

**GASIC 10 – Continuidad del Negocio**

**Preguntas de Auditoría**

**Planes y Controles de Continuidad**

**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

Los planes y controles de continuidad del negocio son esenciales para garantizar que las organizaciones puedan responder eficazmente a interrupciones, mantener operaciones críticas y recuperarse dentro de los tiempos previstos. Estos planes deben ser claros, flexibles y alineados con los objetivos organizacionales, asegurando una gestión eficiente de incidentes y el cumplimiento de requisitos normativos y contractuales. Desde una perspectiva de auditoría, es crucial verificar que estos planes estén documentados, implementados y sujetos a mejora continua.

* 1. **Estructura de Respuesta y Procedimientos**

La organización debe contar con una estructura de respuesta basada en planes y procedimientos que permitan controlar las disrupciones, comunicarse eficazmente con las partes interesadas y utilizar las soluciones de continuidad para reanudar actividades dentro del RTO. Estos planes deben identificar pasos inmediatos, asignar roles y responsabilidades claras, y ser lo suficientemente flexibles para adaptarse a situaciones imprevistas. Un auditor verificará si los planes están documentados y si cumplen con estos requisitos fundamentales.

* 1. **Mecanismos de Control**

Es necesario establecer controles dentro de los procesos de continuidad del negocio para planificar, implementar y monitorear su ejecución. Esto incluye decidir cómo se gestionarán estos procesos, establecer hitos y mantener documentación que demuestre su cumplimiento. Desde una perspectiva de auditoría, se debe garantizar que los controles sean consistentes y que se mantengan registros adecuados para respaldar las decisiones y actividades realizadas.

* 1. **Comunicación y Gestión de Información**

Los procedimientos de comunicación deben incluir estrategias para alertar a las partes interesadas, gestionar las respuestas mediáticas, registrar información clave sobre los incidentes y coordinar con los servicios de emergencia. Estos procedimientos deben detallar quién será responsable de cada acción y asegurar la disponibilidad de equipos de comunicación adecuados. Un auditor evaluará si las estrategias de comunicación son coherentes con la política organizacional y si están alineadas con los objetivos de continuidad.

* 1. **Controles Preventivos y Compensatorios**

Es esencial implementar controles preventivos para mitigar los impactos de las interrupciones, mantener los controles existentes durante incidentes y desarrollar controles compensatorios para aquellos que no puedan sostenerse. Estos controles deben alinearse con los resultados del análisis de impacto y garantizar la protección de la seguridad de la información. Desde el punto de vista de auditoría, es crucial revisar si estos controles están documentados y si son efectivos para minimizar los riesgos.

* 1. **Documentación de Planes de Continuidad**

Cada plan de continuidad debe detallar su propósito, alcance y objetivos, incluyendo roles y responsabilidades, criterios de activación, requisitos de recursos y métodos de comunicación. Además, los planes deben ser accesibles en todo momento y actualizados según sea necesario. Los auditores revisarán si la documentación es clara, está completa y refleja las interdependencias internas y externas de la organización.

