Fundamentos y factores de continuidad del negocio

Breve descripción:

Este componente formativo aborda los fundamentos de la seguridad de la información y la continuidad del negocio, pilares para garantizar la sostenibilidad operativa. Incluye el estudio de activos, riesgos, procesos críticos, resiliencia organizacional y sistemas de gestión de continuidad, junto con la normativa aplicable, para establecer factores que aseguren la estabilidad empresarial ante incidentes o interrupciones.

Octubre 2025

Tabla de contenido

Introducción

Este componente presenta los aspectos esenciales de la continuidad del negocio y la seguridad de la información, abordando los principios, procesos y estrategias que permiten a las organizaciones mantener su operación ante incidentes, interrupciones o crisis. Se orienta al reconocimiento de los activos de información, la identificación de riesgos y la aplicación de mecanismos que garanticen la resiliencia organizacional.

El propósito de este componente es fortalecer las competencias para gestionar la continuidad operativa y la protección de los recursos críticos, comprendiendo su importancia en la sostenibilidad empresarial, la toma de decisiones y el cumplimiento de los estándares nacionales e internacionales, como las normas ISO 22301 e ISO 27001. A través del análisis de casos, herramientas de evaluación y ejercicios prácticos, se promueve una visión integral de cómo la gestión del riesgo y la seguridad de la información contribuyen a la estabilidad institucional.

El desarrollo de los temas se realiza mediante un enfoque teórico-práctico que permite al aprendiz comprender los fundamentos, aplicar metodologías de análisis y proponer estrategias de mejora continua. De esta manera, se busca que el participante adquiera las capacidades necesarias para identificar activos y procesos críticos, analizar amenazas y establecer planes de continuidad acordes con las necesidades de la organización.

Para comprender la importancia del contenido y los temas abordados, se recomienda acceder al siguiente video:

Video 1. Fundamentos y factores de continuidad del negocio

Enlace de reproducción del video

Síntesis del video: Fundamentos y factores de continuidad del negocio
Las organizaciones enfrentan cada día nuevos desafíos: fallos tecnológicos, desastres naturales, ciberataques o crisis inesperadas. En ese contexto, garantizar la continuidad del negocio no es solo una opción, sino una necesidad estratégica. La continuidad del negocio se basa en un principio simple, pero poderoso: prepararse para lo imprevisto. Implica identificar los procesos y activos más críticos, analizar los riesgos que podrían afectarlos y establecer planes que aseguren la operación, incluso en las circunstancias más adversas. Un paso clave es reconocer los activos de información: datos, sistemas, infraestructura y, sobre todo, el conocimiento de las personas. Protegerlos requiere

aplicar los principios de seguridad de la información: confidencialidad, integridad y disponibilidad.

El análisis de riesgos permite anticipar amenazas, evaluar su impacto y definir estrategias de mitigación. De este modo, las organizaciones fortalecen su resiliencia, es decir, su capacidad para resistir, adaptarse y recuperarse rápidamente.

A través de un Sistema de Gestión de Continuidad del Negocio (SGCN), basado en estándares internacionales como la ISO 22301, las empresas pueden planificar, ejecutar y mejorar de forma continua sus respuestas ante emergencias.

La continuidad del negocio no solo protege los recursos, también preserva la confianza, la reputación y la estabilidad de las organizaciones. En un mundo incierto, la preparación se convierte en la mejor estrategia para avanzar con seguridad hacia el futuro.

1. Seguridad de la información y activos organizacionales

La seguridad de la información constituye un pilar fundamental para el funcionamiento y la sostenibilidad de las organizaciones, ya que garantiza la protección de los datos, los sistemas y los recursos tecnológicos que soportan los procesos operativos y estratégicos. Su propósito principal es preservar la confidencialidad, integridad y disponibilidad de la información, evitando accesos no autorizados, modificaciones indebidas o pérdidas que puedan comprometer la continuidad del negocio.

En un entorno empresarial cada vez más digitalizado, la información se ha convertido en un activo estratégico que representa un valor tangible e intangible para las organizaciones. Los activos de información comprenden todos los elementos que intervienen en la creación, almacenamiento, procesamiento y transmisión de datos, incluyendo documentos físicos y digitales, software, hardware, redes, sistemas y, especialmente, el conocimiento del personal. Identificar y clasificar adecuadamente estos activos permite establecer medidas de protección acordes con su nivel de criticidad e impacto potencial ante un incidente.

La gestión de la seguridad de la información implica la aplicación de políticas, procedimientos y controles diseñados para mitigar riesgos. Estas acciones se enmarcan en normas internacionales como la ISO/IEC 27001, que establece requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo la mejora continua y el cumplimiento normativo.

Asimismo, la seguridad de la información debe integrarse con la cultura organizacional, de modo que todos los colaboradores comprendan su rol en la protección de los datos y en la prevención de incidentes. Una organización que gestiona

de forma adecuada sus activos de información fortalece su resiliencia frente a amenazas internas y externas, garantizando la confianza de clientes, proveedores y aliados estratégicos.

1.1. Activos de información y sus características

Los activos de información representan todos los elementos que poseen valor para una organización y que son esenciales para el cumplimiento de sus objetivos estratégicos, operativos y administrativos. Estos activos no se limitan únicamente a los datos digitales o documentos físicos, sino que también abarcan sistemas informáticos, aplicaciones, redes, infraestructura tecnológica, bases de datos, procesos, conocimientos del personal y la reputación institucional. Cada uno de estos componentes contribuye de manera directa o indirecta a la generación de valor y a la continuidad de las operaciones.

La gestión de los activos de información inicia con su identificación, seguida de la clasificación según su nivel de importancia, sensibilidad y criticidad para el negocio. Este proceso permite determinar cuáles son los recursos más vulnerables y establecer medidas de control proporcionales a su relevancia. Un activo puede clasificarse como crítico cuando su pérdida, alteración o divulgación compromete la operatividad, la confianza o la imagen de la organización.

Entre las principales características de los activos de información se destacan:

- ✓ **Valor**: representa el beneficio o utilidad que el activo aporta al cumplimiento de los objetivos del negocio.
- ✓ **Confidencialidad**: garantiza que la información esté protegida frente al acceso, uso o divulgación no autorizada.

- ✓ **Integridad**: asegura la exactitud, coherencia y veracidad de los datos, evitando modificaciones no autorizadas.
- ✓ **Disponibilidad**: permite que la información esté accesible y utilizable por los usuarios autorizados en el momento que se requiera.
- ✓ **Vulnerabilidad**: refleja el grado de exposición del activo frente a amenazas o incidentes que puedan comprometer su seguridad.

Una gestión eficaz de los activos de información permite priorizar los recursos críticos, orientar las estrategias de seguridad de la información y fortalecer la capacidad de respuesta ante posibles interrupciones o incidentes. En este sentido, la identificación y valoración de los activos constituye el primer paso dentro de un sistema integral de seguridad y continuidad del negocio, alineado con las buenas prácticas establecidas en estándares internacionales como la ISO/IEC 27001 y la ISO 22301.

1.2. Principios de seguridad de la información

La seguridad de la información constituye un pilar esencial para la protección de los activos organizacionales, al garantizar que los datos sean tratados, almacenados y transmitidos de forma segura dentro de un marco normativo y técnico. Su propósito es preservar la integridad de los recursos informativos, minimizar los riesgos y asegurar la continuidad de las operaciones frente a amenazas internas o externas.

Los principios de seguridad de la información, establecidos principalmente por la norma ISO/IEC 27001, orientan la gestión y el diseño de controles que protegen los sistemas y la información. Estos principios son los siguientes:

- ✓ **Confidencialidad**: implica que la información solo sea accesible a personas, sistemas o procesos debidamente autorizados. Este principio previene el

acceso, divulgación o uso no autorizado de los datos y se logra mediante mecanismos de autenticación, cifrado, control de accesos y políticas de clasificación de la información.

- ✓ **Integridad**: garantiza que los datos se mantengan completos, coherentes y no sean modificados sin autorización. Este principio protege la exactitud y fiabilidad de la información mediante controles como firmas digitales, auditorías de cambios y verificaciones de consistencia.
- ✓ **Disponibilidad**: asegura que la información, los sistemas y los servicios estén accesibles cuando se requieran para la operación del negocio. Para mantener este principio, se implementan estrategias de respaldo, redundancia, planes de recuperación ante desastres y monitoreo continuo de los sistemas.
- ✓ **Autenticidad**: establece la verificación de la identidad de los usuarios, dispositivos o sistemas que acceden a los recursos de información, garantizando que las comunicaciones y transacciones sean legítimas.
- ✓ **Trazabilidad o responsabilidad (accountability)**: permite registrar y rastrear las acciones realizadas sobre los activos de información, identificando responsables y facilitando la detección de incidentes de seguridad.

Estos principios constituyen la base para el desarrollo de políticas, procedimientos y controles que conforman el Sistema de Gestión de Seguridad de la Información (SGSI). Su aplicación efectiva promueve una cultura organizacional orientada a la protección de los datos y a la resiliencia tecnológica, factores determinantes para la continuidad del negocio y la confianza institucional.

1.3. Identificación de riesgos asociados a los activos de información

La identificación de riesgos asociados a los activos de información constituye un proceso fundamental dentro de la gestión de la seguridad organizacional, ya que permite reconocer las amenazas que pueden afectar la confidencialidad, integridad o disponibilidad de los datos. Comprender los riesgos facilita la implementación de controles preventivos y correctivos que minimicen el impacto de incidentes y aseguren la continuidad de las operaciones.

El riesgo se define como la probabilidad de que una amenaza explote una vulnerabilidad, generando un impacto negativo en los activos de información o en los procesos que dependen de ellos. Por ello, su gestión debe iniciar con una evaluación sistemática que considere los diferentes tipos de amenazas, tanto internas como externas, incluyendo fallas humanas, errores de configuración, accesos no autorizados, pérdida de equipos, ataques cibernéticos, desastres naturales o interrupciones tecnológicas.

