

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Concientización y Capacitación de Respuesta a Incidentes**

**Competencias Básicas del Auditor**

1. **Conocimiento de las Normas y Regulaciones:** Un auditor debe estar familiarizado con las normas, regulaciones y estándares relevantes en el ámbito de la ciberseguridad (como ISO 27001, CIS, NIST CSF, etc.) y la gestión de personas (estatuto administrativo, normativa interna).
2. **Habilidades Analíticas:** La capacidad de analizar datos, identificar patrones y hacer conexiones entre información aparentemente no relacionada es esencial.
3. **Comunicación Efectiva:** Un auditor debe ser capaz de comunicar sus hallazgos de manera clara y concisa, tanto por escrito como verbalmente.
4. **Conocimiento Técnico:** Es esencial tener un conocimiento profundo de las tecnologías y sistemas que se están auditando. En particular, debe conocer el funcionamiento y arquitectura de los sistemas de apoyo para la gestión de recursos humanos (hrms).
5. **Conocimiento de las Amenazas Actuales:** El panorama de amenazas de ciberseguridad está en constante evolución. En particular, la de gestión de personas requiere un conocimiento en profundidad de las técnicas más comunes, como las de ingeniería social.
6. **Capacidad de Evaluación de Riesgos:** Evaluar y priorizar riesgos es una habilidad clave. Un auditor debe ser capaz de determinar qué áreas presentan el mayor riesgo y recomendar medidas para mitigar esos riesgos.

# Visión General

La concientización y capacitación en respuesta a incidentes dentro de la función de seguridad de la información y ciberseguridad (SIC) incluye la concientización sobre la importancia de reportar incidentes de seguridad de inmediato para prevenir o reducir el impacto de estos eventos y advertir sobre los riesgos de probar vulnerabilidades de manera no autorizada. La capacitación en respuesta a incidentes se adapta a las funciones y responsabilidades asignadas, ofreciendo entrenamiento inicial al asumir roles en SIC, capacitaciones adicionales cuando se introducen cambios en el sistema y actualizaciones periódicas según las políticas organizativas.

**1.1 Documentación y Estructura de Políticas de Respuesta a Incidentes**

Para facilitar una respuesta coordinada y efectiva, la organización desarrolla y distribuye políticas de respuesta a incidentes que abarcan desde el propósito y alcance hasta las responsabilidades individuales y colectivas. Estas políticas deben alinearse con la normativa aplicable y los estándares de la industria, y se complementan con procedimientos que guían la implementación y los controles necesarios para gestionar incidentes. Además, se establece un sistema de reporte de eventos y vulnerabilidades, documentando problemas que van desde ineficacias en los controles de seguridad hasta sospechas de malware, permitiendo una visión integral de las amenazas y facilitando una acción rápida. La designación de un responsable para gestionar la documentación y difusión de la política asegura que todos los involucrados conozcan sus roles y tengan acceso a información actualizada.

