

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Selección 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.
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 selección de personal en la función de seguridad de la información y ciberseguridad (SIC) es un proceso estratégico que asegura que los candidatos cumplan con los requisitos de competencia, confiabilidad y cumplimiento de políticas de seguridad. Este proceso incluye la aplicación de controles de verificación de antecedentes para todos los candidatos, teniendo en cuenta leyes y regulaciones aplicables a privacidad y protección de datos personales (PII). Para roles críticos en SIC, las verificaciones pueden ampliarse para incluir referencias, antecedentes laborales, confirmación de identidad y calificaciones, y en algunos casos, revisiones de crédito o antecedentes penales. Estas medidas garantizan que los nuevos empleados tengan la competencia y confiabilidad necesarias para cumplir con las expectativas de seguridad y contribuir positivamente a la organización.

**1.1 Estructura de Procesos y Requisitos en la Selección de Personal**

La estructura de los procesos de selección debe abarcar desde el personal a tiempo completo hasta aquellos con roles temporales, estableciendo un comité de selección que supervise la selección para cargos de responsabilidad y evaluando las competencias específicas necesarias en cada caso. Para cargos de jefatura, el proceso suele incluir concursos y evaluaciones que consideran la experiencia, capacitación, y aptitudes requeridas, asegurando una selección basada en mérito. Además, los procesos de selección incorporan un periodo de prueba para los empleados, permitiendo evaluar su idoneidad y ajuste a la cultura organizacional y los objetivos de SIC. La recopilación y manejo de información sobre los candidatos se lleva a cabo respetando la legislación aplicable, integrando también los requerimientos de seguridad en los procedimientos de contratación para empleados, contratistas y proveedores.

**1.2 Rol de la Auditoría en la Evaluación del Proceso de Selección de Personal en SIC**

Desde la perspectiva de auditoría, la evaluación del proceso de selección en SIC incluye verificar la alineación de los procesos de contratación y selección con las políticas de la organización y sus objetivos de seguridad. Los auditores revisan que los controles de verificación se realicen de manera periódica y que el sistema de selección responda a los cambios en el perfil de riesgo organizacional. La auditoría también se asegura de que los requisitos de seguridad se integren adecuadamente en la gestión de recursos humanos, y que los procesos de selección se adapten en función de los resultados de evaluaciones y controles previos. Este enfoque garantiza que SIC mantenga una dotación de personal confiable y competente, contribuyendo a una base sólida en seguridad de la información y ciberseguridad en toda la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Aplicar los controles de verificación de antecedentes de todos los candidatos para convertirse en personal antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.  2. Incluir dentro de la verificación de antecedentes toda la legislación relevante sobre privacidad, protección de PII y respecto al empleo y, cuando esté permitido, debe incluir lo siguiente:  2.1 disponibilidad de referencias satisfactorias (por ejemplo, referencias comerciales y personales).  2.2 una verificación (de integridad y precisión) del currículum vitae del solicitante.  2.3 confirmación de las calificaciones académicas y profesionales reclamadas.  2.4 verificación de identidad independiente (por ejemplo, pasaporte u otro documento aceptable emitido por autoridades).  2.5 verificación más detallada, como revisión de crédito o revisión de antecedentes penales, si el candidato adquiere un papel crítico.  3. Asegurar que cuando se contrata a una persona para una función específica de seguridad de la información, esta:  3.1 tenga la competencia necesaria para desempeñar la función de seguridad.  3.2 sea confiable para asumir el rol, especialmente si el rol es crítico para la organización. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir los criterios y limitaciones para las revisiones de verificación (por ejemplo, quién es elegible para evaluar a las personas y cómo, cuándo y por qué se  llevan a cabo las revisiones de verificación).  2. Establecer un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. El concurso será preparado y realizado por un comité de selección, conformado por el jefe o encargado de personal y por quienes integran la  junta central o regional.  3. Asegurar que el proceso para seleccionar los cargos de jefes de departamento y los de niveles de jefaturas jerárquicos equivalentes de los ministerios y servicios públicos sean de carrera y se sometan a las siguientes reglas:  3.1 La provisión de estos cargos se hará mediante concursos en los que podrán participar los funcionarios de planta y a contrata de todos los ministerios y servicios que cumplan con los requisitos correspondientes  3.2 el comité de selección propondrá a la autoridad facultada para efectuar el nombramiento, los nombres de a lo menos tres ni más de cinco candidatos pertenecientes a la planta del ministerio o servicio que realice el concurso  3.3 A falta de postulantes idóneos deberá llamarse a concurso público  3.4 La permanencia en estos cargos de jefatura será por un período de tres años, este se podrá prorrogar una vez al término del primer periodo trienal.  4. Asegurar que exista un sistema de empleo a prueba como parte del proceso de selección para él o del personal. Este podrá extenderse entre 3 y 6 meses, según lo determine el jefe superior del servicio.  5. Considerar a lo menos los siguientes factores dentro de los concursos realizados: los estudios y cursos de formación educacional y de capacitación; la experiencia laboral, y las aptitudes específicas para el desempeño de la función.  6. Recopilar y manejar la información sobre todos los candidatos que son considerados para puestos dentro de la organización teniendo en cuenta la legislación pertinente existente en la jurisdicción correspondiente.  7. Incorporar los requerimientos de seguridad de la información en los procesos de gestión de recursos humanos y reclutamiento, tanto para empleados, contratistas o proveedores. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Evaluar los riesgos de la contratación (habilidades no bien definidas, etc.).  2. Mantener los procesos de contratación y retención de personal para el área de SIC en línea con todas las políticas y procedimientos de personal de la organización. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Repetir periódicamente los controles de verificación para confirmar la idoneidad continua del personal, según la importancia del rol que tenga.  2. Revisar periódicamente los procesos de selección y contratación para verificar que están en línea con las políticas y procedimientos de la organización. |
| 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. Realizar modificaciones necesarias para asegurar que los controles de verificación cumplan con los objetivos generales y de SIC de la organización según la información obtenida.  2. Realizar modificaciones a los procesos de selección y contratación según la información obtenida. |