El proceso de identificación de riesgos generalmente incluye los siguientes pasos:

1) **Inventario de activos de información**: registrar y clasificar los activos según su criticidad y valor para la organización.
2) **Identificación de amenazas**: determinar los eventos o agentes que pueden afectar los activos, como malware, accesos indebidos o fallas eléctricas.
3) **Detección de vulnerabilidades**: reconocer debilidades técnicas, organizacionales o procedimentales que puedan ser aprovechadas por una amenaza.
4) **Análisis del impacto potencial**: estimar las consecuencias operativas, financieras, legales o reputacionales que podría generar un incidente.

5) **Determinación del nivel de riesgo**: combinar la probabilidad de ocurrencia con el nivel de impacto para priorizar la atención y definir controles de mitigación.

Una adecuada identificación de riesgos permite establecer una base sólida para la gestión de la seguridad de la información, facilitando la toma de decisiones y el diseño de estrategias de continuidad del negocio. Este proceso debe ser dinámico y revisado periódicamente, considerando los cambios tecnológicos, normativos y organizacionales que puedan modificar el nivel de exposición al riesgo.

Asimismo, los lineamientos de normas internacionales como la ISO/IEC 27005 y la ISO 31000 orientan la aplicación de metodologías estructuradas para la gestión del riesgo, promoviendo una cultura de prevención y resiliencia frente a posibles incidentes de seguridad de la información.

2. Continuidad del negocio y resiliencia organizacional

La **continuidad del negocio** y la resiliencia organizacional son pilares fundamentales para garantizar la sostenibilidad de las operaciones ante eventos que puedan interrumpir la actividad normal de una organización. Estos conceptos se complementan, ya que la continuidad del negocio se orienta a la planificación y ejecución de estrategias que aseguren la operación de los procesos críticos, mientras que la resiliencia organizacional se refiere a la capacidad de adaptarse, resistir y recuperarse eficazmente frente a incidentes o cambios adversos.

La continuidad del negocio comprende un conjunto de políticas, procedimientos y acciones diseñadas para prevenir, mitigar y responder ante eventos disruptivos, como fallas tecnológicas, ciberataques, desastres naturales o errores humanos. Su objetivo principal es garantizar que los servicios esenciales continúen o se restablezcan en el menor tiempo posible, evitando pérdidas significativas para la organización y sus partes interesadas.

Por su parte, la **resiliencia organizacional** implica una visión integral de la gestión del riesgo, donde la empresa desarrolla capacidades internas para anticipar amenazas, mantener el control en situaciones críticas y aprender de la experiencia. No se limita a la recuperación posterior a una crisis, sino que fomenta la mejora continua, la innovación y la adaptabilidad ante escenarios inciertos.

La relación entre continuidad y resiliencia radica en que ambas buscan mantener la estabilidad operativa y la confianza de clientes, aliados y usuarios, incluso bajo condiciones adversas. Mientras la continuidad proporciona los planes y recursos necesarios para actuar, la resiliencia se enfoca en la cultura, el liderazgo y la preparación organizacional para enfrentar los desafíos.

Implementar estrategias de continuidad y fortalecer la resiliencia permite reducir vulnerabilidades, proteger los activos de información y asegurar la disponibilidad de los servicios esenciales. Estos esfuerzos deben estar alineados con marcos de referencia internacionales, como la ISO 22301, que establece los requisitos para un Sistema de Gestión de Continuidad del Negocio (SGCN), y la ISO 27001, que integra la seguridad de la información como un componente esencial de la estabilidad organizacional.

En conjunto, la continuidad del negocio y la resiliencia organizacional promueven una cultura preventiva que favorece la sostenibilidad, la competitividad y la confianza en los entornos digitales y corporativos actuales.

2.1. Relación entre continuidad y resiliencia organizacional

La continuidad del negocio y la resiliencia organizacional se complementan al garantizar que las operaciones se mantengan o se recuperen ante incidentes o interrupciones. La siguiente tabla presenta sus principales diferencias y puntos de conexión:

Tabla 1. Relación entre continuidad del negocio y resiliencia organizacional

Aspecto	Continuidad del negocio	Resiliencia organizacional
Enfoque principal.	Planificación y ejecución de acciones para mantener o restablecer los procesos críticos.	Capacidad de adaptarse, resistir y recuperarse ante eventos adversos.

Aspecto	Continuidad del negocio	Resiliencia organizacional
Objetivo.	Asegurar la operación y minimizar el impacto de las interrupciones.	Fortalecer la organización para afrontar crisis y aprender de ellas.
Perspectiva de tiempo.	Actuación durante y después del evento disruptivo.	Preparación antes, durante y después del evento.
Componente clave.	Procedimientos, planes y recursos técnicos.	Cultura organizacional, liderazgo y adaptabilidad.
Resultado esperado.	Restablecimiento de las operaciones en el menor tiempo posible.	Mejora continua y fortalecimiento institucional a largo plazo.
Normas de referencia.	ISO 22301: Sistema de Gestión de Continuidad del Negocio.	ISO 22316: Gestión de la Resiliencia Organizacional.

En conjunto, la continuidad del negocio proporciona los planes y recursos necesarios para actuar ante una crisis, mientras que la resiliencia organizacional garantiza la capacidad de respuesta, aprendizaje y evolución después de enfrentarla.

2.2. Procesos críticos y su impacto en la sostenibilidad del negocio

Los procesos críticos representan aquellas actividades o funciones esenciales para el cumplimiento de los objetivos estratégicos, operativos y financieros de una organización. Su interrupción puede generar pérdidas económicas, deterioro de la reputación, incumplimiento de obligaciones legales o contractuales, y afectaciones en la confianza de clientes y partes interesadas. Por esta razón, la identificación y gestión de los procesos críticos constituyen un componente central dentro de la planificación de la continuidad del negocio y la resiliencia organizacional. Algunos ejemplos comunes incluyen:

- ✓ Producción
- ✓ Gestión de nómina
- ✓ Ventas
- ✓ Atención al cliente
- ✓ Gestión de inventarios
- ✓ Seguridad informática
- ✓ Comunicaciones
- ✓ Gestión financiera

Cada organización debe analizarlos de acuerdo con su estructura, objetivos estratégicos y nivel de dependencia tecnológica.

El análisis de los procesos críticos inicia con la evaluación de la cadena de valor de la organización, con el fin de determinar cuáles actividades son indispensables para mantener la operatividad y los niveles mínimos aceptables de servicio. Este proceso implica identificar los recursos, activos de información, infraestructuras, personal y

proveedores que sustentan cada función esencial, así como los posibles puntos de falla que podrían afectar su desempeño.

Entre los principales criterios para determinar la criticidad de un proceso se encuentran:

- ✓ **Dependencia operativa**: grado en que otras áreas o procesos requieren su correcto funcionamiento.
- ✓ **Impacto financiero**: nivel de pérdida económica o de ingresos ante su interrupción.
- ✓ **Cumplimiento normativo**: obligaciones legales o contractuales que pueden verse comprometidas.
- ✓ **Impacto reputacional**: daño potencial en la imagen o confianza institucional.
- ✓ **Tolerancia al tiempo de inactividad**: periodo máximo que la organización puede soportar sin operar el proceso.

La gestión adecuada de los procesos críticos permite definir estrategias de recuperación, asignar recursos prioritarios y fortalecer la sostenibilidad del negocio ante escenarios adversos. En este sentido, la continuidad operativa no depende únicamente de la existencia de planes documentados, sino de la capacidad institucional para anticipar riesgos, responder de forma oportuna y adaptarse a los cambios del entorno, garantizando la permanencia y competitividad en el largo plazo.

A continuación, se presenta una tabla orientativa para analizar los procesos críticos y su impacto en la sostenibilidad del negocio:

Tabla 2. Ejemplo de análisis de procesos críticos

Proceso crítico	Dependencias clave	Impacto ante interrupción	Tiempo máximo de recuperación (RTO)	Medidas de mitigación
Gestión de nómina.	Sistema contable y base de datos de empleados.	Retrasos en pagos, pérdida de confianza del personal.	24 horas	Copias de respaldo diarias y plan de contingencia manual.
Atención al cliente.	Plataforma CRM y red de comunicaciones.	Pérdida de clientes y deterioro de imagen.	12 horas	Servidores redundantes y canal alterno de comunicación.
Producción o prestación de servicio.	Suministros, maquinaria y personal técnico.	Interrupción del servicio y pérdida de ingresos.	8 horas	Inventarios de reserva y plan de reemplazo de equipos.

Proceso crítico	Dependencias clave	Impacto ante interrupción	Tiempo máximo de recuperación (RTO)	Medidas de mitigación
Gestión de información financiera.	Software ERP y acceso a bases de datos.	Incumplimiento legal y errores contables.	48 horas	Respaldos cifrados y acceso remoto seguro.

El análisis de estos procesos permite identificar las áreas más sensibles ante posibles fallos o emergencias, facilitando la toma de decisiones estratégicas que fortalecen la sostenibilidad del negocio. Este enfoque promueve la construcción de organizaciones más resilientes, preparadas para adaptarse a los cambios y responder eficazmente a los desafíos del entorno.

