CAIGG
CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO
Ministerio Secretaría General de la Presidencia

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°10

INTRODUCCIÓN A LA CONTINUIDAD DEL NEGOCIO

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°10: Introducción a la Continuidad del Negocio.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, Mayo 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

INTRODUCCIÓN A LA CONTINUIDAD DEL NEGOCIO

La gestión de continuidad del negocio (BCM) es una disciplina estratégica diseñada para preparar y guiar a las organizaciones en la prevención, mitigación y recuperación ante incidentes disruptivos que puedan afectar su operación normal. Esta gestión forma parte integral de un enfoque holístico de resiliencia organizacional, donde se busca proteger no solo los activos físicos y tecnológicos, sino también el capital humano, la reputación, y los servicios críticos que provee la organización.

Hoy en día, las empresas enfrentan un panorama de riesgos altamente diversificado, desde desastres naturales, interrupciones tecnológicas, ciberataques, hasta riesgos socioeconómicos. Las organizaciones que carecen de una planificación adecuada para hacer frente a estos riesgos pueden experimentar pérdidas significativas, no solo financieras, sino también en términos de reputación y confianza de las partes interesadas. De ahí surge la importancia de implementar un sistema de gestión de continuidad del negocio (SGCN), basado en estándares internacionales como ISO 22301.

Nota Importante

Estrictamente hablando, **Seguridad de la Información y Ciberseguridad** son dos conceptos diferentes.

La **"Seguridad de la Información"** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **"Ciberseguridad"** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de "Seguridad de la Información y Ciberseguridad", pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de "Seguridad de la Información", "Ciberseguridad" o el acrónimo "SIC" como sinónimos para mejorar la comprensión lectora.

El principal objetivo de la gestión de continuidad del negocio es asegurar que las operaciones críticas de una organización puedan continuar o ser restauradas en el menor tiempo posible después de un incidente. Un incidente disruptivo puede variar en su naturaleza y alcance, desde una simple falla técnica hasta un desastre mayor que comprometa las operaciones en múltiples niveles.

Ejemplo:

Imaginemos una organización de servicios financieros que depende de sistemas informáticos para procesar transacciones. Una falla en su infraestructura de TI podría detener la operación y generar grandes pérdidas económicas, además de afectar la confianza del cliente. La implementación de un plan de continuidad del negocio garantiza que existan procedimientos para restaurar la funcionalidad clave rápidamente, minimizando el impacto en los clientes y las operaciones comerciales.

¿Por qué es Importante la Continuidad del Negocio?

En el entorno actual, la creciente vulnerabilidad de la sociedad y el amplio acceso a la información han generado una mayor exposición a riesgos que pueden afectar de manera crítica la operatividad de las organizaciones. Ante estos desafíos, diversos reguladores clave, como la Comisión para el Mercado Financiero (CMF), la Superintendencia de Servicios Sanitarios (SISS), el Servicio Nacional de Geología y Minería (SERNAGEOMIN), la Subsecretaría de Telecomunicaciones (SUBTEL), el Servicio Nacional del Consumidor (SERNAC), entre otros, han establecido la necesidad de que las organizaciones implementen estrategias robustas de Respuesta, Reanudación, Recuperación y Restauración de sus productos y servicios.

Estas estrategias tienen como objetivo garantizar que, ante cualquier interrupción significativa —ya sea por desastres naturales, ataques cibernéticos, fallas técnicas o cualquier otro incidente—, las organizaciones estén en capacidad de retomar rápidamente sus operaciones, minimizar el impacto en los usuarios y proteger la integridad de sus datos y recursos.

La continuidad de negocio es un elemento clave en la gestión de cualquier organización, ya que no solo se encarga de prevenir incidentes relacionados con la tecnología de la información, sino también otros eventos transversales que pueden afectar gravemente las operaciones del negocio. Esta práctica busca asegurar que, ante cualquier tipo de interrupción, la organización pueda seguir operando de manera efectiva y minimizar el impacto en sus clientes y operaciones.

Expectativas de los Clientes ante un Incidente

En situaciones de crisis o fallas, los clientes de una organización tienen ciertas expectativas mínimas que deben ser atendidas para no afectar la confianza ni la percepción de la marca. Entre los aspectos que los clientes no están dispuestos a tolerar se encuentran:

01 **Interrupciones Prolongadas**
Cualquier interrupción que se extienda más allá de lo esperado puede generar insatisfacción y pérdida de clientes.

02 **Tiempos de Respuesta y Reanudación Lentos**
Los usuarios esperan que los problemas se resuelvan de manera ágil y que la reanudación del servicio sea rápida y eficiente.

03 **Procesos poco Flexibles, Burocráticos e Ineficaces**
En momentos de crisis, los clientes esperan que la organización tenga la capacidad de adaptarse rápidamente y ofrecer soluciones, evitando largos procesos burocráticos.

