

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Habilidades y Competencias del Personal**

**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 gestión de habilidades y competencias en la función de seguridad de la información y ciberseguridad (SIC) comienza con la identificación de habilidades y competencias actuales tanto de recursos internos como externos y la detección de brechas frente a los requisitos de SIC. Con base en estas brechas, se distribuyen los fondos asignados en programas de capacitación a nivel nacional, regional o local. La capacitación se clasifica según su orden de prioridad en capacitación para la promoción, capacitación de perfeccionamiento para mejorar el desempeño y capacitación voluntaria de interés institucional. También se incluyen programas de desarrollo profesional sobre privacidad y seguridad, tanto en la capacitación inicial como en sesiones frecuentes para gerentes, altos ejecutivos y contratistas, asegurando que todos estén preparados para responder a cambios en el sistema y requisitos de seguridad específicos de cada rol.

**1.1 Desarrollo de Planes de Capacitación y Concientización en Seguridad y Privacidad**

Para cubrir de manera efectiva las brechas de habilidades, se desarrollan planes de acción que abarcan la capacitación en habilidades técnicas y de comportamiento, la contratación y la reasignación. Estos planes incluyen la documentación de políticas y procedimientos de sensibilización y capacitación en seguridad, con un enfoque en el cumplimiento y la coherencia con normativas legales y políticas organizativas. La capacitación específica para roles críticos se ofrece antes de conceder acceso a los sistemas y cuando surgen cambios importantes. Además, la organización establece contacto con grupos y asociaciones en la comunidad de seguridad y privacidad para proporcionar una educación continua, mantenerse al tanto de las mejores prácticas y compartir información actualizada sobre amenazas y vulnerabilidades.

**1.2 Rol de la Auditoría en la Gestión de Habilidades y Competencias en SIC**

Desde la perspectiva de auditoría, gestionar las habilidades y competencias en SIC implica revisar periódicamente las políticas y procedimientos de capacitación, garantizando que los materiales sean pertinentes y se adapten a los requisitos cambiantes de la empresa. La auditoría supervisa la documentación de actividades de capacitación y concientización, evaluando la evolución de las competencias a través de sistemas de calificación del desempeño y verificando que los resultados de la capacitación se utilicen como base para la promoción, los estímulos y las medidas correctivas. La auditoría asegura que las lecciones aprendidas de incidentes de seguridad se incorporen en los programas de capacitación, promoviendo la mejora continua de habilidades en SIC y asegurando una plantilla preparada y consciente de sus responsabilidades de seguridad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar las habilidades y competencias disponibles actuales, tanto de recursos internos como externos.  2. Identificar las brechas entre las habilidades requeridas y las disponibles, según esto, distribuir los fondos que les sean asignados en programas de capacitación nacionales, regionales o locales.  3. Definir los tipos de capacitación existentes, según su orden de preferencia en el plan de acción, como se señala a continuación:  3.1 La capacitación para la promoción que corresponde a aquella que habilita a los funcionarios para asumir cargos superiores  3.2 La capacitación de perfeccionamiento, que tiene por objeto mejorar el desempeño del funcionario en el cargo que ocupa.  3.3 La capacitación voluntaria, que corresponde a aquella de interés para la institución, y que no está ligada a un cargo determinado ni es habilitante para el ascenso.  4. Brindar capacitación y programas de desarrollo profesional sobre privacidad y seguridad de la información (incluidos gerentes, altos ejecutivos y contratistas):  4.1 Como parte de la capacitación inicial para nuevos usuarios y de manera frecuente posteriormente.  4.2 Cuando lo requieran por cambios en el sistema o después de algún evento definido por la organización.  5. Brindar capacitación en seguridad y privacidad específica del rol que desempeña al personal que corresponda:  5.1. Antes de autorizar el acceso al sistema, a la información o de realizar las tareas asignadas  5.2. Cuando sea requerido por cambios en el sistema  6. Utilizar la acreditación para aumentar un conjunto de habilidades profesionales de seguridad de la información de calidad. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Desarrollar planes de acción, como capacitación (habilidades técnicas y de conducta), contratación, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas desde el punto de vista individual y colectivo.  2. Desarrollar la documentación correspondiente a:  2.1 Políticas de concientización, capacitación y seguridad del personal a nivel de organización, de procesos del negocio y de sistema que:  2.1.1 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.  2.1.2 Sea coherente con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, normas y directrices aplicables.  2.2. Procedimientos para facilitar la implementación de la política de sensibilización, formación y seguridad del personal y los controles de sensibilización, formación y seguridad del personal asociados.  3. Establecer e institucionalizar el contacto con grupos y asociaciones seleccionados dentro de las comunidades de seguridad y privacidad:  3.1 Para facilitar la educación y capacitación continua sobre seguridad y privacidad para el personal de la organización.  3.2 Para mantener la vigencia con las prácticas, técnicas y tecnologías de seguridad y privacidad recomendadas.  3.3 Para compartir información actual de seguridad y privacidad, incluidas amenazas, vulnerabilidades e incidentes.  4. Establecer programas apropiados de educación, capacitación y concientización en toda la empresa para la seguridad de la información, conforme a los requisitos de procesos organizativos, incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad.  5. Distribuir la documentación pertinente al personal y a quien corresponda. Estos deben conocer y entender las políticas y procedimientos presentados en la documentación.  6. Designar un responsable para gestionar el desarrollo, documentación y difusión de la política y procedimientos de sensibilización, formación y de seguridad del personal.  7. Proporcionar acceso a los repositorios de conocimiento para respaldar el desarrollo de habilidades y competencias.  8. Obtener un acuerdo formal del personal sobre las políticas y los requisitos de 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. Revisar y actualizar las políticas y los procedimientos de concientización, capacitación y seguridad del personal frecuentemente.  2. Revisar los materiales y programas de capacitación de forma regular. Garantizar su idoneidad con respecto a los requisitos en constante evolución de la empresa y su impacto sobre el conocimiento, capacidades y habilidades necesarias. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Documentar, conservar y monitorear las actividades de capacitación en seguridad y privacidad de la  información, incluida la capacitación en concientización sobre seguridad y privacidad y la capacitación específica en seguridad y privacidad basada en roles.  2. Realizar evaluaciones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos. Evaluar la planificación de los reemplazos.  3. Calificar, mediante un sistema de calificación, que tenga por objeto evaluar el desempeño y las aptitudes de cada funcionario, atendidas las exigencias y características de su cargo, y servirá de base para la promoción, los estímulos y la eliminación del servicio, regido por una junta calificadora, quienes deberán evaluar anualmente a los funcionarios. |
| 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. Proporcionar comentarios sobre los resultados de la capacitación organizacional al personal capacitado y a quienes corresponda.  2. Actualizar el contenido de capacitación y concientización sobre alfabetización frecuentemente incorporando las lecciones aprendidas de incidentes o violaciones de seguridad internos o externos en las técnicas de alfabetización y concientización. |