2.3. Beneficios de la continuidad del negocio para las organizaciones

La continuidad del negocio constituye un elemento esencial dentro de la gestión integral de riesgos, ya que permite garantizar la estabilidad operativa, proteger los activos y fortalecer la confianza de los grupos de interés. Implementar estrategias efectivas de continuidad no solo minimiza las pérdidas ante una interrupción, sino que también potencia la capacidad de adaptación y aprendizaje organizacional. Entre los principales beneficios se destacan los siguientes:

a) **Protección de los activos críticos**: asegura la integridad y disponibilidad de los recursos más importantes de la organización, tales como los sistemas de información, las instalaciones físicas, la infraestructura tecnológica y el capital humano.
b) **Reducción del impacto económico**: al contar con planes y procedimientos previamente definidos, se minimizan los costos derivados de la interrupción de procesos, la pérdida de ingresos o el deterioro de equipos e instalaciones.
c) **Cumplimiento normativo y reputacional**: contribuye a cumplir con regulaciones nacionales e internacionales, como la ISO 22301, y a mantener la confianza de clientes, proveedores, accionistas y entes reguladores.
d) **Continuidad operativa garantizada**: permite mantener la prestación de servicios esenciales o reanudar las operaciones en un tiempo razonable, reduciendo el tiempo de inactividad y evitando afectaciones en la cadena de valor.
e) **Fortalecimiento de la resiliencia institucional**: fomenta una cultura organizacional orientada a la prevención, la anticipación de riesgos y la respuesta efectiva frente a situaciones críticas.
f) **Mejora en la toma de decisiones estratégicas**: el análisis de los procesos críticos y la evaluación de riesgos ofrecen información valiosa para priorizar inversiones, recursos y esfuerzos de mejora continua.
g) **Ventaja competitiva sostenible**: una organización que demuestra estabilidad, cumplimiento y capacidad de recuperación se posiciona

favorablemente en su sector, generando mayor confianza y fidelización de clientes.

En términos prácticos, los beneficios de la continuidad del negocio se reflejan en la capacidad real de la organización para responder ante incidentes y mantener sus operaciones dentro de niveles aceptables de servicio. Este tipo de planificación se traduce en una respuesta organizada, con procedimientos claros y responsables definidos, lo que reduce la improvisación y mejora la coordinación entre las diferentes áreas. A continuación, se presenta un ejemplo práctico:

Una entidad financiera implementa un plan de continuidad del negocio que contempla la replicación de sus servidores en una ubicación alterna, la capacitación de su personal en protocolos de contingencia y la comunicación oportuna con los clientes ante eventos de interrupción. Durante una falla masiva en la red principal, la entidad activa su plan de recuperación, redirige las operaciones hacia su centro de respaldo y mantiene activos sus canales digitales. Gracias a ello, logra continuar ofreciendo servicios sin pérdidas económicas significativas ni afectación en la confianza de sus usuarios.

Este ejemplo refleja cómo la continuidad del negocio, más allá de ser una exigencia técnica, se convierte en una estrategia organizacional que contribuye directamente a la sostenibilidad, reputación y competitividad de la empresa a largo plazo.

3. Proyectos de continuidad del negocio

Los proyectos de continuidad del negocio constituyen un componente esencial dentro de la gestión integral de riesgos y la resiliencia organizacional. Su finalidad es planificar, diseñar e implementar mecanismos que permitan garantizar la operación continua de los procesos críticos ante cualquier evento que pueda interrumpir las actividades normales de la organización.

Estos proyectos se desarrollan con base en políticas, procedimientos y recursos específicos que buscan asegurar que, en caso de incidentes, la entidad pueda responder de manera estructurada y eficiente, minimizando los tiempos de inactividad y los impactos operativos, financieros y reputacionales.

La formulación de un proyecto de continuidad requiere identificar los procesos esenciales del negocio, analizar los riesgos asociados, definir estrategias de respuesta y establecer roles y responsabilidades claras. Asimismo, debe contemplar la coordinación entre las diferentes áreas, la comunicación efectiva durante emergencias y la implementación de mecanismos de recuperación tecnológica y operativa.

En términos generales, los proyectos de continuidad del negocio fortalecen la capacidad de las organizaciones para anticipar, resistir y recuperarse de los incidentes, consolidando una cultura de prevención y sostenibilidad. Los siguientes apartados profundizan en sus tipos, objetivos, alcance, beneficios y buenas prácticas de implementación.

3.1. Tipos y características de los proyectos de continuidad

Los proyectos de continuidad del negocio pueden adoptar diferentes enfoques según la naturaleza de la organización, el tipo de riesgo identificado y el alcance de las

operaciones que se busca proteger. Aunque todos comparten el objetivo de garantizar la continuidad de los procesos críticos, se diferencian por su propósito, nivel de intervención y grado de madurez dentro del sistema de gestión organizacional.

Entre los principales tipos de proyectos de continuidad se destacan:

- ✓ **Proyectos de prevención y preparación**: buscan anticiparse a posibles interrupciones mediante la identificación de amenazas, la implementación de controles preventivos y la capacitación del personal. Por ejemplo, la creación de políticas de respaldo de información o la instalación de sistemas redundantes.
- ✓ **Proyectos de respuesta y recuperación**: se centran en establecer procedimientos claros para actuar ante una crisis, restaurar los servicios esenciales y reducir el tiempo de inactividad. Suelen incluir planes de emergencia, protocolos de comunicación y estrategias de recuperación tecnológica.
- ✓ **Proyectos de mejora y fortalecimiento**: orientados a evaluar la eficacia de los planes existentes, realizar pruebas o simulacros y ajustar las estrategias según los resultados obtenidos. Este tipo de proyectos promueve la mejora continua y la madurez del sistema de gestión de continuidad.

En cuanto a las características clave de los proyectos de continuidad del negocio, se destacan las siguientes:

- ✓ **Enfoque proactivo**: priorizan la anticipación y la preparación frente a la reacción.

- ✓ **Orientación estratégica**: se alinean con los objetivos y políticas generales de la organización.
- ✓ **Integración transversal**: involucran a todas las áreas, desde la alta dirección hasta los equipos operativos.
- ✓ **Actualización constante**: deben revisarse periódicamente para adaptarse a cambios tecnológicos, normativos o estructurales.
- ✓ **Documentación formal**: requieren registros, procedimientos y evidencias verificables.
- ✓ **Medición y evaluación**: incluyen indicadores de desempeño que permiten evaluar su efectividad.

En conjunto, estos proyectos constituyen un marco estructurado que permite fortalecer la resiliencia organizacional, garantizando la continuidad de las operaciones y la sostenibilidad del negocio frente a imprevistos o emergencias.

3.2. Objetivos y alcance de los proyectos

Los proyectos de continuidad del negocio tienen como objetivo principal garantizar que las organizaciones estén preparadas para responder de manera eficaz ante incidentes que puedan interrumpir sus operaciones críticas. Buscan mantener la prestación de servicios esenciales, reducir el impacto de los eventos disruptivos y proteger los activos de información, los recursos humanos y la infraestructura tecnológica.

Entre los objetivos específicos más comunes se encuentran:

- ✓ Proteger la integridad y disponibilidad de la información ante eventos como fallas tecnológicas, ciberataques o desastres naturales.

- ✓ Asegurar la continuidad de los procesos críticos dentro de los niveles mínimos de operación aceptables.
- ✓ Reducir el tiempo de inactividad mediante estrategias de recuperación efectivas.
- ✓ Definir responsabilidades y procedimientos claros para la atención de incidentes.
- ✓ Cumplir con normativas nacionales e internacionales relacionadas con la gestión de la continuidad y la seguridad de la información (por ejemplo, ISO 22301 e ISO 27001).
- ✓ Fomentar una cultura organizacional resiliente, basada en la prevención y la mejora continua.

El alcance de los proyectos de continuidad depende del tamaño de la organización, su estructura operativa, los recursos disponibles y los riesgos a los que se encuentra expuesta. Puede abarcar desde un solo proceso crítico hasta todos los sistemas y áreas de la empresa.

Ejemplos de alcance según el tipo de organización:

a) **Empresa industrial**: un proyecto puede enfocarse en la continuidad de la línea de producción y la protección de la cadena de suministro, asegurando la disponibilidad de materias primas y maquinaria ante interrupciones.
b) **Entidad financiera**: puede centrarse en garantizar la operatividad de los sistemas de pago, la atención al cliente y la protección de la información confidencial.

c) **Institución educativa**: el proyecto podría incluir la disponibilidad de plataformas virtuales, sistemas académicos y servicios administrativos ante fallas tecnológicas.
d) **Entidad pública**: su alcance puede orientarse a la continuidad de los servicios ciudadanos y la preservación de datos institucionales frente a incidentes o ataques cibernéticos.

En todos los casos, definir con claridad el objetivo y alcance del proyecto permite priorizar los procesos esenciales, optimizar los recursos y asegurar que las estrategias implementadas sean coherentes con las necesidades reales de la organización. Esto facilita una respuesta estructurada, coordinada y eficaz ante cualquier evento que amenace la continuidad del negocio.

3.3. Beneficios y buenas prácticas en su implementación

La implementación de proyectos de continuidad del negocio aporta múltiples beneficios que fortalecen la estabilidad y competitividad de las organizaciones. Estos proyectos no solo preparan a las empresas para responder ante situaciones críticas, sino que también promueven una gestión proactiva y resiliente que favorece la mejora continua.

Entre los principales beneficios se destacan:

1) Reducción de pérdidas económicas y operativas, al minimizar el tiempo de inactividad y los costos derivados de interrupciones no planificadas.
2) Protección de la reputación institucional, ya que una respuesta eficaz ante crisis refuerza la confianza de los clientes, proveedores y partes interesadas.

3) Cumplimiento normativo y regulatorio, al alinearse con estándares internacionales como la norma ISO 22301, que establece los requisitos para los sistemas de gestión de continuidad del negocio.
4) Mejora en la toma de decisiones, gracias a la planificación y documentación de procedimientos claros para responder ante incidentes.
5) Fortalecimiento de la cultura organizacional, fomentando la responsabilidad compartida y el compromiso de todas las áreas en la gestión del riesgo.

En términos prácticos, estos beneficios se evidencian cuando las organizaciones logran mantener sus operaciones críticas o restablecerlas en plazos aceptables, evitando pérdidas significativas o impactos negativos en su imagen.

Una empresa de servicios tecnológicos que implementa un proyecto de continuidad del negocio, establece procedimientos para realizar copias de seguridad automáticas y configurar servidores de respaldo. Durante una falla inesperada en su centro de datos principal, la compañía activa su plan de recuperación y logra restablecer los servicios en menos de una hora. Esto evita afectaciones mayores a los clientes y demuestra la eficacia de su planificación.

