

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Preparación y Planificación**

**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 preparación en la gestión de incidentes es esencial para establecer una capacidad de respuesta efectiva y garantizar que la organización pueda manejar incidentes de seguridad de la información de manera eficiente. Esto implica definir responsabilidades, probar regularmente las capacidades de respuesta y utilizar los resultados para mejorar continuamente los procesos. Desde una perspectiva de auditoría, es fundamental que estos procedimientos estén documentados, se implementen consistentemente y se ajusten según los resultados obtenidos.

**1.1 Monitoreo y Evaluación de Incidentes**

La organización debe establecer procedimientos para cuantificar y monitorear los tipos, volúmenes y costos de incidentes de seguridad. La información obtenida debe utilizarse para mejorar el plan de gestión de incidentes, identificar causas recurrentes y actualizar la evaluación de riesgos de seguridad. Además, esta información puede emplearse para fortalecer la formación de usuarios mediante ejemplos prácticos de cómo prevenir y responder a incidentes. Un auditor verificará si estos datos son recopilados de manera sistemática y si se utilizan para mejorar la postura de seguridad de la organización.

**1.2 Definición de Roles y Responsabilidades**

Es esencial asignar responsabilidades claras para la gestión de incidentes, comunicar las funciones a todas las partes interesadas relevantes y designar personal capacitado para apoyar las actividades de manejo de incidentes. Desde la perspectiva de auditoría, se debe garantizar que estas asignaciones estén documentadas, sean comunicadas efectivamente y que el personal cuente con los recursos necesarios para cumplir con sus funciones.

**1.3 Soporte y Recursos para la Respuesta**

La organización debe proporcionar recursos integrales que brinden asesoramiento y asistencia a los usuarios para manejar y reportar incidentes. Esto incluye establecer un punto de contacto centralizado y publicar información sobre cómo notificar anomalías e incidentes. Los auditores revisarán si estos recursos están disponibles, si son accesibles para los usuarios y si se utilizan de manera efectiva durante la respuesta a incidentes.

**1.4 Pruebas de Eficacia de Respuesta**

La capacidad de respuesta a incidentes debe probarse regularmente mediante listas de verificación, ejercicios de recorrido y simulaciones. Estas pruebas deben ser rigurosas, coherentes y abarcar toda la organización para garantizar que los resultados sean comparables y predecibles. Desde una perspectiva de auditoría, es importante revisar los resultados de las pruebas y evaluar si se implementan mejoras basadas en los hallazgos.

**1.5 Uso de Métricas para Mejoras Continuas**

Las métricas cualitativas y cuantitativas obtenidas de las pruebas deben utilizarse para determinar la eficacia de los procesos de respuesta a incidentes y para mejorarlos continuamente. Estas métricas deben ser precisas, coherentes y presentarse en un formato reproducible que facilite su análisis. Los auditores revisarán si estas métricas están alineadas con los objetivos organizacionales y si se utilizan para impulsar mejoras en los procesos.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Establecer procedimientos para cuantificar y monitorear los tipos, volúmenes y costos de Incidentes de seguridad de la información.  2. La información obtenida de la evaluación de los incidentes de seguridad de la información debe utilizarse para:   2.1 Mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos de incidentes.  2.2 Identificar incidentes recurrentes o graves y sus causas para actualizar la información de la organización evaluación de riesgos de seguridad y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o las consecuencias de futuros incidentes similares.   2.3 Mejorar la concienciación y la formación de los usuarios proporcionando ejemplos de lo que puede ocurrir, responder a tales incidentes y cómo evitarlos en el futuro. 3. Asignar cargos y responsabilidades para la respuesta a incidentes.  4. Las funciones y responsabilidades para llevar a cabo los procedimientos de gestión de incidentes deben determinarse y efectivamente comunicada a las partes interesadas internas y externas relevantes.  5. Designar personal de gestión para apoyar el manejo de incidentes |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Proporcionar un recurso de soporte de respuesta a incidentes, integral a la capacidad de respuesta a incidentes de la organización, que ofrezca asesoramiento y asistencia a los usuarios del sistema para el manejo y la notificación de incidentes. 2. Probar la eficacia de la capacidad de respuesta a incidentes del sistema. Las pruebas de respuesta a incidentes incluyen el uso de listas de comprobación, ejercicios de recorrido o de mesa y simulaciones (paralelas o de interrupción completa).  2.1 Asegurar que el rigor, la intensidad, el alcance y los resultados de las actividades de gestión de incidentes sean comparables y predecibles en toda la organización |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Publicar información relacionada con la notificación de anomalías e incidentes informáticos |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Proporcionar medidas y métricas de respuesta a incidentes que sean precisas, coherentes y en un formato reproducible. |
| 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. Utilice los datos cualitativos y cuantitativos de las pruebas para:  1.1 Determinar la eficacia de los procesos de respuesta a incidentes  1.2 Mejorar continuamente los procesos de respuesta a incidentes. |

