

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Concientización y Capacitación en SIC**

**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 seguridad de la información y ciberseguridad (SIC) comienza con la identificación de habilidades y conocimientos específicos para los equipos técnicos, que deben estar capacitados para configurar y mantener los niveles de seguridad necesarios en dispositivos, sistemas y servicios. A partir de esta base, se elabora un programa de concientización que refuerza el compromiso del personal con la seguridad y adapta las actividades de capacitación a los distintos roles dentro de la organización, cubriendo tanto al personal interno como a los contratistas y consultores externos. Los programas de concientización también integran lecciones aprendidas de incidentes de seguridad pasados, proporcionando una visión práctica y continua del impacto de la seguridad en las operaciones diarias.

**1.1 Estrategias de Capacitación y Sensibilización en Seguridad**

Para maximizar la efectividad del programa, la capacitación en SIC emplea diversas metodologías, desde conferencias y autoestudios hasta rotación de roles y asesoría de expertos. La concientización en seguridad cubre aspectos clave, como el compromiso de la dirección, la responsabilidad individual en la protección de información y procedimientos básicos de seguridad, tales como la gestión de contraseñas y la notificación de eventos de seguridad. Además, el programa incorpora canales físicos y digitales, como boletines, módulos de aprendizaje y campañas en redes internas, para difundir de manera eficaz la información y reforzar el cumplimiento de normas y procedimientos de seguridad. Estas actividades de sensibilización proporcionan al personal los recursos y puntos de contacto necesarios para obtener orientación adicional, manteniendo una cultura organizacional comprometida con la seguridad.

**1.2 Rol de la Auditoría en la Evaluación de Concientización y Capacitación en SIC**

Desde la perspectiva de auditoría, el monitoreo de los programas de concientización y capacitación en SIC implica evaluar la comprensión del personal al finalizar cada actividad y medir la transferencia de conocimientos. La auditoría revisa la actualización continua de conocimientos técnicos mediante suscripciones a boletines y participación en eventos especializados, asegurando que el personal se mantenga al día en las mejores prácticas de seguridad. Además, la auditoría supervisa que las políticas y procedimientos de seguridad sean comunicados regularmente a todo el personal y evalúa la eficacia del programa de concientización mediante ajustes y mejoras continuas en función de los resultados obtenidos. Esta supervisión permite que SIC mantenga un programa de capacitación adaptable y efectivo, que responda a los desafíos cambiantes de seguridad y promueva una cultura de protección activa en la organización.

.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. 1. Identificar las habilidades y conocimientos específicos para los equipos técnicos cuyas funciones requieran preparar e implementar un plan de capacitación adecuado. Estos equipos deben tener las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas, aplicaciones y servicios. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. 1. Elaborar un programa de concientización sobre la seguridad de la información que contenga: 2. 1.1 como objetivo que el personal sea consciente de sus responsabilidades con respecto a la seguridad de la información y los medios por los cuales se cumplen 3. esas responsabilidades. 4. 1.2 en cuenta las funciones del personal en el organización, incluido el personal interno y externo (por ejemplo, consultores externos, personal del proveedor). 5. 1.3 actividades programadas con regularidad, para que se repitan y cubran al nuevo personal. También debe basarse en las lecciones aprendidas de los incidentes de seguridad de la información. 6. 2. Considerar dentro del programa de educación y capacitación diferentes formas [p. conferencias o autoestudios, ser asesorado por personal experto o consultores (capacitación en el trabajo), rotar a los miembros del personal para seguir diferentes actividades, reclutar personas ya capacitadas y contratar consultores]. 7. 3. Incluir dentro de la concientización sobre la seguridad de la información aspectos generales como: 8. 3.1 el compromiso de la dirección con la seguridad de la información en toda la organización. 9. 3.2 las necesidades de familiarización y cumplimiento con respecto a las normas y obligaciones de seguridad de la información aplicables, teniendo en cuenta la política de seguridad de la información y las políticas, estándares, leyes, estatutos, reglamentos, contratos y acuerdos específicos del tema. 10. 3.3 responsabilidad personal por las propias acciones e 11. inacciones, y responsabilidades generales para asegurar o proteger la información que pertenece a la organización y las partes interesadas. 12. 3.4 procedimientos básicos de seguridad de la información [p. informes de eventos de seguridad de la información y controles de referencia [p. seguridad de contraseña]. 13. 3.5 puntos de contacto y recursos para obtener información adicional y asesoramiento sobre asuntos de seguridad de la información, incluidos más materiales de concientización sobre la seguridad de la información. 14. 4. Incluir dentro del programa de sensibilización una serie de actividades de sensibilización a través de canales físicos o virtuales apropiados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas, sesiones informativas, módulos de aprendizaje y correos electrónicos. 15. 5. Distribuir al personal de la organización y las partes interesadas relevantes la documentación correspondiente respecto a la concientización, educación y capacitación adecuada en seguridad de la información. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. 1. Realizar programas de concientización, la educación y la capacitación en seguridad de la información periódicamente y cuando sea necesario. 2. 2. Asegurar que el personal técnico mantenga sus conocimientos actualizados suscribiéndose a boletines y revistas o asista a congresos y eventos destinados a la mejora técnica y profesional. 3. 3. Asegurar que el personal de la organización y las partes interesadas reciban actualizaciones periódicas de la política de seguridad de la información de la organización, así como, las políticas y los procedimientos específicos que correspondan para las funciones que desempeñen. 4. 3.1 Estas deben tener en cuenta la información de la organización que debe protegerse y los controles de seguridad de la información que se han implementado para proteger la información. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. 1. Evaluar la comprensión del personal al final de una actividad de sensibilización, educación o formación para probar la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y formación, |
| 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. 1. Realizar modificaciones necesarias para asegurar la eficacia del programa de sensibilización, educación y formación según los resultados de las evaluaciones anteriores. |

