

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Formación y Concientización**

**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

La formación y concientización en continuidad del negocio son fundamentales para integrar esta gestión en la cultura organizacional y garantizar que todos los niveles de la organización comprendan su rol en la preparación y respuesta ante incidentes. Este enfoque fortalece la capacidad de la organización para reaccionar eficazmente frente a disrupciones. Desde una perspectiva de auditoría, es crucial que los programas de formación y concientización sean medibles, estén alineados con los objetivos organizacionales y se ajusten a las necesidades de los distintos roles.

* 1. **Programa de Concientización**

Un programa de concientización debe incluir múltiples iniciativas para fomentar el conocimiento sobre continuidad del negocio. Esto abarca consultas al personal, sesiones informativas, boletines, incorporación de nuevos empleados, publicaciones web, y visitas a ubicaciones alternativas designadas. También se debe incluir la comunicación continua con proveedores para garantizar que comprendan y cumplan los requisitos de continuidad. Desde la perspectiva de auditoría, se debe verificar si estas iniciativas están documentadas y ejecutadas de forma coherente.

* 1. **Integración en la Cultura Organizacional**

La continuidad del negocio debe integrarse en los valores esenciales de la organización, asegurando que todos los niveles, desde la alta dirección hasta los empleados operativos, comprendan su importancia. Esto incluye promover la política de continuidad del negocio y asignar roles claros en los procedimientos. Un auditor evaluará si esta integración se refleja en la documentación organizacional y en la percepción del personal.

* 1. **Evaluación de Competencias y Roles**

El programa de formación debe identificar los conocimientos necesarios para distintos roles relacionados con la continuidad del negocio, desde patrocinadores y directores hasta coordinadores y consultores externos. Este enfoque asegura que cada persona tenga las competencias necesarias para ejecutar sus responsabilidades, como gestión de emergencias, análisis de impacto y recuperación. Un auditor revisará si las competencias requeridas están documentadas y si los programas de formación las abordan adecuadamente.

* 1. **Liderazgo y Compromiso de la Dirección**

La alta dirección debe demostrar liderazgo mediante su participación activa en actividades de continuidad, como incluir el tema en reuniones regulares, asignar recursos adecuados y apoyar la mejora continua del sistema de gestión de continuidad. Desde la perspectiva de auditoría, se verificará si el liderazgo está documentado y si existen evidencias de su implicación en iniciativas de formación y concientización.

* 1. **Frecuencia y Mecanismos de Formación**

Los planes de formación deben detallar la frecuencia de capacitación, los mecanismos de entrega (como ejercicios, simulaciones y formación práctica) y cómo se ajustan a los cambios en el entorno de negocio. La participación en actividades del sector, como conferencias y seminarios, también debe ser parte del programa para mantenerse al día con las tendencias. Un auditor revisará si estas actividades están alineadas con los objetivos organizacionales y si las competencias adquiridas son evaluadas regularmente.

* 1. **Monitoreo y Mejora de Competencias**

La organización debe supervisar las habilidades y competencias adquiridas mediante la evaluación de los resultados de ejercicios y pruebas, utilizando esta información para ajustar y mejorar los programas de formación. Desde una perspectiva de auditoría, se verificará si existe un sistema de monitoreo eficaz y si los cambios implementados reflejan las lecciones aprendidas.

