Estrategias y planes de continuidad del negocio

Breve descripción:

Este componente formativo explora las estrategias y planes necesarios para garantizar la continuidad del negocio ante interrupciones. Aborda el análisis de impacto, la formulación de estrategias efectivas y el diseño del Plan de Continuidad del Negocio (PCN), fortaleciendo la resiliencia organizacional y la capacidad de recuperación operativa frente a eventos críticos.

Octubre 2025

Tabla de contenido

Introducción

Este componente formativo aborda las estrategias y planes que permiten garantizar la continuidad operativa de una organización ante incidentes, crisis o desastres. Se orienta al diseño, validación e implementación de estrategias de continuidad del negocio, considerando criterios técnicos, organizacionales y de gestión del riesgo.

El propósito es que los aprendices comprendan la importancia del Análisis de Impacto al Negocio (BIA), la formulación de estrategias efectivas y la estructuración del Plan de Continuidad del Negocio (PCN) como herramientas clave para fortalecer la resiliencia organizacional y asegurar la recuperación oportuna de los servicios críticos.

A lo largo del componente, se analizan diferentes tipos de estrategias, sus etapas de desarrollo, la aplicación de indicadores técnicos como RTO y RPO, y los beneficios que aportan los planes de continuidad en la sostenibilidad empresarial. Además, se incluyen actividades prácticas que permitirán aplicar los conceptos a contextos reales mediante la simulación de escenarios de interrupción y respuesta.

Para comprender mejor la relevancia del tema y su aplicación en la gestión moderna, se recomienda acceder al siguiente video introductorio.

Video 1. Estrategias y planes de continuidad del negocio

Enlace de reproducción del video

Síntesis del video: Estrategias y planes de continuidad del negocio
Las organizaciones actuales enfrentan un entorno lleno de desafíos, desde fallas tecnológicas y desastres naturales hasta incidentes de seguridad o interrupciones logísticas. En este contexto, la continuidad del negocio se convierte en un pilar esencial para mantener las operaciones, proteger los activos y garantizar la confianza de clientes y aliados. El proceso inicia con la definición de estrategias de continuidad, las cuales pueden ser preventivas, de mitigación, recuperación o transferencia del riesgo. Su

aplicación depende de la naturaleza de cada organización, los recursos disponibles y los resultados del Análisis de Impacto al Negocio, conocido como BIA.

El BIA permite identificar los procesos críticos, establecer los tiempos de recuperación RTO (Recovery Time Objective) y RPO (Recovery Point Objective), y evaluar los impactos financieros, operativos y reputacionales. A partir de esta información, se diseñan estrategias efectivas que aseguran que los servicios esenciales puedan continuar incluso ante una contingencia.

Una vez definidas las estrategias, se formula el Plan de Continuidad del Negocio (PCN), documento que establece los procedimientos, responsables y recursos necesarios para responder ante incidentes. Este plan se complementa con los planes de contingencia y recuperación, que detallan las acciones para mantener o restablecer los servicios en el menor tiempo posible.

Finalmente, las organizaciones deben probar y validar sus estrategias mediante simulaciones y ejercicios prácticos que permitan medir su efectividad. Estas actividades fortalecen la resiliencia institucional, fomentan la preparación del talento humano y garantizan la sostenibilidad operativa, incluso frente a los escenarios más complejos.

1. Estrategias de continuidad del negocio

Las estrategias de continuidad del negocio constituyen el conjunto de acciones, políticas y medidas planificadas para garantizar que una organización mantenga sus funciones esenciales durante y después de un evento disruptivo. Su propósito principal es minimizar el impacto de incidentes operativos, tecnológicos o ambientales sobre los procesos críticos, permitiendo una recuperación ordenada y efectiva.

El diseño de estas estrategias parte del conocimiento profundo de los procesos, activos y dependencias de la organización. En este sentido, las estrategias no deben entenderse únicamente como planes de emergencia, sino como un enfoque integral de gestión del riesgo, que promueve la resiliencia organizacional y la capacidad de adaptación frente a cambios o crisis.

Las estrategias de continuidad se aplican en diferentes niveles, dependiendo de la naturaleza y el alcance de los riesgos identificados. A nivel operativo, buscan mantener la disponibilidad de servicios esenciales mediante redundancias tecnológicas, respaldo de datos, infraestructura alterna o personal capacitado. A nivel estratégico, permiten preservar la reputación institucional, el cumplimiento normativo y la confianza de los grupos de interés.

Entre las medidas más comunes se incluyen la implementación de sitios alternos de trabajo, el uso de nubes híbridas o plataformas virtuales de respaldo, la creación de equipos de respuesta ante incidentes, y la definición de protocolos de comunicación y toma de decisiones durante contingencias.

Una estrategia de continuidad efectiva debe ser proactiva y dinámica, adaptándose a las condiciones cambiantes del entorno y al crecimiento de la organización. Por ello, su desarrollo requiere de una evaluación continua, acompañada de pruebas, simulaciones y revisiones periódicas que aseguren su eficacia y sostenibilidad en el tiempo.

Las estrategias de continuidad del negocio son un pilar esencial de la resiliencia organizacional, al garantizar la protección de los activos críticos, la estabilidad operativa y la sostenibilidad institucional frente a cualquier tipo de interrupción o crisis.

1.1. Tipos de estrategias y su aplicación organizacional

Las estrategias de continuidad del negocio se clasifican de acuerdo con su propósito, alcance y nivel de intervención dentro de la organización. Estas estrategias buscan prevenir, responder y recuperar las operaciones críticas ante eventos que puedan afectar la disponibilidad de los servicios o la integridad de los activos. Su aplicación depende del tipo de riesgo, la criticidad de los procesos y la capacidad de respuesta institucional.

Entre los tipos más comunes de estrategias se destacan las siguientes:

a) **Estrategias preventivas**: tienen como objetivo reducir la probabilidad de ocurrencia de incidentes mediante la implementación de controles y medidas de protección. Incluyen acciones como el mantenimiento preventivo de equipos, la actualización de sistemas de seguridad, la capacitación del personal, la gestión de proveedores críticos y la

redundancia tecnológica. Estas estrategias fortalecen la preparación organizacional y mitigan los efectos de posibles interrupciones.

b) **Estrategias de mitigación**: se enfocan en disminuir el impacto de un evento cuando este ocurre. Implican disponer de respaldos de información, servidores alternos, sistemas de energía ininterrumpida (UPS), o acuerdos con terceros para garantizar la continuidad de servicios esenciales. Su aplicación es clave para asegurar la operación mínima durante una contingencia.

c) **Estrategias de recuperación**: buscan restablecer los servicios y procesos afectados en el menor tiempo posible. Incluyen planes de recuperación ante desastres (DRP), restauración de datos desde copias de seguridad, traslado temporal de operaciones a sitios alternos y procedimientos de comunicación post-incidente. Estas estrategias garantizan el retorno controlado a la normalidad operativa.

d) **Estrategias de transferencia de riesgo**: consisten en delegar parte del riesgo a terceros, generalmente a través de seguros, acuerdos de respaldo mutuo o contratación de servicios especializados. Si bien no eliminan el riesgo, ayudan a mitigar su impacto económico o reputacional.

e) **Estrategias de sustitución temporal**: se aplican cuando no es posible continuar un proceso con los recursos habituales, por lo que se habilitan mecanismos alternativos, como el trabajo remoto, el uso de plataformas en la nube o la externalización de ciertas funciones críticas.

La aplicación organizacional de las estrategias de continuidad requiere un enfoque planificado y transversal, que involucre tanto la alta dirección como las diferentes áreas operativas. Este proceso parte de una evaluación integral de riesgos y del Análisis de Impacto al Negocio (BIA), los cuales permiten determinar qué procesos son críticos, qué recursos los soportan y qué nivel de interrupción puede ser tolerado.

Una vez identificadas estas variables, las estrategias se aplican de forma diferenciada según el contexto de cada organización.

Por ejemplo, en el área tecnológica, se pueden implementar esquemas de respaldo de datos o replicación de servidores; en la gestión del talento humano, planes de reemplazo de personal clave; y en las operaciones logísticas, acuerdos con proveedores alternos o rutas de distribución contingentes.

Además, la aplicación efectiva implica establecer responsables, recursos y métricas de desempeño que permitan evaluar su funcionamiento en escenarios reales o simulados. La comunicación interna, la capacitación del personal y la revisión periódica de los planes son elementos indispensables para asegurar que las estrategias mantengan su vigencia frente a cambios en el entorno o en la estructura organizacional.

La aplicación organizacional de las estrategias de continuidad debe abordarse como un proceso estructurado, articulado con el Sistema de Gestión de Continuidad del Negocio (SGCN) y con la estrategia corporativa general. Este proceso se desarrolla en varias etapas:

1) **Planeación**: consiste en definir los objetivos de continuidad, identificar los procesos críticos y seleccionar las estrategias más adecuadas de acuerdo con el análisis de riesgos y el BIA.
2) **Implementación**: incluye la asignación de recursos, la elaboración de procedimientos, la capacitación del personal y la comunicación de las responsabilidades. En esta fase se formalizan los planes y se integran a la operación diaria.
3) **Ejecución y monitoreo**: corresponde a la puesta en marcha de las estrategias cuando ocurre un evento disruptivo, garantizando la continuidad de los procesos priorizados. Incluye el seguimiento en tiempo real, la toma de decisiones y la activación de los equipos de respuesta.
4) **Evaluación y mejora continua**: una vez controlado el incidente, se realiza un análisis de desempeño para identificar aciertos, fallas y oportunidades de mejora. Esta retroalimentación fortalece la preparación institucional para futuros eventos.

Este enfoque cíclico asegura que las estrategias no sean acciones aisladas, sino parte de un sistema vivo y adaptable. Al integrarlas en la gestión organizacional, se fortalecen la resiliencia, la capacidad de respuesta y la sostenibilidad operativa frente a escenarios cambiantes o de alta incertidumbre.

1.2. Criterios técnicos para la selección de estrategias de continuidad

La selección de estrategias de continuidad del negocio requiere un análisis técnico riguroso que garantice su viabilidad, efectividad y alineación con los objetivos institucionales. Este proceso implica evaluar las condiciones internas y

externas de la organización, los recursos disponibles y la capacidad de respuesta ante posibles interrupciones. Una estrategia efectiva no solo debe ser técnicamente sólida, sino también económicamente sostenible y operativamente alcanzable.

