

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



**CASIG 1 – Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Monitorear la Gestión de Recursos**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Entendimiento profundo de las tecnologías, prácticas y tendencias en ciberseguridad. 2. Experiencia en Inversiones y Finanzas 3. Comprender los principios de gestión financiera y aplicar métodos de valoración. 4. Capacidad para analizar datos complejos, identificar patrones, evaluar riesgos y oportunidades, y hacer recomendaciones basadas en un análisis sólido. 5. Conocimiento de las leyes, regulaciones y estándares aplicables en la industria, especialmente aquellas relacionadas con la ciberseguridad y la protección de datos. |

# Visión General

Monitorear la gestión de recursos en la función de seguridad de la información y ciberseguridad (SIC) incluye la definición de un conjunto equilibrado de objetivos, métricas, metas y benchmarks que permitan medir tanto la actividad como los resultados alcanzados. Al colaborar con TI y otras funciones empresariales, así como con las partes interesadas clave, las métricas se ajustan para reflejar indicadores financieros y no financieros, proporcionando una visión integral y precisa del rendimiento de los recursos. Este proceso de monitoreo facilita la evaluación de progreso en la entrega de valor en comparación con los objetivos establecidos.

**1.1 Procedimientos y Análisis de la Gestión de Recursos en SIC**

Para monitorear de manera efectiva los recursos asignados a SIC, es crucial desarrollar y documentar procesos específicos que incluyan la recopilación de datos relevantes y actualizados sobre el desempeño de los activos. Esto abarca la creación de un sistema robusto de gestión de datos que facilite la recolección, almacenamiento y análisis de información relevante, y la elaboración de informes regulares de rendimiento del portafolio de recursos de SIC. A partir de estos informes, se identifican las áreas que requieren mejoras, y se implementan acciones correctivas que aseguren la optimización de valor en los recursos. El análisis comparativo y de tendencias permite identificar patrones y oportunidades de mejora sostenida, proporcionando un marco que apoya la toma de decisiones y asegura la entrega de valor en alineación con los objetivos de la organización.

**1.2 Rol de la Auditoría en el Monitoreo y Optimización de la Gestión de Recursos**

Desde la perspectiva de auditoría, el monitoreo de la gestión de recursos en SIC implica una revisión exhaustiva de los procesos y sistemas utilizados para gestionar los activos, evaluando su conformidad con las mejores prácticas y su alineación con los objetivos empresariales. La auditoría verifica la efectividad de los procesos de recopilación y análisis de datos, así como de los sistemas de monitoreo y mejora continua basados en los resultados. Además, se realizan análisis cuantitativos detallados para medir el impacto de las acciones de mejora implementadas y se emplean técnicas avanzadas de análisis de datos para identificar patrones y tendencias. Este enfoque de revisión y mejora continua basado en datos permite optimizar la valoración de los activos y recursos asignados a SIC, asegurando que contribuyan de manera efectiva al cumplimiento de los objetivos estratégicos y al crecimiento sostenido 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. Definir un conjunto equilibrado de objetivos, métricas, metas y benchmarks. Las métricas deberían cubrir mediciones de actividad y resultados, incluyendo indicadores de avance y de retraso, rendimiento y puntos de referencia, así como un equilibrio adecuado entre mediciones financieras y no financieras. Revisar y acordar con TI y otras funciones de la empresa, así como con otras partes interesadas relevantes.   2. Recopilar datos relevantes, oportunos, completos, creíbles y precisos para informar sobre el progreso a la hora de la entrega de valor en comparación con los objetivos. Obtener una vista resumen general de 360º del rendimiento del portafolio , programa y de SIC (capacidades técnicas y operativas) que respalden la toma de decisiones. Asegurar el logro de los resultados esperados.   3. Obtener informes regulares y relevantes de rendimiento del portafolio , programa y de SIC (tecnológicos y funcionales). Revisar el progreso de la empresa a la hora de identificar metas y el grado de realización de los objetivos planificados, los entregables obtenidos, los objetivos de desempeño alcanzados y el riesgo mitigado. Los objetivos estratégicos se logran en lugar de cambiar o no se cumplen   4. Realice un seguimiento de los resultados de las iniciativas de seguridad de la información y compárelos con las expectativas para garantizar la entrega de valor frente a los objetivos comerciales. Tomar las medidas de gestión adecuadas según sea necesario. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Desarrollar y documentar procesos y procedimientos para el monitoreo efectivo de los activos y recursos asignados a la función de SIC.  2. Documentar y comunicar los hallazgos del monitoreo y las áreas que requieren mejoras o cambios en la optimización del valor de los activos y recursos.  2.1. Una vez revisados los informes, asegurar que se ha iniciado y controlado acciones correctivas al área de gestión pertinente.   2.2. Una vez revisados los informes, llevar a cabo la acción de gestión adecuada para asegurar la optimización del valor. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Establecer un plan de monitoreo a largo plazo que abarque los activos y recursos asignados a la función de SIC.  2. Implementar un sistema de gestión de datos robusto para recopilar, almacenar y analizar información relevante sobre el desempeño y la optimización del valor de los activos y recursos.  3. Realizar análisis comparativos y tendencias para identificar patrones y oportunidades de mejora sostenida en la optimización del valor de los activos y recursos. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1.Realizar análisis cuantitativos y comparativos detallados para medir el impacto de las acciones de mejora implementadas en la optimización del valor de los activos y recursos.  2. Implementar técnicas avanzadas de análisis de datos para obtener una comprensión más profunda de los patrones y tendencias relacionados con la optimización del valor de los activos y recursos. |
| 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. Mejorar continuamente los procesos y sistemas de monitoreo basados en los resultados de las auditorías y los análisis cuantitativos.  2. Establecer un sistema de revisión y mejora continua basado en datos y resultados para impulsar la optimización de la valoración de los activos y recursos asignados a la función de SIC. |

