

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Políticas y Procedimientos**

**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

La política y los procedimientos de respuesta a incidentes proporcionan un marco estructurado para gestionar eventos de seguridad, definiendo roles, responsabilidades y acciones necesarias para abordar eficazmente los incidentes. Una política bien definida y procedimientos claros aseguran la consistencia en la gestión de incidentes y el cumplimiento de los objetivos organizacionales. Desde una perspectiva de auditoría, es esencial que estas políticas estén alineadas con los estándares de la organización, se revisen regularmente y se adapten a los cambios en el entorno.

**1.1 Creación de una Política de Respuesta a Incidentes**

La política debe incluir una declaración de compromiso de la dirección, establecer su propósito y objetivos, y definir el alcance al que aplica. También debe especificar qué constituye un incidente de seguridad informática, las estructuras organizacionales, roles y responsabilidades, así como la autoridad del equipo de respuesta a incidentes para actuar. Elementos clave como la priorización de incidentes, medidas de rendimiento, y requisitos para notificar y escalar incidentes deben estar claramente documentados. Desde la perspectiva de auditoría, es fundamental verificar si la política aborda todos estos elementos y si está aprobada por la alta dirección.

**1.2 Procesos de Gestión y Respuesta a Incidentes**

Los procesos establecidos deben incluir un método común para notificar eventos de seguridad, un sistema de triaje y priorización de incidentes, y mecanismos para coordinar con las partes interesadas internas y externas. Además, se deben definir procesos para la evaluación, resolución, escalamiento y aprendizaje a partir de los incidentes. Solo personal capacitado debe gestionar los incidentes, y las necesidades de capacitación y certificación deben ser identificadas y abordadas. Un auditor evaluará si estos procesos están documentados, son consistentes y cumplen con los estándares organizacionales.

**1.3 Documentación de Procedimientos**

Los procedimientos de respuesta deben incluir objetivos específicos acordados con la dirección y detallar los pasos a seguir en caso de incidentes. Esto incluye formularios para la denuncia de incidentes, retroalimentación adecuada para quienes informan eventos, y mecanismos para notificar a reguladores u otras partes externas cuando sea necesario. Un auditor revisará si los procedimientos están alineados con la política, si incluyen medidas específicas para incidentes de seguridad y si se actualizan según lo requerido.

**1.4 Revisión y Actualización de Políticas y Procedimientos**

La política y los procedimientos deben actualizarse periódicamente o después de cambios significativos en el entorno organizacional. Es esencial establecer métricas para evaluar el cumplimiento y la necesidad de ajustes. Estas métricas también permiten identificar brechas en la política y los procedimientos, ya sea a través de eventos específicos o análisis regulares. Desde el punto de vista de auditoría, se revisará si las actualizaciones se realizan de manera oportuna y si responden a las necesidades de la organización.