Los criterios técnicos que deben considerarse en este proceso incluyen los siguientes:

Tabla 1. Matriz de criterios técnicos para la selección de estrategias de continuidad

Criterio técnico	Descripción	Ejemplo de aplicación
Análisis costo-beneficio.	Evalúa la relación entre el costo de la estrategia y el valor de los activos que protege, priorizando la rentabilidad y sostenibilidad.	Implementar un sistema de respaldo automatizado que reduzca el tiempo de inactividad frente al costo de un servidor manual.
Capacidad tecnológica y operativa.	Analiza si la infraestructura, el personal y los procesos existentes soportan la estrategia seleccionada.	Verificar si el ancho de banda y el soporte técnico permiten una migración efectiva a la nube.
Compatibilidad con RTO y RPO.	Asegura que las estrategias respondan a los tiempos máximos de	Configurar respaldos automáticos cada hora

Criterio técnico	Descripción	Ejemplo de aplicación
	recuperación y pérdida de datos definidos.	para cumplir con un RPO de una hora.
Cumplimiento normativo y regulatorio.	Garantiza que las estrategias estén alineadas con las normas ISO y la legislación nacional.	Alinear el plan de continuidad con los requisitos de la ISO 22301 y la Ley 1581 de 2012.
Escalabilidad y flexibilidad.	Permite adaptar la estrategia a cambios en la organización o el entorno sin perder eficacia.	Ampliar la capacidad de almacenamiento en la nube al aumentar el número de usuarios o sedes.
Integración con otros sistemas de gestión.	Favorece la coherencia entre los sistemas de calidad, seguridad, riesgos y continuidad.	Incorporar controles de continuidad en el Sistema de Gestión de la Calidad (ISO 9001).
Madurez organizacional.	Evalúa el grado de desarrollo de la cultura de seguridad y gestión del riesgo.	Capacitar al personal y crear comités de continuidad antes de

Criterio técnico	Descripción	Ejemplo de aplicación
		implementar medidas avanzadas.

El cumplimiento de estos criterios permite seleccionar estrategias realistas, sostenibles y coherentes con las capacidades institucionales. La combinación equilibrada entre viabilidad técnica, sostenibilidad económica y cumplimiento normativo garantiza que la organización esté preparada para enfrentar incidentes sin comprometer la estabilidad de sus operaciones.

1.3. Validación de estrategias de continuidad del negocio

La validación de estrategias de continuidad del negocio constituye una fase esencial dentro del ciclo de gestión de la continuidad, ya que permite comprobar la eficacia, pertinencia y capacidad de respuesta de las estrategias implementadas frente a diferentes escenarios de interrupción. Validar implica más que revisar documentos o protocolos; supone verificar, mediante pruebas controladas y análisis de resultados, que las medidas adoptadas realmente funcionan en la práctica.

El proceso de validación tiene como objetivo asegurar que las estrategias seleccionadas sean viables, actualizadas y acordes con la realidad operativa de la organización. Para ello, se aplican diferentes métodos que permiten evaluar tanto la preparación técnica como la respuesta humana y procedimental ante una crisis.

Entre las principales modalidades de validación se encuentran:

Tabla 2. Tipos de pruebas de validación de estrategias de continuidad

Tipo de prueba	Descripción	Objetivo	Frecuencia recomendada	Alcance
Prueba de escritorio.	Simulación teórica basada en escenarios hipotéticos. Se realiza en reuniones con los equipos responsables.	Evaluar la comprensión del plan, los roles y la toma de decisiones.	Al menos una vez al año.	Nivel estratégico y táctico.
Prueba funcional o parcial.	Ejecución controlada de componentes específicos del plan, como respaldo de datos o activación de	Comprobar la operatividad de procedimientos o recursos críticos.	Según criticidad de procesos (cada 6 o 12 meses).	Nivel operativo.

Tipo de prueba	Descripción	Objetivo	Frecuencia recomendada	Alcance
	un sistema alterno.			
Prueba integral.	Simulación completa de un evento disruptivo, involucrando todas las áreas relevantes.	Evaluar la efectividad global del plan y la coordinación interdepartamental.	Anual o semestral.	Toda la organización.
Revisión documental.	Análisis de políticas, registros y procedimientos actualizados.	Asegurar coherencia con los cambios normativos y tecnológicos.	Trimestral o ante cambios relevantes.	Nivel administrativo.

Una vez finalizadas las pruebas, se debe elaborar un informe de resultados que documente los hallazgos, las lecciones aprendidas y las acciones de mejora necesarias. Este proceso de retroalimentación fortalece el Sistema de Gestión de

Continuidad del Negocio (SGCN) y permite ajustar los procedimientos para optimizar la respuesta ante incidentes.

La validación debe realizarse de manera periódica y planificada, preferiblemente al menos una vez al año o cuando se produzcan cambios significativos en los procesos, la tecnología o el personal clave.

En síntesis, la validación garantiza que las estrategias de continuidad del negocio no solo existan en papel, sino que sean operativas, confiables y efectivas, consolidando una cultura de mejora continua y resiliencia organizacional frente a situaciones adversas.

2. Análisis de Impacto al Negocio (BIA)

El Análisis de Impacto al Negocio (BIA, por sus siglas en inglés) constituye una herramienta esencial dentro de la gestión de continuidad del negocio, cuya finalidad es identificar los procesos y recursos críticos de una organización y determinar las consecuencias que tendría su interrupción. A través de este análisis, las entidades pueden comprender la magnitud del impacto que un evento disruptivo puede generar en las operaciones, los ingresos, la reputación o el cumplimiento normativo.

El BIA proporciona una base sólida para la toma de decisiones estratégicas en materia de continuidad y recuperación, ya que permite establecer prioridades, definir tiempos máximos de recuperación (RTO), pérdidas máximas de datos aceptables (RPO) y recursos necesarios para garantizar el funcionamiento mínimo de los servicios esenciales.

Su aplicación contribuye a fortalecer la resiliencia organizacional, ya que permite anticiparse a los efectos de incidentes como fallas tecnológicas,

ciberataques, desastres naturales o interrupciones en la cadena de suministro. Además, el BIA sirve como punto de partida para el diseño de estrategias efectivas y planes de continuidad del negocio (PCN), asegurando que las decisiones estén sustentadas en información objetiva y medible.

Por ejemplo, una empresa de servicios financieros puede utilizar el BIA para determinar que la interrupción del sistema de pagos electrónicos tendría un impacto crítico en menos de una hora, mientras que la suspensión temporal del correo institucional tendría un efecto moderado y una recuperación más flexible. Esta priorización permite asignar recursos de manera eficiente y focalizar las estrategias en los procesos verdaderamente vitales.

En conclusión, el BIA no solo identifica lo que es crítico para la operación, sino que orienta las acciones que permitirán mantener la continuidad, minimizar pérdidas y garantizar la sostenibilidad del negocio ante cualquier eventualidad.

2.1. Metodología del BIA y su importancia en la gestión de continuidad

La metodología del Análisis de Impacto al Negocio (BIA) proporciona un marco estructurado para identificar los procesos críticos, evaluar las consecuencias de su interrupción y establecer prioridades de recuperación. Este proceso constituye una etapa clave dentro del Sistema de Gestión de Continuidad del Negocio (SGCN), pues traduce los impactos potenciales en información medible y útil para la toma de decisiones estratégicas.

Su importancia radica en que permite comprender la dependencia entre procesos, activos y recursos, así como cuantificar los efectos financieros, operativos, legales y reputacionales que surgirían ante diferentes escenarios de interrupción. De

este modo, el BIA se convierte en un insumo fundamental para diseñar estrategias realistas, asignar recursos eficientemente y mantener la resiliencia institucional.

A continuación, se describen las principales etapas metodológicas del BIA:

a) Planificación y alcance

- ✓ En esta fase se define el propósito del BIA, los procesos que serán analizados y los responsables de su ejecución. Se establecen los criterios de evaluación, las unidades de medida del impacto y los umbrales de tolerancia de la organización.
- ✓ Ejemplo: determinar si el análisis cubrirá solo los procesos misionales o también los de apoyo, y quiénes serán los líderes de cada área involucrada.

b) Identificación de procesos críticos y recursos asociados

- ✓ Consiste en listar los procesos operativos, estratégicos y de soporte, junto con los recursos humanos, tecnológicos, financieros e infraestructurales que los sustentan.
- ✓ Ejemplo: un proceso crítico como “gestión de pagos” puede depender de servidores financieros, bases de datos, personal contable y proveedores externos.

c) Evaluación de impactos

- ✓ En esta etapa se analizan los efectos que tendría la interrupción de cada proceso durante distintos periodos de tiempo (por ejemplo, 2, 8, 24 o 48 horas). Los impactos se clasifican en categorías:
    - **Operativos**: pérdida de productividad, atrasos o parálisis de actividades.

- **Financieros**: pérdida de ingresos, sanciones o costos adicionales.
- **Reputacionales**: deterioro de la confianza de clientes o aliados.
- **Legales o normativos**: incumplimiento de leyes, contratos o regulaciones.

✓ Ejemplo: la interrupción del sistema de facturación por más de 12 horas puede ocasionar sanciones por incumplimiento con la DIAN y pérdida de ventas.

d) Determinación de RTO y RPO

✓ Se definen los tiempos máximos de recuperación (RTO) y los niveles de pérdida de datos aceptables (RPO) para cada proceso, lo que orienta las decisiones técnicas y financieras en la implementación de estrategias de continuidad.

✓ Ejemplo: un área de atención al cliente puede tener un RTO de 6 horas y un RPO de 1 hora, mientras que un sistema de soporte interno puede tolerar tiempos más amplios.

e) Priorización y documentación de resultados

✓ Con base en los análisis anteriores, se clasifican los procesos según su nivel de criticidad y se elaboran reportes que describen los impactos esperados, las dependencias, los recursos necesarios y los tiempos objetivos de recuperación.

✓ Ejemplo: elaborar una matriz que relacione los procesos con su nivel de impacto y prioridad de atención, sirviendo como base para los planes de continuidad.

f) Revisión y actualización periódica

- ✓ El BIA no es un documento estático; debe revisarse regularmente o cuando ocurran cambios significativos en la estructura organizacional, los servicios o el entorno tecnológico.
- ✓ Ejemplo: actualizar el análisis tras la apertura de una nueva sede o la implementación de un nuevo sistema de gestión documental.

En conjunto, esta metodología permite establecer un enfoque sistemático para proteger los procesos esenciales, optimizar recursos y fortalecer la capacidad de respuesta institucional. Un BIA correctamente ejecutado asegura que las estrategias de continuidad del negocio estén alineadas con la realidad operativa y los objetivos estratégicos de la organización, convirtiéndose en una herramienta vital para garantizar su sostenibilidad y resiliencia ante cualquier eventualidad.

