

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Respaldo y Redundancia de los Sistemas**

**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 respaldo y la redundancia de sistemas son fundamentales para garantizar la disponibilidad y recuperación de información crítica en caso de interrupciones. Este enfoque combina estrategias de respaldo de datos con arquitecturas redundantes que minimizan los riesgos asociados a la pérdida de información y aseguran la continuidad operativa. Desde la perspectiva de auditoría, es crucial que estos procesos estén alineados con los requisitos organizacionales, se prueben regularmente y sean actualizados según las necesidades del negocio.

**1.1 Identificación de Requisitos de Disponibilidad**

La organización debe identificar los requisitos específicos para la disponibilidad de servicios y sistemas de información, considerando tanto los objetivos del negocio como los riesgos asociados a la interrupción. Esto incluye definir necesidades de almacenamiento en las instalaciones (on-site) y fuera de ellas (off-site), asegurando acceso seguro y controlado para respaldos y restauraciones. Un auditor verificará si estas necesidades están claramente documentadas y si los procedimientos implementados cumplen con las expectativas de continuidad.

**1.2 Gestión de Copias de Seguridad**

Las copias de seguridad deben realizarse de acuerdo con un calendario definido que contemple la frecuencia, el tipo de copia (completa, incremental) y los medios de almacenamiento utilizados. También es necesario garantizar que los respaldos incluyan sistemas, aplicaciones, datos y documentación gestionados por terceros, asegurando su retorno en caso necesario. Además, se deben considerar aspectos como encriptación, derechos de acceso y almacenamiento en ubicaciones seguras. Desde la perspectiva de auditoría, es importante revisar si los respaldos cumplen con los requisitos de seguridad de la información y si están adecuadamente registrados.

**1.3 Diseño de Arquitecturas Redundantes**

La organización debe diseñar e implementar arquitecturas de sistemas con redundancia que cumplan con los requisitos de disponibilidad. Esto incluye redes redundantes, múltiples centros de datos geográficamente separados, y componentes duplicados con equilibrio de carga. Los procedimientos deben especificar cómo activar estos sistemas, ya sea de forma automática o manual, en caso de emergencia. Un auditor evaluará si estas arquitecturas han sido probadas y si garantizan la continuidad operativa según lo planificado.

**1.4 Políticas de Respaldo y Planes de Recuperación**

Se debe establecer una política específica sobre respaldo que contemple los requisitos de retención y recuperación de datos. Los planes de respaldo deben detallar cómo se realizarán las copias, dónde se almacenarán y qué procedimientos seguir para restaurarlas. Esto incluye asegurar que las copias de seguridad estén protegidas físicamente y que los datos puedan recuperarse después de fallas o desastres. Desde una perspectiva de auditoría, se revisará si estos planes reflejan los requisitos comerciales y de seguridad de la organización.