04 **Explicaciones Técnicas Incomprensibles**
Frases como "tuvimos una falla en..." suelen frustrar a los clientes, que en realidad buscan una solución concreta más que una explicación técnica detallada.

05 **Mensajes de Retorno Genéricos o Imprecisos**
Mensajes como "Lo sentimos, regrese más tarde..." no son aceptables para los usuarios, quienes esperan ser atendidos de manera personalizada y recibir información clara sobre el estado de su solicitud o servicio.

Desde la perspectiva de las partes interesadas, el servicio que ofrece una organización debe cumplir con ciertos criterios de calidad para garantizar la confianza y satisfacción de los usuarios, clientes y socios. Las expectativas clave incluyen:

01 **Consistencia y Confiabilidad**
Las partes interesadas esperan que la empresa sea capaz de operar de manera consistente, manteniendo la calidad del servicio y cumpliendo con los compromisos establecidos. Esto tiene un impacto directo tanto en la imagen pública de la organización como en su cumplimiento de regulaciones. Un servicio que presente interrupciones frecuentes o inconsistencias puede afectar negativamente la percepción del cliente y derivar en sanciones regulatorias.

02 **Facilidad de Contacto**
La disponibilidad es fundamental. Los clientes y otras partes interesadas esperan que sea sencillo comunicarse con la empresa, ya sea para resolver dudas, reportar problemas o realizar solicitudes. Un sistema de atención ágil y accesible refuerza la percepción de compromiso y disposición de la organización para atender las necesidades de sus usuarios.

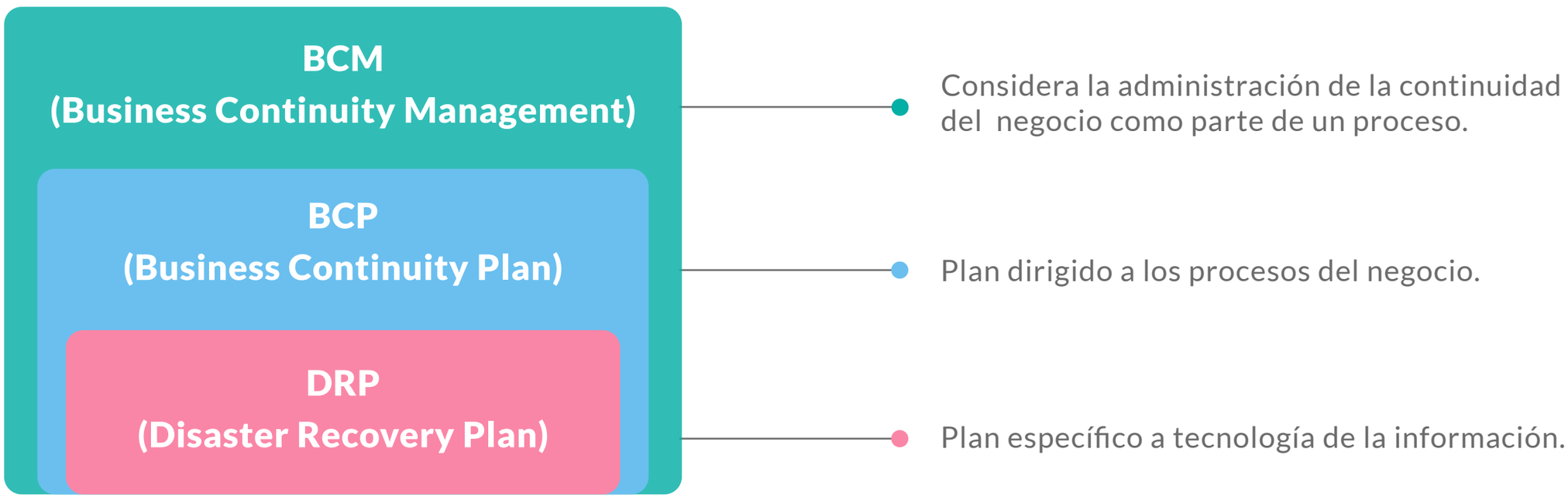
03 **Capacidad de Respuesta**
La prontitud en la atención a las solicitudes o incidentes es otro factor clave. Las partes interesadas valoran una empresa que pueda reaccionar de manera rápida y eficiente frente a problemas o consultas. Un tiempo de respuesta corto no solo mejora la experiencia del cliente, sino que también contribuye a mantener la continuidad operativa y la confianza en el servicio.

04 **Seguridad**
Las partes interesadas demandan seguridad en todas las interacciones con la empresa, esperando que sus datos y operaciones estén protegidos frente a cualquier amenaza física, económica o de integridad. Esto incluye la protección contra ciberataques, fraudes y otros riesgos financieros que puedan comprometer tanto los activos de la empresa como la información personal o sensible de los clientes.

