamente aspectos de Continuidad de Negocio, su objeto es establecer disposiciones mínimas que deben considerar las entidades para establecer un Sistema de Gestión de la

Continuidad del Negocio y criterios para la adopción de políticas, planes, metodologías y procedimientos acordes a las mejores prácticas internacionales, el tamaño, naturaleza de sus operaciones, segmentación de negocios y la complejidad organizacional de cada entidad y, de esta forma, fortalecer su gestión de riesgos operacionales.

Las disposiciones establecidas en estas normas son de estricto cumplimiento de las entidades financieras para garantizar la efectividad de su respuesta frente a eventos de alto impacto que puedan afectar la prestación de sus productos y servicios críticos. La estructura de la norma es la siguiente:

Capítulo I – Objeto, sujetos y términos

En estos apartados se define el objeto de las Normas, los sujetos obligados al cumplimiento de las disposiciones establecidas en estas y se explica los conceptos clave que se deben tener presentes en materia de continuidad de negocio.

Capítulo II – Roles y responsabilidades

En esta sección se definen responsabilidades para la Junta Directiva, Comité de Riesgos, Alta Gerencia y el personal de la entidad, en cuanto a la gestión permanente de la continuidad de negocio. Establece que se debe contar con una estructura organizacional o funcional que delimite claramente las funciones, roles y responsabilidades que deben impulsarse en las entidades financieras.

Capítulo III – Sistema de gestión de continuidad de negocio

Esta sección detalla los elementos mínimos que se deben desarrollar para implementar un Sistema de Gestión de Continuidad de Negocio, entre otros aspectos menciona la Política, el Análisis de Impacto al Negocio, el Análisis de Amenazas de Continuidad de Negocio, diseño y selección de Estrategias y realización de Pruebas de Continuidad de Negocio. Establece lineamientos para el mantenimiento del sistema de gestión.

Capítulo IV – Información y control

Esta sección establece disposiciones para enmarcar la tercerización de servicios críticos desde la gestión de riesgos operacionales. Define los requisitos a solicitar a los proveedores de servicios para demostrar que cuentan con una gestión de continuidad de negocio implementada. Asimismo, define aspectos de actuación ante cambios significativos de la entidad que puedan afectar la continuidad del negocio. Se definen responsabilidades para la Superintendencia del Sistema Financiero para remitir detalles técnicos sobre el envío de la información a requerir a las entidades y establece que las unidades de Auditoría Interna deben considerar en sus planes de trabajo la evaluación del cumplimiento de las disposiciones de la norma.

Capítulo V – Otras disposiciones y vigencia

Esta sección define disposiciones a aplicar en caso de incumplimientos a lo regulado en la norma y aspectos sobre tramites en proceso, como procedimientos y recursos administrativos. Además, se define que las entidades deben presentar a la Superintendencia del Sistema Financiero un Plan de Adecuación, dentro de los 180 días siguientes a la vigencia de la norma, una vez presentado el Plan, las entidades dispondrán para su implementación, un plazo máximo de 24 meses contados a partir de su presentación. Finalmente, define que los aspectos no previstos en la norma serán resueltos por el Banco Central de Reserva por medio del Comité de Normas y se establece la entrada en vigencia a partir del 1 de julio del 2020.

En la figura 12, se presenta los plazos que las entidades disponen para implementar la gestión de continuidad de negocio.

Figura 12. Plazos para la implementación de la gestión de continuidad de negocio

2.4.2. Metodologías y estándares para gestionar la continuidad de negocio

A nivel internacional, existen estándares que sugieren, entre otras actividades de buenas prácticas, amplias guías en materia de Continuidad de Negocio, describiendo métodos, técnicas y enfoques diversos y utilizados en todo el mundo para el desarrollo, implementación y mantenimiento de un sistema eficiente en gestión de Continuidad de Negocio.

a) DRII (Disaster Recovery Institute International)

El DRII, fundado en 1988 en Los Estados Unidos de América, provee mejores prácticas, educación y certificación de profesionales en continuidad del negocio. En la versión a mayo 2013, considera:

- Inicio y administración del programa
- Evaluación y control de riesgos
- Análisis de impacto al negocio
- Estrategias de continuidad del negocio
- Respuesta y operaciones de emergencia
- Planes de continuidad del negocio
- Programas de creación de conciencia y entrenamiento
- Ejercicios, auditoría y mantenimiento del plan de continuidad del negocio
- Comunicación en crisis
- Coordinación con agencias públicas externas

b) BCI (Business Continuity Institute)

El BCI fue fundado en 1994 en Inglaterra, provee mejores prácticas, educación y certificación de profesionales en continuidad del negocio. Su guía de buenas prácticas, versión mayo 2018, se organiza en:

- PP1: Política y Administración del Programa
- PP2: Incorporando la Continuidad del Negocio (cultura)

- PP3: Análisis
  - Análisis de Impacto al Negocio y Análisis de Amenazas
- PP4: Diseño
  - Estrategias y Tácticas de Continuidad y Recuperación
  - Medidas de Mitigación de Amenazas
  - Estructura de Respuesta a Incidentes
- PP5: Implementación
  - El Plan de Continuidad del Negocio
- PP6: Validación
  - Desarrollo de un Programa de Ejercicios, Mantenimiento y Revisión

c) ANSI/ASIS SPC.1

ASIS Internacional fue fundado en 1955, cuenta con más de 230 capítulos a nivel mundial y está integrado por profesionales de la seguridad con roles relacionados a la protección de activos - gente, propiedades y/o información. En el año 2009 publicó el estándar SPC.1 reconocido por ANSI para certificar organizaciones en continuidad del negocio. Un resumen de las secciones y partes más importantes del estándar es:

- Sección 1: Alcance del estándar
- Sección 2: Referencias de la normativa
- Sección 3: Términos y Definiciones
- Sección 4: Requerimientos para la Resiliencia Organizacional o Gestión del Sistema
  - Planeamiento (Evaluación de Riesgos, Análisis de Impacto, Implementación y Operación)
  - Recursos, roles, responsabilidades y autoridades
  - Competencia, entrenamiento y conciencia
  - Documentación y control
  - Prevención, preparación y respuesta a incidentes
  - Evaluación, medición y monitoreo
  - Ejercicios y pruebas

- No conformidades, y acciones correctivas y preventivas, control de registros
- Auditorías Internas, insumos y salidas de la revisión, mantenimiento y mejora continua

d) NFPA 1600 (Standard on Continuity, Emergency, and Crisis Management)

La Norma NFPA fue fundado en 1896 y tiene como principal objetivo la prevención de incendios y otros riesgos que afecten la seguridad y calidad de vida. Ha desarrollado, publicado y distribuido más de 300 códigos consensuados y estándares. Desde el año 1995 se han publicado 6 ediciones de su estándar 1600 siendo la última la revisión del año 2013. El nombre del estándar es: Estándar en Gestión de Desastres / Emergencias y Programas de Continuidad del Negocio.

Un resumen de las secciones y partes más importantes del estándar es:

- Capítulo 1: Administración (alcance, propósito y aplicación)
- Capítulo 2: Publicaciones de referencia
- Capítulo 3: Definiciones
- Capítulo 4: Gestión del Programa
- Capítulo 5: Planeamiento
- Capítulo 6: Implementación
- Capítulo 7: Entrenamiento y Educación
- Capítulo 8: Ejercicios y pruebas
- Capítulo 9: Mejora y Mantenimiento del programa

e) ISO 223O1 (Business continuity management systems – Requirements)

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización. El trabajo de preparación de las normas internacionales normalmente se realiza a través de los comités técnicos de ISO. En mayo del año 2012 se publicó la normativa ISO 22301 - Seguridad de la Sociedad - Sistemas de gestión de continuidad del negocio.

Un resumen de las secciones del estándar es:

0. Introducción
1. Alcance
2. Referencia a Normativas, Términos y Definiciones
3. Contexto de la Organización
   - Partes interesadas
   - Alcance de la continuidad del negocio
4. Liderazgo
   - Compromiso de la Alta Gerencia
   - Política de Continuidad del Negocio
   - Roles y responsabilidades en la Continuidad del Negocio
5. Planeamiento
   - Objetivos de la continuidad del negocio y planes para alcanzarlos
6. Soporte
   - Recursos, Competencias, creación de conciencia, comunicación y documentación
7. Operación
   - Planeamiento y control operacional
   - Análisis de Impacto al Negocio (BIA) y Evaluación de Riesgos
   - Estrategia de Continuidad del Negocio
   - Establecer e Implementar Procedimientos en Continuidad del Negocio
   - Ejercicios y pruebas
8. Evaluación de Desempeño
   - Monitoreo, medición, análisis y evaluación
   - Auditoría Interna y Revisión de la Gerencia
9. Mejora continua
   - No conformidades, y
   - Acciones correctivas, mejora continua

2.5. Análisis financiero – costo de inactividad

Muchas instituciones deciden no invertir en Planes de Continuidad de Negocio o Recuperación ante desastres, sin darse cuenta de que varias horas de inactividad pueden costarles miles o cientos de miles de dólares. La estrategia y el presupuesto de recuperación ante desastres de cada entidad deben basarse en sus requisitos únicos, no en un plan convencional. La mejor manera de abordar el gasto en los esfuerzos de recuperación de desastres es comprender primero sus requisitos de cumplimiento, si los tiene, y luego calcular el costo del tiempo de inactividad por hora. Una vez que tenga una idea de cuál es ese número, comprenderá mejor el Retorno sobre la Inversión (ROI) en los diferentes enfoques de la recuperación ante desastres y podrá definir sus objetivos de disponibilidad del servicio.

Según un estudio de 2016 realizado por Cloud Endure, un proveedor de soluciones de recuperación ante desastres, reveló resultados claves sobre los desafíos de recuperación ante desastres y las mejores prácticas (Cloud Endure, 2016), entre estos resultados se incluyen:

- El riesgo número uno para la disponibilidad de servicios son los errores humanos.
- El 77% de las empresas tienen un objetivo de disponibilidad del servicio de al menos el 99,9%, lo que significa no más de nueve horas de inactividad por año, pero el 57% tuvo una o más interrupciones en los últimos 3 meses.
- El costo del tiempo de inactividad para el 73% de las organizaciones es de $ 10,000 por día o más.

Los costos asociados al tiempo de inactividad, durante la materialización de un incidente disruptivo, pueden llegar a tener un alto impacto económico para las empresas pequeñas, aparte del daño reputacional con los clientes, proveedores y socios. Según la consultora IDC y Carbonite, una empresa que ofrece servicios de respaldo en línea, el 80% de las empresas han experimentado tiempo de inactividad en algún momento en el pasado, con costos de tiempo de inactividad por hora que oscilan entre un promedio de $8,220/hora a $25,600/hora, por un solo evento (IDC / Carbonite, 2015). Esto significa, que el tiempo de inactividad podría costar a las empresas entre $137 a $427 por minuto, con un promedio de $282 por minuto.

Un evento de tiempo de inactividad no planificado típico abarca horas, a menudo hasta 24 horas. Sin embargo, suponiendo un evento de tiempo de inactividad más conservador de 10 horas, le podría llegar a costar a una empresa un promedio de $ 82,200 a $ 256,000. Estos costos pueden comprometer fácilmente la sostenibilidad de cualquier empresa y, por supuesto, se convierten en una preocupación económica.

En una investigación realizada a 63 Centros de Datos por Ponemon Institute, quien se dedica a la investigación y la educación independientes, estableció que el costo promedio del tiempo de inactividad de un Centro de Datos por minuto es de $ 8,851 por incidente (Ponemon Institute 2016).

Con esta información, puede estimarse los costos de tiempo de inactividad según los objetivos de disponibilidad que se tracen como meta, ver Tabla 3.

Objetivo de disponibilidad	Horas de inactividad por año	Días	Costo por hora - empresa pequeña* ($282x60)	**Riesgo de tiempo de inactividad anual total**	Costo por hora de inactividad de Centro de Datos** ($8,851x60)	**Riesgo de tiempo de inactividad anual total**
98%	174.74	7	16,920 $	**2,956,601 $**	531,060 $	**92,797,424 $**
99%	87.36	4	16,920 $	**1,478,131 $**	531,060 $	**46,393,402 $**
99.50%	43.68	2	16,920 $	**739,066 $**	531,060 $	**23,196,701 $**
99.90%	8.736	0.4	16,920 $	**147,813 $**	531,060 $	**4,639,340 $**

Tabla 3. Disponibilidad de servicios y costos de inactividad

* Basado en el costo promedio de tiempo de inactividad por minuto para pequeñas empresas de IDC/Carbonite ($ 282 / min).

** Basado en el costo promedio de tiempo de inactividad del centro de datos de Ponemon Institute 2016 ($ 8,851 / min)

Con estos resultados, se considera de vital importancia que, para definir las Estrategias de Continuidad y Recuperación, las entidades determinen su costo aproximado de tiempo de inactividad por hora, el cual podría incluir pérdida de ingresos por ventas y / o pérdida de productividad.

Miguel Palacios, Líder de Oracle Users Group, propone un método práctico para iniciar con el proceso de cuantificación del impacto financiero que se genera cuando ocurre una interrupción en las operaciones de una organización, donde en primer lugar se debe hacer una clasificación entre los impactos tangibles e intangibles (PALACIOS, 2009).

Tangibles:

- Reducción de la productividad
- Pérdida en la producción
- Pérdida de ventas y de clientes
- Frustración de los empleados
- Descontento de partes interesadas
- Penalidades de los organismos reguladores

Intangibles:

- Impacto negativo en la reputación
- Pérdida de oportunidades
- Moral de los empleados
- Insatisfacción de clientes
- Impacto en el valor de las acciones

Por lo general, en un incidente disruptivo que genera tiempos de inactividad, el impacto siempre será mayor al que inicialmente es asumido, en la figura 13 se muestra un mapa mental de los costos asociados al tiempo de inactividad.

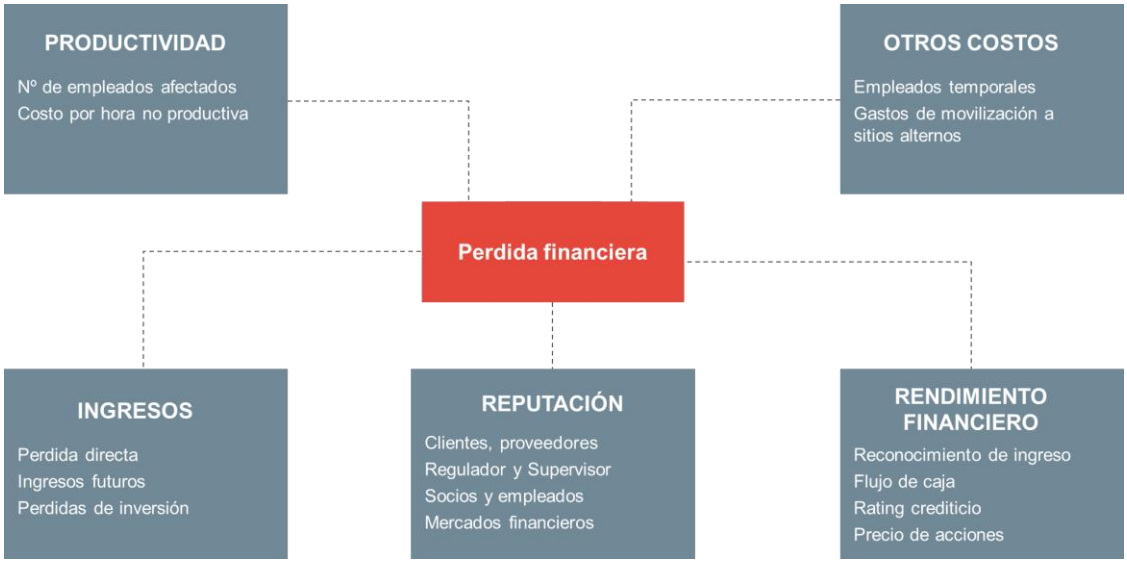


Figura 13. Costos asociados por tiempos de inactividad

La propuesta de Oracle para la elaboración del Análisis Financiero y cálculo del costo de tiempo de inactividad se presenta a continuación:

Costo de pérdida de productividad (P)

$$(\mathbf{P}) = \frac{(\mathbf{A} * \mathbf{B} * \mathbf{C})}{(\mathbf{D} * \mathbf{E} * \mathbf{F})}$$

Donde:

A = Costo anual de empleados.

B = Número de horas de Inactividad.

C = Número de empleados afectados.

D = Número de empleados.

E = Promedio de días trabajados por año.

F = Promedio de horas trabajadas por persona por día.

Ejemplo:

(P) = ($1.2M x 44 x 25) / (100 x 264 x 8) = $6547

La Fórmula anterior es una herramienta que puede apoyar a identificar el costo que genera para la empresa el que la operación normal se descontinúe. Este tema es de gran importancia para las organizaciones y que muy pocas veces se estudia, debido a que se considera poco probable que ocurra.

Valor de pérdida por ventas (S)

$$(\mathbf{S}) = \frac{(\mathbf{G} * \mathbf{H})}{(\mathbf{I})}$$

Donde:

G = Ingreso por ventas anuales.

H = Número estimado de pérdidas de ventas por año.

I = Número total de ventas por año.

Ejemplo:

(S) = ($5M x 500) / (10,000) = $250,000

En la primera fórmula se analizó el costo por horas de trabajo pérdidas. En esta segunda fórmula se analiza la pérdida por ventas, que también es importante tomar en cuenta para el análisis financiero.

Costo de recuperación de servicio (R)

$$(\mathbf{R}) = (\mathbf{J} * \mathbf{K})$$

Donde:

J = Trabajo de horas de soporte de TI

K= Costo hora de personal de soporte

Ejemplo:

(R) = (88 x 50) = $4,400

Costo Estimado de inactividad (T)

(T) = (P + S + R)

(T) = ($6547 + $250,000 + $4,400) = $260,947

El número resultante indica la pérdida financiera por materializarse el incidente disruptivo analizado. Tomando en cuenta el resultado, la entidad determina si el impacto es tan alto como para implementar medidas preventivas y/o de recuperación para evitarlo o afrontarlo e integrarlo así a la Gestión de Continuidad de Negocio.

Se considera importante elaborar un estimado de lo que costará la recuperación de los productos y servicios relevantes para la entidad, así como la operación misma. Esto, con la finalidad de identificar la viabilidad y/o conveniencia de implementar Estrategias de Continuidad y Recuperación para las operaciones analizadas.

Esta estrategia tratará de optimizar la relación entre los costes de implantación de la medida adoptada con las potenciales pérdidas económicas y otros impactos originados por el incidente disruptivo en la organización. La figura 14 pone de manifiesto la necesidad de la entidad de definir la ventana de interrupción que la organización considerará admisible ante una situación de contingencia.

Se debe tener en cuenta que cuanto menor sea la ventana de interrupción y más cercana se encuentre al inicio de la interrupción, más elevados serán los costes para la organización (se necesita más personal, mucha más redundancia en los sistemas de información y la infraestructura, comunicaciones en alta disponibilidad, etc.).

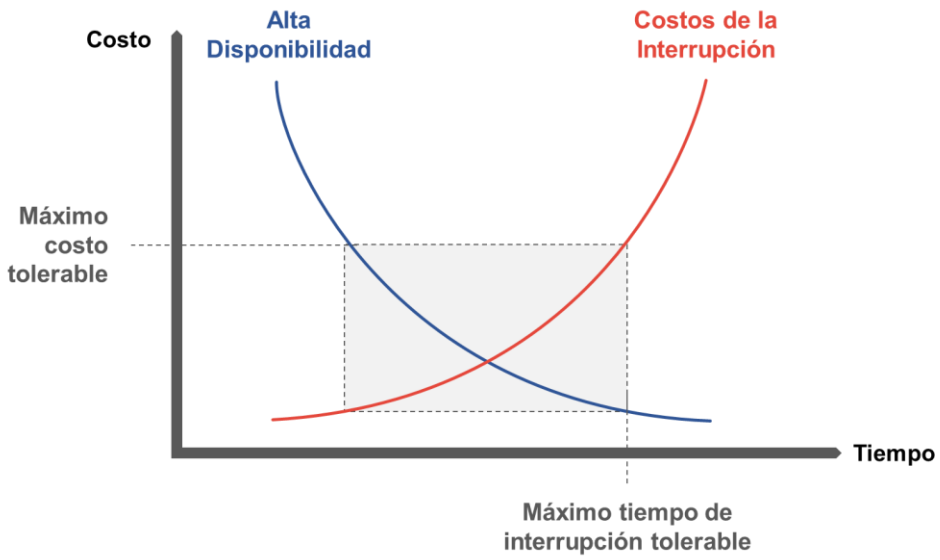


Figura 14. Ventana de coste-tiempo

2.6. Continuidad de negocio y pandemia COVID-19

Muchos profesionales en la implementación de sistemas de gestión de continuidad fueron sorprendidos a raíz de la pandemia de COVID-19. No necesariamente por el evento en sí mismo, sino por la complejidad de su atención tanto en tiempo como en afectación en ciertos pilares que conforman el plan de continuidad.

La pandemia de COVID-19 se convirtió en un evento sin precedentes, de tal forma que cambió la estructura de la convivencia y organización de la sociedad a nivel mundial. Según los informes **Horizon Scan Report** del Business Continuity Institute (BCI) de los últimos cuatro años, la posibilidad de presentarse un evento de pandemia no se había considerado como una situación posible hasta el último informe del año 2020.

A lo largo de los años, este informe sigue demostrando su valor para los profesionales de la continuidad del negocio y la resiliencia al proporcionar tendencias sobre los incidentes a los que se han enfrentado las organizaciones en el último año; las principales amenazas y sus impactos para las organizaciones según los profesionales; el uso de la norma ISO 22301 y el costo de las interrupciones para las organizaciones.

En el reporte 2020, los “Incidentes asociados a la Salud” figuran como los de mayor exposición, ocupando el primer lugar y desplazando al riesgo “Ataque Cibernético e interrupciones de TI” que, históricamente, han encabezado la lista.

En el reporte 2021, el informe también analiza el impacto que COVID-19 ha tenido en las empresas en los últimos 12 meses. Las organizaciones han informado de un aumento en los riesgos y amenazas relacionadas a la salud en el último año, en una gran parte debido a la pandemia de COVID-19. Las enfermedades no laborales han encontrado su camino a la cima de la lista de riesgos empresariales, con la falta de preparación citada como la principal razón de la interrupción.

El impacto de la pandemia también ha provocado una intensificación de los riesgos en otros ámbitos, que van más allá de la pérdida de vidas. Los incidentes relacionados con la salud son la segunda fuente más común de perturbación en los últimos 12 meses, siendo los problemas de salud mental la principal dolencia experimentada por los empleados.

La pandemia también brindó la oportunidad a los ciberdelicuentes de explotar las vulnerabilidades de seguridad creadas al pasar a trabajar desde casa. Esto, unido a las interrupciones imprevistas de la red, hizo que los ciberataques y las interrupciones de las TI ocuparan el cuarto y quinto lugar en la lista de riesgos.

El último informe Horizon Scan identifica nuevos riesgos emergentes para el año 2021 como resultado de los cambios en las circunstancias y contextos empresariales. El legado de la pandemia por COVID-19 ha hecho que los riesgos políticos y la violencia vuelvan a figurar entre los 10 primeros por primera vez en tres años, mientras que se prevé que continúen las

perturbaciones en los servicios de TI y telecomunicaciones, sobre todo a medida que se introduzcan nuevas tecnologías en el mercado para ayudar a la sociedad a recuperarse tras la pandemia.

Los encuestados indicaron que la pandemia ha sido el catalizador para acelerar la introducción de un programa de análisis más estructurado y centralizado, siendo los directivos quienes han impulsado en gran medida el cambio.

