

**1- Políticas de Control de Acceso e Identidad**



**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Evaluar la Gestión de Riesgos**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimiento en Gestión de Riesgos. 2. Conocimientos en normativa de seguridad de la información y ciberseguridad. 3. Conocimiento en normativa específica de riesgos: ISO 27005, NIST 800-30, MAGERIT y en los procesos de riesgos propios de la organización 4. Conocimiento en la normativa propia de la Industria o Sector. |

# Visión General

Dirigir la gestión de riesgos en la función de seguridad de la información y ciberseguridad (SIC) implica la traducción de la estrategia de riesgo de SIC en prácticas operativas, integrándola en la gestión de proyectos, cambios y versiones. La comunicación de riesgos debe extenderse a todos los niveles de la organización, asegurando que la dirección ejecutiva y otras partes interesadas comprendan y respalden las decisiones de riesgo. Al establecer mecanismos de respuesta rápida y principios de escalamiento, SIC garantiza que cualquier cambio en el entorno de riesgos sea notificado a los cargos directivos pertinentes, permitiendo una acción oportuna y adecuada.

**1.1 Formalización de Criterios y Evaluación de Riesgos en SIC**

Para gestionar eficazmente los riesgos, es crucial que SIC formalice criterios claros para la evaluación, priorización y respuesta a riesgos. Esto incluye la definición de términos clave como la severidad de riesgos, los criterios para aceptar, transferir o eliminar riesgos y las metodologías para gestionar estos procesos. Un proceso estructurado que utilice indicadores para evaluar la idoneidad de los criterios de riesgo permite a la organización monitorear si las tolerancias y posiciones generales frente al riesgo son adecuadas o requieren ajustes. Además, el establecimiento de un plan estratégico de gestión de riesgos, con objetivos claros y los recursos necesarios, ayuda a crear un enfoque consistente para la identificación, tratamiento y seguimiento de riesgos, asegurando que SIC cubra los aspectos críticos para la organización.

**1.2 Rol de la Auditoría en la Dirección de la Gestión de Riesgos en SIC**

Desde la perspectiva de auditoría, dirigir la gestión de riesgos en SIC implica una revisión exhaustiva del sistema de gestión de riesgos, verificando que los criterios, métodos y técnicas de evaluación estén alineados con los objetivos organizacionales y las mejores prácticas de la industria. Los auditores evalúan la implementación de un sistema estructurado que permita capturar y comunicar datos de riesgos, asegurando que cualquier riesgo, oportunidad o problema pueda ser identificado y comunicado en cualquier momento. La auditoría fomenta una cultura de aprendizaje y colaboración, promoviendo la mejora continua mediante el intercambio de experiencias y la retroalimentación basada en los hallazgos de las evaluaciones. Al asegurar que los procesos de gestión de riesgos de SIC sean adecuados y eficaces, la auditoría contribuye a una gestión de riesgos resiliente y proactiva que fortalece la postura de seguridad de la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Conocer la organización y su contexto en relación al riesgo de SIC y a los riesgos relacionados con activos de TI según normas nacionales e internacionales para incluirlos en la estrategia de gestión de riesgos. Se deben incluir evaluaciones de riesgos para la continuidad del negocio y la integridad de la información (como propiedad intelectual y memoria colectiva de la organización) derivados del uso de las TI.  2. Evaluar el apetito al riesgo de la organización, es decir, el nivel de riesgo relacionado con SIC que la empresa está dispuesta a tomar en la búsqueda de sus objetivos empresariales. ***[COMPLEMENTAR CON CONTROL: DEFINIR LA TOLERANCIA AL RIESGO]***  3. Evaluar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo. ***[COMPLEMENTAR CON CONTROL: DEFINIR LA TOLERANCIA AL RIESGO]***  4. Evaluar el grado de alineamiento de la estrategia de riesgos en SIC de la empresa con la estrategia de riesgos de la empresa en su conjunto y garantizar que el apetito al riesgo se sitúe por debajo de la capacidad de riesgo de la organización.  5. Establecer metas cuantitativas específicas para evaluar la efectividad de la gestión de riesgos de SIC en la identificación, evaluación, tratamiento y monitoreo de los riesgos de TI. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Revisar el proceso de gestión de riesgos de seguridad, verificando si se lleva a cabo de manera periódica y si se realizan acciones correctivas en función de los resultados obtenidos.  1.2 Evaluar la adecuación de las medidas de tratamiento de riesgos implementadas, asegurando que sean consistentes con las mejores prácticas y las políticas establecidas.  1.3 Analizar la efectividad de los métodos utilizados para identificar y evaluar los riesgos de TI, verificando si se han considerado los riesgos específicos de la organización.  2. Establecer un proceso formal y con responsabilidades definidas para la evaluación de la gestión de riesgos. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Evaluar los factores de riesgo de SIC de forma proactiva antes de tomar decisiones estratégicas a nivel de empresa y garantizar que las consideraciones del riesgo formen parte del proceso de decisión estratégico de la empresa.   2. Revisar las actividades de evaluación de la de gestión riesgos para asegurar que se alineen con la capacidad de la empresa para las pérdidas relacionadas con SIC y la tolerancia correspondiente por parte de la dirección. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer indicadores cuantitativos para evaluar las actividades de revisión y monitoreo del proceso de gestión de riesgos, para identificar posibles falsos positivos o falsos negativos, de esta forma, asegurar que el proceso de monitoreo de gestión de riesgos agrega el máximo valor posible y habilita la mejora continua. |
| 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. Utilizando la información de las métricas cuantitativas y cualitativas, perfeccionar el proceso de evaluación de gestión de riesgos incorporando o modificando las métricas y las formas de evaluar las actividades. |