05 **Evidencias Concretas de un Buen Servicio**
Finalmente, los usuarios y reguladores esperan que la empresa proporcione pruebas tangibles de que el servicio ofrecido cumple con los estándares de calidad. Esto incluye informes de auditoría, certificaciones y otras formas de demostrar que la empresa está operando conforme a los marcos legales y regulatorios vigentes. La transparencia y rendimiento de cuentas son esenciales para mantener la confianza de las partes interesadas.

1.2 COMPONENTES DE CONTINUIDAD DEL NEGOCIO

Aunque existen diferentes nomenclaturas y diferentes formas de enfrentar la continuidad del negocio, desde la perspectiva de la ciberseguridad destacan tres componentes principales: BCM, BCP y DRP



Disaster Recovery Plan (DRP)

El Plan de Recuperación ante Desastres se enfoca específicamente en la recuperación de los sistemas tecnológicos y la infraestructura de Tecnologías de la Información después de un incidente. Su propósito principal es garantizar que los activos tecnológicos clave vuelvan a estar operativos lo más pronto posible, permitiendo que los sistemas críticos funcionen y se recupere la información esencial. Frecuentemente, el DRP se percibe simplemente como un sitio alterno donde se puede restaurar la infraestructura de TI en caso de que la ubicación principal quede inoperativa.

Los elementos que abarca este plan son:

- **Datos:** Garantiza la restauración y protección de la información empresarial crítica.
- **Servicios:** Rehabilitar los servicios esenciales de TI que sustentan las operaciones del negocio.
- **Aplicaciones:** Asegurar que las aplicaciones clave funcionen de nuevo tras un incidente.
- **Sistema Operativo:** Reinstalar y restablecer los sistemas operativos necesarios para que la infraestructura tecnológica funcione.

Business Continuity Plan (BCP)

El Plan de Continuidad de Negocio abarca un espectro más amplio, ya que está diseñado para recuperar todas las funciones críticas de la empresa, no solo las relacionadas con la tecnología. El BCP asegura que, tras un incidente, la organización pueda seguir operando o reanudar sus actividades en el menor tiempo posible.

Los elementos habituales de este plan son:

- **DRP:** El plan de recuperación de TI es una parte integral del BCP.
- **Comités:** Equipos dedicados a coordinar las actividades de recuperación y continuidad.
- **Plan de Emergencia:** Instrucciones claras para actuar ante diversos tipos de emergencias.
- **Notificaciones:** Mecanismos para comunicar la situación a todas las partes interesadas.
- **Sitios Alternos de Trabajo:** Ubicaciones físicas o virtuales donde el personal puede continuar trabajando si las instalaciones principales están inhabilitadas.

Business Continuity Management (BCM)

El Gestión de la Continuidad del Negocio es un programa continuo y estratégico que abarca todas las funciones críticas de la empresa, orientado a asegurar la resiliencia organizacional frente a todo tipo de amenazas. A diferencia del BCP, que es un plan con acciones concretas para ejecutar tras un incidente, el BCM es un enfoque más amplio que se centra en la cultura organizacional, el aprendizaje continuo y la mejora de los planes de continuidad. El BCM tiene un enfoque a largo plazo y pretende crear un marco organizacional que no solo permita la recuperación tras un evento crítico, sino que también fortalezca la capacidad de la empresa para resistir, adaptarse y prosperar en un entorno en constante cambio.

Sus aspectos clave incluyen:

- **Cultura de Continuidad de Negocio:** Fomentar una mentalidad dentro de la organización que priorice la preparación para incidentes.
- **Concientización:** Educación y sensibilización constante de los empleados sobre la importancia de la continuidad operativa.
- **Actualización de Cambios:** Incorporar continuamente los cambios en el entorno empresarial, tecnológico o regulatorio en los planes
- **Pruebas y Mejoras:** Realizar pruebas regulares del plan de continuidad para identificar áreas de mejora y asegurar que la organización esté preparada para enfrentarse a posibles incidentes.