Por lo que respecta a una evaluación de riesgos convencional en donde se considera el impacto y la probabilidad de ocurrencia de un evento, si bien una pandemia puede representar un impacto importante, la probabilidad de ocurrencia es muy baja. En algunos casos se estima una probabilidad de una vez cada 50 años y en otras de una vez cada 100 años (probabilidad anual de 1% y 2%, respectivamente), por lo que en la mayoría de las evaluaciones de riesgos dicho evento era imperceptible o irrelevante para las organizaciones antes del surgimiento de la COVID-19.

La importancia del plan de continuidad de negocio

Esta información nos lleva a reflexionar, una vez más, sobre la importancia de contar con un plan de continuidad de negocio vigente y actualizado, un plan que debería surgir desde la creación de toda organización. Y que se tendría que ir fortaleciendo a medida que la organización evoluciona o se enfrenta a algún incidente o crisis que interrumpe la continuidad de sus operaciones.

De esta forma, se confirmaría que las organizaciones que no cuenten con una estrategia y un plan de continuidad de negocio con un acertado plan de comunicación, conectividad y una extraordinaria capacidad de resiliencia ante posibles desastres estarían en riesgo de extinguirse, ya que se verían envueltas en la complejidad de operar y los impactos económicos serían catastróficos para ellas.

Por otro lado, así como será importante contar con un plan de continuidad en las organizaciones, se tiene que asegurar que los socios de negocio, principales proveedores, socios estratégicos en

las cadenas de valor, etc., estén debidamente alineados con la organización a través de sus respectivos planes de continuidad de negocio. Ello debe ser así porque la rápida reacción y el establecimiento de estrategias conjuntas, homologadas por un plan anticipado de respuesta, puede generar, además de un diferenciador respecto a los competidores, una afectación menor y más controlada.

Otra enseñanza que deja la situación actual es que la decisión de regresar a un esquema normal en las operaciones puede tener una dependencia totalmente externa. Por ello, en los planes se debe reconsiderar que su impacto ha de tener una visión de 360 grados en todo momento. Y los planes deberán contemplar una estructura de adaptabilidad total con el objetivo de que los múltiples factores de afectación puedan considerarse.

Pilares fundamentales

Con respecto a los puntos de impacto que nos trajo la actual pandemia en nuestros planes de continuidad de negocio, deberemos considerar los siguientes pilares fundamentales:

- **Talento**

  Se tiene que asumir que las personas son el principal activo en las organizaciones y que, sencillamente, son las que harían funcionar los planes de continuidad de negocio. No solo se debe tener perfectamente identificadas a las personas que operan procesos críticos. Además, se tiene que asegurarse de que cuentan con las condiciones para operar en escenarios de estrés social, familiar, personal y tecnológico.

- **Socios estratégicos de negocio**

  Un engranaje fundamental para el desarrollo de las actividades. Lo que genera una obligación por parte de toda organización contar con un listado de proveedores que puedan surgir como sustitutos inmediatos en caso de un colapso del socio estratégico principal.

- **Instalaciones**

  Si bien pareciera que es normal que los planes de continuidad de negocio contemplen la habilitación de inmuebles u oficinas alternas en caso de crisis, los mismos, por lo regular, cumplen con las condiciones mínimas necesarias para operar. Sin embargo, la irrupción de la pandemia podría provocar la desaparición de instalaciones corporativas alternas. Ello obligaría a reenfocar los recursos para mejorar las condiciones de los empleados en sus propias casas u otras localidades. O bien, definitivamente, las instalaciones alternas deberán cumplir con los mismos estándares y facilidades con los que cuentan las oficinas de uso diario.

- **Infraestructura tecnológica.**

  En la gran mayoría de organizaciones se volverá aún más importante la renovación y la migración a modelos virtuales en muchas actividades y sectores. Será primordial contar con una estructura tecnológica sólida y redundante, pero, sobre todo, segura y libre de ataques o riesgos en la pérdida de información. Esto deben enfatizarse más en aquellas instituciones o compañías que tienen en su data información sensible y confidencial de clientes, procesos o productos.

Un último aspecto que se debe analizar con mayor detalle es el tiempo en los llamados RTO – Tiempo objetivo de recuperación y RPO – Punto Objetivo de recuperación, tomando en cuenta que el tiempo de duración de esta pandemia es quizá el mayor en toda la historia moderna de El Salvador y, en general, del mundo.

Normalmente, se piensa en una crisis de efecto golpe: muy intensa en los primeros momentos, tendiendo luego a disminuir. Pero se está enfrentando una crisis de tipo quemadura, cuyo peor momento no necesariamente es el inicial, ya que probablemente pueda empeorar con el tiempo. Y aunque en términos absolutos no sea así, su prolongación en el tiempo igual representa una complicación adicional.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo de investigación

El trabajo se diseñó bajo el enfoque mixto, utilizando herramientas propias del enfoque cuantitativo e instrumentos propios del enfoque cualitativo, donde se realizó una recopilación de información que tiene una finalidad descriptiva. Esta investigación no experimental es de naturaleza exploratoria, brinda ayuda para comprender y especificar las propiedades, características, procesos o cualquier otro fenómeno que se someta a un análisis. Para la realización del estudio se utilizó los siguientes métodos de investigación:

a) **Investigación primaria.** Consistió en obtener información para realizar una valoración del nivel de avance que las entidades financieras tenían en materia de gestión de continuidad.

b) **Investigación secundaria.** Análisis de información de aquellos aspectos teóricos acerca de estándares, sanas prácticas y metodologías para gestionar la continuidad de negocio.

3.2. Determinación de la población

Son las entidades que integran el Sistema Financiero, ya que se constituyen como sujetos obligados del cumplimiento de las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24. Con este criterio, la población de estudio queda conformada por 41 instituciones financieras, entre las que se encuentran Bancos Comerciales, Bancos Cooperativos, Sociedades de Ahorro y Crédito, Bancos Públicos, Aseguradoras e Instituciones Públicas de Crédito.

3.3. Técnica de recolección de información

Se utilizó la encuesta como instrumento de recolección de datos, la cual fue dirigida a diferentes puestos gerenciales que pudieran estar relacionados con el tema. La encuesta se dividió en apartados extraídos de las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24.

CAPÍTULO IV: ANÁLISIS DE LOS RESULTADOS

4.1. Análisis de los datos

A continuación, se presentan los resultados obtenidos en la etapa de recolección de información, del total de encuestas remitidas, se recibieron 36 respuestas que representan un 87.8%. Es importante señalar que los resultados son a nivel macro ya que el propósito fundamental de la encuesta fue obtener a nivel general el grado de conocimiento e implementación de la gestión de continuidad en el sistema financiero, por tal razón y en cumplimiento a políticas de confidencialidad y protección de información, asociadas al secreto profesional y comercial de cada entidad, no se presentarán resultados individuales ni por tipo de entidad.

Para la evaluación de los criterios de selección, se utilizaron las siguientes medidas:

- "Cumple" si la entidad considera que cumple con el criterio
- "Cumple Parcial" si la entidad considera que cumple parcialmente con el criterio
- "No Cumple" si la entidad considera que no cumple con el criterio.
- "No Aplica" En caso algún criterio no aplica.

Responsabilidades de la gestión de continuidad del negocio.

Pregunta 1. ¿La Junta Directiva ha aprobado políticas generales que definen el alcance, objetivos, así como los roles y responsabilidades que orienten la gestión de la continuidad?

Opciones	Respuestas	Porcentaje
Cumple	24	66.7%
Cumple parcial	10	27.8%
No cumple	1	2.8%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 4. Aprobación de la Junta Directiva de los elementos de la gestión de continuidad

Figura 15. Aprobación de la Junta Directiva de los elementos de la gestión de continuidad

Según los datos obtenidos, la mayoría de las instituciones respondieron que la Junta Directiva es la instancia responsable de la aprobación de los distintos elementos que conformar la gestión de continuidad de negocio. Al evaluar el total de Instituciones se observa que el 66.7% cumplen con este criterio, el 27.8% cumplen parcialmente, el 2.8% no cumple, y el restante 2.8% respondieron que no les aplica.

Pregunta 2. ¿La Junta Directiva ha aprobado recursos necesarios para el adecuado desarrollo de la gestión de continuidad del negocio, a fin de contar con la infraestructura y personal apropiados?

Opciones	Respuestas	Porcentaje
Cumple	26	72.2%
Cumple parcial	8	22.2%
No cumple	1	2.8%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 5. Aprobación de la Junta Directiva de los recursos para la gestión de continuidad

Figura 16. Aprobación de la Junta Directiva de los recursos para la gestión de continuidad

La mayoría de las instituciones respondieron que la Junta Directiva sí ha aprobado recursos necesarios para la continuidad. De las 36 Instituciones, se observa que el 72% cumplen con este criterio, el 22% cumplen parcialmente, el 3% no cumple, y el 3% respondieron que no les aplica.

Pregunta 3. ¿La Junta Directiva se asegura que la entidad cuente con una efectiva gestión de la continuidad del negocio?

Opciones	Respuestas	Porcentaje
Cumple	21	58.3%
Cumple parcial	14	38.9%
No cumple	0	0.0%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 6. Aseguramiento de la Junta Directiva para la gestión de continuidad de negocio

Figura 17. Aseguramiento de la Junta Directiva para la gestión de continuidad de negocio

El 58% lo cumplen, el 39% cumplen parcialmente. Y el 3% respondieron que no aplica.

Pregunta 4. ¿La Alta Gerencia implementa la gestión de la continuidad de negocios conforme las disposiciones de la Junta Directiva o Consejo de Administración?

Opciones	Respuestas	Porcentaje
Cumple	27	75.0%
Cumple parcial	7	19.4%
No cumple	1	2.8%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 7. Implementación de la gestión de continuidad por parte de la Alta Gerencia

Figura 18. Implementación de la gestión de continuidad por parte de la Alta Gerencia

Se observa que el 75% cumplen con este criterio, el 19% cumplen parcialmente, el 3% respondieron que no aplica y el otro 3% no cumple.

Pregunta 5. ¿La Unidad de Riesgos se asegura que la gestión de la continuidad del negocio de la entidad sea consistente con las políticas y procedimientos definidos para la gestión de riesgos?

Opciones	Respuestas	Porcentaje
Cumple	22	61.1%
Cumple parcial	12	33.3%
No cumple	1	2.8%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 8. Aseguramiento de la Unidad de Riesgos para la gestión de continuidad de negocio

Figura 19. Aseguramiento de la Unidad de Riesgos para la gestión

Se observa que el 61% de las Instituciones Financieras respondieron que, si cumplen con este criterio, un 33% cumplen parcialmente, un 3% no cumple y finalmente el otro 3% dijo que no le aplica.

Responsabilidad de la Unidad de Riegos y función de continuidad de negocio

Pregunta 6. ¿La función de continuidad propone las políticas, procedimientos y metodología apropiados para la gestión en la entidad, incluyendo la asignación de roles y responsabilidades?

Opciones	Respuestas	Porcentaje
Cumple	25	69.4%
Cumple parcial	7	19.4%
No cumple	3	8.3%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 9. Involucramiento de la función de continuidad de negocio en la gestión

Figura 20. Involucramiento de la función de continuidad de negocio en la gestión

Se observa que el 69% respondieron que sí cumplen con este criterio, un 20% respondieron que cumplen parcialmente, un 8% no cumple y finalmente el otro 3% dijo que no le aplica. La mayoría de las entidades comentaron que existen comités de Continuidad, en algunos casos definidos a nivel de país, donde de acuerdo con las políticas, se definen roles específicos para cada área. En buena medida, son las unidades de Riesgos las responsables de definir e impulsar la gestión de continuidad, lo que conlleva a la definición políticas, roles, responsabilidades e instancias que estarán a cargo de la implementación y mantenimiento del sistema.

En algunas entidades, existen representantes de las unidades que apoyan en la gestión, sin embargo, carecen de una figura designada formalmente y con autoridad delegada por parte de la Alta Dirección, responsable de la política e implementación del sistema de gestión. Esto queda más evidenciado en aquellas instituciones donde tiene avances únicamente en contingencias tecnológicas, estando aún en proceso de implementar estructuras más robustas e idóneas al tamaño y tipo de operaciones de la entidad.

Pregunta 7. ¿La función de continuidad del negocio vela por promover la mejora continua en la gestión de continuidad de la entidad?

Opciones	Respuestas	Porcentaje
Cumple	23	63.9%
Cumple parcial	7	19.4%
No cumple	5	13.9%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 10. Promoción de la mejora continua por parte de la función de continuidad

Figura 21. Promoción de la mejora continua por parte de la función de continuidad

El 64% respondió que cumplen con este criterio, un 19% respondieron que cumplen parcialmente, el 14% no cumple, y un 3% de las instituciones respondió que no le aplica.

Pregunta 8. ¿La función de continuidad del negocio informa a la Alta Gerencia y al comité de riesgos los aspectos relevantes de la gestión de la continuidad para una oportuna toma de decisiones?

Opciones	Respuestas	Porcentaje
Cumple	24	66.7%
Cumple parcial	6	16.7%
No cumple	5	13.9%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 11. Nivel de reporte de la función de continuidad con las autoridades de la entidad

Figura 22. Nivel de reporte de la función de continuidad con las autoridades de la entidad

Al comparar los resultados por el total de instituciones, se tiene que el 67% cumplen con este criterio, un 16% cumplen parcialmente, el 14% no cumple, y un 3% de las instituciones respondió que no le aplica.

Entendimiento de la organización

Pregunta 9. ¿La entidad ha desarrollado un análisis para determinar el impacto que tendría la interrupción de los procesos que soportan a sus principales productos y servicios?

Opciones	Respuestas	Porcentaje
Cumple	22	61.1%
Cumple parcial	9	25.0%
No cumple	4	11.1%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 12. Realización del análisis de impacto al negocio en los productos y servicios

Figura 23. Realización del análisis de impacto al negocio en los productos y servicios

Al comparar los resultados por el total de instituciones, se tiene que el 61% cumplen con este criterio, un 25% cumplen parcialmente, el 11% no cumple, y un 3% de las instituciones respondió que no le aplica.

Pregunta 10. ¿El análisis de impacto es revisado periódicamente y actualizado en función de los cambios ocurridos al interior de la organización y en el entorno?

Opciones	Respuestas	Porcentaje
Cumple	16	44.4%
Cumple parcial	10	27.8%
No cumple	9	25.0%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 13. Revisiones periódicas del análisis de impacto al negocio

Figura 24. Revisiones periódicas del análisis de impacto al negocio

Al analizar el total de instituciones el 44% mencionó que cumple, el 28% cumple parcialmente, y un 25% no cumple con dicho criterio, y un 3% no le aplica.

Pregunta 11. ¿La entidad ha identificado y evaluado los riesgos asociados a la interrupción del negocio empleando una metodología formalmente establecida?

Opciones	Respuestas	Porcentaje
Cumple	23	63.9%
Cumple parcial	9	25.0%
No cumple	3	8.3%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 14. Identificación de riesgos asociados a la interrupción del negocio

Figura 25. Identificación de riesgos asociados a la interrupción del negocio

Se puede observar que el 64% de las instituciones financieras respondieron que sí han realizado una identificación y evaluación de los riegos, así como han empleado una metodología formalmente establecida en sus instituciones, por otro lado, el 25% del total de instituciones mencionó que cumple parcialmente, el 8% no cumple con dicho criterio, y un 3% respondió que no le aplica.

Pregunta 12. ¿En función de los resultados del Análisis de Impacto al Negocio - BIA y la Evaluación de Riesgos, la entidad ha identificado los procesos que requieren contar con una estrategia y planes de continuidad de negocio?

Opciones	Respuestas	Porcentaje
Cumple	21	58.3%
Cumple parcial	11	30.6%
No cumple	3	8.3%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 15. Identificación de procesos que requieren estrategias de continuidad

Figura 26. Identificación de procesos que requieren estrategias y planes

Según los resultados obtenidos, se evidencia que el 58% cumple con este requisito, identificando los procesos que requieren contar una estrategia y planes de continuidad de negocio y recuperación de las operaciones, tomando como insumo los resultados del Análisis de Impacto al Negocio BIA y los resultados del análisis y evaluación de amenazas de continuidad de negocio, el 31% cumple parcialmente con este requisito, el 8% no lo cumple y el 3% no le aplica.

Selección de la estrategia de continuidad negocio

Pregunta 13. ¿La entidad ha seleccionado las estrategias que le permitirán mantener la continuidad de los procesos que soportan a sus principales productos y servicios?

Opciones	Respuestas	Porcentaje
Cumple	23	63.9%
Cumple parcial	7	19.4%
No cumple	5	13.9%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 16. Selección de estrategias de continuidad de negocio

Figura 27. Selección de estrategias de continuidad de negocio

El 64% del total de instituciones respondieron que cumplen con este criterio, el 19% cumple parcialmente, frente a 14% que no cumple, por otro lado, al 3% no le aplica.

Pregunta 14. ¿Las estrategias de continuidad de los procesos consideran la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de TI que soporte el proceso, seguridad de la información y recursos?

Opciones	Respuestas	Porcentaje
Cumple	22	61.1%
Cumple parcial	10	27.8%
No cumple	3	8.3%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 17. Alcance de las estrategias de continuidad de negocio

Figura 28. Alcance de las estrategias de continuidad de negocio

En cuanto a esta pregunta, en el total de instituciones se tiene que el 61% cumple con criterio, el 28% cumple parcialmente, el 8% no cumple y un 3% que no aplica.

Desarrollo e implementación de la estrategia de continuidad

Pregunta 15. ¿La entidad cuenta con un plan de gestión de crisis para enfrentar la fase aguda de un evento de interrupción de operaciones, donde se incluye su propósito y alcance, roles y responsabilidades, criterios de invocación y activación, responsables de su actualización, planes de acción, información para comunicarse con el personal, familiares y contactos de emergencia, interacción con los medios de comunicación, y el establecimiento de un centro de comando?

Opciones	Respuestas	Porcentaje
Cumple	20	55.6%
Cumple parcial	9	25.0%
No cumple	6	16.7%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 18. Entidades que cuentan con planes de gestión de crisis

Figura 29. Entidades que cuentan con planes de gestión de crisis

Con base a los resultados obtenidos, se observa un cumplimiento un poco superior al 50% de las entidades en cuanto a tener un plan de gestión de crisis, siendo este uno de los principales planes que se elaboran para responder y recuperarse frente a incidentes disruptivos. Este plan tiene un propósito de permitir gestionar la fase aguda (inicial) de todo evento.

Para el caso de las entidades que cumplen parcialmente o que no cumplen con el criterio, 25% y 17% respectivamente, pueden afrontar serias limitantes para gestionar estos incidentes de alto impacto, ya que carecen de flexibilidad, existen posibles retrasos en la toma de decisiones y se genera un amplio espacio para las improvisaciones. Pudiendo llegar, en caso de materializarse alguna amenaza, no solo a interrumpir sus operaciones sino a afectar la seguridad e integridad de las personas y demás recursos necesarios para el desarrollo de la entrega de productos y servicios de cada entidad.

Finalmente, el no contar con un plan de crisis debidamente implementado y gestionado, expone a las entidades a interrupciones de sus procesos más prolongadas y, por ende, a perdidas e impactos económicos y reputacionales.

Pregunta 16. ¿Se han aplicado los planes de continuidad de negocios de tal manera de dotar a la entidad de la capacidad de mantener o recuperar los procesos críticos de negocio dentro de los parámetros previamente establecidos por la entidad?

Opciones	Respuestas	Porcentaje
Cumple	19	52.8%
Cumple parcial	9	25.0%
No cumple	7	19.4%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 19. Aplicación de planes de continuidad de negocio

Figura 30. Aplicación de planes de continuidad de negocio

Con respecto a este criterio el 53% del total de instituciones respondió que sí cumplen con este criterio, el 25% cumple parcialmente, el 19% no cumple, y el 3% no les aplica.

Pregunta 17. ¿Se han desarrollado planes específicos que considere por lo menos un Plan de Emergencia y Evacuación y un Plan de Recuperación de los servicios de tecnología de información?

Opciones	Respuestas	Porcentaje
Cumple	25	69.4%
Cumple parcial	6	16.7%
No cumple	4	11.1%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 20. Existencia de planes de emergencia y evacuación y plan de tecnología

Figura 31. Existencia de planes de emergencia y evacuación y plan de tecnología

Se observa que el 70 % de las entidades financieras poseen una comprensión razonable de la interrelación que existe entre las disciplinas de respuesta a la emergencia, continuidad operativa y recuperación de tecnología y comunicaciones, siendo estas disciplinas todas importantes para la gestión de incidentes y el manejo coordinado de la respuesta frente a la materialización de un incidente disruptivo.

Este criterio es cumplido parcialmente por el 17%, no cumplen el 11%, y para el 3% no es aplicable.

Pruebas y actualización

Pregunta 18. ¿El alcance de las pruebas es consistente con el alcance de los planes de continuidad y cada prueba tiene objetivos definidos y un reporte que resume los resultados alcanzados?

Opciones	Respuestas	Porcentaje
Cumple	14	38.9%
Cumple parcial	12	33.3%
No cumple	9	25.0%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 21. Consistencia del alcance de las pruebas de continuidad de negocio

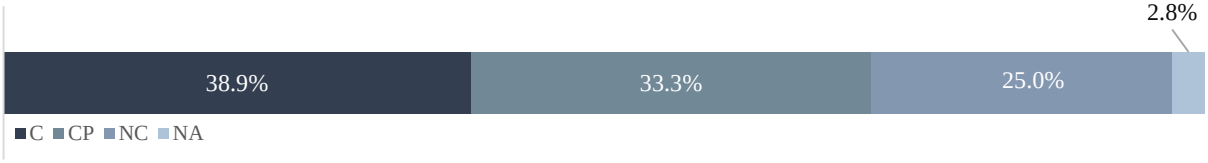


Figura 32. Consistencia del alcance de las pruebas de continuidad de negocio

Solo el 39% de entidades podrían demostrar que desarrollan competencias y capacidades de continuidad de negocio y gestión de incidentes, el 33.3% cumplen parcialmente, el 25% no cumplen y el 3% no les aplica.

Pregunta 19. ¿La entidad revisa y actualiza periódicamente sus planes de continuidad de negocios para lo cual cuenta con políticas y procedimientos definidos?

Opciones	Respuestas	Porcentaje
Cumple	15	41.7%
Cumple parcial	11	30.6%
No cumple	8	22.2%
No aplica	2	5.6%
Total	**36**	**100.0%**

Tabla 22. Periodicidad de revisiones y actualizaciones del plan de continuidad de negocio

Figura 33. Periodicidad de revisiones y actualizaciones del plan de continuidad de negocio

Se puede observar que el 42% del total de instituciones financieras mencionaron que, si cumplen con este criterio, el 31% cumplen parcialmente, el 22% no cumplen, y el 5% no les aplica, siendo estas revisiones periódicas necesarias para el adecuado mantenimiento del sistema de gestión de continuidad de negocio.

Integración de la gestión de la continuidad del negocio dentro de la cultura organizacional

Pregunta 20. ¿La entidad evalúa el grado de conocimiento sobre la gestión de continuidad de negocio?