Para maximizar estos beneficios, se recomienda aplicar las siguientes buenas prácticas:

- ✓ Realizar evaluaciones periódicas de riesgos y actualizar los planes de continuidad.
- ✓ Capacitar al personal en sus roles y responsabilidades dentro del plan.

- ✓ Realizar simulacros y pruebas regulares para validar la eficacia de los procedimientos.
- ✓ Mantener comunicación constante entre las áreas clave y la alta dirección.
- ✓ Documentar y revisar las lecciones aprendidas después de cada evento o ejercicio.

En conjunto, estas acciones fortalecen la resiliencia organizacional y permiten que la empresa responda con eficacia ante cualquier eventualidad, garantizando la continuidad de sus operaciones y la protección de sus recursos más valiosos.

4. Gestión del riesgo en la continuidad del negocio

La gestión del riesgo constituye uno de los pilares fundamentales de la continuidad del negocio, ya que permite anticipar, evaluar y controlar los factores que pueden afectar la estabilidad operativa de una organización. Su objetivo es garantizar que, ante la ocurrencia de incidentes o crisis, la entidad cuente con la capacidad de responder, recuperarse y mantener su funcionamiento esencial dentro de parámetros aceptables.

Históricamente, la gestión del riesgo ha evolucionado desde un enfoque reactivo, centrado en responder a desastres naturales o fallas operativas, hacia una visión preventiva e integral, que busca identificar los riesgos antes de que se materialicen. En la década de 1970, este concepto empezó a ganar relevancia en el ámbito empresarial, especialmente en sectores como la banca y las telecomunicaciones, donde las interrupciones operativas representaban grandes pérdidas económicas. Posteriormente, con el desarrollo de normas internacionales como la ISO 31000 sobre gestión del riesgo y la ISO 22301 sobre continuidad del negocio, se consolidó un marco

metodológico que integra la planificación, la evaluación y la mejora continua como ejes fundamentales.

Hoy en día, la gestión del riesgo no solo se limita a la protección de los activos físicos o tecnológicos, sino que abarca también la gestión reputacional, la seguridad de la información, la sostenibilidad ambiental y la estabilidad social. En un entorno caracterizado por la interdependencia global, la transformación digital y las amenazas emergentes (como los ciberataques o las disrupciones en la cadena de suministro), las organizaciones deben adoptar un enfoque proactivo que combine prevención, respuesta y aprendizaje.

Una gestión del riesgo eficaz dentro de la continuidad del negocio se basa en los siguientes principios:

a) Identificación temprana de amenazas internas y externas.
b) Evaluación sistemática de probabilidad e impacto sobre los procesos críticos.
c) Desarrollo de estrategias de mitigación, contingencia y recuperación.
d) Monitoreo y revisión continua del entorno operativo.
e) Fomento de una cultura organizacional resiliente que promueva la anticipación y la adaptación al cambio.

De esta manera, la gestión del riesgo no se concibe únicamente como un procedimiento técnico, sino como una competencia institucional que fortalece la capacidad de la organización para sostener sus operaciones, proteger sus recursos y asegurar la confianza de sus clientes, colaboradores y partes interesadas.

4.1. Identificación y análisis de riesgos operativos y tecnológicos

La identificación y análisis de riesgos operativos y tecnológicos constituye una etapa esencial dentro del proceso de gestión del riesgo y de la planificación de la continuidad del negocio. Su propósito es reconocer las amenazas que pueden afectar los activos críticos, los procesos esenciales y la infraestructura tecnológica de la organización, evaluando la probabilidad de su ocurrencia y el impacto potencial sobre las operaciones.

Desde una perspectiva organizacional, el riesgo operativo se define como la posibilidad de pérdida o afectación derivada de fallos en los procesos internos, errores humanos, deficiencias en los sistemas o eventos externos que alteren el funcionamiento normal de la entidad. Por su parte, el riesgo tecnológico está relacionado con las vulnerabilidades en los sistemas informáticos, redes, plataformas digitales y dispositivos, cuya explotación o falla puede comprometer la disponibilidad, integridad o confidencialidad de la información.

Estos riesgos pueden originarse por diferentes factores, entre los que se destacan:

- ✓ **Factores humanos**: errores de operación, negligencia, desconocimiento de procedimientos o falta de capacitación del personal.
- ✓ **Factores técnicos**: fallas en hardware, software, redes o servicios tecnológicos esenciales.
- ✓ **Factores físicos o ambientales**: incendios, inundaciones, cortes eléctricos, desastres naturales u otros eventos que afecten la infraestructura.
- ✓ **Factores externos**: ciberataques, sabotajes, fallos en servicios de terceros o interrupciones en la cadena de suministro.

- ✓ **Factores organizacionales**: ausencia de políticas de seguridad, deficiencias en el control interno o falta de mantenimiento preventivo.

El proceso de identificación de riesgos debe desarrollarse de forma sistemática y participativa, involucrando a las áreas claves de la organización para garantizar una visión integral. Entre las principales herramientas empleadas se encuentran:

- ✓ **Matrices de riesgo**: instrumentos que permiten listar las amenazas, estimar su probabilidad e impacto y priorizar las más críticas.
- ✓ **Análisis FODA de riesgos**: identifica fortalezas, oportunidades, debilidades y amenazas relacionadas con los activos y procesos clave.
- ✓ **Entrevistas y talleres con expertos**: facilitan la detección de vulnerabilidades no evidentes en los procedimientos operativos o tecnológicos.
- ✓ **Revisión de incidentes pasados**: permite aprender de experiencias previas y fortalecer las medidas de prevención y respuesta.

Una vez identificados los riesgos, se realiza su análisis, que consiste en evaluar la probabilidad de ocurrencia y el nivel de impacto sobre los objetivos organizacionales. Esta etapa facilita la priorización de los riesgos y la definición de acciones de mitigación adecuadas. El análisis puede ser cualitativo, basado en juicios de expertos y escalas descriptivas (alto, medio, bajo), o cuantitativo, utilizando métricas y datos históricos para calcular pérdidas potenciales y tiempos de recuperación.

Por ejemplo, en una organización de servicios financieros, la caída del sistema de transacciones puede ser clasificada como un riesgo tecnológico de alta probabilidad y alto impacto, mientras que un error en el envío de informes administrativos puede

representar un riesgo operativo de baja probabilidad y bajo impacto. Esta diferenciación permite enfocar los recursos en los riesgos más críticos para la continuidad del negocio.

El resultado final de este proceso se plasma en un mapa o matriz de riesgos, donde se representan gráficamente los riesgos identificados según su nivel de probabilidad e impacto, facilitando la toma de decisiones estratégicas y la asignación eficiente de recursos.

Una gestión eficaz de la identificación y análisis de riesgos contribuye a:

- ✓ Prevenir interrupciones operativas significativas.
- ✓ Optimizar los tiempos de respuesta ante emergencias.
- ✓ Fortalecer la confianza de clientes, usuarios y aliados.
- ✓ Cumplir con normativas internacionales como la ISO 31000 (Gestión del riesgo) y la ISO 22301 (Continuidad del negocio).

En síntesis, el análisis de riesgos operativos y tecnológicos permite anticipar escenarios adversos y diseñar estrategias preventivas que fortalezcan la resiliencia organizacional, asegurando la sostenibilidad y competitividad de la entidad frente a los desafíos del entorno.

4.2. Evaluación de probabilidad e impacto

La evaluación de la probabilidad e impacto es una fase fundamental dentro de la gestión del riesgo, ya que permite determinar el nivel de exposición de una organización frente a las amenazas identificadas y priorizar las acciones necesarias para su tratamiento. Este análisis constituye la base para la toma de decisiones estratégicas

orientadas a la protección de los activos, la continuidad del negocio y la resiliencia organizacional.

La probabilidad se refiere a la posibilidad de que un riesgo se materialice, considerando la frecuencia con la que podría ocurrir un evento adverso. Esta se estima a partir de datos históricos, registros de incidentes, comportamiento del entorno, condiciones tecnológicas y experiencia del personal. Por ejemplo, un ciberataque en una organización con múltiples vulnerabilidades tecnológicas puede considerarse de alta probabilidad, mientras que una falla en un centro de datos con redundancia y mantenimiento constante podría clasificarse de baja probabilidad.

El impacto, por su parte, corresponde a la magnitud de las consecuencias que tendría la ocurrencia del riesgo sobre los objetivos del negocio, la reputación institucional, la seguridad de la información o el cumplimiento normativo. Este puede expresarse en términos financieros, operativos, legales, reputacionales o sociales, dependiendo de la naturaleza de la organización y de los procesos afectados.

La combinación de ambos factores “probabilidad e impacto” permite determinar el nivel de riesgo, que refleja el grado de criticidad o prioridad de atención que debe asignarse a cada evento. En la práctica, este análisis se representa mediante una matriz de evaluación de riesgos, donde se cruzan los niveles de probabilidad e impacto, clasificando los riesgos en categorías como alto, medio o bajo.

Tabla 3. Ejemplo de matriz de evaluación de riesgos

Probabilidad / Impacto	Bajo impacto	Impacto medio	Alto impacto
Alta probabilidad	Riesgo medio	Riesgo alto	Riesgo crítico
Probabilidad media	Riesgo bajo	Riesgo medio	Riesgo alto
Baja probabilidad	Riesgo bajo	Riesgo bajo	Riesgo medio

Esta herramienta facilita la priorización de riesgos, orientando los esfuerzos hacia aquellos eventos con mayor posibilidad de ocurrencia y consecuencias más graves. Por ejemplo:

- ✓ Una interrupción del sistema de facturación podría clasificarse como riesgo alto, al tener alta probabilidad e impacto financiero significativo.
- ✓ Un error menor en reportes administrativos podría considerarse riesgo bajo, por su baja probabilidad e impacto limitado.

