

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Evaluación de Riesgos e Impacto**

**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

El proceso de evaluación de riesgos e impacto permite identificar amenazas, analizar sus consecuencias, y establecer medidas para mitigar riesgos y priorizar actividades críticas para garantizar la resiliencia organizacional frente a eventos disruptivos. Desde la perspectiva de auditoría, es crucial que estos procedimientos estén documentados, se revisen regularmente y se integren de manera efectiva en el Sistema de Gestión de Continuidad del Negocio (SGCN).

* 1. **Evaluación de Riesgos en Funciones y Sitios**

Cada unidad de negocio debe realizar una evaluación de riesgos que considere escenarios potenciales y eventos disruptivos específicos, como los riesgos sísmicos en zonas propensas. Este análisis debe incluir amenazas, vulnerabilidades y la probabilidad de ocurrencia, así como la efectividad de los controles existentes. Desde una perspectiva de auditoría, es fundamental verificar si estas evaluaciones se realizan consistentemente y si las conclusiones se comunican a los responsables de la toma de decisiones.

* 1. **Análisis de Impacto en el Negocio (BIA)**

El análisis de impacto debe identificar procesos de misión crítica, interdependencias y los recursos necesarios para su recuperación. Esto incluye clasificar los impactos como bajos, moderados o altos según los objetivos de confidencialidad, integridad y disponibilidad. También se debe estimar el tiempo de inactividad permitido y determinar los objetivos de tiempo de recuperación (RTO). Un auditor revisará si el BIA está documentado, incluye criterios claros y se alinea con los objetivos de continuidad del negocio.

* 1. **Documentación y Comunicación de Resultados**

Los resultados del análisis de impacto y la evaluación de riesgos deben documentarse e incluir las obligaciones legales, reglamentarias y contractuales. Además, es esencial identificar relaciones entre productos, servicios, actividades y recursos, así como interdependencias con la cadena de suministro y otras partes interesadas. Desde el punto de vista de auditoría, se debe garantizar que esta documentación esté actualizada y accesible para los responsables de la continuidad.

* 1. **Planificación de Acciones y Recursos**

Con base en los resultados del análisis de riesgos e impacto, se deben planificar acciones para prevenir resultados inesperados, aprovechar oportunidades de mejora y garantizar la integración en el SGCN. Esto incluye asignar objetivos de tiempo de recuperación a recursos críticos y especificar los recursos necesarios para actividades prioritarias. Un auditor evaluará si estas acciones están claramente definidas y si su efectividad es monitoreada continuamente.

