

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Términos y Condiciones de Empleo**

**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

Definir y supervisar los términos y condiciones de empleo en la función de seguridad de la información y ciberseguridad (SIC) implica verificar que los términos contractuales estén alineados con el acceso que cada miembro tendrá a los activos de la organización, considerando la política de seguridad de la información y las políticas específicas de privacidad y confidencialidad. Para roles críticos, los acuerdos de confidencialidad, los derechos y responsabilidades legales, y las medidas de protección de la información deben detallarse claramente, garantizando que las responsabilidades contractuales del personal incluyan una continuidad en la protección de información sensible incluso después de finalizar el empleo.

**1.1 Obligaciones y Código de Conducta para Cumplir con la Seguridad de SIC**

Los términos de empleo deben establecer obligaciones específicas del personal, como el cumplimiento de horarios, la dedicación al cargo y la observancia del principio de probidad administrativa, entre otros. Estos lineamientos aseguran que cada miembro del personal esté comprometido con el cumplimiento de los objetivos de la organización y las responsabilidades relacionadas con la seguridad de la información, incluyendo la protección de datos personales y el uso adecuado de los activos de la organización. El mantenimiento de un código de conducta formal proporciona claridad sobre las expectativas éticas, el uso adecuado de la información y la confidencialidad, estableciendo prácticas respetables y de conformidad con las normas de la organización y los requisitos legales aplicables.

**1.2 Rol de la Auditoría en la Revisión de los Términos y Condiciones de Empleo en SIC**

Desde la perspectiva de auditoría, supervisar los términos y condiciones de empleo en SIC implica realizar revisiones periódicas para garantizar que el personal haya aceptado y comprendido sus responsabilidades contractuales en cuanto a la seguridad de la información. Los auditores verifican que se mantengan acuerdos necesarios y que el cumplimiento de términos y condiciones se adapte a los cambios en el entorno normativo, tales como leyes, regulaciones o políticas de SIC. Además, la auditoría revisa la periodicidad de actualización de los términos de empleo y mide la comprensión y conformidad del personal con sus obligaciones, promoviendo mejoras continuas para corregir cualquier ineficiencia y asegurar que los términos se actualicen en respuesta a cambios en los requisitos de cumplimiento. Esta supervisión asegura que la organización mantenga una base de seguridad sólida y adaptativa, alineada con los estándares internos y externos de SIC.

1. **Modelo de Madurez**

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Verificar que los términos y condiciones sean apropiados para la naturaleza y el alcance del acceso que cada miembro del personal o contratista tendrá con los activos de la organización asociados a los sistemas y servicios de información, a través del estudio de los procesos en los que interviene y las funciones que tiene asociadas.  2. Verificar que las obligaciones contractuales del personal tengan en cuenta la política de seguridad de la información de la organización y las políticas específicas de los temas pertinentes. Además, se pueden aclarar y señalar los siguientes puntos:  2.1 acuerdos de confidencialidad o no divulgación que el personal al que se le da acceso a información confidencial debe firmar antes de tener acceso a la  información y otros activos asociados.  2.2 responsabilidades y derechos legales [p. en relación con las leyes de derechos de autor o la legislación de protección de datos.  2.3 responsabilidades para la clasificación de la información y la gestión de la  información de organización y otros activos asociados, instalaciones de procesamiento de información y servicios de información manipulados por el personal.  2.4 responsabilidades por el tratamiento de la  información recibida de las partes interesadas.  2.5 las responsabilidades contenidas continúen por un período definido después de poner fin al empleo y cuando corresponda.  2.6 acciones a tomar si el personal ignora los requisitos de seguridad de la organización.  3. Incluir dentro de las obligaciones contractuales del personal:  3.1 Desempeñar personalmente las funciones del cargo en forma regular y continua, sin perjuicio de las normas sobre delegación.  3.2 Orientar el desarrollo de sus funciones al cumplimiento de los objetivos de la institución y a la mejor prestación de los servicios que a ésta correspondan.  3.3 Realizar sus labores con esmero, cortesía, dedicación y eficiencia, contribuyendo a materializar los objetivos de la institución.  3.4 Cumplir la jornada de trabajo y realizar los trabajos extraordinarios que ordene el superior jerárquico.  3.5 Cumplir las destinaciones y las comisiones de servicio que disponga la autoridad competente.  3.6 Obedecer las órdenes impartidas por el superior jerárquico.  3.7 Observar estrictamente el principio de la probidad administrativa regulado por la ley Nº 18.575 y demás disposiciones especiales.  3.8 Guardar secreto en los asuntos que revistan el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por  instrucciones especiales.  3.9 Observar una vida social acorde con la dignidad del cargo.  3.10 Proporcionar con fidelidad y precisión los datos que la institución le requiera relativos a situaciones personales o de familia, cuando ello sea de interés para la Administración, debiendo ésta guardar debida reserva de estos.  3.11 Denunciar ante el Ministerio Público, o ante la policía si no hubiere fiscalía en el lugar en que el funcionario presta servicios, con la debida prontitud, los crímenes o simples delitos y a la autoridad competente los hechos de carácter irregular de que tome conocimiento en el ejercicio de su cargo.  3.12 Rendir fianza cuando debido a su cargo tenga la administración y custodia de fondos o bienes, de conformidad con la Ley Orgánica Constitucional de la Contraloría General de la República.  3.13 Justificarse ante el superior jerárquico de los cargos que se le formulen con publicidad, dentro del plazo que éste le fije, atendidas las circunstancias del caso. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Comunicar a los candidatos las funciones y responsabilidades de seguridad de la información durante el proceso previo al empleo.  2. Asegurar que el personal esté de acuerdo con los términos y condiciones relacionados con la seguridad de la información.  3. Mantener un código de conducta para establecer las responsabilidades de seguridad de la información del personal con respecto a la confidencialidad, la protección de la PII, la ética, el uso adecuado de la información de la organización y otros activos asociados, así como las prácticas respetables esperadas por la organización. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Realizar revisiones periódicas para garantizar que el personal contratado haya firmado y aceptado todos los acuerdos necesarios.  2. Realizar revisiones periódicas respecto a los cambios en el entorno que afecten los requisitos de cumplimiento (leyes, regulaciones, acuerdos) o las políticas de seguridad de SIC. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Recopilar información respecto a la periodicidad de actualización y revisión de términos y condiciones de empleo.  2. Medir el entendimiento y la conformidad del personal en el cumplimiento de los términos y condiciones establecidos en sus contratos de trabajo. |
| 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 cambios necesarios para corregir ineficiencias respecto a la periodicidad de actualización y revisión de términos y condiciones de empleo.  2. Actualizar los términos y condiciones cada vez que ocurre un cambio importante en los requisitos de cumplimiento (leyes, regulaciones, acuerdos) o las políticas de seguridad de SIC. |

