

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Preparación y Planificación**

**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 preparación y planificación son esenciales para una organización, ya que una buena gestión de estos puntos ayuda a las organizaciones a anticipar, gestionar y responder eficazmente no solo a posibles amenazas y ataques que puedan comprometer a la empresa, sino que también a problemas del ámbito de los sistemas ya sea una caída de página o de suministro eléctrico. Teniendo una buena preparación más una buena planificación reduciría considerablemente el tiempo de respuesta, ya que permite a las organizaciones reaccionar de manera más rápida y efectiva cuando ocurre un ataque o problema. Esto puede minimizar el tiempo de inactividad, reducir el impacto en los sistemas y acelerar la recuperación. Así mismo con esto se minimizarán los daños y perdidas causados por un ataque o problema debido tanto al tiempo de respuesta más rápidos como a la identificación de riesgos antes de que estos se conviertan en problemas severos.

* 1. **Lineamientos sobre la preparación y planificación**

Tener lineamientos concisos y claros sobre preparación y planificación para la organización es clave porque ayuda a estar preparado para cualquier problema que pueda causar tanto pérdida o robo de información como una interrupción de los sistemas otorgando un tiempo de respuesta rápido además de un claro plan de acción ante cualquier suceso

**1.2 Criterios para la implementación de un buen plan de preparación y planificación.**

Una buena implementación de un plan de preparación y planificación ayudará a prevenir, detectar y responder a amenazas, además de garantizar que la organización esté preparada para enfrentar incidentes de seguridad de manera efectiva. Para esto es necesario tener en cuenta los siguientes criterios.