Opciones	Respuestas	Porcentaje
Cumple	11	30.6%
Cumple parcial	10	27.8%
No cumple	14	38.9%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 23. Nivel del grado de conocimiento del personal sobre la continuidad de negocio

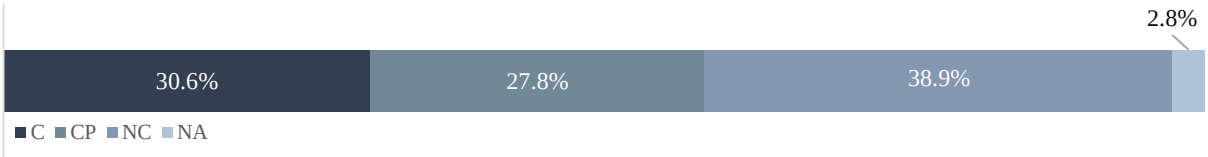


Figura 34. Nivel del grado de conocimiento del personal sobre la continuidad de negocio

Se observa que el 30% mencionó que sí cumplen con este criterio, el 28% cumple parcialmente, el 39% no cumple con este criterio, y un 3% no les aplica.

Pregunta 21. ¿Se ha diseñado e implementado planes de capacitación y campañas de concientización a fin de cubrir las deficiencias de conocimiento identificadas?

Opciones	Respuestas	Porcentaje
Cumple	11	30.6%
Cumple parcial	16	44.4%
No cumple	8	22.2%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 24. Elaboración de planes de capacitación de campañas de concientización

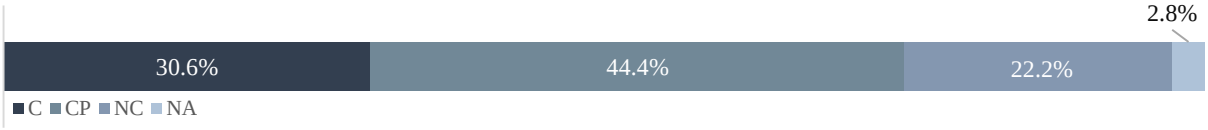


Figura 35. Elaboración de planes de capacitación de campañas de concientización

El 31% los ha realizado, el 44% cumplen parcialmente, el 22% no cumplen, y el 3% no aplica.

Pregunta 22. ¿La entidad revisa periódicamente el nivel de entendimiento de la gestión de la continuidad del negocio a fin de identificar requerimientos adicionales?

Opciones	Respuestas	Porcentaje
Cumple	11	30.6%
Cumple parcial	12	33.3%
No cumple	12	33.3%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 25. Periodicidad de revisión del nivel de entendimiento de la gestión de continuidad

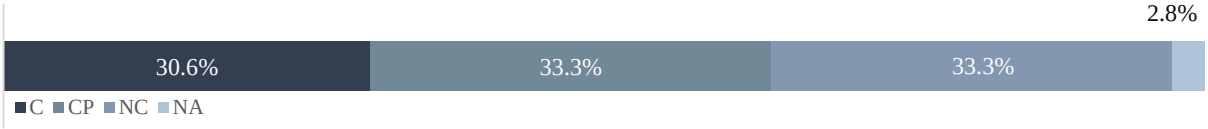


Figura 36. Periodicidad de revisión del nivel de entendimiento de la gestión de continuidad

El 31% cumplen, el 33% cumplen parcialmente, el 33% no cumplen y 3% no aplica.

Cambios significativos

Pregunta 23. ¿La entidad analiza los cambios significativos que puedan afectar la continuidad, tales como cambios procesos y prioridades y requerimientos legales?

Opciones	Respuestas	Porcentaje
Cumple	25	69.4%
Cumple parcial	4	11.1%
No cumple	6	16.7%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 26. Análisis de cambios significativos que pueden afectar la continuidad de negocio

Figura 37. Análisis de cambios significativos que pueden afectar la continuidad de negocio

El 69% cumple, el 11% cumple parcialmente, el 17% no cumple y el 3% no les aplica.

Revisión Alta Gerencia y Auditoría Interna

Pregunta 24. ¿La Unidad de Auditoría Interna verifica el cumplimiento de las políticas y planes de continuidad de negocios de la entidad?

Opciones	Respuestas	Porcentaje
Cumple	21	58.3%
Cumple parcial	8	22.2%
No cumple	6	16.7%
No aplica	1	2.8%
Total	**36**	**100.0%**

Tabla 27. Nivel de verificación de Auditoría Interna

Figura 38. Nivel de verificación de Auditoría Interna

En el 58% cumple, el 22% cumple parcialmente, el 17% no cumple y el 3% no les aplica.

4.2. Evaluación del nivel de madurez del sistema financiero

A continuación, se presentan los resultados consolidados por apartado, a fin de evaluar el nivel de desarrollo de cada uno ellos en gestión de continuidad de las entidades del sistema financiero.

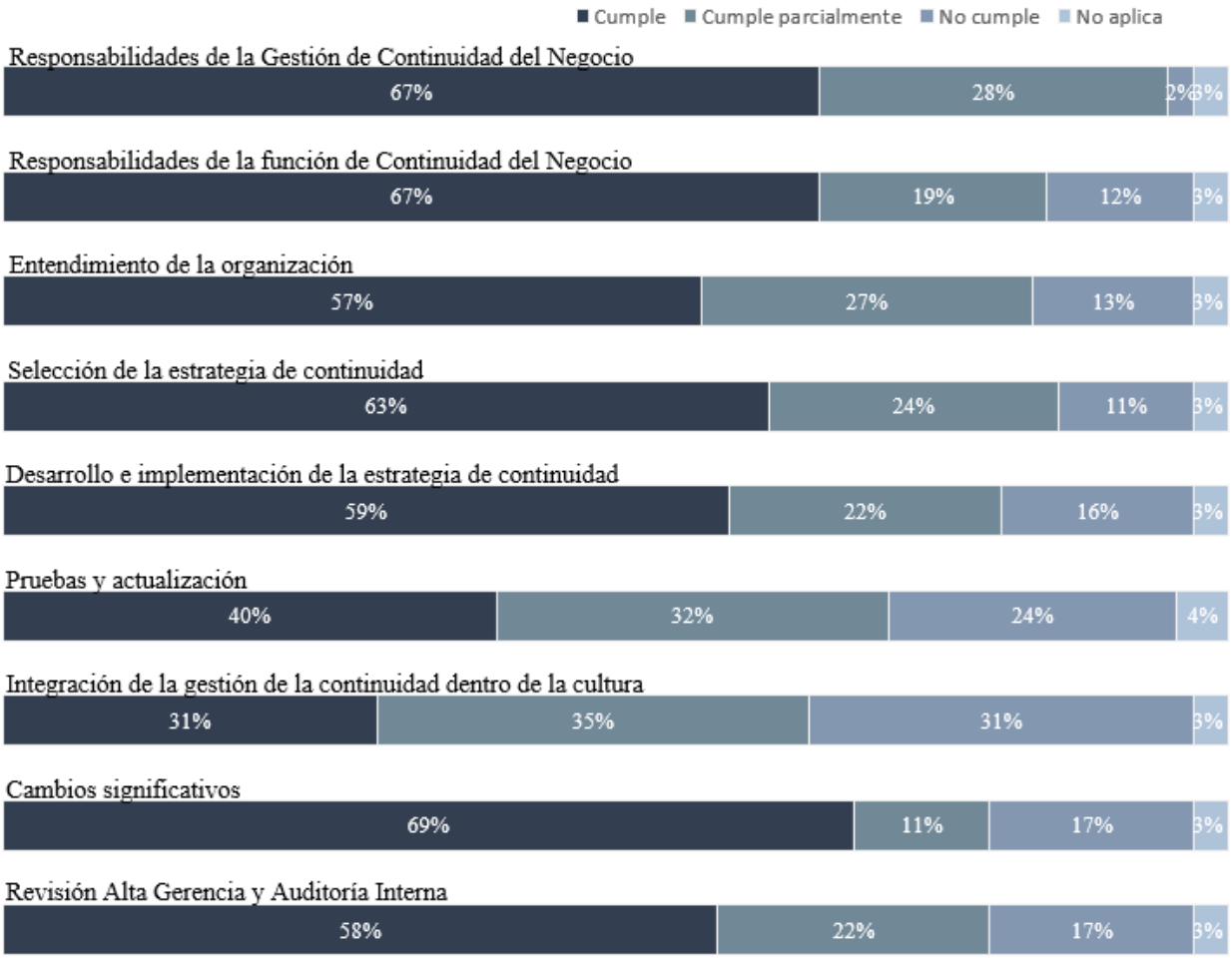


Tabla 28. Resultados promedio de los 9 apartados del instrumento de medición

Con esta información, se procedió a evaluar el nivel de avance y desarrollo que poseen en gestión de continuidad las entidades sujetas del estudio, para ello se promedió a nivel general los resultados por apartado, los resultados obtenidos se muestran en la siguiente grafica.

Figura 39. Resultados globales del nivel de avance de la gestión en el sistema financiero

Para determinar el nivel de madurez del sistema, se tomó el grado de cumplimiento global, es decir el 57%, y se contrastó con una valoración mediante una escala de Likert de cinco niveles (Inexistente (0), Inicial (1), Repetible (2), Administrado (3), Optimizado (4).

Nivel de Madurez	Criterios para validar el nivel de clasificación	Rango
0 Inexistente	• Administración de Continuidad no reconocida. • Unidades se organizan por sus medios y se autogobiernan. • Ausencia o limitación de procesos de continuidad de negocio.	**0-30%**
1 Inicial	• Al menos una unidad reconoce la importancia de la continuidad. • No hay procesos documentados, la gestión es desorganizadas. • Alta dirección considera el valor de la gestión, pero no es prioridad.	**30%-50%**
2 Definido	• Existen algunos procedimientos y políticas documentadas de continuidad, pero con poca o nula evaluación y entrenamiento. • Personas o unidades con responsabilidades básicas para la continuidad. • Limitada formación formal, comunicación o pruebas. • Alta Dirección aún no tiene un fuerte compromiso con Continuidad.	**50%-70%**
3 Gestionado	• Estrategia completa, procedimientos documentados, entrenamiento, políticas desarrolladas, pruebas parciales, Mantenimiento. • Elementos críticos de las funciones del negocio han sido identificadas, valoradas y se han desarrollado planes de continuidad. • Existe compromiso de la Alta Dirección.	**70%-90%**
4 Optimizado	• Procesos establecidos a un nivel de buenas prácticas, sobre la base de los resultados de la mejora continua. • Existe total coordinación entre áreas ante un evento disruptivo. • Pruebas de estrategia, planes documentados y formación, políticas desarrolladas, Mantenimiento y actualización. • Personal con alto grado de competencia y existe planeación medible • Alta Dirección completamente comprometida y participativa.	**90%-100%**

Tabla 29. Ponderado y calificación de los niveles de madurez

La madurez del sistema financiero se ubica como nivel 2 “Definido”, existiendo brechas de desarrollo en elementos indispensables para una adecuada gestión, tales como el fortalecimiento de instancias con responsabilidades, procesos de análisis y un mayor alcance de los planes, acciones de formación, pruebas, entre otros. Por otra parte, con estos resultados se muestra la necesidad de establecer una metodología que permita brindar apoyo en la implementación de continuidad con base a las Normas Técnicas para la Gestión de Continuidad NRP-24.

CAPÍTULO V: PROPUESTA E IMPLEMENTACIÓN DE LA METODOLOGÍA

5.1. Aspectos generales

Esta metodología es una propuesta fundamentada en las normas, estándares y sanas prácticas internacionales con el fin de formular, lo más sencillo y práctico posible, los elementos necesarios de un sistema de gestión de continuidad, que permita cumplir con los requerimientos mínimos y lo más relevante, brinde a las entidades la posibilidad de desarrollar capacidades de respuesta y continuidad de las operaciones a un nivel aceptable en un escenario de incidente disruptivo.

Para su formulación se tomó como base las metodologías descritas en el Capítulo II, apartado 2.4.2, luego de una revisión, se seleccionaron los puntos más fuertes de cada una de ellas y que se consideran cumplen o exceden lo requerido en las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24.

5.2. Uso de la metodología

Esta metodología busca ser una guía para las entidades financieras que tengan como objetivo implementar la gestión de continuidad en sus organizaciones, se identifica y define una secuencia lógica de actividades y recomendaciones para el desarrollo de cada una de las fases que integran el ciclo de vida de esta gestión.
La metodología contiene un gran compendio de la terminología utilizada en distintos estándares internacionales que regulan aspectos de la gestión de continuidad del negocio. La metodología proveerá la base de conocimiento necesaria para comprender el proceso realizar dicha gestión.

Este documento, y sus disposiciones, no constituye de ninguna manera una obligación ni compromiso de cumplimiento para las entidades del sistema financiero. Esta metodología tiene una naturaleza orientativa, es una guía que tiene la finalidad de facilitar la implementación de un sistema de gestión de continuidad de negocio, las actividades y tareas que se sugieren en este documento son únicamente recomendaciones.

Queda a criterio de cada entidad la aplicabilidad total o parcial de las sugerencias que se brindan en el presente documento. Así mismo, el cumplimiento de esta metodología no exime a las entidades financieras de las responsabilidades y obligaciones que se regulan en la Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24.

5.3. Base metodológica y regulatoria

Con el objetivo de desarrollar una metodología alineada a la normativa nacional, así como a estándares internacionales, se tomará como referencia principal a la estructura propuesta por las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24; aprobada por el Comité de Normas del Banco Central de Reserva, teniendo en consideración aspectos relevantes de la ISO 22301:2012, así como de la Guía de buenas prácticas del Business Continuity Institute (BCI).

En tal sentido, se realizó una comparación de los requisitos establecidos en la norma ISO 22301:2012 y la Guía de buenas prácticas del BCI con las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24, con la finalidad de garantizar que se encuentren alineadas.

Componente PHVA	Numeral ISO (N)	Guía de buenas prácticas BCI – Practica Profesional (PP)	Norma NRP-24 – Continuidad de Negocio
Planificar (Establecer)	N4 – Contexto de la Organización N5 – Liderazgo N6 – Planeación N7 - Soporte	PP1 – Política y Gestión del Programa PP2 – Incorporación Continuidad de Negocio	Art. 4 Gestión de Continuidad Art. 5 Responsabilidades Junta Directiva Art. 6 Responsabilidades Comité de Riesgos Art. 7 Responsabilidades Alta Gerencia Art. 8 Responsabilidad Unidad de Riesgos Art. 9 Sistema de Gestión de Continuidad

Componente PHVA	Numeral ISO (N)	Guía de buenas prácticas BCI – Practica Profesional (PP)	Norma NRP-24 – Continuidad de Negocio
			Art. 10 Funciones unidad Continuidad Art. 11 Política de Continuidad Art. 12 Incorporación de la Continuidad Art. 20 Tercerización
Hacer (Implementar y Operar)	N8 - Operación	PP3 – Análisis PP4 – Diseño PP5 – Implementación PP6 – Validación (Programa de Pruebas)	Art. 13 Análisis de Impacto al Negocio Art. 14 Análisis Amenazas de Continuidad Art. 15 Diseño y selección de la estrategia Art. 16 Implementación de la estrategia Art. 17 Pruebas de Continuidad
Verificar (Monitoear y revisar)	N9 – Evaluación de Desempeño	PP6 – Validación (Revisión)	Art. 19 Revisión y mantenimiento Art. 23 Auditoría Interna
Actuar (Mantener y mejorar)	N9 - Mejora	PP6 – Validación (Mantenimiento)	Art. 19 Revisión y mantenimiento Art. 21 Cambios significativos

Tabla 30. Comparación entre estándares internacionales y norma para continuidad

A continuación, se presenta las etapas de la metodología propuesta para que las entidades financieras puedan implementar la gestión de continuidad de negocio, sus fases y actividades toman en consideración principalmente el ciclo de vida de continuidad de negocio y las disposiciones establecidas en las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24 y estándares internacionales de referencia.

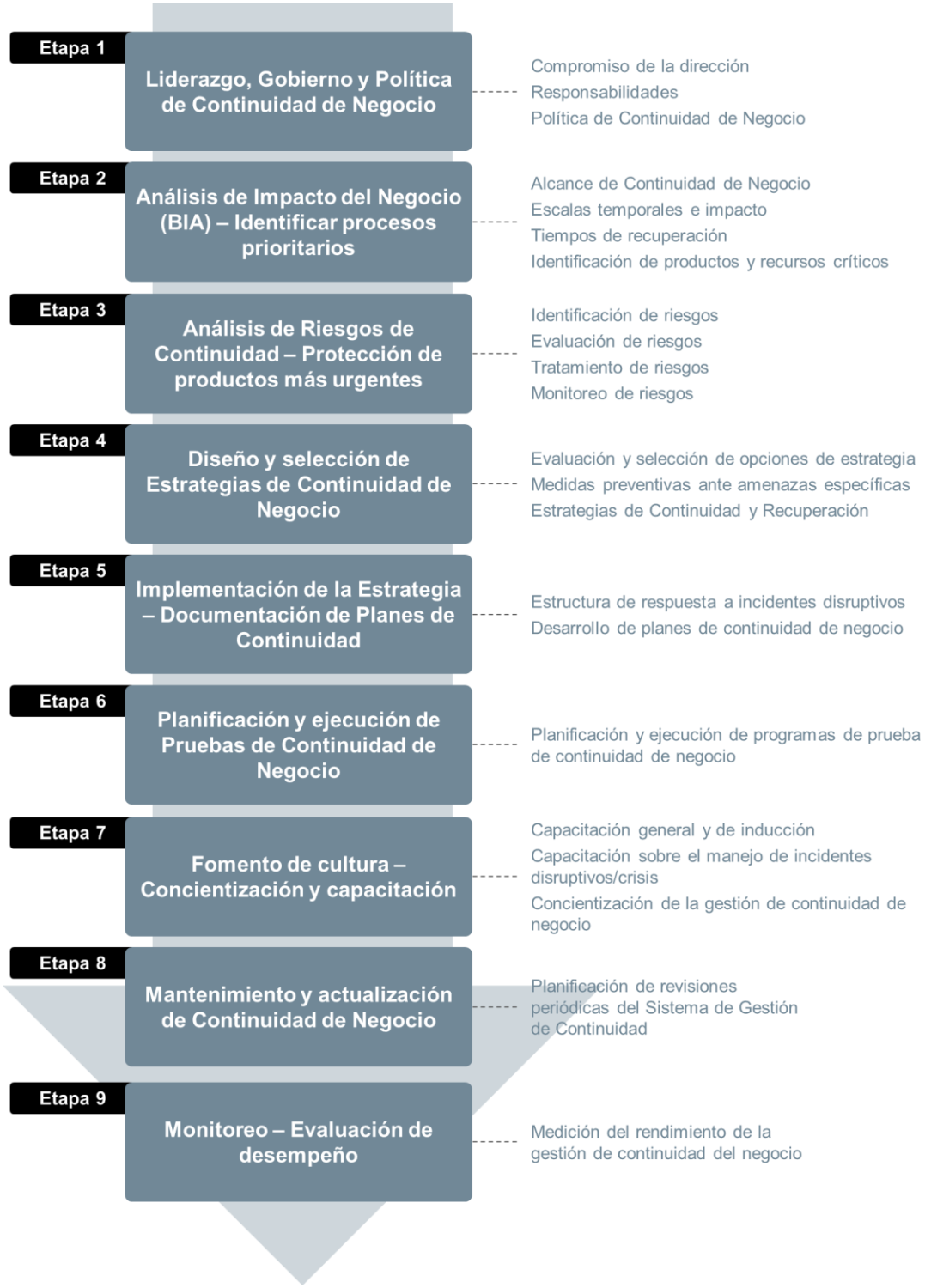


Figura 40. Metodología para la implementación de la gestión de continuidad

5.4. Metodología para la gestión de continuidad de negocio

A continuación, se describen las etapas que incluye la metodología para implementar la gestión de la continuidad del negocio:

5.4.1. Etapa 1. Liderazgo, gobierno y política de continuidad de negocio.

La participación, liderazgo y compromiso de todos los niveles de dirección es fundamental para asegurar que los procesos de la gestión de continuidad se introduzcan de forma correcta, tengan el apoyo suficiente y se definan como parte de la cultura. A pesar de que en muchas instituciones la Alta Dirección puede estar consciente de la importancia de tener implementado un proceso formal de continuidad, muchas veces no demuestran o dan el apoyo necesario para las iniciativas orientadas a la resiliencia. Por otra parte, un error muy común es confundir la continuidad con tener formulado el documento del plan de contingencia y ese es otro error muy común.

Uno de los primeros objetivos y retos en materia de continuidad, es lograr el empoderamiento apropiado en todo el nivel jerárquico de la entidad: Junta Directiva, gerencias, jefaturas y expertos del conocimiento en las actividades. Conseguir este empoderamiento fomenta un gobierno al proceso permanente de continuidad del negocio. Los roles o instancias asociadas en el gobierno de continuidad se definen en la siguiente figura:

Figura 41. Roles/instancias participantes en la continuidad de negocio

a) Compromiso de la Dirección

El Compromiso de la Dirección se refiere a las obligaciones y responsabilidades que adquiere la alta dirección en el desarrollo y la implementación de la gestión de continuidad de negocio. A continuación, se definen responsabilidades globales y complementarias a las descritas en las Normas Técnicas para la Gestión de Continuidad de Negocio NRP-24.

Junta Directiva

Siendo la instancia de dirección institucional, es responsable de establecer y mantener una adecuada gestión de la continuidad del negocio en la entidad. Encarga esta responsabilidad a la autoridad de mayor rango jerárquico en la entidad, entiéndase un gerente general y le exige rendimiento de resultados en el tema al final de cada periodo que estime conveniente. Aprueba las políticas y estrategias generales que definen el alcance, principios y guías que orienten la gestión de continuidad en la entidad. La Junta Directiva también es responsable de aprobar, según le corresponda, las inversiones en recursos necesarios para lograr implementar la continuidad del negocio. Es también la Junta Directiva quien debe evidenciar que la continuidad del negocio soporte la continuidad y sobrevivencia de los objetivos estratégicos de la entidad.

Comité de Riesgos

Siendo la instancia responsable de velar por una sana gestión de la continuidad del negocio de la entidad, evalúa, revisa y propone las políticas y estrategias generales que definen el alcance, principios y guías que orienten la gestión de continuidad. También es responsable de aprobar el o los planes de continuidad de negocio que se definan en función a su tamaño, complejidad y tipo de operación. Finalmente, vela por la efectividad de la gestión de continuidad de negocio, asegurándose que se realice cada una de las fases de implementación de la gestión, como el análisis de impacto al negocio, análisis de amenazas, definición de estrategias y pruebas de continuidad de negocio.

Alta Gerencia

Responsable de impulsar la gestión de continuidad en la entidad, por medio de la implementación de las políticas y estrategias generales que definan el alcance, principios y guías que orienten la gestión de continuidad en la entidad, en cumplimiento con lo autorizado por la Junta Directiva. Vela porque se realicen las pruebas de continuidad del negocio y se fomente una cultura de continuidad, motivando la participación activa y el compromiso de todos los empleados. También es responsable de activar los planes de continuidad en respuesta a la ocurrencia de incidentes de interrupción. Impulsa la mejora continua en la gestión de continuidad del negocio y delega o nombra las personas competentes para ser responsables de la implementación de la continuidad de negocio y dotarlas de la autoridad apropiada.

Las autoridades de la organización, bajo el liderazgo de la gerencia general, deben establecer, mantener y practicar un esquema de respuesta a los incidentes y crisis que puedan presentarse tanto a nivel operativo, de emergencias o de afectación de la reputación; para ello deberán definir un equipo de respuesta y asignar roles de gobierno del incidente y de la crisis y brindarle lo necesario para crear las competencias necesarias.

Unidad de Riesgos

Responsable de apoyar en el diseño de las políticas y estrategias generales que definan el alcance, principios y guías que orienten la gestión de continuidad en la entidad, para aprobación de la Junta Directiva. Apoya en el diseño y somete para aprobación del Comité de Riesgos, los planes de continuidad. Asegura que la gestión sea consistente con las políticas, metodologías y procedimientos aplicados para la gestión de riesgos.