* 1. **Revisión Regular y Mejora Continua**

La evaluación de riesgos y el análisis de impacto deben revisarse en intervalos planificados o tras cambios significativos en el contexto operativo. Esto garantiza que las evaluaciones sigan siendo relevantes y efectivas frente a nuevas amenazas. Desde una perspectiva de auditoría, es esencial verificar si las revisiones se realizan según lo programado y si los resultados se utilizan para mejorar continuamente las prácticas de continuidad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. La unidad de negocio o la gerencia regional deben completar una evaluación de riesgos de continuidad del negocio para cada una de sus funciones comerciales y sitios asociados (ciudad o región). Este proceso de evaluación debe responder a preguntas fundamentales, como las siguientes:     1.1 ¿Qué podría suceder?     1.2 ¿Cuál es la probabilidad de que suceda?     1.3 ¿Cuáles serían las consecuencias?     1.4 ¿Hay algo que podría mitigar las consecuencias o reducir la probabilidad? 2. Los participantes en la evaluación de riesgos deben incluir personas como personal de la empresa, así como personal del grupo de salud, seguridad y medio ambiente; gestión de las instalaciones; legal; recursos humanos; y personal del campo médico.      2.1 Si el sitio de operaciones está en una zona sísmica, esto debe considerarse un evento disruptivo probable, lo que a menudo se denomina evento creíble.  3. Mantener dentro del proceso son los siguientes puntos:     3.1 Identificar escenarios potenciales que podrían ocasionar eventos que darían lugar a incidentes disruptivos significativos.     3.2 Identificación de riesgos. Esta debe incluir:         3.2.1 Amenazas específicas que podrían, en algún punto, crear disrupciones en las actividades y los recursos.         3.2.2 Disrupciones, que podrían surgir de vulnerabilidades de los recursos.     3.3 Análisis de riesgos. Esta debe:         3.3.1 Tener en cuenta las causas y las fuentes de riesgo, la probabilidad de que se produzcan consecuencias tanto positivas como negativas y los efectos que otros factores podrían tener en esa probabilidad.         3.3.2 Determinar los riesgos, basándose principalmente en su probabilidad y en las consecuencias previstas, pero teniendo en cuenta también la eficacia y eficiencia de los controles existentes.      3.4 Tener en cuenta el contexto de la organización y ponerse en conocimiento de los responsables de la toma de decisiones y de otras partes interesadas.     3.5 Valoración de los riesgos.      3.6 Considerar todas las obligaciones financieras, reglamentarias o legislativas o administrativas que exijan la comunicación de estas conclusiones. 4. Tener en cuenta los riesgos y las oportunidades y su impacto potencial dentro de un sistema de gestión de continuidad del negocio (SGCN). Los riesgos y las oportunidades pueden surgir de:            4.1 La falta de liderazgo y compromiso de la alta dirección.           4.2 Una financiación insuficiente del SGCN que dé lugar a una respuesta ineficaz.           4.3 Información mal documentada.           4.4 La falta de personal con competencias demostradas.           4.5 Un proceso insuficiente de revisión por la dirección.           4.6 La incapacidad de penetrar en nuevos mercados en los que la continuidad del negocio sea una obligación. 5. Planificar las acciones necesarias para abordar los riesgos y las oportunidades de tal forma que:     5.1 Se impidan los resultados no imprevistos.     5.2 Se saque partido de todas las oportunidades para mejorar el SGCN.     5.3 Se consiga la integración en el proceso del SGCN.     5.4 Se garantice que la información documentada esté disponible para evaluar si las acciones han sido eficaces. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Realizar el análisis de impacto de modo que este:     1.1 Determine los procesos de misión, los procesos del negocio y la criticidad de la recuperación. Este último debe contemplar:         1.1.1 Procesos soportados por el sistema. Los procesos empresariales deben identificarse por separado si tienen distinto personal (p. ej., funciones del personal), proveedores de servicios (p. ej., terceros, subcontratista, etc.) o recursos (por ejemplo, sistemas informáticos).         1.1.2  Identificar de las interdependencias de las actividades prioritarias.         1.1.3  Impacto de una interrupción del sistema en dichos procesos. Estos se deben clasificar como de bajo impacto, impacto moderado o alto impacto para los objetivos de seguridad de confidencialidad, integridad y disponibilidad.         1.1.4  Impacto de la interrupción y el tiempo de inactividad estimado.     1.2 Identificar las necesidades de recursos.      1.3 Identificar las prioridades de recuperación de los recursos del sistema.      1.4 Uso de los criterios de evaluación para evaluar los impactos previstos en el tiempo derivados de una disrupción de estas actividades.  2. El análisis del impacto sobre el negocio debe documentarse e incluir:     2.1 La identificación de los requisitos (obligaciones) legales, reglamentarios y contractuales y sus efectos en los requisitos de la continuidad del negocio.     2.2 El respaldo o las modificaciones del campo de aplicación del SGCN de la organización.     2.3 La evaluación de los impactos en las horas extras de la organización como justificación para los requisitos de continuidad del negocio.     2.4 La identificación de las relaciones entre productos y servicios, actividades y recursos.     2.5 La identificación de los recursos de apoyo que dependen de las actividades prioritarias     2.6 La identificación de las interdependencias de otras actividades, cadenas de suministro, socios y otras partes interesadas.  3. Determinar las condiciones y los dueños de las decisiones clave que ocasionarán que se invoquen 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. Analizar los impactos de los procesos identificados con regularidad en términos de disponibilidad, integridad, confidencialidad y el nivel de impacto. 2. El análisis del impacto sobre el negocio y la evaluación del riesgo debería revisarse a intervalos planificados y siempre que se produzca algún cambio significativo en la organización o en el contexto en el cual opera. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Definir como requisitos de continuidad en base al resultado del análisis de impacto empresarial (BIA).     1.1 El proceso de BIA debe utilizar tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo resultantes de la interrupción de las actividades comerciales que entregan productos y servicios.     1.2 La magnitud y duración del impacto resultante deben usarse para identificar actividades prioritarias a las que se les debe asignar un objetivo de tiempo de recuperación (RTO).     1.3 BIA debería determinar qué recursos se necesitan para apoyar las actividades prioritarias. También se debe especificar un RTO para estos recursos. Un subconjunto de estos recursos debería incluir servicios TIC. |
| 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. **Prácticas de auditoría para la Evaluación de Riesgos e Impacto**