En algunos casos, la organización puede aplicar métodos cuantitativos, utilizando métricas y fórmulas para estimar la pérdida esperada o el tiempo de recuperación necesario. Entre los indicadores más utilizados se encuentran:

- ✓ **RTO (Recovery Time Objective)**: tiempo máximo de recuperación permitido para un proceso o sistema.
- ✓ **RPO (Recovery Point Objective)**: punto máximo de pérdida de datos aceptable.

- ✓ **MTD (Maximum Tolerable Downtime)**: tiempo máximo que la organización puede soportar sin ejecutar un proceso crítico.

Estas métricas permiten establecer umbrales de tolerancia y definir los tiempos y recursos requeridos para mantener la operatividad mínima durante una interrupción.

La evaluación de probabilidad e impacto no solo cuantifica el riesgo, sino que también promueve una visión preventiva, fortaleciendo la cultura de gestión anticipada en la organización. De esta manera, los equipos pueden priorizar inversiones, diseñar planes de contingencia realistas y establecer políticas de seguridad coherentes con la criticidad de los procesos y activos.

En síntesis, la evaluación de probabilidad e impacto permite pasar del simple reconocimiento de los riesgos a una gestión estratégica basada en evidencia, contribuyendo al desarrollo de organizaciones más resilientes, seguras y sostenibles frente a las amenazas emergentes del entorno.

4.3. Estrategias para mitigar riesgos y fortalecer la resiliencia organizacional

Una vez identificados y evaluados los riesgos, el siguiente paso dentro del proceso de gestión consiste en diseñar y aplicar estrategias de mitigación que permitan reducir la probabilidad de ocurrencia o el impacto potencial de los eventos adversos. Estas estrategias constituyen la base para la resiliencia organizacional, entendida como la capacidad de anticiparse, resistir, adaptarse y recuperarse ante interrupciones que puedan afectar la continuidad del negocio.

En términos generales, las estrategias de mitigación se clasifican en cuatro enfoques principales:

a) **Evitar el riesgo**: implica eliminar la causa o modificar las condiciones que generan la amenaza. Por ejemplo, suspender el uso de una tecnología obsoleta que presenta vulnerabilidades de seguridad.
b) **Reducir el riesgo**: consiste en aplicar controles preventivos o correctivos para disminuir su probabilidad o impacto, como la implementación de sistemas de respaldo, planes de mantenimiento o actualización de software.
c) **Transferir el riesgo**: se refiere a delegar parcial o totalmente la responsabilidad del riesgo a un tercero, a través de mecanismos como seguros, contratos de servicios externos o acuerdos con proveedores especializados.
d) **Aceptar el riesgo**: ocurre cuando los costos de mitigación superan los beneficios o cuando se considera que el riesgo es tolerable, siempre y cuando se mantenga bajo monitoreo y con planes de respuesta definidos.

La selección del enfoque depende del nivel de riesgo residual, los recursos disponibles y la tolerancia al riesgo de la organización. Para garantizar su efectividad, las estrategias deben alinearse con los objetivos estratégicos y los marcos de referencia internacionales, como la ISO 31000 (Gestión del riesgo), la ISO 27005 (Gestión del riesgo de seguridad de la información) y la ISO 22301 (Continuidad del negocio).

Entre las principales estrategias de mitigación y fortalecimiento de la resiliencia organizacional, se destacan las siguientes:

- ✓ Implementación de controles de seguridad de la información, tales como autenticación multifactor, cifrado de datos y gestión de accesos.

- ✓ Diseño de planes de contingencia y continuidad, que definan roles, responsabilidades, protocolos de comunicación y procedimientos de recuperación.
- ✓ Redundancia tecnológica, mediante la duplicación de sistemas críticos, servidores espejo o respaldos automáticos para garantizar la disponibilidad de la información.
- ✓ Capacitación y sensibilización del personal, orientada a promover buenas prácticas de seguridad y respuesta ante incidentes.
- ✓ Gestión de proveedores críticos, asegurando que las entidades externas también mantengan estándares adecuados de seguridad y continuidad.
- ✓ Simulacros y pruebas periódicas, que permitan validar la eficacia de las estrategias y detectar oportunidades de mejora.
- ✓ Análisis post-incidente, para identificar causas raíz, evaluar la efectividad de las acciones correctivas y fortalecer la capacidad de respuesta institucional.

Estas medidas no solo disminuyen la vulnerabilidad operativa y tecnológica, sino que fomentan una cultura organizacional proactiva, donde la prevención, la adaptación y la mejora continua se convierten en principios fundamentales de gestión.

A continuación, se presenta un ejemplo práctico:

Una empresa del sector financiero identifica como riesgo crítico la posible indisponibilidad del sistema de pagos en línea debido a un ataque informático. Como estrategias de mitigación, decide:

- ✓ Implementar una infraestructura de respaldo geográficamente separada.

- ✓ Aplicar controles de acceso más estrictos y cifrado de extremo a extremo.
- ✓ Realizar copias de seguridad diarias automáticas.
- ✓ Ejecutar pruebas de recuperación trimestrales.

Gracias a estas acciones, la organización logra mantener la continuidad del servicio y proteger la confianza de sus clientes, incluso ante un incidente real.

Las estrategias de mitigación de riesgos y fortalecimiento de la resiliencia organizacional deben concebirse como un proceso dinámico, integral y evolutivo, en el que la prevención, la preparación y la adaptación permiten a las organizaciones afrontar con éxito los desafíos de un entorno cada vez más incierto y complejo.

5. Sistema de Gestión de Continuidad del Negocio (SGCN)

Constituye el marco estructurado que permite a una organización prepararse, responder y recuperarse eficazmente ante interrupciones que afecten sus operaciones críticas. Su propósito principal es garantizar la disponibilidad de los recursos esenciales y la prestación continua de productos o servicios, incluso en condiciones adversas.

Un SGCN integra políticas, procedimientos, responsabilidades y recursos orientados a mantener la operatividad y la confianza de los grupos de interés. Además, promueve una cultura organizacional basada en la prevención, la mejora continua y la resiliencia. Este sistema no se limita a reaccionar frente a emergencias, sino que busca anticiparse a los riesgos, estableciendo medidas preventivas y planes de recuperación previamente probados.

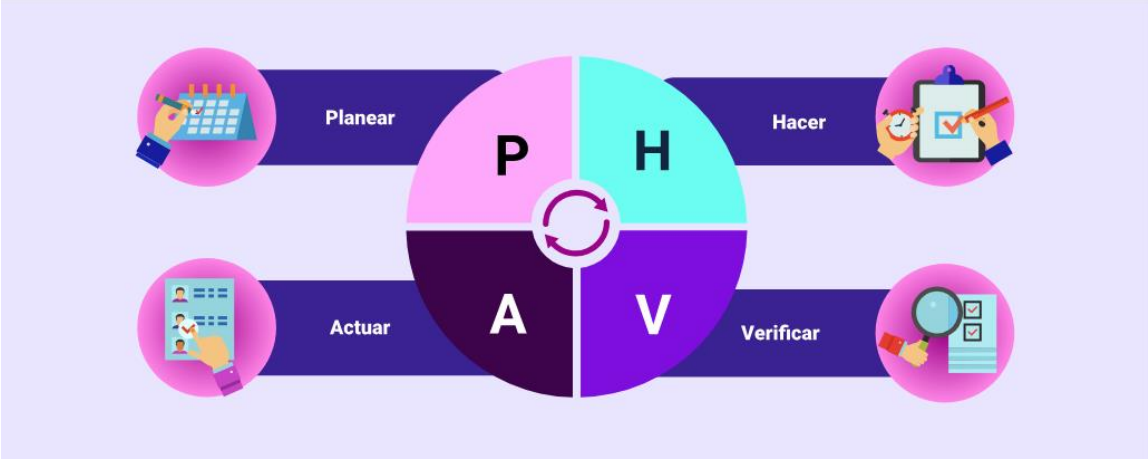
La adopción de un SGCN representa una ventaja competitiva, ya que fortalece la reputación institucional, mejora la toma de decisiones bajo presión y contribuye a cumplir con requisitos legales, normativos y contractuales. De esta manera, el SGCN se

convierte en una herramienta estratégica esencial para garantizar la sostenibilidad organizacional a largo plazo.

5.1. Estructura y componentes del sistema

El Sistema de Gestión de Continuidad del Negocio (SGCN) se compone de un conjunto de elementos interrelacionados que permiten planificar, implementar, operar, supervisar, revisar y mejorar continuamente la capacidad de una organización para responder ante interrupciones. Su estructura garantiza un enfoque sistemático y de mejora continua, y se fundamenta en el ciclo PHVA (Planear, Hacer, Verificar y Actuar):

Figura 1. Ciclo PHVA



Ciclo PHVA

- ✓ Planear
- ✓ Hacer
- ✓ Actuar
- ✓ Verificar

A continuación, se describen los componentes esenciales que conforman el SGCN:

a) **Política de continuidad del negocio**: define el compromiso de la alta dirección con la continuidad operativa. Esta política establece los principios, objetivos generales y el alcance del sistema, garantizando que las decisiones estratégicas se alineen con la resiliencia organizacional.
b) **Análisis de impacto en el negocio (BIA, por sus siglas en inglés)**: es un proceso clave que identifica las funciones críticas, los recursos necesarios y los tiempos máximos tolerables de interrupción. Su propósito es determinar las prioridades para la recuperación de operaciones, facilitando la toma de decisiones informada.
c) **Evaluación de riesgos**: consiste en identificar las amenazas que pueden afectar las operaciones (tecnológicas, naturales, humanas o externas), analizar su probabilidad de ocurrencia y el impacto potencial sobre los procesos críticos.
d) **Estrategias de continuidad**: comprenden las medidas preventivas y de recuperación que la organización diseña para garantizar la disponibilidad de recursos, la comunicación efectiva y la continuidad del servicio. Estas estrategias pueden incluir planes de respaldo de datos, redundancia tecnológica, acuerdos con proveedores o sitios alternos de operación.
e) **Planes de continuidad y recuperación**: son documentos operativos que detallan los procedimientos a seguir antes, durante y después de una interrupción. Incluyen asignación de responsabilidades, pasos de recuperación, protocolos de comunicación y mecanismos de activación del plan.
f) **Programa de capacitación y concienciación**: involucra la formación continua del personal en temas de gestión del riesgo, respuesta ante

emergencias y continuidad del negocio. Un personal capacitado garantiza una reacción coordinada y reduce errores durante situaciones críticas.

g) **Pruebas, ejercicios y simulaciones**: permiten evaluar la eficacia de los planes y detectar oportunidades de mejora. A través de simulacros, ejercicios de escritorio o pruebas técnicas, la organización valida la funcionalidad de los procedimientos y la capacidad de respuesta de los equipos.

h) **Seguimiento y mejora continua**: incluye auditorías internas, revisiones por la dirección y análisis de desempeño del sistema. Este componente asegura que el SGCN se mantenga actualizado y alineado con los cambios del entorno, las tecnologías emergentes y las lecciones aprendidas.