# Preguntas de Auditoría para Evaluar la Gestión de Riesgos

|  |
| --- |
| 3.1 Temática: Evaluación de Políticas y Procedimientos de la Gestión de Riesgos |
| Esta revisión debe ser detallada y minuciosa, se examina la documentación relacionada con las políticas y procedimientos establecidos por la organización para la gestión de riesgos. El objetivo principal de esta práctica de auditoría es asegurarse de que las políticas y procedimientos sean adecuados, apropiados y alineados con los objetivos estratégicos de la organización. Se evalúa la coherencia y consistencia de estas políticas, asegurando que no haya conflictos o redundancias entre ellas. Además, verifica si las políticas y procedimientos están actualizados y reflejan las prácticas actuales de la organización en relación con la gestión de riesgos.   |  | | --- | | ℹ El establecimiento de la función de riesgos específica para SIC es un tema relevante que debe ser abordado en la Política de Seguridad de la Información. La política se detalla en el control “Política de Seguridad de la Información” |   Este levantamiento puede incluir análisis específicos tales como:   * ¿Los documentos de gestión de riesgos cumplen con los requisitos y lineamientos establecidos en las normas nacionales e internacionales, y los requisitos de cumplimiento?   + ¿Estos requisitos son aplicables y están relacionadas con la gestión de riesgos de SIC y activos de tecnologías de la información? * ¿En los documentos está establecido claramente cuál es el objetivo de identificar los factores y eventos que puedan afectar la seguridad de la información y los activos de TI durante este análisis? * ¿Existe de un marco de dirección para la gestión de riesgos de SIC en la organización? * ¿Los documentos relacionados con la gestión de riesgos, como políticas, procedimientos y registros, están adecuadamente documentados y actualizados?   + Revise si se encuentren listados en los maestros de gestión documental   + Revise si los documentos cuentan con una firma de revisor y aprobación formal   + Revise que existe los documentos mantienen un control de cambios y se hallan actualizados * ¿Se examina el contexto interno y externo de la organización en relación con el riesgo de Seguridad de la Información y los activos de TI? * ¿Se analizan las políticas de gestión de riesgos de la organización, y se verifica que incluya el establecimiento de la función gestión de riesgos para SIC?   + ¿Se establece claramente el apetito al riesgo y los criterios para tomar decisiones con SIC? * ¿Se evalúa la efectividad de los procesos utilizados para identificar, evaluar, tratar y monitorear los riesgos en SIC (Seguridad de la Información y Comunicaciones)?   + ¿Se verifica si se siguen los procedimientos establecidos para la gestión de riesgos en SIC? * ¿Se evalúan los procesos establecidos para la identificación, evaluación, tratamiento y monitoreo de los riesgos de TI en función de SIC?   + Verifique si la organización evalúa la metodología y criterios para los mecanismos de tratamiento de riesgo, en especial, la aceptación y transferencia al riesgo. * ¿Se establecen plazos definidos para la revisión y actualización de los riesgos identificados? ¿Estos plazos están documentados en los procedimientos, políticas o instructivos?  |  | | --- | | ⚠ El establecimiento de la Tolerancia al Riesgo es crítico en este control. Dada su relevancia, se encuentra separado en el control “Definir la Tolerancia al Riesgo” | |