|  |
| --- |
| Temática: Planificación de acciones para riesgos y oportunidades |
| En una planificación se debe tener información detallada de cómo, por qué y cuando hacer ciertos puntos en un proyecto. Por lo que el auditor para lograr auditar de forma concisa debe lograr entender ciertas preguntas de relevancia que debiese hacerse y así, tener en cuenta ciertos factores y puntos de vista. Por lo que a continuación se dejan preguntas que un auditor puede tener en cuenta a la hora de hacer la auditoria.  Este levantamiento puede incluir preguntas para el análisis específicos tales como:   * ¿La unidad de negocio o gerencia regional ha completado evaluaciones de riesgos de continuidad del negocio para cada una de sus funciones comerciales y sitios asociados?   + Verifique si existe evidencia de la consideración de diversos escenarios y eventos en las evaluaciones de riesgos, demostrando una evaluación integral de posibles situaciones.   + ¿Se evalúa la probabilidad de que sucedan los eventos identificados en las evaluaciones de riesgos?   + ¿Las evaluaciones de riesgos abordan las consecuencias potenciales de los eventos identificados?   + ¿Se identifican medidas para mitigar las consecuencias o reducir la probabilidad de los eventos evaluados? * ¿Se incluyen los roles adecuados en la evaluación de riesgos, como personal de la empresa, personal del grupo de salud, seguridad y medio ambiente, gestión de instalaciones, legal, recursos humanos y personal del campo médico?   + ¿Existe evidencia de que se lleva a cabo una evaluación de riesgos integral que involucre a diversos departamentos?   + ¿Se considera la ubicación del sitio de operaciones como un factor relevante en la evaluación de riesgos, especialmente si está en una zona sísmica?     - ¿Se clasifica correctamente la ubicación en una zona sísmica como un evento creíble en la evaluación de riesgos? * ¿Se lleva a cabo regularmente la identificación de escenarios potenciales que podrían ocasionar eventos desencadenantes de incidentes disruptivos significativos?   + ¿La identificación de riesgos abarca amenazas específicas y disrupciones relacionadas con las vulnerabilidades de los recursos?   + ¿El análisis de riesgos tiene en cuenta causas, fuentes, probabilidades y efectos tanto positivos como negativos?   + ¿Se realiza una valoración de riesgos considerando la probabilidad y las consecuencias previstas, y teniendo en cuenta la eficacia de los controles existentes? * ¿Se ha identificado y evaluado el impacto potencial de la falta de liderazgo y compromiso de la alta dirección en el sistema de gestión de continuidad del negocio (SGCN)?   + ¿Se cuenta con una financiación adecuada del SGCN para garantizar una respuesta efectiva ante interrupciones?   + ¿La información relacionada con el SGCN está debidamente documentada?     - Entreviste al personal responsable de la documentación para confirmar la existencia y accesibilidad de la información necesaria.   + ¿Existe un proceso efectivo de revisión por la dirección que aborde los riesgos y las oportunidades en el SGCN? * ¿Existe un plan documentado para abordar los riesgos identificados y aprovechar las oportunidades en el SGCN?   + ¿Las acciones planificadas buscan prevenir resultados no previstos en el SGCN?     - Revise informes de incidentes anteriores para determinar si las acciones preventivas fueron eficaces y si se tomaron medidas adicionales después de su implementación.   + ¿Las acciones planificadas buscan la integración efectiva del proceso del SGCN?   + ¿Se garantiza que la información documentada esté disponible para evaluar la eficacia de las acciones planificadas? |