En conjunto, estos elementos proporcionan una base sólida para garantizar la continuidad operativa, la protección de los activos y la confianza de los clientes y socios estratégicos. Un SGCN bien estructurado no solo responde ante crisis, sino que también fortalece la cultura organizacional, promoviendo la anticipación, la prevención y la resiliencia como pilares de la gestión empresarial moderna.

5.2. Características clave para su implementación efectiva

La implementación efectiva de un Sistema de Gestión de Continuidad del Negocio (SGCN) requiere la integración de una serie de características fundamentales que garanticen su funcionalidad, sostenibilidad y alineación con los objetivos estratégicos de la organización. Estas características aseguran que el sistema no sea solo un conjunto de procedimientos documentados, sino una práctica viva que fortalece la resiliencia y la capacidad de respuesta institucional.

Entre las principales características se destacan:

- ✓ **Enfoque basado en el riesgo**: la identificación, evaluación y priorización de riesgos es el punto de partida del SGCN, permitiendo enfocar los esfuerzos en los procesos más críticos y vulnerables para la organización.
- ✓ **Compromiso de la alta dirección**: el liderazgo y apoyo de la alta dirección son esenciales para asignar recursos, definir responsabilidades, promover la cultura de continuidad y garantizar la integración del sistema con la estrategia corporativa.
- ✓ **Participación y sensibilización del personal**: la continuidad del negocio no depende únicamente de políticas o procedimientos, sino de la preparación del talento humano. La capacitación, los simulacros y la comunicación interna fortalecen la respuesta colectiva ante incidentes.
- ✓ **Integración con otros sistemas de gestión**: un SGCN efectivo se articula con los sistemas de gestión de calidad, seguridad de la información, salud y seguridad en el trabajo, y gestión ambiental, evitando duplicidades y fomentando la coherencia institucional.
- ✓ **Documentación y control de la información**: los procedimientos, planes de respuesta y registros deben mantenerse actualizados, accesibles y protegidos, de manera que sirvan de guía práctica en situaciones de emergencia.
- ✓ **Pruebas y ejercicios periódicos**: la verificación constante mediante simulaciones y auditorías permite evaluar la eficacia de los planes de continuidad, identificar oportunidades de mejora y reforzar la capacidad operativa.

- ✓ **Mejora continua:** el sistema debe revisarse y ajustarse de forma permanente con base en los resultados de pruebas, auditorías o incidentes reales, promoviendo la innovación y la adaptación al cambio.

Estas características, en conjunto, garantizan que el SGCN se mantenga como una herramienta dinámica que evoluciona con la organización y sus entornos de riesgo, asegurando la continuidad operativa, la protección de los activos críticos y la confianza de las partes interesadas.

La puesta en marcha de un SGCN, implica seguir una secuencia estructurada que asegure la eficacia y coherencia del proceso. Las etapas más comunes son:

1) **Diagnóstico inicial**: evaluación del contexto, análisis de brechas y revisión de los procesos críticos existentes.
2) **Definición del alcance**: delimitación de los procesos, áreas y activos que estarán cubiertos por el SGCN.
3) **Política y compromiso de la dirección**: establecimiento de la política de continuidad y asignación de recursos.
4) **Análisis de impacto en el negocio (BIA)**: identificación de funciones esenciales, tiempos de recuperación y dependencias clave.
5) **Evaluación de riesgos**: determinación de amenazas, vulnerabilidades y probabilidad de ocurrencia.
6) **Desarrollo de estrategias de continuidad**: diseño de planes de respuesta, recuperación y comunicación.
7) **Implementación y capacitación**: ejecución de los planes, formación del personal y difusión de responsabilidades.

8) **Pruebas, mantenimiento y mejora continua**: validación periódica del sistema, revisión de resultados y ajustes según los cambios organizacionales o tecnológicos.

Estas etapas permiten asegurar que el SGCN no solo se documente correctamente, sino que funcione en la práctica como un sistema preventivo, adaptable y sostenible.

5.3. Normativa y estándares internacionales aplicables

La gestión de la continuidad del negocio en Colombia se encuentra respaldada por diversas disposiciones legales y lineamientos nacionales, que establecen la necesidad de proteger la información, garantizar la prestación continua de los servicios y fortalecer la resiliencia institucional. Estas normativas constituyen la base sobre la cual se desarrollan los sistemas de gestión, asegurando su alineación con los estándares internacionales.

Entre las principales normas y marcos regulatorios nacionales se destacan:

- ✓ **Ley 1581 de 2012 y Decreto 1377 de 2013**: regulan la protección de datos personales y establecen obligaciones sobre el tratamiento seguro de la información.
- ✓ **Circular Básica Jurídica (Capítulo VI, Título I) de la Superintendencia Financiera de Colombia**: exige a las entidades vigiladas implementar planes de continuidad del negocio para garantizar la estabilidad operativa y la protección de los recursos financieros.

- ✓ **Decreto 1083 de 2015**: compila normas del sector público y promueve la adopción de prácticas de gestión del riesgo y continuidad en las entidades estatales.
- ✓ **Política de Seguridad y Privacidad de la Información del Estado Colombiano (PSPIEC)**: define directrices para la protección de la información, la gestión de incidentes y la continuidad de los servicios en el ámbito gubernamental.

Estas disposiciones nacionales se articulan con normas y estándares internacionales, que proporcionan metodologías y marcos de referencia para el diseño e implementación de sistemas de gestión eficaces. Entre ellos se destacan:

A. ISO 22301:2019-Sistemas de Gestión de la Continuidad del Negocio

Establece los requisitos para planificar, implementar, mantener y mejorar un sistema que garantice la continuidad de las operaciones ante interrupciones. Su enfoque se basa en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), fomentando la mejora continua y la preparación ante emergencias.

B. ISO/IEC 27001:2022-Sistemas de Gestión de la Seguridad de la Información

Complementa la ISO 22301 al establecer controles para proteger la confidencialidad, integridad y disponibilidad de la información, aspectos esenciales para la continuidad organizacional.

C. ISO 31000:2018-Gestión del Riesgo

Proporciona principios y directrices para identificar, analizar y tratar los riesgos que puedan afectar el logro de los objetivos institucionales y la continuidad operativa.

De manera complementaria, otras referencias internacionales como la NFPA 1600 (gestión de emergencias), NIST SP 800-34 (planificación de continuidad de TI) y los marcos COBIT e ITIL (gobierno y gestión de servicios tecnológicos) ofrecen buenas prácticas aplicables según el tipo de organización y su nivel de madurez.

En conjunto, estas normativas y estándares fortalecen la capacidad institucional para anticipar, responder y recuperarse de incidentes que puedan afectar la operación, promoviendo una cultura de resiliencia y cumplimiento normativo.

6. Aplicación práctica

La aplicación práctica de los conceptos relacionados con la continuidad del negocio y la seguridad de la información permite trasladar los conocimientos teóricos a escenarios reales, fortaleciendo la capacidad de análisis, diagnóstico y toma de decisiones en contextos organizacionales. En esta etapa, el aprendiz integra las competencias desarrolladas para identificar activos de información, analizar riesgos y establecer prioridades que aseguren la sostenibilidad operativa.

El propósito de esta sección es que el aprendiz reconozca, dentro de un entorno simulado o real, cómo los diferentes elementos del Sistema de Gestión de Continuidad del Negocio (SGCN) interactúan para garantizar la protección de los recursos críticos, la mitigación de riesgos y la continuidad de las operaciones ante posibles incidentes.

A través de ejercicios de análisis, caracterización y evaluación, se busca promover una comprensión integral del ciclo de continuidad, desde la identificación de activos

hasta la definición de estrategias de respuesta, permitiendo aplicar las mejores prácticas basadas en estándares internacionales como la ISO 22301 y la ISO 27001.

6.1. Identificación de activos y procesos críticos en una organización

La identificación de activos y procesos críticos es una actividad esencial dentro del Sistema de Gestión de Continuidad del Negocio (SGCN), ya que permite determinar los elementos cuya pérdida o interrupción podría comprometer gravemente la capacidad operativa, financiera, legal o reputacional de una organización. Este proceso constituye la base para el análisis de riesgos, la definición de estrategias de recuperación y la priorización de recursos en situaciones de crisis.

En primer lugar, se debe realizar una identificación exhaustiva de los activos que soportan los procesos misionales y de apoyo. Un activo se entiende como todo recurso que posee valor para la organización, y puede clasificarse en las siguientes categorías:

- ✓ **Activos de información**: datos, bases de datos, registros, documentos y sistemas que contienen información crítica.
- ✓ **Activos tecnológicos**: hardware, software, redes, servidores, dispositivos de comunicación y sistemas de respaldo.
- ✓ **Activos humanos**: conocimientos, habilidades y experiencia del personal clave en la operación.
- ✓ **Activos físicos**: infraestructura, instalaciones, equipos y mobiliario.
- ✓ **Activos intangibles**: reputación, propiedad intelectual, relaciones comerciales y confianza institucional.