* 1. **Evaluación y Mejora Continua**

La organización debe revisar regularmente sus procedimientos documentados, gestionar cambios planificados y abordar cualquier deficiencia identificada durante incidentes o ejercicios de simulación. Esto incluye la extracción de lecciones aprendidas y su incorporación en los planes existentes para mejorar su efectividad. Desde una perspectiva de auditoría, es importante verificar si las revisiones se realizan de manera consistente y si los planes se ajustan según los resultados obtenidos.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | **1. La organización debe tener una estructura de respuesta apoyada en planes y procedimientos de continuidad del negocio para:**  **1.1 Controlar la respuesta a la disrupción.**  **1.2 Comunicarse de manera eficaz con las partes interesadas.**  **1.3 Utilizar las soluciones de continuidad del negocio para reanudar las actividades dentro del objetivo de tiempo de recuperación (R**TO). **2. Asegurar que los planes y procedimientos de continuidad cumplan con:**  **2.1 Identificar los pasos inmediatos que deben darse y ayudar en la toma de decisiones puntual.**  **2.2 Ser lo bastante flexibles para adaptarse a amenazas imprevistas y situaciones cambiantes.**  **2.3 Centrarse en los impactos previstos de las disrupciones.**  **2.4 Estar alineados con las soluciones de continuidad del negocio seleccionadas por la organización para minimizar los impactos.**  **2.5 Identificar con claridad los roles y asignar las responsabilidades para todas las tareas que hay que realizar.** **3. Establecer mecanismos de control dentro de los procesos necesarios para establecer y mantener una gestión de la continuidad del negocio que incluyan:**  **3.1 Decidir cómo se deberían determinar, planificar, implantar y controlar estos procesos.**  **3.2 Asegurarse de que se implanten controles de estos procesos de conformidad con las decisiones adoptadas, por ejemplo, al establecer los hitos del proyecto y especificar los resultados requeridos;**  **3.3 Mantener información documentada para demostrar que los procesos se han llevado a cabo según lo planificado.** 4. La organización debe establecer procedimientos documentados para las siguientes acciones de aviso y comunicación e identificar quiénes serán responsables de llevarlas a cabo:  4.1 Encargarse de la comunicación interna entre los distintos niveles y funciones de la organización, lo que incluye la estructura de respuesta.  4.2 Alertar a las partes interesadas, así como recepción, documentación y respuestas a las comunicaciones procedentes de ellas.  4.3 Asegurarse de que los equipos e instalaciones de comunicaciones estén disponibles.  4.4 Facilitar comunicaciones estructuradas con los servicios de emergencias.  4.5 Gestionar las respuestas de la organización a los medios de comunicación y asegurarse de que sea coherente con la estrategia de comunicaciones de la organización.  4.6 Registrar la información vital sobre el incidente, las acciones realizadas y las decisiones adoptadas. 5. Implementar y mantener dentro de la organización:  5.1 Controles preventivos para mitigar los impactos de las interrupciones identificados en el análisis de impacto, según el tipo y la configuración del sistema.  5.2 Controles de seguridad de la información, sistemas de soporte y herramientas dentro de la continuidad del negocio y las tecnologías de información.  5.3 Procesos para mantener los controles de seguridad de la información existentes durante la interrupción.  5.4 Controles compensatorios para los controles de seguridad de la información que no pueden mantenerse durante ruptura. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Preparar procedimientos documentados para actividades operativas de organización asociadas a seguridad de información. Los procedimientos operativos deben especificar:  1.1 Las personas responsables.  1.2 La instalación y configuración seguras de sistemas.  1.3 Procesamiento y tratamiento de información como manual.  1.4 Copia de seguridad y la capacidad de recuperación.  1.5 Requisitos de programación, incluyendo interdependencias con otros sistemas.  1.6 Instrucciones para tratar errores u otras condiciones excepcionales (por ejemplo, restricciones en uso de programas de utilidad), que pueden surgir durante la ejecución del trabajo.  1.7 Contactos de apoyo y escalada, incluyendo contactos de apoyo externo en caso de dificultades operativas o técnicas inesperadas.  1.8 Instrucciones de manipulación de los medios de almacenamiento.  1.9 Procedimientos de reinicio y recuperación de sistema para su uso en caso de fallo de este.  1.10 La gestión de información de pista de auditoría y de registro de sistema y sistemas de vigilancia por video.  1.11 Procedimientos de control, como capacidad, rendimiento y seguridad.  1.12 Instrucciones de mantenimiento. 2. Documentar cada plan de continuidad del negocio, el cual debe identificar su finalidad, campo de aplicación y objetivos de un modo que resulte claro a los equipos que lo usen.   2.1 Los enlaces a otros procedimientos documentados requeridos o pertinentes deben indicarse claramente y se debe describir el método para obtener acceso a ellos.   2.2 El plan de continuidad del negocio plan debe incluir, además:  2.2.1 Criterios y procedimientos de activación.  