Este enfoque asegura que la organización esté preparada para gestionar la continuidad del negocio de manera efectiva, con un personal capacitado y consciente de su rol en los procedimientos de continuidad. Esto no solo fortalece la resiliencia organizacional, sino que también asegura el cumplimiento con estándares y requisitos regulatorios.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Un programa de toma de conciencia debe incluir:     1.1 Un proceso de consulta al personal de toda la organización respecto a la configuración y la administración de la gestión de la continuidad del negocio.     1.2 La explicación de la continuidad del negocio en los boletines, las sesiones informativas, los programas de introducción o las revistas de la organización (así como la orientación para nuevos empleados).     1.3 La inclusión de la continuidad del negocio en las páginas web pertinentes.     1.4 La inclusión del tema de la gestión de la continuidad del negocio en las reuniones del personal y del equipo de dirección.     1.5 La publicación selectiva de informes sobre los incidentes después de que se produzcan.     1.6 Las sesiones informativas para la alta dirección.     1.7 Las visitas a ubicaciones alternativas designadas (por ejemplo, un sitio de recuperación).     1.8 La comunicación habitual con proveedores para asegurarse de que se entiendan los requisitos de continuidad del negocio de la organización y puedan demostrar su capacidad para cumplir las capacidades de continuidad acordadas. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Crear, promover e integrar la gestión de la continuidad del negocio en la cultura de la organización, de tal forma que:     1.1 Pase a formar parte de los valores esenciales y la gestión de la organización.     1.2 Las partes interesadas tomen conciencia de la política de continuidad del negocio y de su rol en los procedimientos asociados. 2. Evaluar que el programa de concientización exija los distintos grados de conocimientos necesarios para la gestión de continuidad del negocio. Algunos de los roles y los conocimientos que se deben incluir son para:     2.1 El patrocinador del plan de continuidad debe:         2.1.1 Comprender los conceptos del plan de continuidad y la propuesta de valor del plan de continuidad.     2.2 El director del plan de continuidad debe:         2.2.1 Comprender la gestión de emergencias.         2.2.2 Obtener la certificación Certified Business Continuity Professional (CBCP) de DRI International (DRII), Business Continuity Institute (BCI) o equivalente.          2.2.3 Creación de un programa de gestión de continuidad del negocio y/o despliegue de procesos (mejor si está alineado con la metodología de la organización, como la eficiencia operativa, la seguridad y/u otros procesos relacionados).     2.3 Los coordinadores del plan de continuidad deben:         2.3.1 Poseer un sólido conocimiento de la metodología del proceso del plan de continuidad de la organización (normalmente impartido a través de la organización o de formación externa).     2.4 El consultor del plan de continuidad (interno o externo) debe:         2.4.1 Obtener un certificado CBCP o Master Business Continuity Professional (MBCP) de DRII, BCI o equivalente.         2.4.2 Tener amplia experiencia en la realización de lo siguiente Evaluación de riesgos del plan de continuidad , análisis de impacto, planificación de la recuperación, ejercicios, etc.     2.5 El personal de la organización debe:         2.5.1 Comprender los conceptos del plan de continuidad y la propuesta de valor del plan de continuidad.         2.5.2 Comprender los procedimientos de comunicaciones de emergencia.         2.5.3 Conocer las urgencias de su centro o región. 3. La alta dirección y los demás niveles de la dirección deben demostrar liderazgo y compromiso. Esto se puede realizar mediante:     3.1 Implicación operativa mediante grupos de dirección.     3.2 Inclusión de la continuidad del negocio como punto fijo en las reuniones de dirección.     3.3 Otras actividades como:         3.3.1 Comunicando la importancia de la continuidad del negocio y cumpliendo los requisitos del sistema de gestión de continuidad del negocio.         3.3.2 Poniendo a disposición los recursos necesarios, incluidos los niveles de financiación adecuados.         3.3.3 Promocionando la mejora continua.         3.3.4 Proporcionando a los demás niveles de dirección apoyo que les permita demostrar el liderazgo y el compromiso aplicables a sus áreas de responsabilidad.         3.3.5 Integrando los requisitos del sistema de gestión de continuidad del negocio en los procesos de negocio de la organización.         3.3.6 Participando activamente en el programa de ejercicio.         3.3.7 Dirigiendo y apoyando la mejora del sistema de gestión de continuidad del negocio. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Asegurar que los planes de formación consideren la frecuencia de capacitación y los mecanismos de prestación de la formación. 2. Los cambios en el entorno de negocio y en las operaciones afectan al enfoque y al modo en que se planifican, diseñan e implantan las actividades de continuidad del negocio. La organización puede demostrar su toma de conciencia respecto a las tendencias de gestión de la continuidad del negocio, por ejemplo, participando activamente en las actividades del sector relacionadas con esa cuestión, lo que puede incluir:     2.1 Ser miembro de un grupo de interés del sector.     2.2 Ser miembro de un comité organizador de conferencias.     2.3 Presentar ponencias en conferencias y seminarios.     2.4 Asistir a conferencias locales o internacionales de continuidad del negocio. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Desarrollar competencias basadas en formación práctica, incluida la participación en ejercicios y pruebas. |
| 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. Supervisar habilidades y competencias de acuerdo con los resultados de los ejercicios y las pruebas. |

