

**CASIG 4 - Gestión de Recursos Humanos**

**Preguntas de Auditoría**

**Segregación y Continuidad de Funciones**

**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 aplicación de la segregación y continuidad de funciones en la función de seguridad de la información y ciberseguridad (SIC) asegura que ninguna persona tenga control absoluto sobre procesos críticos, reduciendo así el riesgo de errores o acciones malintencionadas. Como precaución de seguridad, establecer directrices para el tiempo mínimo de vacaciones de personas clave ayuda a detectar cualquier dependencia o irregularidad. Además, al manejar cambios laborales, especialmente terminaciones de contrato, la captura y el intercambio de conocimientos, la planificación de sucesión y el respaldo de personal garantizan que la organización no dependa de un solo individuo para desempeñar funciones críticas, reforzando así la continuidad operativa.

**1.1 Planificación de Respaldo y Evaluación de Funciones Críticas**

Para asegurar una continuidad eficaz, es crucial revisar regularmente los planes de respaldo de personal y la planificación de reemplazos de acuerdo con la importancia de los cargos y funciones críticas en SIC. Esta planificación incluye la evaluación periódica de la estructura de personal en posiciones clave, verificando que las prácticas de segregación de funciones se implementen correctamente y que haya personal capacitado disponible para cubrir funciones en caso de cambios imprevistos. La recopilación de información sobre la periodicidad y efectividad de estos planes de respaldo proporciona datos útiles para ajustar y mejorar las funciones actuales y futuras, asegurando que la estructura de SIC mantenga su efectividad y confiabilidad a lo largo del tiempo.

**1.2 Rol de la Auditoría en la Segregación y Continuidad de Funciones en SIC**

Desde la perspectiva de auditoría, la segregación y continuidad de funciones en SIC involucra la revisión de los planes de respaldo y los mecanismos de sucesión en roles críticos, verificando que se cumplan las mejores prácticas y que los riesgos de dependencia se mantengan bajo control. La auditoría evalúa si la segregación de funciones se ha implementado eficazmente, revisando la rotación de roles y la adherencia a las directrices de vacaciones mínimas, y si existe documentación adecuada y procesos de transferencia de conocimiento en roles clave. Este enfoque asegura que la organización esté preparada para enfrentar cualquier cambio en el personal, promoviendo una estructura robusta y adaptable que refuerce la seguridad y continuidad operativa de SIC.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Aplicar la segregación de tareas en el diseño de cargo y funciones de posiciones críticas. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Proporcionar directrices sobre un tiempo mínimo de vacaciones anuales que tomarán las personas clave como precaución de seguridad.  2. Tomar las acciones pertinentes relativas a cambios laborales, en especial terminación de contratos.  3. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único  individuo que realice un trabajo crítico.  4. Garantizar la segregación de funciones (SoD por sus siglas en inglés) en puestos críticos. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Comprobar regularmente los planes de respaldo de personal.  2. Evaluar regularmente la planificación de los reemplazos según la importancia del cargo y funciones de las posiciones críticas . |
| NIVEL 4 [Gestionado  Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Recopilar información sobre la periodicidad y la aplicación de los planes de regulación y respaldo. |
| 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. Utilizar la información obtenida de la aplicación de segregación de funciones para mejorar los cargos actuales y futuros. |

# Preguntas de Auditoría para la Segregación y Continuidad de Funciones

|  |
| --- |
| Temática: Definición de Responsabilidades y Segregación de Funciones |
| Este análisis es esencial para garantizar el cumplimiento normativo, reducir riesgos operativos y financieros, y mejorar la confianza y transparencia en las operaciones de la organización. Durante la auditoría, el auditor examina cómo la organización define y documenta las funciones y responsabilidades de cada empleado, y cómo se asegura de que exista una segregación adecuada entre las tareas que puedan generar conflictos de interés. Para la evaluación, el auditor debe tener en consideración: Definición de Responsabilidades Este levantamiento puede incluir análisis específicos tales como:   * ¿Las responsabilidades y funciones de cada cargo están claramente definidas?   + ¿Las funciones y responsabilidades se ajustan a los criterios y mejores prácticas adoptadas por la organización? Por ejemplo, ¿Utiliza el lenguaje común de definiciones de los marcos generales como NICCS? * ¿Las descripciones de cargos críticos están actualizadas?   + Verifique que las descripciones de los cargos corresponden a las actividades descritas en los procedimientos y tareas. * ¿Se ha evaluado la estructura organizativa para identificar posiciones críticas?   + ¿La estructura organizativa evita concentración excesiva de responsabilidades en puestos críticos? * Verifique que la organización revisa los registros de incidentes de seguridad pasados para identificar si hubo problemas relacionados con la definición de responsabilidades.  Segregación de Funciones  * ¿Los niveles de acceso y autorización cumplen con los principios de segregación de funciones? * ¿Existen controles y salvaguardas para garantizar la segregación de funciones y prevenir conflictos de interés?   + Verifique que se aplica una matriz de segregación de funciones que contenga en sus ejes la lista de funciones/tareas y los empleados/roles.   + Compruebe que la matriz de segregación de funciones identifica que roles tienen acceso a qué sistemas, e identifica los escenarios de riesgo de acceso excesivo o insuficiente   + Verifique que existe una clara separación de deberes, esto incluye revisar las responsabilidades de autorización, ejecución y registro de transacciones en los SI. Puede incluir otro tipo de responsabilidades asociadas a los activos de información.   + Realice pruebas de efectividad para determinar si el esquema de segregación de funciones trabaja de forma efectiva. Pruebe realizando y revisando transacciones. * ¿Los procesos y flujos de trabajo en las posiciones críticas han sido analizados? * ¿Las exclusiones y excepciones en la segregación de funciones se encuentran identificadas, documentadas y aprobadas? ¿Qué controles alternativo se aplica? * Verifique que ninguna persona puede realizar un proceso de punta a punta, sobre todo, aquellos procesos que derivan en ciber riesgo * ¿Se mantienen registros de revisiones periódicas de la segregación de funciones? |