* **Evaluación de riesgos y amenazas:** Proporciona una comprensión clara de las amenazas que enfrenta una organización y las vulnerabilidades en su infraestructura. Esto permite priorizar y dirigir los recursos hacia las áreas de mayor riesgo y tomar decisiones informadas sobre medidas de seguridad específicas.
* **Roles y responsabilidades definidos:** Establecer roles y responsabilidades claros para garantizar que las tareas y responsabilidades relacionadas con la ciberseguridad estén claramente asignadas dentro de la organización. Esto evita confusiones, lo cual ayuda a tener una rápida reacción contra incidentes.
* **Plan de respuestas a incidentes:** Describe cómo la organización responderá en caso de un problema o incidente de seguridad. Proporcionando un marco estructurado para actuar rápidamente, el cual se debe enfocar en minimizar el daño y restaurar la operación normal de los servicios y sistemas.
* **Documentación de incidentes y mejora:** La documentación adecuada mantiene a la organización al tanto de las deficiencias que pudo tener los planes o evaluaciones anteriores. Por esto es necesario documentar los sucesos para que la organización tome decisiones de mejora basándose en estos incidentes evitando la ocurrencia de un incidente similar.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar los procesos y su aplicación en toda la organización, esta debe incluir:  1.1 Determinar las entradas requeridas y las salidas previstas de estos procesos.  1.2 Determinar la secuencia y las interacciones entre estos procesos.  1.3 Determinar y aplicar los criterios y los métodos (incluidos el seguimiento, las mediciones y los indicadores de desempeño correspondientes) que se necesitan para asegurarse de la operación y el control eficaces de estos procesos.  1.4 determinar los recursos necesarios para estos procesos y asegurarse de que estén disponibles.  1.5 Asignar las responsabilidades y autoridades para estos procesos.  1.6 Abordar los riesgos y las oportunidades.  1.7 Evaluar estos procesos e implantar todos los cambios precisos para asegurarse de que consigan los resultados previstos.  1.8 Mejorar los procesos y el sistema de gestión de la continuidad. 2. Definir un miembro de la alta dirección, quien debe ser responsable sistema de gestión de la continuidad y rendir cuentas al respecto. La alta dirección puede designar a otros organismos (por ejemplo, un comité de dirección) que supervise la implantación y el seguimiento continuo del sistema de gestión de la continuidad.  2.1 Asegurar que se asignen y se comuniquen las responsabilidades y las autoridades en el seno del sistema de gestión de la continuidad. 3. Designar representantes con roles, responsabilidades y autoridades definidos, independientemente de las demás responsabilidades que tengan, para:  3.1 Asegurarse de que el sistema de gestión de la continuidad cumpla la política de continuidad del negocio.  3.2 Informar a la alta dirección sobre el desempeño del sistema de gestión de la continuidad con el fin de revisarlo y utilizarlo como base para la mejora.  3.3 Fomentar la toma de conciencia respecto a la continuidad del negocio en toda la organización.  3.4 Garantizar la eficacia de los procedimientos desarrollados para responder a los incidentes. 4. Deben integrarse los roles, obligaciones de rendición de cuentas, responsabilidades y autoridades en las descripciones del puesto de trabajo. Esto puede reforzarse con la inclusión de tales características en la política de evaluación, recompensa y reconocimiento de la organización. 5. La dirección deberá determinar las competencias requeridas para todos los roles y responsabilidades del SGCN, así como la toma de conciencia, los conocimientos, la comprensión, las aptitudes y la experiencia necesarios para desempeñarlos.  5.1 Todas las personas a quienes se asignen roles en la organización deberán demostrar las competencias requeridas y recibir formación, educación, desarrollo y otros tipos de apoyo que necesiten para ello.  5.2 La organización deberá contar con un proceso para identificar e impartir los requisitos de formación de continuidad del negocio de todos los participantes, así como evaluar la eficiencia de su impartición.  5.3 La organización deberá exigir a los contratistas que trabajen en su nombre que demuestren que las personas que lleven a cabo las labores que están bajo su control cuentan con las competencias requeridas para el SGCN y para los roles de respuesta que desempeñan. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Determinar y garantizar la disponibilidad de los recursos necesarios para el sistema de gestión de la continuidad para:  1.1 Lograr su política y sus objetivos de continuidad del negocio.  1.2 Cumplir los requisitos cambiantes de la organización.  1.3 Permitir una comunicación eficiente, tanto interna como externa, sobre los asuntos del SGCN.  1.4 Velar por la operación y las mejoras continuas del SGCN.  1.5 Los recursos deberán estar disponibles de manera puntual y eficaz. 2. Al identificar los recursos que se requieren para el SGCN, la organización debería aprovisionarse de cantidades suficientes de:  2.2 Personal y recursos relacionados con el personal, tales como:  2.2.1 Tiempo preciso para cumplir con los roles y las responsabilidades del SGCN.  2.2.2 Formación, educación, toma de conciencia y ejercicios.  2.2.3 Gestión del personal del SGCN.  2.3 Instalaciones, incluidas las ubicaciones e infraestructuras de trabajo apropiadas.  2.4 Sistemas de tecnología de la información y comunicación (TIC), incluidas aplicaciones que respalden una gestión eficaz y eficiente del programa.  2.5 Gestión y control de todos los formatos de información documentada.  2.6 Comunicación con las partes interesadas.  2.7 Financiación.  3. Identificar necesidades de capacidad de instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones, teniendo en cuenta la criticidad de sistemas y procesos en cuestión. 4. Mantener información documentada para:  4.1 Respaldar la operación de sus procesos  4.2 Considerar un plan de gestión de la capacidad documentado para los sistemas de misión crítica.  4.3 Someter a auditorías a todos los roles, las responsabilidades y las autoridades relativos al SGCN. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Los recursos y su asignación deberían revisarse periódicamente con el fin de asegurarse de que sean suficientes.  1.1 Es apropiado que la alta dirección tome parte de esta revisión. 2. Monitorear el uso de los recursos con largos plazos de adquisición o costes elevados. Los gestores, propietarios de servicios o productos deben supervisar la utilización de recursos clave de sistema. 3. Documentación y seguimiento de la formación recibida. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Realizar pruebas de estrés de los sistemas y servicios para confirmar que hay suficiente capacidad de sistema para cumplir con los requisitos de rendimiento máximo. |
| 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. Usar información sobre la capacidad para identificar y evitar las posibles limitaciones de recursos y dependencia del personal clave que puedan suponer una amenaza para la seguridad de sistema o los servicios y planificar las medidas adecuadas. 2. Proyectar futuras necesidades de capacidad teniendo en cuenta las nuevas necesidades de la empresa y de sistema, así como las tendencias actuales y previstas de capacidades de procedimiento de información de la organización. 3.Mejora del programa de desarrollo, según sea preciso.  3.1 Evaluación de la formación recibida respecto a las necesidades y los requisitos de formación definidos con el fin de comprobar la conformidad con los requisitos de formación del SGCN. |