# Preguntas de Auditoría para la Selección del Personal

|  |
| --- |
| Temática: Selección del personal de seguridad de la información y ciberseguridad |
| La selección del personal es fundamental para garantizar que los empleados estén adecuadamente asignados a roles y responsabilidades en función de su nivel de riesgo y competencias. Para la evaluación, el auditor debe tener en consideración: Asignación de riesgos a los puestos organizacionales Este levantamiento puede incluir análisis específicos tales como:   * ¿Los registros de asignación de riesgos a los puestos contienen detalles exhaustivos sobre los factores considerados en la asignación? * ¿Las designaciones de riesgo se corresponden con las funciones y responsabilidades de cada puesto de seguridad de la información y ciberseguridad? * ¿Los empleados y partes interesadas conocen las implicaciones y responsabilidades asociadas con sus designaciones de riesgo? * ¿La organización mantiene planes de mitigación claros para abordar los riesgos asociados con las designaciones de alto riesgo?   + Verifique que los planes de mitigación están disponibles y accesibles para asegurar una respuesta rápida a los incidentes. * ¿Se revisan y actualizan periódicamente las asignaciones de riesgo para reflejar cambios en funciones y responsabilidades?  Criterios de selección de personal Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización establece y documenta los criterios específicos y relevantes para cada puesto en función de seguridad de la información y ciberseguridad? * ¿Los criterios de selección incluyen habilidades, experiencia, conocimientos técnicos y competencias necesarias para cada puesto? * ¿El proceso de reclutamiento y selección se guía por criterios objetivos y justos, evitando cualquier forma de discriminación o sesgos injustos? * ¿Los candidatos seleccionados cumplen con los criterios establecidos? * ¿Se comunican claramente a los candidatos los criterios de selección utilizados? * ¿El proceso de selección es consistente y se aplica de manera similar a todos los candidatos para un puesto dado. |

|  |
| --- |
| Temática: Evaluación de políticas y procedimientos de verificación de antecedentes |
| La evaluación de políticas y procedimientos de verificación de antecedentes se refiere a revisar y examinar cómo la organización lleva a cabo la revisión de antecedentes de los candidatos durante el proceso de selección de personal. Esta auditoría se enfoca en asegurarse de que las políticas y los procedimientos establecidos para verificar los antecedentes de los candidatos sean efectivos, consistentes y cumplan con los estándares de seguridad y legalidad. Este levantamiento puede incluir análisis específicos tales como:   * ¿Las políticas y procedimientos de verificación de antecedentes están alineados con las leyes, regulaciones y ética aplicables? * ¿Se consideran los requisitos comerciales y los riesgos percibidos al establecer los controles de verificación? * ¿Se verifican los antecedentes de los candidatos tanto antes de la contratación como de manera continua durante su empleo? * ¿Se documentan adecuadamente los resultados de las verificaciones de antecedentes? * ¿Las verificaciones de antecedentes cumplen con las leyes de privacidad y protección de datos? * ¿Se realizan verificaciones proporcionales a la clasificación de la información a la que los empleados tienen acceso? * ¿Las verificaciones de antecedentes se actualizan según las políticas y cambios en la situación del empleado? |