**1.5 Medición y Mejora Continua**

La implementación de métricas permite evaluar el desempeño de las políticas y procedimientos de gestión de incidentes, identificar brechas y proponer mejoras. Los hallazgos deben documentarse y utilizarse para ajustar los procesos, fortaleciendo la capacidad de respuesta organizacional. Un auditor verificará si estas métricas son relevantes, se monitorean regularmente y contribuyen a la mejora continua.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Creación de una política de respuesta a incidentes.  2. La organización debe establecer procesos adecuados de gestión de incidentes de seguridad de la información. Se debe tener en cuenta lo siguiente:  2.1 Establecer un método común para notificar eventos de seguridad de la información, incluido el punto de contacto;  2.2 Establecer un proceso de gestión de incidentes para proporcionar a la organización la capacidad de gestión de incidentes de seguridad de la información, incluida la administración, documentación, detección, triaje, priorización, análisis, comunicación y coordinación de las partes interesadas;  2.3 Establecer un proceso de respuesta a incidentes para proporcionar a la organización la capacidad de evaluar, responder a los incidentes de seguridad de la información y aprender de ellos;  2.4 Permitir únicamente que el personal competente maneje los problemas relacionados con los incidentes de seguridad de la información dentro de la organización;  2.5 Establecer un proceso para identificar la capacitación, la certificación y la formación profesional continua requeridas.  3. Documentar los procedimientos de respuesta de incidentes. Este debe incluir los objetivos de la gestión de incidentes de seguridad de la información, los cuales deben ser acordados con la dirección.  4. Debe garantizarse que los responsables de la gestión de incidentes de seguridad de la información comprendan Las prioridades de la organización para manejar los incidentes de seguridad de la información, incluido el tiempo de resolución en función de las posibles consecuencias y gravedad. " |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Las políticas deben incluir elementos clave:   1.1 Declaración de compromiso de la dirección   1.2 Finalidad y objetivos de la política   1.3 Alcance de la política (a quién, qué se aplica y en qué circunstancias)   1.4 Definición de incidentes de seguridad informática y términos relacionados   1.5 Estructura organizacional y definición de roles, responsabilidades y niveles de autoridad;   1.6 La autoridad del equipo de respuesta a incidentes para confiscar o desconectar el equipo y actividades sospechosas, los requisitos para notificar determinados tipos de incidentes, los requisitos y directrices para las comunicaciones externas y el intercambio de información (por ejemplo, qué se puede compartir con quién, cuándo y a través de qué canales), y los puntos de entrega y escalada en el incidente.  1.7 Priorización o calificaciones de gravedad de incidentes   1.8 Medidas de rendimiento (como se explica en la sección 3.4.2)   1.9 Formularios de denuncia y contacto.  2. Los procedimientos de presentación de informes deben incluir:   2.1 Las medidas que deben adoptarse en caso de que se produzca un evento de seguridad de la información (por ejemplo, anotar todos los detalles pertinentes; como el mal funcionamiento que se produce y los mensajes en la pantalla, informando inmediatamente al punto de contacto y solo tomar acciones coordinadas).  2.2 Uso de formularios de incidentes para apoyar al personal a realizar todas las acciones necesarias al informar incidentes de seguridad de la información.  2.3 Procesos de retroalimentación adecuados para garantizar que las personas que informan sobre eventos de seguridad de la información notificado, en la medida de lo posible, de los resultados después de que se haya abordado y cerrado el problema.  2.4 Elaboración de partes de incidencias.   2.5 Cualquier requisito externo sobre la notificación de incidentes a las partes interesadas pertinentes dentro de la (por ejemplo, requisitos de notificación de infracciones a los reguladores).  2.6 Implementación de procedimientos de gestión de incidencias. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Actualizar política y procedimientos periódicamente o después de un cambio en el entorno que lo requiera. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer métricas para evaluar el cumplimiento y la actualización de políticas y procedimientos de gestión de incidentes. |
| 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. Identificar brechas dentro de la política y los procedimientos de gestión de incidentes mediante las métricas de evaluación establecidas o ante un evento que lo requiera. |

1. **Prácticas de auditoría para Políticas y Procedimientos**

|  |
| --- |
| Temática: Políticas y Procesos |
| La evaluación de esta temática se centra en la estructura formal que guía las acciones, incluyendo políticas, procedimientos y métodos de reporte que aseguran que la organización esté preparada y alineada con sus objetivos estratégicos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido una política formal de respuesta a incidentes de seguridad de la información?   + ¿Incluye esta política una declaración de compromiso de la dirección?   + ¿Están claramente definidos los objetivos y el alcance de la política?   + ¿Se han establecido roles, responsabilidades y niveles de autoridad en la política? * ¿Se ha establecido un método común para notificar eventos de seguridad de la información?   + ¿Existe un punto de contacto claro y accesible para la notificación?   + ¿Están los empleados informados sobre el proceso y saben cómo notificar incidentes? * ¿Se ha establecido un proceso formal de gestión de incidentes de seguridad de la información?   + ¿Incluye este proceso la administración, documentación, detección, triaje, priorización, análisis, comunicación y coordinación de las partes interesadas?   + ¿Se documentan adecuadamente todos los incidentes, incluyendo los detalles de su resolución? * ¿Se ha establecido un proceso de respuesta a incidentes de seguridad de la información?   + ¿Se evalúan y responden adecuadamente los incidentes en función de su gravedad y potencial impacto?   + ¿Se realizan sesiones de aprendizaje post-incidente para mejorar futuros procesos? * ¿Se han documentado los procedimientos de respuesta a incidentes de seguridad de la información?   + ¿Se han acordado estos procedimientos con la dirección?   + ¿Se revisan y actualizan regularmente estos procedimientos? * ¿Se han establecido procedimientos claros para la presentación de informes de incidentes de seguridad de la información?   + ¿Se utilizan formularios específicos para la denuncia de incidentes?   + ¿Se proporciona retroalimentación a las personas que informan sobre incidentes?   + ¿Se cumplen los requisitos externos de notificación a reguladores u otras partes interesadas? |

|  |
| --- |
| Temática: Capacidades y Ejecución |
| Durante esta evaluación se revisa la implementación práctica de las políticas, asegurando que el personal esté capacitado, los incidentes sean gestionados eficazmente y las prioridades de la organización se respeten en la ejecución diaria.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se garantiza que solo el personal competente maneja incidentes de seguridad de la información?   + ¿Se han identificado claramente las necesidades de capacitación y certificación?   + ¿Se realiza formación continua y actualización para el personal involucrado en la gestión de incidentes? * ¿Comprenden los responsables de la gestión de incidentes las prioridades de la organización?   + ¿Se tiene en cuenta el tiempo de resolución en función de las posibles consecuencias y la gravedad del incidente?   + ¿Existen procedimientos específicos para la priorización y escalación de incidentes críticos? |