2.2. Identificación y priorización de procesos críticos

La identificación y priorización de procesos críticos es una de las fases más relevantes dentro del Análisis de Impacto al Negocio (BIA), ya que permite determinar cuáles funciones son esenciales para la continuidad operativa de la organización y qué grado de afectación tendría su interrupción. Este proceso facilita enfocar los esfuerzos en aquellas actividades que sustentan la misión institucional, los compromisos legales y la confianza de los clientes o usuarios.

Un proceso crítico se define como aquel cuya interrupción comprometería gravemente la capacidad de la organización para cumplir sus objetivos estratégicos o regulatorios. Para identificarlo, es necesario analizar la interdependencia entre áreas, los recursos que lo soportan y los impactos que se generarían si dejara de operar durante un periodo determinado.

A continuación, se presenta una metodología orientativa para realizar esta identificación y priorización de manera sistemática:

a) **Identificación de los procesos organizacionales**
   - ✓ Se elabora un inventario que incluya los procesos misionales, estratégicos y de apoyo. Esta información suele obtenerse a partir de los mapas de procesos o los sistemas de gestión de calidad existentes.
   - ✓ Ejemplo: en una entidad educativa, los procesos misionales podrían ser “gestión académica”, “evaluación del aprendizaje” y “admisiones”; mientras que los procesos de apoyo incluyen “tecnología de la información” o “recursos humanos”.

b) **Análisis de dependencias internas y externas**
   - ✓ Cada proceso se analiza en función de los recursos, servicios o proveedores que necesita para operar correctamente, así como de las áreas que dependen de él.
   - ✓ Ejemplo: el proceso de “gestión financiera” depende del sistema contable y del acceso a la red bancaria, pero también provee información a “gestión de compras” y “tesorería”.

c) **Evaluación del impacto ante interrupciones**
   - ✓ Se evalúan las consecuencias de una interrupción temporal en cada proceso, considerando los impactos operativos, financieros, reputacionales, legales y de seguridad.

- ✓ Ejemplo: la suspensión de la “plataforma de aprendizaje” en un centro de formación tendría un impacto operativo alto por la imposibilidad de impartir formación y evaluaciones virtuales.

d) Priorización según el nivel de criticidad

- ✓ Con base en los resultados del análisis, los procesos se clasifican según su nivel de criticidad: crítico, alto, medio o bajo. Este nivel se determina a partir de la magnitud del impacto y del tiempo máximo de recuperación (RTO) que la organización puede tolerar sin comprometer su operatividad.
- ✓ Ejemplo:
  - **Crítico**: sistema de gestión académica (RTO = 4 horas).
  - **Alto**: gestión de nómina (RTO = 12 horas).
  - **Medio**: atención al público (RTO = 24 horas).
  - **Bajo**: actividades de archivo físico (RTO = 72 horas).

e) Documentación y comunicación de resultados

- ✓ Los resultados se consolidan en una matriz o informe de priorización que servirá como insumo para definir las estrategias de continuidad.
- ✓ Este documento debe ser validado por la alta dirección y compartido con los responsables de cada área.

Para dar contexto a la metodología anterior, se presenta el siguiente ejemplo práctico:

Una empresa del sector logístico realiza un BIA con el fin de fortalecer su sistema de continuidad del negocio. En el proceso de análisis, se identifican los

principales procesos que soportan la operación y se evalúan sus interdependencias, recursos asociados e impactos ante una interrupción prolongada.

Entre los resultados se destacan los siguientes procesos críticos:

- ✓ **Gestión de transporte**: su interrupción impactaría directamente la entrega oportuna de mercancías, ocasionando retrasos, pérdida de contratos y sanciones por incumplimiento. Este proceso depende de sistemas de rastreo satelital, disponibilidad de vehículos, personal operativo y comunicación con clientes.
- ✓ **Atención a clientes**: su suspensión generaría pérdida de confianza, deterioro de la reputación e incumplimiento de acuerdos de nivel de servicio (SLA). Depende de plataformas CRM, canales de comunicación y personal capacitado en gestión de reclamos.
- ✓ **Gestión de inventarios**: una falla en este proceso afectaría el control de existencias, la trazabilidad de productos y la planeación de despachos, con impacto financiero y operativo significativo.

Luego del análisis, la organización clasifica estos procesos como críticos, con RTO de entre 4 y 8 horas y establece medidas como respaldo tecnológico, replicación de servidores, capacitación del personal y acuerdos con operadores alternos de transporte.

En conclusión, la identificación y priorización de procesos críticos permiten a las organizaciones enfocar sus esfuerzos en lo verdaderamente esencial, asignar recursos estratégicamente y fortalecer su capacidad de respuesta frente a eventos disruptivos. Este enfoque sistemático no solo mejora la gestión del riesgo, sino que

constituye la base para el desarrollo de planes de continuidad del negocio sólidos y sostenibles.

2.3. Determinación de RTO y RPO

La determinación de los tiempos máximos de recuperación constituye un componente esencial del Análisis de Impacto al Negocio (BIA), ya que permite establecer límites temporales aceptables para restablecer los procesos críticos y recuperar la información afectada tras un incidente. Estos tiempos orientan las decisiones técnicas, financieras y operativas relacionadas con las estrategias de continuidad del negocio.

En la práctica, se definen dos parámetros fundamentales:

- ✓ **RTO (Recovery Time Objective)**: es el tiempo máximo que un proceso o sistema puede permanecer inactivo antes de que la interrupción afecte gravemente la operación o la sostenibilidad del negocio. Representa el plazo dentro del cual deben restaurarse los servicios críticos para evitar daños significativos.
- ✓ **RPO (Recovery Point Objective)**: es la cantidad máxima de datos que la organización puede permitirse perder, medida en tiempo. Determina el momento hasta el cual deben estar disponibles los respaldos o copias de seguridad de la información.

Ambos parámetros son interdependientes: el RTO se relaciona con el tiempo de recuperación de la operación, mientras que el RPO está vinculado con la pérdida de datos aceptable. Establecerlos correctamente garantiza que las estrategias de

respaldo, replicación y recuperación estén alineadas con los requerimientos reales del negocio.

A continuación, se presentan las principales etapas para su determinación:

1) **Identificación del impacto temporal**: se analiza cómo varía el impacto de la interrupción a medida que transcurre el tiempo. Esto permite establecer puntos críticos en los que las pérdidas se vuelven insostenibles. Por ejemplo, un banco puede tolerar una hora de interrupción en su plataforma de pagos (RTO = 1 hora), pero no más de 15 minutos de pérdida de información (RPO = 15 minutos).
2) **Definición de los niveles de servicio aceptables**: se establecen los umbrales de tolerancia que la organización está dispuesta a aceptar antes de que un proceso se considere en falla crítica. Por ejemplo, una empresa de comercio electrónico puede definir que su sitio web debe estar operativo el 99,9 % del tiempo, lo que limita su RTO a menos de 30 minutos.
3) **Evaluación de capacidades técnicas y recursos disponibles**: el RTO y el RPO deben definirse considerando la infraestructura tecnológica, la redundancia de sistemas, las capacidades del personal y los mecanismos de respaldo existentes. Por ejemplo, si la empresa no cuenta con replicación en tiempo real, el RPO podría ampliarse a 4 horas para ajustarse a las capacidades actuales.
4) **Documentación y validación**: los tiempos definidos se registran en el informe del BIA y deben ser validados por la alta dirección y los

responsables de cada área. Además, deben revisarse periódicamente para ajustarse a cambios tecnológicos o de operación.

Para contextualizar la información, se presenta un ejemplo claro de la determinación de RTO y RPO:

Tabla 3. Ejemplo de determinación de RTO y RPO en procesos críticos

Proceso crítico	Impacto ante interrupción	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Estrategias asociadas
Plataforma de pagos electrónicos.	Muy alto (pérdida de ingresos, reputación y cumplimiento legal).	1 hora	15 minutos	Replicación en tiempo real, respaldo automático, servidor alterno.
Sistema contable y financiero.	Alto (retraso en reportes y obligaciones fiscales).	8 horas	2 horas	Copias de respaldo diarias, almacenamiento seguro en la nube.

Proceso crítico	Impacto ante interrupción	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Estrategias asociadas
Gestión de clientes (CRM).	Medio (afecta atención y seguimiento comercial).	12 horas	4 horas	Sincronización en la nube y respaldo incremental.
Portal web institucional.	Bajo (afecta comunicación externa temporalmente).	24 horas	12 horas	Servidor espejo y sistema de monitoreo.

El análisis de esta información permite comprender cómo las organizaciones pueden establecer parámetros diferenciados de recuperación según la criticidad de sus procesos. Cada proceso presenta características y requerimientos únicos, por lo que los valores de RTO y RPO no deben interpretarse como estándares fijos, sino como referencias personalizadas que orientan la toma de decisiones. Este tipo de análisis facilita priorizar recursos, definir estrategias adecuadas de respaldo y determinar los mecanismos de comunicación y coordinación necesarios durante una contingencia.

Para dar mayor claridad a la metodología, a continuación, se presenta un ejemplo práctico que aclara su aplicación en un entorno real:

Una empresa de servicios de salud realiza su BIA y determina los tiempos de recuperación de los procesos más sensibles:

- ✓ Para el sistema de historias clínicas electrónicas, define un RTO de 2 horas y un RPO de 30 minutos, debido a la criticidad de la información médica.
- ✓ El proceso de facturación de servicios médicos obtiene un RTO de 8 horas y un RPO de 2 horas, pues una interrupción prolongada afectaría el flujo de ingresos y los reportes regulatorios.
- ✓ En el caso de la plataforma de agendamiento de citas, se establece un RTO de 4 horas y un RPO de 1 hora, ya que su inactividad afecta directamente la atención al paciente.

Con base en estos parámetros, la organización implementa estrategias de replicación en tiempo real, sistemas redundantes y planes de comunicación para garantizar la continuidad operativa.

En conclusión, la determinación de los tiempos máximos de recuperación (RTO y RPO) es esencial para planificar acciones de respuesta acordes con la capacidad institucional y las necesidades del negocio. Estos indicadores proporcionan un marco objetivo para diseñar estrategias de respaldo, priorizar recursos y fortalecer la resiliencia organizacional ante posibles interrupciones.

2.4. Evaluación de impactos operativos, financieros y reputacionales

La evaluación de impactos constituye una fase fundamental del Análisis de Impacto al Negocio (BIA), ya que permite determinar las consecuencias que tendría la interrupción de los procesos críticos sobre la estabilidad y sostenibilidad de la organización. Este análisis no solo cuantifica las pérdidas económicas, sino que también considera los efectos en la operación, la reputación institucional y el cumplimiento legal o normativo.

