

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Gestión del Personal Externo**

**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 del personal externo en la función de seguridad de la información y ciberseguridad (SIC) incluye garantizar que el número de empleados contratados no supere el límite del 20% del personal de planta y que los términos de sus contratos, en particular la duración y las escalas de remuneración, se ajusten a las políticas institucionales. Los acuerdos contractuales con terceros deben prever que la organización tiene el derecho de supervisar el uso de recursos de TI por parte de los contratistas, permitiendo una gestión segura y alineada con las expectativas organizacionales.

**1.1 Definición de Roles y Responsabilidades en Contratos para Personal Externo**

Para asegurar una colaboración efectiva y conforme a los requisitos de SIC, los contratos con personal externo deben ser claros en cuanto a roles, responsabilidades y normas de seguridad aplicables. Las responsabilidades de seguridad y privacidad deben estar documentadas y exigir que los proveedores externos cumplan con las políticas y procedimientos de la organización, incluyendo la notificación sobre cualquier cambio en el personal con privilegios de acceso a sistemas de información. Este nivel de especificidad en los contratos proporciona claridad a los contratistas y garantiza que las funciones de seguridad estén debidamente integradas en el trabajo del personal externo. Además, un acuerdo formal de cumplimiento con los controles de SIC debe ser obtenido de los contratistas al inicio del contrato, incluyendo el respeto a los controles de acceso, requisitos de confidencialidad y acuerdos de no revelación.

**1.2 Rol de la Auditoría en la Gestión de Personal Externo en SIC**

Desde la perspectiva de auditoría, la gestión del personal externo en SIC implica verificar que los roles y derechos de acceso de los contratistas sean adecuados y estén alineados con los términos del contrato. Los auditores realizan revisiones periódicas para asegurar que el cumplimiento de los requisitos de SIC esté actualizado, considerando los cambios en el entorno normativo y en las políticas de seguridad. Además, la auditoría evalúa la periodicidad de las actualizaciones en los términos y condiciones de los contratos con personal externo, proporcionando recomendaciones para corregir ineficiencias y asegurar que los contratos se adapten en respuesta a cambios significativos en los requisitos de cumplimiento. Este enfoque garantiza una gestión de personal externo que no solo cumpla con las políticas de seguridad de SIC, sino que también fortalezca la seguridad organizacional en todos los niveles de colaboración.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Asegurar que el número de funcionarios a contrata de una institución no exceda la cantidad equivalente al veinte por ciento del total de los cargos de la planta de personal de ésta.  2. Verificar que los terceros, con el que el personal del proveedor esté asociado, mantenga acuerdos contractuales en nombre de la persona contratada.  3. Avisar a los contratistas de que los directivos se reservan el derecho a supervisar e inspeccionar todo el uso de los recursos de TI, incluido el correo electrónico, comunicaciones de voz y todos los programas y archivos de datos.  4. Verificar que los empleos a contrata duren, como máximo, hasta el 31 de diciembre de cada año y que los empleados que los sirvan expiren en sus funciones en esa fecha.  5.Asegurar que se revisa el trabajo de contratistas y se basa la aprobación de los pagos en los resultados.  6. Verificar que las escalas de remuneraciones que se asignen a los empleos a contrata no excedan el tope máximo que se contempla para el personal de las plantas de Profesionales, de Técnicos, de Administrativos y de Auxiliares en el respectivo órgano o servicio, según sea la función que se encomiende. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir en contratos formales y no ambiguos todo el trabajo realizado por personal externo en términos de roles y responsabilidades. Estos deben incluir:  1.1 Establecer los requisitos de seguridad del personal, incluidas las funciones y responsabilidades de seguridad de los proveedores externos.  1.2 Exigir a los proveedores externos el cumplimiento de las políticas y procedimientos de seguridad del personal establecidos por la organización.  1.3 Documentar los requisitos de seguridad del personal.  1.4 Exigir a los proveedores externos que notifiquen a los encargados sobre cualquier transferencia de personal o despido de personal externo que posea credenciales y/o distintivos de la organización, o que tenga privilegios del sistema.  1.5 Vigilar el cumplimiento por parte de los proveedores de los requisitos de seguridad del personal.  2. Proporcionar a los contratistas, como parte de sus contratos, una definición clara de sus roles y responsabilidades, incluidos los requisitos explícitos para documentar su trabajo conforme a los estándares y formatos acordados. Se deben Incorporar roles y responsabilidades de seguridad y privacidad en las descripciones de puestos organizacionales.  3. Obtener el acuerdo formal de los contratistas de que deben cumplir con el marco de control de SIC empresarial, así como con las políticas y verificaciones de seguridad, control del acceso físico y lógicos, uso de las instalaciones, requisitos de confidencialidad de la información y acuerdos de no revelación al inicio del contrato |
| 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 los roles de los contratistas y los derechos de acceso sean adecuados y conforme a los contratos.  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 por parte del personal externo o de carácter transitorio. |
| 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 del personal externo o de carácter transitorio. |
| 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 del personal externo o de carácter transitorio.  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. |