Capítulo 2

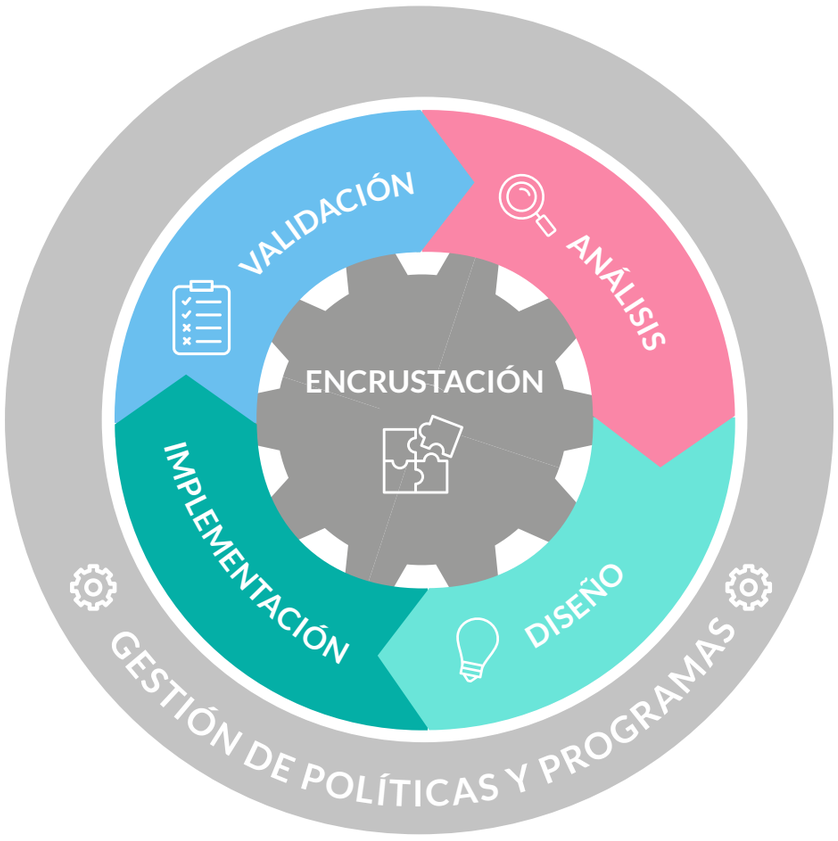
CICLO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

2. CICLO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

El ciclo de gestión de continuidad del negocio se estructura en una serie de fases que permiten a las organizaciones planificar, implementar, mantener y mejorar continuamente su capacidad de respuesta ante interrupciones.

Este ciclo está basado en seis prácticas profesionales, cada una de las cuales cubre un aspecto fundamental del proceso .

BCI. Business Continuity Institute. (2018). Good Practice Guidelines. Berkshire, UK.



2.1 POLITICA Y GESTIÓN DEL PROGRAMA

El establecimiento de la política de continuidad del negocio es el primer paso en el ciclo de BCM. Esta política define el propósito, el contexto, el alcance y la gobernanza del programa de continuidad del negocio. La gestión del programa, por su parte, implica un ciclo continuo de actividades diseñadas para implementar esta política y asegurar que esté alineada con los objetivos estratégicos de la organización.

Elementos clave de esta fase:

- **Definir el Propósito:**
  ¿Qué busca la organización con su programa de continuidad del negocio?
  En esta etapa se clarifica cómo el programa apoyará la capacidad de la organización para responder a interrupciones.

- **Establecer el Alcance:**
  Se identifican los productos, servicios, y procesos críticos que estarán incluidos dentro del programa.

- **Establecer Gobernanza:**
  Se designan roles y responsabilidades claras, asegurando que la alta dirección participe activamente en la supervisión y apoyo del programa.

2.2 INTEGRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

La integración de la continuidad del negocio en la cultura de la organización es esencial para su éxito a largo plazo. No basta con desarrollar planes de continuidad, es crucial que estos sean conocidos y comprendidos por todos los miembros de la organización, desde la alta gerencia hasta el personal operativo.

Estrategias para la integración:

- **Comunicación Eficaz:**
  Establecer canales de comunicación claros y efectivos para que todos los empleados sepan qué hacer en caso de una interrupción.

- **Capacitación Regular:**
  Realizar entrenamientos y simulacros para asegurar que el personal esté preparado para reaccionar de acuerdo con los planes de continuidad.

- **Colaboración Interdisciplinaria:**
  Involucrar a diferentes áreas de la organización, como la gestión de riesgos, recursos humanos, TI, y seguridad, en la implementación y mejora continua de los planes de continuidad.

2.3 ANÁLISIS

El análisis dentro del ciclo de BCM implica la identificación de las necesidades de continuidad del negocio a través del análisis de impacto en el negocio (BIA) y la evaluación de riesgos. El BIA es un proceso crítico que permite a la organización priorizar sus actividades según su importancia estratégica, identificando el impacto que una interrupción tendría en cada una de ellas.

Tipos de análisis realizados:

- **Análisis de Impacto Inicial:**
  Ofrece una visión general de alto nivel sobre cómo las interrupciones afectarían las operaciones.

- **Análisis de Productos y Servicios:**
  Este análisis clasifica los productos y servicios según su importancia y el impacto de su interrupción.

- **Análisis de Procesos:**
  Profundiza en los procesos operativos que respaldan los productos y servicios críticos.

