

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Políticas de Continuidad**

**Competencias Básicas del Auditor**

1. **Conocimiento en Continuidad del Negocio:** Un auditor debe tener un sólido conocimiento de los principios y prácticas de la continuidad del negocio, incluyendo estándares internacionales como ISO 22301. Comprender los conceptos clave y las mejores prácticas es esencial para evaluar la implementación de controles.
2. **Habilidades Técnicas en Auditoría:** Experiencia en técnicas de auditoría, incluyendo la capacidad de realizar revisiones documentales, entrevistas y evaluaciones en el terreno. Esto implica habilidades para analizar procedimientos, políticas y registros relacionados con la continuidad del negocio.
3. **Conocimiento de Normativas y Regulaciones:** Familiaridad con las normativas y regulaciones específicas del sector y geográficas que puedan afectar a la organización. Esto es crucial para evaluar el cumplimiento de los controles en el marco legal aplicable.
4. **Habilidades Analíticas:** Habilidades analíticas sólidas para evaluar la efectividad de los controles y entender las interconexiones dentro del sistema de gestión de continuidad del negocio.
5. **Conocimientos en Tecnología de la Información:** Dado que muchos controles de continuidad del negocio involucran sistemas de tecnología de la información, es útil que un auditor tenga conocimientos básicos en esta área para evaluar la seguridad y la resiliencia de los sistemas.

# Visión General

Estos controles específicos para la gestión de la continuidad del negocio abarcan diversos aspectos cruciales, se destaca la importancia de establecer objetivos mínimos y delimitar el alcance de la resiliencia del negocio, proporcionando una base clara para las estrategias de contingencia. La planificación de contingencias se aborda de manera integral, detallando funciones, responsabilidades, alcance aplicable a distintas plataformas y funciones organizativas, así como necesidades de recursos, requisitos de capacitación, cronograma de ejercicios y pruebas, programación de mantenimiento y frecuencia mínima de copias de seguridad.

La política de continuidad del negocio se expande para incluir la especificación del alcance y los límites de la continuidad del negocio, identificación de autoridades y delegaciones necesarias, así como referencias a normas y regulaciones pertinentes. En términos generales, se insita a que la política sea una declaración clara de la intención de la alta dirección, adaptada a la organización en términos de tamaño, naturaleza y complejidad, y reflejando su cultura, interdependencias y entorno operativo. Se subraya un compromiso explícito con el cumplimiento de requisitos aplicables, incluyendo obligaciones legales y reglamentarias, y se fomenta la mejora continua del Sistema de Gestión de Continuidad del Negocio (SGCN).

Además, se destaca la necesidad de que la política sea accesible, comprensible y aplicable dentro de la organización, y esté disponible para las partes interesadas según lo apruebe la dirección. Se establecen disposiciones específicas para aprobar la política, conservar información documentada sobre ella y revisarla periódicamente, reconociendo que la idoneidad de estas disposiciones dependerá del tamaño, complejidad, naturaleza y alcance de la organización.

**1.1 Sistema de Gestión de Continuidad del Negocio (SGCN)**

El Sistema de Gestión de Continuidad del Negocio (SGCN) desempeña un papel integral en la aplicación de los controles detallados en el modelo de madurez para la gestión efectiva de la continuidad del negocio en la organización. Este sistema proporciona el marco esencial para definir y documentar los objetivos mínimos y el alcance de la resiliencia del negocio, asegurando una alineación estratégica con los objetivos organizativos. En el ámbito de la planificación de contingencias, el SGCN facilita la elaboración de planes detallados al establecer funciones y responsabilidades, definir alcances aplicables y programar ejercicios y pruebas.

Un SGCN contribuye a la formulación y gestión de la política de continuidad del negocio, asegurando que sea coherente con la dirección estratégica, apropiada para el tamaño y la complejidad de la organización, y que cumpla con requisitos legales y reglamentarios. También garantiza la aplicación efectiva de la política al facilitar su disponibilidad, comprensión y aplicación dentro de la organización.

**1.2 Planificación de Contingencias**

La Planificación de Contingencias desempeña un papel fundamental en la gestión de la continuidad del negocio, establece una estructura organizativa y asigna responsabilidades claras durante situaciones de crisis. Al definir objetivos generales específicos para enfrentar interrupciones, la planificación de contingencias asegura que la organización pueda mantener operaciones esenciales. Además, los controles presentados en el modelo de madurez abordan elementos clave de la política de continuidad del negocio, incluyendo funciones y responsabilidades, alcance organizacional, necesidades de recursos, requisitos de capacitación, calendario de ejercicios y pruebas, planificación de mantenimiento, y la frecuencia mínima de copias de seguridad.