2.2.2 Procedimientos de implantación.  2.2.3 Requisitos y procedimientos de comunicación.  2.2.4 Interdependencias e interacciones internas y externas.  2.2.5 Requisitos de recursos.  2.2.6 Requisitos de informes.  2.2.7 Flujo de información y procesos de documentación. 2. Cada plan debe incluir:  2.1 Roles, responsabilidades y autoridades:  2.1.1 Roles, responsabilidades y autoridades definidos para las personas que vayan a usar el plan.  2.1.2 Directrices y criterios relativos a quién tiene autoridad para aplicar el plan y en qué circunstancias.  2.2 Criterios de activación:  2.2.1 Un proceso para activar la respuesta de la organización a la disrupción y, en cada procedimiento documentado, sus criterios y procedimientos de activación.  2.2.2 Locales de reunión con alternativas adecuadas.  2.3 Parámetros de operación:  2.3.1 Identificación de acciones y tareas que han de realizarse, en particular en relación con el modo en que la organización continuará o recuperará sus actividades prioritarias dentro de los plazos predeterminados.  2.3.2 Requisitos de recursos pertinentes.  2.3.3 Medios para registrar la información sobre el incidente, las acciones realizadas y las decisiones adoptadas.  2.4 Información de apoyo a la coordinación y la comunicación:  2.4.1 Datos de contacto de los miembros de los equipos y otras personas con roles y responsabilidades. La organización debe ser consciente de los requisitos legales aplicables en relación con la protección de la información y debe retener pruebas de su cumplimiento.  2.4.2 Datos de contacto y movilización de todos los organismos, organizaciones y recursos pertinentes que puedan necesitarse.  2.5 Criterios de retirada de medidas:  2.5.1 Mecanismos para retirar las medidas una vez que el incidente haya pasado.  2.5.2 Instrucciones que hay que seguir. 3. Al igual que con cualquier forma de información documentada, la organización debe asegurarse de que los planes de continuidad del negocio sean utilizables y estén disponibles en todos los momentos y lugares en que se necesiten. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar y documentar los procedimientos operativos documentados cuando sea necesario.  1.2 Los cambios en procedimientos operativos documentados se deben autorizar.  1.3 Cuando sea técnicamente posible, los sistemas de información se deben gestionar de forma coherente, usando los mismos procedimientos, herramientas y utilidades. 2. La organización se asegurará de que se controlen los cambios planificados, se revisen los cambios imprevistos y se emprendan las acciones apropiadas. 3. La organización tiene que asegurar que se controlen los procesos externalizados y la cadena de suministro. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Al abordar un incidente, puede que deban tenerse en cuenta varias acciones. Estas deben integrarse en los procedimientos documentados e incluir:  1.1 La respuesta a y la evaluación del incidente, lo que incluye:  1.1.1 Determinar qué y cómo ha sucedido.  1.1.2 Identificar qué partes de la organización y partes interesadas se han visto o podrían verse afectadas.  1.1.3 Intentar prever la duración del incidente y sus impactos probables.  1.1.4 Evaluar si el incidente se gestionará mediante las disposiciones de gestión rutinarias.  1.1.5 Determinar, mediante referencia a los umbrales predefinidos, si el incidente podría dar lugar a una disrupción.  1.2 La gestión de las consecuencias inmediatas del incidente, teniendo en cuenta debidamente los aspectos de bienestar de las personas afectadas y los impactos en el medioambiente, así como las posibles opciones para responder al incidente e impedir pérdidas o daños adicionales.  1.3 La evaluación de la evaluación del incidente respecto a los criterios de activación de cada procedimiento.  1.4 La declaración de incidente y la activación de los procedimientos una vez que se cumplan los criterios de activación.  1.5 La movilización del personal de respuesta a incidentes en equipos para que realicen las actividades de estabilización, continuidad y recuperación.  1.6 El establecimiento de una ubicación central para que la utilice el equipo encargado de gestionar y controlar el incidente.  1.7 La priorización de los problemas y las actividades que se deben realizar para gestionar el incidente y sus impactos.  1.8 El control y la coordinación de todos los procedimientos activados.  1.9 La activación o el establecimiento de centros alternativos con el fin de restaurar las capacidades de las infraestructuras de TI y de otro tipo y para operar provisionalmente las actividades de la organización.  1.10 El seguimiento del incidente a medida que evoluciona.  1.11 La revisión y la adaptación de los planes en respuesta a las circunstancias cambiantes.  1.12 La desescalada, la retirada de medidas y la vuelta a las operaciones rutinarias a medida que se recupera la capacidad sostenible.  1.13 La elaboración de un informe y la identificación de oportunidades de aprendizaje.  1.14 El aseguramiento de una gobernanza adecuada y la contrastación y seguridad de la documentación generada durante la gestión y la recuperación del incidente. |
| 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. Utilizar la información obtenida durante los ejercicios y extraer las lecciones aprendidas durante las disrupciones. |