- **Análisis de Actividades:**
  Evalúa las actividades específicas necesarias para mantener o restaurar los productos y servicios críticos.

- Evaluación de Riesgos:
  Este proceso analiza las amenazas que podrían interrumpir las operaciones comerciales.
  Estas amenazas pueden ser internas (fallos técnicos, errores humanos) o externas (desastres naturales, ciberataques). Al identificar los riesgos más relevantes, la organización puede priorizar la implementación de soluciones de mitigación adecuadas.

2.4 DISEÑO

El diseño de soluciones de continuidad es la siguiente fase en el ciclo de BCM. Con base en los resultados del análisis de impacto y la evaluación de riesgos, se diseñan estrategias que permitan a la organización mantener o restaurar sus actividades prioritarias en caso de un incidente. Esta fase involucra la creación de medidas de mitigación de riesgos y la planificación de soluciones de recuperación.

Principios del diseño de soluciones:

- **Coste-beneficio:**
  Las soluciones de continuidad deben equilibrar el coste y la capacidad de respuesta.

- **Colaboración Interdisciplinaria:**
  Involucrar a expertos en riesgos, seguridad física, y seguridad de la información para diseñar soluciones integrales.

- **Escalabilidad:**
  Las soluciones deben ser escalables, es decir, adaptables tanto a incidentes menores como a desastres mayores.

2.5 IMPLEMENTACIÓN

La implementación de las soluciones diseñadas implica la creación de los planes de continuidad del negocio (BCP) y la estructura de respuesta que se activará durante un incidente.

Los BCP pueden incluir:

- **Plan Estratégico:**
  Define cómo se gestionarán las cuestiones estratégicas derivadas de un incidente.

- **Plan táctico:**
  Coordina la respuesta al incidente para garantizar la continuidad de las actividades prioritarias.

- **Plan Operativo:**
  Establece las acciones específicas que deben tomar los departamentos afectados.

2.6 VALIDACIÓN

La validación es la fase final del ciclo de BCM, donde se prueba y revisa la efectividad de los planes de continuidad implementados. Esta fase incluye ejercicios de simulación, mantenimiento y revisión continua de los planes para garantizar que estén actualizados y preparados para responder a incidentes.

Tipos de validación:

- **Ejercicios:**
  Simulaciones diseñadas para probar la capacidad de la organización para responder a incidentes.

- **Mantenimiento:**
  Garantizar que los planes estén actualizados y reflejen los cambios en la organización.

- **Revisión:**
  Evaluar la idoneidad y efectividad del programa de continuidad del negocio y su alineación con los objetivos de la organización.

Capítulo 3

MARCO NORMATIVO: ISO 22301 E ISO 22313

3. MARCO NORMATIVO: ISO 22301 E ISO 22313

Los estándares internacionales ISO 22301 e ISO 22313 son fundamentales para la gestión de continuidad del negocio. Proporcionan un marco que las organizaciones pueden utilizar para establecer, implementar, mantener y mejorar su capacidad de responder a incidentes disruptivos.

3.1 ISO 22301:2013 - REQUISITOS DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO (SGCN)

Este estándar establece los requisitos mínimos para implementar un SGCN. Cubre todos los aspectos, desde el análisis de impacto hasta la implementación y validación de los planes de continuidad. ISO 22301 también especifica que el SGCN debe estar alineado con los objetivos estratégicos de la organización, garantizando que el programa de continuidad sea eficaz y esté adecuadamente respaldado por la alta dirección.

ISO 22301:2013. Gestión de Continuidad del Negocio - Requisitos. Ginebra: Organización Internacional de Normalización.

3.2. ISO 22313:2019 – DIRECTRICES PARA LA IMPLEMENTACIÓN

ISO 22313 proporciona orientación detallada sobre cómo cumplir los requisitos de ISO 22301. Incluye ejemplos de buenas prácticas para implementar un SGCN eficaz y estrategias para mantenerlo a lo largo del tiempo. Este estándar también destaca la importancia de involucrar a todas las áreas de la organización en el proceso de continuidad (ISO 22313, 2019).

ISO 22313:2019. Orientación para la Gestión de Continuidad del Negocio. Ginebra: Organización Internacional de Normalización.

Capítulo 4

PLANIFICACIÓN Y ESTRUCTURA DE LOS PLANES DE CONTINUIDAD

4. MARCO, PLANIFICACIÓN Y ESTRUCTURA DE PLANES DE CONTINUIDAD

La planificación efectiva de la continuidad del negocio se basa en la creación de una serie de planes estructurados, que permiten a la organización gestionar diferentes tipos de interrupciones o desastres de manera proactiva y eficiente. Estos planes de continuidad del negocio (BCPno son documentos únicos, sino un conjunto de planes interconectados que cubren distintos niveles de respuesta ante incidentes, desde lo estratégico hasta lo operativo.