# Preguntas de Auditoría para las Habilidades y Competencias del Personal

|  |
| --- |
| Temática: Identificación de habilidades y competencias |
| Este análisis es un proceso esencial para asegurar que la organización cuente con el personal adecuado, con las capacidades correctas para lograr sus objetivos estratégicos, mantener la seguridad de la información y mantenerse competitiva en un entorno empresarial en constante cambio. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha revisado la documentación relacionada con la identificación de habilidades y competencias disponibles, incluyendo registros de recursos humanos y contratos con proveedores externos? * ¿El plan de recursos humanos de la organización incluye una evaluación de las habilidades necesarias para alcanzar los objetivos estratégicos y los objetivos de la función de SIC?¿Se ha evaluado si el personal posee las certificaciones, capacitaciones y habilidades requeridas? * ¿La organización tiene una metodología formal para identificar las brechas entre habilidades requeridas y disponibles?   + ¿Se evaluaron los requisitos actuales y futuros de personal especializado en SIC?   + ¿Se identificaron carencias en habilidades, conocimientos o experiencia en personal de SIC?   + ¿Se evaluó la capacidad y competencia del personal actual en áreas relevantes de SIC? * ¿Los informes de evaluación de desempeño del personal se utilizan para identificar tendencias y brechas en habilidades? * ¿Los planes de acción para abordar las brechas de habilidades están alineados con los objetivos estratégicos y se centran en áreas críticas? * ¿Existe un proceso para identificar y abordar las brechas de habilidades emergentes debido a cambios en las amenazas de seguridad o avances tecnológicos? |

|  |
| --- |
| Temática: Programas de capacitación y concientización |
| El análisis del programa de capacitación y concientización es esencial para garantizar su eficacia, relevancia y alineación con los objetivos estratégicos de la organización. A través de la evaluación, se puede verificar si el programa está cumpliendo con los estándares de calidad y cumplimiento, si está abordando adecuadamente las necesidades y brechas de habilidades y competencias identificadas, y si está manteniendo al personal actualizado en temas críticos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han revisado las políticas y procedimientos de capacitación para asegurar que incluyan diferentes tipos de capacitación y su orden de preferencia? * ¿Las responsabilidades y funciones de las partes involucradas en la capacitación y concientización están definidas claramente? * ¿Los materiales y programas de capacitación tienen fechas de actualización claramente indicadas? * ¿Existe una metodología para la capacitación en privacidad y seguridad de la información?¿Se imparte antes de autorizar el acceso o asignar tareas? * ¿Se tienen registros de capacitación en privacidad y seguridad de la información para empleados y contratistas? * ¿Los programas de capacitación abarcan todos los aspectos relevantes de privacidad y seguridad de la información (incluyendo las políticas y procedimientos de la organización) y se alinean con necesidades de SIC?? * ¿Se establecen contactos con grupos y asociaciones en el ámbito de la seguridad y privacidad para facilitar la capacitación continua para el personal de la organización? * ¿Cómo se asegura la alineación de los programas de capacitación con las regulaciones, estándares de la industria y las necesidades cambiantes de seguridad de la información? * ¿Se proporciona capacitación específica para los diferentes roles dentro de la organización, adaptada a las responsabilidades individuales en términos de seguridad de la información? |

|  |
| --- |
| Temática: Evaluación y monitoreo continuo de las habilidades, competencias y programas de capacitación |
| El proceso de revisión implica saber cómo la organización realiza evaluaciones periódicas del personal para identificar sus habilidades y competencias actuales. Además, se analiza cómo se identifican las brechas de habilidades y se establecen planes de capacitación adecuados para abordar esas brechas. El monitoreo constante es esencial para asegurarse de que el personal esté adquiriendo las habilidades necesarias y que los programas de capacitación se adapten según sea necesario.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se llevan a cabo evaluaciones periódicas de habilidades y competencias? ¿Qué criterios se utilizan y cómo se documentan los resultados? * ¿Existen registros de calificación y evaluación anual de los funcionarios? ¿Los resultados se utilizan para la promoción y el estímulo o la eliminación del servicio de los funcionarios? * ¿La organización proporciona retroalimentación de la capacitación a través de reuniones individuales o sesiones grupales? * ¿Se realiza un seguimiento regular del progreso de las acciones de capacitación y planes de acción para abordar las brechas de habilidades? ¿Cómo se reportan los resultados? * ¿El contenido de capacitación incluye lecciones aprendidas de incidentes de seguridad relevantes? * ¿El contenido de capacitación se actualiza en función de incidentes y cambios en la seguridad de la información? |