

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Comunicación y Coordinación**

**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

Una comunicación eficaz es clave para garantizar que la organización pueda coordinar su respuesta a eventos disruptivos, mantener la transparencia con las partes interesadas y cumplir con las obligaciones legales y reglamentarias. Los procedimientos de comunicación deben ser claros, estructurados y adaptados a las necesidades de cada público objetivo. Desde una perspectiva de auditoría, es esencial que estos procedimientos estén documentados y se implementen de manera coherente para mitigar los riesgos asociados con la mala gestión de la comunicación.

**1.1 Requisitos de Comunicación con Terceras Partes**

La organización debe identificar los requisitos específicos para la comunicación con entidades gubernamentales, reguladores y otras partes externas. Esto incluye establecer umbrales de notificación obligatoria y voluntaria, determinar las áreas de interés de cada entidad y designar a las personas responsables de interactuar con ellas. También es importante definir los medios y canales de comunicación que se utilizarán para garantizar una transmisión eficiente de la información. Un auditor verificará si estos requisitos están claramente definidos y si los procesos para cumplir con ellos están documentados.

**1.2 Gestión y Coordinación durante Incidentes**

Los procedimientos de comunicación durante un incidente deben detallar cómo la organización se comunicará con empleados, familiares, medios de comunicación y otras partes interesadas. Esto incluye desarrollar una estrategia de comunicación mediática, designar portavoces capacitados y mantener un enfoque coherente en todos los mensajes externos. Desde la perspectiva de auditoría, es importante revisar si estos procedimientos están alineados con la estrategia general de continuidad del negocio y si se han probado para garantizar su efectividad.

**1.3 Manejo de Partes Interesadas**

Se debe establecer un procedimiento separado para gestionar las partes interesadas, asignando prioridades y designando responsables para cada grupo. Esto asegura que las necesidades y expectativas de cada parte interesada se aborden de manera efectiva, minimizando los riesgos de malentendidos o falta de información. Un auditor evaluará si este procedimiento está documentado y si se implementa de manera coherente durante los incidentes.

**1.4 Documentación y Plan de Comunicación**

El plan de comunicación debe documentar todos los puntos de contacto externos y detallar cómo se dirigirán los mensajes a los distintos públicos, incluyendo empleados, familiares, medios de comunicación, inversores, reguladores y vecinos. Este plan debe adaptarse a las necesidades específicas de cada audiencia y garantizar que la información sea accesible y relevante. Un auditor revisará si el plan es integral y si incluye referencias al Sistema de Gestión de Continuidad del Negocio (SGCN).