1. **Prácticas de auditoría para los Planes y Controles de Continuidad**

|  |
| --- |
| Temática: Copia de seguridad, la capacidad de recuperación y planes para la continuidad del negocio |
| Evaluar de manera exhaustiva la efectividad de los procedimientos y sistemas implementados para respaldar y recuperar datos críticos en situaciones adversas. Esto incluye revisar la frecuencia y consistencia de las copias de seguridad, la ubicación segura de los datos respaldados, así como la integridad y disponibilidad de estos. Además, se analiza la infraestructura tecnológica y los procesos asociados para garantizar una rápida y eficiente recuperación de sistemas y aplicaciones esenciales. La auditoría abarca pruebas de recuperación periódicas, documentación detallada de los procedimientos, y la alineación de las capacidades de recuperación con las necesidades reales del negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene una estructura de respuesta claramente definida respaldada por planes de continuidad del negocio?   + ¿La respuesta a la disrupción está controlada de acuerdo con los planes y procedimientos establecidos?   + ¿La comunicación con las partes interesadas se realiza de manera eficaz durante situaciones de interrupción?   + ¿La organización utiliza soluciones de continuidad del negocio para reanudar las actividades dentro del objetivo de tiempo de recuperación (RTO)?     - Revise informes de pruebas de recuperación para confirmar la capacidad de la organización para utilizar soluciones de continuidad del negocio en el tiempo previsto. * ¿Los planes y procedimientos de continuidad identifican los pasos inmediatos que deben darse y ayudan en la toma de decisiones puntual?   + Revise los planes de continuidad existentes para verificar si incluyen secciones claras que identifiquen los pasos inmediatos a seguir en caso de interrupción o crisis.   + ¿Los planes y procedimientos son lo bastante flexibles para adaptarse a amenazas imprevistas y situaciones cambiantes?     - ¿Se centran en los impactos previstos de las disrupciones?     - ¿Están alineados con las soluciones de continuidad del negocio seleccionadas para minimizar los impactos? * ¿Se ha definido claramente cómo se determinarán, planificarán, implementarán y controlarán los procesos relacionados con la gestión de la continuidad del negocio?   + ¿Se asegura de que se implanten controles de estos procesos de conformidad con las decisiones adoptadas, como la definición de hitos del proyecto y los resultados requeridos?   + ¿Se mantiene información documentada que demuestre que los procesos se han llevado a cabo según lo planificado? * ¿Cuándo fue la última vez que se realizaron pruebas completas de recuperación ante desastres, y cuáles fueron los resultados obtenidos?   + Revisar los registros de pruebas de recuperación ante desastres y evaluar su exhaustividad. Realizar una simulación de recuperación para verificar la capacidad del sistema para restablecerse después de una interrupción.     - ¿Cómo se garantiza que las pruebas de recuperación ante desastres sean completas y reflejen de manera precisa la capacidad de recuperación del sistema? * ¿Existen procedimientos documentados para la comunicación interna entre los distintos niveles y funciones de la organización, incluyendo la estructura de respuesta?   + ¿Existe un sistema para alertar a las partes interesadas y gestionar las comunicaciones procedentes de ellas?   + ¿Hay medidas establecidas para garantizar la disponibilidad de equipos e instalaciones de comunicaciones?   + ¿Se facilitan comunicaciones estructuradas con los servicios de emergencias? * ¿Cómo se gestionan y protegen las copias de seguridad, y cuáles son los procedimientos para garantizar su integridad y disponibilidad?   + Revise los procedimientos y protocolos de seguridad para la gestión de copias de seguridad. Evalúe la implementación de cifrado, controles de acceso y auditoría de las copias de seguridad para garantizar su integridad y protección contra accesos no autorizados.     - ¿Cuáles son las medidas específicas implementadas para proteger las copias de seguridad, y cómo se asegura la integridad y disponibilidad de estas frente a posibles amenazas? * ¿Existen políticas claras para la retención de datos en las copias de seguridad, y cómo se asegura de que se cumplan adecuadamente?   + Revise las políticas de retención de datos y compararlas con la implementación real en las copias de seguridad. Evalúe la eficacia de los controles automatizados y manuales para garantizar que se cumplan las políticas de retención.     - ¿Cómo se verifica y garantiza el cumplimiento de las políticas de retención de datos en las copias de seguridad, y cuáles son los controles implementados para evitar retenciones excesivas o insuficientes? * ¿Cuál es el procedimiento para la restauración de datos y sistemas a partir de las copias de seguridad, y cómo se verifica su eficacia?   + Simule un escenario de recuperación y evaluar la efectividad del procedimiento de restauración. Analizar los registros y documentación relacionada con restauraciones anteriores para identificar posibles mejoras.     - ¿Cuál es el procedimiento exacto para la restauración de datos y sistemas a partir de las copias de seguridad, y cómo se asegura de que sea eficiente y efectivo? * ¿Se realiza una revisión periódica de la estrategia de copias de seguridad y recuperación ante desastres para asegurar su alineación con los cambios en la infraestructura y las necesidades del negocio?   + Revise la estrategia de copias de seguridad y recuperación ante desastres a la luz de cambios recientes en la infraestructura y las necesidades del negocio.     - ¿Cómo se revisa periódicamente la estrategia de copias de seguridad y recuperación ante desastres para asegurar su alineación con los cambios en la infraestructura y las necesidades del negocio, y cuáles son los ajustes realizados en respuesta a estas revisiones? |