1. **Prácticas de auditoría para Preparación y Planificación**

|  |
| --- |
| Temática: Capacidad de Preparación para la Gestión de Incidentes |
| La revisión de cumplimiento incluye verificar si la organización ha implementado procedimientos específicos para asegurar una respuesta efectiva ante incidentes, si ha asignado responsabilidades claras y si se realizan pruebas regulares para validar su capacidad de respuesta.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han establecido procedimientos formales para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información?   + ¿Estos procedimientos están documentados y alineados con estándares organizacionales? * ¿La organización publica información clara y accesible sobre la notificación de anomalías e incidentes informáticos? * ¿Se han asignado cargos y responsabilidades claras para la respuesta a incidentes?   + ¿Están estas funciones y responsabilidades comunicadas efectivamente a las partes interesadas internas y externas relevantes? * ¿Se ha designado personal de gestión específico para apoyar el manejo de incidentes? * ¿Se cuenta con un recurso de soporte integral que ofrezca asesoramiento y asistencia para la notificación y el manejo de incidentes?   + ¿Los usuarios del sistema conocen cómo acceder a este recurso de soporte? |

|  |
| --- |
| Temática: Cuantificación y Monitoreo de Incidentes de Seguridad de la Información |
| Esta temática aborda la capacidad de la organización para cuantificar y monitorear de manera continua los tipos, volúmenes y costos asociados con los incidentes de seguridad de la información verificando la existencia de herramientas y procedimientos para registrar y analizar incidentes, asegurando que se utilicen métricas específicas para medir su impacto.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización utiliza sistemas o herramientas para registrar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información?   + ¿Se aseguran de que los datos sean centralizados y accesibles para el análisis posterior? * ¿Las métricas utilizadas para medir el impacto de los incidentes son precisas, coherentes y reproducibles? * ¿Se utilizan datos cualitativos y cuantitativos de las pruebas para determinar la eficacia de los procesos de respuesta a incidentes?   + ¿Estos datos son revisados regularmente para identificar patrones o tendencias? * ¿Se generan informes periódicos sobre el monitoreo de incidentes que sean accesibles para la alta dirección y las partes interesadas?   + ¿Se incluyen métricas financieras y operativas en estos informes? |

|  |
| --- |
| Temática: Mejora Continua Basada en la Cuantificación y Monitoreo |
| La revisión del cumplimiento de la mejora continua basada en la cuantificación y monitoreo incluye verificar si la organización aplica las lecciones aprendidas de incidentes anteriores para ajustar sus procesos, si documenta y comunica las mejoras realizadas, y si integra estos datos en la evaluación de riesgos de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se utiliza la información de incidentes anteriores para mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos? * ¿Se identifican incidentes recurrentes o graves, y se actualiza la evaluación de riesgos para implementar controles adicionales? * ¿Se mejora la formación y concienciación de los usuarios con ejemplos reales de incidentes y las respuestas dadas?   + ¿Se incluyen medidas prácticas para evitar incidentes similares en el futuro? * ¿Se realizan pruebas regulares para evaluar la eficacia de los procesos de respuesta a incidentes?   + ¿Las pruebas incluyen simulaciones, ejercicios de mesa o escenarios de interrupción total?   + ¿Los resultados de estas pruebas son documentados y utilizados para mejorar continuamente los procesos? * ¿Los hallazgos de las pruebas de respuesta a incidentes se documentan y comunican a las partes interesadas relevantes para su implementación?   + ¿Se ajustan las medidas en función de los resultados obtenidos para asegurar consistencia en toda la organización? |