|  |
| --- |
| 3.2 Temática: Evaluación de las medidas de Control |
| Este control implica un análisis exhaustivo de las medidas implementadas por la organización para mitigar y controlar los riesgos identificados. Esta evaluación tiene como objetivo asegurarse de que las medidas de control sean efectivas, adecuadas y estén alineadas con los riesgos identificados y los objetivos estratégicos de la organización.  Se revisa detalladamente los controles internos y las acciones correctivas establecidas para reducir la probabilidad e impacto de los riesgos identificados. Se examina cómo se han diseñado e implementado estos controles, y si están funcionando de manera efectiva para proteger a la organización de las amenazas y vulnerabilidades que puedan surgir.  Este levantamiento puede incluir análisis específicos tales como:   * Evalué la efectividad de las medidas de control implementadas para mitigar los riesgos.   + Revise si se implementan adecuadamente y se monitorean regularmente en el entorno empresarial o en las decisiones estratégicas.     - ¿Se realiza un monitoreo y seguimiento periódico de la eficacia de los controles implementados? * Evalué la efectividad de los controles internos implementados para gestionar el riesgo.   + ¿Se mantienen los controles internos y los niveles de tolerancia establecidos?   + ¿Los controles son adecuados y se siguen correctamente para evitar desviaciones significativas del apetito de riesgo? |

|  |
| --- |
| 3.3 Temática: Evaluación de los procesos de monitoreo para la gestión |
| El monitoreo efectivo permite identificar cambios en el entorno empresarial y en los riesgos, lo que ayuda a la organización a tomar decisiones informadas y oportunas para proteger sus activos y alcanzar sus objetivos. Se evalúa si la organización tiene mecanismos para identificar riesgos emergentes y si se toman acciones preventivas para abordarlos. Además, se revisan los procesos para abordar y corregir las desviaciones significativas que puedan surgir durante el monitoreo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se analiza el proceso de monitoreo de gestión de riesgo para determinar si se identifican de manera adecuada los riesgos relevantes y si se toman las acciones necesarias?   + Revise si se aplican técnicas apropiadas de revisión y monitoreo para minimizar los falsos positivos (identificación de riesgos que no se materializan) y los falsos negativos (no identificación de riesgos reales). * ¿Se evalúan los resultados obtenidos del monitoreo de la gestión de riesgos y se comparan con los indicadores establecidos? * ¿Los riesgos son detectados y documentados correctamente durante el proceso de monitoreo en la organización? * ¿Se toman las acciones adecuadas para mitigar los riesgos identificados en base a los resultados obtenidos del monitoreo?   + ¿El proceso de monitoreo de gestión de riesgo agrega valor a la organización al identificar oportunidades de mejora y permitir la toma de decisiones informadas? * Revise si se han implementado medidas correctivas y de mejora basadas en los resultados de monitoreo. * ¿Se realiza un monitoreo continuo de los riesgos de TI y los controles implementados?   + ¿Las revisiones periódicas son revisadas, para garantizar que los riesgos y controles sigan siendo relevantes y efectivos en la gestión de riesgos de TI? |