**1.5 Inclusión en Programas de Toma de Conciencia**

La organización debe integrar disposiciones de continuidad del negocio en boletines y sesiones informativas dirigidas a proveedores y clientes. Esto incluye proporcionar comunicación externa eficaz dentro del programa de toma de conciencia y durante la respuesta a incidentes. Desde el punto de vista de auditoría, es crucial garantizar que estas disposiciones se implementen y que las partes externas relevantes estén informadas de las estrategias de continuidad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar requisitos de comunicación que se deben tener en cuenta al momento de involucrar a terceras partes en la comunicación. Se deben responder a preguntas como:  1.1 ¿Qué entidades gubernamentales deben ser contactadas después de un evento?  1.2 ¿Qué umbrales existen para la notificación obligatoria? ¿Y bajo qué circunstancias la organización haría una notificación voluntaria?  1.3 ¿Qué áreas de preocupación tendrá cada agencia, y ¿En qué se diferenciarán o se parecerán?  1.4 ¿Cómo puede la organización involucrar a las entidades gubernamentales durante el proceso de planificación o ejercicio para beneficiarse desde su experiencia sin comprometer la independencia de la organización?  1.5 ¿Qué requisitos del programa de continuidad existen por parte de las agencias reguladoras y cómo la organización los cumple?   1.6 ¿Existen agencias externas que deban revisar o aprobar estrategias de continuidad, como producir productos temporalmente en una instalación no certificada, realizar funciones reguladas fuera de una geografía separada, o alterar la forma en que las materias primas o productos terminados ¿Los productos ingresan al país?  1.7 ¿Qué medio de comunicación se utilizará para hacer efectiva la comunicación?  1.8 Dentro de la organización, ¿Quién interactuará con cada entidad gubernamental y ¿cómo?  2. Gestionar y coordinar las comunicaciones que se entreguen y reciban durante el incidente. Los procedimientos deberían contener:  2.1 Detalles sobre cómo y en qué circunstancias la organización se comunicará con los empleados y sus familiares, otras partes interesadas y los contactos de emergencia.  2.2 Detalles sobre la respuesta mediática de la organización tras un incidente, que pueden incluir:  2.2.1 La estrategia de comunicación de incidentes.  2.2.2 El punto de contacto preferente con los medios de comunicación.  2.2.3 Directrices o una plantilla para elaborar una declaración para los medios de comunicación.  2.2.4 Una cantidad adecuada de portavoces formados y competentes que estén autorizados para transmitir información a los medios de comunicación.  3. Desarrollar un procedimiento separado para gestionar las partes interesadas, proporcionar criterios de establecimiento de prioridades y adoptar disposiciones para asignar a personas a cada parte interesada o grupo de ellas. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Documentar cada uno de los puntos de contacto con agencias externas. 2. Documentar el plan de comunicación para ser dirigido a:  2.1 Miembros del equipo de respuesta de la organización.  2.2 Gerentes responsables de continuar con las operaciones y interactuar con los empleados.  2.3 Empleados de línea cuya comprensión del panorama más amplio puedan ser menos completos que el equipo de gestión.  2.4 Familiares de los empleados, especialmente familiares. de miembros de los empleados directamente afectados por el evento o la respuesta de la organización.  2.5 Medios de comunicación nacionales, incluidos los medios financieros, cuyo interés en la organización se centra principalmente en la gestión del evento actual.  2.6 Medios locales, tanto impresos como audiovisuales, que cubren la organización regularmente sobre una amplia variedad de temas.  2.7 Los inversores, especialmente los inversores institucionales, que Desean transparencia en las ramificaciones a corto y largo plazo de un incidente.  2.8 Gobiernos locales y estatales/provinciales que están interesado en la viabilidad a largo plazo de la base imponible y otros beneficios que la organización aporta a sus constituyentes.  2.9 Agencias reguladoras responsables de garantizar cumplimiento continuo incluso cuando se opera en modo de recuperación.  2.10 Vecinos que puedan verse afectados negativamente por la evento, la respuesta de la organización o las autoridades. 3. La organización puede incluir referencias a su sistema de gestión de continuidad del negocio y a las disposiciones de continuidad del negocio en los boletines y las sesiones informativas para los proveedores y clientes.  3.1 La organización debe proporcionar una comunicación externa eficaz dentro de su programa de toma de conciencia, así como al responder a un incidente. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. |  |
| 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 la Comunicación y Coordinación**

|  |
| --- |
| Temática: Medios de Comunicación |
| Implica realizar una revisión exhaustiva de los recursos y canales de comunicación utilizados para asegurar la disponibilidad y eficacia de la información durante situaciones adversas. Esto incluye evaluar la diversidad y redundancia de los medios, como redes de comunicación, sistemas de telecomunicaciones, plataformas de colaboración y canales de difusión de información crítica. La auditoría busca confirmar que estos medios estén diseñados para resistir posibles fallas y garantizar la continuidad de las operaciones. Además, implica verificar la integración de los medios con otros elementos del plan de continuidad, como sistemas de respaldo y recuperación, y evaluar la capacidad de adaptación de los medios a escenarios cambiantes. La eficacia de los protocolos de comunicación y la disponibilidad de recursos tecnológicos clave son aspectos centrales que se examinan para fortalecer la capacidad de la organización para mantener operaciones fluidas incluso en condiciones adversas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha identificado todas las situaciones en las que es necesario comunicarse como parte de su Sistema de Gestión de la Continuidad del Negocio (SGCN)? * ¿Se han identificado y categorizado a las partes interesadas clave que deben ser informadas durante una crisis, teniendo en cuenta la naturaleza de la organización y sus obligaciones legales? * ¿La organización ha establecido canales de comunicación efectivos para diferentes tipos de situaciones de crisis, considerando la naturaleza de la organización y las expectativas de las partes interesadas? * ¿Existen mensajes clave predefinidos para diferentes escenarios de crisis y están disponibles para su uso inmediato? |