|  |
| --- |
| Temática: La instalación y configuración seguras de sistemas |
| Examinar detalladamente la implementación de medidas de seguridad en los sistemas críticos para garantizar su disponibilidad y funcionalidad durante eventos disruptivos. Esto incluye la revisión de protocolos de instalación para asegurar que se sigan las mejores prácticas de seguridad, la validación de configuraciones para identificar posibles vulnerabilidades y la verificación de la aplicación adecuada de parches y actualizaciones.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cuál es el proceso de instalación de sistemas críticos y cómo se asegura de que se adhiera a las mejores prácticas de seguridad?   + Revise los procedimientos documentados para la instalación de sistemas críticos y compararlos con las mejores prácticas de seguridad reconocidas.     - ¿Cuáles son los protocolos y procedimientos específicos que se siguen durante la instalación de sistemas críticos para garantizar una implementación segura y conforme a las mejores prácticas de seguridad? * ¿Cuáles son los controles de configuración implementados en los sistemas críticos y cómo se verifica su eficacia para prevenir posibles vulnerabilidades?   + Revise la configuración de sistemas críticos en busca de posibles vulnerabilidades y compararla con los estándares de configuración segura.     - ¿Qué medidas concretas se aplican para asegurar la configuración de sistemas críticos y cómo se verifica la eficacia de estos controles para prevenir posibles vulnerabilidades? * ¿Cómo se gestionan las actualizaciones y parches de seguridad en los sistemas críticos, y cuáles son los procedimientos para verificar su implementación oportuna?   + Revise los procesos de gestión de parches y actualizaciones, y evaluar la implementación de las últimas actualizaciones en un sistema crítico seleccionado.     - ¿Cuál es el proceso establecido para gestionar las actualizaciones y parches de seguridad en los sistemas críticos, y cómo se asegura de que estas actualizaciones se implementen de manera oportuna? * ¿Cómo se gestiona y audita el acceso a los sistemas críticos, y cuáles son los controles implementados para garantizar privilegios mínimos y monitorear actividades de usuario?   + Revise los controles de acceso implementados en los sistemas críticos y realizar una auditoría de los registros de acceso.     - ¿Cuáles son los procedimientos y controles utilizados para gestionar el acceso a los sistemas críticos, y cómo se asegura de que los usuarios tengan privilegios mínimos necesarios? * ¿Cuál es el proceso para la configuración de firewalls y filtros de red en los sistemas críticos, y cómo se verifica que estén alineados con las políticas de seguridad?   + Revise la configuración de firewalls y filtros de red en los sistemas críticos y compararla con las políticas de seguridad establecidas. Realice pruebas de penetración controladas para evaluar la eficacia de las medidas de seguridad perimetral.     - ¿Cómo se lleva a cabo la configuración de firewalls y filtros de red en los sistemas críticos, y cuál es el proceso para verificar que estas configuraciones estén alineadas con las políticas de seguridad establecidas? |