|  |
| --- |
| 3.4 Temática: Evaluación del tratamiento de riesgos |
| Este control se enfoca en revisar cómo la organización implementa las medidas de mitigación y controles para reducir la probabilidad e impacto de los riesgos y asegurarse de que sean efectivos y adecuados para enfrentar los desafíos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se evalúan las políticas y mejores prácticas relacionadas con el tratamiento de riesgos en la organización?   + Revise si las políticas y prácticas están actualizadas y si son consistentes con los estándares y marcos reconocidos en la gestión de riesgos. * ¿Se evalúa la implementación de medidas de tratamiento de riesgos en la organización?   + ¿Se han identificado y evaluado de manera adecuada los riesgos relevantes?   + ¿Se han establecido acciones adecuadas para mitigar los riesgos identificados?   + ¿Las medidas de tratamiento de riesgos implementadas son consistentes con las políticas y directrices establecidas por la organización?   + ¿Las medidas de tratamiento de riesgo están alineadas con el apetito y tolerancia al riesgo?   + ¿Las medidas de tratamiento de riesgo consideran un análisis específico de ciber riesgo? * Revise si las medidas de tratamiento de riesgos siguen los procedimientos y protocolos establecidos por la organización para el tratamiento de riesgos. * ¿Las medidas de tratamiento que requieran mayor nivel de autoridad (tales como aceptación, transferencia o eliminación) han sido documentadas en sus requisitos y condiciones?   + ¿Se solicita autorización formal de la dirección antes de aplicar estas medidas de tratamiento? * ¿Cómo se evalúa la eficacia de las medidas de tratamiento de riesgo implementadas en función de su capacidad para reducir la probabilidad y el impacto de los riesgos?   + Revise si se han logrado los resultados esperados en cuanto al tratamiento de riesgos y si se han evitado o mitigado los riesgos identificados. * ¿Cómo se evalúa el proceso de identificación de riesgos de seguridad de la información (SIC) en la organización?   + ¿Se revisa la efectividad de las metodologías utilizadas para evaluar los riesgos de SIC? * ¿Se revisan los análisis de riesgos y las evaluaciones de impacto asociadas?   + Evalue la calidad y exhaustividad de dichos análisis.   + ¿Se asegura de que se consideren los posibles efectos en la estrategia empresarial durante este proceso de revisión? * ¿Se revisa la incorporación de las consideraciones de riesgo en el proceso de toma de decisiones estratégicas?   + Evalué si los riesgos de SIC se toman en cuenta al evaluar opciones estratégicas y al establecer los objetivos empresariales. * ¿Se ha evaluado de manera exhaustiva si se han identificado los riesgos relacionados con SIC que podrían afectar a la empresa?   + Verifique si se han considerado tanto los riesgos internos como externos, así como las amenazas y vulnerabilidades relevantes. * ¿Se ha evaluado la calidad y el rigor de las evaluaciones de riesgos realizadas?   + Revise si se han utilizado técnicas adecuadas, como análisis cualitativo y cuantitativo, para evaluar los riesgos, a través de métricas, evaluaciones, encuestas, etc. * ¿La dirección ha establecido una tolerancia al riesgo adecuada para las pérdidas relacionadas con SIC?   + Verifique si las actividades de evaluación de riesgos se alinean con esta tolerancia y si se toman medidas correctivas cuando se excede la tolerancia establecida. * ¿Cómo se realiza la evaluación de los riesgos que podrían afectar la continuidad del negocio y cómo se identifican las medidas de mitigación y los planes para la continuidad de negocio relacionados con la seguridad de la información y los activos de TI? |

|  |
| --- |
| 3.5 Temática: Evaluación de los roles y responsabilidades |
| Es una actividad esencial para garantizar que la organización cuente con una estructura clara y eficiente que defina quiénes son los responsables de identificar, evaluar, mitigar y monitorear los riesgos que enfrenta. Durante esta evaluación, se revisa detalladamente la documentación organizacional para identificar los roles y responsabilidades asignados a diferentes niveles jerárquicos y áreas funcionales en relación con la gestión de riesgos. Esto incluye la identificación de los equipos o comités dedicados a la evaluación y seguimiento de riesgos, así como los individuos responsables dentro de cada equipo.   |  | | --- | | ℹ Estas prácticas de auditoría se desarrollan con más profundidad en los controles: Establecer el Proceso de Gestión de Riesgos |   Este levantamiento puede incluir análisis específicos tales como:   * Realice una revisión de los documentos relacionados con el proceso de evaluación de gestión de riesgos, como: políticas, procedimientos y manuales.   + Revise si se ha establecido un procedimiento formal que describa claramente las etapas y responsabilidades involucradas para la evaluación de riesgos. * ¿Se analiza la estructura organizativa para identificar los roles y responsabilidades asignados a la evaluación de la gestión de riesgos?   + Verifique si se han designado responsables claros para llevar a cabo la evaluación de riesgos y si tienen la autoridad, habilidades, capacidad y documentos necesarios. * ¿Se han involucrado las partes interesadas relevantes en el proceso de evaluación de riesgos   + Verifique si se han considerado las perspectivas y opiniones de estas, en la identificación y evaluación de riesgos realizando encuestas o entrevistas. |