El propósito principal de esta evaluación es establecer prioridades de recuperación y orientar la asignación de recursos a las áreas más vulnerables. Para lograrlo, se analizan tres tipos de impacto: operativo, financiero y reputacional, los cuales deben ser valorados de forma integral, considerando su interdependencia.

- ✓ **Impacto operativo**: hace referencia a la afectación sobre la capacidad de la organización para ejecutar sus funciones esenciales. Una interrupción operativa puede traducirse en retrasos en la producción, pérdida de eficiencia o incumplimiento de compromisos con los clientes. Por ejemplo, si un sistema de gestión logística falla, los pedidos pueden no ser despachados a tiempo, generando retrasos en la cadena de suministro y afectando la satisfacción del cliente.
- ✓ **Impacto financiero**: se relaciona con las pérdidas económicas derivadas de la interrupción, incluyendo costos directos (reparaciones, reemplazos, multas) e indirectos (pérdida de ventas, penalizaciones contractuales o disminución de ingresos). Por ejemplo, en una entidad bancaria, una caída de su plataforma de pagos durante varias horas

podría generar pérdidas millonarias por transacciones no procesadas, además de afectar su flujo de caja diario.

- ✓ **Impacto reputacional**: evalúa el efecto que una interrupción o incumplimiento puede tener sobre la imagen y la confianza de clientes, socios y la sociedad en general. En muchos casos, este impacto puede superar las pérdidas económicas iniciales. Por ejemplo, una empresa de servicios públicos que no comunique adecuadamente una falla prolongada podría ver deteriorada su reputación, generando desconfianza y pérdida de usuarios.

Para estructurar la evaluación, se recomienda utilizar una matriz que asigne valores de severidad (alta, media o baja) a cada tipo de impacto, de acuerdo con la duración de la interrupción y la criticidad del proceso afectado.

Tabla 4. Ejemplo de evaluación de impactos en procesos críticos

Proceso crítico	Impacto operativo	Impacto financiero	Impacto reputacional	Nivel global de impacto
Sistema de facturación.	Alto (retraso en pagos y reportes contables).	Alto (pérdida de ingresos).	Medio (afecta confianza de proveedores).	Alto
Plataforma web comercial.	Medio (interrupción	Alto (disminución de	Alto (afecta percepción de clientes).	Alto

Proceso crítico	Impacto operativo	Impacto financiero	Impacto reputacional	Nivel global de impacto
	temporal de ventas).	ingresos diarios).		
Gestión de personal.	Medio (demora en pagos o trámites).	Bajo (afecta costos administrativos).	Bajo (impacto interno limitado).	Medio
Infraestructura tecnológica.	Alto (afecta todos los sistemas dependientes).	Alto (costos de recuperación elevados).	Alto (riesgo reputacional por fallas críticas).	Crítico

La información obtenida de esta matriz permite a la organización jerarquizar procesos según su nivel de impacto y establecer estrategias de respuesta más precisas. Por ejemplo, los procesos clasificados como “críticos” deben contar con medidas de respaldo redundantes y protocolos de comunicación específicos para minimizar los daños.

En conclusión, la evaluación de impactos operativos, financieros y reputacionales ofrece una visión integral del riesgo empresarial. Este enfoque facilita la toma de decisiones informadas, fortalece la planificación estratégica y contribuye

a consolidar una cultura organizacional orientada a la resiliencia y la continuidad del negocio.

3. Diseño de estrategias de continuidad del negocio

El diseño de estrategias de continuidad del negocio constituye una de las fases más críticas dentro de la gestión de la resiliencia organizacional, ya que permite transformar los resultados del Análisis de Impacto al Negocio (BIA) y la evaluación de riesgos en acciones concretas que garanticen la operación continua de los procesos esenciales. En esta etapa, se definen las medidas, recursos y procedimientos necesarios para prevenir interrupciones, mitigar sus efectos y asegurar la recuperación oportuna de los servicios críticos.

El diseño de una estrategia efectiva debe responder a tres principios fundamentales: prevención, mitigación y recuperación. Esto implica anticipar los posibles escenarios de interrupción, definir cómo mantener las funciones esenciales durante la crisis y establecer mecanismos para restaurar la normalidad en el menor tiempo posible.

En la práctica, el proceso de diseño parte de la información obtenida del BIA, donde se identifican los procesos críticos, los tiempos máximos de recuperación (RTO), la pérdida de datos aceptable (RPO) y los impactos asociados. Con base en estos datos, se seleccionan las estrategias más adecuadas según el contexto, los recursos disponibles y las capacidades tecnológicas y humanas de la organización.

Por ejemplo, una empresa de servicios financieros puede diseñar estrategias basadas en la replicación de datos en tiempo real, el uso de servidores espejo y la implementación de centros alternos de operaciones, para garantizar la continuidad

de sus servicios ante una falla tecnológica o desastre natural. Por su parte, una institución educativa puede definir estrategias de plataformas virtuales de respaldo, docencia remota y comunicación digital de emergencia, para mantener la prestación del servicio formativo ante contingencias.

El diseño también requiere establecer los niveles de responsabilidad, las líneas de comunicación y los recursos necesarios para la ejecución de las estrategias. Es indispensable que estas medidas sean realistas, sostenibles y verificables, es decir, que puedan ponerse en práctica con los medios existentes y ajustarse a los cambios del entorno o de la estructura organizacional.

Asimismo, el diseño de estrategias debe estar alineado con la política de continuidad del negocio, los planes de gestión de riesgos, y los sistemas de gestión integrados (como ISO 22301, ISO 27001 o ISO 9001), para garantizar coherencia y cumplimiento normativo.

Finalmente, las estrategias diseñadas deben someterse a procesos de validación, prueba y mejora continua, asegurando que respondan eficazmente a los escenarios previstos y que se actualicen conforme evolucionan las tecnologías, las amenazas o las condiciones del negocio. Su éxito depende de la correcta interpretación de la información del BIA, la articulación interinstitucional y la capacidad de anticipar los posibles impactos, fortaleciendo así la resiliencia y sostenibilidad de la organización frente a cualquier eventualidad.

3.1. Características de las estrategias efectivas

Las estrategias de continuidad del negocio son efectivas cuando logran garantizar que los procesos críticos puedan mantenerse o restablecerse dentro de

los tiempos definidos (RTO y RPO), con el menor impacto posible para la organización. Su eficacia depende no solo de la solidez técnica de las medidas implementadas, sino también de su alineación con la estructura organizacional, los recursos disponibles y la cultura de resiliencia institucional.

Una estrategia efectiva debe ser integral, práctica y adaptable. Su diseño debe contemplar tanto los aspectos tecnológicos como los humanos, logísticos y comunicacionales, asegurando que la organización esté preparada para actuar antes, durante y después de una interrupción.

A continuación, se presentan las principales características que debe cumplir una estrategia de continuidad efectiva:

Tabla 5. Criterios y ejemplos de estrategias de continuidad efectivas

Característica	Descripción	Ejemplo de aplicación
Integración.	La estrategia debe estar alineada con los sistemas de gestión existentes (calidad, seguridad de la información, riesgos, etc.) y con los objetivos institucionales.	Integrar las medidas de continuidad dentro del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO 27001.
Viabilidad técnica y económica.	Debe ser factible de implementar con los recursos y capacidades	Implementar respaldos automáticos en la nube, en lugar de montar un

Característica	Descripción	Ejemplo de aplicación
	reales de la organización, sin generar sobrecostos o complejidades innecesarias.	centro de datos alterno de alto costo.
Flexibilidad y escalabilidad.	Debe poder adaptarse a cambios en la estructura organizacional, la tecnología o el entorno operativo.	Ampliar la capacidad del sistema de respaldo a medida que aumentan los usuarios o los servicios digitales.
Simplicidad operativa.	Debe ser clara y comprensible para todos los niveles de la organización, evitando procedimientos excesivamente técnicos o difíciles de ejecutar.	Incluir protocolos paso a paso en el Plan de Continuidad para facilitar su ejecución por cualquier responsable.
Medibilidad y control.	Debe permitir evaluar su desempeño mediante indicadores o métricas que reflejen su efectividad.	Medir el tiempo real de recuperación de un servidor frente al RTO establecido.

Característica	Descripción	Ejemplo de aplicación
Enfoque preventivo.	Prioriza la anticipación y mitigación del riesgo antes de que ocurra la interrupción.	Mantener mantenimiento preventivo y actualizaciones de software para evitar fallas críticas.
Actualización continua.	Debe revisarse y mejorarse regularmente según los resultados de pruebas, auditorías y cambios en el entorno.	Revisar las estrategias anualmente o tras eventos relevantes como ciberataques o cambios regulatorios.

Además de estas características, una estrategia efectiva debe contar con respaldo de la alta dirección, garantizar la comunicación oportuna entre las áreas involucradas y fomentar una cultura de compromiso entre el personal. La efectividad no solo depende de los recursos tecnológicos, sino también del nivel de preparación humana para responder ante emergencias.

Por ejemplo, una organización que dispone de sistemas de respaldo automáticos, pero no capacita a su personal para activarlos correctamente, podría fallar en su respuesta ante una contingencia. Por ello, las estrategias deben contemplar tanto los aspectos técnicos como los procedimentales y humanos.

En conclusión, las estrategias efectivas son aquellas que logran equilibrio entre viabilidad, eficiencia y adaptabilidad, permitiendo a la organización responder de manera ordenada, minimizar pérdidas y mantener la confianza de sus partes interesadas ante cualquier interrupción significativa.

3.2. Etapas y pasos para la formulación de estrategias

La formulación de estrategias de continuidad del negocio constituye un proceso sistemático que permite diseñar y estructurar acciones concretas para garantizar la recuperación y sostenibilidad operativa ante interrupciones. Su desarrollo debe seguir una secuencia lógica que asegure la coherencia entre los resultados del Análisis de Impacto al Negocio (BIA), la evaluación de riesgos y los objetivos institucionales.