|  |
| --- |
| Temática: Evaluación de competencias y requisitos de personal |
| Durante la auditoría, el auditor revisa los procedimientos documentados para llevar a cabo verificaciones de antecedentes, como verificación de referencias laborales, revisión de historiales criminales, validación de credenciales académicas y otras investigaciones relevantes. Se evalúa si estos procedimientos se aplican de manera coherente y equitativa a todos los candidatos y si se ajustan a las leyes y regulaciones aplicables. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se verifican las competencias técnicas requeridas para las funciones de seguridad? * ¿Se evalúan las referencias y antecedentes laborales para asegurar la confiabilidad de los candidatos? * ¿Los candidatos son asignados a roles que se ajustan a sus competencias y habilidades? * ¿Las políticas de contratación incluyen criterios específicos de competencia y confiabilidad para funciones de seguridad? * ¿El personal mantiene sus certificaciones y capacitaciones actualizadas? * ¿Los proveedores de servicios cumplen con los requisitos de selección establecidos en los contratos? * ¿Las verificaciones de antecedentes son adecuadas para garantizar la idoneidad de los candidatos para roles de TI? |

|  |
| --- |
| Temática: proceso de selección y evaluación de candidatos |
| El proceso de selección y evaluación de candidatos se refiere a revisar y evaluar cómo la organización lleva a cabo todo el proceso de selección de nuevos empleados, desde la identificación de vacantes hasta la elección final de candidatos para ocupar los puestos. Esta evaluación se enfoca en asegurar que el proceso sea justo, transparente, eficiente y esté alineado con los objetivos estratégicos de la organización, incluyendo la seguridad de la información. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se siguen criterios claros para determinar quién puede llevar a cabo las revisiones de verificación? * ¿Las entrevistas se realizan de manera consistente y justa para todos los candidatos? * ¿Los métodos de evaluación de candidatos son adecuados y consistentes con los objetivos de las revisiones? * ¿Los candidatos son informados de manera transparente acerca de los pasos del proceso de selección, los criterios de evaluación y el tiempo estimado para la toma de decisiones? * ¿Las pruebas de habilidades y evaluaciones durante el proceso de selección son relevantes y suficientes? * ¿Se toman decisiones de contratación considerando todos los factores relevantes y evitando sesgos? |

|  |
| --- |
| Temática: Evaluación de riesgos y controles en el proceso de contratación |
| La evaluación de riesgos y controles en el proceso de contratación se refiere a revisar y evaluar cómo la organización identifica, analiza y mitiga los riesgos asociados con la incorporación de nuevos empleados. Esta evaluación se centra en asegurarse de que se hayan implementado medidas adecuadas para mitigar los riesgos potenciales que podrían surgir durante el proceso de contratación.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han identificado y evaluado los posibles riesgos asociados al proceso de contratación? * ¿Se realizan comprobaciones adecuadas para validar la experiencia y la formación de los candidatos? * ¿Las descripciones de puestos están libres de vacíos o ambigüedades que puedan generar riesgos? * ¿Se realizan evaluaciones periódicas para asegurarse de que los controles son efectivos? * ¿Los registros y documentación de contratación cumplen con los requisitos establecidos? * ¿La organización identifica los factores que podrían aumentar el riesgo de que el candidato no permanezca en el puesto a largo plazo? * ¿Se implementan estrategias de retención para mitigar estos riesgos? |

|  |
| --- |
| Temática: Evaluación de controles de verificación y procesos de contratación |
| La evaluación de controles de verificación y procesos de contratación implica revisar cómo la organización implementa y gestiona medidas de seguridad y verificación para asegurarse de que el proceso de contratación sea adecuado, confiable y alineados con los objetivos de SIC. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han implementado estrategias efectivas para retener al personal en el área de SIC? * ¿Los procesos de contratación y retención cumplen con todas las leyes laborales y regulaciones aplicables? * ¿Se proporciona capacitación adecuada al personal involucrado en el proceso de contratación y retención? * ¿Se implementan medidas sólidas para garantizar la privacidad y seguridad de los datos personales de los candidatos durante el proceso de selección y contratación? |

|  |
| --- |
| Temática: Evaluación de resultados y mejora continua |
| La evaluación de resultados y mejora continua implica revisar cómo la organización evalúa y utiliza los resultados de sus operaciones para mejorar de manera constante y adaptarse a las demandas cambiantes. Además de asegurar que la organización esté comprometida con la eficiencia, efectividad y seguridad en sus operaciones, incluyendo la seguridad de la información y la gestión de riesgos asociado. Este levantamiento puede incluir análisis específicos tales como:   * ¿Los controles de verificación han sido efectivos para detectar y prevenir desviaciones o riesgos en los procesos de SIC? * ¿Los procesos de selección y contratación han proporcionado personal con las habilidades y conocimientos necesarios? * ¿Las métricas de contratación, como la calidad y la duración del servicio, han mejorado después de implementar modificaciones en el proceso de contratación? * ¿La información personal de los candidatos se maneja y protege de acuerdo con las leyes de privacidad? |