1. **Preguntas de Auditoría para Monitorear la Gestión de Recursos**

|  |
| --- |
| 3.1 Temática: Revisión de la estrategia, objetivos y métricas de la SIC |
| La importancia de este proceso radica en su capacidad para proporcionar información en tiempo real sobre el rendimiento de la organización. Al monitorear constantemente los KPIs y métricas relevantes, los líderes pueden tomar decisiones informadas y ágiles para abordar desafíos y aprovechar oportunidades.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación clara sobre el proceso de monitorización del rendimiento y priorización de recursos? * ¿Se establecen metas y objetivos claros para los recursos asignados y se monitorea su rendimiento? * ¿Se establece que se mantenga un monitoreo regular y periódico del rendimiento de los recursos asignados? * ¿Se establece que se analicen las desviaciones del rendimiento en relación con los objetivos y se toman acciones correctivas?   **3.1.1 Auditar el proceso de supervisión de asignación y optimización de recursos**  El proceso de supervisión busca identificar posibles ineficiencias en la asignación de recursos y tomar acciones correctivas para mejorar la eficacia y productividad de la organización. Al analizar cómo se están utilizando los recursos, se pueden identificar áreas donde se están desperdiciando recursos o donde existe un desequilibrio en la distribución de estos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación clara sobre el proceso de supervisión de la asignación y optimización de recursos? * ¿Se establecen metas y métricas acordadas para evaluar el rendimiento y eficiencia en el uso de recursos? * ¿El proceso de asignación de recursos considera objetivos y prioridades establecidas? * ¿Se utilizan metas y métricas acordadas para guiar la asignación y optimización de recursos?   **3.1.2 Auditar el proceso de supervisión de estrategias de abastecimiento y arquitectura empresarial**  Mantener una supervisión de estrategias de abastecimiento y arquitectura empresarial es esencial para garantizar la gestión eficiente de recursos, la alineación estratégica y la competitividad de la organización. Proporciona una visión integral de los procesos de abastecimiento y la estructura organizacional, permitiendo identificar oportunidades de mejora y tomar decisiones informadas para asegurar el éxito y la sostenibilidad en el mercado.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación clara sobre el proceso de supervisión de las estrategias de abastecimiento y arquitectura empresarial? * ¿Las estrategias de abastecimiento y arquitectura se alinean adecuadamente con los objetivos actuales y futuros de la empresa? * ¿Se realiza una evaluación regular de las capacidades y recursos empresariales y de TI? * ¿Se desarrollan estrategias para abordar brechas y satisfacer necesidades actuales y futuras?   **3.1.3 Auditar el proceso de monitorización del rendimiento y priorización de recursos**  La importancia de este proceso radica en su capacidad para proporcionar  información en tiempo real sobre el rendimiento de la organización. Al monitorear constantemente los KPIs y métricas relevantes, los líderes pueden tomar decisiones informadas y ágiles para abordar desafíos y aprovechar oportunidades.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación clara sobre el proceso de monitorización del rendimiento y priorización de recursos? * ¿Se establecen metas y objetivos claros para los recursos asignados y se monitorea su rendimiento? * ¿Se establece que se mantenga un monitoreo regular y periódico del rendimiento de los recursos asignados? * ¿Se establece que se analicen las desviaciones del rendimiento en relación a los objetivos y se toman acciones correctivas? |