Unidad o área especializada en continuidad del negocio

Responsable de diseñar políticas, estrategias generales, alcance y principios que orienten la gestión de continuidad en la entidad. Realiza el análisis de impacto al negocio y el análisis de amenazas e informa los resultados a las autoridades. Diseña los planes de continuidad y coordina el diseño ejecución de un programa de pruebas. También es responsable de establecer programas

de capacitación y concientización al personal, directamente relacionados con la continuidad, para que éste conozca su rol a la hora de un evento disruptivo.

Según el tamaño de la entidad, esta función podría ser compartida con otras funciones encargadas a algún rol en materia de respuesta y recuperación dentro de la institución. En entidades de mayor tamaño, esta función podría ser exclusiva y a tiempo completo. La implementación de la gestión de continuidad no debe recaer solo en esta función si no que se debe involucrar a las jefaturas de las áreas o líderes de procesos.

Unidades de la entidad

Responsables de implementar y mantener la continuidad en su ámbito y responsabilidad de operaciones. Para ello deberán designar, si es posible, un enlace de continuidad de su área o proceso con la autoridad necesaria para articular los esfuerzos internos, en coordinación y bajo el liderazgo de la función de la continuidad de la entidad. En caso no se pueda designar un responsable, serán las jefaturas directamente las responsables de implementar y mantener la continuidad al interior de sus unidades. Además, informan sobre cualquier suceso o evento que pueda representar una amenaza a la continuidad de operaciones de la entidad. Tienen una participación activa en los programas de capacitación y pruebas de continuidad.

En el caso de las unidades que administran procesos de apoyo a las operaciones, como Seguridad, Recursos Humanos, Servicios Generales, Tecnología de Información, u otras, deberán participar liderando la respuesta al incidente de los eventos más comunes dentro de su ámbito (pandemia, incendio, sismo o terremoto, caída del centro de cómputo, etc.) así como apoyar a la respuesta a incidentes que interrumpen las operaciones de las actividades más críticas de la entidad.

Enlaces o líderes de continuidad

En aquellas entidades que definan este rol, tienen la responsabilidad de apoyar y garantizar que se desarrollen, mantengan y prueben los planes de continuidad de su unidad. Facilitan la coordinación de la respuesta ante incidentes y realizan los esfuerzos de recuperación de sus

procesos. Asimismo, actualiza y custodia el plan de continuidad del negocio del proceso que tenga a cargo gestionar. Participan en las capacitaciones relacionadas y, a solicitud de la función de continuidad del negocio, participa en los talleres de Análisis de impacto al negocio y evaluación de riesgos de interrupción.

Miembros de los equipos de planificación, respuesta y continuidad

Usualmente estos equipos están conformados por personal operativo debajo de las jefaturas, que durante el proceso de implementación y mantenimiento de la continuidad; brindan conocimiento especializado sobre las prioridades y necesidades de recuperación. Durante un ejercicio o un incidente real participan en la respuesta al incidente aplicando los planes y estrategias de continuidad elaborados.

Los miembros de estos equipos deben tener las competencias necesarias, credenciales de formación especializada y evidenciable en temas de continuidad del negocio, deberán también conocer sus planes y deberán tener experiencia en la respuesta a los incidentes aplicando sus planes.

Personal en general

A pesar de que no necesariamente participa de la continuidad de negocio de manera activa, participa en la gestión de la siguiente forma: Conoce cómo y a quién notificar y escalar un incidente que pudiera causar interrupción de operaciones. Conoce al equipo de recuperación de su área o proceso y conoce cómo y cuándo y con quién reportarse en caso de un incidente real. Asimismo, ante un incidente disruptivo, conoce cómo canalizar requerimientos de los medios de comunicación u otros interesados sobre la situación.

Responsabilidad de comunicar a la Superintendencia del Sistema Financiero (SSF)

La función de continuidad puede asumir la responsabilidad de comunicar a la SSF: Los resultados de las pruebas, la activación del plan de continuidad del negocio cuando ocurra un incidente de interrupción; dicha comunicación deberá incluir; una descripción sobre cada interrupción que afecte a los servicios financieros en el momento después de su ocurrencia y

completar información relacionado al evento reportado, a más tardar diez días después de haber notificado sobre la interrupción. También deben comunicar las interrupciones que afecten la conexión directamente con el sistema de Liquidación Bruta en Tiempo Real del Banco Central, en este caso también deberá informarse a la unidad que administra los sistemas de pagos.

Auditoría Interna

Debe asegurar que la gestión de continuidad se ejecute según las disposiciones dadas por la Junta Directiva y acorde a las mejores prácticas profesionales al respecto. El auditor debe ser alguien independiente y debe tener competencias adecuadas para aportar oportunidades de mejora alineadas a los objetivos de la gestión.

b) Política de continuidad de negocio

La Junta Directiva de las entidades, debe aprobar la Política de Continuidad, asegurándose que ésta proporcione el marco para implementarla. Esta política hace mención del alcance a nivel de productos, servicios y áreas, por ende, todo lo que no está en el alcance, se considera que no es prioritario ni urgente recuperar, y con lo cual, se tendrá el suficiente tiempo para restablecer dichas actividades. En el anexo 1 se presenta un ejemplo de una política de continuidad que puede ser adaptada a cualquier entidad, considerando su tamaño y naturaleza de operaciones.

5.4.2. Etapa 2. Análisis de impacto del negocio (BIA)

Las entidades deben determinar y documentar el impacto de interrupción en los procesos y recursos que permiten la entrega de sus productos y servicios fundamentales, a este proceso generalmente se le conoce como Análisis de Impacto al Negocio. (ISO 22317, 2015).

El principal objetivo del BIA es brindar insumos para establecer el alcance de la gestión y la preparación para afrontar un incidente disruptivo; permite identificar los productos y procesos críticos; el orden, nivel y tiempos de recuperación de estos; así como la dependencia que existe entre ellos; otro objetivo importante es la identificación de los recursos mínimos necesarios para la recuperación de los productos y procesos y sirve de base para el diseño y definición de estrategias de continuidad que sean costo efectivas.

Lineamientos para realizar el análisis de impacto al negocio

Para la ejecución de este análisis se deben considerar los siguientes lineamientos:

- Antes de realizar el BIA, el alcance, escalas, niveles de criticidad, tipos y descripción de impactos y demás información relevante deben ser aprobadas por el Comité de Riesgos.
- El BIA se ejecutará de forma anual a todos los procesos de negocio y soporte que dan apoyo a los productos y servicios de la entidad. Los productos se priorizan primero; luego a nivel de procesos y recursos asociados a estos.
- El BIA debe identificar, cuantificar y calificar los impactos de incidentes de interrupción en la entidad en términos (1) Personas, (2) Financiero, (3) Reputacional, (4) Legal y (5) Clientes.
- Se realizarán talleres BIA, que consisten en reuniones con los expertos a nivel estratégico y operativo de cada proceso y/o producto, su fin es medir el impacto de interrupción de estos productos. El BIA se realiza usando el juicio experto de los participantes, así como datos reales de operaciones disponibles.
- Para la evaluación del BIA se tendrá en consideración el peor escenario que pueda ocurrir y se preferirá un criterio conservador ante las dudas o cuestionamientos en el proceso.
- Los entregables del proceso BIA, sujetos a aprobación son:
  - Escalas temporales, niveles de criticidad, tipos y descripción de impactos.
  - Listado de productos y procesos críticos obtenidos a partir del análisis de impacto realizado.
  - Tiempos objetivos de recuperación (RTO), Nivel mínimo Aceptable de Operación (MBCO) y el Máximo tiempo tolerable de interrupción (MTPD).
  - Recursos críticos necesarios para la recuperación e Interdependencias de procesos.
- El Tiempo Objetivo de Recuperación (RTO) de cada proceso/producto se obtiene de una decisión estratégica/táctica que considere la mejor opción costo/beneficio para la entidad. El RTO debe ser menor que el MTPD. Solo se calculará el RTO para los procesos que soportan productos críticos.
- El enlace de continuidad designado de cada unidad brindará la información base para el hacer el BIA.

- Un recurso será considerado crítico, siempre y cuando brinde soporte a un proceso o producto crítico.
- Se puede definir como crítico todo proceso o producto que tenga un MTPD menor o igual a 24 horas.
- El proceso BIA consistirá en las etapas descritas en la siguiente gráfica:

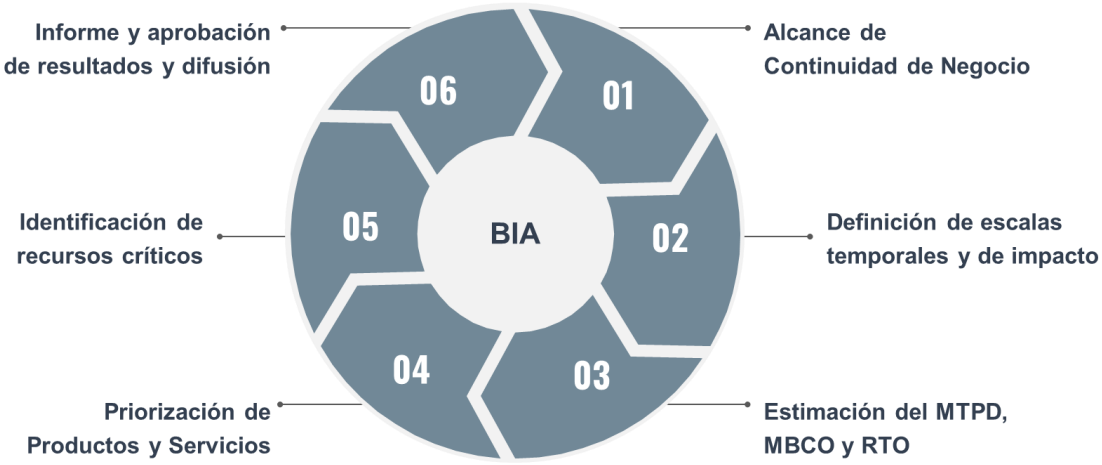


Figura 42. Proceso de realización del BIA

Paso 1. Alcance de la continuidad de negocio

Como paso previo, es importante que las entidades orienten esfuerzos y recursos a aquello que es realmente urgente de recuperar. Es recomendable definir el alcance de continuidad de negocio por productos y servicios que la entidad brinda. Una priorización preliminar de los productos y servicios puede ser efectuada por la Alta Dirección al plantearse el escenario y pregunta: En caso de un incidente disruptivo de alto impacto, ¿Cuáles productos y servicios deben seguirse brindando como mínimo?

Luego de establecer el alcance de los productos y servicios, puede establecerse un alcance geográfico, en caso de que las entidades cuenten con múltiples sedes donde se brindan los servicios o los centros alternos de operación, finalmente el alcance puede ser definido a nivel de actividades que permiten la entrega de los productos y servicios, esto permite también definirlo a nivel de departamentos o unidades funcionales.

Para llevar a cabo esta etapa, se debe recopilar los siguientes insumos de información:

- Misión, objetivos y dirección estratégica vigentes de la entidad.
- Listado actualizado de productos y servicios vigentes, macroprocesos, procesos y subprocesos; así como estructura organizacional.
- Lista de requisitos legales y regulatorios a los cuales la entidad o los productos y servicios están sujetos.
- Requisitos contractuales, incluyendo sanciones por falla en la entrega.
- Revisión de los impactos reputacionales, financieros u otros, por fallas en la entrega.

Paso 2. Validación (Revisión/actualización) de escalas temporales y de impacto

Para identificar los tiempos de recuperación, es necesario definir los umbrales de no tolerancia para la entidad. Para ello, la Alta Dirección debe establecer qué es lo que no soportaría que le ocurra a la entidad, ante un incidente disruptivo, en las siguientes categorías de impacto:

- **Seguridad de las personas**: ¿Qué nivel de afectación en las personas es intolerable?
- **Financiero**: ¿Cuánto dinero comprometido es intolerable perder para la entidad?
- **Procesos:** ¿Cuántos procesos afectados, o de qué tipo, es intolerable para la entidad?
- **Afectación de clientes:** ¿Cuántos clientes afectados, o de qué tipo, es intolerable para la entidad?
- **Legal/regulatorio**: ¿Qué nivel de sanciones o demandas por incumplimiento es intolerable?
- **Reputacional**: ¿Qué nivel de afectación en la imagen y reputación es intolerable para la entidad?

Estas preguntas deben responderse considerando la percepción y exigencias mínimas que tendrían las partes interesadas de la entidad durante un incidente disruptivo que interrumpa las operaciones. Ejemplos de estas partes interesadas son: usuarios o clientes, dueños o accionistas, autoridades públicas y organismos reguladores, socios de negocio, personal de la organización, entre otros.

Otras consideraciones importantes es conocer si existen niveles mínimos de servicios exigidos por el ente regulador o supervisor, también evaluar escenarios donde la afectación severa solo se produce en la entidad o es un evento que afecta una región o todo el país. Adicionalmente

debe analizarse el momento en el tiempo en el cual existe una mayor demanda o necesidad de contar con el producto o servicio, área, proceso, o localidad. Las respuestas a todas estas interrogantes darán como resultado la definición de los umbrales no tolerables de la entidad.

La siguiente actividad es estimar el Máximo Tiempo Tolerable de Interrupción (MTPD), determinando el tiempo más corto cuando se alcance el umbral intolerable para cualquier categoría. El MTPD es el resultado de plantear la siguiente pregunta: En caso de interrupción del producto / localidad / departamento / proceso, ¿en cuánto tiempo se alcanzan los umbrales no tolerables?, para responder esta pregunta se utilizará la siguiente escala temporal:

4 h	8 h	1 día	2 días	3 días	+ 1 sem	+ 1 mes

Tabla 31. Tiempos máximos permitidos de interrupción (MTPD)

Paso 3. Estimación del MTPD, MBCO y RTO

La estimación del **Máximo Tiempo Tolerable de Interrupción (MTPD)** se ejecutará a través de talleres BIA estratégicos en los cuales deberá participar al menos el gerente general y los gerentes de cada una de las divisiones de la entidad. Esta estimación se realizará, considerando el supuesto de qué escenario y en qué momento se estresa más al elemento analizado; esto permite identificar si la afectación más apremiante ocurre en alguna fecha específica. Así mismo, se debe calcular el costo de interrupción para cada producto.

El MTPD de cada producto será definido por el tiempo más pequeño de todas las respuestas dadas para los diferentes tipos de impacto de los umbrales no tolerables y siempre será estimado considerando el "peor escenario" o más estresante para lo entidad.

Con el MTPD definido, es necesario establecer **el Nivel Mínimo Aceptable de Operación (MBCO)** para cada producto y/o servicio, el MBCO corresponde al mínimo nivel del productos o servicio que puede brindarse para que la entidad alcance sus objetivos durante un incidente disruptivo.

El siguiente paso, es estimar el **Tiempo Objetivo de Recuperación (RTO)**, el cual es un valor expresado en tiempo entre cero y el MTPD definido cada producto. En la medida que más se acerque a cero, la alternativa estratégica de continuidad y recuperación será más costosa; en cambio, mientras más se acerque al MTPD, la alternativa será más riesgosa. El RTO más apropiado será aquel que genere el mejor balance entre el costo y el riesgo. Las dependencias que existen entre productos / servicios / instalaciones / unidades de negocio / procesos / actividades deben también analizarse para aplicar o corregir los MTPDs y RTOs de aquellos de los que dependen, considerando que deben ser menores los MTPDs y RTOs de los dependientes.

Para el registro del MTPD, MBCO y RTO se utilizará la siguiente tabla:

Producto/ Servicio	**Escenario más estresante**	**Costo de interrupción**	**¿En cuánto tiempo se alcanzan los umbrales no tolerables? 4h, 8h, 1día, 2 días, 3 días, 1 sem, 1 mes+**					**MTPD final**	**MBCO**	**RTO**
			Personas	Económico	Imagen	Legal	Clientes			
Producto 1										
…										
Servicio 1										

Tabla 32. Matriz para estimar MTPD, MBCO y RTO

Estimar MTPDs y RTOs deberá ser una labor permanente en la entidad debido a los cambios que ésta pueda tener en su entorno, la aparición de nuevos servicios (o nuevas instalaciones, o nuevas unidades funcionales) y nuevos procesos y tecnología hará necesario que las prioridades de urgencias de recuperación sean revaluadas. Si no se actualizan las prioridades de recuperación en un tiempo prudente puede pasar un incidente disruptivo donde la toma de decisiones será improvisada debido a la información desactualizada con la que se cuenta.

Paso 4. Priorización de productos y servicios

Después de definir MTPDs y RTOs, los productos y servicios de la entidad deben agruparse desde la menor franja de tiempo de recuperación, es decir productos o servicios que se recuperan en horas, los que se recuperan en días, los que se recuperan en semanas y los que se recuperan en un mes o más. La prioridad de recuperación vendrá dada por aquellos productos y servicios

que tengan un RTO menor a dos días. En este paso también se debe identificar los procesos relacionados que permiten la entrega de los productos y servicios en análisis, estos procesos heredan los MTPDs y RTOs de dichos productos.

Producto/ Servicio	MBCO	Procesos	MTPD	RTO (de menor a mayor)
Producto 1				
Servicio 1				
Producto 2				
Servicio 2				
Producto 3				
Servicio 3				
…				

Tabla 33. Matriz para priorizar productos y servicios de la entidad

Paso 5. Identificación de recursos críticos

En esta etapa se reúne información detallada sobre los recursos mínimos requeridos para continuar, recuperar y reanudar los procesos del negocio que soportan los productos y servicios de la entidad, durante un incidente disruptivo. La siguiente tabla explica algunas consideraciones para realizar esta identificación.

Recurso	Consideraciones para tomar en cuenta
Personas / Puestos	Perfiles mínimos necesarios para continuar operando los productos.

Tecnología de Información	Considerar los servicios de TI que se deberán utilizar en el momento del incidente disruptivo, así como la información u otros datos necesarios para el servicio o actividad.
Infraestructura / Edificios / Instalaciones	Consideran las alternativas de lugares de trabajo u otras sedes desde donde se podría continuar operando durante el incidente disruptivo.
Transporte	Considerar las facilidades de movilidad con las que la entidad cuenta para ser brindadas al personal durante el incidente disruptivo
Comunicaciones	Considerar las capacidades de comunicación entre el personal con las que cuenta la entidad y que podrían estar disponibles durante el incidente disruptivo.
Servicios públicos	Considerar las alternativas de la provisión de energía eléctrica, agua y telefonía que puedan utilizarse durante el incidente disruptivo.
Proveedores / Partes Interesadas	Considerar aquellos que soportan los productos críticos, participación de partes interesadas como clientes, autoridades públicas, entes reguladores y supervisores, así como la comunidad en general.

Tabla 34. Consideraciones para identificar recursos críticos

Como resultado de este paso, se obtiene el detalle de recursos mínimos de continuidad de los productos y servicios de la entidad, considerando el MBCO definido previamente. En la siguiente tabla se ilustra la necesidad de recursos mínimos de un producto o servicio, en términos de escalas de tiempo.

Nombre de Producto/Servicio		Tiempo a partir del cual es necesario el recurso						
Recurso	**Comentarios**	**4h**	**8h**	**1día**	**2 días**	**3 días**	**1 sem**	**1 mes+**
Personas/Puestos								
Nombre o cargos								
Tecnología de Información								
Listado de servicios informáticos								
Infraestructura / Edificios								
Detalle de instalaciones - sedes								
Transporte								
Detalle de recursos								
Comunicaciones								
Detalle de recursos								
Servicios públicos								
Listado de servicios								
Proveedores / Partes Interesadas								
Listado de proveedores/servicio								

Tabla 35. Tiempo de recuperación de recursos mínimos

Paso 6. Elaboración de Informe y aprobación de resultados y difusión

Una vez completado el análisis de la información, se debe preparar un informe de resultados del BIA que deberá ser revisado y avalado por las gerencias correspondientes y aprobado por el Comité de Riesgos de la entidad. Un informe típico debe incluir los siguientes elementos:

- Priorización de productos y servicios, con un orden cronológico de recuperación de estos.
- Identificación y análisis de recursos e interdependencias.
- Recomendaciones claras que ayuden al diseño y selección de estrategias de continuidad y recuperación.

El BIA debe ser revisado y actualizado periódicamente, tomando en cuenta cambios en el plan estratégico de la entidad, así como cuando existan lanzamientos de nuevos productos o servicios, cambios significativos en los procesos o infraestructura tecnológica y que puedan afectar de manera relevante las actividades y procesos críticos de la entidad.

5.4.3. Etapa 3. Análisis de riesgos de continuidad

La evaluación de riesgos o amenazas de continuidad se realiza a fin de identificar las principales amenazas que podrían interrumpir los procesos críticos de la entidad. Es importante establecer opciones preventivas frente a estas amenazas, definiendo medidas de protección en los lugares donde se ejecutan estos procesos. Para poder realizar esta evaluación se puede utilizar distintos métodos o buenas prácticas reconocidas internacionalmente, el estándar más recomendado es el análisis de riesgos planteado en la ISO 31000, el cual valora el riesgo como la combinación de la probabilidad y el impacto que genera un evento disruptivo.

Es necesario acotar los eventos de riesgo que pueden resultar de interés de la continuidad de negocio, para ello se debe enfocarse en las consecuencias resultantes de las amenazas cuando afectan los principales activos y recursos de la entidad. Algunos ejemplos son: "afectación del personal ante la ocurrencia de un terremoto", "afectación de la edificación y centros de procesamiento de datos ante la ocurrencia de un incendio", "afectación de los proveedores ante la ocurrencia de una pandemia".

Lineamientos para realizar el análisis de riesgos de continuidad de negocio

Para la ejecución de este análisis, y en alineación a la normativa nacional y a estándares internacionales, se deben considerar los siguientes lineamientos:

- El nivel de riesgo debe entenderse en función a los procesos críticos de la entidad y el riesgo de interrupción de estos y los recursos (personal, locales, tecnología, datos, suministros y grupos de interés).
- La entidad debe establecer, implementar y mantener un proceso formal documentado de análisis de amenazas de continuidad que de forma sistemática identifique y evalúe el riesgo de incidentes de interrupción en dicha entidad. Para lo anterior, la entidad debe realizar las actividades siguientes:
  - Identificar las amenazas de interrupción capaces de afectar los procesos y sistemas críticos de la entidad, información, personas, activos, partes interesadas y otros recursos de soporte; y
  - Analizar y evaluar las amenazas identificadas y definir planes de tratamiento según aplique, acordes con los objetivos de continuidad del negocio y de acuerdo con el apetito de riesgo de la entidad.
- Dado que es difícil extender el Análisis de Riesgos a toda la entidad, se debe centrarse en los recursos necesarios para operar las actividades más urgentes de la entidad (es decir, siguiendo el BIA).
- La Evaluación de Riesgos puede identificar concentraciones de riesgos inaceptables y lo que se llama "puntos únicos de fallo". Estos deben ser comunicados lo antes posible a quien realice la función de Continuidad de Negocio, además de presentarle opciones para resolver el problema. La decisión estratégica de mitigar, transferir o aceptar el riesgo debe estar documentada y ratificada.
- Para el caso de las entidades que posean agencias u otras locaciones, deben realizar la evaluación de riesgos según su zona geográfica.
- El alcance de la evaluación de riesgos debe considerar las siguientes ubicaciones, en los casos que aplique:
  - Sedes principales y alternas de operaciones.
  - Sede principal y alterna de comando del comité de crisis.
  - Centro de procesamiento de datos principal y alterno.
  - Área para atención de personas.

