

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Manejo de los 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

El manejo de incidentes en la función de seguridad de la información y ciberseguridad (SIC), específicamente en el contexto de recursos humanos, comienza con el establecimiento y mantenimiento de un equipo de respuesta a incidentes que pueda actuar rápidamente en cualquier ubicación identificada por la organización. Además, se requiere que el personal informe los presuntos incidentes a los encargados dentro de la organización y, cuando sea necesario, a las autoridades, empleando un método de comunicación seguro y no asociado al incidente. En caso de una contaminación, es necesario aislar el sistema afectado y erradicar la información dañada, además de investigar si otros sistemas podrían haber sido comprometidos. La pronta notificación y el conocimiento del procedimiento para reportar incidentes aseguran que el personal actúe rápidamente para mitigar el impacto de cualquier evento de seguridad.

**1.1 Plan de Respuesta a Incidentes y Capacidades Organizativas**

Para una respuesta efectiva, se desarrolla un plan de respuesta a incidentes que sirva como hoja de ruta y establezca la estructura y organización de la capacidad de respuesta a incidentes, adaptado a las características y necesidades únicas de la organización. Este plan debe definir claramente los tipos de incidentes a reportar, las métricas para medir la efectividad de la respuesta, y los recursos y apoyo administrativo necesarios para su implementación. La protección del plan contra accesos no autorizados y su distribución a personal clave aseguran que solo el personal responsable tenga acceso a esta información. Además, la organización proporciona un recurso de soporte que ofrece asesoría y asistencia a los usuarios del sistema, accesible en todo momento para facilitar la gestión y reporte de incidentes.

**1.2 Rol de la Auditoría en el Manejo de Incidentes en SIC**

Desde la perspectiva de auditoría, el manejo de incidentes en SIC implica el seguimiento y la documentación de cada incidente, así como la recopilación de datos sobre los incidentes para evaluar su impacto en la organización. Los auditores revisan que el plan de respuesta a incidentes esté actualizado y adaptado a los cambios organizativos y del sistema, y que se implementen adecuaciones según las lecciones aprendidas durante la ejecución o pruebas del plan. La auditoría garantiza que los cambios en el plan sean comunicados eficazmente al personal responsable y que los procesos de manejo de incidentes se mantengan alineados con las necesidades de la organización, promoviendo una respuesta rápida y eficiente que minimice el impacto de futuros incidentes.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Establecer y mantener un equipo integrado de respuesta a incidentes y derrames de información que pueda desplegarse en cualquier ubicación identificada por la organización al momento en que se identifique un incidente.  2. Requerir que el personal informe los presuntos incidentes a los encargados dentro de la organización y a las autoridades cuando sucedan. Se debe tener en cuenta:  2.1 Un método de comunicación no asociado con el derrame o incidente.  2.2 Aislar el sistema o componente contaminado  2.3 Erradicar la información del sistema o componente contaminado  2.4 Identificar otros sistemas o componentes del sistema que pueden haber sido posteriormente contaminados.  3. Requerir que el personal sea consciente de 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 y conozca el procedimiento para reportar eventos de seguridad de la información y el punto de contacto al que se debe informar de los hechos.  4.Identificar la información específica involucrada en la contaminación del sistema, en el caso de que exista un incidente en seguridad de la información. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Desarrollar un plan de respuesta a incidentes que:  1.1 Proporcione a la organización una hoja de ruta para  implementar su capacidad de respuesta a incidentes.  1.2 Describa la estructura y organización de la capacidad de respuesta a incidentes.  1.3 Proporcione un enfoque de alto nivel sobre cómo encaja la capacidad de respuesta a incidentes en la organización general.  1.4 Cumpla con los requisitos únicos de la organización, que se relacionen con la misión, el tamaño, la estructura y las funciones.  1.5 Defina los incidentes que deban ser reportados.  1.6 Proporcione métricas para medir la capacidad de respuesta a  incidentes dentro de la organización.  1.7 Defina los recursos y el apoyo administrativo necesario para mantener y madurar la capacidad de respuesta a  incidentes.  1.8 Aborde el intercambio de información sobre incidentes.  1.9 Sea revisado y aprobado por las autoridades correspondientes de la organización.  1.10 Designa explícitamente la responsabilidad de la respuesta a incidentes a las entidades y al personal correspondiente.  2. Proteger el plan de respuesta a incidentes de la divulgación y modificación no autorizadas.  3. Distribuir copias del plan de respuesta a incidentes al personal responsable de la respuesta a incidentes (identificado por nombre y/o función).  4.Proporcionar un recurso de soporte de respuesta a incidentes, parte integral de la capacidad de respuesta a incidentes de la organización, que ofrece asesoramiento y asistencia a los usuarios del sistema para el manejo y reporte de incidentes, que sea de fácil acceso y que esté siempre disponible. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Comunicar los cambios en el plan de respuesta a incidentes al personal responsable de la respuesta a incidentes (identificado por nombre y/o función). |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Realizar un seguimiento y documentar incidentes.  2. Recopilar datos respecto a los incidentes ocurridos y abordados por la organización para medir el impacto del incidente en SIC. |
| 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. Actualizar el plan de respuesta a incidentes para abordar los cambios organizativos y del sistema o problemas encontrados durante la implementación, ejecución o prueba del plan. |