# Preguntas de Auditoría para Concientización y Capacitación en SIC

|  |
| --- |
| Temática: Cumplimiento de políticas y procedimientos de concientización y capacitación en SIC |
| Es fundamental que la concientización y las capacitaciones en seguridad de la información y ciberseguridad estén documentadas en políticas y procedimientos para garantizar la consistencia, trazabilidad y cumplimiento en toda la organización. La documentación formal establece un marco claro para la planificación, ejecución y seguimiento de las iniciativas de concientización, asegurando que se aborden adecuadamente las necesidades de formación de todos los empleados. Por lo tanto, el auditor debe evaluar la existencia y contenido, así como el cumplimiento de políticas y procedimientos relevantes.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Los empleados conocen las políticas, estándares, leyes, reglamentos y otros acuerdos específicos relacionados con la seguridad de la información y ciberseguridad? ¿La organización establece sanciones en caso de incumplimiento? * Revisar la política de seguridad de la información y evaluar lo siguiente:   + ¿La política está actualizada y es comunicada efectivamente?   + ¿Está alineada con los objetivos y necesidades de la organización?   + ¿ Establece los controles de seguridad necesarios para proteger la información de acuerdo con su nivel de sensibilidad y valor para la organización?   + ¿Abarca todos los activos de información críticos y los sistemas relevantes? * ¿Existen políticas documentadas que respalden programas periódicos de concientización? ¿Cómo se planifican, desarrollan e implementan los programas? * ¿Se han implementado métodos efectivos para comunicar las actualizaciones de la política de seguridad de la información y las políticas y procedimientos específicos? * ¿Se fomenta la suscripción a boletines y revistas técnicas, así como la asistencia a eventos para mantener conocimientos ¿Cómo se incentiva al personal técnico a mantenerse actualizado? * ¿Cómo asegura la organización que todos los empleados estén al tanto de las políticas y actualizaciones? * ¿Se asignan los recursos adecuados para implementar y mantener controles de seguridad efectivos? |