El proceso se organiza generalmente en etapas interdependientes, cada una con actividades específicas orientadas a construir un plan de acción sólido y realista. Estas etapas son:

a) **Diagnóstico y análisis preliminar**: en esta etapa se recopila la información clave sobre los procesos críticos, activos de información, riesgos asociados y tiempos máximos de recuperación (RTO y RPO). El propósito es conocer la situación actual de la organización y sus vulnerabilidades. Por ejemplo, identificar que el sistema financiero depende de un único servidor central sin respaldo en la nube.
b) **Definición de objetivos y alcance**: se establecen los propósitos de la estrategia, los procesos incluidos y los límites operativos. El alcance puede abarcar toda la organización o concentrarse en áreas críticas. Por

ejemplo, formular una estrategia específica para asegurar la continuidad del servicio al cliente y la facturación electrónica.

c) **Selección de alternativas de continuidad**: a partir de los riesgos identificados, se evalúan distintas opciones de respuesta y recuperación, tales como sitios alternos, respaldo en la nube, redundancia de servidores, planes de reemplazo de personal o acuerdos con terceros. Por ejemplo, contratar un centro de datos externo como respaldo ante fallos en la infraestructura principal.

d) **Evaluación técnica, financiera y operativa**: cada alternativa debe analizarse en función de su viabilidad técnica, costo-beneficio y compatibilidad con las capacidades organizacionales. Se priorizan las soluciones que ofrezcan equilibrio entre eficiencia y sostenibilidad.

e) **Diseño y documentación de la estrategia**: en esta fase se formalizan los procedimientos, responsables, recursos y cronogramas. La documentación debe incluir protocolos de activación, comunicación, seguimiento y retorno a la normalidad.

f) **Validación y aprobación**: la estrategia diseñada se presenta a la alta dirección para su revisión, prueba y validación. Es importante que su aprobación esté acompañada de la asignación de recursos y compromisos institucionales.

g) **Implementación y mejora continua**: finalmente, las estrategias se ponen en marcha mediante simulaciones, capacitaciones y ejercicios prácticos. Los resultados obtenidos permiten identificar oportunidades de mejora, fortaleciendo la capacidad de respuesta y la cultura de resiliencia organizacional.

Para una mejor comprensión del proceso, a continuación, se presenta una tabla que resume las etapas, objetivos, actividades y resultados esperados en la formulación de estrategias de continuidad del negocio. Este formato permite demostrar de forma estructurada los pasos necesarios para diseñar e implementar estrategias efectivas.

Tabla 6. Etapas del proceso de formulación de estrategias de continuidad del negocio

Etapa	Objetivo principal	Actividades clave	Resultado esperado
Diagnóstico y análisis preliminar.	Identificar el contexto y vulnerabilidades.	Revisión del BIA, análisis de riesgos.	Mapa de procesos y riesgos críticos.
Definición de objetivos y alcance.	Determinar prioridades y límites.	Reuniones con líderes de proceso.	Documento de alcance y objetivos.
Selección de alternativas.	Elegir opciones de continuidad adecuadas.	Evaluación técnica y operativa.	Lista de estrategias viables.
Evaluación técnica y financiera.	Analizar viabilidad y costos.	Estimación de recursos y beneficios.	Estrategia priorizada por factibilidad.

Etapa	Objetivo principal	Actividades clave	Resultado esperado
Diseño y documentación.	Formalizar la estrategia.	Elaboración de procedimientos y protocolos.	Documento de estrategia validado.
Validación y aprobación.	Garantizar respaldo institucional.	Revisión por la alta dirección.	Estrategia aprobada e institucionalizada.
Implementación y mejora continua.	Ejecutar y optimizar la estrategia.	Simulacros, capacitaciones y auditorías.	Estrategia operativa y actualizada.

La formulación de estrategias de continuidad del negocio no debe entenderse como una tarea aislada, sino como un proceso cíclico y colaborativo que involucra a todas las áreas de la organización. Cada etapa aporta información y decisiones clave que, en conjunto, permiten construir una respuesta sólida frente a contingencias, garantizando la resiliencia institucional y la continuidad de los servicios esenciales.

3.3. Aplicación de criterios técnicos y de gestión en el diseño

El diseño de estrategias de continuidad del negocio requiere un equilibrio entre los criterios técnicos y de gestión, de manera que las soluciones planteadas sean viables, sostenibles y coherentes con la realidad operativa de la organización.

Estos criterios garantizan que las estrategias no solo respondan a los riesgos identificados, sino que también se integren de manera efectiva en la estructura organizacional, la cultura institucional y los sistemas de gestión existentes.

Los criterios técnicos se enfocan en la capacidad de los recursos tecnológicos, la infraestructura y los mecanismos de respaldo para soportar las estrategias definidas. Por su parte, los criterios de gestión están orientados a la planeación, asignación de responsabilidades, coordinación interdepartamental, seguimiento y mejora continua de las acciones de continuidad.

Entre los principales criterios aplicables al diseño se destacan los siguientes:

Tabla 7. Criterios técnicos y de gestión en el diseño de estrategias de continuidad

Tipo de criterio	Criterio específico	Descripción	Ejemplo de aplicación
Técnico	Viabilidad tecnológica.	Evalúa la compatibilidad de la estrategia con los sistemas y recursos existentes.	Implementar replicación en la nube solo si la infraestructura actual soporta el volumen de datos.
Técnico	Capacidad de recuperación.	Determina si los mecanismos de respaldo y recuperación	Configurar copias automáticas cada hora para garantizar una

Tipo de criterio	Criterio específico	Descripción	Ejemplo de aplicación
		cumplen con los tiempos definidos (RTO y RPO).	pérdida máxima de una hora de datos.
Técnico	Redundancia y disponibilidad.	Asegura que existan recursos alternos para continuar la operación ante fallas del sistema principal.	Tener servidores espejo en otra sede o proveedor externo.
De gestión	Gobernanza y roles definidos.	Establece responsables y procedimientos claros para la activación y control de las estrategias.	Designar un líder de continuidad en cada área crítica.
De gestión	Comunicación y coordinación.	Define protocolos de comunicación interna y externa durante incidentes.	Crear una cadena de comunicación institucional ante emergencias.

Tipo de criterio	Criterio específico	Descripción	Ejemplo de aplicación
De gestión	Evaluación costo-beneficio.	Analiza la relación entre la inversión en la estrategia y los beneficios esperados en reducción de riesgos.	Invertir en respaldo en la nube que reduce el tiempo de recuperación en un 80 %.
De gestión	Alineación normativa.	Garantiza que las estrategias cumplan con los estándares ISO y la legislación nacional.	Alinear el plan de continuidad con la ISO 22301 y la Ley 1581 de 2012.
De gestión	Mejora continua.	Asegura la revisión y actualización periódica de las estrategias según cambios organizacionales o tecnológicos.	Realizar simulacros anuales y ajustar procedimientos según resultados.

La aplicación práctica de estos criterios debe integrarse dentro de un proceso estructurado que combine la evaluación técnica, el análisis de riesgos, la asignación de recursos y la toma de decisiones basada en evidencia. Por ejemplo, una organización que identifique la vulnerabilidad de su infraestructura tecnológica puede aplicar criterios técnicos para evaluar la capacidad del sistema de respaldo y criterios de gestión para priorizar la inversión más rentable y sostenible.

Asimismo, la participación activa de la alta dirección resulta fundamental, ya que permite garantizar la asignación de recursos, el respaldo institucional y la incorporación de las estrategias en la política global de continuidad del negocio. La gestión debe orientarse no solo a la reacción frente a incidentes, sino también a la prevención, mediante la creación de una cultura organizacional resiliente.

En conclusión, la aplicación equilibrada de criterios técnicos y de gestión en el diseño de estrategias de continuidad del negocio permite crear soluciones realistas, adaptadas a las necesidades y capacidades de la organización. Este enfoque integral asegura que las estrategias sean sostenibles, auditables y efectivas, fortaleciendo la capacidad institucional para enfrentar y superar eventos disruptivos.

3.4. Pruebas, validación y mejora continua de las estrategias

Las pruebas, la validación y la mejora continua son fases fundamentales dentro del ciclo de gestión de la continuidad del negocio, ya que permiten comprobar la eficacia real de las estrategias diseñadas, identificar brechas y fortalecer la capacidad de respuesta de la organización ante situaciones críticas. Sin estos procesos, los planes de continuidad se convierten en documentos teóricos sin garantía de aplicación práctica.

Las pruebas de continuidad del negocio tienen como propósito verificar que las estrategias funcionen adecuadamente en escenarios reales o simulados. Su ejecución debe ser planificada, documentada y evaluada con base en objetivos claros y medibles. De acuerdo con la ISO 22301, estas pruebas deben realizarse de forma periódica y abarcar diferentes niveles de complejidad.

A continuación, se presentan los principales tipos de pruebas utilizadas en la gestión de continuidad:

Tabla 8. Tipos de pruebas de continuidad del negocio

Tipo de prueba	Descripción	Ejemplo de aplicación
Prueba de escritorio o revisión documental.	Consiste en revisar el plan de continuidad en sesiones de trabajo, verificando que la información sea completa y actualizada.	El comité de continuidad revisa los procedimientos de recuperación de sistemas críticos y los contactos de emergencia.
Simulación o ejercicio teórico.	Recrea un escenario hipotético para evaluar la toma de decisiones y la coordinación entre áreas.	Simular una falla en el servidor principal y analizar cómo cada equipo aplica el plan.
Prueba técnica o funcional.	Evalúa el desempeño real de los sistemas, respaldos	Desconectar temporalmente un servidor secundario para

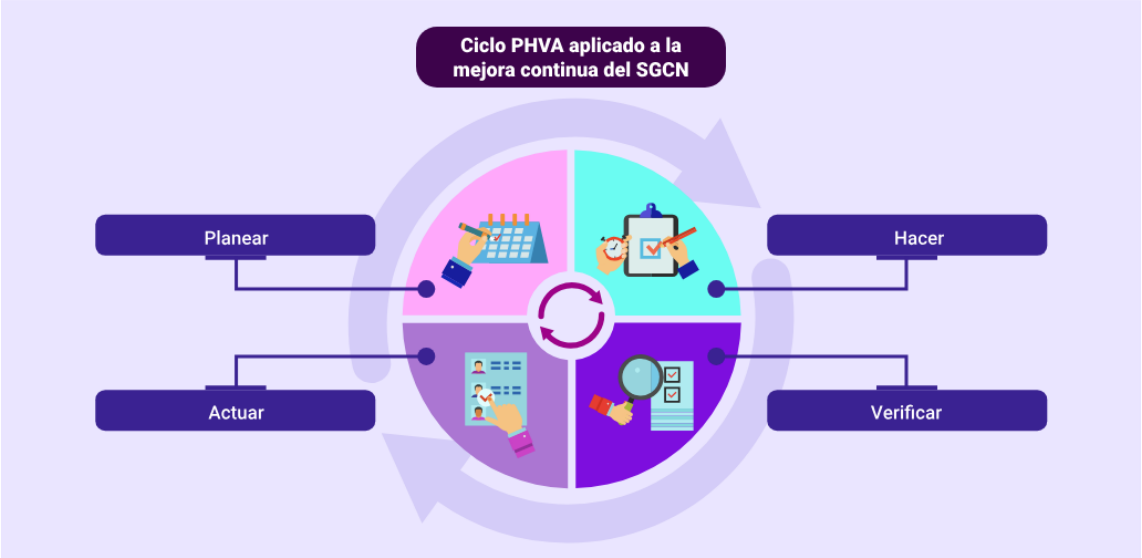
Tipo de prueba	Descripción	Ejemplo de aplicación
	y recursos durante una interrupción controlada.	verificar la activación del servidor espejo.
Prueba integral o de campo.	Involucra a toda la organización en la ejecución práctica del plan, bajo condiciones simuladas.	Realizar un simulacro de evacuación y continuidad operativa por un corte de energía prolongado.
Prueba de recuperación total.	Valida la capacidad de restablecer por completo las operaciones en un entorno alterno.	Trasladar temporalmente los servicios críticos a un centro de datos externo y comprobar la operatividad total.

