

**GASIC 9 – Gestión de Incidentes**

**Preguntas de Auditoría**

**Contención, erradicación y recuperación**

**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 contención, erradicación y recuperación son fases críticas en la gestión de incidentes que buscan mitigar el impacto de las interrupciones y restaurar la seguridad de la información a los niveles requeridos. Estas actividades requieren una planificación meticulosa, la implementación de controles adecuados y un monitoreo continuo para garantizar su efectividad. Desde una perspectiva de auditoría, es esencial que los procesos asociados estén documentados, alineados con los requisitos organizacionales y sujetos a mejora continua.

**1.1 Adaptación de Controles durante Interrupciones**

La organización debe determinar cómo adaptar los controles de seguridad durante una interrupción, garantizando que se mantengan los procesos críticos para la continuidad del negocio. Esto incluye integrar los requisitos de seguridad en los planes de continuidad y compensar los controles que no puedan mantenerse. Un auditor evaluará si estas medidas han sido adecuadamente documentadas y si se revisan periódicamente para adaptarse a posibles cambios en el entorno operativo.

**1.2 Respuesta a Derrames de Información**

Los derrames de información deben abordarse siguiendo un enfoque estructurado que incluya asignar responsabilidades, identificar la información contaminada y aislar los sistemas afectados. Además, se deben erradicar los datos contaminados y evaluar posibles impactos en otros sistemas. Desde el punto de vista de auditoría, es crucial revisar si los procedimientos para manejar estos eventos están documentados y si las actividades realizadas están alineadas con las políticas organizacionales.

**1.3 Coordinación con Planificación de Contingencias**

Las actividades de manejo de incidentes deben coordinarse con los planes de contingencia para garantizar una respuesta integrada y eficaz. Esto incluye implementar y mantener herramientas y procesos que respalden la continuidad de la seguridad de la información durante una interrupción. Un auditor verificará si esta coordinación se ha implementado y si los planes son probados y evaluados regularmente.

**1.4 Restauración de la Seguridad y Recuperación**

Los planes deben incluir acciones para restaurar la seguridad de la información al nivel requerido en el tiempo estipulado, asegurando la continuidad de los procesos críticos. Estas actividades deben ser coherentes con el plan de respuesta a incidentes, cubriendo desde la preparación y detección hasta la recuperación. Desde una perspectiva de auditoría, se debe garantizar que estas actividades estén alineadas con los objetivos organizacionales y que se mantengan registros detallados de las acciones realizadas.

**1.5 Evaluación y Mejora Continua**

Es esencial mantener métricas que evalúen la efectividad de los procesos de contención, erradicación y recuperación. Estas métricas deben analizarse para identificar brechas y áreas de mejora, estableciendo un ciclo de mejora continua. Un auditor revisará si estas métricas se utilizan de manera efectiva para fortalecer los procesos y reducir los tiempos de respuesta ante futuros incidentes.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. La organización debe determinar sus requisitos para adaptar los controles de seguridad de la información durante la interrupción.  2. Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Se debe responder a los derrames de información de la siguiente manera:  1.1 Asignar un responsable de responder a los derrames de información  1.2 Identificar la información específica involucrada en la contaminación del sistema  1.3 Alerta al personal responsable del derrame de información utilizando un método de comunicación no asociado con el derrame  1.4 Aislar el sistema o componente del sistema contaminado  1.5 Erradicar la información del sistema o componente contaminado  1.6 Identificación de otros sistemas o componentes del sistema que puedan haber sido posteriormente contaminado  2. Coordinar las actividades de manejo de incidentes con las actividades de planificación de contingencias |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Los planes deben desarrollarse, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos comerciales críticos después de una interrupción o falla.  2. La seguridad de la información debe restablecerse al nivel requerido y en los plazos requeridos.  3. La organización debe implementar y mantener:  3.1 controles de seguridad de la información, sistemas y herramientas de apoyo dentro de los planes de continuidad del negocio y continuidad de las TIC  3.2 procesos para mantener los controles de seguridad de la información existentes durante la interrupción  3.3 Compensar los controles de seguridad de la información que no se pueden mantener durante la interrupción.  4. Implementar una capacidad de manejo de incidentes que sea coherente con el plan de respuesta a incidentes e incluya preparación, detección y análisis, contención, erradicación y recuperación |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener métricas de evaluación en la contención, erradicación y recuperación del incidentes de acuerdo a los niveles y plazos requeridos para poder verificar la efectividad del proceso. |
| 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. Establecer un proceso de mejora mediante el análisis de resultados y brechas que se haya podido identificar en el proceso de contención, erradicación y recuperación. |

