

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Pruebas y Ejercicios**

**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.

**1.1 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.

**1.2 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.

**1.3 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.

**1.4 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.

**1.5 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.

**1.6 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.

# Modelo de Madurez

|  |  |  |  |
| --- | --- | --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | | 1. Diseñar un programa de ejercicio que valide la eficacia de sus planes, procedimientos, estrategias y soluciones de continuidad del negocio con el paso del tiempo.  1.1 Definir objetivos para ejercitar y probar los sistemas del negocio, técnicos, logísticos, administrativos, procedimentales y operativos  1.1 Asignar roles y responsabilidades para la ejecución de ejercicios y pruebas del plan de continuidad.  1.1 El programa debe cubrir los planes individuales, las personas, las capacidades y los recursos que contribuyen a los objetivos estratégicos de la organización.  1.3 El campo de aplicación de un programa de ejercicio debe basarse en el tamaño y la naturaleza de la organización que va a llevar a cabo los ejercicios, así como en el campo de aplicación, la funcionalidad, la complejidad y el nivel de madurez de los planes y capacidades que se ejercitan.  1.4 En las fases iniciales de la madurez, los ejercicios y los ensayos deben limitarse al uso de listas de verificación, simulaciones y ejercicios de toma de conciencia.   1.5 A medida que el programa madura, se debe ampliar para incluir ejercicios de simulación teórica y simulacros en directo a escala natural. 2. Asegurar que el programa de ejercicio sea flexible y tenga en cuenta los cambios de la organización y el resultado de ejercicios anteriores.  2.1 El programa de ejercicio debe tener en cuenta los roles de todas las partes, incluidos los proveedores externos y otras personas que cabría esperar que participen en las actividades de recuperación.  2.2 Para asegurarse de que los ejercicios se lleven a cabo de manera eficiente y eficaz dentro de los plazos especificados, el programa de ejercicio debe incluir lo siguiente:  2.2.1 Análisis de necesidades.  2.2.2 Respaldo de la alta dirección.  2.2.3 Objetivos claros.  2.2.4 Extensión, número, tipos, duración, ubicaciones y programaciones de los ejercicios.  2.2.5 Personal apropiado para apoyar el programa.  2.2.6 Recursos y presupuesto necesarios.  2.2.7 Procesos de gestión de la confidencialidad, la seguridad de la información, la salud, la seguridad y otros asuntos semejantes. | |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | | 1. Determinar los procedimientos para el seguimiento, la medición, el análisis y la evaluación del desempeño y la eficacia del SGCN deberían incluir:  1.1 Procedimientos de notificación a utilizar.  1.2 Especificar qué hay que someter a seguimiento y medir.   1.3 Identificar cómo, cuándo y quién debe hacer el seguimiento y la medición.   1.4 Establecer métricas de desempeño que incluyan mediciones cualitativas y cuantitativas que sean apropiadas para la organización y garanticen resultados válidos.  1.5 Registrar los datos y los resultados para facilitar el análisis posterior de las acciones correctoras.  1.6 Examinar las pruebas históricas.  1.7 Hacer el seguimiento de en qué medida se cumplen la política y los objetivos de continuidad del negocio de la organización.  1.8 Medir el cumplimiento del SGCN de los requisitos legales y reglamentarios aplicables.  1.9 Hacer el seguimiento de las no conformidades y de otras pruebas de un desempeño deficiente del SGCN. 2. Incluir dentro de los resultados que indican la eficacia de los planes, procedimientos y capacidades de continuidad del negocio lo siguiente:  2.1 si se ha habilitado una capacidad de gestión de incidentes y ha proporcionado una respuesta eficaz.  