La validación de las estrategias se realiza mediante la comparación de los resultados obtenidos con los objetivos establecidos en el plan, analizando la efectividad, los tiempos de respuesta, la coordinación y la disponibilidad de los recursos. Este proceso permite confirmar que las estrategias cumplen con los niveles de servicio definidos (RTO y RPO) y con los requisitos normativos aplicables.

En caso de detectarse desviaciones, debe generarse un informe de resultados y acciones correctivas, en el que se especifiquen los hallazgos, las oportunidades de

mejora y las lecciones aprendidas. Estos informes constituyen un insumo esencial para la siguiente etapa de mejora continua.

Figura 1. Ciclo PHVA aplicado a la mejora continua del SGCN



Ciclo PHVA aplicado a la mejora continua del SGCN

- ✓ **Planear**: definir objetivos, políticas, estrategias y recursos necesarios para la continuidad del negocio.
- ✓ **Hacer**: implementar las estrategias, ejecutar las pruebas y poner en marcha los procedimientos definidos.
- ✓ **Actuar**: aplicar acciones correctivas y de mejora basadas en los hallazgos, garantizando la actualización constante del sistema.
- ✓ **Verificar**: evaluar los resultados obtenidos en las pruebas, auditorías o incidentes reales.

La mejora continua implica revisar, actualizar y optimizar las estrategias con base en la información obtenida de las pruebas, auditorías internas, cambios tecnológicos o lecciones aprendidas tras incidentes reales. Este principio asegura

que el Sistema de Gestión de Continuidad del Negocio (SGCN) evolucione junto con la organización y mantenga su vigencia ante nuevos riesgos o contextos.

Por ejemplo, una empresa que detecte durante una prueba técnica que sus respaldos automáticos no se ejecutan correctamente debe ajustar su configuración, documentar el cambio y programar una nueva validación. De igual forma, si una simulación revela fallas en la comunicación interna, se deben actualizar los protocolos y reforzar la capacitación del personal.

Las pruebas, la validación y la mejora continua son pilares esenciales para garantizar la efectividad y sostenibilidad de las estrategias de continuidad del negocio. A través de un proceso cíclico y sistemático, las organizaciones pueden asegurar que sus planes sean dinámicos, confiables y estén preparados para responder de forma eficiente ante cualquier contingencia.

4. Plan de Continuidad del Negocio (PCN)

Es un instrumento estratégico que permite a las organizaciones mantener o restablecer sus operaciones críticas ante incidentes que interrumpan su funcionamiento normal. Su propósito principal es minimizar el impacto de los eventos disruptivos, como fallas tecnológicas, desastres naturales, ataques cibernéticos o crisis operativas, garantizando la sostenibilidad, resiliencia y confianza institucional.

El PCN constituye la materialización práctica del Sistema de Gestión de Continuidad del Negocio (SGCN), ya que traduce las políticas, estrategias y resultados del Análisis de Impacto al Negocio (BIA) y la gestión del riesgo en un

conjunto de procedimientos claros y coordinados para actuar antes, durante y después de una interrupción.

Un PCN bien estructurado no se limita a documentar los pasos de recuperación; debe ser un plan dinámico y actualizado, capaz de adaptarse a los cambios organizacionales, tecnológicos y normativos. Además, debe involucrar a todas las áreas de la entidad, desde la alta dirección hasta el personal operativo, integrando la continuidad dentro de la cultura organizacional.

De acuerdo con la norma ISO 22301, el Plan de Continuidad del Negocio debe contener como mínimo los siguientes elementos esenciales:

- ✓ **Alcance y objetivos**: definen los procesos, recursos y ubicaciones que cubre el plan, junto con los propósitos que se busca alcanzar.
- ✓ **Estrategias y procedimientos**: describen las acciones específicas para mantener la operación o restablecer los servicios en tiempos definidos.
- ✓ **Roles y responsabilidades**: asignan funciones claras a cada actor dentro de la organización, garantizando coordinación y rendición de cuentas.
- ✓ **Protocolos de comunicación**: establecen los mecanismos para informar oportunamente a empleados, proveedores, clientes y autoridades.
- ✓ **Procedimientos de activación y cierre**: definen los criterios para poner en marcha el plan y declarar el retorno a la normalidad.
- ✓ **Mecanismos de evaluación y mejora**: permiten revisar el desempeño del plan mediante pruebas, auditorías y lecciones aprendidas.

En la práctica, el PCN actúa como una guía operativa integral, que orienta la toma de decisiones bajo presión y facilita la recuperación eficiente. Por ejemplo, en

una empresa del sector financiero, el PCN puede detallar los pasos para activar un centro de respaldo, transferir servicios críticos a una sede alterna, recuperar datos desde copias de seguridad y establecer canales de comunicación con los clientes durante la contingencia.

La implementación del PCN aporta beneficios tangibles, entre los que se destacan:

- ✓ Cumplimiento de requisitos regulatorios y estándares internacionales.
- ✓ Reducción del tiempo de inactividad y las pérdidas económicas.
- ✓ Protección de los activos de información y la reputación institucional.
- ✓ Fortalecimiento de la resiliencia organizacional y la confianza de las partes interesadas.

El Plan de Continuidad del Negocio constituye el pilar operativo de la resiliencia institucional. Su correcta formulación y actualización constante garantizan que la organización esté preparada para responder de manera estructurada ante cualquier evento disruptivo, protegiendo tanto sus recursos esenciales como su sostenibilidad a largo plazo.

4.1. Relación entre planes de continuidad, contingencia y recuperación

Dentro de la gestión integral de la continuidad del negocio, los planes de continuidad, contingencia y recuperación cumplen funciones complementarias que, al integrarse, aseguran la resiliencia organizacional ante eventos disruptivos. Aunque estos planes comparten el propósito común de mantener la operación frente a incidentes, difieren en su alcance, enfoque temporal y nivel de intervención.

El Plan de Continuidad del Negocio (PCN) se centra en mantener las operaciones críticas durante y después de una interrupción significativa, garantizando la prestación de servicios esenciales y la protección de los activos. El Plan de Contingencia, por su parte, está orientado a la respuesta inmediata frente a un evento imprevisto, con el fin de controlar la situación y minimizar daños. Finalmente, el Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés) se enfoca en la restauración técnica de sistemas, infraestructura y datos tras un evento que ha comprometido los recursos tecnológicos.

Comprender la relación entre estos tres planes permite establecer una jerarquía lógica de actuación, donde cada uno cumple un papel específico dentro del proceso general de continuidad. Mientras el plan de contingencia aborda la respuesta inicial, el plan de continuidad asegura la operación mínima del negocio, y el plan de recuperación restablece los servicios a su estado normal.

Tabla 9. Relación entre planes de continuidad, contingencia y recuperación

Tipo de plan	Propósito principal	Enfoque temporal	Alcance	Responsables principales	Ejemplo de aplicación
Plan de Contingencia.	Responder de forma inmediata ante un evento inesperado para	Inmediato (durante el incidente).	Personas, instalaciones y entorno.	Equipos de emergencia, líderes operativos.	Activación de protocolos ante incendio o

Tipo de plan	Propósito principal	Enfoque temporal	Alcance	Responsables principales	Ejemplo de aplicación
	controlar daños.				falla eléctrica.
Plan de Continuidad del Negocio (PCN).	Mantener la operación de los procesos críticos y servicios esenciales.	Corto y mediano plazo (durante y después del evento).	Procesos críticos, personal clave, comunicación y operaciones.	Comité de continuidad, alta dirección.	Ejecución de operaciones desde un sitio alterno tras un ciberataque.
Plan de Recuperación ante Desastres (DRP).	Restablecer infraestructura tecnológica y sistemas afectados.	Posterior al evento (fase de restauración).	Recursos tecnológicos, datos, redes, aplicaciones.	Personal de TI y administradores de sistemas.	Restauración de bases de datos y servidores en un centro alterno.

Además de estas características, una estrategia efectiva debe contar con respaldo de la alta dirección, garantizar la comunicación oportuna entre las áreas involucradas y fomentar una cultura de compromiso entre el personal. La efectividad no solo depende de los recursos tecnológicos, sino también del nivel de preparación humana para responder ante emergencias.

Por ejemplo, una organización que dispone de sistemas de respaldo automáticos, pero no capacita a su personal para activarlos correctamente, podría fallar en su respuesta ante una contingencia. Por ello, las estrategias deben contemplar tanto los aspectos técnicos como los procedimentales y humanos.

En conclusión, las estrategias efectivas son aquellas que logran equilibrio entre viabilidad, eficiencia y adaptabilidad, permitiendo a la organización responder de manera ordenada, minimizar pérdidas y mantener la confianza de sus partes interesadas ante cualquier interrupción significativa.

4.2. Elementos esenciales para su implementación

La implementación efectiva de un Plan de Continuidad del Negocio (PCN) requiere la integración de una serie de elementos estructurales y operativos que garanticen su funcionalidad y sostenibilidad a lo largo del tiempo. Estos elementos conforman el marco metodológico y organizacional necesario para preparar, responder y recuperarse de cualquier evento que interrumpa la operación normal de la entidad.

Cada elemento cumple un papel específico dentro del sistema, desde la definición de políticas y responsabilidades hasta la ejecución de pruebas y la mejora continua. Su correcta aplicación asegura que el PCN no sea solo un documento

formal, sino una herramienta viva y dinámica que fortalece la resiliencia institucional.