- El proceso que se llevará a cabo incluye las siguientes etapas:

Figura 43. Etapas de la evaluación de riesgos de continuidad de negocio

Paso 1. Identificación de riesgos

El primer paso es identificar todos los riesgos que tengan la capacidad de interrumpir las operaciones de la entidad, ya sean estos naturales (huracanes, terremotos, tormentas tropicales y erupciones volcánicas), tecnológicos (fallas de ingeniería, fallas en los equipos y cortes de energía) o de causas humanas (como incendios provocados, actos de terrorismo, ataques cibernéticos y disturbios sociales). Resulta demasiado difícil tener una previsión perfecta sobre la ocurrencia de los riesgos, y aunque el pasado no siempre es la mejor manera de saber lo que sucederá en el futuro, puede ayudar a identificar posibles desastres.

Paso 2. Evaluación de riesgos

La evaluación del riesgo promueve la comprensión de los riesgos para las funciones priorizadas y sus dependencias y las consecuencias potenciales de un incidente de interrupción. Esta comprensión posibilita que la entidad seleccione estrategias de continuidad de negocio adecuadas.

Con un listado de riesgos identificados, el siguiente paso es evaluar cada uno de ellos en función de los impactos que pudiera generar a las funciones y productos críticos de la entidad, así como la probabilidad de que ocurra una situación de este tipo. Esta valoración brinda un proceso estructurado para el análisis de riesgos en términos de las consecuencias y probabilidad antes de decidir acerca del tratamiento adicional que se puede necesitar. La siguiente tabla puede ser utilizada para recopilar esta información.

Riesgo	Probabilidad (P)	Impacto (I)	Categoría (PxI)
Riesgo 1			
Riesgo 2			
…			

Tabla 36. Análisis de riesgos

Para la evaluación de riesgos se sugiere utilizar un mapa como se muestra en la figura 44, donde se ubiquen de forma visual cada uno de los riesgos que amenaza la entidad en función de su criticidad. Esta matriz se define identificando escalas de probabilidad y escalas de impacto. Si en la entidad existe una unidad de riesgos se recomienda alinearse al tamaño de la matriz existente.

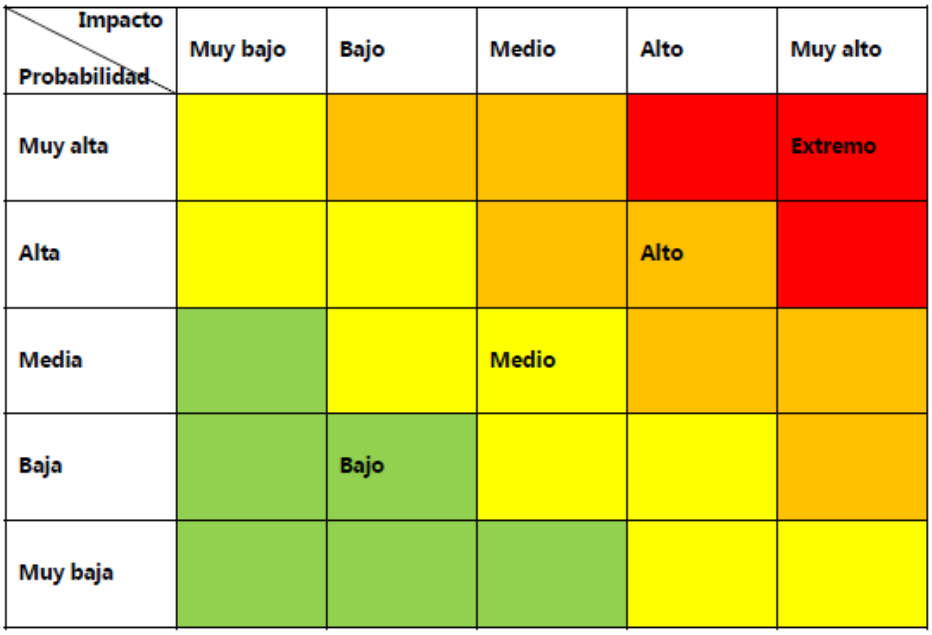


Figura 44. Matriz para la evaluación de riesgos

La escala de **probabilidad** está definida en base la incidencia del evento de riesgo en el tiempo considerando el contexto aplicable para la entidad.

Escala	Descripción
Muy Alta	Ocurre el incidente al menos una vez al año en los últimos cinco años
Alta	Ocurre al menos una vez cada cinco años en los últimos 25 años
Media	Ocurre al menos una vez cada 10 años en los últimos 50 años
Baja	Ocurre al menos una vez cada 25 años
Muy Baja	Ocurre en espacios de tiempos mayores de 25 años

Tabla 37. Escalas y criterios de probabilidades

La escala de impacto está definida en base al nivel de daño que podría causar en la entidad, en continuidad se entiende el daño como el tiempo de indisponibilidad o interrupción del incidente, así como la afectación en las personas y en los principales recursos de la entidad. Para la evaluación y estimación del impacto de un incidente disruptivo se pueden considerar los siguientes criterios:

Escala	Descripción
Muy Alta	• Estimación del tiempo de interrupción mayor al MTPD. • Indisponibilidad del 50% o más de funcionarios de una misma área clave. • Pérdidas muy altas de activos o ingresos. • Difusión negativa externa a nivel internacional. • Pérdida de participación de mercado mayor al 20%.
Alta	• Estimación del tiempo de interrupción entre ((RTO + MTPD) / 2) y MTPD. • Indisponibilidad del 25% al 50% de funcionarios de una misma área clave. • Pérdidas altas de activos o ingresos. • Difusión negativa externa a nivel nacional (país). • Pérdida de participación de mercado entre el 15 y el 20%.

Escala	Descripción
Media	• Estimación del tiempo de interrupción entre RTO y ((RTO + MTPD) / 2) • Indisponibilidad del 10% al 25% de funcionarios de una misma área clave, por un mismo evento. • Pérdidas medias de activos o ingresos. • Difusión negativa externa a nivel departamental. • Pérdida de participación de mercado entre el 7 y el 15%.
Baja	• Estimación del tiempo de interrupción entre (RTO / 2) y RTO • Indisponibilidad de menos del 5% de funcionarios de una misma área clave. • Pérdida baja de activos o ingresos. • Difusión negativa externa a nivel local y/o de organización a nivel nacional. • Pérdida de participación de mercado entre el 2 y el 7%.
Muy Baja	• Estimación del tiempo de interrupción entre 0 y (RTO / 2) • Indisponibilidad temporal de algunos funcionarios no críticos de una misma área clave por un mismo evento. • Pérdida muy baja de activos o ingresos. • Difusión negativa a nivel interno (proceso, equipo de trabajo) • Pérdida de participación de mercado menor al 2%.

Tabla 38. Escalas y criterios de impacto

Habiendo definido e identificado los posibles eventos de riesgo, la matriz de riesgo con sus respectivas escalas de probabilidad e impacto se procede a estimar la probabilidad de ocurrencia del evento de riesgo y su impacto, esto se realiza convocando a los expertos en la entidad que conocen sobre las amenazas y la efectividad de los controles implementados, los cuales considerando su juicio experto determinan el nivel de riesgo resultante.

Paso 3. Tratamiento de riesgos

Esta etapa busca aplicar nuevas medidas o controles donde resulten riesgos extremos, altos o medios, o en todo caso mejorarlos, para ayudar a reducir el nivel de riesgo. La prioridad de

implementación de las medidas nuevas o por mejorar se dará en función del mayor nivel de riesgo determinado, es decir en primer lugar no deben permitirse riesgos extremos, resueltos éstos no deberán permitirse riesgos altos, y así también luego con los riesgos medios.

Considerando los resultados del BIA y del análisis de riesgos, la entidad debe identificar y aplicar controles o medidas preventivas que:

- Reduzcan la probabilidad de que los productos y servicios críticos sufran interrupciones.
- Disminuyan el tiempo de una eventual interrupción.
- Limiten el impacto que una paralización de las actividades críticas pueda provocar en la entidad.
- Incrementen la fortaleza del negocio mediante la eliminación de puntos de fallo únicos.

Esto permite definir tratamientos que consideren las actividades para prevenir y evitar en la medida de lo posible los riesgos que impactan en la disponibilidad de los productos críticos. Los tratamientos predefinidos según el nivel de riesgos pueden ser los siguientes:

Continuidad de negocio

Cuando las entidades definen planes de continuidad de negocio para productos y servicios fundamentales, deben considerar los RTO de estos y evaluar las estrategias de continuidad y recuperación descritas en el apartado 4.4.4 Diseño y Selección de Estrategias de Continuidad de Negocio.

Las estrategias de continuidad de negocio buscan mejorar la flexibilidad de la entidad ante una interrupción, asegurando que las actividades críticas continúen o se recuperen a un nivel mínimo aceptable y en plazos estipulados en el BIA.

Transferencia

Para algunos riesgos, la mejor respuesta puede ser transferirlos, generalmente esto se logra mediante la contratación de un seguro convencional o por medio de pago a un tercero para que este asuma el riesgo de otra forma. Esta medida de tratamiento es particularmente buena para

poder mitigar los riesgos financieros o riesgos a los que puedan exponerse los activos. Los riesgos podrán transferirse para reducir la exposición de la entidad a las amenazas o porque otra organización es más capaz de gestionar el riesgo de forma eficaz.

La adquisición de un seguro podrá formar parte de la estrategia de tratamiento de riesgo y proporcionará alguna indemnización económica por algunas perdidas. Sin embargo, no todas las pérdidas son plenamente asegurables (por ejemplo, daños en la reputación, incidentes fuera de cobertura, pérdida de valor, reducción de participación de mercado o pérdidas humanas). Lo más recomendable y habitual es que la cobertura de seguro se use en combinación con una o más estrategias.

Aceptación

Un riesgo podría ser aceptable sin que sea necesario tomar otras medidas. Incluso si no es aceptable, la habilidad para hacer algo en previsión de los riesgos podría estar limitada, o el coste de tomar alguna medida podría resultar desproporcionado con respecto al beneficio obtenido. En estos casos, la respuesta podrá ser tolerar el nivel de riesgo existente si la alta dirección estima que el riesgo es aceptable y que corresponde al apetito de la entidad. En algunas circunstancias, el impacto de un riesgo puede encontrarse fuera del apetito por el riesgo normal de la entidad, pero, debido a la baja posibilidad de que se produzca el riesgo y/o debido al alto coste económico que supone el control, la alta dirección podrá aceptarlo.

Cambio, suspensión o terminación

En algunas circunstancias, podría ser apropiado cambiar, suspender o terminar el servicio, producto, actividad, función o proceso. Esta opción solo puede considerarse cuando no exista conflicto con los objetivos, cumplimiento legal y expectativas de grupos de interés de la entidad.

Paso 4. Monitoreo de riesgos

Los procesos de monitoreo de riesgos que realice las entidades deberán englobar todos los aspectos del proceso de gestión de riesgos con el objetivo de:

- Asegurar que los controles son eficaces y eficientes, tanto en el diseño como en la operación.
- Analizar y aprender con los eventos materializados.
- Detectar alteraciones en el contexto externo e interno, que pueden requerir la revisión de los tratamientos del riesgo y de las prioridades.
- Identificar los riesgos emergentes.

El progreso en la implementación de los planes de tratamiento del riesgo proporciona una medida del rendimiento. Los resultados pueden ser incorporados en la gestión global del rendimiento de la entidad, en su medición y en las actividades de reporte interno y externo.

5.4.4. Etapa 4. Diseño y selección de estrategias de continuidad de negocio.

El diseño y selección de estrategias se centran en la determinación de los arreglos operativos más apropiados para lograr el nivel mínimo aceptable de operación (MBCO) definido. En la mayoría de los casos, la amplitud y profundidad de las estrategias elegidas se ven influidas por las necesidades de recuperación de productos y servicios críticos, incluidas la urgencia, la complejidad y los tipos de recursos.

Las estrategias que se definan deben también considerar el costo de su implementación y deberán satisfacer el RTO establecido. Si fuera necesario puede hacerse un ajuste al valor del RTO por consideraciones de factibilidad técnica o financiera.

Las opciones pueden ir desde las más exigentes y costosas a las menos exigentes y más económicas, definiendo con ello cuán "caliente" o "fría" debe ser la alternativa elegida. Las alternativas más "calientes" dividen las operaciones en dos o más partes y reubicar dichas partes de forma estratégica, fuera del alcance de riesgos de mayor cobertura geográfica; tienen infraestructura vacía o equipada esperando ser ocupada de inmediato en cuanto pase un evento. Las alternativas "tibias" tienen esquemas trasportables a otros los lugares de operación; o un espacio en uso que será desocupado para ser usado por las actividades más urgentes.

Las alternativas más "frías" pasan por tener casi nada pre montado esperando que pase el evento o hasta inclusive no hacer nada en el momento actual y dejar todo para cuando pase el incidente de continuidad y buscar reaccionar en dicho momento.

El siguiente grafico ilustra el costo-beneficio de las opciones de estrategias de Continuidad de Negocio. Todas las alternativas pueden ser implementadas de manera propia, es decir mantenidas y operadas por la propia entidad, o buscar un tercero que se encargue de brindar dichas alternativas.

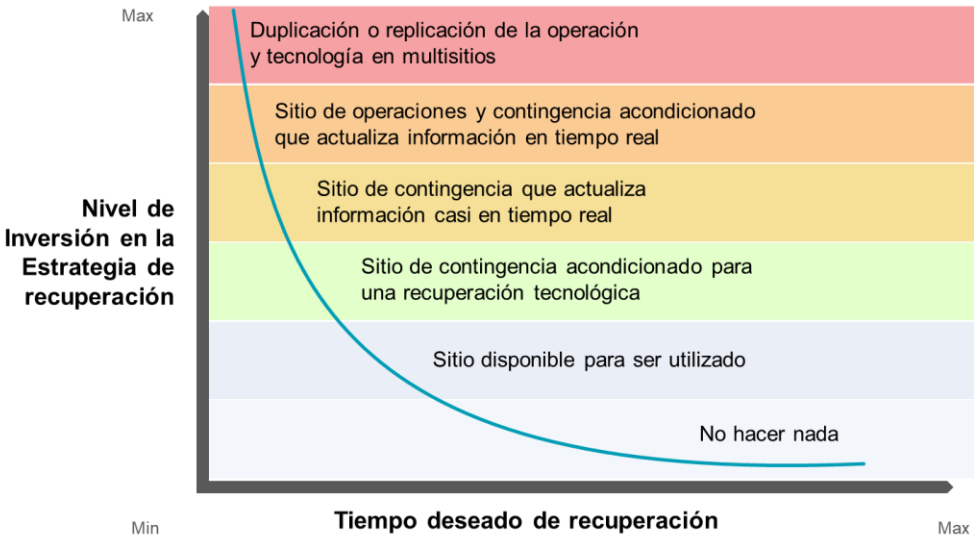


Figura 45. Costo-beneficio de las opciones de estrategias de continuidad de negocio

Esta etapa consta de los siguientes elementos:

1. Evaluación y selección de opciones de estrategia
2. Medidas preventivas ante amenazas específicas
3. Estrategias de Continuidad y Recuperación
4. Consolidación de los recursos de recuperación
5. Informe sobre selección y desarrollo de estrategias

Paso 1. Evaluación y selección de opciones de estrategia

La identificación y selección de estrategias debe basarse en las necesidades de recuperación de recursos de los productos y servicios críticos. Esta información ayuda a establecer los criterios para evaluar la opción más adecuada. Aunque el factor tiempo desempeña un papel vital en el proceso de selección, también deben tenerse en cuenta los siguientes aspectos con respecto a la selección de las estrategias de recuperación y continuidad de negocio de la entidad:

- **Requisitos operativos**: Se refiere a lograr el estándar o nivel mínimo de prestación de servicios para cumplir con las obligaciones contractuales y reglamentarias. La elección de las diferentes alternativas de recuperación depende de las necesidades de la entidad: tiempos de recuperación objetivo (RTO), costos, recursos humanos, recursos técnicos, etc. Lo más común y recomendable es adoptar una combinación de las estrategias de recuperación para los distintos recursos críticos.

- **Costo**: Esto está directamente relacionado con la velocidad de recuperación. Un RTO más corto representa un mayor costo de implementación, mientras que un RTO más largo tiende a proporcionar una opción más barata. La decisión puede basarse en un análisis de costo-beneficio, que evalúa el impacto operacional y financiero de la función crítica frente al costo de implementar la opción de recuperación.

- **Fases de recuperación**: Aunque es importante abordar todas las fases de la recuperación - Continuidad (fase inmediata), Reanudación (fase de estabilización) y Restablecimiento (fase de negocios como de costumbre) - la decisión de la Alta Dirección a menudo depende de la criticidad y el impacto de los productos y servicios individuales. En muchos casos, los productos con un impacto significativo requieren opciones de recuperación que puedan mantener un nivel mínimo de operación definido para cumplir con los requisitos corporativos y obligatorios. Por el contrario, aquellos con menor impacto pueden adoptar opciones de fase posterior, como la reparación y el restablecimiento.

Recomendaciones para la evaluación y selección de las estrategias de continuidad

Las estrategias de continuidad y recuperación deben considerar los siguientes recursos:

1. **Personal**: La estrategia que se defina en este ámbito debe considerar en todo momento mantener las principales habilidades y conocimiento necesario para asegurar la continuidad de los productos y servicios de la entidad, suministrar información para proveedores y para gestionar y retener el conocimiento. Es recomendable formular un Plan de capacitación y formación para el personal, el cual permita identificar cuáles son las funciones que la organización llevará a cabo con el personal a lo largo de un tiempo determinado. Este plan debe tener un alcance tanto para empleados actuales como los de nuevo ingreso, y debe ser para las áreas estratégicas, de negocio y de soporte.

2. **Instalaciones**: Se debe verificar que las instalaciones alternas permitan llevar a cabo los procesos que apoyen a las operaciones de la entidad, estas instalaciones alternas deben contar con la infraestructura necesaria que permita continuar con la operación a un nivel aceptable. Para otro tipo de escenario puede tomarse la medida para trabajar desde casa o vía remota. Las instalaciones alternas con las que cuente la entidad van a depender directamente del presupuesto que posea para el Plan de Continuidad de Negocio.

   En algunos casos las entidades pueden optar por instalaciones multi-sitio, este enfoque es ideal para entidades que operan en varios sitios diferentes donde se entregan los productos y servicios críticos. Tener ubicaciones geográficamente dispersas minimiza la probabilidad de que los sitios se vean afectados por los mismos incidentes disruptivos. Si un incidente hace que un sitio no esté disponible, los productos críticos se pueden transferir a otras ubicaciones para minimizar el impacto en las operaciones.

3. **Información**: Se debe verificar que se posea la información necesaria para dar continuidad a las operaciones, esta información debe cumplir con las características de seguridad indispensables, integridad, disponibilidad y confidencialidad, aunque se esté en las instalaciones alternas. Como parte de las estrategias de información, y siendo este tema muy sensible, es necesario el disponer de copias de seguridad actualizadas, accesibles y protegidas, de datos y aplicaciones críticas, a las que se pueda recurrir como contingencia cuando la ubicación principal, deja de operar o pierde conectividad.

Como primera opción, el enfoque tradicional de la recuperación ante desastres requiere el disponer de un espacio físico secundario en un segundo data center para realizar copias de seguridad de las operaciones críticas que se desarrollan en el sitio primario. Esta opción implica una serie de costes operacionales que implica una inversión adicional en equipos e infraestructura para replicar la infraestructura principal. Una segunda opción es contar con un proveedor de infraestructura como servicio que permita disponer de un respaldo en la nube. Esta opción permite dimensionar la infraestructura secundaria de apoyo según las necesidades de la entidad y pagar solo por lo que se utilice. Además, se facilita adicionar espacio de alojamiento cuando se requiera, sin necesidad de adquirir y configurar nuevos equipos. Un aspecto importante de las copias de seguridad, tanto si son en instalaciones en un data center o en la nube, es que han de estar en una ubicación geográfica diferente al de la infraestructura principal.

4. **Tecnología**: El tipo e infraestructura tecnológica depende del tipo de funciones y productos que realice cada entidad, lo importante a verificar es que la tecnología que se posea sea suficiente para poder ejecutar la operación a un nivel aceptable, predefinido previamente y ante un escenario de contingencia. Para esta estrategia se debe elegir la infraestructura según las necesidades y el presupuesto de la entidad.

   Para una mejor implementación de la estrategia de Tecnología se sugiere elaborar Inventarios de los activos y recursos tecnológicos, indicando la criticidad que cada elemento representa para las operaciones. Entre los inventarios sugeridos se tienen: Sistemas de Información Críticos, Hardware de Redes, servidores, usuarios y comunicaciones, Software y relaciones entre cada uno de estos elementos.

   Las estrategias tecnológicas variaran significativamente entre entidades según el tamaño, naturaleza y complejidad del negocio. Deben desarrollarse estrategias de recuperación específicas para salvaguardar, sustituir o restablecer tecnologías especializadas o hechas a la medida con plazos de entrega dilatados.

En todo caso, la entidad debe plantearse el escenario donde sea necesario realizar operaciones manuales antes de recuperarse plenamente los servicios y recursos tecnológicos.

5. **Registros vitales**: Adicionalmente de la tecnología, de la información y del personal que apoyará en la continuidad de negocio, es necesario considerar algunos recursos necesarios para que las actividades puedan realizarse, como:
   - Hojas membretadas.
   - Formatos necesarios para llevar a cabo alguna actividad.
   - Documentos que se necesiten para el trabajo diario.
   - Documentos legales como contratos de los proveedores.

   Estos ejemplos son identificados como registros vitales. Para contar con ellos en un escenario de contingencia, dónde lo más factible es continuar con la operación en un sitio alterno, se debe asegurar que los registros vitales estén disponibles. Algunas de las recomendaciones para solucionar este requerimiento son:
   - Contratar los servicios de un proveedor especializado en este tema.
   - Tener instalaciones alternas que sirvan como bóveda para el resguardo de estos recursos.

6. **Suministros**

   La entidad debería identificar y mantener un inventario con los suministros que dan soporte a las actividades críticas, entre estos suministros puede mantener:
   - Almacenaje de suministros adicionales en una local alternativo.
   - Acuerdos con terceros para la entrega de material en periodos cortos de tiempo.
   - Incrementar el número de proveedores (p.ej. diversos proveedores de Internet).

Paso 2. Medidas preventivas ante amenazas específicas

Este paso consiste en aplicar medidas preventivas para evitar incidentes que de no ser gestionados se vuelvan en una interrupción mayor. A continuación, se presenta algunos ejemplos de estas medidas o controles frente amenazas o riesgos específicos que puede sufrir la entidad:

Riesgo	Medida preventiva
Interrupción eléctrica	• Fuentes alternas de generación eléctrica: UPS y plantas eléctricas. • Mantenimiento de las fuentes alternas de generación eléctrica. • Lámparas de emergencia.
Fallos en Hardware	• Política de sustitución y obsolescencia de equipo. • Monitoreo y capacidad de redundancia entre servidores. • Contratos de mantenimiento preventivo y correctivo. • Condiciones físicas y ambientales (limpieza, humedad, temperatura).
Fallas en Software	• Desarrollo local de aplicaciones (metodologías/ estándares). • Cambios y configuración en aplicaciones.
Fallas en Comunicaciones	• Soporte técnico de los equipos utilizados. • Mantenimiento preventivo y correctivo de los equipos de comunicación.
Desastres naturales	• Pólizas de seguro vigentes. • Brigadas de atención ante situaciones de emergencia. • Capacitación al personal. • Rutas de evacuación, iluminación de pasillos y salidas de emergencia.
Incendio	• Pólizas vigentes de seguro. • Sistema automático y manual contra incendios. • Detectores de humo revisados regularmente.
Fallas en Respaldos	• Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación, y configuración de los sistemas. • Facilidades y protección para el almacenamiento dentro y fuera de sitio. • Documentación actualizada sobre procedimientos de respaldo y recuperación.
Virus	• Programa antivirus instalado en computadoras y servidores. • Configuración y actualización del antivirus. Políticas para el ataque de virus. • Capacitación al personal para identificar potenciales fuentes de ataque de virus.