4.1 TIPOS DE PLANES DE CONTINUIDAD DEL NEGOCIO

Dependiendo de la magnitud del incidente y las áreas afectadas dentro de la organización, los BCP se dividen en tres categoríaías principales:

4.1.1. Plan Estratégico

El Plan Estratégico está diseñado para la alta dirección y aborda cuestiones de mayor alcance y de toma de decisiones críticas a nivel organizacional. Este plan responde a preguntas como:

- **¿Cuáles son las decisiones clave que deben tomarse en caso de un incidente mayor?**
- **¿Qué líneas de comunicación deben establecerse con las partes interesadas externas, como accionistas, clientes y reguladores?**
- **¿Cómo debe gestionarse la reputación de la empresa durante y después de una interrupción significativa?**

El plan estratégico se activa principalmente cuando la continuidad de la empresa está en riesgo debido a un incidente que impacta sus operaciones esenciales o su imagen pública. Este plan abarca cuestiones como la comunicación con los medios, la gestión de relaciones con inversores y accionistas, y la asignación de recursos financieros para la recuperación.

Ejemplo Práctico:

En una gran corporación internacional, una brecha de seguridad cibernética que compromete datos sensibles de clientes podría activar el plan estratégico. La alta dirección debe decidir si comunicar la situación públicamente de inmediato o esperar a que se complete una evaluación interna. Las decisiones tomadas en esta fase pueden influir significativamente en la reputación de la organización y la confianza de los clientes.

4.1.2. Plan Táctico

El Plan Táctico se centra en la coordinación operativa necesaria para gestionar la interrupción. Está dirigido a los líderes de departamentos clave que deben trabajar de manera conjunta para restablecer las funciones críticas del negocio en un tiempo razonable. A través de este plan, se determinan los recursos necesarios y se coordina la respuesta para garantizar la continuidad de las actividades más prioritarias.

Las principales tareas dentro del plan táctico incluyen:

- **Asignación de responsabilidades para cada área funcional (TI, operaciones, finanzas, recursos humanos, etc.)**
- **Coordinación de los equipos de respuesta de cada departamento para asegurar que trabajen juntos de manera eficiente.**
- **Implementación de las soluciones diseñadas en la fase previa, como la activación de centros de recuperación o la restauración de sistemas informáticos críticos.**

Ejemplo Práctico:

Si una empresa de manufactura sufre un incendio que destruye una de sus plantas de producción, el plan táctico se activaría para organizar una reubicación temporal de la producción, identificar a los proveedores que pueden ofrecer equipos y materiales alternativos, y coordinar el transporte de mercancías desde otras ubicaciones.

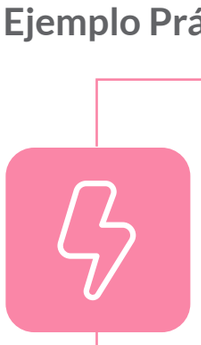
4.1.3. Plan Operativo

El Plan Operativoes más específico y detallado, centrado en la respuesta de los departamentos y equipos directamente involucrados en la gestión del incidente. Este plan determina las acciones exactas que debe tomar cada área operativa para mitigar el impacto del incidente y restaurar las funciones críticas. Por ejemplo:

- **El equipo de TI implementa medidas de recuperación de desastres, como la restauración de sistemas a partir de copias de seguridad.**
- **El departamento de logística reorganiza las rutas de distribución si una sede ha quedado inoperativa.**
- **El equipo de recursos humanos gestiona la reubicación temporal del personal y asegura el bienestar de los empleados afectados por el incidente.**

Este tipo de plan se enfoca en resolver problemas operativos específicos, garantizando que cada departamento cumpla con su rol dentro del esfuerzo de recuperación general.

Ejemplo Práctico:



Si una tormenta afecta una central de datos, el plan operativo del departamento de TI se activaría para restaurar el acceso a los servidores de respaldo y asegurar que las aplicaciones críticas vuelvan a estar en funcionamiento dentro de los tiempos establecidos por el análisis de impacto en el negocio (BIA).

4.2. ESTRUCTURA DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO

Cada uno de estos tipos de planes tiene una estructura básica que guía su implementación de manera ordenada. A continuación, se describen los componentes principales de un BCP:

4.2.1. Definición de Roles y Responsabilidades

Uno de los aspectos más importantes de cualquier plan de continuidad es definir claramente los roles y las responsabilidades de cada miembro del equipo de respuesta. Durante un incidente, no puede haber confusión sobre quién toma decisiones clave o quién está a cargo de ejecutar acciones específicas.

