

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



**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Monitorear la Gestión de Riesgos**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimiento en Gestión de riesgos 2. Conocimiento del Contexto organizacional. 3 - Conocimiento de Controles internos. 3. Conocimiento de Evaluación de Controles. |

# Visión General

Monitorear la gestión de riesgos en la función de seguridad de la información y ciberseguridad (SIC) implica comunicar de manera regular cualquier problema significativo de gestión de riesgos al consejo de administración o al comité ejecutivo y monitorear que el perfil de riesgo, así como las evaluaciones y escenarios, se actualicen y comuniquen adecuadamente. Las metas y métricas clave de rendimiento deben revisarse de manera constante, comparándolas con los objetivos establecidos y, en caso de desviaciones, analizando sus causas para implementar las acciones remediales necesarias. La participación de partes interesadas clave asegura una revisión integral del progreso de la empresa en relación con sus metas de gestión de riesgos.

**1.1 Establecimiento de Procesos y Herramientas para el Monitoreo Eficaz de Riesgos**

Para supervisar de forma eficaz la gestión de riesgos, es fundamental establecer un proceso formal de monitoreo con roles y responsabilidades claramente definidos. Este proceso debe incluir instrumentos formales como cuadros de mando, indicadores clave de rendimiento (KPI), objetivos y resultados clave (OKR), entre otros. Además, supervisar la gestión del perfil de riesgo garantiza que las actividades de SIC se mantengan dentro de los límites de tolerancia y apetito al riesgo, alineando la capacidad de la organización para enfrentar pérdidas con las expectativas de la dirección. Las métricas y los métodos de monitoreo deben ser cuidadosamente definidos y ajustados a los objetivos de la organización, asegurando que aporten al alineamiento de la estrategia de gestión de riesgos, la estrategia de seguridad y los objetivos empresariales.

**1.2 Rol de la Auditoría en el Monitoreo de la Gestión de Riesgos en SIC**

Desde la perspectiva de auditoría, el monitoreo de la gestión de riesgos en SIC implica evaluar la eficacia y precisión de los instrumentos de monitoreo implementados. Los auditores revisan si las métricas de monitoreo, los métodos de cálculo y los umbrales están bien definidos y cumplen con su propósito de apoyar la estrategia de gestión de riesgos. Además, la auditoría asegura que las actividades de monitoreo se alineen con la capacidad de la organización para enfrentar pérdidas relacionadas con SIC y con la tolerancia de riesgo de la dirección. Al proporcionar retroalimentación sobre el desempeño del sistema de monitoreo, la auditoría promueve la mejora continua en la gestión de riesgos, ayudando a la organización a tomar decisiones informadas y a mantener una postura de riesgo adaptada a su entorno y objetivos estratégicos.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Comunicar cualquier problema de gestión de riesgos al consejo de administración o comité ejecutivo.  2. Monitorizar si el perfil, evaluaciones y escenarios de riesgo se actualizan con frecuencia y si los resultados se comunican adecuadamente   3. Monitorizar las metas y métricas clave de rendimiento, de procesos de gobierno y gestión de riesgos contra los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales para solucionar las causas subyacentes.   4. Facilitar la revisión por parte de las partes interesadas clave del progreso de la empresa con respecto a las metas identificadas. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa.  2. Establecer un proceso formal y con responsabilidades definidas para el monitoreo del proceso de gestión de riesgos.   3. Establecer instrumentos formales de monitoreo, tales como: cuadros de mando, esquemas de indicadores, OKR, KPI o instrumentos similares. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Revisar las actividades de monitoreo 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. Evaluar si las métricas de monitorización, su definición, método de cálculo y umbrales están bien definidas, se ajustan a su objetivo y aportan al alineamiento de la estrategia de gestión de riesgo, la estrategia general de seguridad y la estrategia organizacional. |

