

**05 - Control de Acceso**

**CASIG 1 – Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Establecer Roles y Responsabilidades**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimientos en normativa de seguridad de la información y ciberseguridad. 2. Conocimientos en contextos de riesgos de SIC. 3. Conocimientos en modelos de gobernanza, 3 LoD, roles y responsabilidades en SIC. 4. Conocimientos en análisis y alineamiento estratégico. |

# Visión General

Definir roles y responsabilidades específicas permite claridad en cuanto a las expectativas de cada puesto y también facilita el establecimiento de líneas claras de autoridad y comunicación, promoviendo una colaboración sin fricciones entre los diferentes equipos involucrados. Con la asignación precisa de funciones, cada miembro del equipo comprende qué se espera de su rol y cómo sus acciones contribuyen a proteger los activos de información, mitigando riesgos de seguridad y garantizando el cumplimiento de las normativas aplicables. La falta de roles definidos puede llevar a ineficiencias, responsabilidades difusas y una gestión de incidentes inadecuada, factores que aumentan la vulnerabilidad ante ataques y el riesgo de incumplimientos regulatorios.

**1.1** **Asignación de Roles en Equipos de Seguridad de la Información**  
Dentro de los equipos de seguridad, el establecimiento de responsabilidades detalladas abarca desde la identificación de amenazas hasta la implementación de controles de seguridad. Cada equipo debe contar con un grupo de analistas de riesgo encargados de evaluar vulnerabilidades en el sistema, técnicos de ciberseguridad responsables de ejecutar medidas de protección, y un equipo de respuesta rápida para gestionar los incidentes que puedan surgir. Este enfoque especializado permite a la organización actuar de manera rápida y precisa ante potenciales riesgos de seguridad. Además, los gerentes de seguridad, a cargo de la supervisión global de los controles de seguridad, son responsables de revisar periódicamente el estado de protección de los sistemas y reportar avances y desafíos a la alta dirección. Esta estructura jerárquica optimiza el uso de recursos, asegurando que cada miembro de seguridad esté dedicado a áreas críticas específicas y que haya una vigilancia constante sobre los activos más valiosos.

**1.2** **El Rol de Auditoría en la Evaluación de Procesos y Conformidad Normativa**  
Por su parte, los equipos de auditoría cumplen una función complementaria en la gestión de la seguridad de la información al enfocarse en la evaluación sistemática de procesos, la verificación de conformidad y la revisión de registros. Este grupo de trabajo realiza auditorías tanto internas como externas, examinando cada uno de los procesos y controles de seguridad implementados para asegurar que se mantengan en alineación con los estándares organizacionales y regulatorios. Durante las auditorías, se evalúa no solo la efectividad de los controles, sino también la eficiencia operativa y la capacidad de respuesta ante incidentes. Estas revisiones periódicas contribuyen a identificar brechas de seguridad, debilidades en la infraestructura y deficiencias en el cumplimiento normativo, permitiendo a la organización mejorar continuamente sus prácticas de seguridad y establecer un entorno de transparencia y confianza.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1.- Desarrolla una estructura organizacional y las definiciones de roles generales para la SIC, sin una asignación de responsabilidades formalizada. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establece un proceso para evaluar y asignar roles y responsabilidades de seguridad de la información de acuerdo con la política de seguridad de la información y las políticas específicas del tema. Esto mediante la asistencia de expertos en SIC que comprenden el valor y los procesos del negocio.  1.1 Documenta los procesos y asegura que son faciles de encontrar para el personal  2. Documenta los roles y responsabilidades de seguridad de la información para los individuos o equipos en la organización.  3. Establece un proceso para garantizar que los individuos que asumen roles específicos de seguridad de la información sean competentes en el conocimiento y las habilidades requeridas para el rol y se les apoye para mantenerse actualizados con los desarrollos relacionados con el rol y requeridos para cumplir con las responsabilidades del rol. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Define formalmente las responsabilidades de seguridad de la información para:  1.1 Protección de la información y otros activos asociados.  1.2 Realizar procesos específicos de seguridad de la información.  1.3 Actividades de gestión de riesgos de seguridad de la información y en particular aceptación de riesgos residuales.  1.4 Todos los usuarios que utilizan la información y otros activos asociados de la organización.  1.5 Relaciones de informes con todo el personal de TI y SIC que corresponde  2. Proporciona orientación detallada adicional sobre las responsabilidades para sitios específicos y facilidades de procesamiento de información.  3. Define y documentar áreas de seguridad de las que son responsables los individuos.  4. Determina los niveles adecuados de delegación de autoridad, incluidas las reglas de limitaciones para las decisiones de SIC.  5. Define y documenta los deberes y las áreas de responsabilidad que deben segregarse para reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información. Los siguientes son ejemplos de actividades que pueden requerir segregación:  5.1 iniciar, aprobar y ejecutar un cambio;  5.2 solicitar, aprobar e implementar derechos de acceso;  5.3 diseñar, implementar y revisar el código;  5.4 desarrollar software y administrar sistemas de producción;  5.5 usar y administrar aplicaciones;  5.6 utilizar aplicaciones y administrar bases de datos;  5.7 diseñar, auditar y asegurar los controles de seguridad de la información.  6. Garantizar que los individuos que asumen roles específicos de seguridad de la información tengan las habilidades y conocimientos necesarios para realizar sus responsabilidades de manera efectiva.  7. Formaliza a través de una resolución el comité estratégico de SIC.  8. Formaliza a través de una resolución al encargado de la función de SIC. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establece metas y objetivos para el proceso de asignación de roles y responsabilidades de seguridad de la información, y medir el desempeño del proceso en relación con estos objetivos.  2. Establece un proceso para la identificación y gestión de los riesgos asociados con la asignación de roles y responsabilidades de seguridad de la información, y para la evaluación regular de la efectividad del proceso. |
| 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. Establece un proceso para la mejora continua del proceso de asignación de roles y responsabilidades de seguridad de la información, basado en la medición del desempeño y la evaluación de la efectividad.  2. Establece un proceso de innovación continua para la asignación de roles y responsabilidades de seguridad de la información, basado en la identificación de mejores prácticas y la implementación de mejoras continuas.  3. Establece un proceso para la gestión del cambio en la asignación de roles y responsabilidades de seguridad de la información, para garantizar que los cambios se gestionen de manera efectiva y eficiente y se minimice el impacto en la seguridad de la información. |

