

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Estrategias de Recuperación de Sistemas y Datos**

**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

Las estrategias de recuperación de sistemas y datos son fundamentales para garantizar la continuidad del negocio tras un incidente disruptivo. Este proceso implica identificar, desarrollar e implementar soluciones que minimicen el impacto de los incidentes en las operaciones críticas. Desde una perspectiva de auditoría, estas estrategias deben estar documentadas, alineadas con los requisitos organizacionales y sujetas a revisión y mejora continua.

* 1. **Análisis de Brechas y Desarrollo de Estrategias**

El proceso comienza con un análisis de brechas que compare los requisitos de continuidad aprobados con las capacidades actuales de recuperación. Esto permite identificar áreas críticas que necesitan mejoras. Posteriormente, se deben considerar diversas opciones estratégicas y seleccionar la más adecuada. Este proceso debe incluir la definición de alcance, asignación de recursos, comunicación de expectativas y recopilación de lecciones aprendidas para futuras mejoras. Desde el punto de vista de auditoría, se debe verificar si este análisis está documentado y si las estrategias seleccionadas cumplen con los objetivos del negocio.

* 1. **Consideraciones para el Desarrollo de Estrategias**

Las estrategias deben abordar una amplia gama de elementos, como procesos manuales, subcontratación, recuperación de TI en caso de desastres, personal e instalaciones alternativas, y redundancia de sistemas y datos. También se deben considerar las comunicaciones, redes, acceso remoto y sistemas de gestión de información. Un auditor evaluará si las estrategias incluyen todos estos elementos y si están diseñadas para manejar los escenarios creíbles identificados en la evaluación de riesgos.

* 1. **Implementación y Mantenimiento**

Una vez seleccionadas, las estrategias deben documentarse e implementarse de manera que estén listas para activarse en cualquier momento. Esto incluye instrucciones detalladas para la recuperación de sistemas y gestión de información, con referencias claras a procedimientos, diagramas y materiales de soporte. Además, la organización debe asegurarse de que los recursos necesarios, como espacio de trabajo, personal y equipos, estén disponibles en el momento de un incidente. Desde una perspectiva de auditoría, se debe garantizar que estas estrategias sean realizables y que los recursos estén preparados para su activación.

* 1. **Seguimiento y Evaluación del Desempeño**

El desempeño de las estrategias debe monitorearse regularmente para asegurarse de que cumplen con los requisitos de continuidad del negocio. Esto incluye el uso de métricas para evaluar procesos, procedimientos y cumplimiento normativo, así como el seguimiento de errores, incidentes y deficiencias. Si las estrategias no cumplen con los requisitos, el proceso de determinación y selección debe repetirse para ajustar las capacidades necesarias. Un auditor revisará si los procedimientos de monitoreo están bien definidos y si los datos recopilados se utilizan para realizar mejoras.

