

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Plan de Respuestas a Incidentes**

**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

Un plan de respuesta a incidentes bien diseñado es esencial para establecer una hoja de ruta clara que permita a la organización gestionar eficazmente los incidentes de seguridad de la información. Este plan debe detallar las estrategias, procedimientos y métricas necesarios para garantizar una respuesta coordinada y efectiva. Desde la perspectiva de auditoría, es crucial que el plan esté documentado, sea revisado periódicamente y se ajuste a las necesidades y riesgos específicos de la organización.

**1.1 Elementos Clave del Plan de Respuesta a Incidentes**

El plan debe incluir una misión clara, estrategias y objetivos específicos aprobados por la alta dirección. También debe detallar el enfoque organizacional para la gestión de incidentes, los canales de comunicación internos y externos, y las métricas para medir la efectividad de la capacidad de respuesta. La hoja de ruta para madurar esta capacidad debe integrarse en la estructura organizacional general, asegurando que el plan sea escalable y sostenible. Un auditor revisará si estos elementos están claramente definidos y alineados con los objetivos organizacionales.

**1.2 Procedimientos para Escenarios y Actividades Específicas**

El plan debe considerar diferentes escenarios y detallar procedimientos específicos para la evaluación, seguimiento, clasificación y manejo de incidentes. Esto incluye la gestión integral de incidentes, desde la detección hasta la conclusión, considerando la escalación según la categoría y gravedad del incidente, así como la activación de planes de continuidad y recuperación. Además, deben documentarse actividades como la coordinación con partes interesadas, manejo de pruebas, análisis de causa raíz y lecciones aprendidas. Desde la perspectiva de auditoría, es fundamental verificar que estos procedimientos sean implementables y estén respaldados por registros claros.

**1.3 Revisión y Capacitación Regular**

El plan debe ser revisado al menos una vez al año para garantizar que se ajusta a los objetivos de madurez y capacidad de respuesta de la organización. También debe incluir la frecuencia de las capacitaciones para los encargados de gestionar incidentes, asegurando que el personal esté preparado para actuar de manera efectiva. Un auditor evaluará si estas revisiones y capacitaciones se realizan según lo planificado y si contribuyen a mejorar la capacidad de respuesta.

**1.4 Métricas y Evaluación de Efectividad**

El establecimiento de métricas o KPIs permite evaluar la efectividad del plan y su implementación. Estas métricas deben reflejar el desempeño del plan durante los incidentes y proporcionar datos para identificar áreas de mejora. Un auditor revisará si estas métricas son relevantes, actualizadas y si se utilizan para ajustar y optimizar el plan de manera continua.

**1.5 Identificación de Brechas y Mejora Continua**

La ejecución del plan debe analizarse para identificar brechas o áreas de mejora basadas en las métricas establecidas. Esto incluye ajustar procedimientos, actualizar controles y documentar las lecciones aprendidas para fortalecer la capacidad de respuesta de la organización. Desde una perspectiva de auditoría, es importante garantizar que este ciclo de mejora continua esté documentado y se implemente de manera efectiva.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Se debe tener un plan de respuesta a incidentes que proporcione la hoja de ruta para implementar la capacidad de respuesta a incidentes. Este debe incluir los siguientes elementos:  1.1 Misión Estrategias y objetivos  1.2 Aprobación de la alta dirección  1.3 Enfoque organizacional para la respuesta a incidentes  1.4 Cómo se comunicará el equipo de respuesta a incidentes con el resto de la organización y con otros  1.5 Organizaciones Métricas para medir la capacidad de respuesta a incidentes y su efectividad  1.6 Hoja de ruta para madurar la capacidad de respuesta a incidentes  1.7 Cómo encaja el programa en la organización general. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Asegurar que se cree un plan considerando diferentes escenarios y procedimientos que se desarrollan e implementan para la siguientes actividades:   1.1 Evaluación de eventos de seguridad de la información de acuerdo con criterios de lo que constituye una información incidente de seguridad.  1.2 Seguimiento, detección, clasificación, análisis y presentación de informes de eventos e incidentes de seguridad de la información (por medios humanos o automáticos).  1.3 Gestionar los incidentes de seguridad de la información hasta su conclusión, incluida la respuesta y el escalamiento, según el tipo y la categoría del incidente, la posible activación de la gestión de crisis y activación de planes de continuidad, recuperación controlada de un incidente y comunicación a los y partes interesadas externas.  1.4 Coordinación con las partes interesadas internas y externas, tales como autoridades, grupos y foros, proveedores y clientes.  1.5 Registro de las actividades de gestión de incidentes.  1.6 Manejo de pruebas.  1.7 Análisis de causa raíz o procedimientos post-mortem.  1.8 Identificación de las lecciones aprendidas y cualquier mejora de los procedimientos de gestión de incidentes, o controles de seguridad de la información en general que se requieran. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar el plan al menos una vez al año para asegurarse de que la organización está siguiendo la hoja de ruta para madurar la capacidad y cumplir sus objetivos de respuesta a incidentes.  1.1 El plan de respuesta a incidentes también debe indicar la frecuencia con la que los encargados de gestionar incidentes deben estar capacitados y los requisitos para los manejadores de incidentes. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer métricas o KPIs para evaluar la efectividad del plan de respuesta a incidentes y la actualización constante de este. |
| 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 o mejoras en base a los resultados en la ejecución del plan y métricas de evaluación establecidas. |