# Preguntas de Auditoría para la Gestión del Personal Externo

|  |
| --- |
| Temática: Plantilla del personal interno y externo de la institución |
| Durante esta evaluación, el auditor examina la composición de la plantilla de personal, considerando tanto a los empleados a contrata como a los de planta. El auditor debe examinar si existe un equilibrio adecuado entre ambas categorías, si las capacidades y competencias de los empleados son acordes a sus roles y responsabilidades, y si se cumple con la normativa laboral y contractual correspondiente.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La plantilla de personal de la institución incluye información detallada sobre cada funcionario, tanto contratados, de planta y externos, que abarque su cargo, roles, responsabilidades y antecedentes laborales? * ¿Existen documentos que respalden la contratación de funcionarios a contrato? * ¿Se han justificado las necesidades temporales, como proyectos específicos, picos de trabajo u otras necesidades? * ¿Los contratos de los funcionarios contratados están disponibles para su evaluación? ¿Se verifica que los contratos estén vigentes y que no superen el período permitido por la normativa? |

|  |
| --- |
| Temática: Contratos con terceros y proveedores |
| El auditor también debe asegurarse de que los contratos sean sólidos, cumplan con las necesidades y expectativas de la organización, y aborden de manera adecuada los aspectos relacionados con SIC. Durante esta evaluación, el auditor revisa los contratos celebrados con terceros y proveedores para asegurarse de que sean claros, comprensibles y detallen adecuadamente los términos, condiciones, roles y responsabilidades de ambas partes. Este levantamiento puede incluir análisis específicos tales como:   * ¿Los acuerdos contractuales con terceros están formalizados por escrito? ¿Se verifica que los contratos estén firmados y en vigencia?   + Verifique que todos los contratos pasan por una evaluación de riesgo previo a su firma.   + Evalúe el riesgo asociado a la cadena de suministro, en consideración de la continuidad de las operaciones. Identifique la existencia de riesgos por proveedores críticos / únicos.   + Verifique que se toman acciones para mitigar los riesgos asociados al trabajo de personal y proveedores externos.   + Verifique que la contratación externa se encuentra justificada, en consideración de otras alternativas de contratación.   + Verifique que se han utilizado los mecanismos de contratación o compras públicas que corresponden según lo indica la ley. * ¿Los contratos establecen de manera clara y detallada que el personal del proveedor está autorizado para representar y actuar en nombre del proveedor ante terceros?   + ¿Los acuerdos contractuales estipulan los límites y alcance de la autorización del personal del proveedor? * ¿Los acuerdos contractuales han sido revisados para asegurar que sean apropiados y adecuados para las relaciones y transacciones previstas con terceros?   + ¿Los contratos definen claramente los roles y responsabilidades?   + ¿Los contratos establecen los términos para documentar el trabajo?   + ¿Los roles y responsabilidades son coherentes con los acuerdos previos?   + ¿Los requisitos de seguridad específicos para el personal externo están definidos? * ¿Se ha verificado que los contratos cumplan con los requisitos legales y regulaciones aplicables en las jurisdicciones pertinentes? * ¿Los acuerdos contractuales se actualizan y renuevan según sea necesario para reflejar cambios en las relaciones comerciales y requisitos legales y regulatorios? * ¿Los contratos tienen fechas de inicio y finalización claras? ¿Cómo se notifica a los empleados sobre la finalización de sus contratos? |