Riesgo	Medida preventiva
Violaciones a la Seguridad física	• Control de ingreso a instalaciones y área de servidores y equipos de comunicación. • Capacitación al personal para detectar situaciones que puedan representar riesgo. • Circuitos cerrados de televisión, sensores de movimiento, alarmas.
Intrusión (Hackeo)	• Control de acceso a las aplicaciones y políticas de acceso lógico. • Administración y configuración de “firewalls”. • Disponibilidad de herramientas para el monitoreo de la seguridad.
Recurso Humano	• Capacitación. • Documentación de las funciones del personal.
Pandemia	• Distanciamiento social. • Teletrabajo y Protocolos de actuación ante casos de contagio

Tabla 39. Ejemplo de medidas preventivas

Paso 3. Estrategias de continuidad y recuperación

Existen diversas estrategias que pueden implementarse para la continuidad y recuperación de los productos críticos de la entidad, ya sea de forma total o parcial, según la naturaleza, capacidad y tamaño de estas.

Antes de implementar estas estrategias, las entidades deben realizar las gestiones pertinentes a fin de determinar la viabilidad técnica y financiera de llevarlas a cabo.

Recurso crítico	Estrategia de recuperación
Personas que participan en productos críticos	• Documentar actividades críticas. • Capacitación y conocimiento compartido. • Separación de tareas claves. • Planeación de la sucesión puestos clave.
Instalaciones	• Instalaciones alternativas, acuerdos recíprocos y teletrabajo.

Recurso crítico	Estrategia de recuperación
Tecnología.	• Replicar centro de cómputo en sitio alterno. Los datos, unidades de red y/o arreglos de almacenamiento están sincronizados en tiempo real. • Sistema de alimentación ininterrumpida (UPS) para los centros de datos primarios y de respaldo y las infraestructuras críticas. • Redundancia de equipos y comunicaciones. Copias de software crítico.
Información y Documentación.	• Copias de seguridad y procedimientos de recuperación. • Datos disponibles desde replicación en línea. • Disponibilidad de información basada en papel.
Proveedores / Insumos	• Contacto con proveedores alternativos y acuerdos con terceros. • Envío y almacenamiento de recursos críticos en ubicaciones alternativas.
Transporte	• Capacidad adicional proporcionada por una empresa de transporte. • Acuerdos para transportar al personal a sitios alternativos o su casa.
Comunicación interior y exterior	• Mantener, adquirir y montar un sistema de notificación masiva y plataforma de colaboración para ser usados durante el incidente disruptivo; adquirir teléfonos satelitales; tener acuerdos pre-establecidos con medios y emisoras para difundir mensajes claves en caso no haber otro medio disponible.
Relación con regulador y supervisor	• Establecer de antemano canales y responsabilidades para notificar en cuanto ocurra el incidente disruptivo.
Relación con clientes	• Contar con procedimientos de comunicación en crisis considerando posibles escenarios de afectación de la imagen y priorizando las audiencias afectadas.
Servicios civiles de emergencia.	• Recomendaciones de rutas de evacuación y puntos de reunión. • Participación en simulacros.

Tabla 40. Estrategias de continuidad y recuperación

Paso 4. Consolidación de recursos de continuidad y recuperación

Los recursos de recuperación tienen una gran influencia en la selección de estrategias de continuidad y están directamente relacionados con los requisitos definidos en la BIA. Esta etapa evalúa los niveles de recursos necesarios para implementar las soluciones de continuidad.

Consta de tres siguientes actividades:

1. **Compilar**: recopilar y validar todos los requisitos de recursos de las estrategias de continuidad seleccionadas, incluidas las admitidas por proveedores de terceros.
2. **Comprobar**: comparar y evaluar los requisitos con la lista de inventario de recursos actual de la entidad y los resultados del BIA. Esto garantiza que las demandas propuestas son coherentes con la disponibilidad actual y no hay conflictos de requisitos entre las soluciones.
3. **Confirmar**: una vez que se han finalizado los requisitos de recursos, la información se prepara y se propone para aprobación de la alta dirección de la entidad. Esto genera una serie de proyectos para implementar las estrategias y soluciones de continuidad de negocio.

Paso 5. Informe sobre la selección y desarrollo de estrategias

Como mínimo, un informe completo de desarrollo de la estrategia debe incluir los elementos:

1. **Una lista de opciones de estrategia de continuidad**: establece la estrategia de continuidad de alto nivel para cada producto y servicio crítico. Cada opción seleccionada debe abordar las preocupaciones de la administración en términos de requisitos de negocio, el costo de implementación y cómo la opción logra los objetivos de recuperación. Esto debería estar respaldado por un análisis de costo-beneficio.
2. **Descripción de cada estrategia**: cada solución de continuidad debe incluir los costos operativos, los términos y condiciones, el alcance de la planificación, la disponibilidad de recursos, el calendario de implementación y la adaptabilidad para admitir otras funciones y productos críticos.
3. **Consideraciones operativas**: esto incluye los supuestos y limitaciones operativas de cada solución de continuidad: sus fortalezas y debilidades en términos de efectividad, aplicaciones y rendimiento bajo ciertas condiciones.

4. **Gestión de proyectos**: cubre los aspectos de gestión de proyectos del desarrollo de la estrategia de recuperación y continuidad, es decir, la duración, las tareas definidas, los recursos necesarios (dónde y cómo protegerlas) y los entregables.

5.4.5. Etapa 5. Implementación de la estrategia – documentación de planes.

En esta etapa tiene lugar la implementación y formalización de la estrategia de continuidad para garantizar la continuidad de productos, servicios, actividades críticas y la gestión de incidentes. Esto se logra por medio de la formulación de planes de continuidad, siendo este un documento que busca ser consultado y utilizado durante un incidente disruptivo. Este proceso parte de la información identificada previamente relativa a los productos críticos, amenazas, medidas de mitigación y estrategias para la continuidad o recuperación.

Paso 1. Estructura de respuesta a incidentes disruptivos

Una actividad importante en la implementación de la estrategia de continuidad es la definición de una estructura de respuesta a incidentes disruptivos que permita confirmar la naturaleza del incidente, tomar el control de la situación y comunicar a las partes interesadas el mismo evento y sus impactos, así como las soluciones de respuesta a realizar. Estos equipos deben disponer de planes, procesos y procedimientos para la gestión de incidentes disruptivos. En la siguiente figura se observan 3 periodos bien delimitados que corresponden a la respuesta al incidente, la continuidad del negocio y la recuperación del estado normal.

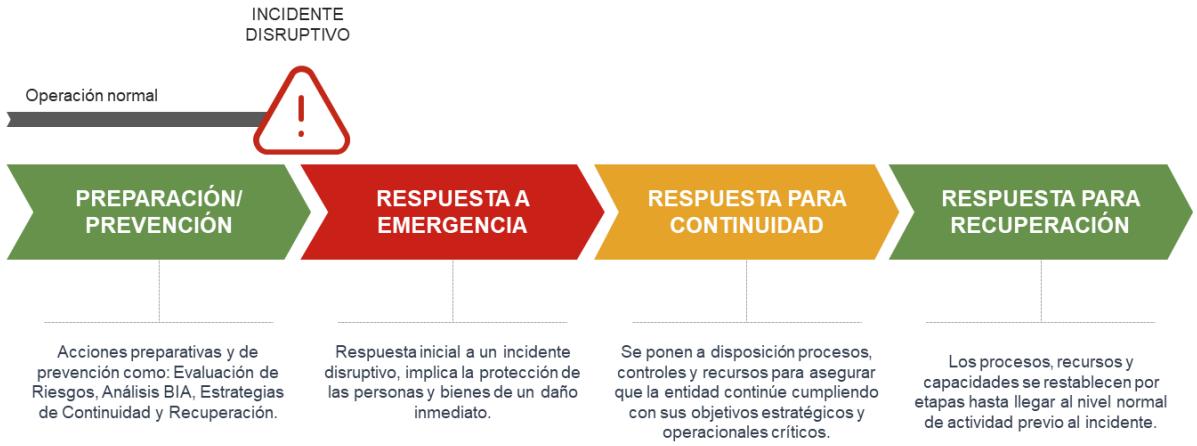


Figura 46. Línea de tiempo en la respuesta de incidentes disruptivos

Esta estructura debe basarse en la conformación de equipos que intervienen en acciones de prevención y en la respuesta de incidentes potenciales y reales, su composición y tamaño pueden variar en función a la naturaleza y complejidad de cada entidad, así como en las estrategias de continuidad y de recuperación definidas. No obstante lo anterior, se pueden designar personas o conformar equipos por tema de especialidad y por funciones claves que serán llevadas a cabo durante la activación y ejecución del Plan de Continuidad:

- **Equipo de respuesta a incidentes**: Responsables de evaluar y minimizar el impacto que un incidente puede generar en la entidad de forma que no se tenga que recurrir a la activación del Plan de Continuidad.
- **Comité de crisis**: Responsable de activar el Plan de Continuidad de Negocio y dirigir las acciones durante la contingencia.
- **Equipos de recuperación**: Asume la recuperación en servicio de la infraestructura tecnológica y otros recursos necesarios y vitales para la continuidad de las operaciones de la entidad.
- **Equipos de logística**: Responsable de reunir todos los medios y recursos necesarios para contribuir a la reactivación de la actividad.
- **Equipos de relaciones públicas**: Responsable de las comunicaciones con clientes, accionistas, medios de comunicación, etc.

Estos equipos en conjunto constituyen la estructura de gestión de incidentes, teniendo responsabilidades de dirigir, controlar y coordinar los esfuerzos de continuidad y recuperación dentro de la entidad. Los equipos trabajan hacia el objetivo común de contener el incidente: proteger vidas, los activos y el medio ambiente.

En el sentido más amplio, estos equipos, se centran en diferentes niveles de actividades de gestión: **estratégico, táctico y operativo**. Dependiendo de la escala y complejidad de la entidad, la estructura de gestión de incidentes se puede adaptar para encajar en el contexto organizacional. Por ejemplo, para las entidades con una estructura más ágil, a menudo se adopta un enfoque de dos niveles, es decir, los equipos estratégicos y tácticos se fusionan y proporcionan dirección al equipo operativo.

1. **Estratégico**: este equipo está formado por tomadores de decisiones estratégicas. Establecen el marco general, sus directrices y políticas para la gestión de incidentes. Además, aborda las implicaciones más amplias a largo plazo del incidente en las áreas de negocio afectadas. Predominantemente, se centra en preservar la reputación corporativa y comunicarse con los medios de comunicación. También refuerza los equipos tácticos y operativos al proporcionar los recursos necesarios para la gestión del incidente.

2. **Táctico**: el equipo táctico es responsable de determinar cómo se gestiona el impacto del incidente dentro de la política establecida por el equipo estratégico. Considera los problemas que provoca directamente el incidente, como el acceso a las instalaciones afectadas y la transferencia de operaciones críticas a ubicaciones alternativas. También asume el papel crucial de facilitar las actividades entre los equipos estratégicos y operativos. Dependiendo de la naturaleza del incidente, puede haber grupos específicos que se ocupen de aspectos clave de la respuesta a incidentes, como la gestión de instalaciones, la comunicación, el bienestar del personal y la coordinación de emergencias.

3. **Operacional**: las funciones generales incluyen la implementación de estrategias de recuperación basadas en las decisiones tomadas por los equipos estratégicos y tácticos. Se pueden establecer sub-equipos operativos adicionales para centrarse en cuestiones específicas del incidente, como la recuperación del negocio, la tecnología de la información y la seguridad del sitio.

Con el fin de fomentar una comunicación efectiva entre los diferentes grupos de gestión de incidentes, debe haber coordinadores o líderes para regular la información y su flujo. Sus principales responsabilidades son:

- **Validar la información**: verificar y garantizar la confiabilidad de la información antes de su difusión.
- **Comunicar información**: Difundir oportunamente la información para la toma de decisiones.

- **Actuar como el punto de enlace entre los equipos**: actuar como la única fuente de contacto para controlar el flujo de información entre los equipos. Esto establece un conocimiento claro de las decisiones tomadas con el fin de difundirlas a los equipos relevantes.

La figura siguiente ilustra la estructura de gestión de incidentes y sus componentes clave:

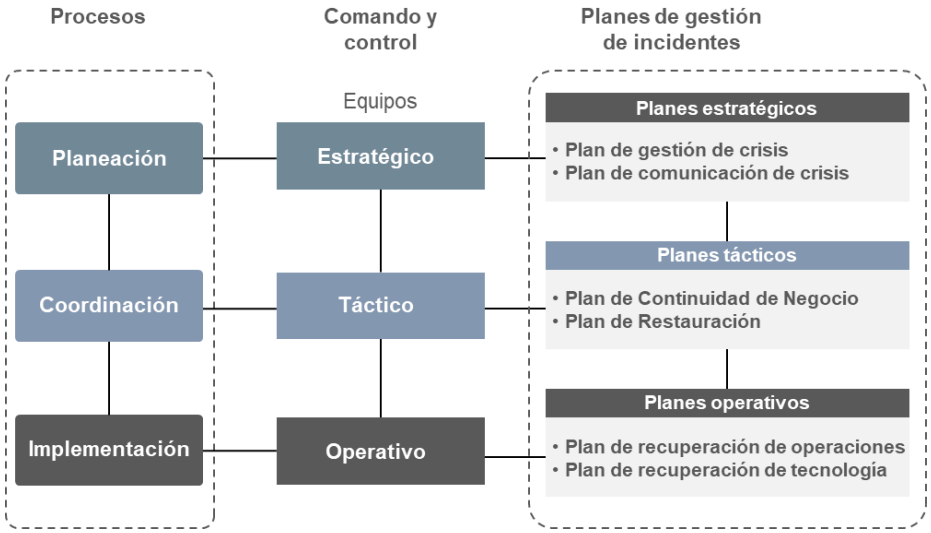


Figura 47. Estructura de gestión de incidentes

En el cuadro siguiente se resumen las principales características de los tres equipos de gestión.

	Equipo estratégico	Equipo táctico	Equipo operativo
Rol	**Coordinación**	**Supervisión**	**Ejecución**
Objetivo	• Gestión de crisis	• Gestión de continuidad de negocio	• Gestión de emergencia, recuperación y restauración.
Responsabilidades	• Recibir y evaluar información del equipo táctico sobre el impacto del incidente en las operaciones críticas.	• Determinar las respuestas de recuperación para minimizar el impacto en las personas, locales y las infraestructuras críticas. • Decidir, actuar y comunicar las	• Implementar respuestas de recuperación. • Actuar sobre las decisiones y estrategias de los equipos estratégicos y tácticos.

	• Decidir sobre la activación de continuidad de negocio y las estrategias apropiadas para hacer frente al incidente y su impacto.	instrucciones estratégicas. • Informar al equipo estratégico sobre el estado del incidente o los efectos de las respuestas. • Acatar instrucciones de los servicios de emergencia. • Instruir a los equipos operativos para gestionar el incidente. • Monitorear el incidente. • Escalar los problemas clave.	• Decidir, actuar y comunicarse dentro de las instrucciones recibidas. • Informar al equipo táctico sobre el estado del incidente y las respuestas tomadas. • Acatar instrucciones de los servicios de emergencia. • Monitorear el incidente. • Escalar los problemas clave.
Conformación	• Puestos de alto nivel y de importancia estratégica. • Puestos gerenciales a cargo del negocio y soporte. • Puestos gerenciales del área de riesgos y continuidad de negocio.	• Jefes de unidades de negocio. • Jefes de unidades de servicios y recursos críticos: Continuidad de Negocio, Seguridad física, tecnología y seguridad de la información, seguridad laboral, recursos humanos, servicios generales y comunicaciones.	• Personal que participa en procesos críticos, personal de supervisión y personal especializado en servicios y soporte.
Tipo de decisiones y acciones que toma	• Estrategia de continuidad para funciones críticas si la ubicación principal deja de estar disponible (sedes alternativas o trabajo desde casa). • Contacto con medios de comunicación y partes interesadas sobre el incidente y la respuesta.	• Responsabilidad y bienestar del personal y las partes interesadas afectadas por el incidente. Identificar cualquier víctima y servir de enlace con los servicios de emergencia sobre su atención • Transferencia de operaciones y recursos críticos a ubicaciones alternativas. • Comunicación con las partes interesadas locales.	• Orientación de los equipos apropiados si la aplicación de las decisiones y respuestas plantea cuestiones importantes. • Medidas para garantizar la seguridad de los locales afectados hasta que el incidente haya terminado y posteriormente sean reocupados.

	• Proteger la reputación. • Efectos de la falla de entrega de productos. • Impactos operativos, financieros y no financieros.	• Plazos de recuperación de funciones críticas. • Impactos operativos y financieros.	• Impactos operacionales.

Tabla 41. Características de la estructura de gestión de incidentes

Paso 2. Desarrollo de planes de continuidad de negocio

Para el desarrollo de los planes se debe tener en cuenta que no necesariamente seguirá los mismos pasos que se siguen con los procedimientos diarios de la entidad en situaciones normales; un plan de continuidad no busca documentar nuevos procedimientos de operación para la contingencia; la premisa es que se seguirán haciendo los mismos procesos diarios, pero con diferente prioridad, llegando inclusive a detenerse alguna actividad no urgente. En algunos casos los procedimientos de continuidad pueden incorporar actividades manuales que se utilizarán cuando los sistemas y servicios tecnológicos no estén disponibles.

El plan de continuidad de negocio de una entidad, desde un enfoque general se puede clasificar en cinco categorías según el objetivo de lo que persigan proteger:

1. Respuesta a incidentes de **seguridad del personal y de los activos físicos** de la entidad.
2. Respuesta a incidentes de afectación de la **reputación** de la entidad.
3. Respuesta a incidentes de interrupción de los **sistemas y servicios tecnológicos**.
4. Respuesta a incidentes de interrupción de las **operaciones**.
5. Plan **que gobierna el manejo de cualquiera de los incidentes** a través de un Comité de Crisis.

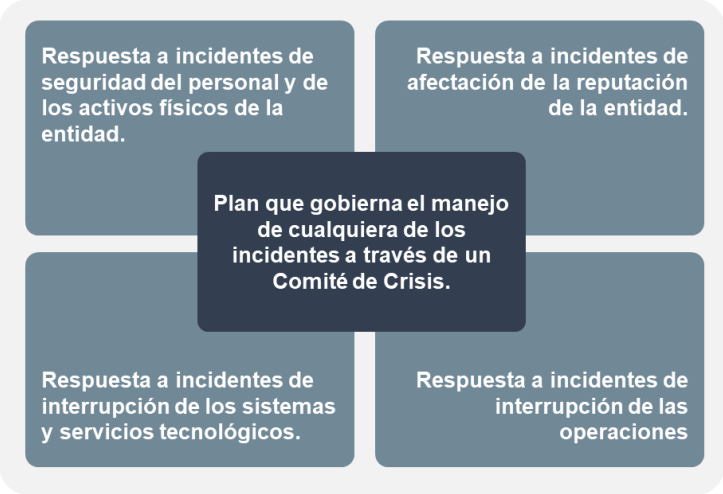


Figura 48. Tipos de planes de continuidad de negocio según su objetivo

Cabe destacar que, para cualquier tipo de plan, deberán ser concisos y accesibles a las personas o equipos que tengan responsabilidades definidas en los planes, en general tendrán la siguiente estructura:

- Objetivos y alcance.
- Productos y servicios por recuperar y priorizados según MTPDs y RTOs.
- Criterios de activación, quien tiene la autoridad tanto para la activación como desactivación.
- Equipo de respuesta o continuidad o recuperación. Actividades del equipo, de preferencia por rol.
- Estrategia a utilizar a nivel de personas, de infraestructura física, alternativas de sitios de operación y materiales, consumibles e insumos.
- Datos de contactos y plantillas a utilizarse en el momento del incidente.

1. **Plan para la respuesta a incidentes de seguridad del personal y activos de la entidad**

   Su principal propósito es salvaguardar la integridad física de las personas, bienes y valores de la entidad, su actuación se enmarca en acciones de respuesta a eventos que afectan a las personas y activos, como pandemias, un incendio o terremoto. Los tipos de incidentes guardan relación con la evaluación de riesgos más probables o de mayor impacto. Los

equipos de respuesta se orientan más brigadas de primera respuesta, como, por ejemplo: evacuación, primeros auxilios, combate a incendio, entre otros.

2. **Plan para la respuesta a incidentes de afectación de la reputación de la entidad**

   El objetivo principal es proteger la reputación de la entidad estableciendo qué posibles riesgos de afectación de imagen existen, qué públicos son afectados y en qué prioridad, qué medios de comunicación son los apropiados y qué voceros se tienen para comunicar el mensaje. El equipo estará liderado por el responsable de imagen institucional y su personal de apoyo, así como los propios voceros.

3. **Plan para la respuesta de incidentes de interrupción de los sistemas y servicios tecnológicos.**

   El principal objetivo es continuar brindando los servicios de tecnología de información y comunicación, así como los datos y la información. Las prioridades de recuperación serán dadas en función a los RTOs definidos para los servicios de tecnología que soportan los procesos críticos de la entidad. El equipo de recuperación estará conformado por la autoridad de la tecnología de información y participará de las decisiones más importantes en la recuperación, además de mantener informadas a las autoridades de la entidad.

   También forma parte del equipo el personal técnico a nivel de servidores, bases de datos, telecomunicaciones y aplicaciones responsables de la recuperación a nivel operativo de estos servicios.

4. **Plan para la respuesta a incidentes de interrupción de las operaciones.**

   Su principal objetivo es continuar brindando los productos y servicios críticos de la entidad. Las prioridades de recuperación serán dadas en función a los RTOs que definidos para estos productos y servicios. El equipo de recuperación de continuidad de las operaciones estará liderado por los jefes de las unidades funcionales o líderes de procesos (según como mejor la entidad se estructure para responder a un incidente disruptivo, siendo la parte clave la capacidad de liderazgo que pueda tener en la entidad durante el incidente). Forman parte del equipo el personal de los puestos clave para realizar las actividades mínimas según los RTOs establecidos.

5. **Plan de continuidad que gobierna el manejo de cualquiera de los incidentes**

   En el caso del plan de continuidad que gobierna el manejo de cualquier incidente disruptivo, el principal objetivo es la coordinación y toma de decisiones de cualquiera de los tipos de planes antes mencionados a través de la conformación de un Comité de Manejo del Incidente o de Crisis. Este comité de crisis conformado por las autoridades de la entidad será el equipo que deberá convocarse para apoyar en las decisiones del equipo que está respondiendo al incidente de seguridad del personal, o del equipo que está protegiendo la reputación, o del que está recuperando los servicios de tecnología de información, o del que está recuperando las unidades funcionales de negocio.

5.4.6. Etapa 6. Planificación y ejecución de pruebas de continuidad de negocio.

Como premisa básica, se considera que no se sabrá la efectividad de los Planes de Continuidad si no llegan a ser probados, su éxito no depende solamente de que tan documentado se encuentra sino cuán bien practicado e interiorizado está en la entidad; por lo tanto, el principal propósito de las pruebas, es practicar el plan y exponerlo de forma progresiva al mayor estrés posible para identificar las oportunidades de mejora que pueda tener y/o determinar las habilidades adicionales que hay que formar en el personal participante.