**1.2 Rol de la Auditoría en la Capacitación y Respuesta a Incidentes en SIC**

Desde la perspectiva de auditoría, la capacitación en respuesta a incidentes en SIC se supervisa mediante la revisión de la efectividad de las políticas y procedimientos de respuesta a incidentes, evaluando su rigor, alcance y consistencia en toda la organización. Las auditorías incluyen la revisión y actualización frecuente de los contenidos de capacitación y pruebas para asegurar que estén alineados con las políticas actuales y las necesidades emergentes. Además, se realizan pruebas periódicas para verificar la capacidad de respuesta de los sistemas ante incidentes, y las lecciones aprendidas de eventos anteriores se integran en las políticas y programas de capacitación para mejorar continuamente la eficacia del manejo de incidentes. Este enfoque ayuda a fortalecer la resiliencia de la organización, asegurando que tanto la capacitación como la respuesta a incidentes se mantengan efectivas y adaptativas en un entorno en constante cambio.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Concientizar a todos los usuarios y el personal sobre su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información.  2. Advertir al personal y a los usuarios que no intenten probar vulnerabilidades de seguridad de la información sospechosas.  3. Brindar capacitación en respuesta a incidentes a los usuarios del sistema de acuerdo con las funciones y responsabilidades asignadas:  3.1 Dentro de un tiempo definido después de asumir un rol o responsabilidad de respuesta a  incidentes o adquirir acceso al sistema.  3.2 Cuando sea requerido por cambios en el sistema.  3.3 Frecuentemente según las políticas de la organización. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Desarrollar, documentar y distribuir al personal, con roles clave dentro de la organización y a quien corresponda, la documentación correspondiente a:  1.1 Políticas de respuesta a incidentes a nivel de organización, de procesos del negocio y de sistema que:  1.1.1 Aborde el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento.  1.1.2 Sea coherente con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas y directrices aplicables.  1.2. Procedimientos para facilitar la implementación de la política de respuesta a incidentes y los controles de respuesta a incidentes asociados.  2. Definir un reporte de eventos, incidentes, violaciones y vulnerabilidades de SIC. Este reporte puede incluir, pero no estar limitado a:  2.1 controles de seguridad de la información ineficaces;  2.2 incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información;  2.3 errores humanos;  2.4 incumplimiento de la política de seguridad de la información, políticas específicas del tema o normas aplicables;  2.5 incumplimientos de las medidas de seguridad física;  2.6 cambios del sistema que no han pasado por el proceso de gestión de cambios;  2.7 mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware;  2.8 infracciones de acceso;  2.9 vulnerabilidades;  2.10 sospecha de infección por malware.  3. Designar un responsable para gestionar el desarrollo, la documentación y la difusión de la política y los procedimientos de respuesta a incidentes.  4. Implementar una capacidad de manejo de incidentes para incidentes que sea consistente con el plan de respuesta a incidentes e incluya preparación, detección y análisis, contención, erradicación y recuperación.  5. Coordinar las actividades de manejo de incidentes con las actividades de planificación de contingencia. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Garantizar que el rigor, la intensidad, el alcance y los resultados de las actividades de manejo de incidentes sean comparables y predecibles en toda la organización.  2. Revisar y actualizar el contenido del entrenamiento de respuesta a incidentes frecuentemente y según las políticas de la organización.  3. Revisar y actualizar las políticas y los procedimientos de respuestas a incidentes frecuentemente. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Realizar pruebas frecuentemente para probar la efectividad de la capacidad de respuesta a incidentes para el sistema. |
| 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 de respuesta a incidentes, capacitación y pruebas, e implementar los cambios resultantes en consecuencia. |

# Preguntas de Auditoría para la Concientización y Capacitación de Respuesta a Incidentes

|  |
| --- |
| Temática: Cumplimiento de políticas y procedimientos de concientización y capacitación y estructura del reporte de incidentes de seguridad |
| Realizando esta evaluación, el auditor puede verificar que las políticas estén actualizadas y alineadas con las mejores prácticas y regulaciones, lo que garantiza que la organización esté preparada para enfrentar incidentes de seguridad de manera eficiente y legalmente conforme. Además, la revisión de los procedimientos asegura que exista un enfoque estructurado y predefinido para la identificación, reporte y manejo de incidentes, lo que minimiza la incertidumbre y reduce el tiempo de respuesta. También le permite al auditor verificar la efectividad de la estructura de reporte, evaluando si los incidentes de documentan y comunican de manera completa y precisa.  Para la evaluación, el auditor debe tener en consideración: Políticas y procedimientos Este levantamiento puede incluir análisis específicos tales como:   * Evaluar la existencia y vigencia de políticas de respuesta a incidentes y confirmar que contenga los siguientes aspectos relevantes:   + La clasificación de incidentes   + Los procedimientos de notificación (que incluya quién y cuándo debe notificar y límites de tiempo)   + Los roles y responsabilidades del personal en las etapas del proceso de respuesta   + Se han tenido en cuenta las regulaciones específicas de la industria en la que opera la organización (las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas y directrices aplicables). * ¿El personal relevante ha sido informado y tiene acceso a las políticas de manera oportuna? * ¿Se reportan incumplimientos de políticas de seguridad y otras políticas aplicables? * ¿Existe un mecanismo para reportar incumplimientos de políticas? * ¿Se toman medidas adecuadas en respuesta a los reportes y se documenta la resolución? * ¿La organización cuenta con procedimientos claros, completos y alineados con la política de respuesta a incidentes?   + ¿Se incluye detalles como los pasos a seguir para detectar, informar, analizar y responder a incidentes de seguridad?   + ¿La documentación incluye una descripción clara de los tipos de eventos, incidentes, violaciones y vulnerabilidades que deben ser reportados? * ¿Las políticas y procedimientos reflejan los cambios en las amenazas de seguridad de la información?  Estructura del reporte de incidentes Este levantamiento puede incluir análisis específicos tales como:   * ¿Se tiene un formato documentado para el reporte de eventos, incidentes, violaciones y vulnerabilidades de seguridad?   + ¿El formato incluye campos esenciales como fecha, hora, tipo de incidente, impacto y acciones tomadas?   + ¿El reporte proporciona suficiente información para comprender el evento o incidente?   + vulnerabilidades incluye información sobre las personas responsables de reportar y gestionar dichos eventos * ¿La organización ha definido una lista de eventos e incidentes que deben ser reportados? ¿La lista incluye información sobre las vulnerabilidades identificadas como una descripción, nivel de severidad, impacto potencial y clasificación de riesgo? * ¿Los roles clave y sus responsabilidades están definidos en la estructura de manejo de incidentes? * ¿Se proporciona capacitación adecuada al personal involucrado en el manejo de incidentes? * Solicitar reportes de incidentes realizados y evaluar si el reporte proporciona la * información necesaria para comprender el evento o incidente de manera adecuada * ¿Se reportan errores humanos y se documentan adecuadamente? |