1. **Prácticas de auditoría para la Preparación y Planificación**

|  |
| --- |
| Temática: Planes de preparación y planificación. |
| Se debe asegurar que la preparación de la organización frente a incidente o fallos en los sistemas este correctamente informada viendo con esto la documentación de la evaluación de riesgos, clasificación de activos, políticas, la asignación de roles y responsabilidades.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha identificado claramente los procesos relacionados con la gestión de la continuidad del negocio?   + ¿Se han determinado las entradas requeridas y las salidas previstas para cada proceso?     - ¿Se ha establecido la secuencia y las interacciones entre estos procesos?   + ¿Se han definido y aplicado los criterios y métodos necesarios para el control efectivo de estos procesos, incluyendo el monitoreo y las mediciones?   + ¿Se han determinado los recursos necesarios y se asegura de que estén disponibles para estos procesos?     - ¿Las responsabilidades y autoridades para estos procesos han sido asignadas claramente?   + ¿Se abordan los riesgos y oportunidades asociados con estos procesos?   + ¿Los procesos se evalúan regularmente, y se implementan cambios para asegurar que logren los resultados previstos? * ¿Existe un proceso establecido para mejorar continuamente los procesos y el sistema de gestión de la continuidad?   + ¿Se aseguran de la eficacia de los procedimientos desarrollados para responder a incidentes? * ¿Se proporciona formación, educación y desarrollo adecuado para las personas asignadas a roles en el SGCN?   + ¿La organización exige a los contratistas que demuestren competencias requeridas para el SGCN y para los roles que desempeñan?   + ¿Existe un proceso para identificar e impartir los requisitos de formación, y se evalúa la eficiencia de su impartición? * ¿La organización ha identificado adecuadamente los recursos necesarios para el SGCN?   + ¿Estos recursos son adecuados para lograr la política y los objetivos de continuidad del negocio?   + ¿Se asegura de que los recursos pueden adaptarse a los requisitos cambiantes de la organización?   + ¿Los recursos permiten una comunicación eficiente, tanto interna como externa, sobre los asuntos del SGCN?   + ¿Están destinados a garantizar la operación y las mejoras continuas del SGCN?   + ¿Se garantiza que los recursos estarán disponibles de manera puntual y eficaz? * ¿Se han provisto cantidades suficientes de personal y recursos relacionados, como tiempo para cumplir con roles y responsabilidades del SGCN?   + ¿Se garantiza el tiempo necesario para la formación, educación, toma de conciencia y ejercicios?   + ¿Existe una gestión adecuada del personal del SGCN?   + ¿Se han asegurado de contar con instalaciones adecuadas, incluyendo ubicaciones e infraestructuras de trabajo?   + ¿La organización tiene sistemas de Tecnologías de la Información y Comunicación que respalden una gestión eficaz y eficiente del programa? |

|  |
| --- |
| Temática: Documentación y mejoras |
| Se debe asegurar la correcta documentación de incidentes y fallas de sistemas además de que tomaran acciones para evitar incidentes similares a futuro.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización lleva a cabo revisiones periódicas de los recursos y su asignación para asegurarse de que son suficientes?   + ¿Se realiza un monitoreo del uso de recursos con largos plazos de adquisición o costos elevados?   + ¿Los gestores, propietarios de servicios o productos supervisan la utilización de recursos clave del sistema? * ¿La organización documenta la formación recibida por su personal?   + ¿Existe un proceso para el seguimiento continuo de la formación recibida por el personal? * La organización realiza pruebas de estrés de manera regular en los sistemas y servicios para confirmar que existe suficiente capacidad del sistema para cumplir con los requisitos de rendimiento máximo   + ¿Con qué frecuencia se llevan a cabo estas pruebas de estrés?   + ¿Se documentan los resultados de estas pruebas y se toman acciones correctivas basadas en los hallazgos?   + ¿La organización utiliza esta información sobre la capacidad para identificar y prevenir posibles limitaciones de recursos? * ¿Se evalúan las dependencias de personal clave como parte de esta identificación de limitaciones?   + ¿Se planifican y aplican medidas adecuadas para abordar las limitaciones identificadas? * ¿La organización proyecta las futuras necesidades de capacidad teniendo en cuenta las nuevas necesidades de la empresa y del sistema?   + ¿Se tienen en cuenta las tendencias actuales y previstas en las capacidades de procesamiento de información de la organización al realizar estas proyecciones?   + ¿La organización realiza evaluaciones de la formación recibida en relación con las necesidades y requisitos definidos? * ¿Se verifica la conformidad de la formación recibida con los requisitos de formación del Sistema de Gestión de Continuidad del Negocio (SGCN)?   + ¿Se implementan acciones correctivas en caso de desviaciones respecto a los requisitos de formación del SGCN? |