A continuación, se presentan los principales elementos esenciales que deben considerarse en la implementación de un plan de continuidad del negocio:

Tabla 10. Elementos esenciales del Plan de Continuidad del Negocio (PCN)

Elemento	Descripción	Ejemplo de aplicación
Política de continuidad del negocio.	Define los principios, objetivos y alcance del sistema, aprobados por la alta dirección.	Documento oficial que establece el compromiso institucional con la continuidad y la resiliencia.
Gobernanza y roles definidos.	Determina la estructura organizativa, los responsables del plan y las líneas de autoridad.	Conformar un Comité de Continuidad del Negocio liderado por la alta dirección.
Análisis de impacto al negocio (BIA).	Identifica los procesos críticos, tiempos máximos de recuperación y dependencias operativas.	Determinar que la plataforma de pagos debe recuperarse en máximo 1 hora.

Elemento	Descripción	Ejemplo de aplicación
Gestión de riesgos.	Evalúa amenazas, vulnerabilidades y escenarios que puedan afectar la continuidad operativa.	Analizar el impacto de una falla eléctrica o un ataque cibernético.
Estrategias y procedimientos de continuidad.	Establecen las acciones específicas para mantener o restablecer los procesos críticos.	Definir alternativas de operación desde un sitio remoto o el uso de servidores redundantes.
Recursos y capacidades.	Incluyen los medios tecnológicos, humanos, financieros y logísticos necesarios para ejecutar el plan.	Contratar servicios de respaldo en la nube o capacitar personal clave.
Protocolos de comunicación.	Definen cómo y a quién se informan los incidentes y las decisiones durante una crisis.	Establecer canales de contacto entre líderes de área y voceros institucionales.
Procedimientos de activación y respuesta.	Especifican los criterios, pasos y responsables para	Iniciar el PCN al detectar una interrupción mayor

Elemento	Descripción	Ejemplo de aplicación
	activar el plan en caso de incidente.	en los sistemas de información.
Mecanismos de validación y pruebas.	Permiten verificar la efectividad del plan mediante ejercicios y simulacros.	Realizar pruebas anuales de recuperación de datos.
Revisión y mejora continua.	Aseguran la actualización permanente del plan ante cambios internos o del entorno.	Revisar el PCN tras un cambio tecnológico o una auditoría interna.

La implementación de estos elementos debe realizarse de forma gradual y coordinada, garantizando la participación activa de todas las áreas involucradas. Es fundamental que cada procedimiento esté documentado, probado y revisado periódicamente, de modo que el plan evolucione con las necesidades del negocio y los cambios del entorno.

Por ejemplo, en una institución educativa, la implementación del PCN podría incluir la creación de un comité responsable, la definición de estrategias para respaldar los sistemas académicos, la elaboración de un directorio de contactos de emergencia y la realización de simulacros semestrales para validar la capacidad de respuesta.

Los elementos esenciales del PCN constituyen la base operativa de la continuidad del negocio. Su correcta integración garantiza que la organización cuente con los mecanismos necesarios para anticiparse a las crisis, responder eficazmente y mantener la confianza de sus partes interesadas, fortaleciendo así su sostenibilidad a largo plazo.

5. Aplicación práctica

La aplicación práctica de los conocimientos sobre continuidad del negocio, permite consolidar las competencias desarrolladas en las etapas anteriores, trasladando la teoría a contextos reales o simulados. En esta fase, los aprendices ponen en práctica los principios de resiliencia organizacional, la gestión del riesgo y la planificación estratégica mediante el diseño y validación de estrategias adaptadas a las necesidades específicas de una organización.

La práctica incluye tres actividades clave: el desarrollo de estrategias, la formulación de un plan básico de continuidad y la simulación de escenarios de interrupción.

5.1. Desarrollo de estrategias de continuidad según requerimientos organizacionales

El desarrollo de estrategias de continuidad del negocio implica adaptar las acciones preventivas, de mitigación y recuperación a las condiciones particulares de cada organización. Este proceso debe basarse en los resultados del Análisis de Impacto al Negocio (BIA) y en la evaluación de riesgos, garantizando que las medidas propuestas sean viables, sostenibles y efectivas ante los escenarios identificados.

Para lograrlo, la organización debe analizar sus procesos críticos, los recursos que los soportan y las vulnerabilidades que pueden afectar su funcionamiento. A partir de esta información, se establecen estrategias diferenciales que respondan a los requerimientos institucionales, considerando aspectos como la naturaleza del negocio, el tamaño de la empresa, la infraestructura tecnológica, la disponibilidad presupuestal y la madurez organizacional en gestión de continuidad.

El proceso de desarrollo de estrategias suele incluir las siguientes fases:

- ✓ **Definición de objetivos de continuidad**: determinar qué servicios o procesos deben mantenerse operativos y en qué condiciones.
- ✓ **Selección de estrategias adecuadas**: identificar y combinar medidas preventivas, de mitigación, recuperación y transferencia de riesgos, según el nivel de criticidad.
- ✓ **Asignación de responsables y recursos**: designar equipos de trabajo, definir presupuestos y establecer mecanismos de seguimiento y control.
- ✓ **Validación y pruebas piloto**: verificar la eficacia de las estrategias mediante simulaciones o ejercicios prácticos que permitan ajustar procedimientos.

Con el fin de aclarar la aplicación de este proceso, se presenta a continuación un ejemplo práctico contextualizado:

Caso práctico sobre una empresa de servicios tecnológicos:

Una empresa del sector tecnológico que provee soluciones en la nube a instituciones educativas identifica, a través de su BIA, que sus procesos más críticos

son el soporte técnico, la gestión de datos de clientes y la operación de servidores. A partir de este diagnóstico, desarrolla las siguientes estrategias de continuidad:

- ✓ **Estrategias preventivas**: implementación de mantenimientos programados, actualizaciones automáticas de software y monitoreo de servidores las 24 horas, con el fin de anticipar posibles fallos.
- ✓ **Estrategias de mitigación**: establecimiento de copias de respaldo en tres ubicaciones geográficas distintas y configuración de un sistema de redundancia en la nube para garantizar la disponibilidad de los datos.
- ✓ **Estrategias de recuperación**: creación de un protocolo de restauración de servicios en menos de dos horas (RTO = 2 h) y establecimiento de un RPO de 30 minutos para evitar pérdida significativa de información.
- ✓ **Estrategias de comunicación**: diseño de un plan de comunicación interna y externa que defina los canales, responsables y mensajes a emitir durante un incidente, garantizando la transparencia y confianza con los clientes.

Como resultado, la empresa logra mantener la continuidad de sus servicios esenciales incluso ante cortes eléctricos o fallas de red, asegurando la satisfacción del cliente y el cumplimiento de los acuerdos de nivel de servicio (SLA). Además, la organización fortalece su cultura de resiliencia, al integrar la gestión de continuidad como parte de la planeación estratégica y del ciclo de mejora continua de su Sistema de Gestión.

El desarrollo de estrategias de continuidad según los requerimientos organizacionales permite transformar los resultados del análisis de riesgos y del BIA en acciones concretas, priorizadas y adaptadas al contexto de la empresa. De esta

manera, se garantiza la sostenibilidad operativa y la capacidad de respuesta ante cualquier eventualidad que pueda comprometer la estabilidad del negocio.

5.2. Formulación de un plan básico de continuidad del negocio

La formulación de un Plan de Continuidad del Negocio (PCN) consiste en estructurar un conjunto de procedimientos, recursos y responsabilidades que permitan mantener o restablecer las operaciones críticas ante la ocurrencia de incidentes disruptivos. Su propósito es minimizar los efectos negativos sobre la organización, garantizar la protección de los activos esenciales y preservar la confianza de los clientes y partes interesadas.

Un PCN básico debe incluir elementos esenciales como:

- ✓ La identificación de procesos críticos y sus dependencias.
- ✓ Los escenarios de riesgo que podrían afectarlos.
- ✓ Las estrategias de continuidad seleccionadas.
- ✓ La asignación de responsabilidades y equipos de respuesta.
- ✓ Los procedimientos de recuperación con sus tiempos de ejecución (RTO y RPO).
- ✓ Los canales de comunicación interna y externa.
- ✓ El plan de pruebas, mantenimiento y mejora continua.

A continuación, se presenta un caso práctico que describe la formulación de un PCN en una empresa del sector financiero:

Caso práctico sobre la formulación del PCN en una entidad financiera:

Una entidad financiera regional identifica, a través del Análisis de Impacto al Negocio (BIA), que sus procesos más críticos son la atención al cliente, la operación

de la plataforma de pagos electrónicos y la gestión contable. Con base en este diagnóstico, formula su Plan de Continuidad del Negocio bajo las siguientes fases:

a) **Definición del alcance del plan**: el PCN cubrirá las operaciones centrales de la entidad, incluyendo servicios en línea, atención presencial y procesamiento de pagos.
b) **Establecimiento del comité de continuidad**: conformado por representantes de tecnología, operaciones, finanzas, comunicaciones y recursos humanos, responsables de activar y coordinar las acciones del plan.
c) **Identificación de escenarios de interrupción**: entre ellos, ciberataques, fallas eléctricas, daños en servidores y emergencias naturales que afecten las sucursales.
d) **Diseño de estrategias y procedimientos**:
   - ✓ **Prevención**: fortalecimiento del sistema de seguridad perimetral y respaldo diario de bases de datos.
   - ✓ **Mitigación**: contratación de un centro de datos alterno con replicación en tiempo real.
   - ✓ **Recuperación**: protocolo de restauración de servicios priorizados con un RTO de 1 hora y RPO de 15 minutos.
   - ✓ **Comunicación**: difusión de mensajes automáticos a los clientes a través de la aplicación móvil y página web.
e) **Asignación de recursos y responsables**: cada área dispone de un plan operativo que detalla las funciones del personal durante la emergencia, los recursos necesarios y los tiempos de respuesta.

f) **Pruebas y validación**: se realizan simulacros semestrales de interrupción tecnológica, evaluando la eficiencia de las estrategias y ajustando los procedimientos de acuerdo con los resultados obtenidos.

Gracias a la implementación del PCN, la entidad logra reducir significativamente el tiempo de respuesta ante fallos, mantener la confianza del cliente y asegurar la estabilidad operativa de los servicios financieros, incluso en situaciones de alta presión o crisis.

En conclusión, la formulación de un plan básico de continuidad del negocio permite estructurar una respuesta organizada, práctica y alineada con los objetivos estratégicos de la organización. Este documento se convierte en una herramienta clave para garantizar la resiliencia institucional, la protección de los activos críticos y la sostenibilidad del negocio ante cualquier eventualidad.