Una entidad que recién inicia su gestión no puede someter sus planes a un nivel de complejidad alta que implique detener sus operaciones y operar con las estrategias de recuperación definidas. Es recomendable que inicie con pruebas de escritorio, con un escenario general de incendio o sismo y validando el funcionamiento de ciertos componentes críticos, haciendo énfasis en la evacuación del personal; luego podrá ser el mismo escenario, abarcando heridos, con lo cual después de la evacuación parte del personal estaría indispuesto, lo que conlleva a una participación del personal alterno; de esta forma progresiva se irá creando complejidad en cada una de las pruebas. También la entidad debe planificar sus objetivos de prueba en el tiempo, es decir qué espera lograr en un año, en dos, en tres, quizás hasta en cinco años.

Las pruebas de continuidad de negocio se llevan a cabo con la finalidad de cumplir los siguientes objetivos:

1. Garantizar que la documentación prevista para ser usada durante eventos o situaciones de crisis sea validada por la práctica y la evaluación.
2. Mantener vigente la documentación de la gestión de la continuidad de negocio.
3. Asegurar que los planes se ajusten a los objetivos del negocio, mediante prácticas, auditorías y procesos de auto-evaluación.
4. Cumplir con los requerimientos temporales de los procesos clave de la entidad.
5. Familiarizar a los equipos de recuperación con el proceso de pruebas de continuidad.
6. Satisfacer los requerimientos legales, regulatorios y de auditoría interna.

Las pruebas deben considerar escenarios realistas, deben ser planificadas cuidadosamente y acordadas con los grupos de interés de la entidad, de forma que exista el mínimo riesgo de interrupción a los productos y servicios de la entidad. Una vez realizada la prueba, se deben documentar los resultados, ordenando todas las evidencias recolectadas después de la prueba y definir planes de acción para administrar los problemas surgidos durante la prueba o ejercicio. En la siguiente figura se presentan los tipos de pruebas que van de los menos complejos y a su vez menos costosos a los más complejos y costosos.

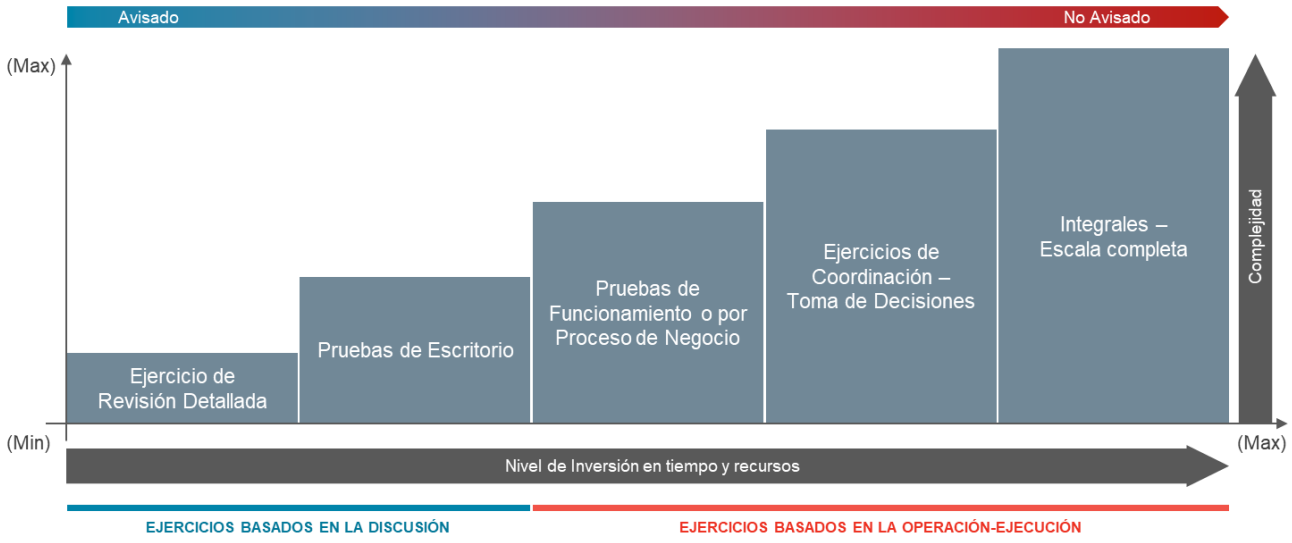


Figura 49. Tipos de pruebas según su complejidad

Las pruebas de menor complejidad son las de repaso, escritorio y juegos, cuyo objetivo principal es difundir y crear conocimiento en el uso del plan y de las alternativas de estrategias que posee la entidad; luego están las pruebas de funcionamiento de la infraestructura y de equipos para asegurar que se encuentren operativas y funcionando y que el personal que los opera conoce su rol y lo hace dentro los objetivos de tiempo establecidos; luego están las pruebas de movilización que buscan brindar conocimiento de los sitios a dónde desplazarse, cómo o con qué medios hacerlo y si se logran desplazar dentro de los tiempos establecidos; luego están las pruebas de coordinación, comando e integración donde más de un equipo de respuesta o continuidad o recuperación participan de forma integral bajo la coordinación del comité de manejo de incidentes o crisis; luego están las simulaciones más complejas que pueden ser una combinación de las pruebas anteriores y por lo general es el objetivo del año para el que, con el uso de las pruebas previas, la entidad se ha venido preparando; y finalmente está la prueba de escala completa donde adicionalmente a lo que se simula se busca detener algún servicio crítico y recuperarlo dentro de los tiempos esperados.

Por lo general las pruebas son anunciadas, pero también conviene realizar pruebas que no se avisan al personal, ya que se busca crear en las personas las competencias de manejo de estrés y niveles de alerta adecuados para un incidente disruptivo; aunque no se avise a los participantes, siempre se deberá comunicar a la autoridad correspondiente para que pueda prever cualquier riesgo de indisponibilidad del servicio. Las pruebas no avisadas pueden ser en cualquiera de los tipos de pruebas.

5.4.7. Etapa 7. Fomento de cultura – concientización y capacitación.

Para que la gestión de continuidad de negocio tenga éxito, ésta debe formar parte de la gestión cotidiana de la entidad, ya que se reconoce la relevancia y beneficios que poseen los temas de continuidad de negocio, sin embargo la misma operación diaria de la entidad hará que dentro de sus prioridades el tema de continuidad cada vez en el tiempo baje de importancia; es por ello que el fomento de una cultura de continuidad del negocio al interior de la entidad es una labor que debe ser constante.

Si el tema de continuidad aún no ha sido implementado en la entidad, la sensibilización a realizar será diferente y buscará dar a conocer o justificar la necesidad de establecer una gestión de continuidad del negocio, ya sea a partir de incidentes pasados, de incidentes ocurridos en otras organizaciones, de obligaciones regulatorias o legales, o de requerimientos de auditoría. Si la continuidad ya está implementada, entonces el objetivo será reforzar al personal que es un tema importante en la entidad.

El alcance al implementar acciones de sensibilización y capacitación debe abarcar:

1. Desarrollar y llevar a cabo una capacitación de concientización sobre continuidad de negocio para todo el personal;
2. Desarrollar y llevar a cabo la capacitación del equipo de gestión de crisis; y
3. Desarrollar y llevar a cabo la capacitación de continuidad de negocio para personal clave que participa o es responsable de la ejecución de procesos críticos.

El proceso para desarrollar e incorporar de forma sostenida la continuidad de negocio en la cultura de la entidad es el resultado de los siguientes tres pasos:

1. Evaluar el actual nivel de concienciación y compromiso con la continuidad de negocio con respecto al nivel deseado.
2. Identificar las "carencias de formación" que existen entre los dos niveles.
3. Diseñar y realizar una campaña para crear una concienciación corporativa y desarrollar las habilidades, conocimientos y compromiso necesarios para garantizar una exitosa gestión de continuidad.
4. Comprobar que la campaña de creación de concienciación ha logrado los resultados esperados y supervisar la concienciación en el largo plazo

La campaña de concienciación y sus mensajes deberían estar adecuados a cada grupo objetivo de audiencia. Estas audiencias son tanto internas, por ejemplo, los que llevan a cabo los procesos de continuidad y el personal en general, como externas, por ejemplo, proveedores, clientes y

terceros que dependen de (o pueden afectar de forma negativa a) la iniciativa de continuidad de la entidad. Es importante y necesario un trabajo en conjunto con el área de comunicaciones de la entidad para estructurar las mejores formas de dar el mensaje al personal y los medios apropiados para hacerlo; pueden usarse boletines, portales web, afiches, charlas, juegos y una vez al año el día, la jornada o la semana de la continuidad.

A continuación, se presenta una propuesta de plan de concientización a implementarse en la entidad:

1. **Capacitación general y de inducción**

   Capacitación a nivel general y de inducción, en temas afines a la continuidad de negocio para que todo el personal de la entidad pueda:

   - Conocer los elementos más relevantes de la gestión de continuidad de negocio
   - Conocer las amenazas de continuidad de negocio
   - Reconocer un incidente disruptivo,
   - Alertar a los equipos de emergencia y gestión de incidentes cuando corresponda,
   - Recurrir a las instancias de gestión de continuidad,
   - Responder adecuadamente a amenazas específicas,
   - Responder adecuadamente al evacuar las instalaciones,
   - Comprender los planes de continuidad relevantes y su papel en ellos.

2. **Capacitación sobre el manejo de incidentes disruptivos/crisis**

   En el manejo de un incidente existen habilidades adicionales y específicas que son necesarias que el personal que forma parte de los equipos de respuesta las conozca y domine, entre estas habilidades se mencionan algunas como:

   - Gestión de Crisis / Liderazgo de incidentes y toma de decisiones,
   - Manejo con medios de comunicación,
   - Continuidad de Servicios de TI y recuperación ante desastres,
   - Evaluación de daños, salvamento de activos y restauración de equipos,
   - Dirección y seguridad en las evacuaciones de emergencia,
   - Primeros auxilios, prevención y control de incendios

3. Concientización de la gestión de continuidad de negocio

Se realizarán acciones de concientización la cual puede incluir:

- Proceso formativo en temas relacionados a la continuidad de negocio, distribuido por medio de comunicados o cápsulas informativas diferentes. Cada cápsula estará enfocada en un ámbito relevante en cuanto a continuidad se refiere:
    - Que es la Continuidad de Negocio,
    - El impacto de la interrupción de los productos y servicios críticos de la entidad,
    - Emergencias y Evacuación,
    - Actuación ante eventos disruptivos.

  Para su distribución pueden utilizarse los siguientes medios:
    - Jornadas de formación
    - Entrega directa al personal para su lectura y visualización, mediante:
        - Correo electrónico, publicación en intranet, o
        - Habilitación de un directorio compartido al que puedan acceder los empleados.

5.4.8. Etapa 8. Mantenimiento y actualización de continuidad de negocio.

Las entidades son sensibles a los cambios que pueden ocurrir en los productos y servicios, procesos, personal y recursos, desactualizando el plan y afectando las prioridades de recuperación. De lo anterior, interesarán aquellos que impacten directamente a la continuidad y son:

- Cambios en personal clave, objetivos, procesos de negocio, estructura organizativa o instalaciones,
- Cambios causados por nuevas funciones, servicios y tecnología,
- Cambios en las evaluaciones de riesgos,
- Después de la revisión o auditoría donde se han identificado mejoras,
- Después de realizado pruebas de continuidad donde se han identificado oportunidades de mejora,
- Inconsistencia de los resultados de los indicadores de continuidad del negocio.

Una vez identificado un cambio de interés para la continuidad, deberá registrarse el cambio y analizar el impacto en la desactualización de la gestión; si es bajo o moderado, podrá esperarse al ciclo de actualización del siguiente periodo; si es alto o muy alto, deberá modificarse el plan de trabajo operativo del año en curso y contemplar la actualización de los componentes de la continuidad que sean necesarios. Las entidades deben definir su programa de mantenimiento a intervalos periódicos, por ejemplo:

Componente de mantenimiento	Plazo de mantenimiento
Política de Continuidad de Negocio	Revisada y actualizada bianualmente
Análisis de Impacto en el Negocio y Estrategias de Continuidad	Revisado y actualizado una vez al año o después de cualquier cambio significativo en el negocio
Evaluación de riesgos	Si ya no es válido o si ha habido un cambio significativo dentro de su departamento y en general.
Plan de Continuidad del Negocio	Revisado y actualizado una vez al año, y después de cualquier cambio significativo en el negocio
Listas de contactos claves	Revisado y actualizado cada 3 meses, o después de un cambio de personal
Operaciones de respuesta a emergencias	Según sea necesario, sobre la base de las recomendaciones de las lecciones aprendidas de una emergencia o prueba real
Sensibilización y formación	Cuando surgen nuevas ideas para crear conciencia o capacitación

Tabla 42. Elementos de continuidad de negocio para revisar periódicamente

Una vez realizado el cambio, el documento debe ser controlado, el contenido es responsabilidad del dueño del departamento o proceso del plan y el coordinador de continuidad es responsable del acceso al documento y de distribuirlo únicamente a los que el plan necesite ser entregado.

5.4.9. Etapa 9. Monitoreo – evaluación de desempeño

Una de las actividades principales es la medición del rendimiento de la gestión de continuidad del negocio. Una buena gestión implica el análisis de los procesos del negocio en curso para asegurarse de que se están cumpliendo los objetivos de la entidad. En la mayoría de las actividades de gestión de la continuidad del negocio se realiza (o se debería realizar) una revisión general y un proceso de evaluación.

De manera práctica, existen elementos mínimos y claves que toda entidad debe desarrollar para evidenciar que se tiene implementada una adecuada gestión de continuidad de negocio:

1. La entidad posee al menos un plan de gestión de incidentes y un plan de continuidad, que la habilita para gestionar cualquier posible incidente que afecte a los productos, independientemente de la causa.
2. La entidad posee uno o varios equipos responsables de gestionar todos los posibles incidentes que afectan a la continuidad. Cada equipo incluye a Enlace de Procesos que son responsables y que poseen la autoridad y conocimiento para responder de forma efectiva a cualquier incidente.
3. Cada miembro del equipo tiene al menos un sustituto con similar nivel de autoridad y formación.
4. Cada equipo dispone de autoridad y recursos para ser siempre movilizado y responder a tiempo.
5. Los integrantes del equipo han recibido formación adecuada para operar en una situación de crisis.
6. Cada plan:
    a. Define un proceso de invocación y escalado que permite su activación rápida o inmediata.
    b. Contiene tareas para obstaculizar las consecuencias inmediatas por un incidente en el negocio.
    c. Contiene directrices para gestionar la comunicación en situación de emergencia y crisis.
    d. Identifica responsables de atender eventos relacionados con la salud y bienestar del personal.

e. Describe los medios para coordinar todos los equipos y entidades involucradas en la recuperación.
f. Contiene tareas que permiten un análisis efectivo de la situación y una evaluación de los daños.
g. Identifica una ubicación alternativa en caso de que no se pueda acceder a la ubicación primaria.
h. Describe con claridad cómo elegir, adaptar y poner en marcha las estrategias de continuidad.
i. Identifica los niveles de recuperación que deben lograrse en relación a los RTOs.
j. Contiene tareas y listas de verificación para restaurar las operaciones después de un incidente.
k. Contiene tareas que aseguran la continuidad de cada acuerdo de subcontratación.
l. Incluye el contacto y los detalles para movilizar a todos los proveedores y clientes clave.
m. Identifica a aquellos responsables de su revisión, mantenimiento y difusión autorizada.
n. Cuenta con un presupuesto adecuado para su desarrollo y mantenimiento.
o. Cumple con todas las obligaciones legales y estatutarias.
p. Es probado, revisado y actualizado regularmente.
q. Describe con claridad su relación con todos los demás planes o documentos relevantes.

Por otro lado, las acciones para evaluar el desempeño y eficacia de la gestión de continuidad de negocio deben incluir el establecimiento de métricas o indicadores de desempeño; la evaluación de la protección de los productos y servicios priorizados; la confirmación del cumplimiento de los requisitos legales y regulatorios; y el uso de información documentada para facilitar las acciones correctivas posteriores.

Una organización sin indicadores que midan su progreso o sin un plan estratégico no tendrá cómo medir si está mejorando en el tiempo. Lo mismo ocurre con la gestión de continuidad del negocio; si no se mide su maduración y no se plantean objetivos estratégicos en el tiempo no podrá mostrar a la Alta Dirección si está mejorando o no. Como parte de propiciar la medición

del rendimiento de la gestión de continuidad de negocio en las entidades, se proponen los siguientes indicadores:

Nº	Indicador	Forma de calculo	Periodicidad	Umbral límite[1]
1	Número de interrupciones por línea de negocio, diferenciadas según sean de operaciones, tecnología y proveedores	Conteo	Trimestral	Operaciones: 5 Tecnología: 10 Proveedores: 3
2	Tiempo total de interrupción por línea de negocio, diferenciadas según sean de operaciones, sistemas y proveedores	Conteo	Trimestral	2 horas
3	N° de veces de activación de planes (Continuidad, recuperación de tecnología, emergencia y crisis)	Conteo	Trimestral	3 para cada tipo
4	% de RTO no cumplidos al activarse planes (Continuidad y tecnología)	(N° RTOs sin alcanzar) / (N° total RTOs que debieron alcanzarse al activar planes)*100%	Trimestral	10%
5	% de proveedores con planes de continuidad (PCN)	(N° de proveedores con planes de continuidad) / (total de proveedores)	Semestral	90%

[1] Valores de referencia, la entidad debe adecuarlos según su tamaño y naturaleza.

Nº	Indicador	Forma de calculo	Periodicidad	Umbral límite[1]
6	% de planes probados	(N° de planes probados) / (Total de planes)	Semestral	3 por tipo de plan
7	% RTO no cumplidos en pruebas (continuidad y tecnología)	(N° de RTO no cumplidos) / (N° total de RTOs que debieron alcanzarse al probar los planes)	Trimestral	10%

Tabla 43. Indicadores de continuidad de negocio

5.5. Guía de implementación para la gestión de continuidad de negocio

5.5.1. Guía de implementación para la continuidad de negocio

La presente sección brinda una guía metodológica para la implementación de una Gestión de Continuidad del Negocio, a fin de estructurar los planes de trabajo tanto para la implementación por primera vez de la gestión y para su posterior mantenimiento en el tiempo.

Una gestión de Continuidad del Negocio no debe ser entendida como un proyecto que termina una vez que se documentan los planes y se realiza la primera prueba, sino como un proceso permanente de mejora continua que debe revisarse anualmente.

Nº	Etapa / Actividades
1.0	**Liderazgo, gobierno y política de continuidad de negocio**
1.1	Identificar participantes o “dueños” de las disciplinas de la continuidad del negocio, los cuales serán involucrados según convenga en cualquiera de las actividades metodológicas descritas en la presente guía. *Nota: se sugiere considerar*

	- *Patrocinador ejecutivo de la continuidad de negocio* - *Dueño de la parte relacionada a la comunicación en crisis* - *Dueño de la parte relacionada a las emergencias y protección del personal e instalaciones* - *Dueño de la parte relacionada a los procesos clave de negocio* - *Dueño de la parte relacionada a la tecnología y seguridad de información*
1.2	Definir Roles y Responsabilidades de la Continuidad del Negocio.
1.3	Elaborar y aprobar la Política de Continuidad del Negocio.

2.0	**Análisis de impacto del negocio (bia) – identificar procesos prioritarios**
2.1	Establecer el alcance de la gestión de Continuidad del Negocio a nivel de Productos y Servicios.
2.2	Validar (Revisión/actualización) de escalas temporales y de impacto.
2.3	Identificar las amenazas de mayor posibilidad de ocurrir y que podrían hacer que el Producto o Servicio en el alcance no se pueda entregar.
2.4	Para cada producto y servicio: Estimar el escenario más estresante, su costo de interrupción, el MTPD, MBCO y RTO (tomar como insumo 2.2 y 2.3).
2.5	Priorizar productos y servicios, agrupándolos desde la menor franja de tiempo de recuperación.
2.6	Identificar procesos relacionados que permiten la entrega de los productos y servicios definidos en 2.5, estos procesos heredan el MTPD y RTO de los productos a los que soportan.
2.7	Para cada proceso, identificar las unidades funcionales que lo ejecutan.
2.8	Para cada unidad funcional, identificar los recursos críticos necesarios para ejecutar los procesos definidos en 2.6 (personas, instalaciones, tecnología, información clave, proveedores y recursos económicos.
2.9	Elaborar informe y gestionar probación de resultados BIA.

3.0	Análisis de riesgos de continuidad – protección de productos más urgentes
3.1	Identificar las sedes más críticas de la entidad que permiten la ejecución de los procesos definidos en 2.6.
3.2	Identificar los riesgos de amenazas de continuidad de negocio a nivel global, continental, regional, nacional, local e internas que pueden causar una interrupción de los recursos que son requeridos por los procesos críticos.
3.3	Definir la matriz de riesgo identificando las escalas de probabilidad y las escalas de impacto aplicables, y cuál es el nivel de riesgo no deseado.
3.4	Para cada sede, identificar y valorar si son eficientes los controles existentes que mitigan la paralización de cada recurso ante la posible ocurrencia de cada amenaza identificada.
3.5	En caso existir recursos expuestos a niveles de riesgo no deseados y extremos, identificar mejoras o nuevas medidas de control que bajen el nivel de riesgo.

4.0	Diseño y selección de estrategias de continuidad de negocio
4.1	Consolidar a nivel de toda la organización las cantidades de recursos por cada RTO que han sido identificados para cada Unidad Funcional. *Nota: Considerar como insumo 2.8*
4.2	Aplicar medidas preventivas ante amenazas específicas. *Nota: Considerar Tabla 39.*
4.3	Para cada tipo de recurso y para cada ventana de tiempo, definir las estrategias de continuidad y recuperación más apropiadas y costo eficientes de acuerdo con las cantidades requeridas. *Nota: Considerar Tabla 40.*
4.4	Definir las estrategias de respuesta relacionadas a la gestión de crisis: - Conformar el Comité de Manejo de Incidentes o Crisis - Definir lugar(es) para la Sala de Gestión de Crisis - Identificar recursos necesarios para la Sala de Crisis - Definir esquema general de actuación del Comité de Manejo de Incidentes o Crisis
4.5	Definir las estrategias de respuesta relacionadas a la comunicación en crisis:

4.0	Diseño y selección de estrategias de continuidad de negocio
	- Identificar riesgos de reputación - Identificar audiencias afectadas por cada riesgo (escenario) y mecanismos / medios de comunicación - Identificar roles y voceros apropiados por audiencia - Diseñar plantillas clave o mensajes prediseñados - Definir esquema general de actuación de los roles y voceros identificados
4.6	Definir las estrategias de respuesta relacionadas a salvaguardar la vida y las instalaciones: - Definir escenarios más relevantes - Para cada escenario, conformar equipo de brigadista más apropiado - Definir equipamiento necesario para ser utilizado durante la emergencia - Definir esquema general de actuación del equipo de brigadistas
4.7	Consolidar recursos de continuidad y recuperación y preparar informe sobre la selección y desarrollo de estrategias.
4.8	Establecer un plan de implementación de las estrategias preventivas, de continuidad y de respuesta identificadas.
4.9	Ejecutar plan de acción de implementación de las estrategias.