Una vez identificados los activos, se procede a determinar los procesos críticos, entendidos como aquellas actividades o funciones que, de ser interrumpidas, afectarían

de manera significativa los objetivos estratégicos de la organización, el cumplimiento normativo o la prestación de servicios esenciales. Para ello, se recomienda realizar un Análisis de impacto en el negocio (BIA, por sus siglas en inglés), el cual permite:

1) Identificar los procesos organizacionales y sus dependencias.
2) Evaluar las consecuencias de su interrupción, considerando aspectos financieros, operativos, legales, reputacionales y de seguridad.
3) Estimar el tiempo máximo de inactividad tolerable (RTO) y el nivel de pérdida de datos admisible (RPO).
4) Clasificar y priorizar los procesos según su nivel de criticidad e impacto.

Durante este análisis, es importante incluir las interdependencias internas y externas, es decir, la relación entre procesos, áreas y proveedores, ya que una interrupción en un componente puede generar un efecto en cadena sobre otros servicios esenciales. Asimismo, se deben registrar los controles existentes y las brechas identificadas, con el fin de definir acciones preventivas o correctivas.

El resultado de esta etapa se materializa en un inventario documentado de activos y procesos críticos, que incluye su descripción, responsable, ubicación, nivel de criticidad y medidas de protección existentes.

A continuación, se presenta un ejemplo de formato para registrar los activos y procesos críticos de una organización, con el fin de facilitar su análisis y priorización dentro del Sistema de Gestión de Continuidad del Negocio (SGCN):

Tabla 4. Ejemplo de inventario de activos y procesos críticos

Activo o recurso	Proceso asociado	Descripción / Función principal	Impacto ante interrupción	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Nivel de criticidad	Responsable
Servidor principal de datos.	Gestión académica.	Almacena la base de datos institucional, registros académicos y financieros.	Alta afectación en la operación y pérdida de información sensible.	4 horas	1 hora	Crítico	Coordinador de TI.
Plataforma virtual de	Formación en línea.	Permite el acceso de instructores y	Alta, afecta continuidad del	6 horas	2 horas	Crítico	Administrador LMS.

Activo o recurso	Proceso asociado	Descripción / Función principal	Impacto ante interrupción	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Nivel de criticidad	Responsable
aprendizaje.		aprendices a contenidos y evaluaciones.	servicio educativo.				
Sistema contable.	Finanzas.	Registra y gestiona transacciones financieras y presupuestales.	Media, genera retrasos en reportes y pagos.	12 horas	4 horas	Alta	Contador general.

Activo o recurso	Proceso asociado	Descripción / Función principal	Impacto ante interrupción	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Nivel de criticidad	Responsable
Red eléctrica y UPS.	Soporte tecnológico.	Garantiza suministro de energía a servidores y equipos críticos.	Muy alta, afecta toda la operación tecnológica.	2 horas	0 horas	Crítico	Jefe de mantenimiento.
Personal técnico especializado.	Soporte operativo.	Brinda mantenimiento y atención a incidentes técnicos.	Media, afecta tiempos de respuesta y	8 horas	N/A	Media	Coordinador de soporte.

Activo o recurso	Proceso asociado	Descripción / Función principal	Impacto ante interrupción	RTO (Tiempo máximo de recuperación)	RPO (Pérdida máxima de datos aceptable)	Nivel de criticidad	Responsable
			resolución.				

Esta tabla ejemplifica cómo se documentan los activos y procesos críticos dentro del Sistema de Gestión de Continuidad del Negocio. Cada fila representa un elemento esencial para el funcionamiento organizacional, incluyendo información clave sobre su función, impacto, tiempos de recuperación (RTO y RPO), nivel de criticidad y responsable directo.

El análisis conjunto de estos datos permite priorizar recursos, establecer estrategias de respaldo y definir planes de contingencia más eficaces.

Por ejemplo, en una institución educativa, los sistemas de gestión académica, la plataforma virtual de aprendizaje y la base de datos de aprendices representan activos y procesos críticos, ya que su interrupción afectaría directamente la prestación del servicio y la confianza de la comunidad educativa.

En conclusión, la identificación de activos y procesos críticos no solo permite conocer los puntos más vulnerables de la organización, sino que también orienta la toma de decisiones estratégicas para asegurar la resiliencia y la continuidad de las operaciones ante cualquier contingencia.

6.2. Análisis de riesgos y continuidad operativa

El análisis de riesgos constituye una etapa fundamental dentro del Sistema de Gestión de Continuidad del Negocio (SGCN), ya que permite identificar, evaluar y priorizar las amenazas que pueden afectar los activos, procesos críticos y operaciones esenciales de una organización. Su propósito es determinar el nivel de exposición ante eventos que podrían interrumpir las actividades normales y, a partir de ello, definir medidas de control y recuperación que garanticen la continuidad operativa.

El proceso inicia con la identificación de riesgos, donde se reconocen los eventos potenciales que podrían afectar los activos de información, los recursos humanos, la infraestructura tecnológica o las instalaciones físicas. Estos riesgos pueden clasificarse en tres grandes categorías:

- ✓ **Riesgos operativos**: fallas humanas, errores de procedimiento, deficiencias en la cadena de suministro o interrupciones en servicios esenciales.
- ✓ **Riesgos tecnológicos**: ataques cibernéticos, pérdida de datos, caídas de sistemas, fallas de hardware o software.
- ✓ **Riesgos externos o ambientales**: desastres naturales, cortes de energía, disturbios sociales o emergencias sanitarias.

Una vez identificados los riesgos, se procede a su evaluación, considerando dos variables principales:

a) Probabilidad de ocurrencia, es decir, la frecuencia o posibilidad de que el evento se materialice.
b) Impacto potencial, que representa el grado de afectación que tendría el riesgo sobre los objetivos estratégicos, la continuidad de las operaciones y la reputación de la organización.

El cruce de estas variables permite establecer un nivel de riesgo (bajo, medio o alto) y priorizar la implementación de controles y estrategias de mitigación. Esta valoración puede representarse en una matriz de riesgos, una herramienta visual que facilita la toma de decisiones y el seguimiento de acciones preventivas.

La siguiente tabla presenta un ejemplo de cómo estructurar una matriz de análisis de riesgos para apoyar la continuidad operativa:

Tabla 5. Ejemplo de matriz de análisis de riesgos y continuidad operativa

Riesgo identificado	**Tipo de riesgo**	**Activo o proceso afectado**	**Probabilidad**	**Impacto**	**Nivel de riesgo**	**Estrategia de mitigación**	**Responsable**
Falla del servidor principal.	Tecnológico	Plataforma virtual de	Alta	Alto	Alto	Implementar servidores redundant	Coordinador de TI.

Riesgo identificado	Tipo de riesgo	Activo o proceso afectado	Probabilidad	Impacto	Nivel de riesgo	Estrategia de mitigación	Responsable
		aprendizaje.				es y copias de seguridad diarias.	
Interrupción del suministro eléctrico.	Operativo / Externo	Sistemas críticos y red interna.	Media	Alto	Alto	Instalación de UPS y planta eléctrica de respaldo.	Jefe de mantenimiento.
Error humano en carga de información.	Operativo	Base de datos académica.	Alta	Medio	Medio	Capacitación y procedimientos de control de cambios.	Administrador de base de datos.

Riesgo identificado	Tipo de riesgo	Activo o proceso afectado	Probabilidad	Impacto	Nivel de riesgo	Estrategia de mitigación	Responsable
Ciberataque (ransomware).	Tecnológico	Información institucional.	Media	Alto	Alto	Políticas de ciberseguridad, antivirus actualizado y respaldos cifrados.	Coordinador de seguridad.
Emergencia sanitaria.	Externo	Actividades presenciales.	Baja	Alto	Medio	Implementar modalidad de teletrabajo y clases virtuales.	Dirección académica.

El análisis de riesgos no solo se limita a detectar amenazas, sino que también permite planificar respuestas operativas y definir responsabilidades claras ante diferentes escenarios. De esta manera, la organización puede anticipar sus vulnerabilidades y preparar planes de acción que reduzcan el impacto de los eventos disruptivos.

Por ejemplo, una institución educativa que identifique como riesgo la caída de su plataforma virtual puede establecer un sistema de respaldo en la nube y protocolos de comunicación alternativos, garantizando así la continuidad del proceso formativo sin mayores interrupciones.

En síntesis, el análisis de riesgos constituye el puente entre la prevención y la respuesta efectiva. Al integrar los resultados de este análisis con los planes de continuidad del negocio, la organización fortalece su capacidad de resiliencia, minimiza pérdidas y asegura su sostenibilidad operativa ante cualquier eventualidad.

6.3. Caracterización de necesidades de seguridad de la información

La caracterización de las necesidades de seguridad de la información consiste en identificar, analizar y priorizar los requerimientos que garantizan la protección de los activos de información y el cumplimiento de los principios de confidencialidad, integridad y disponibilidad. Esta etapa es esencial dentro del Sistema de Gestión de Continuidad del Negocio (SGCN), ya que permite establecer controles adecuados que aseguren la resiliencia tecnológica y operativa frente a posibles amenazas.

El proceso inicia con la evaluación del contexto organizacional, que implica analizar el entorno interno y externo, los objetivos estratégicos, los requisitos legales o normativos, y las expectativas de las partes interesadas (clientes, proveedores,

entidades de control, entre otros). A partir de este diagnóstico, se determinan los requisitos de seguridad específicos de cada activo y proceso crítico.

Entre las principales necesidades de seguridad de la información se destacan las siguientes:

- ✓ **Protección de la confidencialidad**: asegurar que solo las personas autorizadas accedan a la información sensible o restringida.
- ✓ **Garantía de la integridad**: mantener la exactitud, coherencia y confiabilidad de los datos a lo largo de su ciclo de vida.
- ✓ **Disponibilidad operativa**: garantizar el acceso oportuno a la información y los sistemas cuando sea necesario para la operación.
- ✓ **Trazabilidad y control de acceso**: registrar y monitorear las acciones realizadas sobre los activos de información.
- ✓ **Cumplimiento normativo**: adoptar controles alineados con estándares internacionales (como ISO/IEC 27001 e ISO 22301) y la normativa nacional aplicable.