# Preguntas de Auditoría para el Manejo de los Incidentes

|  |
| --- |
| Temática: Equipo y política de respuesta a incidentes |
| Al realizar esta evaluación, el auditor puede verificar que el equipo de respuesta a incidentes esté compuesto por miembros de diversas áreas para una respuesta integral, y que estén identificadas las locaciones de despliegue rápido. Además, se asegura que la política y los procedimientos sean claros, conocidos por el personal y seguidos en la notificación de incidentes. El auditor también puede evaluar la comunicación interna y la comprensión de responsabilidades, y verificar si contribuyen a una respuesta coordinada, eficiente y mejorada ante cualquier eventualidad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿El equipo de respuesta a incidentes incluye representantes de diversas áreas funcionales (como como TI, seguridad de la información, legal, comunicaciones, recursos humanos, entre otros)? * ¿Se han identificado las ubicaciones clave en donde se pueda requerir el equipo de respuesta a incidentes? * ¿La política de notificación de incidentes está claramente definida e incluyen los pasos específicos para la notificación de incidentes? * ¿Existe un método seguro y confidencial para reportar incidentes? ¿El personal tiene conocimiento y acceso a este método? * ¿El personal está al tanto de la política y procedimientos de notificación de incidentes? * ¿Los procedimientos se siguen al notificar incidentes a responsables internos y externos? * ¿El personal comprende su responsabilidad de reportar eventos rápidamente? |

|  |
| --- |
| Temática: Gestión de incidentes |
| Analizar los procedimientos, registros y acciones tomadas en respuesta a incidentes pasados, el auditor puede identificar posibles deficiencias en la preparación y ejecución del proceso de gestión de incidentes, verificando la capacidad de la organización para responder de manera rápida y precisa a futuros incidentes. Asimismo, evaluar la Gestión de Incidentes contribuye a la identificación temprana de patrones y tendencias, permitiendo implementar mejoras continuas y estrategias preventivas. Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen procedimientos documentados para la gestión de incidentes? * ¿Los procedimientos cubren todo el ciclo de vida de un incidente, desde la detección hasta la resolución y el cierre? * ¿Los procedimientos establecen claramente los roles y responsabilidades de las personas involucradas en la gestión de incidentes? * ¿Se han definido niveles de escalamiento y criterios de priorización para los incidentes? * ¿Los registros de incidentes incluyen información clave como la fecha y hora de detección, la descripción del incidente, el impacto, la prioridad y el estado actual? * ¿Se registran las acciones tomadas para resolver cada incidente, incluyendo los tiempos de respuesta y resolución? * ¿Se capturan los detalles de las comunicaciones realizadas durante el manejo de un incidente? * ¿Se registran las lecciones aprendidas y las oportunidades de mejora identificadas durante la resolución de incidentes? |

|  |
| --- |
| Temática: Plan de respuesta a incidentes y acceso a la información |
| En esta evaluación, el auditor debe asegurar que el plan de respuesta a incidentes y el acceso a la información sea efectiva, coherente con las políticas de la organización y comprensible para todos los involucrados. Esto garantiza que, durante situaciones críticas, la organización cuente con un recurso valioso que pueda orientar a su personal en la toma de decisiones informadas y en la adopción de acciones adecuadas para protegerse contra amenazas SIC.  Este levantamiento puede incluir análisis específicos tales como:   * ¿El plan de respuesta a incidentes abarca todos los aspectos mencionados en el apartado 3? * ¿El plan ha sido aprobado por las autoridades competentes? * ¿Existe un mecanismo de control de versiones para el plan? * ¿Las personas autorizadas para modificar el plan están claramente designadas? * ¿Se registran los cambios realizados en el plan de manera apropiada? * ¿Hay registros de comunicación sobre cambios en el plan de respuesta a incidentes?   + ¿La comunicación detalla cambios y proporciona instrucciones claras?   + ¿Todas las partes involucradas reciben las comunicaciones necesarias?   + ¿La comunicación ha sido entregada a todos los miembros del personal o equipos responsables de la respuesta a incidentes? * ¿El acceso a la documentación del plan está restringido y protegido tanto en formato digital como físico?   + ¿Se utilizan métodos de autenticación seguros, como contraseñas fuertes o autenticación de dos factores?   + ¿Los permisos de acceso a los archivos y carpetas están configurados adecuadamente? * ¿Las personas responsables han recibido una copia del plan de respuesta a incidentes y están familiarizadas con su contenido?¿Se han realizado capacitaciones sobre cómo utilizar el plan? * ¿Los recursos de soporte están disponibles y accesibles en todo momento (una línea telefónica de soporte, un correo electrónico o un portal en línea, entre otros)? |

|  |
| --- |
| Temática: Manejo de incidentes y la mejora continua |
| Para esta evaluación, el auditor debe evaluar que la organización cuente con un enfoque efectivo para el manejo de incidentes y la mejora continua. Para realizarlo, debe verificar si los procedimientos y protocolos están alineados con las mejores prácticas en SIC, si se toman medidas y se mide el impacto luego de un incidente y si la organización demuestra una voluntad constante de aprender y evolucionar en función de las experiencias pasadas mediante la actualización del plan de respuesta a incidentes.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se mide y registra el impacto de los incidentes en la seguridad (pérdida de datos, el tiempo de inactividad del sistema, el daño a la reputación, entre otros)? * ¿Se toman medidas de respuesta pertinentes y se documentan? * ¿Se implementan acciones correctivas después de cada incidente?¿Se realizan acciones correctivas para abordar causas raíz? * ¿El impacto de los incidentes se evalúa de manera adecuada? * ¿Se han actualizado el plan y las prácticas según lecciones aprendidas? * ¿Los cambios realizados en el plan son justificados y documentados? * ¿El personal responsable está al tanto de las actualizaciones y cambios? |