|  |
| --- |
| Temática: Procedimiento de Comunicación |
| Implica examinar críticamente los protocolos y procesos establecidos para la transmisión efectiva de información durante situaciones disruptivas. Esto abarca la revisión detallada de los planes de comunicación, identificación de las partes interesadas clave, y evaluación de la claridad y accesibilidad de los procedimientos en momentos de crisis. La auditoría se centra en asegurar que los protocolos estén alineados con los objetivos de continuidad del negocio, facilitando la coordinación eficiente entre equipos y departamentos. Además, implica la validación de la capacidad del personal para activar y seguir los procedimientos de comunicación de manera rápida y precisa, promoviendo así una respuesta organizativa coherente y efectiva ante eventos adversos. La revisión de la documentación y la retroalimentación de simulacros o eventos pasados contribuyen a mejorar y fortalecer los procedimientos para garantizar una comunicación resiliente en escenarios de crisis.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha realizado una revisión exhaustiva de los procedimientos de comunicación en el plan de continuidad del negocio?   + Realice una revisión detallada del plan de continuidad del negocio, centrándose en los procedimientos de comunicación. Analice la documentación para identificar la claridad de las instrucciones, la inclusión de roles y responsabilidades, y la coherencia con los objetivos de continuidad.     - ¿Cuándo fue la última revisión exhaustiva del plan de continuidad del negocio, centrándose específicamente en los procedimientos de comunicación, y qué hallazgos clave surgieron de esa revisión? * ¿Los procedimientos de comunicación están alineados con las necesidades específicas de la organización?   + Realice entrevistas con el personal clave para comprender las necesidades particulares de comunicación durante interrupciones.   + Evalúe si los procedimientos existentes satisfacen estas necesidades y, si es necesario, proponer ajustes para garantizar que la comunicación se adapte a las circunstancias específicas de la organización.     - ¿Cómo se han identificado y evaluado las necesidades específicas de comunicación de la organización para asegurar que los procedimientos estén alineados con estas necesidades? * ¿El personal está debidamente capacitado y familiarizado con los procedimientos de comunicación de continuidad del negocio?   + Realice sesiones de capacitación y concientización para el personal sobre los procedimientos de comunicación durante eventos de continuidad. Proporcionar material educativo y realizar simulacros para garantizar que el personal esté bien preparado y pueda ejecutar los procedimientos de manera efectiva.     - ¿Cuál es el enfoque actual para la capacitación del personal en relación con los procedimientos de comunicación de continuidad del negocio, y cómo se asegura de que estén debidamente preparados y familiarizados? * ¿Se han llevado a cabo simulacros o pruebas de los procedimientos de comunicación?   + Organice simulacros regulares o pruebas de los procedimientos de comunicación. Evaluar el rendimiento del personal, identificar posibles puntos de mejora y garantizar que los procedimientos sean efectivos en la práctica.     - ¿Se han llevado a cabo simulacros o pruebas recientes de los procedimientos de comunicación durante eventos de continuidad, y qué lecciones se han aprendido de estas actividades? * ¿Existe un mecanismo claro para la retroalimentación y la mejora continua de los procedimientos de comunicación?   + Establecer un proceso formal de retroalimentación y revisión de los procedimientos de comunicación. Recopilar comentarios del personal y partes interesadas clave después de eventos de continuidad o simulacros.     - ¿Existe un proceso establecido para recopilar y utilizar la retroalimentación del personal y otras partes interesadas después de eventos de continuidad o simulacros, y cómo se ha traducido esta retroalimentación en mejoras concretas en los procedimientos de comunicación? |