# Preguntas de Auditoría para Monitorear la Gestión de Riesgos

|  |
| --- |
| 3.1 Temática: Evaluación de la Gestión de Riesgos |
| El proceso de gestión de riesgo debe ser continuamente evaluado en búsqueda de la mejora continua, en particular, asegurar que las estructuras documentales sean las adecuadas y que las partes interesadas relevantes sean participantes activos del proceso de evaluación y mejora de la función de gestión de riesgos de ciberseguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se revisan específicamente las actas de las reuniones del consejo de administración, comité ejecutivo de TI, comité del SGSI o comité ejecutivo de SIC?   + ¿En las actas de las reuniones del consejo o comités se han discutido o mencionado problemas de gestión de riesgos de SIC?   + ¿Se han propuesto actividades para abordar los problemas relacionados con la gestión de riesgos de SIC en las reuniones del consejo de administración o comité ejecutivo? * ¿Qué tipo de informes y documentos se examinan durante la auditoría de gestión de ciber riesgos de la organización?   + ¿Se busca evidencia de informes periódicos o especiales que hayan sido preparados específicamente para el consejo de administración o comité ejecutivo? * ¿Cómo ha respondido el consejo de administración o comité ejecutivo ante los problemas de gestión de riesgos comunicados?   + ¿Se han tomado medidas correctivas como resultado de los problemas de gestión de riesgos identificados?   + ¿Se han asignado recursos adicionales para abordar los problemas de gestión de riesgos identificados? * ¿Realizan entrevistas o consultas con los responsables de la gestión de riesgos para obtener información sobre cómo se supervisa el perfil de riesgo en relación con los umbrales establecidos? * ¿La organización verifica que métodos se utilizan para supervisar el perfil de riesgo en la organización, y que estos sean adecuados, consideren las perspectivas de riesgos, panoramas de amenazas e información del contexto necesario para una toma de decisión informada?   + ¿Con qué frecuencia se lleva a cabo la supervisión del perfil de riesgo? * ¿Se ha establecido un mecanismo para evaluar el cumplimiento de los umbrales de tolerancia y apetito de riesgo? ¿Se examinan y generan informes periódicos que muestren el grado de cumplimiento? Además, ¿se toman acciones correctivas cuando se superan los umbrales establecidos?   **3.1.2 Evaluación del Perfil de Riesgos**   * ¿Se examina la documentación relacionada con el perfil de riesgo de la organización, las evaluaciones de riesgo y los escenarios de riesgo?   + ¿Se verifica si se han realizado actualizaciones periódicas o si existen indicadores que demuestren revisiones regulares?   + ¿Se buscan registros de fechas de actualización y evidencia de los cambios realizados? * ¿Cómo se comunican los resultados de las evaluaciones de riesgo y los escenarios de riesgo * ¿Se utilizan informes claros y comprensibles, y se proporciona información detallada sobre los riesgos identificados, su probabilidad, impacto y cualquier acción de mitigación propuesta? * ¿Se analizan los informes y registros que demuestren el seguimiento del perfil de riesgo en relación con los umbrales de tolerancia y apetito de riesgo? ¿Se busca evidencia de monitoreo regular y comparaciones entre el perfil de riesgo actual y los umbrales establecidos? |