**1.5 Pruebas y Verificación**

Es fundamental probar regularmente los sistemas redundantes y las copias de seguridad para garantizar su efectividad. Esto incluye pruebas de conmutación por error en modo de producción y refresco periódico de los datos archivados. Un auditor verificará si las pruebas se realizan de manera consistente y si los resultados son documentados para identificar mejoras necesarias.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1.Identificar los requisitos para la disponibilidad de servicios y sistemas de información.  2. Definir requisitos para el almacenamiento en las instalaciones (on-site) y fuera de ellas (off-site) de copias de seguridad de datos, conforme a los requisitos de negocio. Considerar el acceso requerido para hacer copias de seguridad de los datos 3. Garantizar que se haga una copia de seguridad o se aseguren de forma adecuada los sistemas, aplicaciones, datos y documentación mantenida o procesada por terceros. Considerar que se requiera que los terceros devuelvan las copias de seguridad. Considerar la opción de mantenimiento en fiducia (escrow, por su término en inglés) o acuerdos de depósitos. 4. Garantizar que los requisitos de seguridad de la información estén incluidos en los acuerdos de copia de seguridad y restauración. 5. Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido.   5.1 Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (p. ej., disk mirroring para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios.   5.2 Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (p. ej., hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Diseñar e implementar una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos. 2. Implementar procedimientos para la activación de los componentes redundantes y las instalaciones de procesamiento. Los procedimientos deben establecer si los componentes redundantes y las actividades de procesamiento están siempre  activados, o en caso de emergencia, activados automática o manualmente. 3. Considerar lo siguiente al implementar sistemas redundantes:  3.1. Contratar dos o más proveedores de redes e instalaciones de procesamiento de información crítica.  3.2. Utilizar redes redundantes.  3.3. Utilizar dos centros de datos geográficamente separados con sistemas reflejados.  3.4. Utilizar fuentes o fuentes de alimentación físicamente redundantes.  3.5. Utilizar múltiples instancias paralelas de componentes de software, con equilibrio de carga automático entre ellos.  3.6. Tener componentes duplicados en los sistemas o en redes  4. Establecer una política de temática específica sobre respaldo para abordar los requisitos de seguridad de la información y retención de datos de la organización. Se debe:   4.1 Proporcionar instalaciones de respaldo adecuadas para garantizar que toda la información y el software esenciales puedan recuperarse después de un incidente, falla o pérdida de los medios de almacenamiento.  4.2 Desarrollar e implementar planes sobre cómo la organización realizará copias de seguridad de la información, el software y los sistemas, para abordar la política específica del tema sobre copias de seguridad. 5. Tener en cuenta los siguientes elementos al diseñar un plan de respaldo:  5.1 Producir registros precisos y completos de las copias de seguridad y los procedimientos de restauración documentados.  5.2 Reflejar los requisitos comerciales de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización en la medida (por ejemplo, respaldo completo o diferencial) y frecuencia de las copias de seguridad.  5.3 Almacenar las copias de seguridad en una ubicación remota segura, a una distancia suficiente para evitar cualquier daño causado por un desastre en el sitio principal.  5.4 Brindar a la información de respaldo un nivel apropiado de protección física y ambiental, consistente con los estándares aplicados en el sitio principal. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Probar, cuando corresponda y preferiblemente en modo de producción, los sistemas de información redundantes para garantizar que la conmutación por error de un componente a otro funcione según lo previsto. 2. Probar y refrescar de forma periódica los datos archivados y las copias de seguridad de los datos. |
| 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. **Prácticas de auditoría para el Respaldo y Redundancia de los Sistemas**

|  |
| --- |
| Temática: Componentes y Respaldos de los Sistemas |
| Los controles de respaldo y redundancia en los sistemas de una organización son fundamentales porque garantizan la integridad de los datos críticos, la disponibilidad continua de los servicios, el cumplimiento normativo y la capacidad de recuperación ante desastres. Además, ayudan a identificar y abordar posibles riesgos y debilidades en los procesos de respaldo y redundancia, lo que contribuye a mantener la eficiencia operativa y la confidencialidad de los datos, asegurando así la protección de los activos de información de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se garantiza que todos los datos críticos estén incluidos en esta programación de respaldo y que no se omita ningún componente importante?”   + ¿Puede proporcionar detalles sobre la programación de las copias de seguridad, incluyendo la frecuencia con la que se realizan y los horarios específicos en los que se ejecutan? * ¿De qué manera se registran y documentan los resultados de estas pruebas?   + ¿Cuáles serían las medidas a abordar al momento de identificar problemas durante las pruebas de recuperación? * ¿Cuáles son los procedimientos y políticas establecidos para garantizar que solo el personal autorizado tenga acceso a las copias de seguridad?   + ¿Puede proporcionar una lista de las personas o roles específicos que tienen acceso y autorización para recuperar datos de las copias de seguridad?   + ¿Cómo se gestionan y mantienen las credenciales de acceso? * ¿La arquitectura de sistemas ha sido diseñada e implementada con la redundancia adecuada para cumplir con los requisitos establecidos?   + ¿Existen procedimientos claros para la activación de componentes redundantes y las instalaciones de procesamiento?   + ¿Los procedimientos establecen claramente si los componentes redundantes y las actividades de procesamiento están siempre activados, o en caso de emergencia, activados automática o manualmente? * ¿Se ha contratado dos o más proveedores de redes e instalaciones de procesamiento de información crítica?   + ¿Se utilizan redes redundantes según lo especificado en la implementación de sistemas redundantes?     - Realice pruebas de conectividad para confirmar que las redes redundantes están operativas y responden según lo esperado.   + ¿Se utilizan dos centros de datos geográficamente separados con sistemas reflejados?     - Realice una revisión de la ubicación física de los centros de datos y confirmar que estén geográficamente separados.   + ¿Se utilizan fuentes de alimentación físicamente redundantes?   + ¿Existen componentes duplicados en los sistemas o en redes? * ¿Se realizan pruebas de sistemas redundantes en condiciones de producción para asegurar que la conmutación por error funcione según lo previsto?   + Examine los registros de pruebas de sistemas redundantes anteriores para confirmar la realización de pruebas en modo de producción y verificar si se documentaron los resultados y las acciones correctivas, en caso necesario.   + ¿Existe evidencia de pruebas periódicas y refrescamiento de datos archivados y copias de seguridad?   + ¿Las pruebas de sistemas redundantes incluyen escenarios de conmutación por error realistas y representativos de situaciones de producción?   + ¿Los resultados de las pruebas de datos archivados y copias de seguridad incluyen verificación de la integridad, disponibilidad y capacidad de recuperación de los datos?   + ¿Se mantiene un registro completo y detallado de todas las solicitudes de acceso al código fuente y las decisiones tomadas? |