Roles clave incluyen:

- **Gerente de Continuidad del Negocio: Responsable de activar y coordinar el plan general.**
- **Gerente de Crisis: Encargado de tomar decisiones críticas en situaciones de crisis, como la activación de sitios de recuperación.**
- **Responsables de Áreas Específicas: Como el jefe de TI, encargado de la recuperación de sistemas, o el jefe de logística, encargado de reanudar las operaciones de distribución.**

La planificaciónón también debe contemplar reemplazos para cada rol clave, garantizando que las responsabilidades se mantengan aun cuando ciertos individuos no estén disponibles.

A.17.4 Plan de Continuidad de Negocio (2020). Documento interno.

4.2.2. Activación y Desactivación del Plan

Cada plan de continuidad debe incluir criterios claros para su activación y desactivación. Estos criterios se basan en la evaluación del impacto del incidente en la operación y el tiempo estimado de interrupción. La activación del plan generalmente es responsabilidad del gerente de continuidad del negocio o del gerente de crisis.

Una vez que las condiciones se hayan estabilizado y las funciones críticas se hayan restaurado, se puede proceder con la desactivación del plan. Sin embargo, esta decisión solo debe tomarse después de una evaluación exhaustiva que asegure que las operaciones pueden continuar sin riesgo de nuevas interrupciones (ISO 22313, 2019).

4.2.3. Comunicación durante la Crisis

La comunicación es uno de los pilares fundamentales de una respuesta efectiva ante incidentes. Un plan de continuidad bien estructurado debe incluir:

- **Canales de comunicación designados para uso durante la crisis (teléfonos, correos, sistemas de mensajería de emergencia).**
- **Procedimientos para informar a los empleados, partes interesadas, clientes y proveedores.**
- **Líneas claras de reporte para evitar la sobrecarga de información y asegurar que los mensajes críticos lleguen a las personas adecuadas en el momento oportuno.**

En las situaciones de crisis, se suele establecer un Gabinete de Crisis, responsable de centralizar y coordinar las comunicaciones.
Este gabinete se encarga de informar a las partes interesadas internas y externas, incluyendo a los medios de comunicación, sobre la situacion y las acciones que la organizacion esta tomando para mitigar el impacto del incidente.

A.17.3 Estrategia de Continuidad de Negocio (2020). Documento interno.

4.2.4. Recursos Necesarios

La planificación de la continuidad del negocio debe contemplar una lista detallada de los recursos necesarios para la recuperación.

Estos recursos incluyen:

- **Recursos humanos: Personal clave para la implementación del plan y su recuperación.**
- **Tecnología: Sistemas de TI críticos, equipos de respaldo y acceso a centros de datos alternativos.**
- **Instalaciones: Ubicaciones alternativas donde se puedan reanudar las operaciones si las instalaciones principales quedan inutilizadas.**
- **Finanzas: Fondos necesarios para cubrir gastos inesperados durante la crisis, como la adquisición de nuevos equipos o la contratación de servicios de recuperación especializados** *(ISO 22313, 2019).*

4.2.5. Plan de Recuperación ante Desastres

Un componente esencial del BCP es el plan de recuperación ante desastres (DRP, por sus siglas en inglés), especialmente para áreas críticas como TI y comunicaciones. Este plan describe las medidas necesarias para restaurar los sistemas y datos en caso de una interrupción severa.

Los DRP deben incluir:

- **Procedimientos para la recuperación de datos mediante copias de seguridad.**
- **Configuraciones de sistemas redundantes que permitan el acceso continuo a datos críticos.**
- **Escenarios de restauración para diversas situaciones, como fallos del servidor o pérdida de datos.**

Ejemplo Práctico:

Si una empresa de servicios financieros experimenta una interrupción en sus servidores debido a un ataque cibernético, el DRP asegurará que las transacciones financieras puedan continuar a través de servidores de respaldo y que los datos se restauren desde copias de seguridad sin pérdida de información.

5. CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

Para que el auditor interno pueda aprovechar al máximo esta publicación, es conveniente que se refiera a los instrumentos complementarios: Las preguntas de auditoría temáticas y el modelo de madurez general. Cada GASIC se compone de tres componentes:

Guía de Auditoría de la Seguridad de la Información y Ciberseguridad (GASIC):
Este es el cuerpo teórico y consiste en el marco contextual necesario para que el auditor interno comprenda el alcance y del dominio de seguridad que está evaluando. Es un instrumento con los conceptos fundamentales recopilados de mejores prácticas.

Modelo de Madurez:
Recopila controles desde las mejores prácticas asociadas al tema central de Guía de Auditoría, organiza los controles en una propuesta de madurez y permite al auditor conocer los requisitos que debería evaluar.

Ejemplos de Preguntas de Auditoría:
Complementa el modelo de madurez a través de una serie de preguntas organizadas en varios documentos. Cada documento representa un control que pertenece a uno de los ejes temáticos definidos al interior de la Guía de Auditoría.