La programación de ejercicios y pruebas periódicos permite evaluar la efectividad de los planes y garantizar que el personal esté preparado. Asimismo, el establecimiento de un cronograma de mantenimiento y una frecuencia mínima de copias de seguridad contribuye a la prevención y recuperación de interrupciones, asegurando la integridad y disponibilidad de datos cruciales.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Definir y documentar los objetivos de política mínimos acordados y el alcance de la resiliencia del negocio. 2. Definir los objetivos generales de contingencia de la organización y establecer el marco organizacional y responsabilidades para la planificación de contingencias del sistema. Los elementos clave de la política son los siguientes:  2.1 Funciones y responsabilidades.  2.2 Alcance aplicable a tipos de plataformas comunes y funciones de organización (es decir, telecomunicaciones, legales, relaciones con los medios) sujetos a planificación de contingencias.  2.3 Necesidades de recursos.  2.4 Requisitos de capacitación.  2.5 Calendario de ejercicios y pruebas.  2.6 Planificar el cronograma de mantenimiento.  2.7 Frecuencia mínima de copias de seguridad y almacenamiento de medios de copia de seguridad 3. Incluir dentro de la política de continuidad del negocio:  3.1 Especificar el campo de aplicación y los límites de la continuidad del negocio de la organización, incluidas las limitaciones y las exclusiones.  3.2 Identificar todas las autoridades y delegaciones necesarias, incluidas las personas responsables del SGCN de la organización.  3.3 Incluir referencias a las normas, las directrices, las normativas o las políticas que el SGCN debería tener en cuenta o cumplir. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir la política de continuidad del negocio en términos de objetivos y obligaciones de la organización, así como asegurarse de que:   1.1 Sea una declaración general y concisa de la intención de la alta dirección y de la orientación del SGCN.   1.2 Sea apropiada para el propósito de la organización (en función de su tamaño, naturaleza y complejidad, así como para reflejar su cultura, interdependencias y entorno operativo).   1.3 Proporcione un marco para fijar los objetivos.   1.4 Incluya un compromiso claro con el cumplimiento de los requisitos aplicables, incluidas las obligaciones legales y reglamentarias.   1.5 Incluya un compromiso con la mejora continua del SGCN.  2. Asegurarse de que la política de continuidad del negocio cumpla con:   2.1 Estar disponible y mantenerse como información documentada.   2.2 Comunicase, entenderse y aplicarse en el seno de la organización.   2.3 Ponerse a disposición de las partes interesadas según lo apruebe la dirección. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Incluir disposiciones adecuadas para aprobar la política, conservar la información documentada sobre ella y revisarla periódicamente cuando se produzcan cambios significativos en los factores internos o externos. La idoneidad de estas disposiciones dependerá del tamaño, la complejidad, la naturaleza y la extensión de la organización.  2. A medida que el plan de continuidad del negocio evolucione, esta política deberá revisarse de forma periódica y actualizarse siempre que proceda. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. |  |

1. **Preguntas de auditoría para las Políticas de Continuidad**

|  |
| --- |
| Temática: Objetivos y obligaciones de la política |
| Los objetivos y obligaciones de la política de continuidad del negocio es esencial para garantizar la efectividad y el alineamiento estratégico del Sistema de Gestión de Continuidad del Negocio (SGCN) con los objetivos organizacionales. Al evaluar la claridad de la declaración de intenciones y la orientación proporcionada por la política, así como su adaptación al propósito y contexto específico de la organización, se asegura que la alta dirección haya comunicado de manera efectiva su compromiso con la resiliencia del negocio. La identificación y revisión de los objetivos específicos, así como el compromiso con el cumplimiento de requisitos legales y normativos, son cruciales para asegurar la robustez y la aplicabilidad de la política. Además, la consideración de la mejora continua y la participación de las partes interesadas garantizan un enfoque dinámico y adaptativo que se ajusta a la evolución de la organización y su entorno operativo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han definido claramente los objetivos de política mínimos acordados para la resiliencia del negocio?   + Revise la documentación de políticas del negocio para identificar y verificar la presencia de objetivos claramente definidos. Esto puede incluir documentos como manuales, procedimientos o políticas formales.   + ¿Los objetivos de política mínimos acordados están alineados con las necesidades y riesgos específicos de la organización? * ¿La política es una declaración general y concisa de la intención de la alta dirección y la orientación del SGCN? * Compare las funciones y responsabilidades definidas con el desempeño real de los roles durante ejercicios anteriores de planificación de contingencia. * ¿La política proporciona un marco claro para fijar los objetivos y refleja la cultura, interdependencias y entorno operativo de la organización? * ¿Se incluye un compromiso claro con el cumplimiento de requisitos aplicables, incluidas obligaciones legales y reglamentarias?   + ¿La política incluye un compromiso con la mejora continua del SGCN? * ¿Cómo se asegura la claridad de la política para que sea entendida por los diferentes niveles de la organización?   + ¿Existen mecanismos de comunicación efectiva para garantizar la comprensión y aplicación de la política? * ¿Cómo la política se adapta al propósito de la organización, considerando su tamaño, naturaleza y complejidad? * ¿Está alineada con la cultura organizacional y refleja las interdependencias y el entorno operativo? * ¿La política incluye disposiciones para la participación de las partes interesadas en el proceso de desarrollo y revisión?   + ¿Se han identificado y considerado adecuadamente las expectativas de las partes interesadas en la política? |