5.3. Simulación de escenarios de interrupción y respuesta organizacional

La simulación de escenarios de interrupción constituye una herramienta fundamental para evaluar la eficacia del Plan de Continuidad del Negocio (PCN) y medir la capacidad real de respuesta de la organización ante situaciones críticas. Su propósito es verificar si los procedimientos establecidos son funcionales, si los responsables conocen sus roles y si los recursos disponibles permiten cumplir con los tiempos de recuperación definidos.

Estos ejercicios permiten fortalecer la cultura de resiliencia organizacional, identificar debilidades en los procesos de comunicación, detectar fallas en los sistemas de respaldo y generar oportunidades de mejora continua. Además,

promueven la coordinación interdepartamental y la toma de decisiones basada en la experiencia práctica.

Las simulaciones pueden clasificarse en tres tipos principales:

1) **Pruebas de escritorio o teóricas**: se realizan mediante sesiones de análisis en las que los líderes revisan los pasos del plan y evalúan la pertinencia de las acciones ante escenarios hipotéticos.
2) **Simulacros parciales**: implican la ejecución de algunas actividades del plan, como el restablecimiento de un servidor o la reubicación temporal de personal.
3) **Simulacros integrales**: reproducen un evento disruptivo de forma completa, involucrando a todas las áreas, con el fin de medir tiempos reales de reacción, comunicación y recuperación.

A continuación, se presenta un caso práctico que ejemplifica la aplicación de un ejercicio de simulación:

Caso práctico sobre simulación de interrupción tecnológica en una empresa de servicios públicos:

Una empresa de servicios públicos decide evaluar la efectividad de su Plan de Continuidad del Negocio mediante la simulación de una falla crítica en su sistema central de facturación y atención al usuario. El escenario simulado consiste en una caída total del servidor principal durante la jornada de mayor demanda.

Etapas de la simulación:

a) **Activación del escenario**: el equipo de continuidad notifica la falla y activa los protocolos definidos.
b) **Ejecución de estrategias de respaldo**: se habilita el servidor alterno y se redirige el tráfico de solicitudes al centro de datos secundario.
c) **Comunicación interna y externa**: se informa a los empleados sobre el procedimiento de contingencia y se emite un comunicado preventivo a los usuarios por canales oficiales.
d) **Seguimiento y evaluación**: se registran los tiempos de respuesta, las dificultades técnicas y el cumplimiento de los RTO y RPO definidos en el PCN.
e) **Retroalimentación y mejora**: finalizado el ejercicio, se elabora un informe con las lecciones aprendidas, ajustes requeridos en la infraestructura y nuevas medidas preventivas.

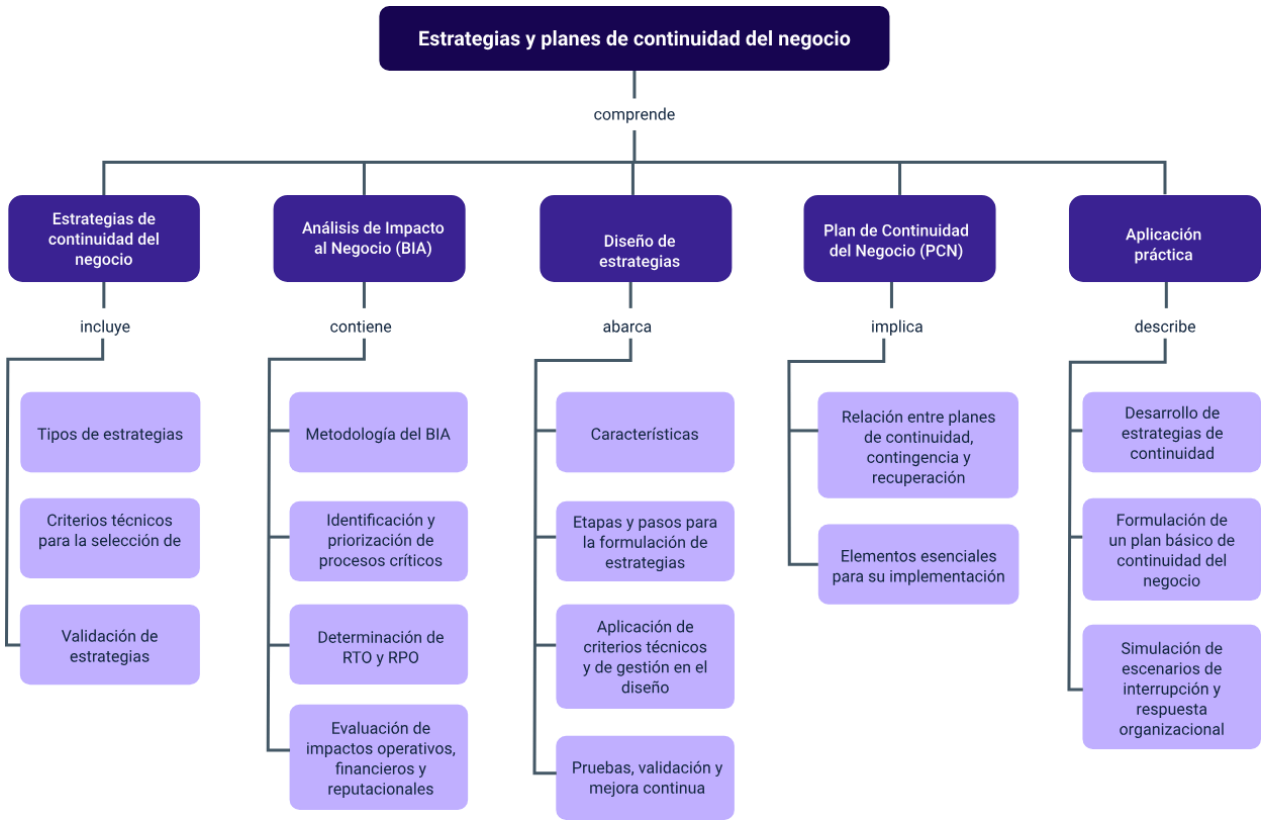
El resultado del ejercicio demuestra que la empresa logró restablecer el servicio en menos de 45 minutos, manteniendo la atención al usuario y evitando pérdidas significativas. Sin embargo, se detectaron deficiencias en la comunicación entre áreas técnicas y administrativas, lo que llevó a incorporar nuevos protocolos de coordinación y capacitación.

La simulación de escenarios de interrupción y respuesta organizacional permite a las entidades pasar de la teoría a la práctica, comprobando la efectividad de sus estrategias de continuidad. Este tipo de ejercicios fortalecen la confianza institucional, optimizan la preparación del personal y aseguran que la organización

esté realmente lista para enfrentar cualquier eventualidad con eficiencia y resiliencia.

Síntesis

El componente formativo aborda el diseño e implementación de estrategias orientadas a garantizar la continuidad del negocio ante incidentes o interrupciones. Se analizan los tipos de estrategias, los criterios técnicos para su selección y las metodologías del Análisis de Impacto al Negocio (BIA) para identificar procesos críticos y definir los tiempos de recuperación (RTO y RPO). Asimismo, se estudian las etapas para la formulación y validación de estrategias efectivas, junto con los elementos esenciales del Plan de Continuidad del Negocio (PCN) y su relación con los planes de contingencia y recuperación. Finalmente, se promueve la aplicación práctica mediante la elaboración de planes y simulaciones, fortaleciendo la resiliencia organizacional y la capacidad de respuesta ante eventos adversos.



Material Complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Estrategias de continuidad del negocio	Ecosistema de Recursos Educativos Digitales SENA. (2022). Elementos de una estrategia SGCN [Video]. YouTube.	Video	https://www.youtube.com/watch?v=f4gr8Z15bKQ
Análisis de Impacto al Negocio	Ecosistema de Recursos Educativos Digitales SENA. (2022). Medición de impacto [Video]. YouTube.	Video	https://www.youtube.com/watch?v=EeSChaxCbkY
Elementos esenciales para su implementación	Ecosistema de Recursos Educativos Digitales SENA. (2022). La mejora continua en las organizaciones; generalidades [Video]. YouTube.	Video	https://www.youtube.com/watch?v=Xv6z-0kyTtY

Glosario

Estrategias de continuidad: acciones planificadas que buscan prevenir, mitigar o recuperar la operación de los procesos esenciales frente a interrupciones, fortaleciendo la resiliencia organizacional.

Gestión del riesgo: proceso sistemático para identificar, analizar, evaluar y controlar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales o la continuidad operativa.

Impactos financieros: consecuencias económicas derivadas de una interrupción operativa, como pérdida de ingresos, costos adicionales de recuperación, sanciones contractuales o disminución del valor de los activos.

Impactos operativos: efectos que una interrupción puede generar sobre la capacidad de una organización para ejecutar sus procesos, cumplir con sus objetivos o mantener la prestación de servicios esenciales.

Impactos reputacionales: daños en la imagen, confianza o credibilidad de una organización ante clientes, aliados y la opinión pública como resultado de incidentes, fallas o mala gestión de crisis.

Mejora continua: proceso permanente de revisión, evaluación y optimización de los sistemas, procedimientos y estrategias, orientado a incrementar la eficacia, la eficiencia y la capacidad de respuesta de la organización ante cambios o incidentes.

Plan de Continuidad del Negocio (PCN): documento que define los procedimientos, recursos y responsables necesarios para mantener o restablecer los procesos críticos de una organización ante una contingencia.

Proceso crítico: actividad o función esencial cuyo fallo o interrupción puede generar un impacto significativo en la operación, la reputación o las finanzas de la organización.

Resiliencia organizacional: capacidad de una organización para anticiparse, resistir, adaptarse y recuperarse eficazmente frente a eventos disruptivos, manteniendo la continuidad de sus operaciones.

Referencias bibliográficas

ISO. (2015). ISO 9001:2015 - Quality management systems - Requirements. International Organization for Standardization.

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

ISO. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization.

República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentario del Sector de Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ruiz, A., & Rodríguez, M. (2019). El ciclo PHVA como herramienta para la mejora continua en los sistemas de gestión. Revista de Administración y Calidad, 27(3), 45–58.

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocío Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Armando Javier López Sierra	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Viviana Esperanza Herrera Quiñonez	Evaluadora instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Ivan Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Jose Yobani Penagos Mora	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Sebastian Trujillo Afanador	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Gilberto Junior Rodríguez Rodríguez	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Jorge Eduardo Rueda Peña	Evaluador de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima
Jorge Bustos Gómez	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima