

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Monitoreo, Detección y Análisis**

**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

El monitoreo, la contención y el análisis son elementos centrales en la gestión de incidentes, permitiendo identificar, clasificar y responder de manera eficiente a eventos de seguridad de la información. Un enfoque estructurado que priorice incidentes, documente las decisiones y evalúe tendencias garantiza no solo una respuesta efectiva, sino también una mejora continua de los procesos. Desde la perspectiva de auditoría, es esencial que estas actividades estén respaldadas por documentación detallada y métricas claras para evaluar su efectividad.

**1.1 Priorización y Clasificación de Incidentes**

La organización debe implementar un esquema de priorización que asigne puntuaciones a los incidentes según su impacto y gravedad, estableciendo criterios claros para clasificar eventos como incidentes de seguridad. Esto asegura que los recursos se asignen eficientemente a las situaciones más críticas. Desde el punto de vista de auditoría, es crucial verificar que este régimen esté documentado y que se aplique consistentemente para garantizar un manejo equitativo de los incidentes.

**1.2 Documentación y Evaluación de Incidentes**

Cada incidente debe ser registrado con información detallada, incluyendo su estado, análisis forense y decisiones tomadas. Este registro no solo respalda el análisis forense, sino que también facilita la evaluación de tendencias y la identificación de brechas. Los resultados de la evaluación deben documentarse con precisión para referencia futura y para verificar la efectividad del manejo de incidentes. Un auditor revisará si estos registros cumplen con los criterios establecidos y si la documentación permite un análisis exhaustivo.

**1.3 Análisis de Tendencias y Brechas**

Los datos recopilados sobre incidentes deben analizarse regularmente para identificar tendencias recurrentes o brechas en la respuesta a incidentes. Este análisis permite ajustar procedimientos y priorizar mejoras en las áreas más críticas. Además, los indicadores de cumplimiento deben monitorearse para evaluar la efectividad del monitoreo, la detección y el análisis de incidentes. Desde la perspectiva de auditoría, es importante verificar que estos análisis se realicen de manera sistemática y que se utilicen para impulsar mejoras concretas.

**1.4 Incorporación de Lecciones Aprendidas**

Las lecciones aprendidas durante el manejo de incidentes deben integrarse en los procedimientos operativos, la capacitación y las pruebas de respuesta. Esto garantiza que las mejoras identificadas durante la evaluación se implementen y se traduzcan en una capacidad de respuesta más efectiva. Un auditor evaluará si las lecciones aprendidas se documentan y aplican de manera oportuna, fortaleciendo los procesos organizacionales frente a futuros incidentes.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Crear un esquema de priorización y puntuación de incidentes de seguridad de la información para la Identificación de las consecuencias y prioridad de un incidente.  1.1. El régimen debe incluir los criterios para clasificar los eventos como incidentes de seguridad de la información |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. La documentación de incidentes debe incluir el mantenimiento de registros sobre cada incidente, el estado del incidente, y otra información pertinente necesaria para el análisis forense, así como para la evaluación de detalles, tendencias y manejo de incidentes  2. El personal responsable de coordinar y responder a los incidentes de seguridad de la información debe realizar la evaluación y tomar una decisión sobre los eventos de seguridad de la información.  2.1 Los resultados de la evaluación y la decisión deben registrarse en detalle a efectos de referencia futura y verificación. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Mantener la documentación de los resultados de la evaluación clasificados según criterios establecidos para el posterior análisis  2. Verificar si existen tendencias o brechas de mejora dentro de cada evaluación y decisión registrada. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener indicadores para evaluar el cumplimiento de monitore, detección y análisis 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. Incorporar las lecciones aprendidas de las actividades de manejo de incidentes en curso en los procedimientos, la capacitación y las pruebas de respuesta a incidentes, e implementar los cambios resultantes en consecuencia |

1. **Prácticas de auditoría para Monitoreo, Detección y Análisis**

|  |
| --- |
| Temática: Proceso de Monitoreo, Detección y Análisis |
| Evaluar el proceso de monitoreo, detección y análisis en el contexto de la gestión de incidentes implica asegurar que la organización mantenga la vigilancia constante de los sistemas, redes y aplicaciones para detectar comportamientos anómalos o indicadores de compromiso que puedan señalar un incidente de seguridad. El reconocimiento de incidentes se lleva a cabo a través de herramientas automatizadas y procesos manuales que alertan al equipo, los cuales evalúan y analizan la naturaleza y alcance de la amenaza determinando la causa raíz y las implicaciones para la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha creado un esquema para la identificación de las consecuencias y prioridad de un incidente? * ¿Existen criterios definidos para la clasificación de incidentes? * ¿Se revisa y actualiza regularmente el esquema de priorización? * ¿Se documentan todos los incidentes de seguridad de la información? * ¿Se registra el estado actual del incidente en cada etapa del proceso de manejo? * ¿Se incluye información necesaria para análisis forense y la evaluación de detalles y tendencias? * ¿Se realiza mantenimiento y revisión de los registros sobre cada incidente? * ¿Se asigna personal responsable para coordinar y responder a los incidentes de seguridad de la información? * ¿Se realiza una evaluación sobre los eventos de seguridad de la información? * ¿Qué métodos utiliza para realizar esta evaluación? * ¿Existen registros que detallen los procedimientos de estas evaluaciones? * ¿Se registran en detalle los resultados de la evaluación y las decisiones tomadas? * ¿Se integran las lecciones aprendidas de la gestión de incidentes en los procedimientos de respuesta a incidentes? * ¿Se actualizan los programas de capacitación y pruebas de respuesta a incidentes basados en las lecciones aprendidas? * ¿Se implementan los cambios resultantes de las lecciones aprendidas en los procedimientos y estrategias de respuesta a incidentes? * ¿Se monitorea el impacto de las modificaciones en los procedimientos de respuesta? * ¿Se evalúan los resultados de estos cambios en el manejo de incidentes? |