|  |
| --- |
| Temática: Programa de concientización y capacitación de respuestas a incidentes |
| En esta evaluación, el auditor debe realizar un examen exhaustivo de cómo una organización se prepara y educa a su personal para enfrentar situaciones de seguridad. Esta evaluación busca asegurar que el programa no solo sea un conjunto de instrucciones estáticas, sino una herramienta dinámica que equipa a los empleados con el conocimiento y las habilidades necesarias para responder de manera efectiva a incidentes de seguridad. En última instancia, el objetivo es asegurar que el personal esté bien preparado para identificar, notificar y mitigar incidentes de seguridad. Este levantamiento puede incluir análisis específicos tales como:   * ¿Qué temas específicos abarca el programa de concientización? * ¿El programa incluye información sobre la responsabilidad de informar eventos de seguridad? * ¿El programa se adapta a las necesidades cambiantes del entorno de seguridad? * ¿Se ofrece capacitación al personal en seguridad de la información? ¿Cómo se asegura que todos los empleados reciban la capacitación adecuada? * ¿Se realiza seguimiento para verificar la participación y efectividad de la capacitación? * ¿Se han establecido canales claros y seguros para reportar eventos de seguridad?   + ¿Qué canales se proporcionan para reportar eventos de seguridad?   + ¿Se promueve el uso de canales confidenciales para fomentar la denuncia de incidentes? * ¿El programa aborda adecuadamente las necesidades de capacitación de los usuarios en función de sus roles y responsabilidades en la respuesta a incidentes?   + ¿Existe registro de las personas con acceso al sistema? * ¿Con qué frecuencia se proporciona capacitación a los usuarios en respuesta a incidentes? * ¿Se han proporcionado capacitaciones sobre la importancia de informar a los responsables de seguridad sobre posibles vulnerabilidades sospechosas en lugar de intentar explotarlas? * ¿Se verifica la efectividad de las capacitaciones en el mejoramiento del conocimiento y la comprensión de los usuarios sobre cómo responder a incidentes? |

|  |
| --- |
| Temática: Evaluación y mejora continua del programa |
| El auditor mediante la revisión de simulacros puede verificar la efectividad de la capacitación y la respuesta del equipo en situaciones simuladas, lo que permite identificar debilidades y oportunidades de mejora. Revisar las lecciones aprendidas ayuda al auditor a recopilar información valiosa sobre incidentes pasados, cómo se manejaron, y si se evitaron errores futuros. Finalmente, la revisión de la mejora continua asegura que los cambios implementados en base a las lecciones aprendidas tengan un impacto positivo en la respuesta a incidentes, manteniendo a la organización preparada para enfrentar desafíos de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realizan simulacros periódicos de incidentes?¿Se basan en escenarios realistas y abordan diferentes tipos de incidentes? * ¿Se evalúa la efectividad del equipo en la respuesta a estos simulacros? * ¿La organización cuenta con un sistema efectivo de comunicación y coordinación entre los equipos de respuesta a incidentes y otras partes interesadas? * ¿Se realizan análisis de postmortem después de incidentes reales? ¿Las lecciones aprendidas se documentan y se usan para mejorar procedimientos? * ¿Se han implementado cambios en procedimientos basados en lecciones aprendidas? * ¿Se realizan mejoras basadas en las lecciones aprendidas de incidentes anteriores? * ¿Los cambios implementados han mejorado la capacidad de respuesta a incidentes? |