|  |
| --- |
| Temática: Procedimiento de Comunicación |
| Implica examinar críticamente los protocolos y procesos establecidos para la transmisión efectiva de información durante situaciones disruptivas. Esto abarca la revisión detallada de los planes de comunicación, identificación de las partes interesadas clave, y evaluación de la claridad y accesibilidad de los procedimientos en momentos de crisis. La auditoría se centra en asegurar que los protocolos estén alineados con los objetivos de continuidad del negocio, facilitando la coordinación eficiente entre equipos y departamentos. Además, implica la validación de la capacidad del personal para activar y seguir los procedimientos de comunicación de manera rápida y precisa, promoviendo así una respuesta organizativa coherente y efectiva ante eventos adversos. La revisión de la documentación y la retroalimentación de simulacros o eventos pasados contribuyen a mejorar y fortalecer los procedimientos para garantizar una comunicación resiliente en escenarios de crisis.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha realizado una revisión exhaustiva de los procedimientos de comunicación en el plan de continuidad del negocio?   + Realice una revisión detallada del plan de continuidad del negocio, centrándose en los procedimientos de comunicación. Analice la documentación para identificar la claridad de las instrucciones, la inclusión de roles y responsabilidades, y la coherencia con los objetivos de continuidad.     - ¿Cuándo fue la última revisión exhaustiva del plan de continuidad del negocio, centrándose específicamente en los procedimientos de comunicación, y qué hallazgos clave surgieron de esa revisión? * ¿Los procedimientos de comunicación están alineados con las necesidades específicas de la organización?   + Realice entrevistas con el personal clave para comprender las necesidades particulares de comunicación durante interrupciones.   + Evalúe si los procedimientos existentes satisfacen estas necesidades y, si es necesario, proponer ajustes para garantizar que la comunicación se adapte a las circunstancias específicas de la organización.     - ¿Cómo se han identificado y evaluado las necesidades específicas de comunicación de la organización para asegurar que los procedimientos estén alineados con estas necesidades? * ¿El personal está debidamente capacitado y familiarizado con los procedimientos de comunicación de continuidad del negocio?   + Realice sesiones de capacitación y concientización para el personal sobre los procedimientos de comunicación durante eventos de continuidad. Proporcionar material educativo y realizar simulacros para garantizar que el personal esté bien preparado y pueda ejecutar los procedimientos de manera efectiva.     - ¿Cuál es el enfoque actual para la capacitación del personal en relación con los procedimientos de comunicación de continuidad del negocio, y cómo se asegura de que estén debidamente preparados y familiarizados? * ¿Se han llevado a cabo simulacros o pruebas de los procedimientos de comunicación?   + Organice simulacros regulares o pruebas de los procedimientos de comunicación. Evaluar el rendimiento del personal, identificar posibles puntos de mejora y garantizar que los procedimientos sean efectivos en la práctica.     - ¿Se han llevado a cabo simulacros o pruebas recientes de los procedimientos de comunicación durante eventos de continuidad, y qué lecciones se han aprendido de estas actividades? * ¿Existe un mecanismo claro para la retroalimentación y la mejora continua de los procedimientos de comunicación?   + Establecer un proceso formal de retroalimentación y revisión de los procedimientos de comunicación. Recopilar comentarios del personal y partes interesadas clave después de eventos de continuidad o simulacros.     - ¿Existe un proceso establecido para recopilar y utilizar la retroalimentación del personal y otras partes interesadas después de eventos de continuidad o simulacros, y cómo se ha traducido esta retroalimentación en mejoras concretas en los procedimientos de comunicación? |