|  |
| --- |
| Temática: Análisis de riesgo e impacto en el SGCN |
| A continuación, el auditor debe comprender cómo y por qué se hacen estos análisis, además de cómo deben hacerse, para ello, existen preguntas que pueden ayudar a comprender cuales son los puntos para auditar y algunas consideraciones.  Este levantamiento puede incluir preguntas para el análisis específicos tales como:   * ¿Se ha llevado a cabo un análisis de impacto que determine los procesos de misión, los procesos del negocio y la criticidad de la recuperación?   + ¿Se han identificado de manera separada los procesos empresariales que tienen distinto personal, proveedores de servicios o recursos?   + ¿Se han identificado las interdependencias de las actividades prioritarias y se ha evaluado el impacto de una interrupción del sistema en dichos procesos?     - Verifique la existencia de registros que documenten el análisis de impacto en las interdependencias, incluyendo la clasificación del impacto en confidencialidad, integridad y disponibilidad.   + ¿Se utilizan criterios de evaluación para evaluar los impactos previstos en el tiempo derivados de una disrupción en las actividades? * ¿Está documentado el análisis del impacto sobre el negocio?   + Entreviste al personal responsable de realizar el análisis para confirmar que se ha llevado a cabo y que existe documentación respaldatoria.   + ¿Se han identificado los requisitos legales, reglamentarios y contractuales, así como sus efectos en los requisitos de la continuidad del negocio?   + ¿Se han respaldado o modificado adecuadamente el campo de aplicación del SGCN de la organización?     - Verifique si hay una clara conexión entre los cambios en el campo de aplicación y los resultados del análisis del impacto sobre el negocio   + ¿Se ha evaluado el impacto en las horas extras de la organización como justificación para los requisitos de continuidad del negocio?   + ¿Se han identificado las relaciones entre productos y servicios, actividades y recursos?   + ¿Se ha identificado adecuadamente los recursos de apoyo que dependen de las actividades prioritarias? * ¿Existe un proceso formal para determinar las condiciones que activarán los planes de continuidad?   + ¿Se han identificado claramente los dueños de las decisiones clave relacionadas con la activación de los planes de continuidad?   + ¿Se mantiene actualizada la lista de condiciones y dueños de decisiones clave que activarán los planes de continuidad?     - Compare la lista de condiciones y dueños de decisiones clave con eventos recientes para asegurar que refleje con precisión la realidad operativa y las amenazas actuales.   + ¿Las condiciones se han comunicado claramente y también los dueños de decisiones clave a todo el personal relevante?     - Revise las comunicaciones internas para verificar si se han compartido de manera clara y efectiva las condiciones y dueños de decisiones clave con el personal pertinente.   + ¿Los requisitos de continuidad se definen en base al resultado del Análisis de Impacto Empresarial (BIA)?     - Evaluar la consistencia entre los resultados del BIA y los tipos y criterios de impacto aplicados para determinar si se utiliza una evaluación integral.     - ¿La magnitud y duración del impacto resultante se utilizan para identificar actividades prioritarias con objetivos de tiempo de recuperación (RTO)?     - ¿El BIA determina los recursos necesarios para apoyar las actividades prioritarias, incluyendo servicios TIC, y especifica RTO para estos recursos? |