# 3. Preguntas de auditoría para los Términos y Condiciones de Empleo

|  |
| --- |
| Temática: Alcance de los contratos |
| En esta evaluación, el auditor debe examinar y evaluar cómo la organización define y gestiona el alcance de sus contratos comerciales y legales, garantizando que los contratos estén claramente definidos, que aborden todos los aspectos SIC necesarios para todos los miembros de la organización, contratistas, proveedores y otros agentes externos a la organización que tengan una implicancia para SIC. Durante la auditoría, el auditor revisa los contratos existentes para asegurarse de que el alcance de los acuerdos y compromisos esté claramente establecido y definido.  Para la evaluación, el auditor debe tener en consideración: Términos y condiciones de accesos y su cumplimiento normativo Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene un proceso establecido para revisar y actualizar regularmente los términos y condiciones relacionados con el acceso a sistemas y servicios? * ¿Se asegura que los términos estén alineados con las leyes y regulaciones vigentes? * ¿Se define claramente el alcance del acceso requerido por cada miembro del personal o contratista a los sistemas y servicios de información? * ¿Se consideran las necesidades mínimas de acceso necesarias para desempeñar sus funciones? * ¿Se verifica que los términos y condiciones definidos para cada miembro del personal o contratista sean apropiados para la naturaleza y el alcance de su acceso? * ¿Los términos y condiciones reflejan los niveles de acceso necesarios y las responsabilidades asociadas? * ¿Se registra y verifica la revisión de términos y condiciones antes de otorgar acceso a los sistemas? * ¿Existen registros de acceso a sistemas y servicios que muestren el cumplimiento del proceso de verificación de términos y condiciones? * ¿Qué acciones toma la organización en caso de incumplimiento de los requisitos de seguridad de la información por el personal?  Contratos con contratistas y proveedores Este levantamiento puede incluir análisis específicos tales como:   * ¿Los contratos con terceros que involucran acceso a activos de la organización incluyen cláusulas de seguridad de la información? * ¿Se mencionan en los contratos las responsabilidades específicas, la clasificación de la información, y el manejo de datos sensibles? * ¿Los contratos establecen claramente las consecuencias en caso de incumplimiento de las cláusulas de seguridad?  Contratos de trabajo con empleados Este levantamiento puede incluir análisis específicos tales como:   * ¿Los contratos de trabajo de los empleados que manejan información sensible incluyen cláusulas relacionadas con la seguridad de la información? * ¿Los contratos definen las responsabilidades y obligaciones del personal en relación con la seguridad y manejo de la información? * ¿Se detallan las consecuencias del incumplimiento de las cláusulas de seguridad en los contratos de trabajo? * ¿Las descripciones de los puestos incluyen claramente las funciones y responsabilidades de seguridad de la información que se esperan del candidato? * ¿Las descripciones son precisas y específicas en cuanto a las tareas de seguridad?  3.2.4 Acuerdos de confidencialidad y políticas Este levantamiento puede incluir análisis específicos tales como:   * ¿Todos los empleados han firmado acuerdos de confidencialidad y políticas de seguridad?   + ¿Los empleados conocen su responsabilidad en cuanto a la protección de la seguridad de la información contenidas en los acuerdo de confidencialidad y políticas asociadas?   + ¿Las responsabilidades contenidas en los acuerdo de confidencialidad continúan por un período definido después de poner fin al empleo y cuando corresponda? * ¿El código de conducta de la organización aborda aspectos relevantes de seguridad de la información? |