|  |
| --- |
| Temática: Seguridad en la Comunicación |
| Implica examinar detenidamente las medidas y controles implementados para garantizar la confidencialidad, integridad y disponibilidad de la información transmitida durante eventos disruptivos. Esto incluye la evaluación de los protocolos de cifrado utilizados, la resistencia contra posibles ataques cibernéticos durante situaciones de crisis, y la revisión de las salvaguardias implementadas para proteger la infraestructura de comunicaciones. Además, la auditoría se centra en verificar que los canales de comunicación críticos estén protegidos contra posibles amenazas, como la interceptación no autorizada, y que se cumplan los estándares de seguridad establecidos. Garantizar la seguridad en la comunicación es esencial para mantener la confianza en la integridad de la información durante eventos que puedan afectar la continuidad del negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cuál es el protocolo de cifrado utilizado para proteger las comunicaciones críticas durante situaciones de continuidad del negocio?   + Revise la configuración de los protocolos de cifrado utilizados en los canales de comunicación críticos.   + Evalúe la robustez y actualización de estos protocolos para asegurar la confidencialidad de la información en tránsito.     - ¿Cuál es el protocolo de cifrado actualmente implementado en los canales de comunicación críticos durante situaciones de continuidad del negocio, y cómo se asegura de que cumple con los estándares de seguridad necesarios? * ¿Cómo se protegen los canales de comunicación contra posibles ataques cibernéticos durante situaciones de crisis?   + Realice pruebas de penetración controladas para evaluar la resistencia de los canales de comunicación a posibles ataques cibernéticos. Identificar posibles vulnerabilidades y garantizar que se hayan implementado medidas de seguridad adecuadas, como firewalls y sistemas de detección de intrusiones.     - ¿Cuáles son las medidas específicas implementadas para proteger los canales de comunicación contra posibles ataques cibernéticos durante eventos de continuidad del negocio, y cómo se verifica su efectividad? * ¿Se han establecido salvaguardias para proteger la infraestructura de comunicaciones durante eventos disruptivos?   + Evaluar la implementación y eficacia de las salvaguardias, como redundancia de enlaces y sistemas de respaldo, para garantizar la disponibilidad y la integridad de la infraestructura de comunicaciones.   + Realice una revisión exhaustiva de los planes de contingencia para identificar posibles mejoras en la seguridad de la infraestructura de comunicación.     - ¿Cuáles son las salvaguardias establecidas para proteger la infraestructura de comunicaciones durante eventos disruptivos, y cómo se garantiza su adecuada implementación y eficacia? * ¿Cómo se verifica que los canales de comunicación críticos estén protegidos contra amenazas como la interceptación no autorizada?   + Realice análisis de tráfico y monitoreo de seguridad para identificar posibles intentos de interceptación no autorizada.   + Revise los registros de eventos de seguridad para detectar comportamientos anómalos y asegurar que los canales críticos estén protegidos contra amenazas externas.     - ¿Cómo se verifica regularmente que los canales de comunicación críticos estén protegidos contra amenazas como la interceptación no autorizada, y qué medidas se toman en respuesta a posibles anomalías detectadas? * ¿Se cumplen los estándares de seguridad establecidos para la protección de la comunicación durante eventos que puedan afectar la continuidad del negocio?   + Realice una revisión comparativa de los estándares de seguridad establecidos y la implementación actual en los canales de comunicación. Identificar posibles brechas de cumplimiento y proponer medidas correctivas para garantizar la conformidad con los estándares de seguridad relevantes.     - ¿Cuál es el proceso para garantizar que la implementación de los canales de comunicación cumpla con los estándares de seguridad establecidos, y cómo se abordan las posibles brechas de cumplimiento identificadas durante la auditoría? |