|  |
| --- |
| Temática: Criterios y procedimientos de activación |
| Implica examinar minuciosamente los protocolos establecidos para la puesta en marcha de los planes de continuidad. Esto abarca la revisión de los criterios que determinan cuándo activar estos planes, considerando factores como la gravedad de la interrupción, el impacto en las operaciones y la evaluación de riesgos. Además, implica analizar los procedimientos detallados que guían la ejecución de las acciones específicas durante la activación, asegurándose de que sean claros, actualizados y alineados con los objetivos de continuidad del negocio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cuáles son los criterios establecidos para la activación de los planes de continuidad del negocio y cómo se asegura de que sean adaptativos a diferentes escenarios de interrupción?   + Revise los criterios de activación documentados y compararlos con los riesgos y amenazas actuales.   + Realice entrevistas con los responsables de la gestión de la continuidad del negocio para comprender la lógica detrás de los criterios y su capacidad para adaptarse a situaciones cambiantes.     - ¿Cómo se garantiza que los criterios de activación de los planes de continuidad del negocio se revisen periódicamente para reflejar cambios en el entorno operativo y amenazas emergentes? * ¿Cómo se comunican y verifican los procedimientos detallados para la activación de los planes de continuidad del negocio, y cuál es el proceso para su actualización y revisión continua?   + Revise la documentación de procedimientos de activación y compararla con las mejores prácticas y estándares de la industria.   + Realice entrevistas con el equipo encargado de la continuidad del negocio para comprender cómo se comunica y valida la comprensión de los procedimientos.     - ¿Cuál es el enfoque para asegurar que los procedimientos detallados de activación se comuniquen de manera efectiva a todo el personal clave y cómo se gestionan las actualizaciones y revisiones continuas? * ¿Cuál es el proceso para entrenar al personal en la activación de los planes de continuidad del negocio y cómo se verifica la competencia de los equipos designados?   + Verifique los registros de entrenamiento del personal en relación con la activación de los planes de continuidad.   + Realice simulacros de activación controlados para evaluar la capacidad del personal para seguir los procedimientos establecidos.     - ¿Cómo se planifica y ejecuta el entrenamiento del personal en la activación de los planes de continuidad del negocio, y cuáles son los indicadores utilizados para evaluar la competencia del personal? * ¿Cómo se realiza la simulación y revisión posterior de eventos de activación de los planes de continuidad del negocio, y cuáles son los mecanismos para aprender y mejorar basándose en estas experiencias?   + Evalúe los registros de simulacros pasados y analizar las revisiones posteriores a eventos de activación.     - ¿Cuál es el proceso formal para realizar revisiones después de simulacros de activación o eventos reales, y cómo se aplican las lecciones aprendidas para mejorar la preparación y respuesta futuras? * ¿Cómo se realiza la coordinación con partes interesadas externas durante la activación de los planes de continuidad del negocio, y cómo se asegura la colaboración efectiva con socios y proveedores clave?   + Evalúe los procedimientos para la coordinación con partes interesadas externas y verificar la existencia de acuerdos de colaboración formalizados.   + Realice entrevistas con los responsables de relaciones externas y revisar la documentación contractual relacionada.     - ¿Cómo se establecen y mantienen relaciones colaborativas con socios y proveedores clave para asegurar una activación eficiente de los planes de continuidad del negocio en situaciones que involucren a terceros? |