

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Comunicación con Terceros**

**Competencias Básicas del Auditor**

* **Conocimiento Profundo en Gestión de Incidentes de Seguridad:** Entender los principios y mejores prácticas en la gestión de incidentes de seguridad, incluyendo la identificación, contención, erradicación, y recuperación de incidentes.
* **Experiencia en Identificación y Clasificación de Incidentes**: Tener habilidades para identificar, clasificar y priorizar incidentes de seguridad, diferenciando entre eventos menores y amenazas críticas, y asignando los recursos apropiados.
* **Conocimiento en Normativas y Estándares de Gestión de Incidentes**: Estar familiarizado con normativas y estándares internacionales relacionados con la gestión de incidentes, como ISO/IEC 27035, NIST SP 800-61, y las políticas internas de la organización.
* **Habilidades en Evaluación de Impacto y Riesgo**: Ser capaz de evaluar el impacto y los riesgos asociados con los incidentes de seguridad, considerando la criticidad de los activos afectados y la potencial repercusión en la organización.
* **Conocimientos en Técnicas de Contención y Erradicación**: Comprender las diversas técnicas y herramientas utilizadas para contener y erradicar incidentes de seguridad de manera eficaz y con el menor impacto posible en las operaciones.
* **Capacidad Analítica para la Investigación de Incidentes**: Ser capaz de analizar y correlacionar datos de incidentes para identificar la causa raíz, tendencias de ataques, y posibles brechas en las defensas de seguridad.
* **Habilidades de Comunicación en Situaciones de Crisis**: Ser capaz de comunicar de manera clara y efectiva durante incidentes de seguridad, tanto a nivel técnico como ejecutivo, garantizando que todos los interesados estén informados y alineados en la respuesta.
* **Conocimiento en Recuperación y Aprendizaje Post-Incidente**: Entender los procesos de recuperación tras un incidente, incluyendo la restauración de sistemas, la revisión de lecciones aprendidas, y la implementación de mejoras preventivas.

# Visión General

Establecer procedimientos claros para interactuar con partes externas, documentar comunicaciones y compartir información relevante ayuda a minimizar el impacto de los incidentes y a fomentar la colaboración en la detección y análisis de amenazas. Desde el punto de vista de auditoría, es esencial que estos procesos estén bien definidos, sean consistentes y cumplan con las políticas organizacionales.

**1.1 Procedimientos y Canales de Comunicación**

La organización debe definir y comunicar procedimientos específicos para responder a incidentes de seguridad, asegurando que todas las partes interesadas pertinentes, tanto internas como externas, estén informadas de cómo reportar y manejar incidentes. Esto incluye mantener actualizada la información de contacto para notificaciones rápidas y efectivas. Desde la perspectiva de auditoría, es crucial revisar si los procedimientos están documentados y si se han comunicado adecuadamente a las partes interesadas.

**1.2 Comunicación con Partes Externas**

Los detalles del incidente deben compartirse con partes externas relevantes, como medios de comunicación, agencias de aplicación de la ley y organizaciones especializadas en informes de incidentes, siguiendo los lineamientos establecidos. La información proporcionada debe ser precisa y adecuada para cada audiencia, respetando las normativas aplicables y evitando la divulgación innecesaria de datos sensibles. Un auditor verificará si las comunicaciones externas se han realizado siguiendo los procedimientos establecidos y si los registros correspondientes están documentados.

**1.3 Documentación y Métricas de Comunicación**

Todos los contactos y comunicaciones con terceros deben ser documentados para asegurar la trazabilidad, la responsabilidad y la generación de evidencia en caso de auditorías o investigaciones posteriores. Esto incluye mantener métricas que evalúen si la información se comunicó adecuadamente y mediante los canales establecidos. Desde el punto de vista de auditoría, estas métricas son fundamentales para identificar áreas de mejora y garantizar la consistencia en el proceso de comunicación.

**1.4 Intercambio Proactivo de Información**

La organización debe compartir de manera proactiva indicadores relevantes de incidentes con sus pares para mejorar la detección y el análisis de amenazas, fomentando una colaboración más amplia en el ecosistema de seguridad. Este intercambio de información debe realizarse respetando las políticas organizacionales y normativas de privacidad aplicables. Un auditor evaluará si estas prácticas de intercambio se documentan y si contribuyen efectivamente a mejorar las capacidades de detección y respuesta.

# 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 establecer y comunicar procedimientos sobre incidentes de seguridad de la información respuesta a todas las partes interesadas pertinentes.  2. Mantener información de contacto para reportar incidentes de seguridad |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. La organización debe comunicar los detalles apropiados del incidente a partes externas, como los medios de comunicación, las agencias de aplicación de la ley y las organizaciones de informes de incidentes. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. El equipo debe actualizar y documentar todos los contactos y comunicaciones con terceros con fines de responsabilidad y evidencia. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener métricas para la revisión del proceso de comunicación con terceros, de forma que se pueda establecer si se comunica la información de forma que se cumpla con el proceso y mediante los canales adecuados |
| 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. La organización comparte de forma proactiva información relevante de indicadores de incidentes con sus pares para mejorar la detección y el análisis de incidentes. |

1. **Prácticas de auditoría para Comunicación con Terceros**

|  |
| --- |
| Temática: Comunicación con Terceros |
| Durante esta evaluación se revisa el proceso de interacción y coordinación con entidades externas, como proveedores, clientes, autoridades reguladoras y socios estratégicos, en un incidente de seguridad, de manera que se asegure la transparencia al informar a los terceros afectados de manera clara y precisa sobre el incidente al mismo tiempo mitigar el impacto, asegurando el cumplimiento de todas las obligaciones legales y contractuales relacionadas con la notificación y la gestión del incidente que, a su vez, protegen la imagen de la organización en contexto de incidente.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido un proceso formal para la notificación de incidentes a terceros? * ¿Qué procedimientos están documentados para asegurar que las notificaciones se realicen de manera oportuna y adecuada? * ¿Qué medidas específicas se implementan en el proceso para garantizar la comunicación? * ¿Existen registros o documentación de las notificaciones a terceros? * ¿Quién es el responsable de ejecutar este proceso y cómo se asegura su cumplimiento? * ¿Se ha establecido un protocolo claro para la divulgación de información en función de la gravedad del incidente? * ¿Se proporciona información clara y precisa sobre el incidente a los terceros afectados? * ¿Qué factores se consideran al priorizar la notificación y cómo se documentan las decisiones tomadas? * ¿Cómo se ajusta la priorización si el incidente evoluciona? * ¿Cómo se asegura que la información comunicada sea comprensible y relevante para cada tercero? * ¿Se documentan sistemáticamente todos los contactos y comunicaciones con terceros durante la gestión de incidentes? * ¿Existen políticas o procedimientos que definan cómo deben documentarse los contactos y comunicaciones con terceros durante un incidente? * ¿Cómo se asegura que la información documentada sea completa y correcta? * ¿Qué procesos existen para revisar y aprobar la documentación antes de su archivo final? * ¿Cómo se gestiona la evidencia relacionada con los contactos y comunicaciones con terceros para cumplir con los requisitos legales o regulatorios? * ¿Qué procesos existen para asegurar que esta evidencia esté disponible para inspecciones o investigaciones posteriores? * ¿Se lleva a cabo una revisión regular de los indicadores de incidentes para identificar oportunidades de mejora? * ¿Se comparte de manera proactiva información relevante de indicadores para mejorar la detección y análisis de incidentes? * ¿Existe integración de los indicadores en el diseño de protocolos para prevenir incidentes? |