* 1. **Mejora Continua**

La organización debe revisar la eficacia de sus estrategias después de cada incidente disruptivo y utilizar las métricas y lecciones aprendidas para ajustar y mejorar su enfoque. Esto asegura que las estrategias sean adecuadas, efectivas y estén alineadas con las necesidades cambiantes del negocio. Desde una perspectiva de auditoría, es crucial verificar que estas revisiones se realicen de manera oportuna y que las mejoras se implementen según sea necesario.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Llevar a cabo un análisis de las carencias comparando los requisitos aprobados de continuidad del negocio (tiempo y capacidad) con las capacidades actuales de respuesta y recuperación tras el análisis de impacto. 2. Identificar una amplia variedad de opciones de estrategias y, a continuación, implementar la estrategia elegida como uno o varios proyectos. Las tareas deben incluir:  2.1 Decidir el alcance del proceso de determinación y selección de las estrategias de continuidad del negocio.  2.2 Comunicar las expectativas a los participantes en la determinación y selección de las estrategias.  2.3 Identificar a la persona promotora de la determinación y selección de las estrategias, así como la participación de la alta dirección.  2.4 Especificar las competencias para las responsabilidades relativas a la determinación y selección de las estrategias.  2.5 Establecer el plan del proyecto.  2.6 Asignar los recursos para la determinación y selección de las estrategias.  2.7 Conseguir la aceptación del planteamiento y el plan del proyecto.  2.8 Dotarse interna o externamente de las destrezas necesarias para cumplir los objetivos del proceso de la estrategia.  2.9 Elaborar informes periódicos sobre el estado de la determinación y selección, para mejorar el desempeño en consonancia con las expectativas de la alta dirección.  2.10 Realizar modificaciones del enfoque y el alcance de las estrategias para cumplir las expectativas de la alta dirección y los requisitos externos (reglamentarios, legales, de clientes o contractuales).  2.11 Recopilar y revisar las lecciones aprendidas.  2.12 Realizar recomendaciones para la mejora del enfoque de la determinación y selección de las estrategias de cara a su uso en el futuro. 3.Asegurar que aquellas estrategias que cumplan los requisitos de continuidad del negocio sean la mejor opción posible y que no haya otras opciones mejores.  3.1 Se debe tener en cuenta los sucesos creíbles identificados durante la evaluación de riesgos de continuidad del negocio, junto con sus posibles repercusiones sobre los recursos a a la hora de desarrollar estrategias de recuperación y continuidad de la actividad. 4. Las estrategias de recuperación y continuidad de la actividad deben considerar:  4.1 Procesos de trabajo manuales.  4.2 Subcontratación.  4.3 Recuperación de TI en caso de catástrofe.  4.4 Personal alternativo.  4.5 Instalaciones alternativas.  4.6 Sistemas informáticos, incluidos:  4.6.1 Centro de datos de TI.  4.6.2 Aplicaciones y datos necesarios para la organización.  4.6.3 Servidores y otro hardware.  4.6.4 Comunicaciones como teléfono, radio, etc.  4.6.5 Red, incluidas las conexiones externas (de terceros).  4.6.6 Infraestructura de TI (por ejemplo, servicios de inicio de sesión y distribución de software).  4.6.7 Servicios de acceso remoto.  4.6.8 Sistemas de control de procesos (por ejemplo, SCADA/DCS).  4.7 Sistemas de gestión de la información, incluidos:  4.7.1 Salas de archivo.  4.7.2 Sistemas de gestión de documentos (eléctricos y  manuales) |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Implementar y mantener las estrategias elegidas a lo largo del tiempo.  1.1 Debe documentarse el proceso y todas las decisiones adoptadas y debe describir las estrategias de recuperación de los sistemas informáticos y de gestión de la información. Este debe incluir instrucciones detalladas de recuperación que pueden incluir referencias a procedimientos, referencias de proveedores, diagramas de sistemas y otros materiales de recuperación relacionados. 2. Asegurar que, tras la selección de las estrategias de continuidad del negocio, la dirección debe implicarse en la selección de los recursos de continuidad del negocio (por ejemplo, el espacio de trabajo, las personas, los equipos y los suministros).   2.1 Deben extremarse las precauciones para asegurarse de que estos recursos estén disponibles en el momento del incidente. 3. Asegurar que las estrategias de reanudación y mitigación sean realizables, la organización debe definir e implementar todas las capacidades y medidas que han de estar preparadas antes de un incidente disruptivo. 4. Verificar que, si el plazo que se tarda en activar una capacidad o una medida es superior a los requisitos de continuidad del negocio, la organización implemente o tenga en cuenta las estrategias que se hubieran elegido con anterioridad al incidente disruptivo. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Hacer un seguimiento de su desempeño para asegurarse de que las estrategias siguen cumpliendo los requisitos de continuidad del negocio una vez que una organización selecciona e implementa las estrategias de continuidad del negocio.  1.1 Si las estrategias no cumplen los requisitos, la organización debería repetir el proceso de determinación y selección de las estrategias, con el objetivo de ajustar las capacidades de las estrategias para satisfacer los requisitos 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. Revisar y hacer el seguimiento del desempeño, tanto real como previsto, de sus estrategias de continuidad del negocio. Los procedimientos deben incluir lo siguiente:  1.1 Establecer métricas del desempeño de las operaciones normales y de las simulaciones durante los ejercicios.  1.2 Evaluar el desempeño de los procesos, los procedimientos y las funciones que protegen las actividades priorizadas.  1.3 Confirmar el cumplimiento continuo de la legislación aplicable y de los requisitos legales y reglamentarios.  1.4 hacer el seguimiento de los errores, los incidentes y las no conformidades (incluidos los cuasi-accidentes y las falsas alarmas), así como de otras pruebas de deficiencias del desempeño.  1.5 Obtener datos adecuados de seguimiento y medición y adoptar medidas al respecto. 2. Mantener registros de las revisiones del desempeño y de 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. Mejorar la adecuación, idoneidad y eficacia continuas de las estrategias de continuidad del negocio tras obtener información de métricas o lecciones aprendidas.  1.1 Se debe realizar una revisión de la eficacia de las estrategias de continuidad del negocio después de cada incidente disruptivo, independientemente del resultado. |

1. **Prácticas de auditoría para las Estrategias de Recuperación de Sistemas y Datos**