# Preguntas de Auditoría para Establecer Roles y Responsabilidades

|  |
| --- |
| 3.1 Temática: Definición de Roles y Responsabilidades |
| La evaluación y definición de roles y responsabilidades incluye la documentación detallada y sistemática del proceso para el establecimiento de la estructura organizacional que refleje los roles y responsabilidades generales para la SIC y que mantenga una jerarquización y una integración de funciones claramente establecidas y relacionadas entre individuos y departamentos de la organización.  Desde la perspectiva del auditor, esto implica verificar que se haya cumplido un proceso de evaluación y definición de roles y responsabilidades con la ayuda de expertos en SIC para alinear los procesos a los objetivos de seguridad de la información de la organización. Para esto el auditor debe abordar los siguientes puntos:  **3.1.1 Estructura organizacional**  Esto a modo de garantizar una distribución adecuada de tareas y funciones, lo que mejora la eficacia de la gestión de riesgos y la protección de los activos de la organización. Al involucrar a expertos en SIC, se asegura que las decisiones se tomen de manera informada y que se alinee la seguridad con los objetivos del negocio.   * ¿Se ha establecido una estructura organizacional que refleje roles, responsabilidades, autoridades y competencias y alcance de cada rol en cuanto a SIC? * ¿Mantienen relaciones jerárquicas y de reporte entre roles y entre departamentos de la organización? ¿Existen roles relacionados específicamente con SIC?   **3.1.2 Conocimiento y respaldo técnico para cumplir los estándares de SICAl**  Al contar con el respaldo técnico adecuado, se asegura que las funciones y responsabilidades asignadas sean efectivas y estén alineadas con las necesidades de protección de la organización. Esto contribuye a fortalecer la resiliencia ante posibles amenazas y vulnerabilidades, proteger los activos de información, y mantener la confidencialidad, integridad y disponibilidad de los datos críticos.  Asimismo, al contar con expertos en SIC, se promueve una cultura de seguridad proactiva y un enfoque estratégico hacia la protección de la información en toda la organización.   * ¿Existe la integración de expertos en SIC en el proceso de evaluación y asignación de roles y responsabilidades? * ¿Comprenden los expertos en SIC como la organización crea valor y como están establecidos los procesos del negocio de la organización? * ¿Se tomaron en cuenta las recomendaciones en base a criterios de evaluación sólidos y relevantes según el cumplimiento normativo o una evaluación de riesgos? |

|  |
| --- |
| **3.2 Temática: Mejora de procesos de asignación de Roles y Responsabilidades** |
| A través de la mejora continua, se busca identificar oportunidades de optimización, corregir posibles deficiencias y adaptar los roles y responsabilidades para abordar nuevos desafíos de seguridad. Este enfoque permite mantener la efectividad de los controles de seguridad y asegurar que los individuos asignados a cada función tengan el conocimiento y las habilidades adecuadas para cumplir con sus responsabilidades de manera efectiva.  Desde la perspectiva del auditor, esto implica verificar que se haya establecido un proceso de mejora continua basado en mediciones objetivas de desempeño y evaluaciones de efectividad del proceso. Para esto el auditor debe abordar los siguientes puntos:  **3.2.1 Proceso de recolección y análisis de datos**  Mediante la recopilación de datos cuantitativos, se busca medir y comparar el cumplimiento de las metas y objetivos establecidos, identificar posibles áreas de mejora y tomar decisiones informadas para optimizar el proceso. Estos datos proporcionan una visión objetiva del rendimiento del proceso, permitiendo a la organización tomar acciones correctivas y preventivas, asegurando que los roles y responsabilidades asignados sean apropiados, y garantizando una gestión más efectiva de la seguridad de la información y la ciberseguridad en la organización.   * ¿Se han establecido metas y objetivos claros en la organización en cuanto al proceso de asignación y evaluación de roles y responsabilidades? ¿Estas metas y objetivos son claros, medibles, alcanzables y tienen relación con SIC? * ¿Existe un proceso de recolección, tratamiento y análisis de datos que nos entregue información respecto al desempeño del proceso de evaluación y asignación de roles y responsabilidades en relación con SIC?   **3.2.2 Proceso formalizado de mejora continua, innovación y gestión del cambio**  El proceso de mejora continua y gestión del cambio busca adaptar la organización a nuevos desafíos y avances en el ámbito de la seguridad de la información, incorporando innovaciones y mejores prácticas. Al mantener un enfoque en la mejora constante, la organización se vuelve más resiliente y capaz de anticipar y responder proactivamente a los riesgos y amenazas emergentes.   * ¿Existe un proceso formalizado de mejora continua, innovación y de gestión del cambio implementada en la organización?   ¿Se utilizan los análisis de datos, lecciones aprendidas o un análisis de brechas y oportunidades dentro de este proceso? ¿Existen registros que respalden que se hayan realizado cambios dentro de las políticas de verificación y asignación de roles y responsabilidades que tengan que ver con SIC? |