|  |
| --- |
| Temática: Objetivos generales de contingencia, marco organizacional y responsabilidades |
| Los objetivos generales de contingencia, el marco organizacional y las responsabilidades dentro de la política de continuidad del negocio es crucial para asegurar la efectividad y la capacidad de respuesta de la organización frente a eventos disruptivos. Estos aspectos constituyen a la planificación de contingencia, ya que definen claramente los objetivos estratégicos para mantener la continuidad operativa en situaciones adversas, establecen una estructura organizacional que facilita la toma de decisiones y la coordinación eficiente durante crisis, y asignan responsabilidades específicas para la ejecución de planes. Se busca verificar si estos elementos están alineados con los objetivos globales de la organización, si las funciones y responsabilidades están claramente definidas, y si el marco organizacional promueve la colaboración y la gestión efectiva de recursos. Garantizar la solidez y la efectividad de estos componentes es esencial para fortalecer la resiliencia organizacional y minimizar el impacto de eventos imprevistos en la continuidad del negocio  Este levantamiento puede incluir análisis específicos tales como:   * ¿Los objetivos generales de contingencia de la organización están claramente definidos?   + ¿Se ha establecido un marco organizacional para la planificación de contingencias del sistema? * ¿Se ha establecido un marco organizacional que incluye funciones y responsabilidades para la planificación de contingencias? * ¿La documentación aborda de manera adecuada las necesidades de recursos, requisitos de capacitación, calendario de ejercicios y pruebas, y el cronograma de mantenimiento?   + ¿Se han establecido y documentado las frecuencias mínimas para copias de seguridad y almacenamiento de medios de copia de seguridad? * ¿El marco define claramente las funciones y responsabilidades de los diversos equipos o departamentos involucrados en la continuidad del negocio?   + ¿Las funciones y responsabilidades de los equipos de contingencia están claramente definidas en la documentación? * ¿Se han identificado y asignado responsables específicos para la ejecución de planes de contingencia en cada área funcional?   + ¿Existe un plan de comunicación claro para notificar a los responsables y a otros interesados durante una situación de contingencia?   + ¿Se han establecido roles de reemplazo o sucesión para garantizar la continuidad de las responsabilidades clave en caso de indisponibilidad de personal? |

|  |
| --- |
| Temática: Revisión periódica y actualización de la política |
| La revisión periódica y actualización de la política de continuidad del negocio garantiza la eficacia continua del Sistema de Gestión de Continuidad del Negocio (SGCN). Este proceso asegura que la política esté alineada con los cambios en el entorno operativo, la estructura organizativa y la naturaleza del negocio. La revisión periódica permite adaptar la política a nuevas amenazas, tecnologías y regulaciones, asegurando que las medidas de continuidad del negocio sean pertinentes y eficientes. Al abordar lecciones aprendidas de eventos pasados y mantener la conformidad con requisitos regulatorios cambiantes, la auditoría de la revisión periódica y actualización de la política no solo fortalece la resiliencia organizativa, sino también promueve la mejora continua del SGCN para enfrentar los desafíos en constante evolución.  Este levantamiento puede incluir análisis específicos como:   * ¿Existe un proceso establecido para la revisión periódica de la política de continuidad del negocio?   + ¿La política se actualiza cuando sea necesario, especialmente ante cambios significativos en el plan de continuidad del negocio?   + ¿Se ha establecido un calendario específico para la revisión periódica de la política de continuidad del negocio?   + ¿La revisión periódica se realiza de acuerdo con el calendario establecido? * ¿Quién es responsable de llevar a cabo la revisión periódica de la política?   + ¿Durante la revisión periódica, se evalúan los cambios en el entorno operativo y los factores internos y externos relevantes? * ¿Se documentan los cambios realizados durante la actualización de la política? * ¿Existe un proceso formal para la aprobación de las actualizaciones de la política? * ¿Se comunica eficazmente a todas las partes interesadas relevantes sobre las actualizaciones de la política? |