|  |
| --- |
| Temática: Supervisión y control de personal contratista |
| Evaluar la supervisión y control de personal contratista se refiere a examinar y evaluar cómo la organización gestiona y monitorea a los trabajadores a contrata que realizan labores para la organización, asegurándose que existan procesos efectivos para supervisar y controlar las actividades de los contratistas, incluyendo aspectos relacionados con SIC. Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha proporcionado una comunicación clara y formal a los contratistas sobre el derecho de supervisión e inspección por parte de los directivos de la organización? * ¿Existen registros que demuestren que se han llevado a cabo inspecciones sistemáticas de los recursos de TI utilizados por los contratistas? * ¿Se ha generado documentación durante las inspecciones, como registros de uso de correo electrónico, comunicaciones de voz, programas y archivos de datos? * ¿Las inspecciones se han realizado de acuerdo con las políticas y procedimientos establecidos y se han implementado medidas para proteger la privacidad y confidencialidad de la información de los contratistas? * ¿Se verifican los registros de supervisión e inspección para confirmar que se están realizando de manera adecuada y que se están siguiendo los procedimientos establecidos? * ¿La organización supervisa que el personal contratista haya participado en inducción, capacitación y concienciación respecto de los principios y responsabilidades de SIC? Esto podría incluir:   + Que conocen su responsabilidad para con la seguridad de la información de la organización.   + Que conocen los requisitos contractuales que se desprenden de sus obligaciones con la SIC en la organización.   + Que conocen la clasificación de información que manejan, hayan suscrito y comprendan los NDA.   + Que controlan sus propios sistemas y tienen implementadas salvaguardas y controles de seguridad mínimos.     - Considere solicitar auditorías de segunda parte para asegurar que la     - información compartida con proveedores es recibida y almacenada de forma segura. * ¿Se aplican los controles básicos de seguridad y control de acceso con los proveedores y personal externo? Algunos de estos controles pueden ser:   + Exigencia de MFA   + Principio de Mínimo Privilegio   + Acceso Temporal a los Sistemas Formación en Básica en SIC Monitoreo y Registro de Actividades   + Aplicación de Políticas y Procedimientos de BYOD o Teletrabajo Exigencia de la gestión de actualización y parches   + Suscripción a Políticas de Uso Aceptable * ¿La organización cuenta con procedimientos para desactivar rápidamente el acceso del personal externo en caso de terminación del contrato anticipado, o comportamiento sospechoso? * ¿El personal externo cuenta y conoce los mecanismos para reportar incidentes de seguridad?   + Verifique que existen planes de respuesta a incidentes que incluya procedimientos específicos para abordar brechas de seguridad relacionadas con el personal externo. Por ejemplo:     - Acceso Inadecuado     - Uso de Dispositivos Infectados / No seguros Filtración de Información     - Transmisión insegura de datos     - Detección de acceso persistente Introducción de malware |

|  |
| --- |
| Temática: Actualización y revisión de términos y condiciones del personal externo |
| Esta evaluación se enfoca en asegurarse de que los términos y condiciones sean adecuados, estén alineados con las necesidades y regulaciones cambiantes, y aborden asuntos de SIC, aquí, el auditor revisa cómo se lleva a cabo la actualización y revisión de los términos y condiciones para el personal externo, y analiza si existen mecanismos establecidos para identificar y abordar los cambios necesarios en los acuerdos, especialmente aquellos relacionados con SIC. Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe una política documentada que establece claramente la necesidad de actualizar y revisar periódicamente los términos y condiciones de empleo para el personal externo o de carácter transitorio? * ¿Se mantiene un registro actualizado del personal externo o de carácter transitorio que trabaja en la organización y cuyos términos y condiciones deben ser actualizados y revisados periódicamente? * ¿Los términos y condiciones de empleo del personal externo se actualizan y revisan según lo estipulado en la política y los procedimientos establecidos? * ¿Se han implementado acciones correctivas en caso de ineficiencias o retrasos en el proceso de actualización y revisión de términos y condiciones? * ¿Se verifican los registros y documentación para asegurarse de que se mantienen registros precisos y completos de las actualizaciones y revisiones realizadas en los términos y condiciones de empleo del personal externo o de carácter transitorio? |