|  |
| --- |
| Temática: Plan de Respaldo |
| Monitorear un plan de respaldo garantiza que una organización cuente con medidas sólidas para proteger y recuperar sus datos críticos en caso de fallos o desastres. Evaluar la precisión de los registros de respaldo, la alineación con los requisitos comerciales y de seguridad, el almacenamiento seguro en ubicaciones remotas y la protección física y ambiental de los datos respaldados ayuda a mitigar riesgos significativos. Esto incluye la pérdida de datos importantes, interrupciones en la operación y la vulnerabilidad ante amenazas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene un proceso formal para identificar los requisitos de disponibilidad de servicios y sistemas de información?   + ¿Se han definido y documentado claramente los requisitos específicos de disponibilidad para cada servicio o sistema de información crítico?   + ¿Existe una evaluación periódica de los requisitos de disponibilidad para adaptarse a cambios en la organización o en las demandas del negocio? * ¿Se han definido claramente los requisitos para el almacenamiento on-site y off-site de copias de seguridad de datos?   + ¿Los requisitos para el almacenamiento de copias de seguridad cumplen con los requisitos de negocio establecidos?   + ¿Se ha considerado adecuadamente el acceso requerido para realizar copias de seguridad de los datos en los requisitos definidos? * ¿Se han establecido procedimientos para garantizar la realización de copias de seguridad de sistemas, aplicaciones, datos y documentación mantenida o procesada por terceros?   + ¿Se asegura de manera adecuada la integridad y confidencialidad de las copias de seguridad?   + ¿Se han establecido requisitos para que los terceros devuelvan las copias de seguridad y cómo se verifica este proceso?   + ¿Se ha considerado la opción de mantenimiento en fiducia (escrow) o acuerdos de depósitos para asegurar la continuidad y disponibilidad en caso de problemas con terceros? * ¿Se realiza una copia de seguridad de los sistemas, aplicaciones, datos y documentación de acuerdo con un calendario definido?   + Verifique los registros de copias de seguridad pasadas para asegurarse de que se están realizando regularmente de acuerdo con el calendario establecido.   + ¿Se ha definido y considerado adecuadamente la frecuencia, el modo y el tipo de copia de seguridad?   + ¿Se consideran opciones de copias de seguridad online automatizadas?     - Consulte con el personal encargado de las copias de seguridad para confirmar la implementación y funcionamiento de copias de seguridad online automatizadas.   + ¿Están definidos y documentados aspectos adicionales como tipos de datos, creación de logs, ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación? * ¿Dónde se almacenan las copias de seguridad de forma remota?   + ¿Cuál es la distancia entre el sitio principal y la ubicación de respaldo remota?   + ¿Se han considerado los riesgos de desastres naturales y otros eventos que podrían afectar ambos lugares?   + ¿Se realizan pruebas regulares para garantizar la accesibilidad y la integridad de los datos almacenados en la ubicación remota? * ¿Cuáles son las medidas de protección física y ambiental implementadas para los datos de respaldo?   + ¿Se utilizan los mismos estándares de seguridad en la ubicación de respaldo que en el sitio principal?   + ¿Cómo se controla el acceso a las instalaciones de almacenamiento de respaldo?   + ¿Existen medidas para proteger los datos de respaldo contra daños físicos, como incendios o inundaciones, y riesgos ambientales? * ¿La organización cuenta con una política de temática específica sobre respaldo que aborde los requisitos de seguridad de la información y retención de datos?   + ¿Se proporcionan instalaciones de respaldo adecuadas para garantizar la recuperación de información y software esenciales después de un incidente, falla o pérdida de medios de almacenamiento?     - Inspeccione las instalaciones de respaldo y verificar si cumplen con los estándares de seguridad necesarios para garantizar la integridad y disponibilidad de la información y el software almacenados.   + ¿La organización ha desarrollado e implementado planes sobre cómo realizar copias de seguridad de la información, el software y los sistemas?   + ¿Los planes de respaldo abordan específicamente la política de temática sobre copias de seguridad? |