|  |
| --- |
| Temática: Continuidad de Funciones |
| La planificación laboral para asegurar la continuidad de funciones se refiere a revisar y evaluar cómo la organización planifica y gestiona la distribución de personal y recursos humanos de manera que las funciones críticas de la organización puedan ser llevadas a cabo de manera continua, incluso en situaciones adversas o de emergencia u otras razones como enfermedades, vacaciones o eventos inesperados. Para la evaluación, el auditor debe tener en consideración: Políticas de seguridad y descanso Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen políticas específicas relacionadas con la seguridad y el tiempo de descanso? * ¿Se cumple con el tiempo mínimo de vacaciones anuales establecido? * ¿Las directrices sobre el tiempo de vacaciones cumplen con regulaciones laborales y legales? * ¿La organización sigue estándares normativos y legales con relación al descanso?  Planes de Respaldos de Personal Este levantamiento puede incluir análisis específicos tales como:   * ¿Hay personal capacitado para asumir funciones clave en ausencia del personal principal?   + Verifique que los perfiles de cargo y hojas de vida del personal de apoyo son adecuados para cumplir con el rol que se le otorgará. * ¿Existen planes de respaldo actualizados que reflejen las necesidades actuales de la organización?   + Verifique que el personal de respaldo cuenta con todos los criterios mínimos para poder operar el proceso o función que cubrirá, incluyendo:     - Haya suscrito los acuerdos de confidencialidad necesarios.     - Cuente con el conocimiento y habilidades técnicas necesarias.     - Se encuentre capacitado a través de un proceso formal.     - Cuenta con información documentada en forma de procesos y procedimientos para guiar su deber.     - Cuenta con el aprovisionamiento temporal necesario en sus usuarios y atributos para los SI que deberá operar. * ¿Los planes de respaldo aseguran continuidad operativa y transición efectiva?   + Verifique que la organización cuenta con análisis formales de continuidad operativa, tales como:     - Cálculo de capacidades mínimas necesarias para la operación Planes de contención a incidentes     - Planes de recuperación ante desastres     - Planes de continuidad del negocio     - Planes de continuidad de procesos de negocio * ¿El personal conoce los planes de respaldo y su papel en situaciones de ausencia?   + Realice entrevistas y verifique si la organización ha realizado simulaciones que permitan determinar si el personal es capaz de cumplir con las tareas de respaldo que le son asignadas.  Planificación de Reemplazos y Continuidad  * Examine los planes de Recuperación ante Desastres (DRP) y Continuidad del Negocio (BCP) para asegurarse de que están actualizados, son exhaustivos y contienen toda la información necesaria para asegurar la continuidad cuando existe una falla de personal.   + Simule escenarios de reemplazo o salida inesperada de personal clave, para evaluar como la organización maneja la situación. * ¿Se ha identificado a sucesores potenciales para posiciones críticas?   + ¿Se captura y documenta el conocimiento relevante para las actividades críticas? Por ejemplo, a través de procedimientos y manuales documentados y validados por los dueños de procesos actuales.   + ¿Existen mecanismos para intercambiar conocimientos y desarrollar sucesores? Algunos ejemplos pueden ser:     - Matriz de Responsabilidades de Continuidad     - Matriz de Capacitación y Transferencia de Conocimientos   + ¿Se han identificado y entrenado sucesores para funciones clave? * ¿La documentación de planificación de reemplazos está en orden y actualizada?   + Verifique que la documentación de planificación incluye también acuerdos con proveedores externos. * ¿La planificación de reemplazos se revisa periódicamente y se actualiza según cambios? |