

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Capacitación y Concientización**

**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 capacitación y concientización en la gestión de incidentes son componentes críticos para preparar al personal para responder eficazmente ante eventos de seguridad. Un enfoque bien estructurado que combine formación específica, simulaciones y análisis continuo permite a las organizaciones fortalecer su postura frente a incidentes. Desde la perspectiva de auditoría, es fundamental garantizar que estos procesos estén documentados, alineados con las políticas organizacionales y que incluyan métricas para evaluar su efectividad.

**1.1 Identificación y Provisión de Capacitación**

El primer paso en la capacitación para la gestión de incidentes es establecer un proceso que identifique las necesidades de formación, certificación y desarrollo continuo del personal encargado de responder a incidentes. Este proceso debe adaptarse a las funciones y responsabilidades asignadas, proporcionando formación específica que abarque cómo identificar y responder a infracciones, así como el procedimiento interno para reportarlas. Un auditor evaluará si estas necesidades han sido claramente definidas y si las capacitaciones ofrecidas cumplen con los estándares organizacionales.

**1.2 Simulaciones y Escenarios Prácticos**

Incorporar eventos simulados y sesiones de escenarios prácticos en la capacitación permite al personal experimentar situaciones reales de crisis y practicar su respuesta. Estos ejercicios deben diseñarse para evaluar habilidades clave y deben incluir indicadores de desempeño (KPIs) para medir su efectividad. Desde el punto de vista de auditoría, es esencial revisar los resultados de estas simulaciones y cómo se utilizan para identificar vulnerabilidades o brechas en las capacidades de respuesta.

**1.3 Evaluación y Mejora Continua**

La efectividad de la capacitación y concientización debe evaluarse mediante indicadores y metas que reflejen la mejora en el manejo de incidentes. Los resultados de las simulaciones y pruebas deben analizarse para identificar vulnerabilidades recurrentes y áreas de mejora. Este análisis debe traducirse en ajustes al proceso de capacitación, asegurando una evolución constante. Un auditor verificará si los resultados se documentan adecuadamente y si las acciones de mejora se implementan de manera oportuna.

**1.4 Concientización General**

Además de la formación técnica, los usuarios del sistema deben recibir capacitación básica sobre cómo identificar señales de posibles incidentes y cómo reportarlos siguiendo los procedimientos establecidos. Esto asegura que todos los miembros de la organización puedan contribuir a la gestión de incidentes, minimizando el impacto de las amenazas. Un auditor revisará si estas iniciativas son consistentes y si alcanzan a todos los usuarios relevantes.

**1.5 Monitoreo y Documentación**

El monitoreo continuo del proceso de capacitación, incluyendo la evaluación de KPIs relacionados con la formación y eventos simulados, es esencial para garantizar su efectividad. La documentación de estos procesos y sus resultados debe estar centralizada y accesible para auditores y responsables de la gestión de incidentes. Esto proporciona evidencia del compromiso organizacional con la mejora de sus capacidades de respuesta.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Establecer un proceso para identificar la capacitación, la certificación y la formación profesional continua requeridas para el personal de respuesta a incidentes. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Proporcionar capacitación en respuesta a incidentes a los usuarios del sistema de acuerdo con las funciones y responsabilidades asignadas  2. Incorporar eventos simulados en la capacitación de respuesta a incidentes para facilitar la respuesta requerida por el personal en situaciones de crisis.  3. Proporcionar capacitación en respuesta a incidentes sobre cómo identificar y responder a una infracción, incluido el proceso de la organización para informar de una infracción. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Llevar a cabo sesiones periódicas de escenarios de incidentes para el personal |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener indicadores o KPIs para evaluar el proceso de capacitación y formación profesional en el manejo de incidentes.  2. Incluir indicadores y metas para evaluar la efectividad de los eventos simulados. |
| 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 los resultados de pruebas y escenarios de incidentes para realizar análisis de vulnerabilidades e identificación de brechas y vulnerabilidades para la mejora continua del proceso de capacitación y concientización. |

1. **Prácticas de auditoría para Capacitación y Concientización**

|  |
| --- |
| Temática: Capacitación y Concientización |
| Evaluar la capacitación y concientización en la gestión de incidentes incluye revisar si se realizó el proceso de identificación de las necesidades de capacitación, la ejecución de programas de formación, la evaluación continua de su efectividad y la promoción de la concientización sobre las mejores prácticas en la gestión de incidentes de acuerdo a la planificación establecida.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido un proceso formal para identificar las necesidades de capacitación, certificación y formación profesional continua para el personal de respuesta a incidentes? * ¿Qué métodos se utilizan para evaluar las necesidades de capacitación y certificación del personal? * ¿Cómo se documenta y revisa este proceso para garantizar su eficacia y actualización? * ¿Se proporciona capacitación en respuesta a incidentes a todos los usuarios del sistema de acuerdo con sus funciones y responsabilidades específicas? * ¿Existen criterios definidos para determinar qué certificaciones y formaciones son necesarias para cada rol específico en la respuesta a incidentes? * ¿Cómo se determinan y documentan las necesidades de capacitación específicas para cada función? * ¿Cómo se asegura que estos criterios se apliquen de manera consistente? * ¿Con qué frecuencia se revisan y actualizan los requisitos de formación? * ¿Se mantiene un registro actualizado de la capacitación proporcionada a cada usuario, incluyendo fechas y contenido de la formación? * ¿Cómo se verifican y supervisan estos registros para asegurar su precisión y completitud? * ¿Existen evaluaciones de efectividad para asegurar que la capacitación proporcionada cumple con los objetivos y mejora la capacidad de respuesta a incidentes? * ¿Qué métodos se utilizan para medir la efectividad de la capacitación en respuesta a incidentes? * ¿Cómo se documentan y aplican las mejoras sugeridas a partir de las evaluaciones de efectividad? |