|  |
| --- |
| Temática: Comunicación, documentación y materiales informativos de los términos y condiciones |
| Evaluar la comunicación, documentación y materiales informativos de los términos y condiciones se refiere a examinar y evaluar cómo la organización comunica y documenta los términos y condiciones de sus acuerdos, contratos o servicios a sus usuarios, clientes o partes involucradas, asegurando que los términos y condiciones sean transparentes, comprensibles y accesibles para todas las partes, y que se proporcione la información necesaria de manera clara y precisa.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Durante las entrevistas de empleo, se discuten las funciones y responsabilidades específicas de seguridad de la información con los candidatos dentro de los términos y condiciones de empleo?¿Se proporciona una visión clara de las expectativas en cuanto a la seguridad? * ¿La organización proporciona documentos como descripciones de trabajo y políticas de seguridad de la información? * ¿La documentación de los términos y condiciones se presenta de manera clara y legible para los usuarios? * ¿La documentación hace referencia a las políticas y estándares de seguridad relacionados con el acceso y la información? * ¿La organización mantiene registros que demuestren que se ha comunicado a los candidatos sobre sus funciones y responsabilidades de seguridad de la información?¿Estos registros incluyen detalles de las comunicaciones y las fechas? * ¿Los formularios de solicitud de empleo incluyen secciones relacionadas con la seguridad de la información? * ¿Se proporcionan materiales informativos adicionales, como resúmenes visuales o videos explicativos, para ayudar a los usuarios a comprender mejor los términos y condiciones?¿Estos materiales complementan la documentación escrita? |

|  |
| --- |
| Temática: Seguimiento, acciones correctivas y mejora continua de la organización |
| Mediante estas pruebas de auditoría, el auditor debe ser capaz de examinar y evaluar cómo la organización supervisa y aborda las acciones necesarias para corregir deficiencias, resolver problemas y mejorar sus procesos y prácticas en materia de seguridad de la información, asegurando que existan procedimientos efectivos para identificar, abordar y prevenir problemas, y que la organización esté comprometida con la mejora constante. Para la evaluación, el auditor debe tener en consideración: Actualización y cumplimiento de términos y condiciones Este levantamiento puede incluir análisis específicos tales como:   * ¿Las revisiones identifican cambios en regulaciones y políticas que afecten los términos y condiciones de empleo? * ¿Existe un registro de fechas de vencimiento de acuerdos firmados por el personal contratado? * ¿La organización tiene una política clara sobre la periodicidad de actualización de términos y condiciones de empleo? * ¿Existen registros que demuestren la actualización y revisión de términos y condiciones? * ¿Se incluyen métricas sobre la actualización en informes de recursos humanos?  Evaluación de conocimientos y monitoreo Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización mide el conocimiento del personal sobre sus términos y condiciones de empleo? * ¿Se lleva a cabo un monitoreo continuo para asegurar el cumplimiento de los términos? * ¿Se implementan medidas correctivas en caso de incumplimiento?  Implementación de medidas correctivas Este levantamiento puede incluir análisis específicos tales como:   * ¿Las medidas correctivas propuestas se implementan en tiempo y forma? * ¿Se han documentado adecuadamente los resultados y acciones tomadas en revisiones anteriores?¿Existe un registro de las acciones tomadas en respuesta a ineficiencias identificadas? * ¿Se verifica la efectividad de las medidas correctivas implementadas?  Seguimiento y documentación de mejoras Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización mantiene registros de seguimiento sobre medidas correctivas implementadas? * ¿Se realizan entrevistas con personal responsable para evaluar la implementación de recomendaciones? * ¿Se documentan las acciones tomadas y las fechas correspondientes para cada mejora realizada? |