|  |
| --- |
| 3.6 Temática: Evaluación de las métricas de la gestión de riesgos |
| Revisar y analizar las medidas y datos utilizados por la organización para cuantificar y monitorear los riesgos identificados. Estas métricas proporcionan información clave para evaluar la efectividad de la gestión de riesgos y la capacidad de la organización para enfrentar los desafíos. Un enfoque basado en métricas permite tomar decisiones informadas y basadas en datos, lo que contribuye a una gestión de riesgos más efectiva y proactiva.  Durante la auditoría, se examina las métricas utilizadas para medir la probabilidad e impacto de los riesgos, así como el rendimiento de las medidas de mitigación implementadas. Se evalúa la relevancia y pertinencia de las métricas para asegurarse de que estén alineadas con los objetivos estratégicos de la organización y reflejen adecuadamente los riesgos específicos a los que se enfrenta. Además, se verifica si las métricas son claras, comprensibles y están definidas de manera coherente en toda la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se evalúan las métricas cuantitativas y cualitativas utilizadas actualmente en el proceso de evaluación de gestión de riesgos?   + Verifique si estas métricas son relevantes, medibles y consistentes con los objetivos y estrategias de la organización.   + Realice una evaluación de la efectividad de las métricas actuales para evaluar las actividades de gestión de riesgos.     - ¿Las métricas actuales están definidas por una metodología específica para la organización?     - ¿Las métricas actuales evitan el uso de estándares globales contenidos como ejemplos en marcos de trabajo? (Y que pueden provocar una sub o sobre estimación del riesgo)     - ¿Las métricas actuales consideran el panorama de amenazas y contexto interno y externo de la organización?   + ¿Estas métricas proporcionan una visión adecuada y precisa del desempeño de la gestión de riesgos?   + ¿Se utilizan métricas específicas para la evaluación de la gestión de riesgos? Algunos ejemplos son:     - Nivel de impacto empresarial inesperado     - Porcentaje de riesgo de SIC que excede la tolerancia al riesgo de la empresa     - Frecuencia de actualización de la evaluación del factor de riesgo * ¿Se identifican áreas donde las métricas existentes pueden mejorarse o donde se requieran nuevas métricas para evaluar de manera más efectiva las actividades de gestión de riesgos?   + Analice las necesidades específicas de la organización y las mejores prácticas en la industria para determinar qué métricas podrían ser más relevantes y útiles.   + Evalúe las nuevas métricas propuestas, para abordar las áreas de mejora identificadas y proporcionar una evaluación más completa y precisa de la gestión de riesgos.   + ¿Se establecen criterios claros y objetivos para medir el desempeño y la efectividad de las actividades de gestión de riesgos? * ¿Se realiza una evaluación de la coherencia y consistencia de las métricas y las formas de evaluar las actividades de gestión de riesgos en diferentes áreas de la organización?   + Revise si se aplican criterios y estándares consistentes en todas las áreas evaluadas. * ¿Se evalúa la existencia de indicadores cuantitativos definidos para evaluar las actividades de revisión y monitoreo del proceso de gestión de riesgo?   + Verifique que estos indicadores son adecuados y medibles, y si están alineados con los objetivos y metas establecidas. * ¿Se revisa durante la auditoría si la organización ha establecido metas cuantitativas específicas para evaluar la efectividad de la gestión de los riesgos de seguridad de la información?   + Evalúe si estas metas son medibles, realistas y están alineadas con los objetivos de la organización. |

|  |
| --- |
| 3.7 Temática: Evaluación de la estrategia de riesgos |
| Implica una revisión detallada y exhaustiva de la estrategia y enfoque adoptado por la organización para gestionar los riesgos a los que se enfrenta. Esta práctica asegura que la organización tenga una estrategia sólida y efectiva que le permita identificar y evaluar los riesgos de manera coherente alineada con sus objetivos estratégicos.  Este levantamiento puede incluir análisis específicos tales como:   * Revise que la estrategia de riesgos en Seguridad de la Información de la organización incluye: objetivos, metas y enfoques utilizados para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información.   + Verifique si están alineadas la estrategia de riesgos en SIC con la estrategia de riesgos de la empresa.   + ¿Contribuye la estrategia de riesgos en SIC a los objetivos y metas de la empresa en su conjunto?     - Verifique que existan instrumentos de planificación estratégica que materialicen el vínculo entre la estrategia de riesgos y la estrategia de la organización, tales como: cascada de metas, mapa estratégico, cuadros de mando. * ¿Se evalúa si el apetito de riesgo en SIC se encuentra por debajo de la capacidad de riesgo de la organización?   + Verifique si el apetito de riesgos en SIC está alineado con el apetito de riesgos de la organización en general. |