

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



**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Dirigir 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. Dirigir la traducción e integración de la estrategia de riesgo de SIC en las prácticas de gestión de riesgos, las actividades operativas y los procesos de gestión de proyectos, cambios y versiones.  2. Dirigir el desarrollo de planes de comunicación de riesgos (que se extiendan a todos los niveles de la empresa como dirección ejecutiva y a otras partes interesadas).   3. Dirigir la implementación de los mecanismos adecuados para responder de forma rápida al cambio de riesgos e informar inmediatamente a los cargos de dirección correspondientes, siguiendo los principios de escalamiento (qué comunicar, cuándo, dónde y cómo).   4. Ordenar que el riesgo, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento. El riesgo debe gestionarse conforme a las políticas y procedimientos publicados y comunicados a los responsables de la toma de decisiones. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Asegurar que el proceso de gestión de riesgos de SIC está alineado con los objetivos empresariales y de seguridad, asegurando que se aborden los riesgos más críticos para la organización.  2. Asegurar la formalización de criterios claros para la evaluación de riesgos, incluyendo la probabilidad de ocurrencia, el impacto potencial y la priorización.  2.1 Establecer, formalizar o aprobar las definiciones clave del proceso de gestión de riesgos, tales como: criterios para determinar la severidad, criterios para la aceptación de riesgos, criterios para la transferencia de riesgos, criterios para la eliminación de riesgos. Mandatar a la organización para que realice los procesos de gestión de riesgo de acuerdo con los criterios establecidos.   2.2 Establecer metodologías de gestión de riesgo documentadas, aprobadas y comunicadas que contengan los principios y definiciones clave para ejecutar el proceso de 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. Establecer un proceso e indicadores a través que proporcione información sobre la idoneidad de las definiciones relativas al riesgo, para determinar si la tolerancia, criterios de aceptación, criterios de transferencia, cálculos de severidad y posición general de la organización frente al riesgo es adecuada o requiere revisión. ***[VER CONTROL: MONITOREAR LA GESTIÓN DE RIESGOS, EVALUAR LA GESTIÓN DE RIESGOS]*** |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Identificar las metas y métricas claves de los procesos de gobierno y gestión de riesgos que deben monitorizarse, y aprobar las estrategias, métodos, técnicas y procesos para capturar y comunicar la información de las mediciones  2. Establecer un plan estratégico de gestión de riesgos de SIC que defina los objetivos, las actividades y los recursos necesarios para su implementación.  3. Implementar un sistema de gestión de riesgos de SIC que proporcione un enfoque estructurado y consistente para la identificación, evaluación, tratamiento y seguimiento de los riesgos. |
| 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. Promover una cultura de aprendizaje y colaboración, donde se compartan experiencias y conocimientos para impulsar la mejora continua en la gestión de riesgos de SIC.  ***[VER CONTROL: MONITOREAR LA GESTIÓN DE RIESGOS, EVALUAR LA GESTIÓN DE RIESGOS]*** |