|  |
| --- |
| 3.2 Temática: Monitoreo de Riesgos. |
| Este control se centra en verificar que se estén implementando adecuadamente las medidas de seguimiento y control para mantener bajo vigilancia constante los riesgos identificados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se observa la estructura organizativa de la empresa durante la auditoría de gestión de riesgos?   + Verifique si se realiza la asignación de roles y responsabilidades en el proceso de monitoreo del proceso de gestión de riesgos. * ¿Se implementaron acciones remediales propuestas para abordar los riesgos identificados?   + Evalué la efectividad de las acciones remediales implementadas en la solución de las causas subyacentes de los riesgos, por ejemplo, a través del cambio en los riesgos inherentes y residuales; y los cambios en los análisis BIA.   + Examine si se establecieron mecanismos para monitorear la efectividad de las acciones remediales a lo largo del tiempo, tales como: tableros de control, indicadores KRO, KPI   + Revise si existe un seguimiento continuo para evaluar la eficacia de las acciones remediales en el manejo de los riesgos en el transcurso del tiempo. * Revise el proceso de las entrevistas o consultas con los responsables designados para el monitoreo del proceso de gestión de riesgos.   + ¿Qué tipo de preguntas se realizan para indagar sobre sus roles, responsabilidades y las actividades específicas que realizan para monitorear el proceso de gestión de riesgos?   + ¿Son contingentes, precias y realizadas por un experto con conocimiento del tema, que pueda usar un lenguaje técnico suficiente? * Examine los documentos organizacionales, manuales de gestión o políticas que están relacionados con el monitoreo y la gestión del desempeño dentro de la organización.   + Revise la información que proporcionan estos documentos y si se han establecido instrumentos formales de monitoreo en la organización. * Realice el levantamiento de información sobre los instrumentos de monitoreo utilizados en la empresa.   + Revise si se aplican en la organización al realizar preguntas o consultas a los responsables de la gestión de riesgos o de la planificación estratégica. * ¿Qué aspectos específicos se analizan para evaluar si se han implementado medidas correctivas o preventivas para abordar los riesgos identificados?   + ¿Las acciones tomadas reflejan una consideración adecuada de la capacidad y tolerancia de la empresa frente a los riesgos?   + Revise si la dirección ha tomado acciones oportunas y adecuadas para responder a los informes de monitoreo de riesgos. |

|  |
| --- |
| 3.3 Temática: Métricas para el Monitoreo de Riesgos. |
| El propósito de este control es asegurar que las métricas seleccionadas sean adecuadas, relevantes y efectivas para evaluar la exposición de la organización a los riesgos y la eficacia de las medidas de mitigación implementadas. Se evalúa si las métricas seleccionadas son apropiadas y relevantes para la naturaleza de los riesgos de la organización y si proporcionan información significativa para la toma de decisiones, analizar si las métricas son relevantes para los objetivos estratégicos de la organización y si reflejan los riesgos críticos que enfrenta la empresa.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se examina la documentación relacionada con los procesos de gobierno y gestión de riesgos de la organización?   + ¿Se verifica si se establecen metas y métricas clave de rendimiento? ¿Y se documenta adecuadamente el proceso de monitorización y análisis de esas metas y métricas?   + ¿Se utilizan métricas relevantes para el monitoreo de riesgos? Por ejemplo:     - Número de áreas potenciales de riesgo de SIC identificadas y gestionadas     - Porcentaje de riesgo crítico que ha sido mitigado efectivamente     - Porcentaje de planes de acción de riesgo de SIC ejecutados a tiempo * ¿Se analizan los informes y registros que muestran el seguimiento de las metas y métricas clave de rendimiento? ¿Se busca evidencia de análisis de desviaciones y acciones remediales implementadas para abordar las causas subyacentes? * ¿Se analizan los informes periódicos, presentaciones de rendimiento u otros documentos similares generados en la organización?   + ¿Qué tipo de indicadores clave y resultados medibles se incluyen comúnmente en estos informes que demuestren el uso de instrumentos formales de monitoreo? * ¿Se ha determinado y documentado cual es el propósito de examinar la documentación relacionada con la gestión de riesgos, la seguridad y la estrategia organizacional?   + Verifique si la organización comprende qué se busca específicamente en esta revisión en cuanto a las métricas de monitorización, su descripción en términos de definición, método de cálculo y umbrales establecidos. * ¿Cómo se analiza la contribución de las métricas de monitorización al alineamiento de la estrategia de gestión de riesgos, la estrategia general de seguridad y la estrategia organizacional?   + ¿Se comparan los objetivos y metas establecidos en cada estrategia con las métricas definidas y se determina si existe coherencia y congruencia entre ellas? * ¿Se evalúa si las métricas proporcionan información relevante y significativa para la gestión de riesgos y la seguridad de la infraestructura crítica? ¿Se considera si las métricas permiten evaluar el rendimiento, detectar tendencias, identificar áreas de mejora y tomar decisiones informadas? |