1. **Prácticas de auditoría para Plan de Respuestas a Incidentes**

|  |
| --- |
| Temática: Estructura y Planificación del Plan de Respuestas a Incidentes |
| Esta temática se enfoca en la creación, aprobación y estructura del plan de respuesta a incidentes, en donde se evaluará si la organización ha desarrollado un plan formal que alinea la misión y objetivos con la gestión de incidentes, asegurando que el plan esté integrado en la estructura organizacional y cuente con métricas y estrategias claras para su implementación y mejora continua.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido un plan formal de respuesta a incidentes en la organización?   + ¿Incluye el plan una declaración clara de la misión, estrategias y objetivos?   + ¿Cuenta el plan con la aprobación formal de la alta dirección?   + ¿El plan define claramente el enfoque organizacional para la respuesta a incidentes? * ¿Cómo se asegura que el equipo de respuesta a incidentes se comunica efectivamente con el resto de la organización y con otras entidades externas?   + ¿Se han definido canales y procedimientos específicos para la comunicación interna y externa?   + ¿Se han realizado pruebas de comunicación para verificar su eficacia? * ¿El plan incluye métricas para medir la capacidad de respuesta a incidentes y su efectividad?   + ¿Se revisan y actualizan regularmente estas métricas?   + ¿Se utilizan las métricas para realizar mejoras continuas en la capacidad de respuesta? * ¿Se ha desarrollado una hoja de ruta para madurar la capacidad de respuesta a incidentes?   + ¿Esta hoja de ruta está alineada con los objetivos estratégicos de la organización?   + ¿Se realizan revisiones periódicas de la hoja de ruta para asegurar su relevancia y cumplimiento? * ¿El plan de respuesta a incidentes está integrado en la estructura organizacional general?   + ¿Se han definido claramente los roles y responsabilidades dentro de la organización respecto al plan?   + ¿Existe una coordinación efectiva entre el equipo de respuesta a incidentes y otras áreas de la organización? |

|  |
| --- |
| Temática: Implementación del Plan de Respuestas a Incidentes |
| Esta temática abarca la aplicación práctica del plan de respuesta a incidentes, evaluando cómo la organización maneja y ejecuta el plan ante distintos escenario, analizando la efectividad de los procedimientos, la coordinación con partes interesadas, y la capacidad para registrar y aprender de los incidentes, asegurando que el plan se mantenga actualizado y operativo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido un plan formal de respuesta a incidentes en la organización?   + ¿Incluye el plan una declaración clara de la misión, estrategias y objetivos?   + ¿Cuenta el plan con la aprobación formal de la alta dirección?   + ¿El plan define claramente el enfoque organizacional para la respuesta a incidentes? * ¿Cómo se asegura que el equipo de respuesta a incidentes se comunica efectivamente con el resto de la organización y con otras entidades externas?   + ¿Se han definido canales y procedimientos específicos para la comunicación interna y externa?   + ¿Se han realizado pruebas de comunicación para verificar su eficacia? * ¿El plan incluye métricas para medir la capacidad de respuesta a incidentes y su efectividad?   + ¿Se revisan y actualizan regularmente estas métricas?   + ¿Se utilizan las métricas para realizar mejoras continuas en la capacidad de respuesta? * ¿Se ha desarrollado una hoja de ruta para madurar la capacidad de respuesta a incidentes?   + ¿Esta hoja de ruta está alineada con los objetivos estratégicos de la organización?   + ¿Se realizan revisiones periódicas de la hoja de ruta para asegurar su relevancia y cumplimiento? * ¿El plan de respuesta a incidentes está integrado en la estructura organizacional general?   + ¿Se han definido claramente los roles y responsabilidades dentro de la organización respecto al plan?   + ¿Existe una coordinación efectiva entre el equipo de respuesta a incidentes y otras áreas de la organización? |