1. **Prácticas de auditoría para Contención, Erradicación y Recuperación.**

|  |
| --- |
| Temática: Proceso de Contención, erradicación y recuperación |
| Evaluar la contención, erradicación y recuperación en la gestión de incidentes implica revisar que los procesos que buscan reducir el daño, eliminar la amenaza y restaurar las operaciones normales tras la detección de un incidente de seguridad cumplan con lo establecido en las mejores prácticas y requisitos de la organización. Las fases de este proceso incluyen la protección de los activos críticos, implementación de procedimientos que tiendan a evitar la propagación del incidente, reparación o corrección de los sistemas, la restauración de los servicios a su estado normal considerando e identificando áreas de mejora en los procedimientos implementados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han identificado y documentado los requisitos para adaptar los controles de seguridad de la información durante una interrupción? * ¿Cómo se determinan estos requisitos? * ¿Existe una revisión periódica de los requisitos para asegurar su actualización y adecuación? * ¿Se incluyen los requisitos de seguridad de la información en los procesos de gestión de la continuidad del negocio? * ¿Cómo se asegura que estos requisitos se integren en todos los aspectos de la continuidad del negocio? * ¿Existen procedimientos para revisar y actualizar estos requisitos en función de cambios en el entorno de amenazas? * ¿Se ha designado un responsable específico para gestionar la respuesta a los derrames de información? * ¿Qué criterios se utilizan para seleccionar a este responsable? * ¿El responsable conoce el procedimiento o plan de respuestas a incidentes? * ¿Se identifican y documentan de manera precisa la información específica involucrada en un derrame? * ¿Qué métodos o herramientas de análisis se utilizan para determinar el alcance de la contaminación del sistema? * ¿Se alerta al personal responsable del derrame utilizando un método de comunicación seguro que no esté asociado con la información derramada? * ¿Cómo evalúan la seguridad de estos métodos de comunicación? * ¿Se aísla el sistema o componente del sistema contaminado de manera oportuna? * ¿Existe un análisis de afectación del incidente que determine el aislamiento? * ¿Existen registros de estos análisis? * ¿Qué procedimientos se siguen para asegurar el aislamiento? * ¿Se erradica la información contaminada del sistema o componente afectado? * ¿Los procedimientos de erradicación incluyen actividades para asegurar que la contaminación haya sido eliminada completamente? * ¿Se identifican y evalúan otros sistemas o componentes que puedan haber sido contaminados posteriormente? * ¿Qué métodos se utilizan para asegurar que no haya contaminación residual en otros sistemas? * ¿Se coordinan las actividades de manejo de incidentes con las actividades de planificación de contingencias? * ¿Cómo se asegura que ambas actividades estén alineadas y se complementen entre sí? * ¿Qué métodos se utilizan para evaluar esta coordinación? * ¿Se desarrollan e implementan planes para mantener o restaurar la seguridad de la información en procesos comerciales críticos tras una interrupción o falla? * ¿Cómo se prueban, revisan y evalúan estos planes? * ¿Con qué frecuencia se revisan y actualizan? * ¿Qué mecanismos de prueba se utilizan para asegurar que los planes funcionen como se espera? * ¿Se restablece la seguridad de la información al nivel requerido y dentro de los plazos establecidos tras una interrupción? * ¿Se utilizan métricas como el RTO y RPO para evaluar si los niveles de seguridad se han restablecido adecuadamente según los niveles acordados? * ¿Se implementan y mantienen controles de seguridad de la información, sistemas y herramientas de apoyo dentro de los planes de continuidad del negocio y continuidad de las TIC? * ¿Existen registros de implementación y mantenimiento de estos controles? * ¿Cómo se evalúa la eficacia de estos controles durante una interrupción? * ¿Se mantienen los controles de seguridad de la información existentes durante la interrupción? * ¿Qué procesos se siguen para asegurar que estos controles sean operativos? * ¿Se implementan controles compensatorios de seguridad de la información cuando los controles existentes no pueden mantenerse durante la interrupción? * ¿Cómo se determina la idoneidad de los controles compensatorios y cómo se evalúa su operatividad? * ¿Se ha implementado un plan de manejo de incidentes que sea coherente con el plan de respuesta a incidentes? * ¿Cómo se evalúa que las etapas de preparación, detección y análisis, contención, erradicación y recuperación se integren en el plan de respuesta a incidentes? |