1. **Prácticas de auditoría para la Formación y Concientización**

|  |
| --- |
| Temática: Planificación y estrategia |
| En la fase de la planificación y estrategia de formación y concientización, se examina cómo la organización ha implementado la capacitación, quiénes son responsables de difundir la información, cuáles son las estrategias y planes establecidos, y si se documentan adecuadamente los incidentes.  Este levantamiento puede incluir análisis específicos tales como:   * ¿El plan de continuidad del negocio incluye estrategias claras para abordar las amenazas y los riesgos identificados en la evaluación de riesgos?   + ¿Se publican selectivamente informes sobre los incidentes después de que se produzcan? * ¿Se lleva a cabo un proceso de consulta al personal de toda la organización sobre la configuración y administración de la gestión de la continuidad del negocio?   + ¿La continuidad del negocio se explica en boletines, sesiones informativas, programas de introducción o revistas de la organización, y se proporciona orientación a los nuevos empleados?     - ¿La continuidad del negocio se incluye en las páginas web pertinentes de la organización?   + ¿El tema de la gestión de la continuidad del negocio se aborda en las reuniones del personal y del equipo de dirección?     - Revise agendas y actas de reuniones para identificar la inclusión del tema de continuidad del negocio. * ¿Se han documentado los procedimientos que la organización debe seguir durante un incidente, incluyendo la asignación de responsabilidades? * ¿La gestión de la continuidad del negocio forma parte de los valores esenciales y la gestión de la organización?   + Entreviste a miembros de la alta dirección para confirmar si la continuidad del negocio se considera como un valor esencial y si se integra en la gestión general de la organización. * ¿Existen procedimientos adecuados de comunicación para mantener a las partes interesadas informadas durante una crisis?   + ¿Las partes interesadas están conscientes de la política de continuidad del negocio y de su rol en los procedimientos asociados? * ¿Cómo se garantiza que el plan de continuidad del negocio sea revisado y actualizado regularmente para mantener su relevancia? * ¿Se han implementado iniciativas específicas para promover la integración de la gestión de la continuidad del negocio en la cultura organizacional? * ¿Se ha documentado la política de continuidad del negocio, los procedimientos y los planes?   + ¿Quién tiene acceso a la documentación y los registros, y de qué forma se controla este acceso?   + ¿Cómo se gestionan y mantienen los registros de actividades como pruebas, ejercicios y revisiones?   + ¿Se lleva a cabo una revisión regular de la política para identificar áreas de mejora?   + ¿Existen procesos para actualizar y dar mejora al plan de continuidad del negocio en función de riesgos o cambios organizativos? * ¿El director del plan de continuidad ha obtenido la certificación CBCP de DRII, BCI u equivalente?   + Validar la información de la certificación con los organismos emisores, como DRII o BCI, para garantizar su autenticidad.   + ¿Los coordinadores del plan de continuidad poseen un sólido conocimiento de la metodología del proceso del plan de continuidad de la organización?   + ¿El consultor del plan de continuidad (interno o externo) posee la certificación CBCP o MBCP de DRII, BCI o equivalente? * ¿El personal de la organización conoce las urgencias de su centro o región?   + Verificar la existencia de materiales de capacitación que aborden las urgencias locales y regionales para el personal de la organización. |