|  |
| --- |
| 3.2 Temática: Rendimiento de la optimización de los recursos |
| La importancia de este proceso radica en su capacidad para evaluar de manera continua cómo se están utilizando los recursos y cómo pueden mejorarse para maximizar su impacto. Mediante la revisión y el análisis detallado de los recursos financieros, tecnológicos y humanos, la organización puede identificar oportunidades para reducir costos innecesarios, eliminar redundancias y realinear los esfuerzos en áreas de mayor prioridad y valor.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación clara sobre el proceso de revisión y análisis periódico de recursos? * ¿Se involucran activamente las partes interesadas pertinentes en el proceso de revisión y análisis? * ¿Se realizan seguimientos regulares de metas cuantitativas específicas y se llevan a cabo revisiones periódicas? * ¿Se implementan acciones correctivas en respuesta a hallazgos y se realiza mejora continua?   **3.2.1 – Integración de sistemas para la recopilación de datos**  La recopilación de datos de diversas fuentes, como sistemas internos, aplicaciones, sensores o plataformas externas, es una práctica común en las organizaciones para obtener una visión holística de sus operaciones y clientes. La integración de estos sistemas permite unificar y centralizar la información, evitando la duplicación de esfuerzos y garantizando la precisión y consistencia de los datos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Los sistemas utilizados permiten la recopilación y registro de datos relevantes sobre la utilización de recursos y el cumplimiento de objetivos? * ¿Los datos están disponibles en un sistema único o son fácilmente accesibles desde diferentes fuentes? * ¿Existe una conexión clara entre las necesidades empresariales y decisiones de abastecimiento y arquitectura?   **3.2.2 – Documentación y comunicación de hallazgos**  La documentación adecuada de los hallazgos obtenidos durante el análisis de recursos permite registrar de manera clara y detallada los resultados obtenidos, las conclusiones alcanzadas y las recomendaciones propuestas. Esto asegura que la información recopilada sea fácilmente accesible para todos los miembros del equipo y la dirección, lo que facilita la colaboración y la alineación en torno a los objetivos de optimización de recursos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen registros documentados de los hallazgos identificados durante la monitorización de recursos? * ¿Se comunican los hallazgos de manera adecuada a las partes interesadas? * ¿Se implementan acciones correctivas en base a los hallazgos de auditorías y análisis?   **3.2.3 – Seguimiento y análisis de metas y objetivos**  En el ámbito de la optimización de recursos, el seguimiento y análisis de metas y objetivos es de suma importancia para evaluar el progreso de la organización hacia sus metas estratégicas y asegurar un uso eficiente de los recursos. Establecer metas y objetivos claros es fundamental para dirigir los esfuerzos de la organización hacia resultados específicos y medibles.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza un seguimiento regular de metas cuantitativas específicas y se llevan a cabo revisiones periódicas de avances? * ¿Los informes proporcionan información clara y actualizada sobre la utilización de recursos asignados? * ¿Se analizan las brechas entre resultados actuales y metas establecidas?   **3.2.3 – Mejora Continua y Acciones Correctivas**  La mejora continua implica un enfoque constante en identificar oportunidades de optimización en el uso de los recursos de la organización. Al adoptar una mentalidad de mejora continua, la organización puede adaptarse rápidamente a los cambios del entorno empresarial y mantenerse competitiva en un mercado en constante evolución.    Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un ciclo de mejora continua implementado en la función de SIC? * ¿Se implementan acciones correctivas en base a hallazgos y se establecen planes de acción? * ¿Se documentan las mejoras realizadas en base a revisiones y se realiza seguimiento a su implementación? |