5.0	Implementación de la estrategia – documentación de planes de continuidad
5.1	Identificar personal para formar equipos expertos para implementar estructura de respuesta a incidentes disruptivos y para documentar los procedimientos de continuidad de negocio.
5.2	Definir la estructura y cantidad de planes a construir considerando el tamaño y complejidad de la entidad. *<u>Entidad pequeña:</u>* - *Un documento para gestión, comunicación en crisis y continuidad del negocio* - *Un documento por escenario o tipo de emergencia para la respuesta a la emergencia* *<u>Entidad mediana:</u>*

	- *Un documento para gestión y comunicación en crisis* - *Un documento para continuidad del negocio* - *Un documento para continuidad de los sistemas informáticos* - *Un documento por escenario o tipo de emergencia para la respuesta a la emergencia*
5.3	Definir plantillas para documentar planes de manera estándar.
5.4	Efectuar documentación de procedimientos de Manejo de Emergencias, Manejo de Incidentes o Gestión de Crisis, Comunicación en Crisis, Continuidad de Negocios en caso de interrupción de las operaciones y de los sistemas informáticos de la entidad.
6.0	**Planificación y ejecución de pruebas de continuidad de negocio**
6.1	Elaborar el Programa de Pruebas de Continuidad que consiste en un conjunto de ejercicios cada cual de mayor complejidad que el anterior. *Nota: Se recomienda sea a 3 años, aunque la primera vez puede ser sólo pensado a 1 año.*
6.2	Para cada prueba, establecer: - Objetivos / propósito, alcance de lo que se prueba o no - Tipo de ejercicio / prueba y escenario considerado - Participantes (según su rol: Planificador, Facilitador(es), Observador(es), Ejecutor(es)) - Cronograma de preparación del ejercicio - Guión de ejecución (durante el ejercicio) - Inyectores a considerar durante el ejercicio - Formatos a utilizar para la evaluación durante el ejercicio - Resultados esperados - Aspectos especiales a tomar en cuenta producto de incidentes reales anteriores o pruebas antes realizadas
6.3	Para cada prueba, elaborar el guión que considera la línea base y los inyectores que serán considerados durante su ejecución, preparar todos los aspectos de logística y formatos para la evaluación de la prueba.
6.4	Efectuar prueba de acuerdo con el guión establecido.
6.5	Terminada la prueba, efectuar sesión de lecciones aprendidas “en caliente”

6.6	Elaborar informe de la prueba, determinando si se cumplieron los objetivos y se superaron las observaciones de pruebas anteriores. Presentar informe e identificar recomendaciones para futuras pruebas.
6.7	De ser necesario, actualizar el Programa de Pruebas.
6.8	Aplicar todas las recomendaciones y actualizaciones que han sido sugeridas en el informe de la prueba.

7.0	**Fomento de cultura – concientización y capacitación**
7.1	Con apoyo de recursos humanos, definir las competencias requeridas por cada rol de continuidad.
7.2	Evaluar el nivel de competencia alcanzado por cada persona según su rol en la continuidad del negocio.
7.3	Determinar objetivos anuales para mejorar el nivel de competencia de cada persona. Según las mejoras identificadas, proponer iniciativas de capacitación.
7.4	Agregar iniciativas de creación de conciencia en temas de continuidad de negocio y formalizar un Programa de Concientización y Capacitación en Continuidad de Negocios con el siguiente alcance: a) Capacitación general y de inducción, b) Capacitación sobre el manejo de incidentes disruptivos/crisis, y c) Concientización de la gestión de continuidad de negocio
7.5	Para cada iniciativa, convocar al área de comunicaciones para diseñar la forma de ejecución.
7.6	Ejecutar iniciativas y medir los resultados logrados y guardar los registros correspondientes.
7.7	Evaluar si los objetivos del Programa de Concientización y Capacitación en Continuidad de Negocios se están alcanzando o si es necesario efectuar ajustes en base a los resultados obtenidos

8.0	**Mantenimiento y actualización de continuidad de negocio**
8.1	Identificar áreas de la entidad que puedan ser fuentes para impulsar cambios en la gestión de continuidad.
8.2	Efectuar acuerdos con las áreas estableciendo las frecuencias de cruce de información de posibles cambios.
8.3	Aplicar los acuerdos e identificar cambios de manera permanente.
8.4	Por cada cambio, evaluar el impacto que genera en la gestión; de ser alto, definir la fecha más apropiada para la actualización; caso contrario, incorporar el cambio en el plan de trabajo anual de la gestión.
8.5	En caso de actualización de la gestión de Continuidad del Negocio, llevar una bitácora de los cambios en los documentos respectivos y el control de las versiones respectivas
8.6	En caso de cambio en alguno de los planes de continuidad del negocio, efectuar la distribución de las nuevas versiones, y asegurar la recolección, retención y destrucción posterior de las versiones no vigentes.
8.7	Al final del año, preparar un plan de trabajo anual de actualización de la gestión de continuidad en base a cambios visibles de la entidad y cambios identificados que no fueron priorizados como urgentes en el año.
9.0	**Monitoreo – evaluación de desempeño**
9.1	Identificar los aspectos a evaluar y definir el sistema de indicadores de continuidad de negocio.
9.2	Convocar a los integrantes de la estructura de gestión de incidentes y responsables de procesos críticos.
9.3	Estructurar los indicadores de continuidad de negocio, definir responsable de medición, fuentes de información, periodicidad, forma de cálculo y elaborar formatos.
9.4	Aplicar la medición los indicadores, solicitando y consolidando la información necesaria para evaluarlos.
9.5	Analizar y socializar los resultados obtenidos.
9.6	Generar propuesta de mejoramiento de la gestión de continuidad de negocio
9.7	Realizar seguimiento a los reportes de mejora.

5.5.2. Propuesta práctica de aplicación de la guía metodológica a 3 semestres

Aplicar la guía en sus nueve fases, puede resultar un gran esfuerzo para las entidades con resultados visibles en el mediano plazo; en muchos casos, la necesidad de resultados es más inmediata. Por ello, se propone un plan de trabajo a 18 meses con una perspectiva práctica que lleve a lograr resultados más inmediatos y a su vez crear y fortalecer una gestión de Continuidad del Negocio sólida y sostenible en el tiempo.

Semestre 1			
Objetivos	**Objetivos específicos**	**Nº**	**Actividad metodológica**
Resultados inmediatos en continuidad	Comprometer el apoyo de personal clave	1.1	Identificar participantes o "dueños" de las disciplinas de la continuidad, serán involucrados en cualquiera de las actividades metodológicas.
		2.3	Identificar las amenazas de mayor posibilidad de ocurrir y que podrían hacer que el Producto o Servicio se interrumpa.
		7.4	Realizar charla de Concientización de la gestión de continuidad de negocio.
	Elaborar Plan de Manejo de Incidentes o Gestión de Crisis	4.4	Definir las estrategias de respuesta relacionadas a la gestión de crisis.
		5.4	Documentar procedimientos de gestión de crisis.
		6.1 al 6.8	Efectuar prueba de escritorio del Manejo de Incidentes o Gestión de Crisis.
	Elaborar el Plan de Comunicación en Crisis	4.5	Definir las estrategias de respuesta relacionadas a la comunicación en crisis.
		5.4	Documentar procedimientos de Comunicación en Crisis.
		6.1 al 6.8	Efectuar prueba de escritorio de Comunicación de Crisis.

Semestre 1			
Objetivos	**Objetivos específicos**	**Nº**	**Actividad metodológica**
	Elaborar Plan de Respuesta a Emergencias	4.5	Definir las estrategias de respuesta relacionadas a salvaguardar la vida y las instalaciones.
		5.4	Documentar procedimientos de Manejo de Emergencias.
		6.1 al 6.8	Efectuar prueba de escritorio de Manejo de Emergencia.
Establecimiento de la gestión de Continuidad	Elaborar la Política de Continuidad	1.2	Definir Roles y Responsabilidades de la Continuidad.
		1.3	Elaborar y aprobar la Política de Continuidad.
Aplicación inicial de la metodología para el Producto o Servicio más crítico	Seleccionar el Producto más crítico	2.1	Establecer el alcance de la gestión de Continuidad del Negocio a nivel de Productos y Servicios.
	Identificar procesos urgentes a recuperar	2.2 al 2.9	Efectuar el Análisis de Impacto del Negocio (BIA).
	Elaborar estrategias de Recuperación	4.1 al 4.9	Consolidar recursos y diseñar estrategias de recuperación.
	Elaborar el Plan de Continuidad del Producto más crítico	5.1 al 5.4	Identificar equipo de elaboración del plan y efectuar preparativos para la documentación.
		6.1 al 6.8	Efectuar prueba de escritorio del plan elaborado.

Semestre 2			
Objetivos	**Objetivos específicos**	**Nº**	**Actividad metodológica**
Refuerzo de conciencia de la importancia de la gestión de continuidad	Crear habilidades en Continuidad del Negocio	7.4	Ejecutar una capacitación especializada en continuidad para todos los participantes de la gestión.
Gestión de Cambios de la Continuidad	Elaborar Plan Anual de Trabajo	8.7	Preparar un plan de trabajo anual de actualización de la gestión de Continuidad del Negocio en base a cambios visibles de la entidad respecto a lo trabajado el semestre 1.
	Actualizar lo realizado el semestre 1	4.9	Implementar la Estrategia de Continuidad del Producto y Servicio del semestre 1.
		8.5	Efectuar los cambios en el programa e implementar una bitácora de los cambios en los documentos respectivos y el control de las versiones respectivas.
		8.6	En caso de algún cambio en alguno de los planes elaborados el semestre 1, efectuar la distribución de las nuevas versiones, y asegurar la recolección, retención y destrucción posterior de las versiones no vigentes.
Ampliación de la aplicación de la metodología de la gestión de Continuidad	Proteger las actividades más críticas sem.1	3.1 al 3.5	Efectuar el análisis de amenazas y evaluación de riesgos para las actividades más críticas.
	Elaborar los Planes de Continuidad del	2.1	Establecer el alcance de la gestión de Continuidad del Negocio a nivel de Productos y Servicios.

Semestre 2			
Objetivos	**Objetivos específicos**	**Nº**	**Actividad metodológica**
	resto de Productos o Servicios clave incluyendo los Sistemas Informáticos	2.2 al 2.9	Efectuar el Análisis de Impacto del Negocio (BIA) para el resto de Productos y Servicios.
		4.1 al 4.2	Consolidar recursos y diseñar estrategia de recuperación incluyendo la de tecnología.
		5.1 al 5.4	Identificar equipo de elaboración del plan y efectuar preparativos para la documentación.
		6.1 al 6.8	Efectuar una prueba de escritorio de los planes elaborados el semestre 2, incluyendo los planes de recuperación ante desastres de los sistemas.
	Efectuar un ejercicio de mayor complejidad	6.1 al 6.8	Efectuar una prueba de mayo complejidad.
	Medir la evaluación de desempeño de Continuidad	9.1 al 9.5	Aplicar medición de indicadores de continuidad de negocio.
Semestre 3			
Objetivos	**Objetivos específicos**	**Nº**	**Actividad metodológica**
Formalización del Programa Concientización y Capacitación	Elaborar Programa de Concientización y Capacitación	7.1 al 7.5	Diseñar iniciativas del Programa de Concientización y Capacitación en Continuidad.
	Aplicar el Programa	7.6 al 7.7	Aplicar iniciativas y medir resultados.

Semestre 2			
Objetivos	**Objetivos específicos**	**Nº**	**Actividad metodológica**
Formalización Programa de Pruebas	Programa de Pruebas	6.1 al 6.3	Diseñar el Programa de Pruebas.
	Ejecutar pruebas semestre	6.4 al 6.8	Ejecutar pruebas.
Mantenimiento y maduración de la metodología de la gestión de continuidad	Diseñar programa de mantenimiento	8.1 al 8.2	Identificar áreas que provean información de posibles cambios y establecer acuerdos con ellas.
	Aplicar programa de mantenimiento	8.3 a 8.4	Aplicar programa de mantenimiento.
		8.5	Efectuar cambios e implementar una bitácora de los cambios en los documentos respectivos y el control de las versiones respectivas.
		8.6	En caso de algún cambio en alguno de los planes, efectuar la distribución de las nuevas versiones.
	Medir la evaluación de desempeño de Continuidad	9.1 a 9.5	Aplicar medición de indicadores de continuidad.
		9.6	Generar propuesta de mejoramiento de la gestión de continuidad de negocio
	Elaborar y ejecutar Plan Anual de Trabajo	8.7	Preparar y ejecutar el plan de trabajo anual de la gestión de Continuidad del Negocio en base a cambios visibles y la inclusión de mejoras sugeridas como resultado de la evaluación de desempeño de continuidad de negocio.

CONCLUSIONES

1. En el contexto mundial actual, donde ningún país ni organización está exenta de las amenazas naturales, biológicas, sociales y tecnológicas, las entidades deben estar preparadas para afrontar incidentes que tengan la capacidad de impactarlas de forma negativa. Los incidentes disruptivos tienen el potencial de desviarlas y afectarlas de forma muy relevante de sus objetivos, poniendo en riesgo su reputación y supervivencia. Estos incidentes disruptivos tienen distintos niveles de riesgo, por lo que las entidades deben identificarlos, analizarlos, evaluarlos y establecer Estrategias de continuidad y Planes para atenuar sus efectos.

2. El Sistema de Gestión de Continuidad de Negocio ofrece un marco de trabajo para que una entidad construya resiliencia y brinda la capacidad de tener una respuesta efectiva ante eventos amenazantes. La continuidad de negocio es una de las disciplinas clave de la resiliencia organizacional. El elemento central de esta disciplina es el proceso de prepararse para situaciones que quizás nunca sucedan. Estas actividades tienen como fin asegurar la reanudación oportuna de la entrega de productos y servicios después de un incidente.

3. Un elemento necesario y diferenciador para entidades que desean superar crisis generadas por incidentes de alto impacto, es la implementación de una gestión de continuidad de negocio que ese base en un proceso integral que identifica los posibles impactos que amenazan a una entidad y ofrece un marco para proporcionar robustez y disponer de una respuesta efectiva hacia estos, salvaguarda los intereses de las partes interesadas, brinda ventajas competitivas y fortalece la creación el valor de la entidad.

4. La documentación de Continuidad de Negocio puede ser muy amplia y compleja, por tanto, debe adecuarse a las características, tamaño y naturaleza de cada entidad. La guía metodológica proporciona orientación y pautas a seguir para implementar dicha gestión, el desarrollo y despliegue que se dé a cada etapa, estará en función de una serie de parámetros que probablemente variarán de acuerdo con los objetivos individuales de cada entidad en particular y de las premisas que se establezcan en los pasos iniciales.

RECOMENDACIONES

1. Las organizaciones, en la búsqueda de ser resilientes, deben considerar el desarrollo de capacidades de adaptarse a las circunstancias cambiantes que pueden tener efectos dañinos en la capacidad de sobrevivir. Estos efectos incluyen aspectos tales como cambios en el mercado en el cual opera la organización, leyes y regulaciones, tecnología, etc., como también incidentes que pueden alterar la capacidad de brindar sus productos y servicios.

2. La Gestión de Continuidad de Negocio debe ser asimilada y totalmente integrada a las entidades como uno más entre sus procesos de gestión. Debe centrarse particularmente en desarrollar una capacidad de recuperación que sea conjunta para toda la organización y le permita sobrevivir a la pérdida total o parcial de su capacidad operativa.

3. Es fundamental contar con el apoyo de la Alta Dirección para impulsar cualquier iniciativa en materia de Continuidad de Negocio, debe estar totalmente convencida de la importancia del tema, las ventajas que se obtienen y el valor agregado que traerá consigo su puesta en marcha. Debe apoyar el fomento y transformación de la cultura organizacional y demostrar su nivel de compromiso facilitando y brindando los recursos necesarios: humanos, tecnológicos y financieros en pro de hacer la entidad más resiliente. La responsabilidad que la Alta Dirección tenga en robustecer la capacidad de recuperación de una entidad será un factor determinante para proteger los intereses a largo plazo del personal, clientes y todos aquellos que dependen de algún modo de la organización. Si bien se pueden calcular las pérdidas financieras ocasionadas por una interrupción, generalmente el mayor daño suele reflejarse en una pérdida de imagen o de confianza fruto de un incidente mal gestionado.

4. Para la implementación del Sistema de Gestión las entidades deben a) determinar el alcance, límites y aplicabilidad en función de los productos y servicios que presta, b) evaluar los factores internos y externos que son pertinentes, c) demostrar compromiso y liderazgo de todos los niveles directivos d) determinar las competencias requeridas para todos los roles y responsabilidades y la toma de conciencia, el conocimiento, el entendimiento, las habilidades y la experiencia necesarias para llevarlos a cabo, y e) enfocarse en los impactos de las interrupciones y no en sus causas, dado que las actividades se interrumpen por una amplia variedad de incidentes, muchos de los cuales son difíciles de predecir o analizar.

REFERENCIAS BIBLIOGRÁFICAS

Banco de España. (2006). *Recomendaciones relativas de continuidad de negocio.*

BSI GROUP. (2006). *BS 25999-1: 2006 Gestión de Continuidad de Negocio. Código de práctica.*

Business Continuity Institute. 2013. Good Practice Guidelines.

Casualty Actuarial Society. (2003). *Overview of Enterprise Risk Management*. Obtenido de https://www.casact.org/area/erm/overview.pdf

Cloud Endure. (2016). *Disaster Recovery Survey*. Obtenido de https://vmblog.com/archive/2016/02/17/2016-cloudendure-survey-reveals-77-of-companies-striving-for-99-9-availability-but-57-had-one-or-more-outages-in-past-3-months.aspx#.YUL2YbhKiUk

Coso. (2004). *Enterprise Risk Management - Integrated Framework*.

Deloitte. (2013). *Exploring Strategic Risk*. Obtenido de https://www2.deloitte.com/global/en/pages/governance-risk-and-compliance/articles/exploring-strategic-risk.html

Eric Conrad, S. M. (2010). *Business Continuity and Disaster Recovery Planning.*

Ernst & Young. (2011). *Los 10 principales riesgos de negocios*. Obtenido de https://riskandopportunities.files.wordpress.com/2014/11/los_nuevos_riesgos_en_los_negocios.pdf

Escobar León. (2011). *Diseño de Gestión de Crédito y Liquidez, en base al Análisis Vertical y Horizontal de los Estados Financieros de las Pequeñas y Medianas Empresas de Servicios de Publicidad.* Universidad de El Salvador.

IDC / Carbonite. (2015). *The Growth Opportunity for SMB Cloud and Hybrid Business Continuity.* Obtenido de https://www.carbonite.com/globalassets/files/white-papers/carb-idc-smb-cloud-growth-opportunity-report.pdf

ISO. (2018). *ISO 31000:2018 Gestión del Riesgo. Directrices.*

ISO. (2015). *ISO 22317:2015 Protección y seguridad de los ciudadanos. Sistemas de gestión de la continuidad del negocio. Directrices para el análisis del impacto sobre el negocio.*

ISO. (2019). *ISO 22301:2019 Seguridad y resiliencia. Sistema de Gestión de la Continuidad del Negocio. Requisitos.*

ISO. (2020). *ISO 22313:2020 Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para la utilización de la norma ISO 22301*.

Palacios, M. (2009). *Propuesta de análisis financiero de ORACLE.*

Ponemon Institute. (2016). *Cost of Data Center Outages*. Obtenido de http://planetaklimata.com.ua/instr/Liebert_Hiross/Cost_of_Data_Center_Outages_2016_Eng.pdf

Sadgrove, K. (2005). *The Complete Guide to Business Risk Management.*

Sistema Económico Latinoamericano y del Caribe. (2013). *La continuidad de negocios y operaciones frente a situaciones de desastre en América Latina y el Caribe. Balance y recomendaciones*.

Superintendencia del Sistema Financiero. (2011). *Norma para la Gestión Integral de Riesgo de las entidades financieras NPB4-47*.

ANEXOS

ANEXO 1: EJEMPLO DE POLÍTICA DE CONTINUIDAD DE NEGOCIO

1. Propietario de la política

La Junta Directiva de la entidad financiera.

2. Alcance de Continuidad de Negocio

a. Es de aplicación para los productos y servicios críticos de la entidad, como lo son… *(especificar los productos y servicios críticos de la entidad*), cuya interrupción pueda afectar a sus partes interesadas.

b. En cuanto a las instalaciones abarca las oficinas centrales, sucursales, centro de procesamiento de datos, sitios alternos de operación y recuperación, etc.

c. Se consideran lo incidentes que tienen consecuencia de perdida de personal, los que interrumpan de forma directa o indirecta el acceso a las instalaciones de trabajo, los que interrumpan los procesos y sistemas críticos para el logro de objetivos de la entidad y los que tiene como consecuencia la perdida de los servicios suministrados por terceros.

3. Objetivos de continuidad de negocio

Mediante esta política de continuidad de negocio se establece el marco para el desarrollo, implementación, revisión y mejora de los Planes de Continuidad de Negocio en la entidad que:

a. Actuar diligentemente frente a una situación de desastre o crisis, resguardando prioritariamente la seguridad de las personas, las instalaciones, los bienes y valores y la reputación e imagen de la entidad.

b. Permita brindar una respuesta adecuada y oportuna ante la materialización de un riesgo o amenaza de características catastróficas, que provoquen un escenario de interrupción de los productos y servicios debido a la falta de disponibilidad de alguno de los componentes básicos de la entidad: personas, edificios y oficinas, tecnología, información y proveedores.

c. Disminuya las consecuencias de las posibles catástrofes sobre los procesos de negocio, asegurando la preservación e integridad de los datos y funciones esenciales o, en su defecto, que tales datos o funciones se recuperen, oportuna y progresivamente, hasta la vuelta a la normalidad de las operaciones de la entidad.

d. Permita reducir la improvisación y el tiempo de recuperación de los productos y servicios críticos del negocio, y como consecuencia, las pérdidas económicas asociadas, directas e inducidas, como resultado del desastre.

4. Principios generales

La Política de Continuidad de Negocio se sustenta el siguiente conjunto de principios:

a. La premisa y objetivo prioritario es la protección y seguridad de las personas, tanto en situación normal como en una situación de crisis derivada de la materialización de un desastre. Asimismo, la protección del ambiente, la protección de los activos de la entidad, y la continuidad de las operaciones.

b. Se crearán las instancias multidisciplinarias de gestión que sean necesarias y adecuadas, para impulsar y administrar la implementación y seguimiento de la Continuidad de Negocio.

c. Se considera prioritaria la asignación de recursos financieros, técnicos y materiales para asegurar el cumplimiento de la presente política y la ejecución del Plan de Continuidad.

d. Para las distintas áreas de la entidad, se nombrarán representantes o enlaces de continuidad de negocio, que posean la debida experiencia y conocimiento, para que participen activamente en la elaboración, implantación, revisión, prueba y actualización de los Planes de Continuidad de Negocio.

e. Se desarrollarán e implementarán Planes de Continuidad de Negocio para la entidad, considerando las áreas y unidades internas, proveedores y servicios y empleando sistemas, recursos y procedimientos adecuados y proporcionados.

f. Se aprovechará las sinergias generadas en el desarrollo e implementación de los Planes de Continuidad de Negocio y cualesquiera otros planes en el ámbito de la continuidad operativa en las entidades del Grupo, contemplando los medios y recursos comunes de los que dispone la institución.

g. Se adoptarán medidas razonables para la continuidad de negocio de los productos, servicios y procesos, en función de la criticidad de estos establecida por la entidad.

h. Se considerará en la elaboración de los Planes de Continuidad de Negocio, procedimientos y disposiciones de comunicación apropiados, tanto a nivel interno como externo, que faciliten la correcta ejecución de estos.

i. Se asegura el fomento de una cultura de Continuidad de Negocio en el personal de la entidad, por medio de acciones y labores de concientización y formación. Se comunicará a todo el personal de su rol y responsabilidades y de los procedimientos que le competen, en el marco de la continuidad de negocio.

j. Se incluirá como parte de la Gestión de Continuidad de Negocio, la realización de revisiones, pruebas y actualizaciones de los Planes de Continuidad de Negocio de forma periódica o ante cambios significativos, en un producto o servicio o como parte de la de mejora continua de los mismos.

k. Se establece una permanente disposición a colaborar con las autoridades competentes ante un escenario de desastre.