Una vez identificadas las necesidades, se procede a definir las medidas de seguridad y control que mitiguen los riesgos detectados en el análisis previo. Estas medidas pueden incluir acciones técnicas, administrativas o físicas, tales como:

- ✓ Autenticación y control de accesos.
- ✓ Cifrado de datos y comunicaciones.
- ✓ Políticas de copias de seguridad y recuperación de información.
- ✓ Capacitación en buenas prácticas de ciberseguridad.
- ✓ Supervisión y auditoría continua de los sistemas.

La siguiente tabla presenta un ejemplo práctico de caracterización de necesidades de seguridad de la información, que permite relacionar los activos críticos con los riesgos asociados y las medidas de control sugeridas.

Tabla 6. Ejemplo de caracterización de necesidades de seguridad de la información

Activo o proceso crítico	Riesgo identificado	Necesidad de seguridad	Medida de control o mitigación	Responsable
Base de datos académica.	Acceso no autorizado.	Confidencialidad y control de acceso.	Implementar autenticación multifactor y perfiles de usuario diferenciados.	Administrador de TI.
Plataforma virtual de aprendizaje.	Falla del sistema o pérdida de datos.	Disponibilidad y respaldo.	Copias de seguridad automáticas y servidores redundantes.	Coordinador de tecnología.
Sistema contable.	Alteración de información financiera.	Integridad y trazabilidad.	Registro de auditoría y validación	Contador general.

Activo o proceso crítico	Riesgo identificado	Necesidad de seguridad	Medida de control o mitigación	Responsable
			cruzada de datos.	
Correo institucional.	Phishing o robo de credenciales.	Confidencialidad e integridad.	Filtros antispam, campañas de sensibilización y políticas de contraseñas seguras.	Área de seguridad informática.
Red de comunicaciones.	Ciberataque o malware.	Continuidad y protección perimetral.	Firewalls, antivirus actualizado y segmentación de red.	Coordinador de infraestructura.

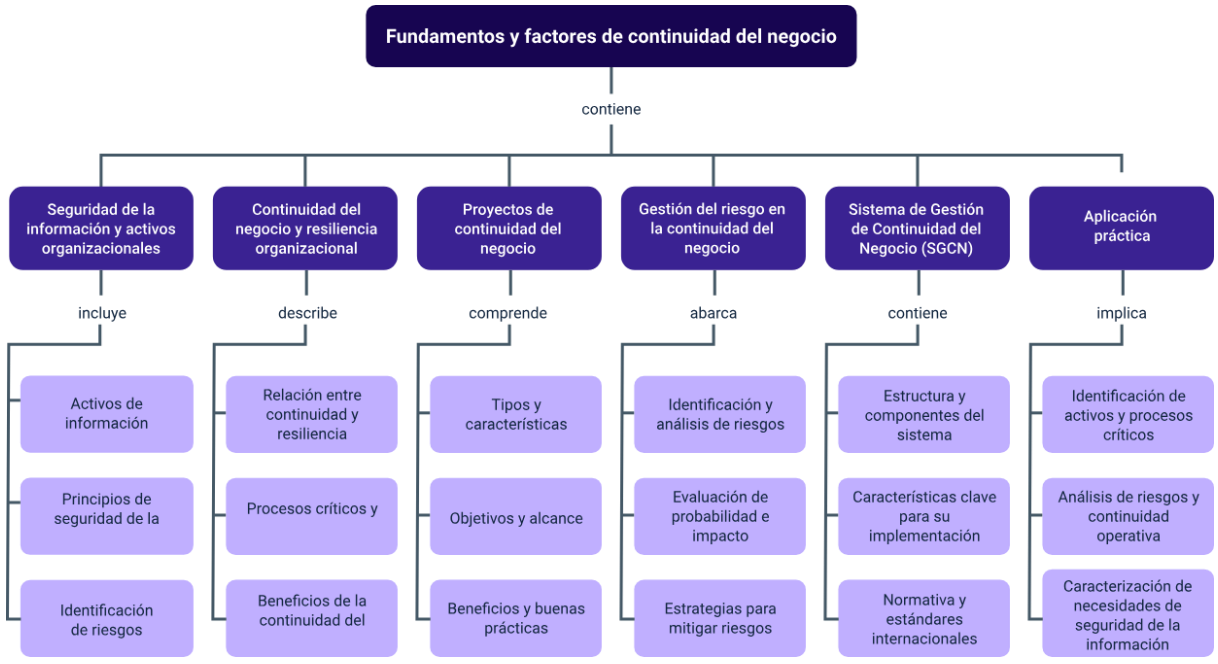
Este ejercicio permite establecer un mapa claro de las prioridades en materia de seguridad, facilitando la asignación de recursos y responsabilidades. Además, contribuye a fortalecer la cultura organizacional hacia la prevención y respuesta ante incidentes de seguridad.

Por ejemplo, en una institución educativa, la caracterización de necesidades de seguridad puede evidenciar que la protección de las bases de datos académicas y la disponibilidad de la plataforma virtual son aspectos prioritarios. En este caso, se implementan controles como respaldos automáticos, restricciones de acceso y monitoreo constante de la infraestructura tecnológica.

En conclusión, la caracterización de necesidades de seguridad de la información proporciona una visión integral de las vulnerabilidades y fortalezas de la organización, permitiendo desarrollar políticas y estrategias alineadas con los objetivos del negocio y los requerimientos de continuidad operativa. Su adecuada gestión contribuye a consolidar una cultura de seguridad, confianza y resiliencia digital.

Síntesis

El componente formativo aborda los fundamentos y factores que garantizan la continuidad del negocio y la protección de los activos de información en las organizaciones. Se analizan los principios de seguridad, la gestión del riesgo y la importancia de la resiliencia organizacional para mantener las operaciones ante posibles interrupciones. Asimismo, se estudian los tipos de proyectos de continuidad, sus objetivos y beneficios, junto con la estructura del Sistema de Gestión de Continuidad del Negocio (SGCN) y las normas internacionales que lo respaldan, como las ISO 22301 e ISO 27001. Finalmente, se incluyen ejercicios prácticos orientados a la identificación de procesos críticos, el análisis de riesgos y la caracterización de necesidades de seguridad, fortaleciendo las competencias necesarias para garantizar la sostenibilidad y la continuidad operativa en cualquier contexto.



Material Complementario

Tema	Referencia	Tipo de material	Enlace del recurso
Seguridad de la información y activos organizacionales	Ecosistema de Recursos Educativos Digitales SENA. (2022). Controles y estándares para el manejo de la seguridad de la información [Video]. YouTube.	Video	https://www.youtube.com/watch?v=n6Dffo75ts0
Sistema de Gestión de Continuidad del Negocio (SGCN)	Ecosistema de Recursos Educativos Digitales SENA. (2022). Sistemas de gestión de continuidad del negocio - SGCN [Video]. YouTube.	Video	https://www.youtube.com/watch?v=qpuZFGZG8Gk
Sistema de Gestión de Continuidad del Negocio (SGCN)	Ecosistema de Recursos Educativos Digitales SENA. (2022). Implementación de un SGCN [Video]. YouTube.	Video	https://www.youtube.com/watch?v=ZbrLjTtDFcY

Glosario

Activo de información: recurso que posee valor para la organización, como datos, sistemas, infraestructura o conocimientos, cuya protección es fundamental para mantener la operación y la seguridad institucional.

Análisis de impacto en el negocio (BIA): herramienta que permite identificar los procesos críticos y evaluar las consecuencias de su interrupción, ayudando a definir estrategias de recuperación efectivas.

Continuidad del negocio: capacidad de una organización para mantener sus funciones críticas y recuperarse rápidamente ante incidentes que interrumpan sus operaciones normales.

ISO 22301: norma internacional que establece los requisitos para implementar y mantener un Sistema de Gestión de Continuidad del Negocio eficaz.

ISO 27001: norma que define los lineamientos para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

Resiliencia organizacional: habilidad de una organización para adaptarse, resistir y recuperarse de situaciones adversas, garantizando su estabilidad y sostenibilidad a largo plazo.

Riesgo operativo: posibilidad de pérdidas o impactos negativos debido a fallas en los procesos, el personal, los sistemas o factores externos.

RPO (Recovery Point Objective): cantidad máxima de datos que una organización puede permitirse perder, medida en el tiempo transcurrido entre la última copia de seguridad y el momento de la interrupción.

RTO (Recovery Time Objective): tiempo máximo aceptable que una organización puede tardar en recuperar un proceso o sistema tras una interrupción.

Sistema de Gestión de Continuidad del Negocio (SGCN): conjunto de políticas, procedimientos y recursos que aseguran la planificación, implementación y mejora continua de la continuidad operativa en la organización.

Referencias bibliográficas

ISO. (2018). ISO 31000:2018 - Risk management: Guidelines. 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.

ISO. (s.f.). ISO/IEC 27005 - Information security risk management. International Organization for Standardization.

República de Colombia. (2013). Decreto 1377 de 2013. En uso de sus atribuciones constitucionales, y en particular las previstas en el numeral 11 del artículo 189 de la Constitución Política y en la Ley 1581 de 2012. Reglamentario del Sector de Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

República de Colombia. (2015). Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=62866

República de Colombia. (2020). Políticas de Operación Proceso de Tecnologías de la Información. Reglamentario del Sector de Función Pública. https://www1.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672

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

Superintendencia Financiera de Colombia. (2014). Circular Básica Jurídica. Circular Externa 029 de 2014 (Capítulo VI, Título I).

Superintendencia Financiera de Colombia. (2025). Circular Externa 006 de 2025 — Versión actualizada de la Circular Básica Jurídica.

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