2.2 si la comprensión de la organización de sí misma y de sus relaciones con otras organizaciones, con las autoridades reglamentarias o los departamentos de la administración pública pertinentes, con las autoridades locales y con los servicios de emergencia se ha desarrollado y documentado correctamente y se entiende bien.  2.3 si los ejercicios periódicos garantizan que el personal esté formado para responder con eficacia a una disrupción.  2.4 si los requisitos de las partes interesadas se comprenden y se pueden cumplir.  2.5 si el personal recibe apoyo y comunicaciones suficientes durante una disrupción.  2.6 si la reputación de la organización está protegida.  2.7 si se ha demostrado el cumplimiento legal y reglamentario.  2.8 si se mantienen los controles financieros durante todo el incidente.  2.9 si la organización puede demostrar un nivel de resiliencia reforzado a sus clientes y otras partes interesadas.  3. Programar ejercicios y actividades de prueba de acuerdo con lo definido en los planes de continuidad | |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | | 1. Asegurar que el programa, una vez implantado, incluya:  1.1 Ejercitar los aspectos técnicos, logísticos, administrativos, procedimentales y operativos de otro tipo de los procedimientos.  1.2 Ejercitar a todas las personas con responsabilidades en los procedimientos, incluidas las pertenecientes a organizaciones externas.  1.3 Ejercitar las disposiciones y la infraestructura de continuidad del negocio.  1.4 Validar la recuperación de la tecnología y las telecomunicaciones, incluida la disponibilidad y reubicación del personal.  1.5 Ejercitar a los equipos de respuesta en la gestión de los impactos derivados de la disrupción de la cadena de suministro. 2. Hacer el seguimiento y medir la implantación del programa de ejercicio para asegurarse de que se cumplan sus objetivos. | |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | | 1. Generar indicadores del desempeño para evaluar el desempeño, la eficacia y los resultados del SGCN, con el fin de identificar los logros y las áreas que es preciso corregir o mejorar. Los datos obtenidos se pueden usar para identificar los patrones y permitir a la organización obtener información sobre el desempeño del SGCN. 2. Usar los ejercicios y los resultados documentados de estos para asegurarse de la eficacia y preparación de sus planes de continuidad del negocio.  2.1 Los ejercicios deben ser realistas, planificarse con atención y acordarse con las partes pertinentes, para minimizar el riesgo de causar disrupciones en las actividades y de que se produzcan incidentes a consecuencia directa del ejercicio.  2.2 La organización debe diseñar escenarios de ejercicios que satisfagan los objetivos del ejercicio y utilizar amenazas identificadas en la evaluación del riesgo o en la información obtenida en disrupciones anteriores. 3. Retener la información documentada apropiada de todas las evaluaciones periódicas y sus resultados. | |
| 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. Asegurar que existe algún método para rastrear problemas y brechas descubiertas en la prueba y realizar un seguimiento de su resolución.  2. Elaborar un informe posterior al ejercicio y un análisis en el que se tenga en cuenta la consecución de las metas y los objetivos del ejercicio.  2.1 Se debe elaborar un informe posterior al ejercicio que contenga recomendaciones y un calendario para su implantación.  2.2 Las lecciones extraídas de los ejercicios y los incidentes reales experimentados deben volver a examinarse durante ejercicios futuros.  2.3 Los ejercicios que presenten deficiencias o imprecisiones graves en los procedimientos deben repetirse una vez completadas las acciones correctoras.  3. Identificar las debilidades u omisiones en los planes y capacidades y realizar recomendaciones de mejora. Obtener la aprobación de la dirección para cualquier cambio en los planes y aplicarlos a través del proceso de control de cambios de la empresa. | |