|  |
| --- |
| Temática: Análisis e implementación de las estrategias |
| El análisis previo a la implementación de las estrategias debe tener en cuenta el requisito establecido de continuidad y compararlo con las carencias que tiene la empresa para que luego con esto se decida el alcance y las áreas en el cual este proceso es más fundamental o su falla o perdida inflija el mayor daño tanto a la economía como a la reputación de la empresa una vez decidido esto se debe definir a los responsables y el plan teniendo en cuenta los recursos necesario para implementarlo y las competencias tanto externas como internas que se deberán usar.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha realizado un análisis comparativo entre los requisitos aprobados de continuidad del negocio y las capacidades actuales de respuesta y recuperación después del análisis de impacto?   + ¿Existen procedimientos documentados para este análisis y comparación?   + ¿Se toman medidas correctivas basadas en los resultados de este análisis?   + ¿La dirección esta de acuerdo con esta medidas y fue parte del proceso selectivo de estas? * ¿Se ha decidido claramente el alcance del proceso de determinación y selección de estrategias de continuidad del negocio?   + ¿Las expectativas han sido comunicadas eficazmente a los participantes involucrados en la determinación y selección de estrategias?   + ¿Se ha identificado de manera clara la persona promotora de este proceso y la participación de la alta dirección?     - ¿Existen especificaciones de competencias para las responsabilidades relacionadas con la determinación y selección de estrategias? * ¿Se ha establecido un plan de proyecto detallado para guiar la implementación de las estrategias?   + ¿Los recursos necesarios para la determinación y selección de estrategias han sido asignados adecuadamente?   + ¿Se ha obtenido la aceptación del planteamiento y el plan del proyecto por parte de las partes pertinentes?   + ¿Se ha considerado la adquisición interna o externa de habilidades necesarias para alcanzar los objetivos del proceso de estrategia? * ¿Se elaboran informes periódicos sobre el estado de la determinación y selección para mejorar el desempeño según las expectativas de la alta dirección?   + ¿Existen mecanismos para realizar modificaciones en el enfoque y alcance de las estrategias según las expectativas de la alta dirección y requisitos externos?   + ¿Se recopilan y revisan de manera sistemática las lecciones aprendidas en el proceso de determinación y selección de estrategias?   + ¿Se realizan recomendaciones periódicas para mejorar el enfoque de la determinación y selección de estrategias en futuras ocasiones? * ¿Se evalúa la factibilidad y realismo de las estrategias de reanudación y mitigación antes de su implementación?   + ¿Se verifica regularmente que el tiempo requerido para activar una capacidad o medida esté dentro de los límites establecidos por los requisitos de continuidad del negocio?   + ¿Se asegura la implementación o consideración de estrategias elegidas con anterioridad al incidente si los plazos de activación son superiores a los requisitos establecidos? * ¿Cómo se asegura que las estrategias seleccionadas cumplan de manera óptima con los requisitos de continuidad del negocio?   + ¿Se toman en cuenta los sucesos creíbles identificados durante la evaluación de riesgos al desarrollar estrategias de recuperación y continuidad?   + ¿Existen estrategias para abordar procesos de trabajo manuales, subcontratación, recuperación de TI, personal alternativo, instalaciones alternativas, sistemas informáticos, y sistemas de gestión de la información (incluyendo salas de archivo y sistemas de gestión de documentos)?   + ¿Existe un proceso documentado para implementar y mantener las estrategias seleccionadas a lo largo del tiempo? * ¿Se documentan todas las decisiones tomadas durante el proceso de implementación y mantenimiento? * ¿La documentación describe de manera detallada las estrategias de recuperación de sistemas informáticos y de gestión de la información? * ¿La documentación incluye una descripción detallada de las estrategias de recuperación de sistemas informáticos y de gestión de la información? * ¿La dirección se implica activamente en la selección de recursos para la continuidad del negocio después de la selección de estrategias? * ¿Se incluyen instrucciones detalladas de recuperación, tales como procedimientos, referencias de proveedores, diagramas de sistemas y otros materiales relacionados?   + ¿La organización ha definido e implementado todas las capacidades y medidas necesarias para que las estrategias de reanudación y mitigación sean realizables?   + ¿Se toman precauciones adecuadas para garantizar la disponibilidad oportuna de recursos como espacio de trabajo, personas, equipos y suministros en caso de un incidente?     - ¿Estas capacidades y medidas están preparadas antes de un incidente disruptivo? * ¿La organización tiene un proceso establecido para realizar un seguimiento continuo del desempeño de las estrategias de continuidad del negocio?   + ¿La organización verifica regularmente el tiempo que tarda en activar una capacidad o medida ante un incidente disruptivo?     - ¿Si el tiempo de activación es superior a los requisitos de continuidad del negocio, se implementan o tienen en cuenta estrategias previamente elegidas?     - ¿Se asegura de que las estrategias seleccionadas sigan cumpliendo con los requisitos de continuidad del negocio a lo largo del tiempo?       * ¿Existe un mecanismo claro para evaluar si las estrategias cumplen con los requisitos establecidos?     - ¿En caso de que las estrategias no cumplan con los requisitos, la organización tiene un proceso para repetir el análisis de determinación y selección de estrategias?     - ¿Se han establecido métricas específicas para evaluar el desempeño durante operaciones normales y simulaciones durante ejercicios de continuidad?   + ¿Se lleva a cabo una evaluación del desempeño de los procesos, procedimientos y funciones que protegen las actividades priorizadas?     - ¿La organización mantiene registros documentados de las revisiones del desempeño de las estrategias de continuidad del negocio?     - Revise informes y registros de métricas relacionados con la continuidad del negocio para verificar la recopilación regular de información pertinente, como tiempos de recuperación, pérdidas financieras, etc.     - ¿Estos registros incluyen los resultados obtenidos durante las revisiones del desempeño?     - ¿Se documentan las acciones correctivas tomadas en caso de identificar deficiencias en el desempeño? |