# Preguntas de Auditoría para Dirigir la Gestión de Riesgos

|  |
| --- |
| 3.1 Temática: Procesos de Gestión de Riesgos |
| El objetivo principal de tener procesos de gestión de riesgos es proporcionar una base sólida para la toma de decisiones informadas. Al contar con una gestión de riesgos bien establecida, la organización puede identificar proactivamente los riesgos potenciales que enfrenta y evaluar su impacto y probabilidad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un plan estratégico de gestión de riesgos de SIC que defina los objetivos, actividades y recursos necesarios para su implementación? ¿Los objetivos del plan están alineados con los objetivos generales de la organización y se centran en la protección de la infraestructura crítica y la mitigación de riesgos? * ¿Se incluyen directrices o instrucciones específicas sobre cómo abordar los riesgos de SIC en los planes y procedimientos utilizados en la gestión de riesgos, las actividades operativas y los procesos de gestión de proyectos, cómo integrar la estrategia de riesgo en estas prácticas? * ¿Existe una comunicación clara y una colaboración estrecha entre los equipos de SIC y los equipos de gestión de proyectos? * ¿Se ofrecen oportunidades de capacitación y desarrollo relacionadas con la gestión de riesgos de SIC? * ¿Se han realizado auditorías internas o externas para evaluar el cumplimiento de la gestión de riesgos de SIC? * ¿Se toman acciones correctivas o preventivas en función de los resultados de las mediciones para mejorar la eficacia de la gestión de riesgos de SIC? * ¿Se asigna una atención especial a los riesgos más críticos y si se les da prioridad en las acciones de mitigación? * El auditor debe buscar la presencia de principios y definiciones clave para ejecutar el proceso de gestión de riesgos y criterios claros y definidos para la evaluación de riesgos. Estos criterios deben incluir:   + Probabilidad de ocurrencia de un evento o incidente   + El impacto potencial que podría tener en la organización La priorización de los riesgos identificados   + Criterios para determinar la severidad   + Criterios para la aceptación de riesgos   + Criterios para la transferencia de riesgos Criterios para la eliminación de riesgos. * ¿Se establece un proceso formal para revisar y evaluar periódicamente las definiciones relativas al riesgo, como la tolerancia, los criterios de aceptación y transferencia, los cálculos de severidad, y la posición general de la organización frente al riesgo? |

|  |
| --- |
| 3.2 Temática: Comunicación de los Riesgos |
| En la gestión de riesgos, el reporte de riesgos es de gran relevancia para la identificación de este, por lo tanto, la organización debe proporcionar canales adecuados de comunicación. El auditor deberá verificar que existan estos canales y su eficiencia dentro del marco de la SIC.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización contempla un plan de comunicación de riesgos que abarque todos los niveles de la empresa y se incluyan a las partes interesadas relevantes, para que cualquier persona pueda identificar y comunicar riesgos, oportunidades, problemas o preocupaciones? * ¿Se llevan a cabo actividades de comunicación periódicas (como reuniones, * informes, boletines informativos, entre otros), para informar a todos los niveles de la empresa sobre los riesgos identificados y las acciones tomadas? * El auditor puede entrevistar a los responsables de la toma de decisiones de la organización sobre los siguientes temas:   + Si están al tanto de los procedimientos establecidos   + Si han recibido reportes de riesgos u otras inquietudes.   + Si consideran que los riesgos se gestionan adecuadamente Si se toman acciones correctivas cuando corresponde. * ¿Se ha comunicado la importancia de seguir los criterios establecidos para la gestión de riesgos?   **3.2.1 Monitoreo y Comunicación de Cambios en los Riesgos**   * ¿Se han establecido sistemas de monitoreo y alerta temprana para detectar cambios en los riesgos? ¿Son eficientes? * ¿El cambio de los riesgos es informado de manera oportuna? |

|  |
| --- |
| 3.3 Temática: Establecimiento de metas y uso de indicadores |
| El objetivo principal del establecimiento de metas y el uso de indicadores en la dirección de la gestión de riesgos es evaluar el desempeño y la efectividad de las estrategias de gestión de riesgos implementadas. Los indicadores proporcionan una medición objetiva del nivel de exposición a los riesgos y de la eficacia de las acciones tomadas para mitigarlos. Esto permite a la organización evaluar si está operando dentro de los límites de tolerancia al riesgo establecidos y si sus estrategias de gestión de riesgos son adecuadas y eficientes para proteger sus activos, reputación y sostenibilidad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Las políticas y procedimientos relacionados con la gestión de riesgos mencionan metas y métricas clave para evaluar el desempeño? * ¿Los indicadores incluyen criterios de aceptación, eficacia de las medidas de mitigación y resultados de evaluaciones de riesgo? * ¿Están los indicadores claramente definidos y alineados con los objetivos de gestión de riesgos de la organización? * ¿Las metas y métricas abarcan aspectos como la efectividad de la identificación y evaluación de riesgos, el cumplimiento de controles y la capacidad de respuesta a incidentes? * ¿Las metas son específicas, medibles, alcanzables, relevantes y con límites de tiempo establecidos? * ¿Se establecen estrategias, métodos y procesos para capturar y comunicar la información de las mediciones? ¿Los mecanismos de medición proporcionan datos precisos y actualizados para evaluar el desempeño de los procesos de gestión de riesgos? |