La ilustración a continuación presenta esta estructura documental:

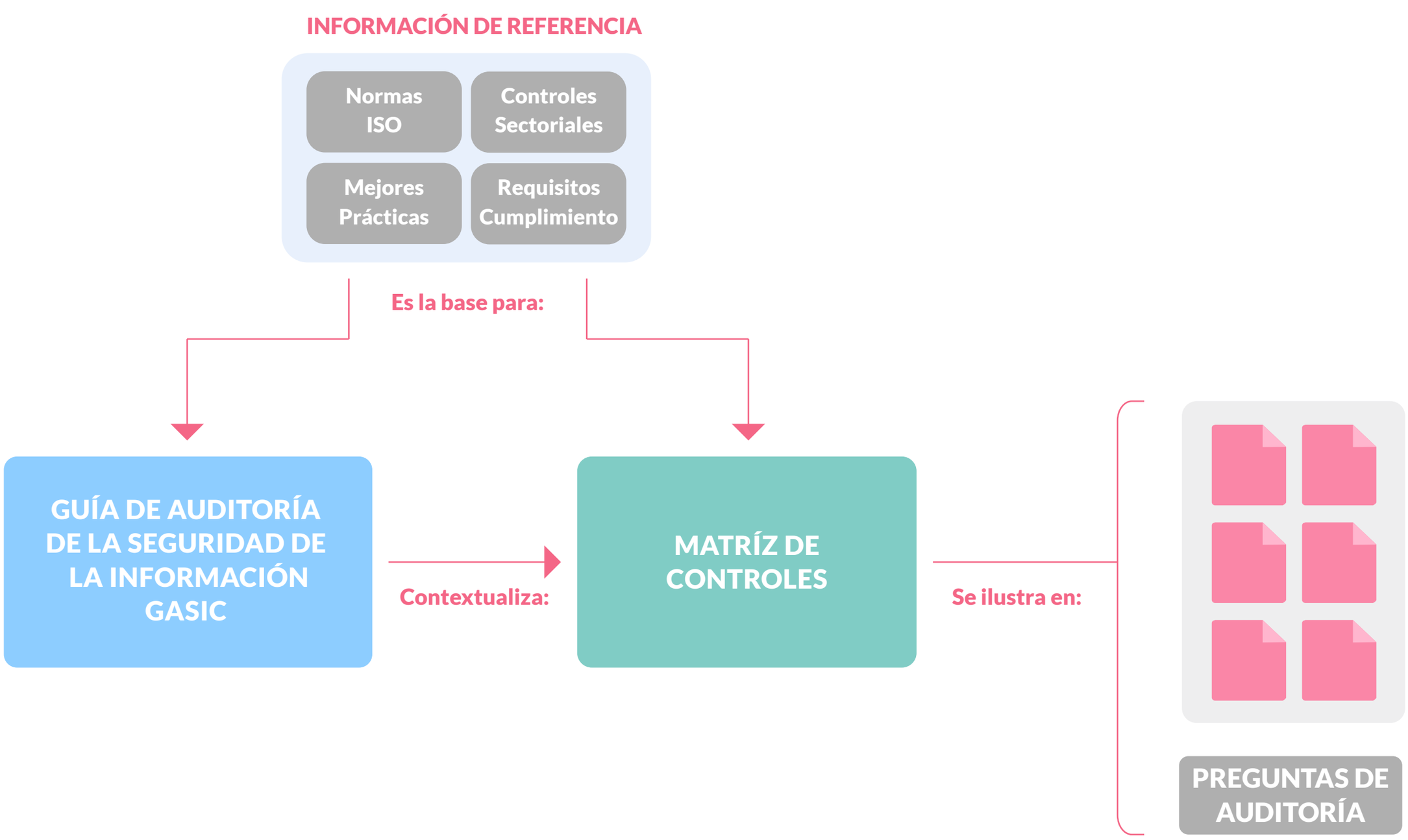


Figura 4. Modo de uso y Estructura Documental GASIC.

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría y su contexto para tener plena comprensión del tema a trabajar.**

02 **A continuación, puede utilizar el Modelo de Madurez para seleccionar los controles que sean apropiados para la organización. La selección de controles debe estar alineados con:**

- **a. La estrategia de la organización.**
- **b. Los resultados de la evaluación de riesgos.**
- **c. Los requisitos de cumplimiento.**
- **d. La estrategia de auditoría interna, expresada en el plan.**

03 **Por último, puede utilizar los documentos de ejemplo para la planificación de las preguntas y pruebas que fuese a realizar. El formato del programa, plan, instrumentos, pruebas y reportería debe ser aquel solicitado en el contexto de cada auditoría, que está fuera del alcance de esta guía.**