1. **Prácticas de auditoría para las Pruebas y Ejercicios**

|  |
| --- |
| Temática: Gestión de las pruebas y ejercicios |
| La gestión de pruebas y ejercicios de continuidad de negocio es un componente crítico de un programa de continuidad. Consiste en el diseño, planificación, ejecución y evaluación de actividades simuladas que tienen como objetivo principal poner a prueba y mejorar la capacidad de una organización para mantener sus operaciones y sistemas operando de manera correcta en situaciones adversas. Estos ejercicios y pruebas ayudan a asegurar que en caso de interrupciones significativas la organización pueda responder de manera eficiente y efectiva minimizando el impacto en sus funciones críticas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un programa de ejercicio diseñado para validar la eficacia de los planes, procedimientos, estrategias y soluciones de continuidad del negocio con el tiempo?   + ¿Se han definido objetivos claros para ejercitar y probar sistemas del negocio, incluyendo aspectos técnicos, logísticos, administrativos, procedimentales y operativos?   + ¿Se han asignado roles y responsabilidades específicas para la ejecución de ejercicios y pruebas del plan de continuidad?   + ¿El programa de ejercicio abarca planes individuales, personas, capacidades y recursos que contribuyen a los objetivos estratégicos de la organización? * ¿Se han establecido análisis de necesidades para garantizar la eficiencia y eficacia de los ejercicios dentro de los plazos especificados?   + ¿Los objetivos de los ejercicios son claros en cuanto a su alcance, número, tipos, duración, ubicaciones y programaciones?   + ¿Se ha especificado claramente qué aspectos deben de ser sometidos a seguimiento y medición?     - ¿Se han identificado los responsables de realizar el seguimiento y la medición, así como los momentos y métodos para llevar a cabo estas actividades?     - ¿Se han establecido métricas de desempeño que incluyan tanto mediciones cualitativas como cuantitativas? * ¿Existe un sistema para registrar datos y resultados que facilite el análisis posterior y la implementación de acciones correctoras?   + ¿Este sistema está protegido y solo es accesible por personal autorizado?   + ¿Se examinan las pruebas históricas para aprender de experiencias pasadas y mejorar continuamente?     - ¿Este análisis incluye una evaluación de la efectividad de las respuestas y soluciones implementadas en situaciones pasadas?     - ¿Existe un proceso formal para asegurar que las lecciones aprendidas se utilicen para mejorar la preparación y respuesta futuras?     - ¿Se actualizan los procedimientos y protocolos en función de las lecciones aprendidas de pruebas históricas? * ¿Se hace seguimiento de la medida en que se cumplen la política y los objetivos de continuidad del negocio de la organización?   + ¿Se realiza seguimiento de no conformidades y otras pruebas de un desempeño deficiente?     - ¿A la hora de encontrar una no conformidad o desempeño deficiente cuales son los pasos a seguir?     - ¿Se tienen constancia de cuando se encuentra un problema de este tipo? * ¿Se ha habilitado una capacidad de gestión de incidentes que proporciona respuestas efectivas durante situaciones de interrupción?   + ¿El personal clave está adecuadamente capacitado y preparado para desempeñar roles durante situaciones de interrupción?   + ¿Existen programas de formación periódica para mantener la competencia del personal en la gestión de incidentes?   + ¿Se realizan simulacros y ejercicios regulares para probar y mejorar la capacidad de gestión de incidentes?     - ¿Estos ejercicios incluyen la participación de todas las partes clave y evalúan la coordinación y comunicación efectivas? |

|  |
| --- |
| Temática: Mejora en base a resultados |
| Se refiere al proceso de revisar, evaluar y perfeccionar los planes y procedimientos de continuidad de una organización. Esta práctica busca identificar oportunidades para fortalecer la capacidad de la organización para mantener operaciones esenciales y recuperarse de interrupciones, basándose en la retroalimentación obtenida de pruebas y ejercicios anteriores utilizando esto como base para la implementación de las mejoras.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza un seguimiento continuo para medir la efectiva implantación del programa de ejercicio?   + ¿Se han establecido métricas y criterios claros para evaluar el cumplimiento de los objetivos del programa de ejercicio?   + ¿Existen mecanismos para evaluar la participación activa y la ejecución exitosa de los ejercicios programados?   + ¿Se lleva a cabo una revisión post ejercicio para analizar los resultados y determinar áreas de mejora? * ¿Se han establecido indicadores de desempeño para evaluar la eficacia y resultados?   + ¿Estos indicadores proporcionan información significativa sobre los logros y áreas que necesitan corrección o mejora?   + ¿Los datos obtenidos a través de estos indicadores se utilizan para identificar patrones y obtener información valiosa sobre el desempeño de los sistema?   + ¿Los ejercicios se planifican con realismo y se acuerdan con las partes pertinentes para minimizar el riesgo de causar disrupciones en las actividades? * ¿La organización diseña escenarios de ejercicios que satisfacen los objetivos establecidos y utilizan amenazas identificadas en la evaluación del riesgo o experiencias previas de disrupciones?   + ¿Se retiene la información documentada apropiada de todas las evaluaciones periódicas y sus resultados?   + ¿Se asegura la accesibilidad y disponibilidad de la información documentada para las partes interesadas pertinentes en caso de necesidad? * ¿Existe un método establecido para rastrear problemas y brechas descubiertas durante las pruebas de continuidad de negocio?   + ¿Se realiza un seguimiento efectivo de la resolución de problemas identificados durante las pruebas?   + ¿La organización tiene un proceso para documentar y analizar las lecciones aprendidas de los problemas identificados durante las pruebas?     - ¿Los encargados y las acciones están correctamente definidas y documentadas? * ¿Se elabora un informe completo después de cada ejercicio que incluya metas, objetivos, resultados y recomendaciones?   + ¿El informe posterior al ejercicio contiene un calendario para la implantación de las recomendaciones identificadas?   + ¿Las lecciones extraídas de los ejercicios y de incidentes reales se revisan y se aplican en ejercicios futuros para mejorar la preparación?   + ¿La organización identifica debilidades u omisiones en los planes y capacidades durante los ejercicios?   + ¿Se realizan recomendaciones de mejora basadas en la identificación de debilidades? |