|  |
| --- |
| Temática: Programa de concientización y capacitación en SIC |
| Evaluar el programa de concientización y capacitación en Seguridad de la Información (SIC) implica llevar a cabo una revisión exhaustiva de las iniciativas implementadas por una organización para educar y preparar a su personal en la adopción de prácticas y comportamientos seguros en relación con SIC. En este sentido, esta evaluación tiene como objetivo fundamental garantizar que el programa sea efectivo, actualizado y abarque temas, tanto relevantes propios de la organización como generales, de SIC.  El auditor debe evaluar el contenido de los materiales educativos, incluyendo seminarios, cursos en línea y recursos informativos, para determinar si abordan de manera adecuada los riesgos y amenazas actuales de SIC. Además, debe verificar si la capacitación es accesible a todos los niveles de empleados, desde la alta dirección hasta los roles más operativos, y si se adapta a las responsabilidades y necesidades específicas de cada grupo. Asimismo, debe verificar la frecuencia y regularidad de la capacitación para asegurar que el programa no solo sea una actividad puntual, sino que haya una planificación continuada para reforzar y actualizar los conocimientos de seguridad.  Para la evaluación, el auditor debe tener en consideración: Revisión de aspectos generales Este levantamiento puede incluir análisis específicos tales como:   * ¿La documentación de concientización, educación y capacitación se distribuye adecuadamente al personal de la organización y a las partes interesadas relevantes? * ¿El programa abarca todos los aspectos relevantes de la seguridad de la información y ciberseguridad?   + ¿Se ha definido claramente su propósito y metas?   + ¿Se han definido los objetivos? ¿Están alineados con las políticas y estrategias de seguridad de la información de la organización?   + ¿Se han establecido KPI’s para medir el impacto del programa en los empleados? * ¿Los métodos utilizados (sesiones presenciales, capacitación en línea, campañas de correo electrónico, entre otros**)** son efectivos para llegar a la audiencia objetivo?   + ¿Los empleados participan activamente en las sesiones?   + ¿Se fomenta la participación? * ¿La organización mantiene el programa actualizado para abordar las nuevas amenazas o riesgos de seguridad de la información? * ¿La organización ha considerado en su programa la diversidad de funciones y roles que pueden existir en la organización?  Contenido del programa Este levantamiento puede incluir análisis específicos tales como:   * ¿El contenido del programa es comprensible y adecuado para el nivel de conocimiento y experiencia del personal?   + ¿Se presentan ejemplos y casos prácticos para ilustrar la responsabilidad personal y las responsabilidades generales relacionadas con la seguridad de la información y ciberseguridad?   + ¿Las campañas, folletos, carteles, boletines, sitios web, sesiones informativas, módulos de aprendizaje y correos electrónicos son claros, relevantes y se ajusta al público objetivo? * ¿Se proporciona información detallada sobre las prácticas de seguridad que se esperan de cada función? * ¿El contenido del programa es adecuado en consideración de las prioridades de la organización? Esto incluye:   + Brindar capacitación que conciencie y ayude a mitigar los riesgos más severos   + Se adecúa al contexto de la organización, y de la función particular de cada participante   + ¿Considera ataques y casos en industrias u organizaciones similares?  Actividades y materiales del programa Este levantamiento puede incluir análisis específicos tales como:   * ¿Están programadas con regularidad para asegurar una cobertura continua? * ¿Están diseñadas para abordar los aspectos clave de la seguridad de la * información y ciberseguridad? ¿Se encuentran actualizadas según las últimas amenazas y riesgos? * ¿El programa incluye actividades específicas destinadas a cubrir al nuevo personal (inducción y capacitación en aspectos relevantes de la seguridad de la * información)? * ¿Los canales seleccionados son apropiados para el público objetivo? ¿Abarcan diferentes medios para llegar a los empleados? * ¿Los materiales utilizados son comprensibles y adecuados para el público objetivo? * ¿abordan aspectos generales y contienen información sobre puntos de contacto y recursos adicionales? * ¿El programa de concientización cubre a todo el personal de la organización, incluyendo tanto el personal interno como el personal externo? |

|  |
| --- |
| Temática: Evaluación y mejora continua del programa |
| En esta evaluación, el auditor debe garantizar que la organización tenga un enfoque sistemático y proactivo para la evaluación y mejora continua mediante la verificación de la efectividad de las evaluaciones y la implementación de cambios en el programa. Esta evaluación tiene como objetivo principal asegurarse de que el programa no solo sea efectivo en su diseño inicial, sino que también evolucione de manera acorde con los cambios en el entorno de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realizan pruebas o cuestionarios de conocimiento al finalizar las actividades de concientización? * ¿Se hace un seguimiento de la aplicación de conocimientos adquiridos ¿Cómo se verifica que los conocimientos se estén aplicando en la práctica? * ¿Se recopila retroalimentación del personal sobre la utilidad del programa? ¿Qué opiniones y percepciones tiene el personal sobre el programa? * ¿Se han identificado áreas de mejora a través de evaluaciones anteriores? ¿Qué aspectos específicos se han destacado para mejorar? * ¿Se han implementado modificaciones basadas en las evaluaciones anteriores? * ¿Las modificaciones han tenido un impacto positivo en la concientización y educación de los empleados sobre la seguridad de la información? |